UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS.

INFLUENCIA DEL USO DE UNA RED PRIVADA VIRTUAL A TRAVÉS DE UN MPLS EN LA INTERCONEXION Y EL ACCESO A LA INFORMACIÓN EN TIEMPO REAL DE LAS NOTARÍAS DEL DISTRITO DE CAJAMARCA, BAÑOS DEL INCA Y EL COLEGIO DE NOTARIOS.

Carlos Alberto León Ortiz

Asesora:

Mg. Diana Jakelin Cruzado Vásquez

Cajamarca- Perú

DICIEMBRE – 2020

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

Facultad de Ingeniería

Escuela Profesional de Ingeniería Informática y de Sistemas.

INFLUENCIA DEL USO DE UNA RED PRIVADA VIRTUAL A TRAVÉS DE UN MPLS EN LA INTERCONEXION Y EL ACCESO A LA INFORMACIÓN EN TIEMPO REAL DE LAS NOTARÍAS DEL DISTRITO DE CAJAMARCA, BAÑOS DEL INCA Y EL COLEGIO DE NOTARIOS.

Tesis presentada en cumplimiento parcial de los requerimientos para optar el Título Profesional de Ingeniero Informático y de Sistemas.

Bach. Carlos Alberto León Ortiz

Asesor: Mg. Diana Jakelin Cruzado Vásquez

Cajamarca- Perú

DICIEMBRE – 2020

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

APROBACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO INFORMÁTICO Y DE SISTEMAS

INFLUENCIA DEL USO DE UNA RED PRIVADA VIRTUAL A TRAVÉS DE UN MPLS EN LA INTERCONEXION Y EL ACCESO A LA INFORMACIÓN EN TIEMPO REAL DE LAS NOTARÍAS DEL DISTRITO DE CAJAMARCA, BAÑOS DEL INCA Y EL COLEGIO DE NOTARIOS.

Presidente: _____

Secretario: _____

Vocal: _____

Asesor: _____

DEDICATORIA

A:

A Dios por haberme dado fuerzas para seguir adelante, a mis padres Pedro y Teresa quienes siempre me brindaron su apoyo y amor incondicionalmente; a mi esposa Nataly, por el cariño, amor y comprensión , al pilar más grande de mi vida Ian a mi sobrina Evolet que es quien es mi motivación e inspiración para poder superarme cada día más; a mis hermanos Teresa, Pedro y Ana Maria, quienes siempre han estado a mi lado ofreciéndome su apoyo diario, a mi Mami Riti por haberme orientado por la senda apropiada sin dudar ni un momento de mí; a mis cuñados Jaime y Astrid por haberme brindado los virtuosos consejos día a día y a todos ustedes que siempre me brindaron su apoyo y sabiduría en cada año de mi carrera Universitaria.

AGRADECIMIENTOS

- A la UPAGU y docentes, por los conocimientos vertidos para adjudicar mi formación profesional.
- Familiares, amigos de la infancia y de la universidad, por todo el apoyo, cariño y aprecio demostrado en cada momento.

RESUMEN

El presente trabajo tiene como propósito el determinar la influencia de la simulación del uso de una RPV a través de un MPLS sobre la interconexión y acceso a la información en tiempo real, dimensionado por el tiempo de latencia entre las notarías del distrito de Cajamarca y Baños del Inca y el colegio de notarios.

La metodología aplicada es de tipo básico, descriptivo correlacional cuantitativo, además de ser un estudio transversal cuasi – experimental.

Como principales resultados que se obtuvieron fueron la configuración de la estructura básica de ATM MPLS empleando el área 0 del Open Shortest Path First (OSPF) así como el Interior Gateway Protocol (IGP). Configuramos dos diferentes VPN mediante la estructura básica. Primero aplicaciones VPN RASGAN tomado como límite del cliente al Routing Protocol del límite del proveedor (CE-PE); el segundo VPN emplea el BGP como su Routing Protocol PE-CE. Luego se configuró diversos loopback y Static rutas en el Routers CE para poder simular la disposición de otro Routers y redes.

La simulación con la estructuración la topología de la red de acuerdo a la distribución geográfica, se realizó descomponiendo en una estructura mínima para la configuración de la tecnología VPN (MPLS), donde se subnetearon en las notarías y el Colegio de Notarios. Se desarrolló el armado físico de la topología, se le asignaron los IPS y se configuró la tecnología RPV (MPLS). La simulación se ejecutó con la petición de data de la notaria 1 a la PC3 de Colegio de Notarios y viceversa con el mensaje de retorno, donde se ejecutó de forma exitosa. Se aplicó pruebas pre prueba y post prueba, de los KPI´s de tiempo de latencia con 24 pruebas. Siendo el tiempo promedio de latencia fue de 1183.25 milisegundos sin la aplicación del sistema y con el sistema

propuesto el tiempo de latencia se reduce de hasta 9.21 milisegundos.

Las conclusiones fueron: el diseño y pruebas de simulación en la aplicación de RPV por medio de un MPLS Packet Tracer, interconectando a las notarías y el Colegio de Notarios de Cajamarca., introduciendo paradigmas completamente nuevos, sin analogías directas con las redes físicas existentes; Introducción de RPV en las redes públicas existentes, lo que aminora esfuerzos en la creación de estándares y el flujo de información en ambos sentidos; La creación de RPV es una solución flexible a bajo costo con datos fluidos con intercambio de información confidencial, integra, segura y veloz, evitando otros costos altos en la implementación de otro tipo de redes que cumplan los mismos objetivos; La simulación de la RPV fue satisfactoria, afirmando que las VPN son una alternativa de solución, la cual accede a una topología de red centralizada entre las notarías y el Colegio de Notarios; en la red se accede a los recursos TI en tiempo real, lo que nos permite disponer de la información requerida en el breve plazo de envío y poder desarrollar las actividades notariales eficientemente en menores tiempos y costes.

Palabras clave: Redes Privadas Virtuales (VPN), Multiprotocol Label Switching (MPLS), enlace de información, interconexión de notarías y Colegio de Notarios de Cajamarca.

ABSTRACT

The purpose of this work is to determine the influence of the simulation of the use of a VPN through an MPLS on the interconnection and access to information in real time, measured by the latency time between the notaries of the Cajamarca district and Baños del Inca and the college of notaries.

The applied methodology is basic, descriptive, correlational, quantitative, as well as being a quasi-experimental cross-sectional study.

The applied methodology is basic, descriptive, correlational, quantitative, as well as being a quasi-experimental cross-sectional study.

The main results that were obtained were the configuration of the basic ATM MPLS structure using area 0 of the Open Shortest Path First (OSPF) as well as the Interior Gateway Protocol (IGP). We configure two different VPNs using the basic structure. First RASGAN VPN applications taken as client boundary to provider boundary Routing Protocol (CE-PE); the second VPN uses BGP as its PE-CE routing protocol. Then various loopback and static routes were configured in the CE routers to be able to simulate the layout of other routers and networks.

The simulation with the structuring of the network topology according to the geographical distribution, was carried out breaking down into a minimum structure for the configuration of the VPN technology (MPLS), where they were subnetted in the notaries and the Notaries Association. The physical assembly of the topology was developed, the IPSs were assigned and the VPN technology (MPLS) was configured. The simulation was executed with the request for data from the notary 1 to the PC3 of the Colegio de Notarios and vice versa with the return message, where it was executed successfully. Pre-test and post-test tests of the latency time KPIs with 24 tests were

applied. Being the average latency time was 1183.25 without the application of the system and with the proposed system the latency time is reduced to 9.21 milliseconds.

The conclusions are that the design and simulation tests were made in the application of RPV through an MPLS Packet Tracer, interconnecting the notaries and the Cajamarca Notaries Association, introducing completely new paradigms, without direct analogies with physical networks. existing. Introduction of VPN in existing public networks, which reduces efforts in the creation of standards and the flow of information in both directions. The creation of VPN is a flexible, low-cost solution with fluid data with confidential, integrated, secure and fast information exchange, avoiding other high costs in the implementation of other types of networks that meet the same objectives. The RPV simulation was successful. Affirming that VPNs are an alternative solution, which accesses a centralized network topology between notaries and the College of Notaries; IT resources are accessed on the network in real time, which allows us to have the required information in the short delivery time and to carry out notarial activities efficiently in less time and costs.

Keywords: Virtual Private Networks (VPN), Multiprotocol Label Switching (MPLS), information link, interconnection of notaries and Cajamarca Notaries Association.

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

LISTA DE ABREVIATURAS

- 3DES : Triple Data Encryption Standard
- AD : Active Directory
- LAN : Local Area Network
- MPLS : Multiprotocol Label Switching
- OSI : Open System Interconnection.
- VPN : Virtual Private Network.
- WAN : Wide Area Nework

CAPÍTULO I: INTRODUCCIÓN

1.1. El problema de investigación

1.1.1. *Planeamiento* del Problema de Investigación

En la actualidad, el crecimiento exponencial de los diferentes mercados globales, tienen la necesidad de apoyarse en sistemas tecnológicos para buscar oportunidades, competitividad y posicionamiento en su entorno.

Teniendo como ejemplo a la Empresa Eléctrica Quito S.A., la cual se halla mejorando y manteniendo en constante evolución los sistemas de seguridad y protección de su red, diseñando Redes Privadas Virtuales, partiendo del análisis en el espacio virtual existente, obteniendo varios beneficios como nuevos servicios de conectividad, transporte de datos, etc. (Hidalgo & Díaz, 2010).

En el Perú, el sector empresarial público y privado que desarrollan diversas actividades productivas en diversos rubros enfrentadas a un mercado competitivo van desarrollando tecnologías e implementando sistemas informáticos alcanzando sinergias con otras organizaciones, confidencialidad de la información, integridad de los datos, autenticación y autorización, velocidad, costos, etc. Sin embargo, en Cajamarca, hay sectores de servicios que todavía no aplican tecnologías digitales.

Un caso específico de ello son las notarías de los distritos de Cajamarca (6) y Baños del Inca (2) respectivamente, son ajenas a este tipo de tecnología y este proceso se lleva a cabo mediante archivos notariales físicos, la demora para la entrega de documentos es de 24 horas a 36 horas y solo lo tiene que realizar personalmente el notario que solicitó dicha información generando una gran pérdida de recursos (dinero, clientes, tiempo). Es decir, se hace necesario usar la tecnología que facilite una gestión eficiente de dicha información.

Para las actividades comunes y que se realizan con frecuencia, los notarios buscan comunicarse en tiempo real para la obtención de una información precisa y detallada, esto conlleva a la pérdida de tiempo y recursos físicos, ya que actualmente se realiza personalmente. En este contexto, la información está vulnerable, ya que estos archivos se ven expuestos físicamente, originando en algunas ocasiones confusión y mal servicio al usuario. Una solución tecnológica al citado problema sería diseñar una Red Privada Virtual (VPN) con la interacción de un MPLS y poder ingresar a la data requerida en tiempo real en las notarías en el Distrito de Cajamarca, Baños del Inca y Colegio de Notarios de Cajamarca.

1.1.2. Formulación del problema

¿Cuál sería la influencia de la simulación de una red privada virtual a través de un MPLS sobre la interconexión en tiempo real entre las notarías del distrito de Cajamarca, Baños del Inca y el Colegio de Notarios de Cajamarca?

1.1.3. Justificación del problema de investigación

- **Justificación Teórica:**

  Se justifica ya que, los aportes permitirán la posibilidad de ampliar el marco referencial sobre las teorías y el uso de las redes privadas virtual sitio a sitio, sus principales beneficios en la gestión empresarial y el entorno organizacional e inclusive a tufuro la interconexión seria no solo con el Colegio de Notarios, también con el Ministerio Publico y/o el Poder Judicial y a nivel nacional.

- **Justificación Práctica:**

  Se justifica ya que se elaborará para dar solución a problemas en trámites documentarios, duplicidad de funciones, flujo de documentos virtuales, racionalización de recursos, mejora del medio ambiente al evitar el mayor uso de papel, etc.

- **Justificación Metodológica:**

  Desde esta perspectiva la investigación es relevante porque puede ser sometida a validez y confiabilidad debido al rigor de la metodología científica. Asimismo, se utilizará como guía metodológica formales para diseñar redes privadas virtual sitio a sitio en las organizaciones constituyéndose de esta manera en un modelo que puede servir como

antecedente para otras investigaciones o aplicarlo a situaciones similares en contextos diferentes.

1.2. Objetivos de la investigación

1.2.1. Objetivo general

Determinar la influencia de la simulación del uso de una RPV a través de un MPLS sobre la interconexión y acceso a la información en tiempo real, dimensionado por el tiempo de latencia entre las notarías del distrito de Cajamarca y Baños del Inca y el colegio de notarios.

1.2.2. Objetivos específicos

- Diseñar un modelo de una red privada virtual a través de un MPLS packet tracer de interconexión notarial del distrito de Cajamarca y Baños del Inca.
- Elaborar un esquema de simulación para la demostración del funcionamiento de la integración de las notarías y el colegio de notarios.
- Determinar la interconexión y acceso a la información antes y después del uso de la simulación del uso de una RPV a través de un MPLS, comprobado por tiempo de latencia.

1.3. Hipótesis de la investigación

1.3.1. Hipótesis general

El uso de una RPV a través de un MPLS influye directamente sobre la interconexión y acceso a la información en tiempo real de las notarías en el distrito de Cajamarca y Baños del Inca con el colegio de notarios.

1.4. Operacionalización de las variables

Tabla 1. *Operacionalización de las variables*

Variable	Definición Conceptual.	Dimensiones	Indicadores	Instrumento
VARIABLE 01 Uso de una Red Privada Virtual a través de un MPLS	"Son un tipo de red de comunicaciones que se construye sobre otra ya existente. La característica fundamental es que permite que distintos equipos en diversas partes del mundo puedan comunicarse al igual que una red tópica" (González, L., De fuentes, J & Romero, G, 2014, p. 68).	Red privada virtual a través de una MPLS	1. Elaborar un diseño en Packet Tracer	Análisis documental de la VPN. Guias de observación y fichas de registro de datos.
VARIABLE 02 Interconexión y el acceso a la Información En Tiempo Real.	"Integrar el flujo de información de empresas (notarias, colegio de notarios), empleados y generar una interacción. (CIO data center services, 2019).	Transferencia de datos por la RPV	1. Tiempo de latencia. 2. N° saltos recorridos de información origen – destino. 3. Tiempo de carga del sistema informático	

Fuente: Elaboración propia.

1.5. Limitaciones de la investigación

Debido a la emergencia sanitaria que el mundo se encuentra atravesando, el gobierno de nuestro país ha dictaminado una serie de procedimientos y acciones que las empresas deben tomar, por resolución ministerial N° 0135-2020-JUS, del 15 de mayo del 2020, a fin de resguardar la salud de sus colaboradores y clientes. Las notaría son ajenas a tales mandatos y han adoptado diversos procedimientos que incluyen el Protocolo sanitario ante el COVID-19 del servicio notarial, donde los oficios notariales se dan por citas a los interesados en hora y fecha determinada sólo para diligencias notariales a fin de evitar aglomeraciones que pongan en riesgo la seguridad sanitaria, teniendo en cuenta el distanciamiento social de 2 metros en la recepción y atención, de igual manera los ambientes ventilados. En el título II de medidas de cumplimiento obligatorio por parte de los usuarios, dice que solo se le permite el acceso al usuario sólo por trámite.

Por las disposiciones de bioseguridad, distanciamiento social y demás normas dictadas por la presencia del COVID 19, no se pudo realizar la presentación del uso de una red privada virtual a través de un MPLS en la interconexión y el acceso a la información en tiempo real de las notarías del distrito de Cajamarca, Baños del Inca y el Colegio de Notarios.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

Peña (2016), en su tesis de grado titulada: "Diseño e implementación de una Red Privada Virtual (RPV-SSL) utilizando el método de autenticación LDAP. Realizada en la Universidad Central de Venezuela, Caracas, Venezuela, siendo su objetivo implementar una RPV-SSL integrada con LDAP en la Organización, permitió ofrecer movilidad, garantías de entereza, privacidad y seguridad de los datos, reducir los costos en la implementación, y lo más importante, permitir a los clientes y consultores externos conectarse desde cualquier ubicación geográfica de forma segura ante cualquier evento que se pueda presentar en el país. Siendo sus conclusiones la implementación de VPN-SSL integrada con LDAP lo cual produjo en la organización accesos a movilidad, integridad y confidencialidad, seguridad de datos y reducción de gastos de implementación, así como la interconexión desde cualquier punto del país, garantizando la continuidad del negocio por medio del internet si requerir estar físicamente en las oficinas. Asimismo concluyo la integración de la VPN-SSL y el protocolo LDAP que aporta la seguridad del uso de credenciales de inicio de sesión de Windows a los usuarios VPN, lo que produce mejoras en el uso de clave única de conexión a los paquetes informáticos locales o a distancia.

Mar (2016), en su tesis de pregrado. titulada: "Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI – Caso: Servidor de Correos. Siendo el objetivo el de emplear tecnología de red Virtual Private Network para mejorar la privacidad de data. Determina que si no se conecta a la intranet vía red privada virtual el atacante observa el flujo aplicado por su víctima, del mismo modo puede extraer información, al aplicar la inter conexión a la intranet vía red privada virtual realizada por la víctima, el atacante no tuvo acceso al tráfico, cuenta del usuario y menos extraer información, con lo que se evidencia que al implementar una red privada virtual es más eficiente la privacidad. Con los percances latentes, es alternativa de solución crear una intranet vía VPN con la finalidad de proteger la privacidad en el flujo de datos en el servidor de e-mail entre las sedes Lima y Cusco del INEI, el aporte es que el INEI puede manejar más dominios de correo "inei.com" en la emisión y retorno de información con los integrantes de las dos sedes, también aumenta la privacidad en la emisión de información a la sede principal, así como el retorno de respuestas. Para llevar a cabo las pruebas de seguridad para verificar que tan eficiente es la VPN para el resguardo de la confidencialidad de la información, se realizaron los ataques manin the middle con una conexión a la intranet vía VPN y otra prueba sin conexión a la misma. Las conclusiones de su investigación fueron que implementó una intranet vía VPN para elevar la confidencialidad del envío y recojo de información de Lima y Cusco. Simulación del intercambio de data del servidor con correos de clientes

VPN, teniendo una comunicación excelente. LA VPN certificó la privacidad y entereza en el envío y recepción de la data enviada entre las dos cuentas.

Espinoza (2015), en su tesis de pregrado. titulada: "Implementación de una IP- red privada virtual para la conexión remota entre servidores de aplicación y base de datos. Realizada en: Universidad Nacional de Ingeniería, Lima", Perú. Establece que la tecnología MPLS permite a los proveedores de Servicios de Internet (ISP) incrementar la fiabilidad y confianza en sus redes ya que brinda beneficios al reducir tiempos en el envío de data y seguridad en los datos. La salida para tener un eficiente servicio web se basa en la integración a la red LAN del Centro de Datos de gerencia, otra acción adicional es de mejorar las tecnologías de la plataforma de atención y conexión para obtener mayor soporte y capacidad de los servicios web, las mejoras se dan aplicando una Red Privada Virtual (VPN) con tecnología Hot Standby Router Protocol (HSRP) y un MPLS, en donde las dos plataformas van a funcionar paralelamente integradas como una sola plataforma. La solución a los problemas es poder acceder a ambas plataformas de TI, lo que hace posible manejar los aplicativos web de manera eficiente, ya sea intranet o intranet. Siendo las conclusiones de su investigación que con la aplicación de VPN SSL con doble factor de autenticación, se disminuyó el grado de riesgo en la operación de accesibilidad remota como se comprueba en el análisis de riesgo aplicado. Al aplicar el protocolo VPN SSL dio como resultado avalar la privacidad del flujo de data recibida y emitida, por datos encriptados bajo el algoritmo 3DES.

Con este procedimiento aporta a generar un medio instructivo de condiciones seguras, donde las operaciones tecnológicas de accesos serán más robustos.

Quiroz (2014), en su tesis de pregrado. titulada: "Calidad de servicio (QoS) en la infraestructura de red del Colegio de Ingenieros del Perú CD Cajamarca". Realizada en la: Universidad Nacional de Cajamarca, Cajamarca Perú. Realizó un análisis en la red propuesta y la red existente del Colegio de Ingenieros del Perú-CDC, donde la red propuesta, se diferencia de la red existente en el incremento del ancho de banda, velocidad en la transmisión de información, errores mínimos de comunicación y tráfico mínimo en la red, esta propuesta permitirá dar soporte a las nuevas tecnologías que se puedan implementar. Se realizó el dimensionamiento de la red a instalar, en los edificios administrativos del CIP CDC, luego se diseñó la estructura de la red, como es el cableado estructurado y equipos regidos a los parámetros según las normas ANSI/EIA/TIA. El estudio concluye que se procedió a la distribución de equipos, canalización y cableado regido a las normas ANSI/EIA/TIA 568 y 569. La red propuesta incrementó el ancho de banda y velocidad de transmisión de información con mínimos errores de comunicación y disminución del tráfico en la red, lo que da soporte a otras tecnologías que se deseen implementar, finalmente la infraestructura de la red se ciñe a los mínimos requerimientos de diseño y acata los parámetros mínimos de QoS.

Correa (2013), en su tesis de pregrado titulada: "Análisis del desempeño de la calidad de servicio (QoS) sobre el protocolo IPv6 en la Red Wireless de la ESFAP

"MARIO URTEAGA ALVARADO" de Cajamarca". Realizada en: Universidad Privada del Norte, Cajamarca, Perú. Determina que, las redes inalámbricas también se encuentran dentro de este escenario, pero, debido a su baja eficiencia por sus características de funcionamiento, el soporte de las técnicas de Calidad de Servicio cobra un especial interés en esta clase de redes. Conclusiones: Para cubrir esta deficiencia, la IEEE desarrolló el estándar 802.11e que permite aplicar Calidad de Servicio a las redes inalámbricas. A través de esta investigación se puede conocer cuáles son los parámetros que determinan la Calidad de Servicio en una aplicación IPv6 sobre redes inalámbricas y que incidencia tienen en el performance de ésta. Además de dar solución al problema planteado en el presente, utilizando la metodología adecuada y los materiales necesarios.

Menéndez (2012), en su tesis de pregrado. titulada: "Estudio del Desempeño e Implementación de una solución MPLS- RPV sobre múltiples Sistemas Autónomos". Realizada en: Pontificia Universidad Católica del Perú, Lima, Perú. Identificó al modelo de implementación "Multi Protocol eBGP Multisalto entre Route Reflectors" como el más adecuado. Determinando que es la mejor opción de servicio y versatilidad, por solo ocupar el 2% del CPU, también disminuyó los tiempos de convergencia a menos de 1 minuto y tiempos de retardo no mayores a 628 ms en el peor de los casos. El modelo asevera la aplicación eficiente del ancho de banda, siendo su rendimiento máximo de extremo a extremo de 1.840 Mbps, lo cual representa el 89.84% conforme a un total de 2.048 Mbps teóricos de la red. Las conclusiones de su investigación fueron: Se desarrolló la estructura MPLS en

redes privadas virtuales, garantizando el desempeño eficiente de la red VPN y con holgura de adición soportes futuros. La oferta tecnológica es proveer servicios VPN a distancia, logrando la conectividad aprovechando la red.

Gonzáles (2012), en su tesis de pregrado. titulada: "Redes Privadas Virtuales y su impacto en las organizaciones", Realizada en: Universidad Autónoma del Estado de Hidalgo, Tulancingo, México. Siendo su objetivo el de crear una red privada virtual de interacción reservada. Concluye que, se trata de una excelente tecnología para el acceso remoto, donde una VPN constituye un sustituto indispensable a los métodos tradicionales caros de marcación telefónica de larga distancia. Además, constituye una buena solución alterna a los métodos de implementación de redes WAN tradicionales, mientras mayor sea la RPV, el ahorro económico será mayor.

Limari (2004), en su tesis de pregrado. titulada: "Protocolos de Seguridad para Redes Privadas Virtuales (RPV)". Realizada en: Valdivia, Chile. Su objetivo principal es el de crear sistemas protegidos de seguridad en las redes privadas virtuales además el objetivo específico. Determina que, VPN es un sistema eficiente que ofrece privacidad y entereza operativa, alternativa que ya viene siendo aplicada masivamente en empresas e instituciones en desarrollo y crecimiento. sistema adquirido por sus grandes bondades en cuanto a menores riesgos en la seguridad de emisión y recepción de datos en un medio masivo público, además de tener costos bajos de instalación y funcionamiento a comparación de los sistemas tradicionales que requieren gran infraestructura, tiempos y costos altos para su operatividad. Siendo sus conclusiones, en las

subredes válidas y máscaras de subred en el RFC 1878, que la red clase B brinda hasta 2048 redes disponibles de 30 hosts lo que amplía el margen de direcciones IP para otros locales. Al desarrollar VLSM efectuado se obtiene hasta 23 redes disponibles y de 2020 redes posibles, asegurando un incremento en redes, lo que respalda 90% de redes accesibles para su expansión empresarial.

La configuración VPN accede seguridad de tráfico de datos y con la Matriz de evaluación de riesgos en el tráfico de información que se ejecutó la configuración VPN ofrece confidencialidad completa en el envío y retorno de paquetes de información entre sedes, lo que accede a la confiabilidad de información real integra y segura, implementar mecanismos de autenticación y control de entrada a los usuarios, teniendo el control por políticas GPO del AD y las restricciones del Firewall que articula las demás sedes de la empresa.

2.2. Bases conceptuales

2.2.1. Red privada virtual (VPN)

a. Definición

Una Red privada virtual es una arquitectura de red que copia a una red privada dentro de una arquitectura de servicio público masivo. Aporta a un nivel de comunicación en las capas 2 o 3 del modelo OSI.

La VPN son de propiedad de una empresa o institución con diversos locales, sedes o sucursales, los cuales se encuentran interconectados por medio de la infraestructura de un proveedor de servicios (Ghein, L., 2006).

Limari, (2004) indica que esta tecnología nos accede a un túnel de encriptación por medio de Internet u otra red pública, lo que acceda a los usuarios a la información de los extremos del túnel con la garantía de privacidad, así como acceder a funciones que solo eran propias de las redes privadas.

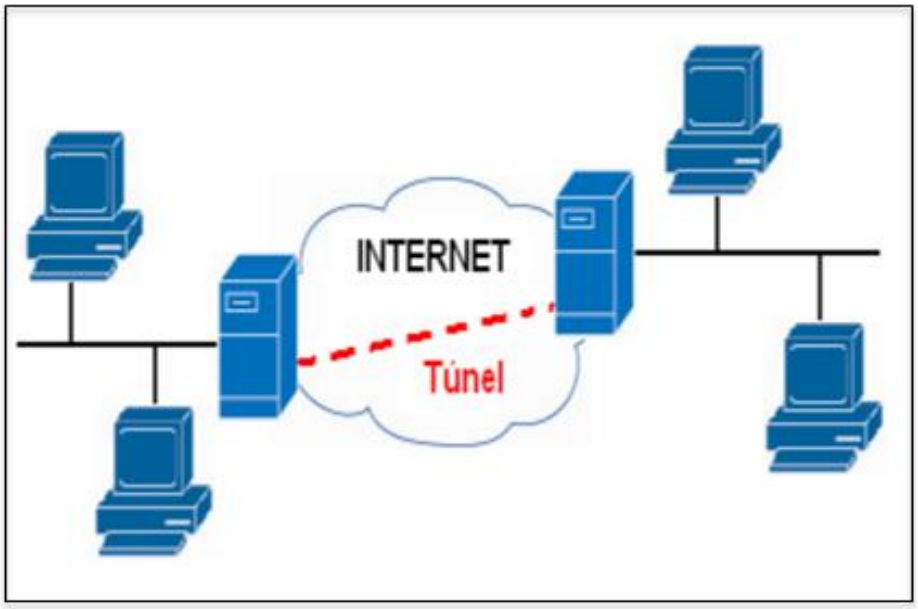


Figura 1. *Modelo estructural de una Red privada Virtual*
Fuente: Red privada virtual. Limari V. (2004).

La equivalencia lógica de la Red privada virtual es el enlace privado punto a punto *(peer-to-peer)* en caso de trabajar en la red a distancias remotas, debido al requerimiento de cableado y equipos en la localidad a la cual se quiera llegar.

b. Ventajas de la implementación de una RVP

- **Reducción de Costos.**

  Limari, (2004). Establece que al desarrollar y ejecutar una red de interconexión entre empresas a distancias remotas ya no se considera necesario aplicar enlaces punto a punto, siendo la nueva opción el uso de accesos ADSL.

  Los costos de implementación y funcionamiento son menores que los sistemas tradicionales, ofreciendo un ancho de banda amplio y es implementado casi en la totalidad de las zonas urbanas. LA aplicación del sistema en zonas alejadas con usuarios o clientes que se movilicen, es suficiente acceder a internet y aplicar el sistema, sin necesidad de realizar llamadas telefónicas a larga distancia.

- **Alta Seguridad**

  Las redes VPN aplican elevados estándares de seguridad para el tráfico de data, siendo más eficientes con una red tipo punto a punto. Aplica protocolos de encriptación de la información a emitir como 3DES (Triple data encryption standard) el protocolo IPSec (IP Security), también en el manejo de los túneles con el software lo que permite garantizar un alto nivel seguro del sistema. . El sistema brinda diversos niveles de autenticación para poder tener accesibilidad a la red privada de la empresa, con el empleo de las llaves de acceso, así tamizando la identidad del usuario autorizado. (Limari, 2004).

- **Escalabilidad**

  Para aumentar usuarios en la red no se requiere incurrir en aportes adicionales. El sistema ofrece mecanismos y máquinas que se pueden configurar y administrar. Los suministradores de internet tiene muy evolucionada la configuración de los proveedores de Internet por lo que no requiere de un enlace físico que nos significa costos adicionales. (Limari, 2004).

- **Concordancia con tecnologías de banda ancha.**

  Limari, (2004) manifiesta que la RPV se cuelga de la estructura que se tiene en la banda ancha, el cable o cualquier dispositivo que tenga elevada velocidad del tipo ADSL o ISDN. Por lo tanto se tiene una amplitud de permisividad en la configuración de la red. Adicionalmente de puede insertar opciones de Voz en el IP (VoIP), lo que nos proporciona una vía alterna del uso de telefonía a larga distancia.

- **Mayor Productividad.**

  Una Red privada virtual provee mayor accesibilidad durante más tiempo, por lo que se traduce en productividad elevada en los usuarios en la red. También reduce las áreas de trabajo, por lo que es una opción de teletrabajo. (Limari, 2004).

c. VPN´s según necesidades empresariales

Pepelnjak, I., & Guichard J., (2002), manifiestan que una entidad organizada aplica una Red privada virtual (intranet) para cumplir sus objetivos operativos, así como las telecomunicaciones con otras entidades externas (internet), también el ingreso de usuarios y trabajadores desde sus celulares, lap top, entre otros, desde su domicilio o de zonas alejadas.

Las opciones que contribuyen a estos fines, son el uso de topologías y tecnologías ofrecidas por los proveedores de la RPV. Los VPN´s adicionalmente optan por los niveles de privacidad que imparten en las programaciones del sistema.

En los enlaces de comunicación interna (intranet), el flujo no siempre está protegido en los host terminales o en los firewalls que se tengan. Siendo la Red Privada Virtual planteada una opción para este flujo de información con el resguardo de confidencialidad, seguridad y privacidad.

La RPV debe adoptar un QoS o calidad en el servicio que soporte en operaciones riesgosas. Las empresas no hacen uso de la red de internet por que no se tiene calidad de servicio de punta apunta, privacidad, entereza e integridad que requieren las empresas. (Pepelnjak, & Guichard, 2002).

En otros casos, las entidades empresariales emplean conexiones entre ellas (extranet) y solo entre centrales, y aplican tecnologías de seguridad como son los firewalls y/o métodos de encriptación. Como podemos ver en la figura 2, las interconexiones generalmente no poseen procedimientos

radicales en lo que respecta a calidad de servicio, y son utilizadas para implementar sistemas de comunicación entre las empresas por medio del Internet.

Las personas que se encuentran lejanas e ingresan a la red de la empresa, donde no se determinan la ubicación conocida y además insegura. Estos inconvenientes producen conflictos de seguridad entre las puntas de los enlaces, para lo que se emplean encriptaciones en la información o también la aplicación de contraseñas de acceso de un solo uso

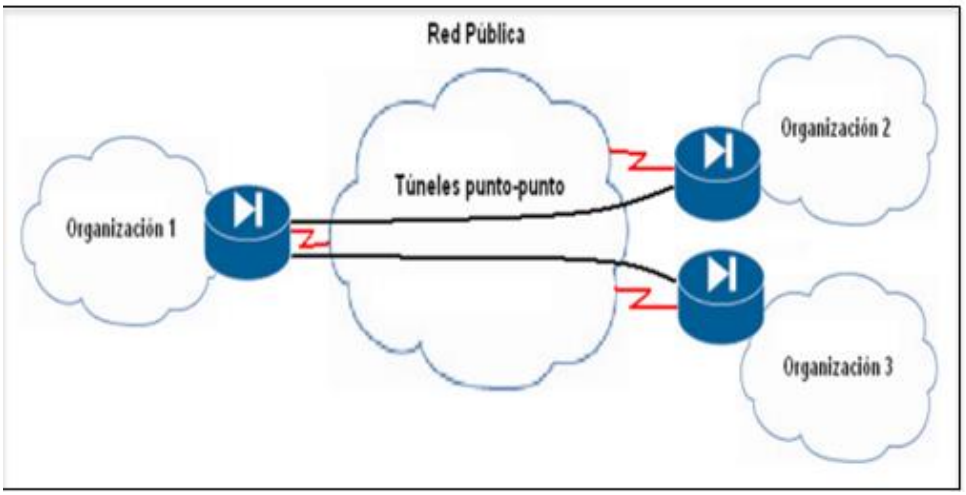


Figura 2. *Modelo de una Red Extranet.*
Fuente: Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures"

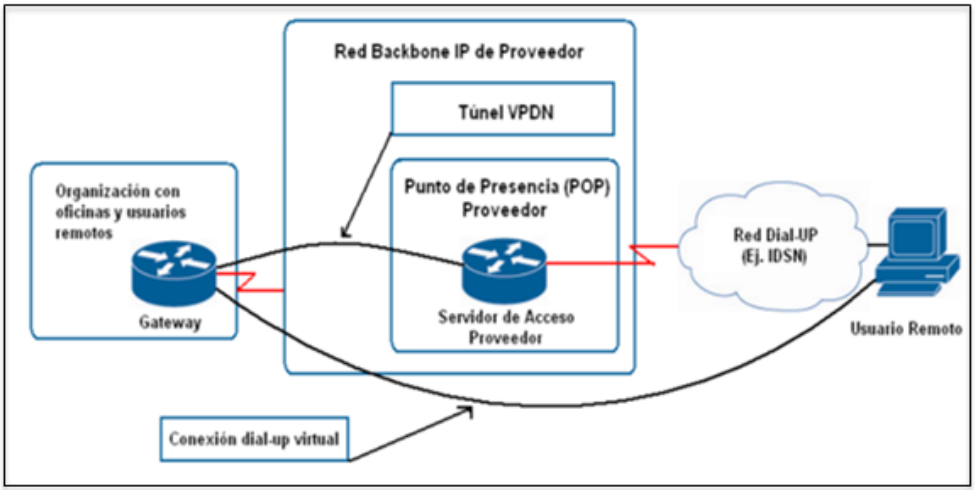


Figura 3. *Red VPDN por medio de Backbone de proveedor.*
Fuente: *Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures".*

Po lo expuesto, la seguridad necesaria para las redes VPDN (Virtual Private Dial-up Network), es de menor grado en comparación de las redes de intranet. En la actualidad la pluralidad de servicios VPDN están desarrollados encima de IP, por medio de la red internet o por el backbone de un proveedor de servicio. (Ver Figura 3).

Términos utilizados en las redes VPDN:

- Servidor de Acceso a Red (Network Access Server NAS): Es el servidor distante administrado por el proveedor, el cual accede al petitorio del cliente, con esto aplica la autenticación del usuario preliminar y deriva el enlace a la puerta de enlace del cliente.
- Puerta de enlace del cliente (Home Gateway): Compuesto por un router de dominio del cliente, el cual permite el enlace reenviada por el NAS, el cual procede a la autenticación del usuario y procede a la autorización

complementaria, terminando la sesión en la zona del usuario de la conexión dial-up. Los términos de ejecución de la sesión (IP) están desarrollados por la empresa usuaria y el Home Gateway. El servidor NAS remite las tramas entre ambos. (Pepelnjak, & Guichard, 2002).

d. Primeras arquitecturas de Red Privada Virtual

- **Modelo Overlay** Red privada virtual

Las primeras Red privada virtual se implementó basado en programas Frame Relay o ATM, en esta red el proveedor de la red ofrece interconexión a nivel de Capa 2 hacia los routers del cliente. Este método desarrollado es denominado Modelo Overlay. Aquí el proveedor del servicio tiene el dominio de los routers de borde (Edge Routers) los cuales los administra ó son conectados a la red del cliente. El objetivo es que los routers se encuentren en el local del cliente. Pepelnjak, I., & Guichard J., (2002).

Asimismo ayudan a mencionan claramente las responsabilidades individuales del proveedor de la red y los clientes. El proveedor suministra una gama de líneas virtuales (emuladas) al cliente o proveedor, denominadas (PVCs) o también proveídas bajo demanda (SVCs). (Ver ilustración 4).

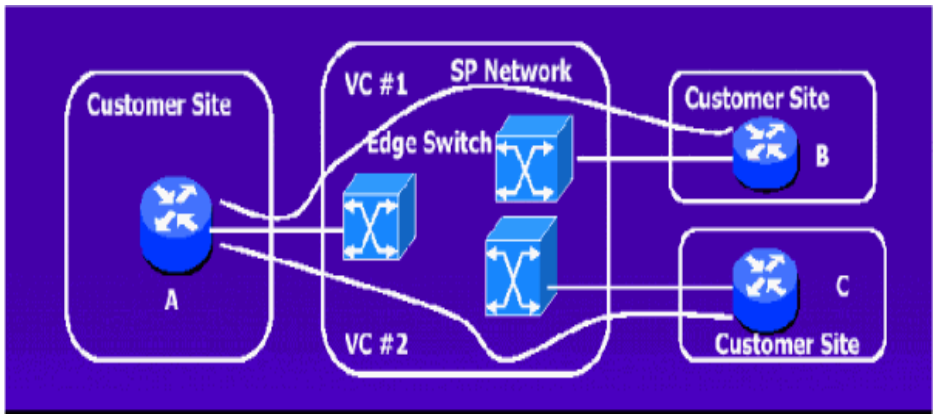


Figura 4. *Red Overlay VPN N. a través de un Backbone de proveedor.*
Fuente: Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures".

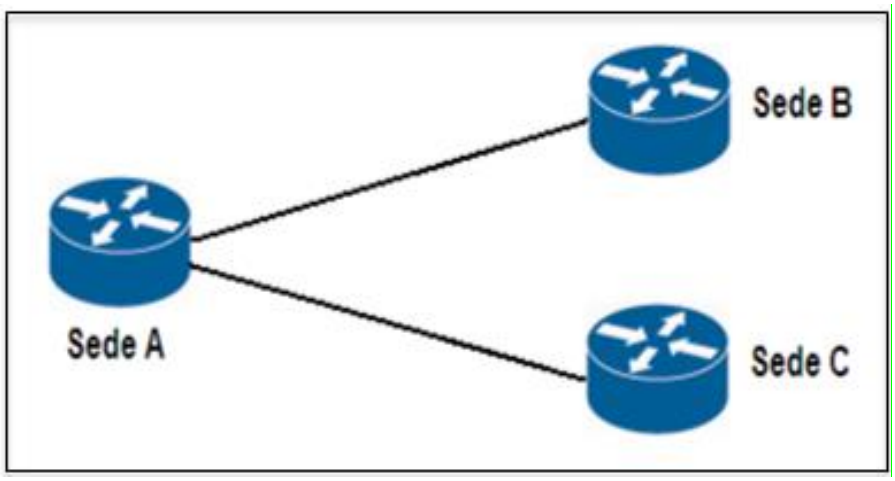


Figura 5*. Enrutado de una red Overlay VPN.*
Fuente: Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures".

Entonces el cliente y/o usuario accede a la comunicación entre routers de los equipos de los clientes o Customer Premises Equipment (CPE) a través de las VCs. La data directriz de enrutamiento son intercambiados entre los CPE, en donde el proveedor de servicio de la red no intervienen en la estructura interna de la red del cliente. (Ver Ilustración 5).

- **Modelo Peer – to – peer VPN**

Ghein, L. (2006). Señala que este método Peer-to-peer se aplicó anteriormente sin éxito. Siendo los inconvenientes dificultades en el despliegue y permanencia por carecer de listados de distribución, carencia de los filtros de paquetes IP, o túneles GRE.

Esta tecnología se implementó para poder subsanar las deficiencias del modelo Overlay. En las VPNs peer-to-peer, el equipo de borde del proveedor o Provider Edge (PE) es un router el cual produce el intercambio de las rutas de forma directa con el router CPE. (Ver ilustración 6).

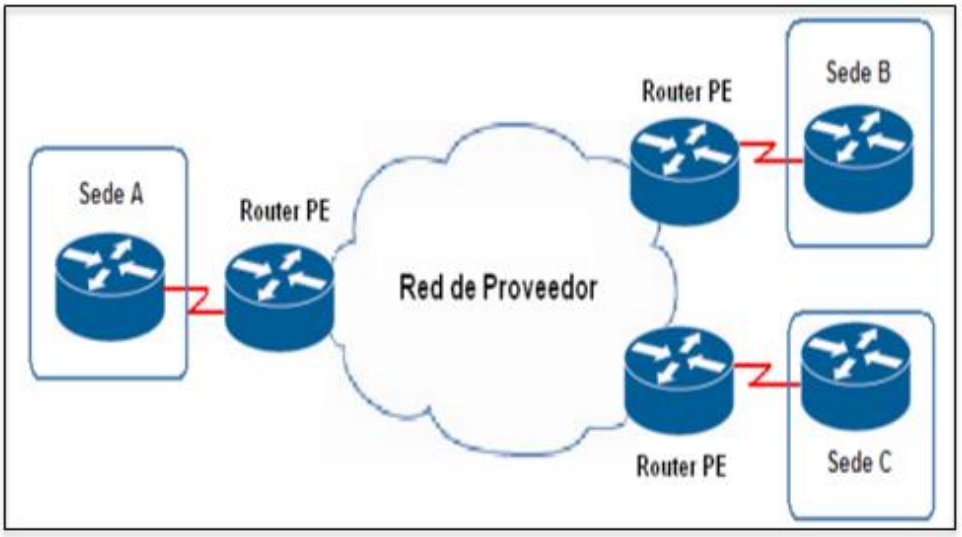


Figura 6. *Modelo Red de Proveedor PEER - TO - PEER VPN.*
Fuente: Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures".

Tabla 2. *Comparativo entre OVERLAY Y PEER - TO - PEER.*

MODELO OVERLAY	MODELO PEER-TO-PEER
Conmutación veloz de tramas en el backbone (capa 2)	Velocidad de conmutación de paquetes de acuerdo a la plataforma.
Autonomía en cada red de clientes (RPV en capa 2)	Sin autonomía de redes, donde se opera una sola tabla de rutas.
Versatil en fluir diversos protocolos de capa 3.	Los protocolos de flujo tienen que ser encapsulados en bloques IP.
La estructura QoS es deficiente, siendo su desenvolvimiento dependiente. del protocolo de capa 3 utilizado	La estructura de QoS en aplicativos se basa en el marcaje de los paquetes de información o reserva de ancho de banda
Para un usuario nuevo se apertura circuitos nuevos (PVCs) en el backbone demás de reconfigurar las máquinas.	Para un usuario nuevo basta aperturar un circuito de acceso y del router.
Uso pésimo de troncales FR/ATM	Uso de Troncales IP de dimensiones eficientes.
Uso deficiente de acceso a la central en esquemas hub & spoke	Acceso eficiente de acceso del ancho de banda (full-mesh virtual)
Requiere nuevos circuitos de acceso del cliente a la red del proveedor en la en capa 2	Accesibilidad idónea a los servicios del proveedor (data center) por medio de las troncales IP existentes
Su mejor enrutamiento efectuado en la capa 3	Su mejor enrutamiento efectuado basado sólo en métricas fijas
Tráfico alto en el intercambio de rutas generado por los diversos vecinos del CPE	Intercambio de rutas con uno o pocos PE
Enrutamiento tedioso en el intranet.	Enrutamiento óptimo entre las sedes del cliente, pues los PE conocen su topología de red.
Para determinar el ancho de banda, el usuario tendrá q direccionar el perfil de tráfico exacto de local a local	El usuario especifica el ancho de banda inbound y outbound sólo para cada local.

Fuente: Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures".

2.2.2. Tipos de VPN

Son 2 tipos de VPN que se aplican, los cuales son de sitio a sitio y los de acceso remoto, los dos tipos pueden contener en común el firewall o servidor VPN.

- **VPN Sitio a Sitio**

  El VPN sitio a sitio se aplica para la conexión entre varias sucursales a distancia y la sede principal de la empresa, teniendo una conexión permanente a internet (servidor o firewall VPN), por este canal se determina un túnel virtual de flujo de comunicación con los servidores de las sedes, las cuales cuentan con conexión local a Internet. La interconexión de la sede principal y las sedes son de naturaleza de banda ancha, factor que produce la reducción de costos de enlace dedicados punto a punto, y además se aplica en conexiones remotas a nivel nacional e internacional. (Trujillo, 2006).

  Con este tipo de topología es posible comunicar dos redes que pertenezcan a la misma empresa o empresas distintas, las configuraciones propias son:

  Topología Intranet: Tipo utilizado cuando la empresa tiene sucursales, las cuales son interconectadas con la sede principal, donde todos comparten igualdad de nivel de seguridad como lo tienen la sede principal.

Topología Extranet: Esta topología se aplica en corporativos o enlaces con empresas con otras similares, clientes y servicios, siendo requerido compartir redes de trabajo para un fin común, redes con restricciones con estratos de seguridad diversos para entrar a la red de la sede principal.

En esta topología de VPN se utiliza servidores, ruteadores que aperturan la conexión VPN, utilizando similares algoritmos de encriptación y encapsulamiento en ambos lados de los usuarios, lo cual se aprecia como una comunicación fluida dentro de la misma área local.

- **VPN de Acceso Remoto**

  Topología VPN utilizado por la gran mayoría de empresas, el cual es aplicado a usuarios móviles como son los proveedores, vendedores, transportistas y otros trabajadores de las distintas empresas en lugares remotos. Para su aplicación se utiliza internet de banda ancha, para que los usuarios lejanos se autentican para ingresar a la red para laborar o hacer uso de la red en condiciones iguales de red local de la empresa o entidad. (Orozco, 2014).

  El usuario remoto que requiera conectarse al sistema de las entidades debe contar con un software aplicado en su terminal y así aperturar un túnel virtual hacia la organización, donde es un servidor, ruteador o firewall quien provee la conexión, no sin antes validar la identidad del usuario que quiera acceder a la red. Cevallos, 2006).

2.2.3. MPLS

- **Definición**

  Multi Protocol Label Switching es un sistema de encapsulamiento aplicado entre las capas 2 y 3 del modelo OSI. Presuriza el flujo de paquetes IP, en vez del enrutamiento de direcciones de capa 3 por una conmutación basada en etiquetas. (Lavado, 2010).

- **Principales ventajas de MPLS**

  Lavado, G. (20109. Nos muestra las ventajas de la tecnología MPLS se pueden resaltar:

  - Conmutación veloz de los paquetes fundamentado en las etiquetas y no direcciones IP destino.
  - Redes de clientes totalmente independientes (MPLS-VPN).
  - Es multi-protocolo tanto hacia arriba (L3) como hacia abajo (PWE3).
  - Trabaja con QoS (Calidad de Servicio) basado en marcación de paquetes.
  - Para crear una nueva VPN se necesita crear el circuito de acceso y la ruta.
  - Es posible implementar la Ingeniería de Tráfico (TE).
  - Aplicación Uso eficaz del ancho de banda en accesos (full-mesh virtual).

- **Esquema básico de funcionamiento**

  Para poder entender el funcionamiento de MPLS, se deben tener claros los términos que describen su arquitectura.

  a) Modo de operación

  Morales (2006) afirma que primero, se requiere implantar un LSP entre los routers que van a comunicar el tráfico FEC. Los LSPs se convierten en túneles de transporte con sus parámetros QoS particulares del flujo, lo que nos proporciona la cuantía de recursos a reservar para el LSP y el desecho y la cola de procesos en cada LSR.

  En el intercambio de datos los routers MPLS emplean protocolos LDP o TDP. Cada flujo de tráfico FEC es otorgado a una etiqueta específica. La designación de nombres y rutas se hacen de forma manual o por el protocolo empleado. (Morales, 2006).

  Cuando un volumen de información ingresa al dominio MPLS, el Edge LSR detecta y halla el tipo de servicio necesario de la red. Posteriormente se determina el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. De no haber ningún LSP, el router de borde opera con los otros LSRs para definirlo. Cuando se encuentra en la soberanía del MPLS, en cada LSR que recepciona la información, van a darse los procesos:

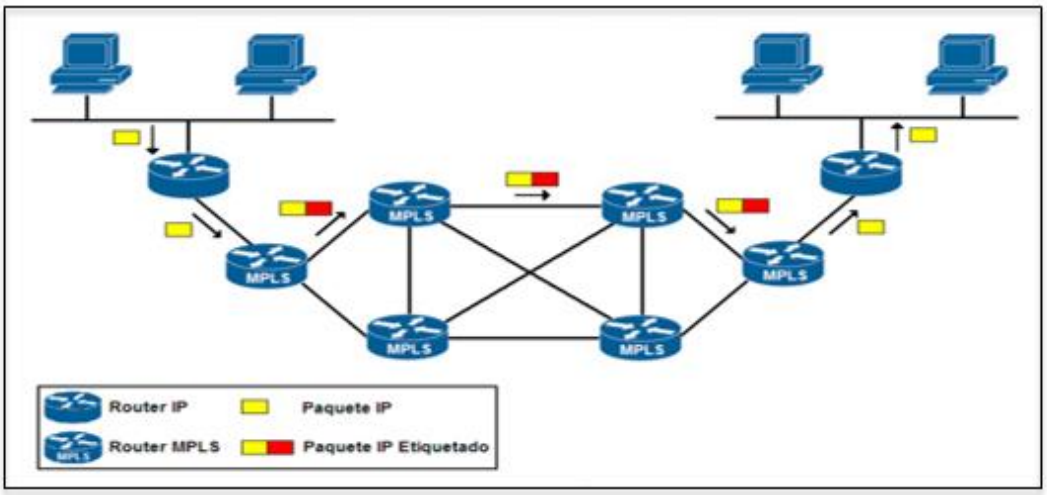


Figura 7. *Esquema y funcionamiento MPLS.*
Fuente: *Morales, L., (2006). "Redes VPN con Tecnología MPLS".*

- Se evacúa la etiqueta de entrada y se le adiciona una nueva etiqueta de salida a la información.
- Se remite la información al siguiente LSR dentro del LSP.
- Como fase final, El LSR de salida apertura la etiqueta e interpreta el encabezado IP para remitirlo al destinatario final.

b) Estructura del MPLS

Los componentes que integran la red MPLS son (Lavado, 2010):

- **Elementos lógicos**

  La estructura MPLS tiene dos elementos lógicos primordiales:

  - Plano de Control (control plane): Hace el intercambio de etiquetas y rutas en capa 3.
  - Plano de Datos (data plane): Reenvía los paquetes de información basado en las etiquetas.

- **Elementos físicos**

Pepelnjak, & Guichard, (2002). Un Edge-LSR es denominado un router que ejecuta la imposición de etiquetas, acciones de empuje, disposiciones de etiqueta, o pop action en el borde de la red MPLS. Se anteponen las etiquetas en un paquete informático en la zona de ingreso al dominio MPLS. La disposición de la etiqueta se refiere a la remoción de la última etiqueta de un paquete informático en la zona de salida y así remitirlo a otro adjunto del dominio MPLS.

Si tenemos un LSR con vecinos que no tengan instalado un MPLS se le denomina como un Edge-LSR. Pero si el LSR contiene interfaces que se conectan a un ATM-LSR por medio de un MPLS, también se considera un ATM Edge-LSR. Los Edge-LSRs emplean una plataforma de reenvío IP estándar con data adicional de etiquetado, de modo que se pueda etiquetar y des etiquetar los paquetes.

Un ATM-LSR es un switch ATM que puede comportarse como un LSR. El ATM-LSR el cual accede al enrutamiento IP y también destina etiquetas en el plano de control y reenvía los paquetes de información por medio de conmutación ATM tradicional (ATM cell switching) en el plano de datos. Entonces en conclusión la matriz de conmutación de un switch ATM se emplea como una

plataforma de reenvío de un nodo MPLS. Lo switches ATM estándares, funcionan como ATM-LSRs si se actualiza el software de su componente de control (Pepelnjak, & Guichard, 2002).

2.2.3.1. Modos de encapsulamiento MPLS

El MPLS contiene dos variantes de encapsulamiento:

- **Modo trama (frame-mode):** Donde los LSR enruta y hacen conexión por medio de uniones de la capa 2, ya sea Ethernet, ATM, entre otros. (Lavado, 2010).

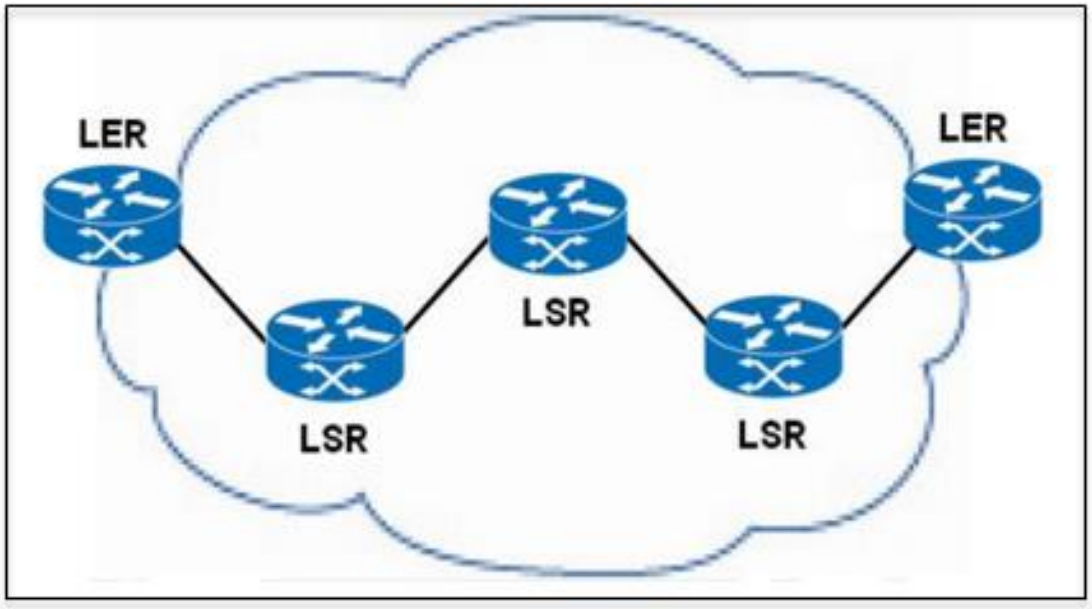


Figura 8. *Esquema modo TRAM.*
Fuente: Lavado, G., (2006). "MPLS-Multiprotocol Label Switching. Versión1.0

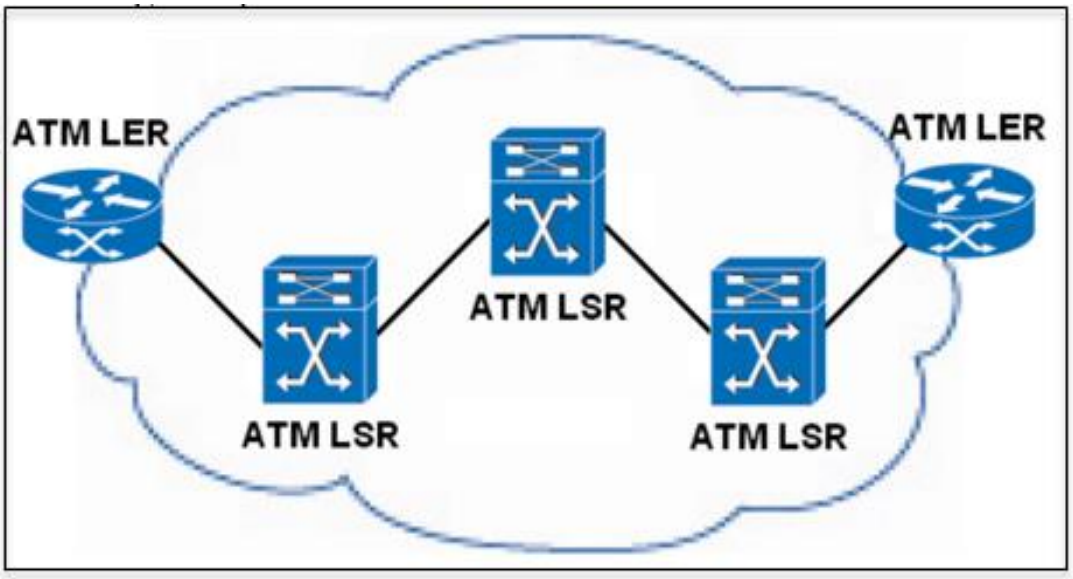


Figura 9. *Esquema CELDA*
Fuente: Lavado, G., (2006). "MPLS-Multiprotocol Label Switching. Versión1.0 Modo de Compatibilidad".

- **Modo celda (cell-mode):** El enlace de los routers de los usuarios se dan por los LSR los cuales son switches ATM. (Lavado, 2010). Se aplica la etiqueta del identificador de Trayecto Virtual y del identificador de canal virtual, del mismo modo las otras áreas se conectan al encapsulado genérico. (Ver Ilustración 9).

2.3. Usos de MPLS

Anteriormente se dijo que los MPLS van a interconectar los routers estándares y los switches ATM en un backbone IP (composición IP + ATM).

Pero la aplicación más importante es el desarrollo y aplicación de la ingeniería de tráfico. Así como llegar a las Redes Privadas Virtuales punto a punto (peer-to-peer Virtual Private Networks). Todas estas aplicaciones funcionan con un tablero de control parecido al tablero de control de enrutado (Pepelnjak, & Guichard, 2002).

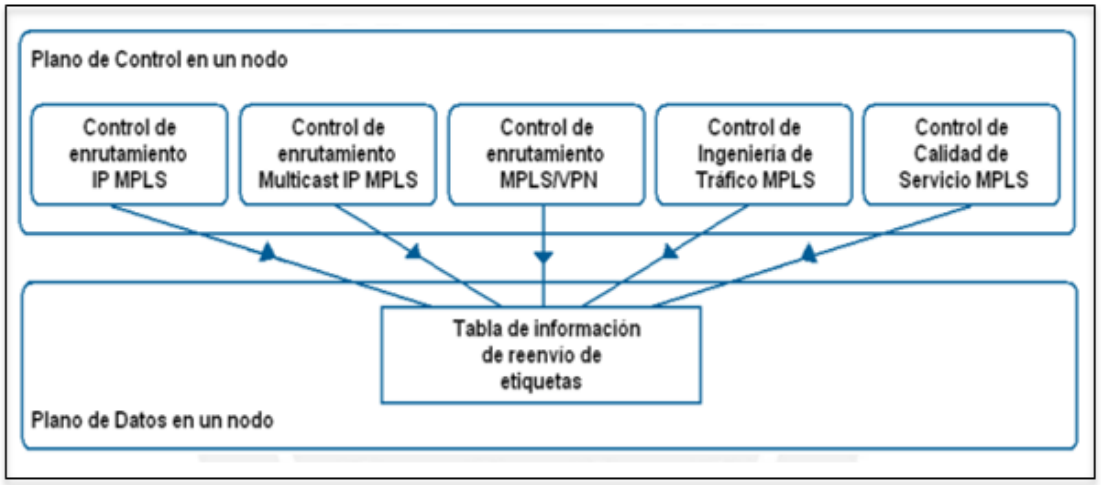


Figura 10. *Aplicación MPLS para el plano de control y plano de datos en un nodo.*
Fuente: Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures".

Cada determinada adaptación MPLS está conformada por los mismos componentes de adaptación de enrutado IP:

Tabla 3. *Protocolos de controles en MPLS.*

Aplicación	Tabla EFC	Parámetros para elaborar el tablero FEC	Parámetros usados en la permuta de trazo EC - etiqueta
Enrutado IP	Tablero de ruta IP	Varios canales de enrutado	Tag Distribution Protocol (TDP) ó Label Distribution Protocol (LDP)
Enrutado VPN	Tabla de enrutamiento Por-VPN	Protocolos de enrutamiento IP entre proveedores y clientes. Multi Protocol BGP dentro de la red del proveedor de servicio.	Multi Protocol BGP
Ingeniería de Tráfico	Definición de túneles MPLS	Definición manual de interfaces, extensiones a IS-IS u OSPF	RSVP ó CR-LDP

Calidad de Servicio MPLS	Tabla de enrutamiento IP	Protocolos de enrutamiento IP	Extensiones a TDP LDP
Enrutamiento IP Multicast	Tabla de enrutamiento Multicast	PIM	Extensiones PIM version 2

Fuente: Pepelnjak, I., & Guichard J., (2002). "MPLS and VPN Architectures".

- La base de datos que demarca el tablero FEC para su ejecución en el tablero de enrutamiento IP.
- Aplicación de parámetros de control que accedan a la permuta del contenido del tablero FEC, esto entre los LSR´s, para esto se toma en consideración los parámetros de enrutado IP ó enrutado estático IP.
- La interconexión de etiquetas con las FEC´s y protocolos de permuta de los enlaces de las etiquetas en los LSR´s (aplicativos de enrutamiento IP: TDP o UDP), acciones que se rigen por un transcurso de control.
- Como una acción adicional optativa, tiene una base interna de datos de trazo FEC´s y etiquetas, donde la base de datos contiene datos de las etiquetas para cada caso de IP. Cada una de las aplicaciones se rigen por protocolos individuales para poder permutar los tableros FEC, así como el trazo FEC – etiquetas de sus nodos.

2.3.1. MPLS VPN´s

Al implementar una red privada virtual requiere que todos los locales del cliente puedan interconectarse y sean completamente separadas de otras VPNs e

incluso dar conectividad al internet. Las MPLS-RPVs ofrecen todo lo anterior, lo cual es posible debido a que existe un desacoplamiento del plano de reenvío y el plano de control que no es posible con IP.

Estos protocolos de interconexión son los mínimos necesarios. Sin embargo, algunos modelos de VPN de Capa 3 pueden requerir más que eso.

Deben ser capaces de brindar conectividad entre diferentes VPNs

2.3.2. Modelo MPLS – RPV

La figura 11, muestra a un proveedor de servicios conectando dos sedes de un cliente. Como señala Ghein,L., (2006). Un router de borde del proveedor se denomina Provider Edge (PE) router, el cual tiene conexión directa a nivel de capa 3 con el router de borde del cliente denominado Customer Edge (CE) router. Un router de proveedor o Provider (P) router es un router sin conexión directa con los routers del cliente. Un router de cliente, o Customer (C) router es un router sin conexión directa con el router PE. Tanto los routers P como los PE tienen implementado MPLS, mientras que los routers CE no lo necesitan.

Como los routers CE y PE interactúan en la Capa 3, deben trabajar con un protocolo de enrutamiento (o enrutamiento estático) entre ellos.

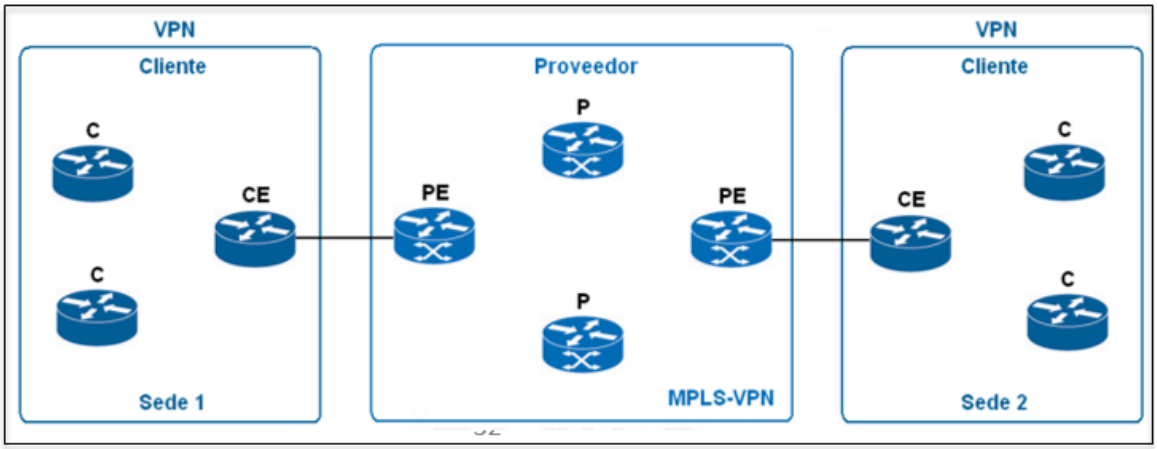


Figura 11. *Cuadro genérico MPLS - VPN.*
Fuente: Ghein,L., (2006). "MPLS Fundamentals."

El enrutador CE contiene un solo externo del local principal, el router PE. Si el router CE es multihomed (está conectado a más de un ISP a la vez), puede ser vecino de múltiples routers PE. El router CE no es vecino de otros routers CE de otros locales conectados a la red del proveedor, como en el modelo Overlay. (Ghein, 2006).

Ghein, L., (2006), Manifiesta que la terminología de punto a punto se desarrolla porque dos routers se emparejan (CE/PE) en la capa 3. Una función primordial de VPN es la privacidad en el flujo de información, para lo que la empresa obtiene un particular IP direccionado. Lo que implica el uso de direcciones Ip del modo público, privado y de los clientes y usuarios que se encuentren conectados a la empresa proveedora contratada esta modalidad es llamada overlapping IP addresing.

Los paquetes de información que se reenvían de modo IP en la red del proveedor, provocarían desorden en los routers IP. Los clientes y usuarios se

deben parametrar en un determinado número de direcciones y el reenvío de los paquetes se dará tomando en cuenta el IP de destino de cada ruteador. Viendo este caso sería necesario tener un tablero extenso y completo de cada uno de los usuarios o clientes de los enrutadores P y PE, esto no es práctico porque se requiere el dominio de un tablero extenso de enrutado. El caso anterior no representa un modelo RPV ya que no tiene privacidad en los clientes. La opción es tener un tablero de enrutado para cada cliente de forma privada aplicando routers P y PE. De este modo todos los flujos de información se presentarían en todos los routers con el fin de repartir los enrutados de las RPV´s. Aun así no es una salida progresiva, porque si agregamos una nueva RPV a la red tendría que desarrollarse un nuevo enrutado para cada router P. Además, si un paquete IP entra a un router P, ¿Cómo determinaría el router P a que RPV pertenece el paquete para poder usar la tabla de enrutamiento que le corresponde? Al ser un paquete IP, no sería factible. Se podría agregar un campo extra al paquete IP indicando a que RPV pertenece para que el router P lo reenvíe basándose en este campo y en la dirección IP destino. También en este caso, todos los routers P deberían conocer este campo extra. Una solución escalable sería que los routers P desconozcan totalmente a las VPNs para que no estén cargados con la información de enrutamiento cada una de ellas. Esto es posible con MPLS. Inclusive, los routers P ya no necesitan tener la tabla de enrutamiento de los clientes, y en su lugar usan dos etiquetas MPLS. Además, ya no es necesario configurar BGP en los routers P. Las rutas RPV solo son conocidas en los

routers PE, lo que hace que la información de las RPV se encuentre sólo en los routers de borde. (Ghein,L., 2006).

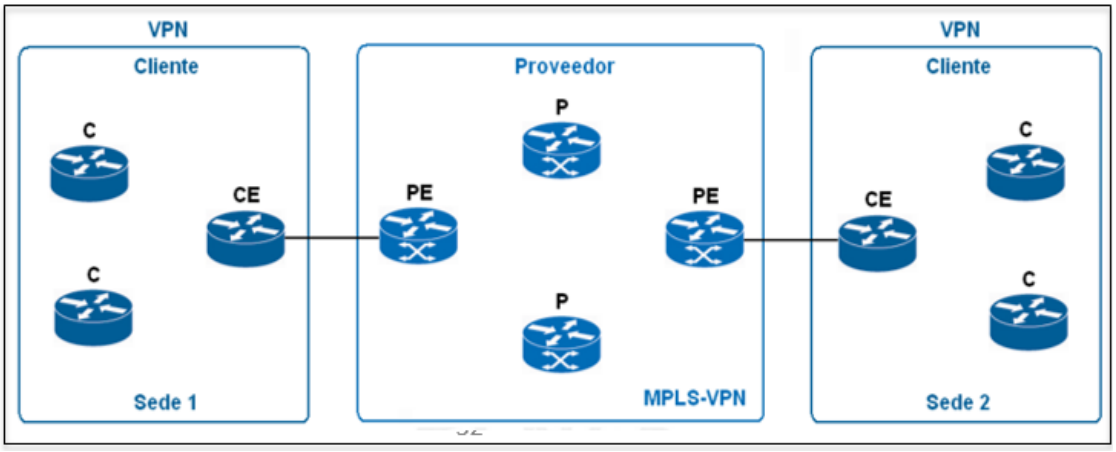


Figura 12. *Esquema general MPLS - VPN.*
Fuente: Ghein,L., (2006). "MPLS Fundamentals."

Ghein, L., (2006). Manifiesta que el nombre peer-to-peer (punto a punto) deriva del hecho que los routers CE y PE forman una "pareja" a nivel de Capa 3. Ya que el principal propósito de una VPN es ser privada, el cliente puede tener su propio esquema de direccionamiento IP. Esto significa que pueden usar direcciones IP públicas, direcciones IP privadas o incluso direcciones IP que también son usadas por otros clientes conectados al mismo proveedor (a esto se le denomina overlapping IP addressing). Si los paquetes fueran reenviados como paquetes IP a través de la red del proveedor, causarían confusión en los routers P. Cada cliente debería usar un único rango de direcciones y los paquetes se reenviarían mirando la dirección IP destino en 35 cada router. Esto implica que todos los routers P y PE tengan la tabla de enrutamiento completa de cada

cliente, lo que haría que manejen una larga tabla de enrutamiento. Este no es un esquema RPV, pues no es privado de cara a los clientes. Otra solución es que todos los routers P y PE tengan una tabla de enrutamiento privada para cada cliente. Esto haría que varios procesos se lleven a cabo en todos los routers para distribuir las rutas de las RPVs. Esta no es una solución muy escalable, ya que cada vez que una RPV sea agregada a la red, se debe agregar un nuevo proceso de enrutamiento a cada router P. Además, si un paquete IP entra a un router P, ¿Cómo determinaría el router P a que RPV pertenece el paquete para poder usar la tabla de enrutamiento que le corresponde? Si el paquete es un paquete IP, esto no es posible. Se podría agregar un campo extra al paquete IP indicando a que RPV pertenece para que el router P lo reenvíe basándose en este campo y en la dirección IP destino. También en este caso, todos los routers P deberían conocer este campo extra. Una solución escalable sería que los routers P desconozcan totalmente a las VPNs para que no estén cargados con la información de enrutamiento cada una de ellas. Esto es posible con MPLS. Inclusive, los routers P ya no necesitan tener la tabla de enrutamiento de los clientes, y en su lugar usan dos etiquetas MPLS. Además, ya no es necesario configurar BGP en los routers P. Las rutas RPV solo son conocidas en los routers PE, lo que hace que la información de las RPV se encuentre sólo en los routers de borde. (Ghein,L., 2006).

2.4. Definición de términos básicos

- **Active Directory:** Terminología utilizada por Microsoft que se dirige al desarrollo y funcionamiento del directorio en una red de computadoras distribuidas en un sector o zona.
- **Dominio MPLS:** Es la agrupación de encaminadores adjuntos, que es experto en t realizar acciones de enlutar y/o conmutar, los que se encuentran inmersos en una determinada parea administrativa.
- **Edge LSR (Edge Label Switch Router) o LER (Label Edge Router):** Nodo de borde que administra el tránsito de ingreso y salida de la red MPLS.
- **Enrutamiento:** Es un procedimiento en donde los paquetes de información van a transportarse dese el origen a los destinos que son las notarías, por medio de la red es que se van a enrutar.
- **El Edge LSR de entrada** Incrementa una etiqueta a MPLS para cada paquete informático y el MPLS de sale saca y enruta de acuerdo a la capa de Red (García, 2009).
- **Forwarding Equivalence Class (FEC):** Es una categoría que conglomera un grupo de paquetes informáticos de envío con una similar característica como es el destino de llegada, tipo de QoS, entre otros. La información enviada que corresponda al mismo FEC, vana a discurrir por la misma ruta de la red MPLS y tendrán igual etiqueta de egreso. (Lavado, 2010).
- **Gateway:** Denominada puerta de enlace. Dispositivo el que nos accede la interconexión a las redes por medio de normativas y estructuras diversas a todos los niveles de comunicación. El objetivo de la puerta de enlace es el de

traducir la información del protocolo aplicado en la red origen en la red del protocolo aplicado en la red destino.

- **Internet:** Es una red globalizada de varios equipos en donde las comunicaciones se desarrollan por medio de un protocolo común, TCP/IP.
- **LIB (Label Information Base):** Es la base de datos creada en un LSR/LER el cual incluye data de las etiquetas e interfaces añadidas a las redes destino (Lavado, 2010).
- **LDP (Label Distribution Protocol):** Normas que implantan reuniones TCP entre LSR/LERs con el fin de permutar las etiquetas en las acciones de que estos utilizarán para el intercambio de paquetes (Lavado, 2010).
- **LSP (Label Switched Path):** Ruta de una sola dirección determinado con QoS y estructurado secuencialmente de LSR´s, por medio del cual se remite la información que corresponde al mismo FEC. (Lavado, 2010).
- **LSR (Label Swtiching Router):** Nodo interno de la red MPLS el cual tiene la competencia de conmutar y enrutar paquetes informáticos examinando la etiqueta sumada a cada paquete. (García, 2009).
- **MPLS:** (Multi Protocol Label Switching). Es un medio tecnológico que nos accede a interconectar íntegramente a las sucursales del cliente, proporcionando una eficiencia mejorada en las comunicaciones (retrasos de envió menores).
- **NODO:** Es el punto final de una conexión de una red conectada a dos o más líneas de una red.

- **Red Privada Virtual:** Es una amplitud de condición segura de la red local (LAN) encima de la red pública que no es controlada (internet). Es una determinada tecnología de redes
- **Ruteador:** Es el dispositivo de capa de red el que aplica de una a mas métricas para poder hallar la mejor ruta por donde se enviará la información por la red.
- **Servidor:** Es una PC o laptop conectada en red a otras similares, las cuales efectúan acciones de acuerdo a la solicitud de las otras máquinas.
- **TDP (Tag Distribution Protocol):** Protocolo similar a LDP, propietario de Cisco.
- **Traffic Engineering (TE):** Desarrollo del control de flujo de tránsito por medio de la red, el cual mejora el uso de medios para tener un eficiente rendimiento. (García, 2009).

CAPÍTULO III: ESTRATEGIAS METODOLÓGICAS

3.1. Metodología de la investigación

El diseño metodológico es descriptivo correlacional – cuantitativo.

La investigación es de tipo Descriptivo, porque se describirá las situaciones o caso que se encuentra en estudio, estudio basado en la adquisición de información, análisis y sustentación de los datos procesados.

El nivel de investigación es Correlacional, técnica que aporta a determinar una relación entre dos variables que se encuentran muy vinculadas como son la pre y post prueba de simulación del sistema.

Es cuantitativo por que se determina conclusiones estadísticas con la información obtenida que es procesable como se determina en el diseño de redes VPN y MPLS Red Privada Virtual para disminuir el tiempo de envío de información entre las notarías y Colegio de Notarios de Cajamarca.

Es un estudio transversal porque se analizan los datos recopilados en un lapso de tiempo en una población muestra definida. (Alvitres, V., 2000).

3.2. Unidad de análisis, universo y muestra.

a. Unidad de análisis.

Está representada por las Notarías de los distritos de Cajamarca, Baños del Inca y el Colegio de notarios de Cajamarca para introducir un sistema de interconectividad de redes.

b. Población

La población estuvo constituida por seis (06) notarías del distrito de Cajamarca y dos (02) de Baños del Inca y (01) del Colegio de Notarios, en total (09), de las que se menciona:

- Notaría Linares Sánchez.
- Notaria Ledesma.
- Notaría Cacho.
- Notaria Vigo Saldaña.
- Notaría Castañeda.
- Notaria Urbina Vásquez.
- Notaría Vigo Rojas.
- Notaría Lozano.
- Y el Colegio de Notarios Cajamarca.

c. Muestra

La muestra fue no probabilística por conveniencia y coincide con la población. Es decir estará formada por seis (06) notarías del distrito de Cajamarca y dos (02) de Baños del Inca y el Colegio de Notarios.

Conformada por seis (06) notarías del distrito de Cajamarca y dos (02) de Baños del Inca y el Colegio de Notarios.

N = 24 testeos de las 8 notarias al Colegio de Notarios

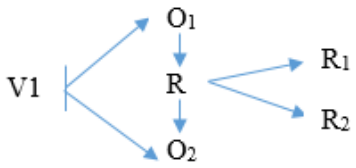
La muestra aplicada son a las 8 notarias que se tienen el distrito de Cajamarca y Baños del Inca donde se envían las pruebas de simulación, se tiene en claro que las notarías realizan el envío de paquetes al Colegio de Notarios y las notarías no realizan el envío de paquetes.

3.3. Métodos de investigación

- **Analítico – Sintético:** Consiste en descomponer el elemento estudiado, separando sus componentes del todo para estudiarlas en forma individual, posteriormente en integrar los componentes y realizar las conclusiones de la investigación (Bernal, 2006). Estudio que aplicó el diagnóstico para hallar características de interconexión entre las notarías del distrito de Cajamarca y Baños del Inca, analizando los procesos de comunicación de cada una con el Colegio de Notarios para después proponer la tecnología de integración, determinando el nivel de influencia de la herramienta a través de una simulación.

3.4. Diseño de la investigación

Diseño Cuasi experimental, según Bernal (2010), en esta investigación este diseño se tiene un poco o ningún control sobre las variables extrañas, donde los grupos experimentales se conservan intactos o estáticos, debido a que se da una asignación aleatoria de lo individual a lo grupal. Sin embargo, los sujetos o las unidades de prueba no se asignan al azar ningún grupo ni se realizan mediciones previas al experimento de la variable dependiente, lo que tiene la expresión:



Donde:

V1: Diseño Red Privada Virtual.

O_1: Notarias de Cajamarca y Baños del Inca. Observación de la V.1..

O_2: Colegio de Notarios de Cajamarca. Observación de la V2.

R: Correlación entre las variables

R_1: Resultado de la aplicación de Red Privada Virtual sobre el acceso a la información en tiempo real de las notarías.

R_2: Resultado de la aplicación de Red Privada Virtual sobre interconexión entre notarías y colegio de notarios de Cajamarca.

3.5. Técnicas e instrumentos de recopilación de datos

Los instrumentos utilizados al adquirir y recopilación de información es de observación directa mediante el uso de fichas de observación o hojas de cotejo de Pre – Prueba y Post- Prueba de tres variables:

Tiempo de latencia del servicio de envío de información;

Número de saltos recorridos por el paquete de datos de origen – destino;

Lapso de tiempo en cargar para transacciones en el sistema informático. (Anexos 4,5 y 6).

La guía de procedimientos de observación de las tres variables se tiene en los anexos 1,2 y 3.

Tabla 4*. Técnicas e instrumentos de investigación documental*

Técnicas	Instrumentos
Internet	Software
Observación directa:	Hojas de cotejo de pre prueba
Registro de datos	Hojas de cotejo de post prueba

Fuente: Elaboración propia.

En la etapa de obtención de información no se pudo realizar por efectos de la pandemia COVID 19, por no contar con autorización de ingreso a las notarías, SUNARP y demás entidades en estudio. Por este motivo se tuvo que optar con la simulación del Uso de una red privada virtual a través de un MPLS en la interconexión y el acceso a la información simulada del proceso en tiempo real por ser una alternativa acertada en esta situación de pandemia. Se realizó un registro de datos de tiempo de latencia en la transferencia de taos del sistema, que luego fueron contrastadas con las hojas de cotejo de pre prueba y post prueba.

3.7. Técnicas de análisis de datos (estadísticas)

Para el desarrollo y evaluación de la información adquirida se aplicó herramientas estadísticas descriptivas. Asimismo se describe el estadígrafo para poder cotejar las hipótesis en estudio, el estadígrafo utilizado es la técnica de Mann – Whitney, porque en el estudio se tienen 3 testeos independientes y los cuales no se encuentran parametrados. Utilizamos esta prueba para poder hallar la heterogéneo que pueden ofrecer dos muestras ordinales (Pre –Prueba y Post – Prueba), las observaciones directas de ambos grupos son independientes y no vinculantes, de acuerdo a la hipótesis alternativa, los valores obtenidos de una de ellas va a exceder a la otra, así determinando la contratación de la hipótesis afirmando o denegándola.

CAPÍTULO IV: PROPUESTA DE UNA RED PRIVADA VIRTUAL

4.1. Factibilidad

4.1.1. Factibilidad técnica

La puesta en funcionamiento de una Red Privada Virtual tiene la factibilidad técnica, ya que al realizar una entrevista informal con las notarías de Cajamarca se comprobó que cuentan con los medios, recursos de información, conocimientos, habilidades, equipos y herramientas informáticas para llevar acabo los procedimientos y aplicación de métodos en el sistema de proyecto.

4.1.2. Factibilidad de uso

Con la elaboración de un diseño para solucionar aspectos de la red, es factible aplicar la gestión de los equipos a utilizar, así reduciendo los incidentes que se puedan ocasionar, haciendo más competentes los tiempos de carga y flujo de los Sistemas Informáticos, lo cual produce menores tiempos de adquisición de información a las notarías, además de tener seguridad e integridad del flujo de información, lo que nos da calidad de servicio a los clientes.

4.1.3. Factibilidad Operativa

Se tiene el compromiso y disposición de las notarías, ya que disminuyeron los tiempos de adquirir información legal y confidencial del Colegio de Notarios hacia las notarías. Además se considera la información contenida la tabla 5.

4.1.4. Factibilidad Económica

El presente estudio de una Red Privada Virtual tiene la posibilidad económica, porque las Notarías y el Colegio de Notarios cuentan con los recursos económicos requeridos para su implementación.

4.2. METODOLOGÍA

La presentación del uso de una red privada virtual a través de un MPLS en la interconexión y el acceso a la información en tiempo real de las notarías del distrito de Cajamarca, Baños del Inca y el colegio de notarios, es una necesidad de modelos de flujo de información vía on line que ya se dan globalmente, siendo una necesidad primordial en el acceso de la información.

La aplicación de redes organizacionales con nodos terminales con diversos procesos con interconexión para la emisión y recepción de información, contando con protocolos seguros en el flujo de información sin tener percances de pérdida de datos o contener modificaciones. Aplicamos la red privada virtual MPLS (VPN MPLS) con el fin de proveer un mecanismo eficiente, fiable y escalable en la conexión las distintas sedes.

Aplicando el VPN utilizando MPLS, nos permite acceder a diversos sitios remotos y que se interconecten por medio de la red proveedora de servicio de internet, empresa que puede brindarnos soporte a varias VPN con IP diversas, en donde vemos que cada IP de VPN se muestra como una red privada. Cada lugar de un VPN remite paquetes del IP a otros sitios (notarias) en la misma plataforma VPN.

Se aplica la configuración de la Red Privada Virtual (VPN) de Multiprotocol Label Switchinf (MPLS) en momentos que el Routing Information Protocol (RIP) este activo en el otro lado de la fuente.

Cada VPN se encuentra asociada entre una a más sucesos de reenvío o también denominado ruteo VPN. El router conserva un ruteo divergente y una tabla CEF para cada VRF. Este propósito impide que la información sea remitida fuera del VPN y a la vez nos accede a que la misma sub red sea usada en diversos VPN, usos que no producen problemas de IP duplicado.

4.2.1. Modelamiento de la Transacción en el Sistema Informático Notarial

En general los notarios que cesan en sus actividades notariales, remiten sus tomos (libros), los cuales contienen documentos que se extendieron escrituras públicas, transferencias vehiculares, entre otros y son remitidos al Colegio de Notarios en nuestro caso al Colegio de Notarios de Cajamarca.

Por lo tanto, en cuanto un cliente requiere algún documento que se encuentre en los tomos antes mencionados (documentos notariales de notarios cesados o retirados), se hace la solicitud de manera presencial en el Colegio de Notarios para poder acceder a los documentos en cuestión.

4.2.2. Equipos y Usuarios de la red

Tabla 5. *Equipos y Usuarios de la red de* ***Notarias y Colegio de Notarios (1)***

EQUIPOS Y USUARIOS DE LA RED DE NOTARIAS Y COLEGIO DE NOTARIOS				
Usuarios	**Nombre de PC**	**Dirección IP**	**Equipo**	**Cant**
Notaria 1 Cajamarca				
Notario	Laptop 0	Laptop-PT	Core 9 /1TB	1
Área Legal	PC1	PC-PT	Core 7 / 1TB	1
Archivo	PC2 – PC3	PC-PT	Core 7 / 1TB	2
Notaria 2 Cajamarca				
Notario	Laptop 1	Laptop-PT	Core 7 /1TB	1
Área Legal	PC4	PC-PT	Core 7 /1TB	1
Archivo	PC5 – PC6	PC-PT	Core 9 / 1TB	2
Notaria 3 Cajamarca				
Notario	PC7	PC-PT	Core 7 /1TB	1
Área Legal	PC8	PC-PT	Core 7 /1TB	1
Archivo	PC9 – PC10	PC-PT	Core 10 / 1TB	2
Notaria 4 Cajamarca				
Notario	PC11	PC-PT	Core 7 /1TB	1
Área Legal	PC12	PC-PT	Core 7 /1TB	1
Archivo	PC13 – PC14	PC-PT	Core 7 /1TB	2
Notaria 5 Cajamarca				
Notario	PC15	PC-PT	Core 7 /1TB	1
Área Legal	PC16	PC-PT	Core 5 /1TB	1
Archivo	PC17 – PC18	PC-PT	Core 9 /1TB	2
Notaria 6 Cajamarca				
Notario	PC19	PC-PT	Core 7 /1TB	1
Área Legal	PC20	PC-PT	Core 5 /1TB	1
Archivo	PC21 – PC22	PC-PT	Core 7 /1TB	2
Notaria 7 Baños del Inca				
Notario	LAP TOP 2	Laptop-PT	Core 7 / 1 TB	1
Área Legal	PC 22	PC-PT	Core 9 / 1 TB	1
Archivo	PC 24 – PC 25	PC-PT	Core 9 / 1 TB	2

Fuente: Elaborado por el autor.

Tabla 6. *Equipos y usuarios de la red de Notarias y Colegio de Notarios (2)*

EQUIPOS Y USUARIOS DE LA RED DE NOTARIAS Y COLEGIO DE NOTARIOS				
Usuarios	**Nombre de PC**	**Dirección IP**	**Equipo**	**Cantidad**
Notaria 8 Baños del Inca				
Notario	PC26	Laptop-PT	Core 7 / 1 TB	1
Área Legal	PC 27	PC-PT	Core 9 / 1 TB	1
Archivo	PC 28 – PC 29	PC-PT	Core 9 / 1 TB	2
Colegio de Notarios				
Administración	LAP TOP 3	Laptop-PT	Core 5 / 1 TB	1
Área Legal	PC 25 – PC 26	PC-PT	Core 7 / 1 TB	2
Archivo	PC 27 – PC-28	PC-PT	Core 7 / 1 TB	2

Fuente: Elaborado por el autor.

También se tiene los aplicativos siguientes:

Tabla 7. *Aplicativos utilizados*

Microsoft Dynamics	Acceso con
Microsoft Office 2019	licencia
Windows server 2003	
Windows XP SP3	
Antivirus AVG 2020	

Fuente: Elaborado por el autor.

4.2.3. Códigos de configuración

Procedemos a realizar la configuración de la Tecnología VPN (MPLS). El código se encuentra en el block de notas.

4.2.3.1. Activación del LoooBack

Los códigos de configuración para la activación del Loopback, se tiene para los router: P1, P2, P3, P4, PE1, PE2. Tenemos:

```
ACTIVACION DEL LOOPBACK
RouterP1
P1(config)#interface loopback 0
P1(config-if)# ip address 1.1.1.1 255.255.255.0

RouterP2
P2(config)#interface loopback 0
P2(config-if)# ip address 2.2.2.2 255.255.255.0

RouterP3
P3(config)#interface loopback 0
P3(config-if)# ip address 3.3.3.3 255.255.255.0

RouterP4
P4(config)#interface loopback 0
P4(config-if)# ip address 4.4.4.4 255.255.255.0

RouterPE1
PE1(config)#interface loopback 0
PE1(config-if)# ip address 5.5.5.5 255.255.255.0

RouterPE2
PE2(config)#interface loopback 0
PE2(config-if)# ip address 6.6.6.6 255.255.255.0
```

4.2.3.2. Activación de OSPF

Los códigos de configuración para la activación de OSP, se tiene para los router: P1, P2, P3, P4, PE1, PE2. Tenemos:

```
ACTIVACION DE OSPF
Router P1
P1#configure terminal
P1(config)# router ospf 1
P1(config-router)#router-id 1.1.1.1
P1(config-router)#network 10.10.0.0 0.0.0.255 area 0
P1(config-router)#network 1.1.1.1 0.0.0.0 area 0
```

```
Router P2
P2#configure terminal
P2(config)# router ospf 1
P2(config-router)#router-id 2.2.2.2
P2(config-router)#network 10.10.0.0 0.0.0.255 area 0
P2(config-router)#network 2.2.2.2 0.0.0.0 area 0

Router P3
P3#configure terminal
P3(config)# router ospf 1
P3(config-router)#router-id 3.3.3.3
P3(config-router)#network 10.10.0.0 0.0.0.255 area 0
P3(config-router)#network 3.3.3.3 0.0.0.0 area 0

Router P4
P4#configure terminal
P4(config)# router ospf 1
P4(config-router)#router-id 4.4.4.4
P4(config-router)#network 10.10.0.0 0.0.0.255 area 0
P4(config-router)#network 4.4.4.4 0.0.0.0 area 0

Router PE1
PE1#configure terminal
PE1(config)# router ospf 1
PE1(config-router)#router-id 5.5.5.5
PE1(config-router)#network 10.10.0.0 0.0.0.255 area 0
PE1(config-router)#network 5.5.5.5 0.0.0.0 area 0

Router PE2
PE2#configure terminal
PE2(config)# router ospf 1
PE2(config-router)#router-id 6.6.6.6
PE2(config-router)#network 10.10.0.0 0.0.0.255 area 0
PE2(config-router)#network 6.6.6.6 0.0.0.0 area 0
```

4.2.3.3. Configuración del LDP

Los códigos de configuración de LDP, se tiene para los router: P1, P2, P3, P4,

PE1, PE2. Tenemos:

```
CONFIGURACION DEL LDP

Router P1
P1#configure terminal
P1(config)# mpls ldp router-id loopback 0

P1(config)#router ospf 1
P1(config-router)#mpls ldp autoconfig
```

```
P1(config-router)#do wr

Router P2
P2#configure terminal
P2(config)# mpls ldp router-id loopback 0

P2(config)#router ospf 1
P2(config-router)#mpls ldp autoconfig
P2(config-router)#do wr

Router P3
P3#configure terminal
P3(config)# mpls ldp router-id loopback 0

P3(config)#router ospf 1
P3(config-router)#mpls ldp autoconfig
P3(config-router)#do wr

Router P4
P4#configure terminal
P4(config)# mpls ldp router-id loopback 0

P4(config)#router ospf 1
P4(config-router)#mpls ldp autoconfig
P4(config-router)#do wr

Router PE1
PE1#configure terminal
PE1(config)# mpls ldp router-id loopback 0

PE1(config)#router ospf 1
PE1(config-router)#mpls ldp autoconfig
PE1(config-router)#do wr

Router PE2
PE2#configure terminal
PE2(config)# mpls ldp router-id loopback 0

PE2(config)#router ospf 1
PE2(config-router)#mpls ldp autoconfig
PE2(config-router)#do wr
```

4.2.3.4. Códigos de subtuneo

El código subteneo se encuentra en el archivo de block de notas.

A continuación el código de subnuteo:

```
Router de notaria 1
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname Notaria1
Notaria1(config)#
Notaria1(config)#interface g0/0/0
Notaria1(config-if)#ip address 172.16.8.2 255.255.255.0
Notaria1(config-if)#no shutdown
Notaria1(config-if)#exit
Notaria1(config)#
Notaria1(config)#interface s0/1/0
Notaria1(config-if)#ip address 10.0.10.2 255.255.255.0
Notaria1(config-if)#no shutdown
------------------------------------------------------------
------------
Router de notaria 2
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname Notaria2
Notaria2(config)#
Notaria2(config)#interface g0/0/0
Notaria2(config-if)#ip address 172.16.0.3 255.255.255.0
Notaria2(config-if)#no shutdown
Notaria2(config-if)#exit
Notaria2(config)#
Notaria2(config)#interface s0/1/0
Notaria2(config-if)#ip address 10.0.20.4 255.255.255.0
Notaria2(config-if)#no shutdown
------------------------------------------------------------
--------------
Router de borde PE1
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname PE1
PE1(config)#
PE1(config)#interface s0/1/0
PE1(config-if)#ip address 10.0.10.5 255.255.255.0
PE1(config-if)#no shutdown
PE1(config-if)#exit
PE1(config)#interface s0/1/1
PE1(config-if)#ip address 10.0.20.5 255.255.255.0
PE1(config-if)#no shutdown
PE1(config-if)#exit
PE1(config)#interface s0/2/0
PE1(config-if)#ip address 10.10.14.5 255.255.255.0
PE1(config-if)#no shutdown
PE1(config-if)#exit
PE1(config)#interface s0/2/1
PE1(config-if)#ip address 10.0.20.5 255.255.255.0
```

```
PE1(config-if)#no shutdown
------------------------------------------------------------
---------------
Router proveedor P1
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname P1
P1(config)#
P1(config)#interface s0/1/0
P1(config-if)#ip address 10.10.14.1 255.255.255.0
P1(config-if)#no shutdown
P1(config-if)#exit
P1(config)#interface s0/2/0
P1(config-if)#ip address 10.10.16.1 255.255.255.0
P1(config-if)#no shutdown
P1(config-if)#exit
P1(config)#interface s0/1/1
P1(config-if)#ip address 10.10.15.1 255.255.255.0
P1(config-if)#no shutdown
P1(config-if)#exit
------------------------------------------------------------
-------------
Router proveedor P2
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname P2
P2(config)#
P2(config)#interface s0/1/0
P2(config-if)#ip address 10.10.18.2 255.255.255.0
P2(config-if)#no shutdown
P2(config-if)#exit
P2(config)#interface s0/2/0
P2(config-if)#ip address 10.10.18.2 255.255.255.0
P2(config-if)#no shutdown
P2(config-if)#exit
P2(config)#interface s0/1/1
P2(config-if)#ip address 10.10.20.2 255.255.255.0
P2(config-if)#no shutdown
P2(config-if)#exit

------------------------------------------------------------
------------
Router proveedor P3
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname P3
P3(config)#
P3(config)#interface s0/1/0
P3(config-if)#ip address 10.10.20.3 255.255.255.0
```

```
P3(config-if)#no shutdown
P3(config-if)#exit
P3(config)#interface s0/2/0
P3(config-if)#ip address 10.10.22.3 255.255.255.0
P3(config-if)#no shutdown
P3(config-if)#exit
P3(config)#interface s0/1/1
P3(config-if)#ip address 10.10.26.3 255.255.255.0
P3(config-if)#no shutdown
P3(config-if)#exit

------------------------------------------------------------
------------
Router proveedor P4
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname P4
P4(config)#
P4(config)#interface s0/1/0
P4(config-if)#ip address 10.10.15.4 255.255.255.0
P4(config-if)#no shutdown
P4(config-if)#exit
P4(config)#interface s0/2/0
P4(config-if)#ip address 10.10.22.4 255.255.255.0
P4(config-if)#no shutdown
P4(config-if)#exit
P4(config)#interface s0/1/1
P4(config-if)#ip address 10.10.28.4 255.255.255.0
P4(config-if)#no shutdown
P4(config-if)#exit

------------------------------------------------------------
------------
Router de borde PE2
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname PE2
PE2(config)#
PE2(config)#interface s0/2/0
PE2(config-if)#ip address 10.10.28.6 255.255.255.0
PE2(config-if)#no shutdown
PE2(config-if)#exit
PE2(config)#interface s0/2/1
PE2(config-if)#ip address 10.10.26.6 255.255.255.0
PE2(config-if)#no shutdown
PE2(config-if)#exit
PE2(config)#interface s0/1/1
PE2(config-if)#ip address 10.0.30.6 255.255.255.0
PE2(config-if)#no shutdown
PE2(config-if)#exit
```

```
PE2(config)#interface s0/1/0
PE2(config-if)#ip address 10.0.40.6 255.255.255.0
PE2(config-if)#no shutdown
PE2(config-if)#exit

------------------------------------------------------------
------------
Router de borde Notaria3
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname Notaria3
Notaria3(config)#
Notaria3(config)#interface s0/1/0
Notaria3(config-if)#ip address 10.0.30.3 255.255.255.0
Notaria3(config-if)#no shutdown
Notaria3(config-if)#exit
Notaria3(config)#interface g0/0/0
Notaria3(config-if)#ip address 192.168.16.2 255.255.255.0
Notaria3(config-if)#no shutdown
Notaria3(config-if)#exit

------------------------------------------------------------
------------
Router de borde ColegioNotarios
-------------------
Router>enable
Router#configure terminal
Router(config)#hostname ColegioNotarios
ColegioNotarios(config)#
ColegioNotarios(config)#interface s0/1/0
ColegioNotarios(config-if)#ip address 10.0.40.3
255.255.255.0
ColegioNotarios(config-if)#no shutdown
ColegioNotarios(config-if)#exit
ColegioNotarios(config)#interface g0/0/0
ColegioNotarios(config-if)#ip address 192.168.10.2
255.255.255.0
ColegioNotarios(config-if)#no shutdown
ColegioNotarios(config-if)#exit
```

4.2.4. Estructura de la Topología de la Red con Distribución Geográfica

La red de distribución es por la interconexión en red privada de las notarías y el colegio de notarios para el acceso de información y documentos en archivo, los cuales se van digitalizando.

Se tienen:

06 Notarias en Cajamarca ciudad

02 Notarias en Baños del Inca

01 Colegio de Notarios

Para evitar la sobre carga de visualización, se descompuso en una estructura mínima en la conformación tecnológica VPN (MPLS), para ellos se subnetearon 3 notarias y el Colegio de Notarios.

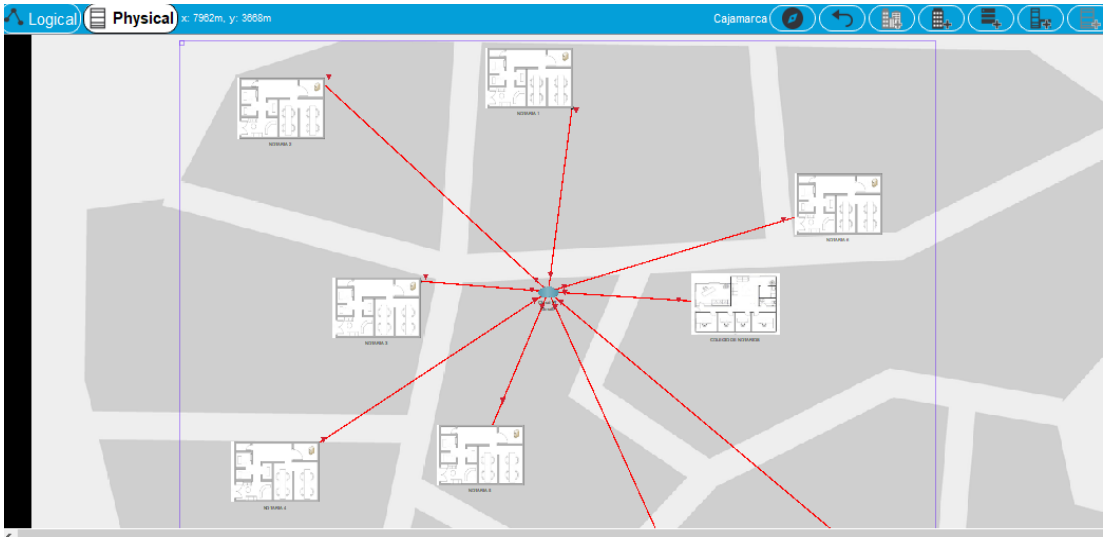


***Figura 13**. Topología física del estudio*

Fuente: Elaborado por el autor.

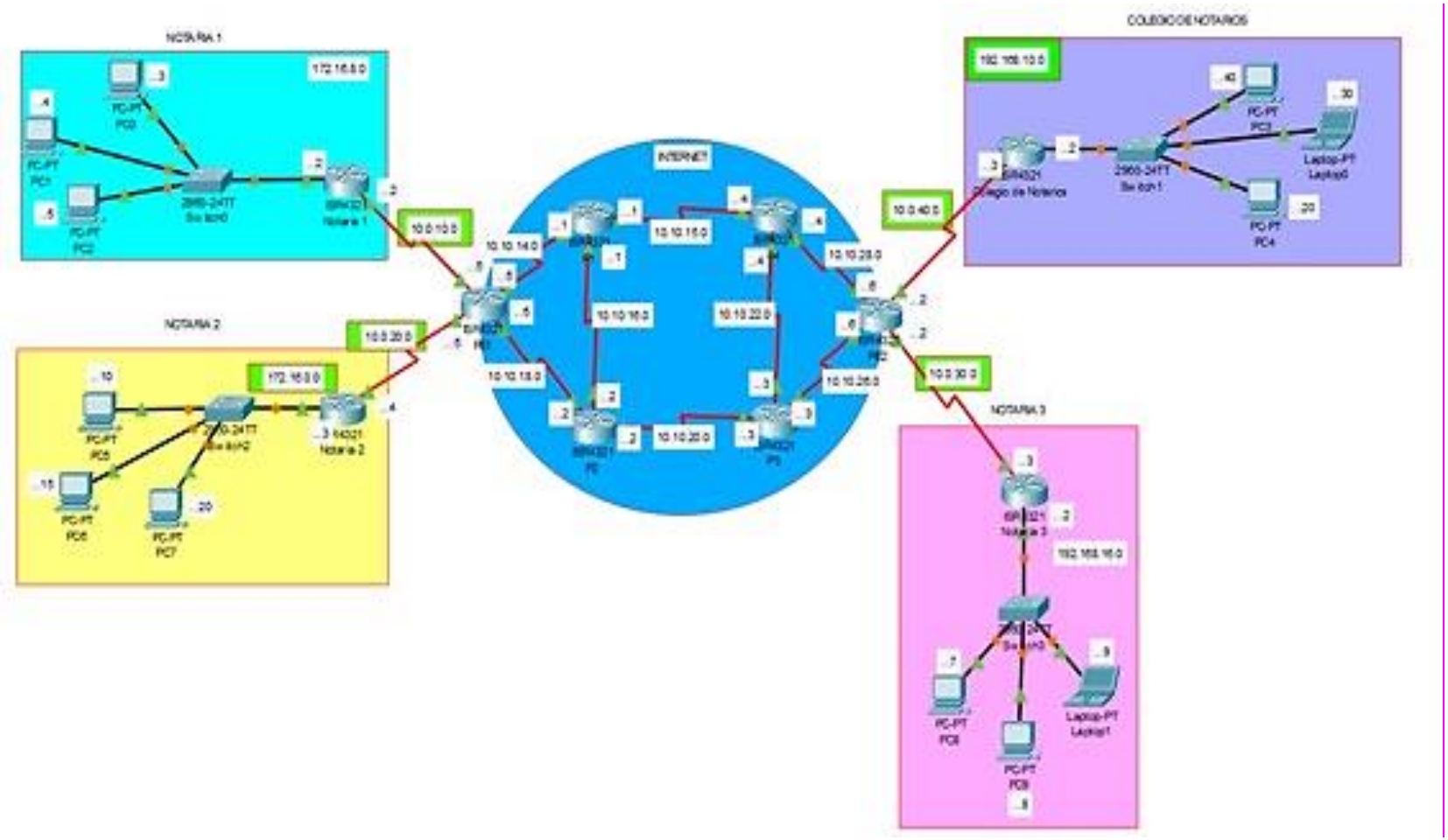


Figura 14. Estructura lógica de configuración de tecnología VPN (MLS)
Fuente: Elaborado por el autor.

4.2.5. Armado de la topología física

La secuencia de desarrollo del armado de la topología física entre las Notarías y el Colegio de Notarios es la siguiente:

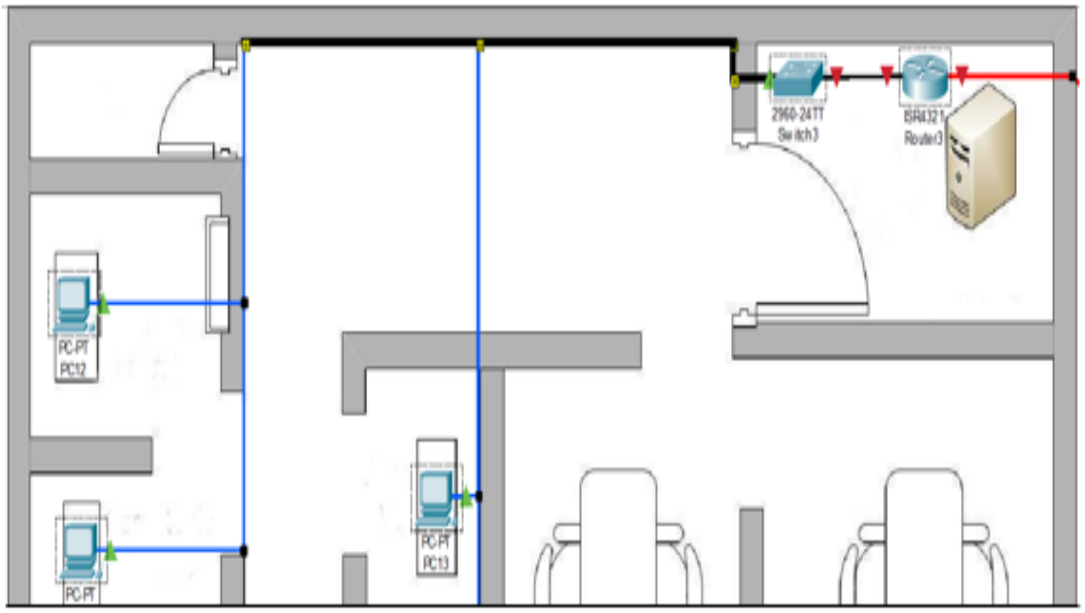


Figura 15. Armado de topología física de la Notaría
Fuente: Elaborado por el autor

La conexión a cada ordenador por áreas, siendo en las notarías lo más común las oficinas de administración o notario, el área legal donde se encuentran los asesores jurídicos, y el área de archivo, vemos en la figura 16 las conexiones del servidor, el router y PC´s.

Podemos observar en la figura 17, la estructura completa, de las Notarías y el Colegio de Notarios.

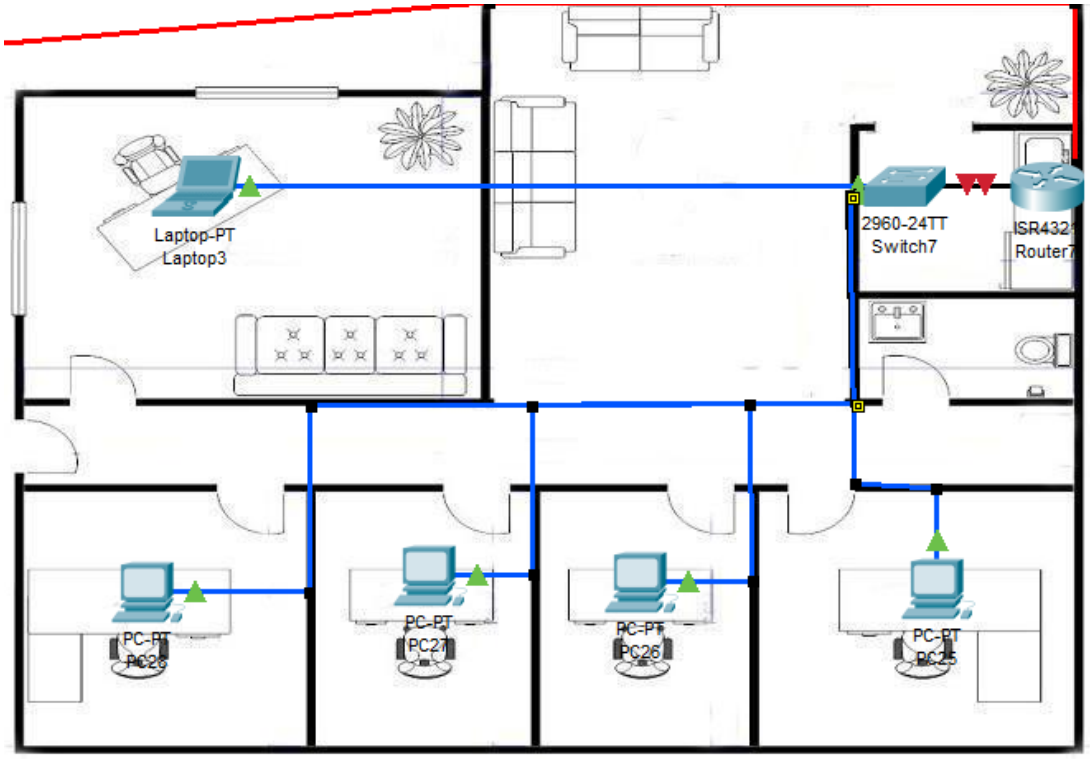


Figura 16. Topología del Colegio de Notarios
Fuente: Elaborado por el autor

4.2.5.1. Asignación de IPS

Luego de tener la estructura lógica, se sigue a destinar, el IPS de cada grupo de red interconectada.

En la figura 15 podemos ver los IPS en el internet en cada ISR (Interruption Service Rutine), el cual dentro de la programación establecida nos va a permitir interrumpir la señal recepcionada por el procesador o MCU, donde se le indica la acción de "interrumpir" el curso del proceso actual y luego proceder a ejecutar el código específico dado para tratar el caso.

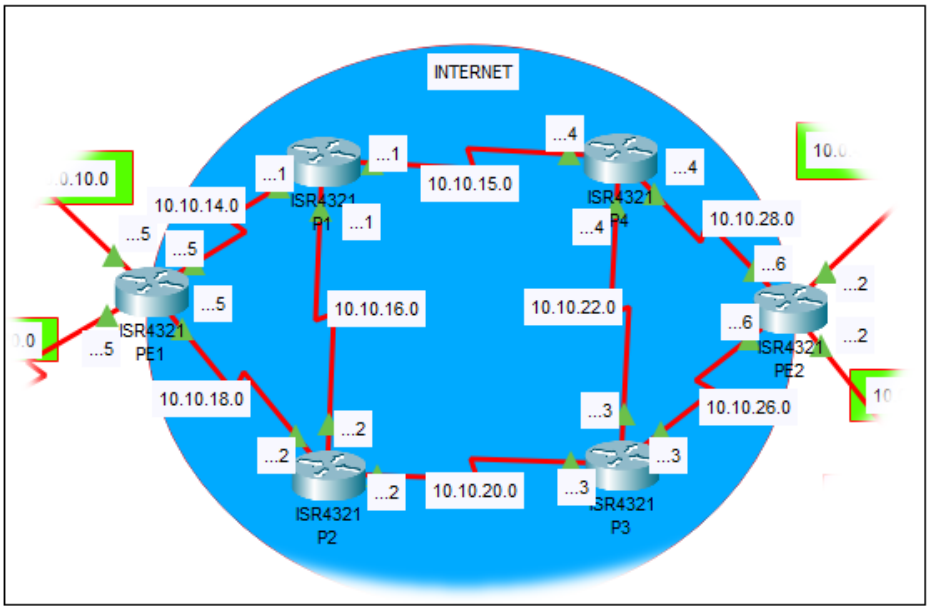


Figura 17. Interruption Service Rutine del sistema con IPS asignados.
Fuente: Elaborado por el autor

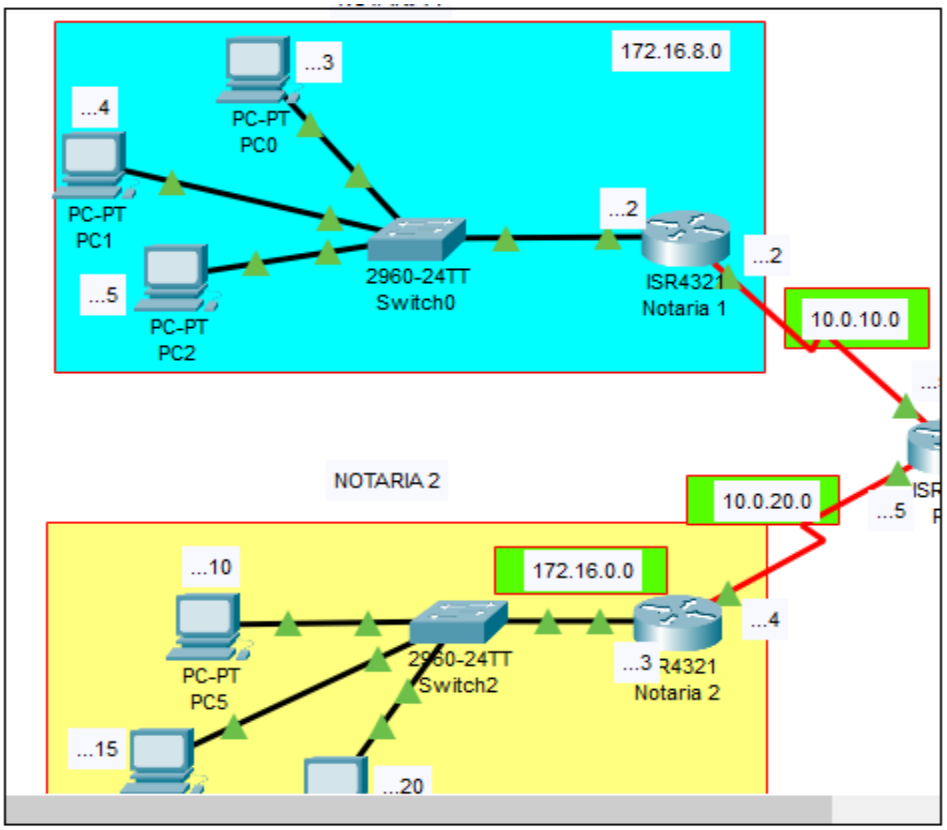


Figura 18. Asignación de IPS en las notarias
Fuente: Elaborado por el autor.

4.2.6. Simulación del proceso y pruebas

En la simulación podemos ver las pruebas del funcionamiento.

a. Se realiza la petición desde la computadora de la Notaría 1 hacia una computadora del Colegio de Notarios

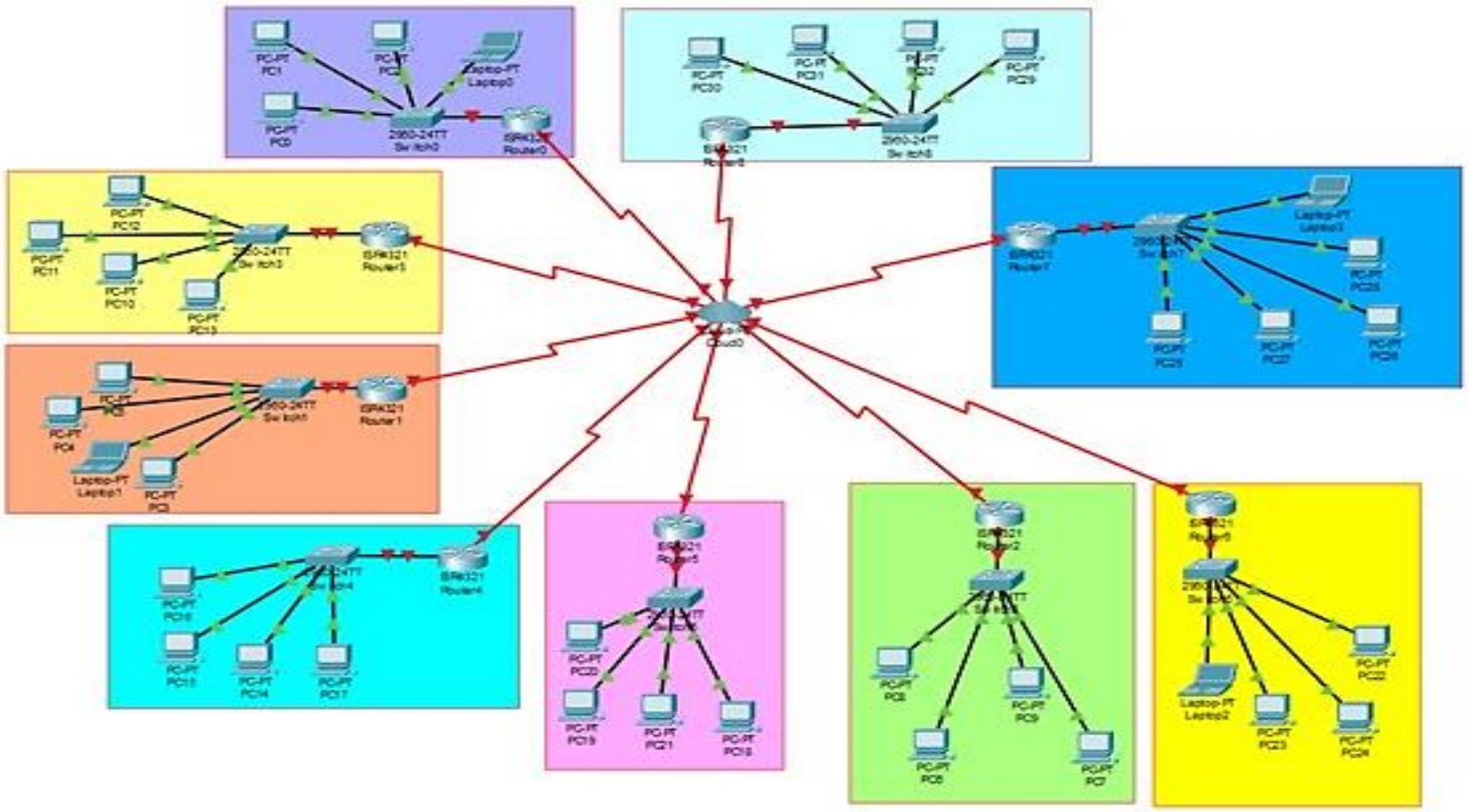


Figura 19. Simulación de conectividad del Colegio de Notarios y 09 notarias
Fuente: Elaborado por el autor.

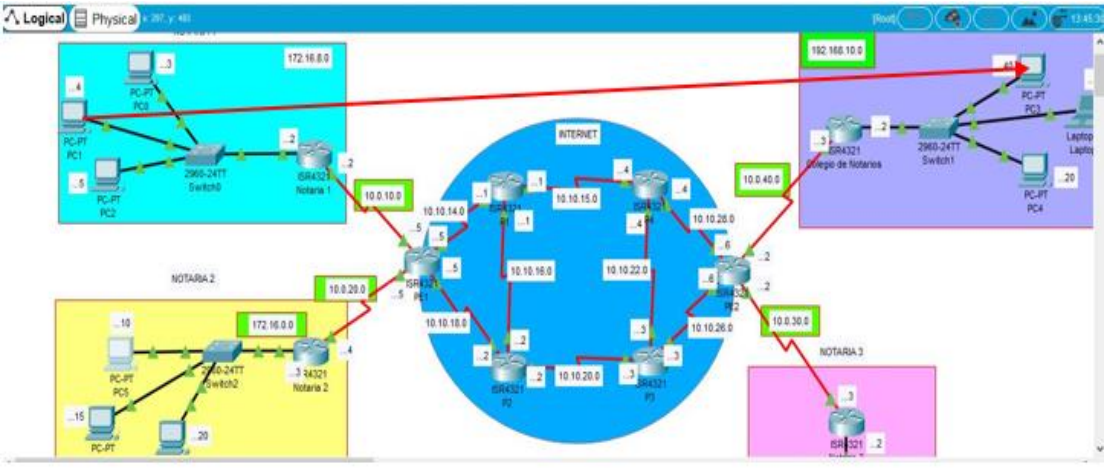


Figura 20. Petición de Notaria a Colegio de Notarios
Fuente: Elaborado por el autor

Como vemos en la figura 22 se realiza la petición de información de la PC1 de la notaria 1, se genera el pedido informático el cual recorre al switch 2960-24TT y se direcciona por el router ISR4321 a la PC3 del Colegio de Notarios.

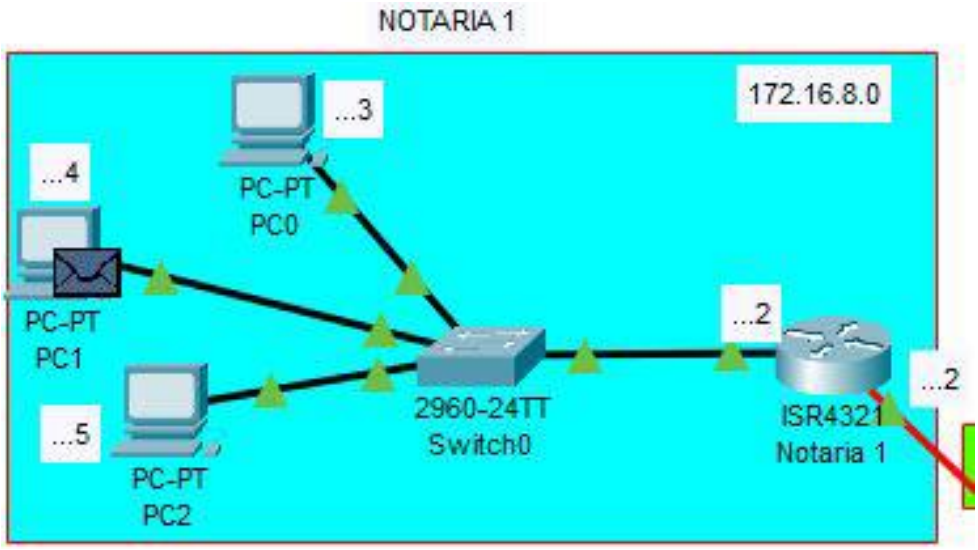


Figura 21. *Petición de información de la Notaria 1*
Fuente: Elaborado por el autor

En la figura 22 vemos el sobre que emigra de la PC1 hacia el ISR4321 de la notaria 1.

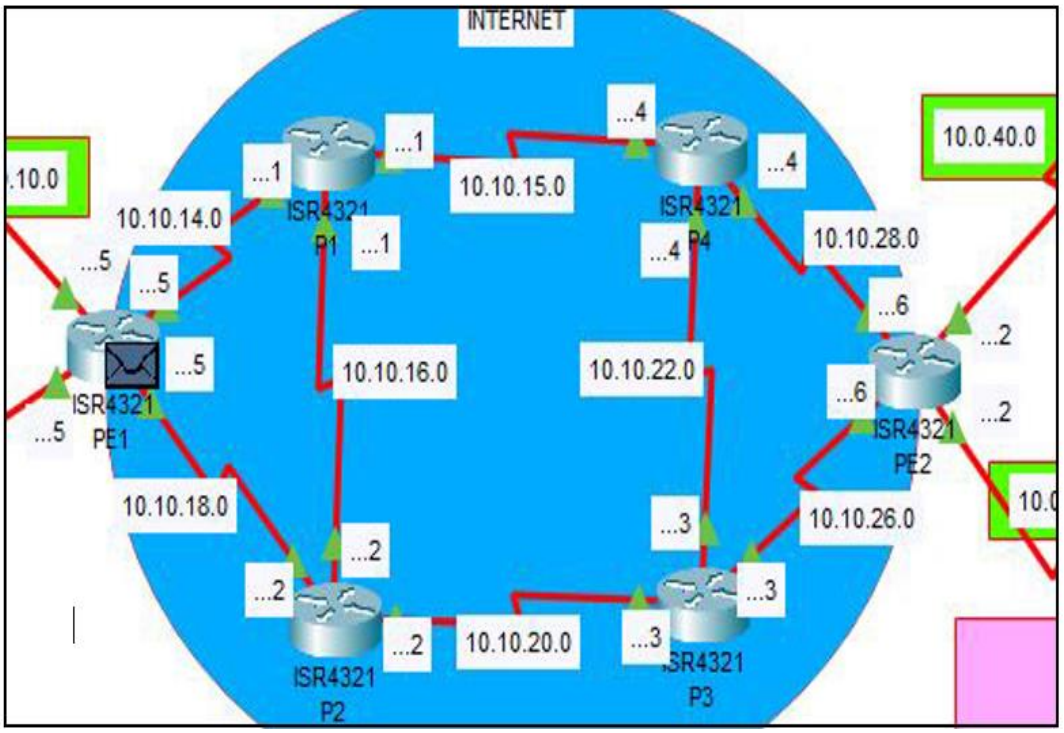


Figura 22. Envío del mensaje por el medio Internet (1).
Fuente: Elaborado por el autor.

b. En la figura 23, 24, 25 y 26, podemos detallar el movimiento de información por medio de internet en dirección del Colegio de Notarios.

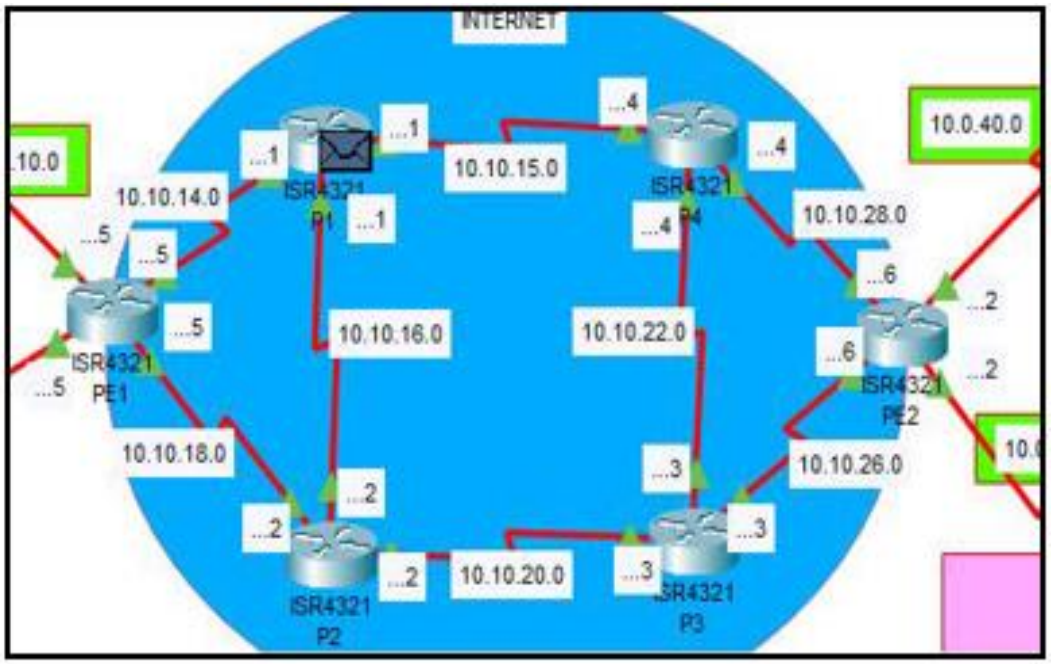


Figura 23. Envío del mensaje por el medio Internet (2).
Fuente: Elaborado por el autor.

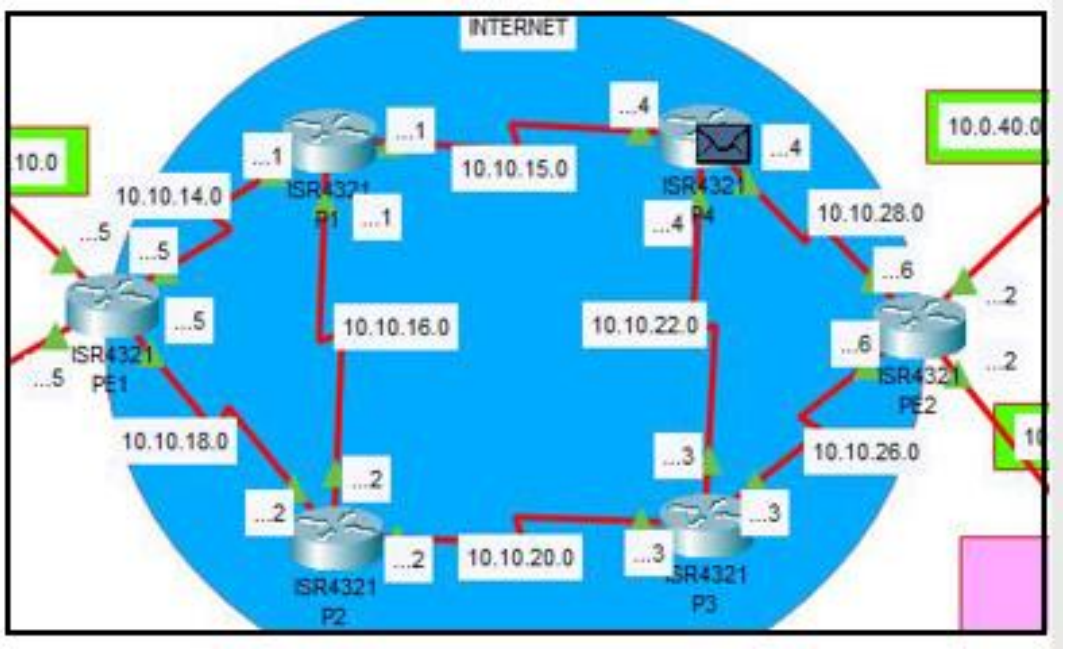


Figura 24. Envío del mensaje por el medio Internet (3).
Fuente: Elaborado por el autor.

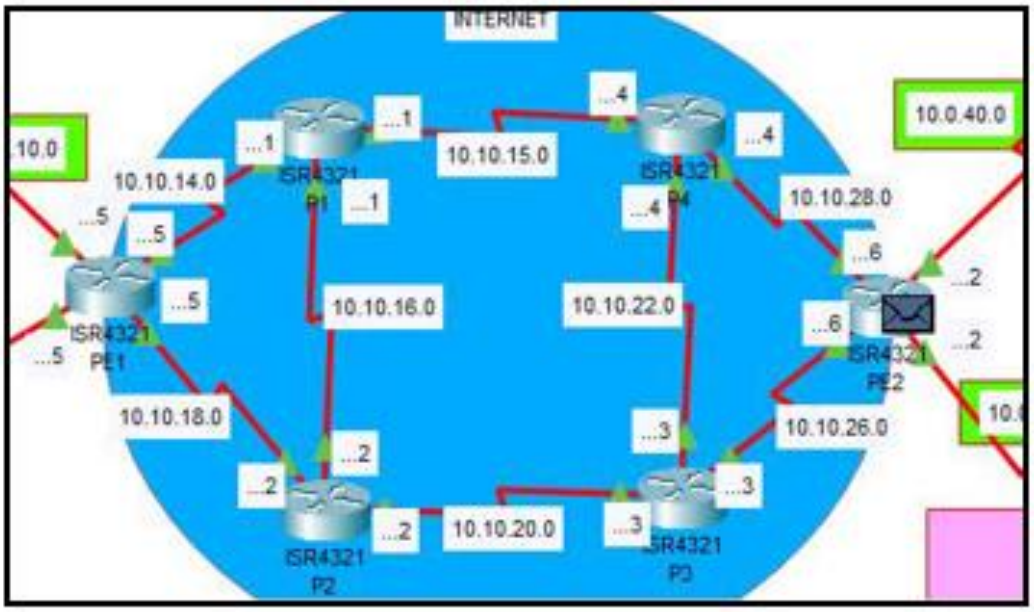


Figura 25. Envío del mensaje por el medio Internet (3).
Fuente: Elaborado por el autor.

c. En la figura 27 y 28, podemos detallar el movimiento de información por el medio de internet, vinculando el ISR del Colegio de Notarios.

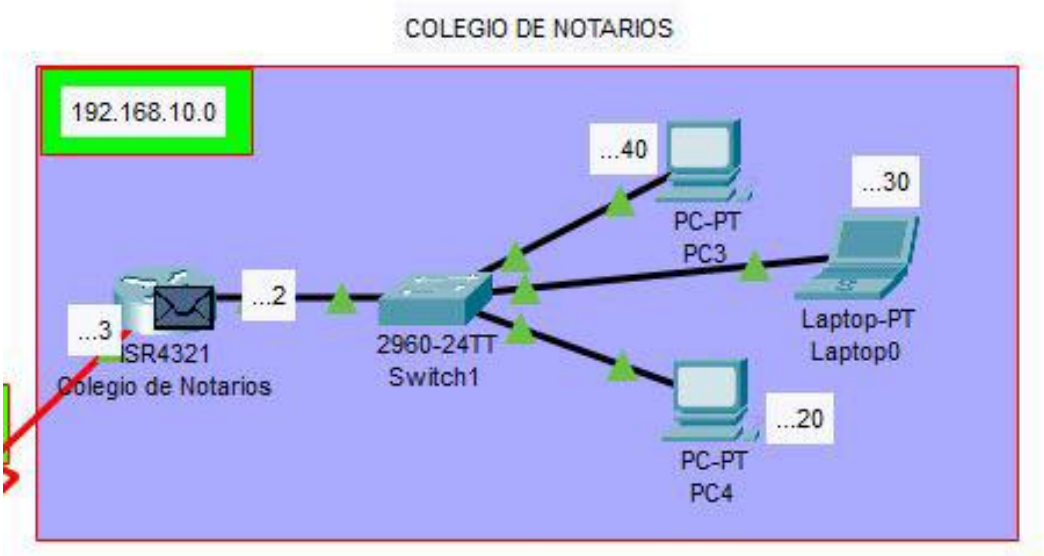


Figura 26. Recepción de la información al ISR del Colegio de Notarios.
Fuente: Elaborado por el autor

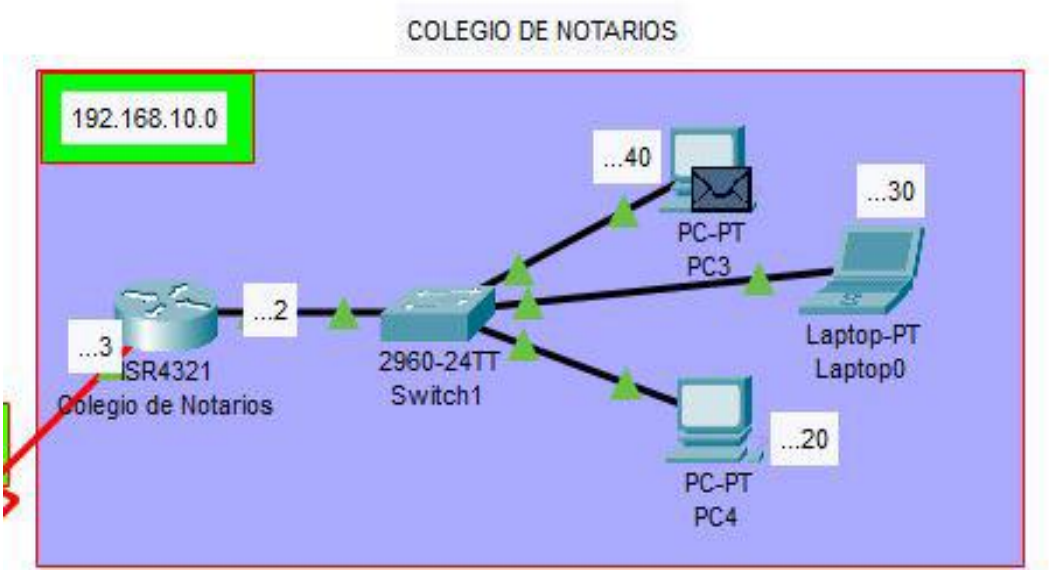


Figura 27. Recepción de la información al ISR del Colegio de Notarios (2).
Fuente: Elaborado por el autor.

4.2.6.1. Prueba alterna del Sistema

Otro medio de corroborar si el sistema funciona correctamente es realizando Ping mediante la consola del sistema. En nuestro caso realizaremos el ping desde el ordenador como se muestra en las figuras 29 y 30.

Luego con el Command Pront del Packet Tracer PC del Command Line aplicamos el ping, por lo tanto quiere decir que si existe comunicación correcta de un punto a otro.

Las pruebas de conectividad (Ping) entre servidores DC y DB primarios con los secundarios, siempre aplicando las direcciones IP privada, con lo que se puede comprobar el estado de la red y el perfecto direccionamiento IP.

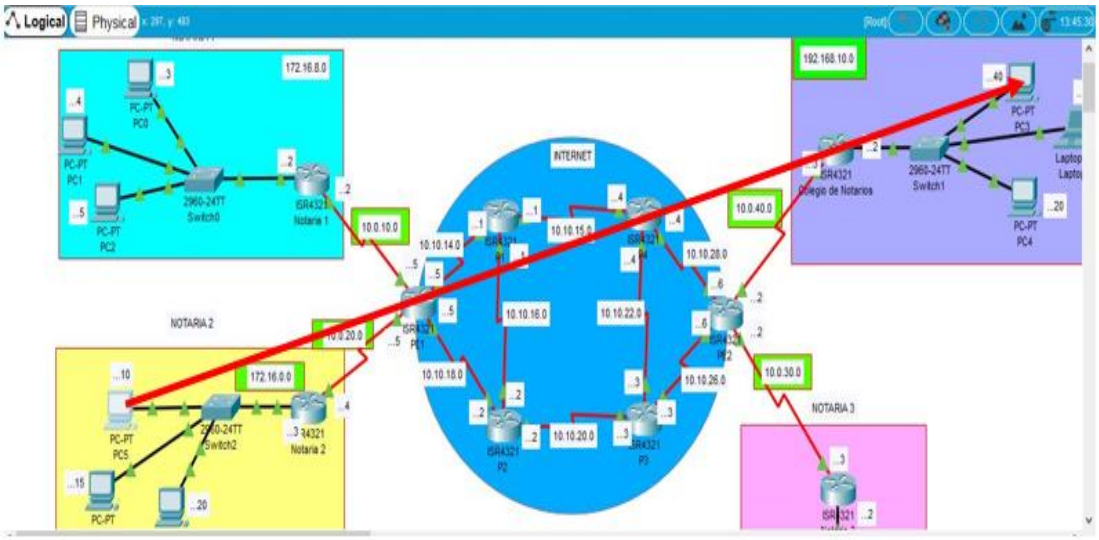


Figura 28. Acción ping desde el ordenador.
Fuente: Elaborado por el autor.

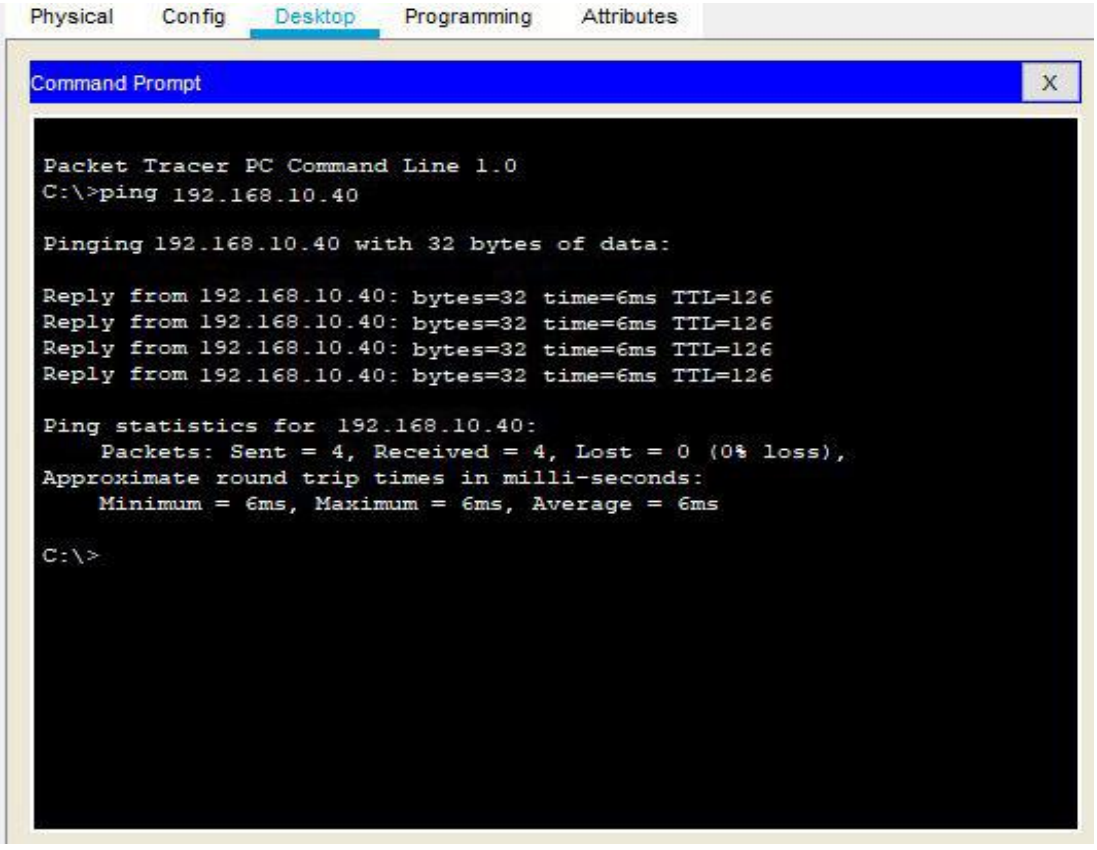


Figura 29. Ping Ping en el Command Promt
Fuente: Elaborado por el autor.

Las pruebas de conectividad (Ping) entre servidores de cada notaria y el Colegio de Notarios utilizando las direcciones IP públicas destinadas por el ISP, con lo que a posterior se realizan las pruebas de conexión y funcionamiento VPN entre ambos servidores DC y BD (Figura 31).

Luego de recepcionada la petición, el área pertinente responde y enviará la información requerida, siguiendo la misma trayectoria de origen y recepciona la información requerida en la petición.

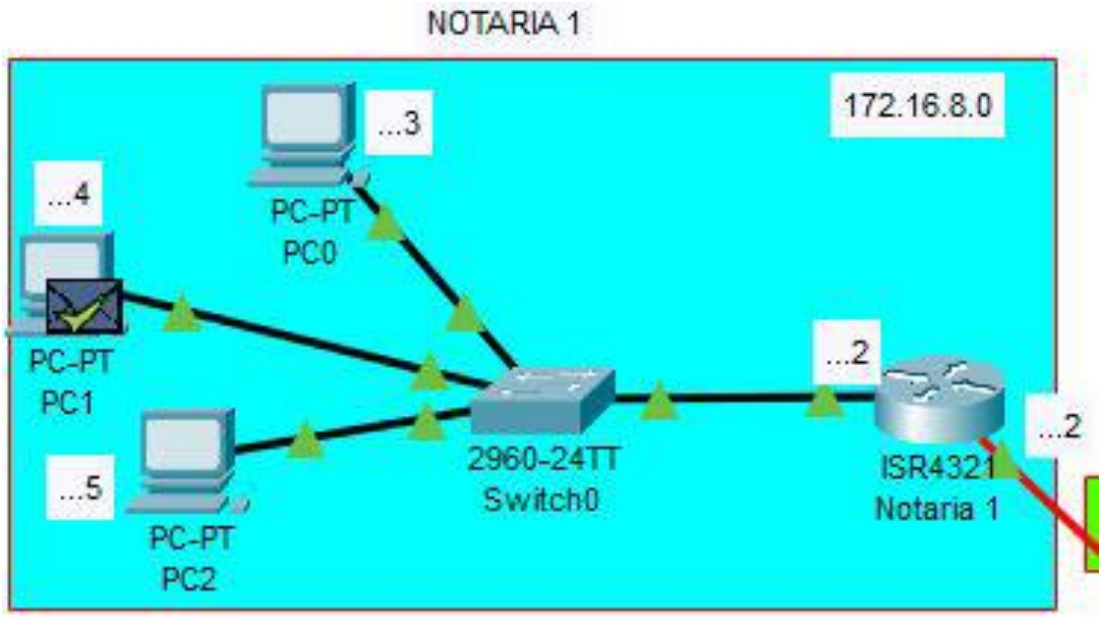


Figura 30. Recepción de notaria 1 de los datos requeridos.
Fuente: Elaborado por el autor.

CAPÍTULO 5

RESULTADOS Y DISCUSIÓN

5.1. Resultados específicos

Tabla 8. *Resultados* de prueba antes y después de los KPI´s

N°	KPI_1 Tiempo de Latencia del servicio de comunicación		KPI_2 N° de saltos que desplaza el paquete de datos		KPI_3 Tiempo de carga en el ingreso al sistema informático	
	Pre - prueba	Post - prueba	Pre - prueba	Post - prueba	Pre - prueba	Post - prueba
1	980	8	6	4	5	0.05
2	940	9	11	8	7	0.05
3	940	8	9	6	5	0.05
4	950	10	9	6	5	0.07
5	960	12	11	8	6	0.07
6	950	10	6	4	5	0.09
7	1300	9	6	4	4	0.06
8	1400	11	8	6	5	0.06
9	940	10	6	4	4	0.06
10	1510	8	6	4	5	0.05
11	1500	8	8	6	5	0.05
12	1500	9	8	6	5	0.06
13	1350	9	6	4	4	0.06
14	1350	10	6	4	5	0.09
15	1450	8	8	6	5	0.09
16	940	10	8	6	6	0.09
17	1400	10	11	8	6	0.07
18	1000	9	6	4	4	0.07
19	1150	8	6	4	4	0.09
20	1300	9	6	4	4	0.09
21	1250	11	8	6	5	0.06
22	1300	8	8	6	5	0.06
23	950	8	6	4	4	0.06
24	1100	9	6	4	4	0.05
$\bar{X}$	1183.75	9.21	7.46	5.25	4.76	0.07
D.E	219.30	1.14	1.74	1.42	0.77	0.02

Fuente: Elaboración propia del autor.

5.2. Análisis de Resultados Genéricos

En la tabla 13 tenemos los resultados de las pruebas realizadas antes y después de la prueba.

Tabla 9. Interpretación de resultados de los datos Pre- Prueba y Post – Prueba.

Indicadores	Pre – prueba (Media: X1)	Post-Prueba (Media X2)
KPI_1: Tiempo de latencia en envío de información.	1229.6 milisegundos	9.21 milisegundos
KPI_2: N° de saltos recorridos del paquete de datos origen – destino.	7.46 saltos	5.25 Saltos
KpI_3: Tiempo de carga en las transacciones en el sistema informático.	4.76 minutos	0.07 minutos

Fuente: Elaboración propia del autor.

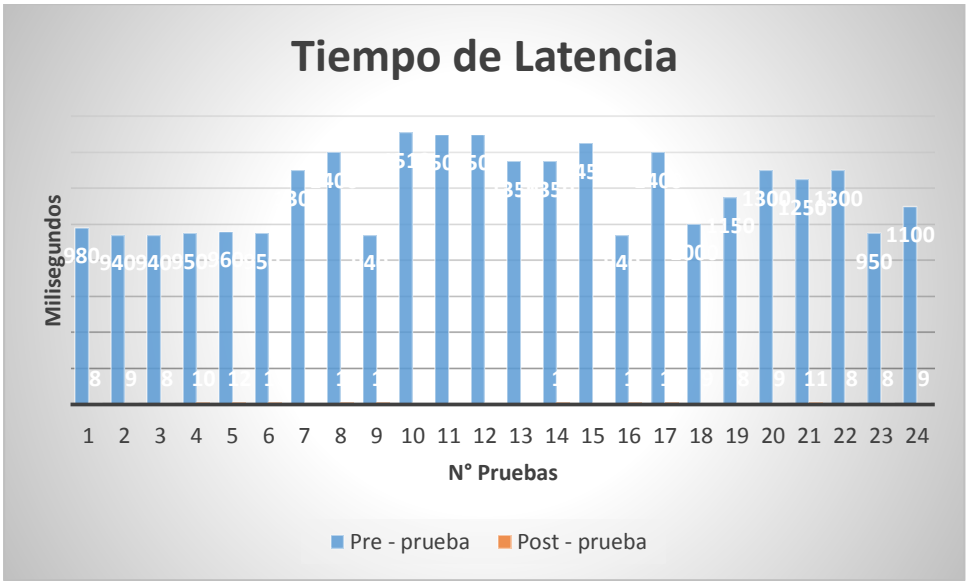


Figura 31. Comparativo de latencia Pre y Post - Prueba
Fuente: Elaboración propia del autor.

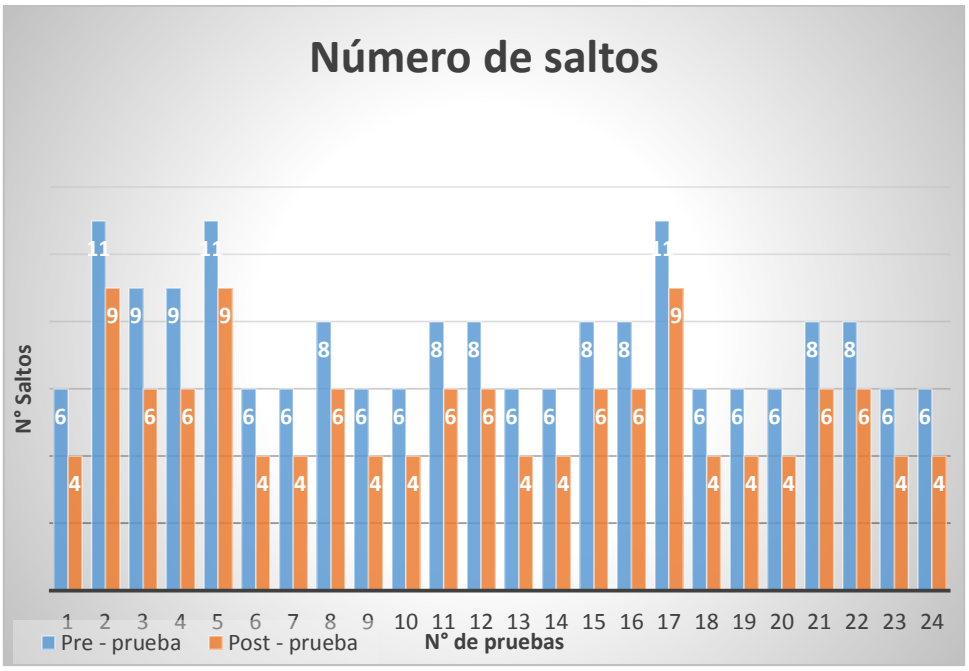


Figura 32. Comparativo de latencia Pre - Post Prueba
Fuente: Elaboración propia del autor.

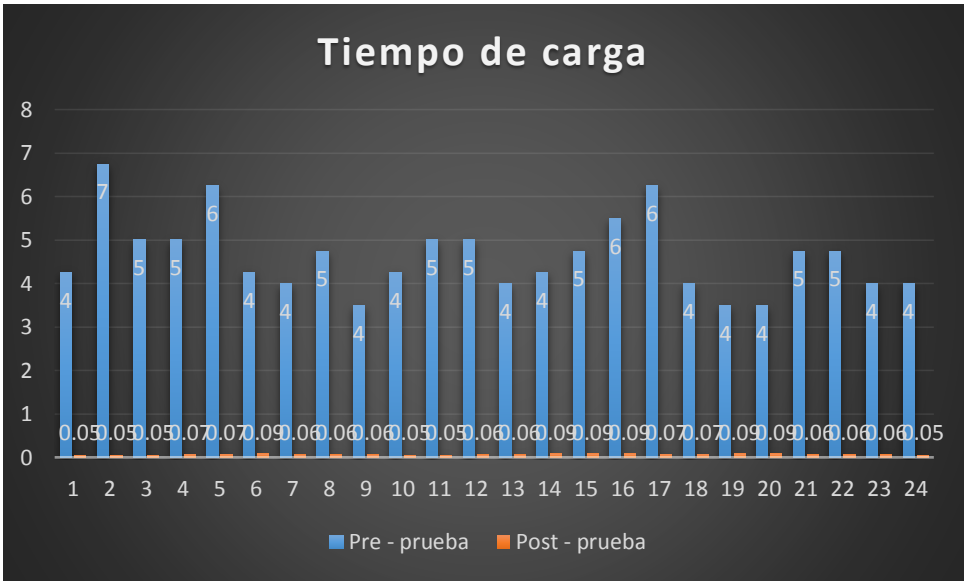


Figura 33. Comparativo de tiempos de carga Pre y Post - Prueba.
Fuente: Elaboración propia del autor.

a. Tiempo de latencia en el envío de información

Conforme a la tabla 9, el 45.83% de tiempo de latencia de pre prueba son mayores al tiempo promedio logrado, con la post prueba tenemos que el 62.5% tiene tiempos menores de tiempo de latencia en el promedio logrado.

La totalidad del producto obtenido en el tiempo latente en la remisión de data en Post- Prueba son menores que los promedios de la Pre- Prueba.

Tabla 10. KPI_1: Mediana y DE.

	KPI_1 Tiempo de Latencia del servicio de comunicación	
	Pre - prueba	**Post - prueba**
Promedio	1183.75	9.21
Desviación estándar	219.30	1.14

Fuente: Elaboración propia del autor.

b. Número de saltos recorridos por paquete de datos origen – destino.

De acuerdo a la tabla 9, el 50% de tiempo de latencia de pre prueba son mayores al tiempo promedio logrado, con la post prueba tenemos que el 50% tiene tiempos menores de tiempo de latencia en el promedio logrado.

El 100% de los resultados obtenidos por el tiempo de latencia del envío de información en la Post- Prueba se ven que son menores que el tiempo promedio de la Pre- Prueba.

Tabla 11. *KPI_2: Mediana y DE.*

	KPI_2 N° de saltos que desplaza el paquete de datos	
	Pre - prueba	**Post - prueba**
Promedio	7.46	5.25
Desviación estándar	1.74	1.42

Fuente: Elaboración propia del autor.

c. Tiempo de carga en las transacciones del sistema informático

De acuerdo a la tabla 9, el 50 % de tiempo de latencia de pre prueba son mayores al tiempo promedio logrado, con la post prueba se advierte que el 75 % tiene tiempos menores de tiempo de latencia en el promedio logrado.

El 100% de los resultados obtenidos por el tiempo de latencia del envío de información en la Post- Prueba se ven que son menores que el tiempo promedio de la Pre- Prueba.

Tabla 12. *KPI_3: Mediana y DE.*

	KPI_4 Tiempo de carga en el ingreso al sistema informático	
	Pre - prueba	**Post - prueba**
Promedio	4.676	0.07
Desviación estándar	0.77	0.02

Fuente: Elaboración propia del autor.

5.3. Limitaciones del estudio

Las limitantes del estudio fueron la de levantar a base de datos SQL, programación de las computadoras y demás dispositivos informáticos para su validación. Por la coyuntura que se da en estos momentos por el COVID 19, donde no hay accesibilidad a las notarías solo del personal mínimo que atiende al público mediante citas.

5.4. Implicancias del estudio

El presente trabajo, es un aporte muy importante para la comunidad en general del pueblo de Cajamarca, el Colegio de Notarios y las Notarías de Cajamarca y Baños del Inca. Contribuyendo por medio de la informática y sistemas a la facilidad y accesibilidad en breves plazos a los diversos documentos legales registrados en décadas pasadas que se encuentran en archivo del Colegio de Notarios de Cajamarca.

Las notarías, de acuerdo a lo solicitado, trámites documentarios legales, procesos judiciales, notariales, entre otros. La documentación legal de períodos donde no se digitalizaban los documentos, notarias fenecidas, entre otros se encuentran en custodia en el archivo del Colegio de Notarios, que con el sistema propuesto, las diversas notarías pueden solicitar la documentación pertinente al Colegio de Notarios, as u vez éste digitaliza los documentos de archivo y los envía vía on line de forma segura la notaría solicitante. Lo cual trae beneficios de rapidez de emisión y recepción e información, menores costos de envío y trámite documentario físico.

5.5. Contrastación de la hipótesis

5.5.1. Nivel de confianza y grado de significancia

En la corroboración de la hipótesis se aplicaron:

- El nivel de confianza del 95%
- El nivel de significancia del 5%

5.5.2. Estadígrafo para determinar la interconexión y acceso a la información antes y después del uso de la simulación del uso de una RPV a través de un MPLS.

Para contrastar la hipótesis vemos el comparativo de las muestra Pre – Prueba y Post – Prueba de los KPI´s para la propuesta de Influencia del uso de una red privada virtual a través de un MPLS en la interconexión y el acceso a la información en tiempo real de las notarías del distrito de Cajamarca, Baños del Inca y el colegio de notarios.

A. Contrastación con la variable KPI_1: Tiempo de Latencia en el Envío de la Información.

En la validación de la repercusión del uso de la Red Privada Virtual por medio de un MPLS en el tiempo de latencia en el envío de datos se procedió haciendo muestreos. La medición se realizó previamente a instalar la RPV (Pre – Prueba) y la otra medición posteriormente a la instalación de la RPV (Post-Prueba). A continuación mostramos los Tiempos de Latencia en el envío de datos de ambas muestras:

Tabla 13. *Datos de muestra Pre - Prueba KPI₁.*

Pre – Prueba							
980	940	940	950	960	950	1300	1400
940	1510	1500	1500	1350	1350	1450	940
1400	1000	1150	1300	1250	1300	950	1100

Fuente: Elaboración propia del autor.

El testeo dirigido al tiempo latente se miden en mili segundos previos a instalar la VPN.

Tabla 14. Datos de muestra Post – Prueba KPI_1

Post – Prueba							
8	9	8	10	12	10	9	11
10	8	8	9	9	10	8	10
10	9	8	9	11	8	8	9

Fuente: Elaboración propia del autor.

El testeo dirigido al tiempo latente se miden en mili segundos posterior a instalar la VPN.

Hi: El uso de una RPV reduce el tiempo de latencia en el envío de información (Post – Prueba en comparación al muestreo donde no se aplica la RPV (Pre – Prueba).

Planteamiento de la Hipótesis

$\bar{x}1$ = Media del Tiempo de latencia en el envío de información Pre – Prueba.

$\bar{x}2$ = Media del Tiempo de latencia del envío de información Post – Prueba.

H0: $\bar{x}1 = \bar{x}2$, en donde:

Ha: $\bar{x}1 > \bar{x}2$

Criterios de decisión

Las muestras son datos independientes y no parametrados de acuerdo a la técnica de Mann – Whitney.

Tabla 15.Estadística KPI_1

Muestra	N	Mediana
¨Pre – Prueba KPI_1	24	1,183.75
Post – Prueba KPI_1	24	9.21

Fuente: Elaboración propia del autor.

Tabla 16. Confianza lograda KPI_1

Diferencia	IC Pre - Prueba	IC Post - Prueba
1175	12.3%	95.4%

Fuente: Elaboración propia del autor.

Decisión estadística

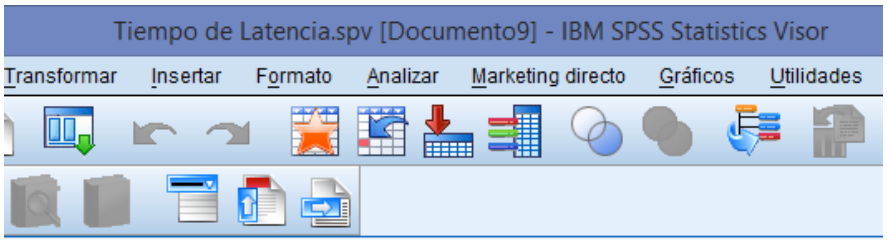
Ha: $\bar{x}1 > \bar{x}2$

Donde la hipótesis alterna es mayor donde $\bar{x}2$ es mayor a 0.05

$\bar{x}1 > \bar{x}2$

1,183.75 > 9.21

Haciendo uso del método estadístico de Mann – Whitney, y aplicando el programa IBM SPSS Statistic, tenemos:




```
NPAR TESTS
  /M-W= Tiempo_latencia BY Grupos(1 2)
  /MISSING ANALYSIS.
```

Pruebas NPar

Prueba de Mann-Whitney

Rangos

	Pre_Post_Prueba	N	Rango promedio	Suma de rangos
Tiempo de latencia	1	24	36,50	876,00
	2	24	12,50	300,00
	Total	48		

Estadísticos de prueba[a]

	Tiempo de latencia
U de Mann-Whitney	,000
W de Wilcoxon	300,000
Z	-5,970
Sig. asintótica (bilateral)	,000

a. Variable de agrupación: Pre_Post_Prueba

Figura 34.Prueba Mann- Whitney: Tiempo de latencia
Fuente: Elaboración propia del autor.

Interpretación: Como podemos ver el estadígrafo de U de Mann – Whitney es de 0.000 y el valor de p (Sig. Asintót. (bilateral)) es 0.000, puesto que el valor $p = 0.000 < \alpha = 0.05$, por lo que se rechaza la hipótesis nula y se concluye que el uso de una RPV reduce el tiempo de latencia en el envío de información (Post – Prueba) con respecto al muestreo donde no se aplica la RPV (Pre – Prueba), con un nivel de significancia del 5%.

Los resultantes evidencian que se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (ha). En donde la prueba estadística es significativa.

B. Contrastación de la variable: Número de saltos recorridos del paquete de datos origen – destino. KPI_2

En la validación del impacto en el uso de una Red Privada Virtual por medio de un MPLS en el número de saltos recorridos del paquete de datos origen – destino, por lo que se aplicó haciendo muestreos. La medición se realizó antes de la implementación de la RPV (Pre – Prueba) y la otra medición después de la implementación de la RPV (Post-Prueba).

En las tablas siguientes mostramos el número de saltos recorridos del paquete de datos origen – destino de los dos muestreos:

Tabla 17. *Saltos de muestra Pre - Prueba KPI_2*

Pre – Prueba							
6	11	9	9	11	6	6	8
6	6	8	8	6	6	8	8
11	6	6	6	8	8	6	6

Fuente: Elaboración propia del autor.

El testeo dirigido al número de saltos recorridos del paquete de datos origen – destino en saltos antes de la implementación de la VPN.

Tabla 18*. Datos de muestra Post - Prueba KPI_2*

Post – Prueba							
4	8	6	6	8	4	4	6
4	4	6	6	4	4	6	6
8	4	4	4	6	6	4	4

Fuente: Elaboración propia del autor.

El testeo dirigido al número de saltos recorridos del paquete de datos origen – destino en saltos después de la implementación de la VPN.

Hi: El uso de una RPV reduce el número de saltos recorridos del paquete de datos origen – destino (Post – Prueba) con respecto al muestreo donde no se aplica la RPV (Pre – Prueba).

Planteamiento de la Hipótesis

$\bar{x}1$ = Media del número de saltos recorridos del paquete de datos origen – destino en la red de Pre – Prueba.

$\bar{x}2$ = Media del número de saltos recorridos del paquete de datos origen – destino de red Post – Prueba.

H0: $\bar{x}1 = \bar{x}2$, en donde:

Ha: $\bar{x}1 > \bar{x}2$

Criterios de decisión

Las muestras son datos independientes y no parametrados.

Tabla 19. *Estadística KPI_2*

Muestra	N	Mediana
¨Pre – Prueba KPI_2	24	7.46
Post – Prueba KPI_2	24	5.25

Fuente: Elaboración propia del autor.

Tabla 20. *Confianza lograda KPI_2*

Diferencia	IC Pre - Prueba	IC Post - Prueba
12.21	95.4%	94.3%

Fuente: Elaboración propia del autor.

Decisión estadística

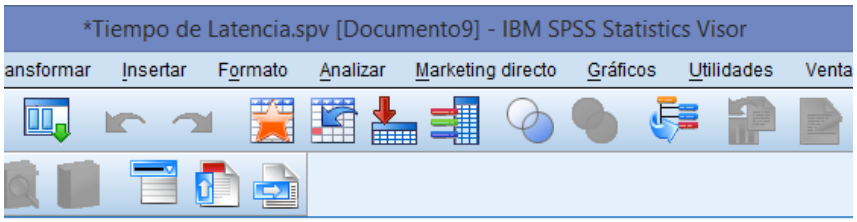
Ha: $\bar{x}1 > \bar{x}2$

Donde la hipótesis alterna es mayor donde $\bar{x}2$ es mayor a 0.05

$\bar{x}1 > \bar{x}2$

7.46 > 5.25

Aplicando el método estadístico de Mann – Whitney, aplicando el programa IBM SPSS Statistic, tenemos:




```
DATASET ACTIVATE Conjunto_de_datos4.
NPAR TESTS
  /M-W= N°_saltos BY Grupos(1 2)
  /MISSING ANALYSIS.
```

Pruebas NPar

```
[Conjunto_de_datos4]
```

Prueba de Mann-Whitney

Rangos

	Pre_Post_Prueba	N	Rango promedio	Suma de rangos
Número de saltos recorridos	1	24	32,31	775,50
	2	24	16,69	400,50
	Total	48		

Estadísticos de prueba[a]

	Número de saltos recorridos
U de Mann-Whitney	100,500
W de Wilcoxon	400,500
Z	-4,094
Sig. asintótica (bilateral)	,000

a. Variable de agrupación: Pre_Post_Prueba

Figura 35*. Prueba Mann- Whitney: Número de saltos.*
Fuente: Elaboración propia del autor.

Interpretación: Como podemos ver el estadígrafo de U de Mann – Whitney es de 100,5 y el valor de p (Sig. Asintót. (bilateral)) es 0.000, puesto que el valor $p = 0.000 < \alpha = 0.05$, por lo que se rechaza la hipótesis nula y se concluye que el uso de una RPV reduce el número de saltos recorridos del paquete de datos origen – destino (Post – Prueba) con respecto al muestreo donde no se aplica la RPV (Pre – Prueba), con un nivel de significancia del 5%.

Los resultantes evidencian que se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (ha). En donde la prueba estadística es significativa.

C. Contrastación de la variable: Tiempo de carga en las transacciones en el sistema informático. KPI_4

En la validación del impacto en el uso de una Red Privada Virtual por medio de un MPLS en el tiempo de carga en las transacciones en el sistema informático, se realizó haciendo muestreos. La medición se realizó antes de la implementación de la RPV (Pre – Prueba) y la otra medición después de la implementación de la RPV (Post-Prueba). En las tablas siguientes mostramos los Tiempos de carga en las transacciones en el sistema informático de los dos muestreos:

Tabla 21. *Datos de muestra Pre - Prueba KPI₄.*

Pre – Prueba							
5	7	5	5	6	5	4	5
4	5	5	5	4	5	5	6
6	4	4	4	5	5	4	4

Fuente: Elaboración propia del autor.

El testeo dirigido al tiempo de carga en las transacciones en el sistema informático en minutos antes de la implementación de la VPN.

Tabla 22. *Datos de muestra Post – Prueba KPI₄*

Post – Prueba							
0.05	0.05	0.05	0.07	0.06	0.06	0.06	0.05
0.05	0.06	0.06	0.07	0.09	0.09	0.09	0.07
0.07	0.09	0.09	0.09	0.06	0.06	0.06	0.05

Fuente: Elaboración propia del autor.

El testeo dirigido al tiempo de carga en las transacciones en el sistema informático posterior a la implementación de la VPN, medido en minutos.

Hi: El uso de una RPV reduce el tiempo de carga en las transacciones en el sistema informático (Post – Prueba) con respecto al muestreo donde no se aplica la RPV (Pre – Prueba).

Planteamiento de la Hipótesis

$\bar{x}1$ = Media del Tiempo de carga en las transacciones en el sistema informático Pre – Prueba.

$\bar{x}2$ = Media del tiempo de carga en las transacciones en el sistema informático Post – Prueba.

H0: $\bar{x}1 = \bar{x}2$, en donde:

Ha: $\bar{x}1 > \bar{x}2$

Criterios de decisión

Las muestras son datos independientes y no parametrados.

Tabla 23. *Estadística KPI_3*

Muestra	N	Mediana
¨Pre – Prueba KPI_1	24	4.76
Post – Prueba KPI_1	24	0.77

Fuente: Elaboración propia del autor.

Tabla 24. *Confianza lograda KPI_3*

Diferencia	IC Pre - Prueba	IC Post - Prueba
3.99	96.9 %	99.0 %

Fuente: Elaboración propia del autor.

Decisión estadística

Ha: $\bar{x}1 > \bar{x}2$

Donde la hipótesis alterna es mayor donde $\bar{x}2$ es mayor a 0.05

$\bar{x}1 > \bar{x}2$

4.76 > 0.77

Aplicando el método estadístico de Mann – Whitney, aplicando el programa IBM SPSS Statistic, tenemos:

```
SAVE OUTFILE='C:\Users\AlvarezDell2\Documents\Tiempo de carga.sav'
  /COMPRESSED.
NPAR TESTS
  /M-W= Tiempo_carga BY Grupos(1 2)
  /MISSING ANALYSIS.
```

Pruebas NPar

```
[Conjunto_de_datos7] C:\Users\AlvarezDell2\Documents\Tiempo de carga.sav
```

Prueba de Mann-Whitney

Rangos

	Pre_Post_Prueba	N	Rango promedio	Suma de rangos
Tiempo de carga	1,00	24	36,50	876,00
	2,00	24	12,50	300,00
	Total	48		

Estadísticos de prueba[a]

	Tiempo de carga
U de Mann-Whitney	,000
W de Wilcoxon	300,000
Z	-6,027
Sig. asintótica (bilateral)	,000

a. Variable de agrupación: Pre_Post_Prueba

Figura 36. *Prueba Mann- Whitney: Número de saltos.*
Fuente: Elaboración propia del autor.

Interpretación: Como podemos ver el estadígrafo de U de Mann – Whitney es de 0.000 y el valor de p (Sig. Asintót. (bilateral)) es 0.000, puesto que el valor $p = 0.000 < \alpha = 0.05$, por lo que se rechaza la hipótesis nula y se concluye que el uso de una RPV reduce el tiempo de carga en el envío de información (Post – Prueba) con respecto al muestreo donde no se aplica la RPV (Pre – Prueba), con un nivel de significancia del 5%.

Los resultantes evidencian que se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (ha). En donde la prueba estadística es significativa.

5.6. Discusión de los resultados con los antecedentes

Contrastando los resultados con los estudios vertidos en los antecedentes tenemos:

De acuerdo a Peña (2016), afirma que la iniciar la sesión Windows a los usuarios VPN, producen mejoras con el uso de la clave única de conexión a los paquetes de información de forma local o a distancia. Conforme a Mar (2016) en el envío y retorno de información entre las sedes de Lima y Cusco del INEI que al implementar el intranet vía VPN elevan la confidencialidad y recojo de información, lo que se corrobora con el sistema en las diligencias de las notarías y el Colegio de Notarios de Cajamarca. Teniendo del mismo modo la confidencialidad e integridad de emisión y recepción de la data en envío.

Aplicando en nuestro estudio el MPLS unificamos varios tipos de información transmitido por medio de la misma red para remitir paquetes de información que no crean problemas de velocidad.

De acuerdo a la tesis de Mar (2016), implementa una intranet vía VPN para elevar la confidencialidad del envío y recojo de información de Lima y Cusco. Realizó una simulación del intercambio de data del servidor con correos de clientes VPN, teniendo una comunicación excelente. LA VPN certificó la privacidad y entereza en el envío y recepción de la data enviada entre las dos cuentas, con el uso de la VPN en la presente tesis de igual manera determina la entereza del envío y la privacidad del mismo, no pudiendo hacerse pruebas de seguridad reales por las limitaciones antes presentadas.

Conforme a la tesis de Espinoza (2015), Al aplicar el protocolo VPN SSL dio como resultado avalar la privacidad del flujo de data recibida y emitida, por datos encriptados bajo el algoritmo 3DESque genera condiciones seguras para las operaciones tecnológicas de accesos más robustos. En nuestro estudio aplicamos protocolo VPN MPLS, donde se aplica para envío y recepción de paquetes de información mas no operaciones tecnológicas, esto difieren por el objetivo de la empresa.

Conforme a la tesis de Quiroz (2014), implementa calidad de servicio (QoS) en la infraestructura de red del Colegio de Ingenieros del Perú CD Cajamarca para dar soporte a las nuevas tecnologías que se puedan implementar. Donde el estudio mejora la red para incrementar el ancho de banda y velocidad de transmisión de información, disminución del tráfico en la red, pero no aplica VPN para el envío

de información fuera de las instalaciones del Colegio de Ingenieros de forma segura e integra solo se enfocan al mejoramiento de la red interna.

De acuerdo a la tesis de Correa (2013). Aplica Calidad de Servicio a las redes inalámbricas ofreciendo los parámetros que determinan la Calidad de Servicio en una aplicación IPv6 sobre redes inalámbricas, el cual es a nivel de propuesta de mejora en calidad de servicio en redes inalámbricas, en contraste con el presente estudio se enfoca en la interconexión y acceso de información en tiempo real, teniendo en cuenta que la calidad de servicio se encuentre en condiciones mínimas requeridas para su desarrollo.

Conforme a la tesis de Menéndez (2012), desarrolló la estructura MPLS en redes privadas virtuales, garantizando el desempeño eficiente de la red VPN y con holgura de adición soportes futuros. La oferta tecnológica es proveer servicios VPN a distancia, logrando la conectividad aprovechando la red. La presente tesis de manera similar aplica VPN MPLS pero es más aplicativa específicamente en notarias y Colegio de Notarios y el estudio de Menéndez es genérico para múltiples sistemas autónomos.

De acuerdo a la tesis de Gonzales (2012) que resalta como una buena solución alterna a los métodos de implementación de redes WAN tradicionales, mientras mayor sea la RPV, el ahorro económico será mayor, se opina favorablemente por que se comprueba menores tiempos en carga y envío de información, lo cual se traduce en eficiencia y tiempo, lo que hay mejor servicio a los clientes de las notarías y menores costos de transacción.

Conforme a la tesis de Limari (2004), implementa Protocolos de Seguridad para Redes Privadas Virtuales (RPV) con el desarrollo VLSM con seguridad y confidencialidad completa en el envío y retorno de paquetes de información entre cedes. En contraste con la tesis presentada se enfocan en los mismos fines a diferencia que se aplica un MPLS específica.

5.7. Análisis e interpretación de los resultados

- Se aplica la configuración de la Red Privada Virtual (VPN) de Multiprotocol Label Switchinf (MPLS) en momentos que el Routing Information Protocol (RIP) este activo en el otro lado de la fuente.

  Aplicando el VPN utilizando MPLS, nos va acceder a diversos sitios transparente se interconecten por medio de la red proveedora de servicio de internet, empresa que puede brindarnos soporte a varias VPN con IP diversas, en donde vemos que cada IP VPN se muestra como una red privada. Cada lugar de un VPN remite paquetes del IP a otros sitios (notarias) en la misma plataforma VPN.
- Cada VPN se encuentra asociada entre una a más sucesos de reenvío o también denominado ruteo VPN. El router conserva un ruteo divergente y una tabla CEF para cada VRF. Este propósito impide que la información sea remitida fuera del VPN y a la vez nos accede a que la misma sub red sea usada en diversos VPN, usos que no producen problemas de IP duplicado.
- Se hizo factible el diseño de una red privada virtual por medio de un MPLS Packet Tracer, interconectando en simulación 8 notarias y el Colegio de Notarios de Cajamarca. Realizando la configuración de la estructura básica de ATM

MPLS empleando el área 0 del Open Shortest Path First (OSPF) así como el Interior Gateway Protocol (IGP). Configuramos dos diferentes VPN mediante la estructura básica. Primero aplicaciones VPN RASGAN tomado como límite del cliente al Routing Protocol del límite del proveedor (CE-PE); el segundo VPN emplea el BGP como su Routing Protocol PE-CE. Luego se configuró diversos loopback y Static rutas en el Routers CE para poder simular la disposición de otro Routers y redes.

- Se desarrolló la simulación de la siguiente manera. Luego de estructurar la topología de la red de acuerdo a la distribución geográfica, se realizó una descomposición para evitar sobre carga visual, descomponiendo en una estructura mínima para la configuración de la tecnología VPN (MPLS), donde se subnetearon las notarías y el Colegio de Notarios. Se desarrolló el armado físico de la topología, se le asignaron los IPS y se configuró la tecnología RPV (MPLS). La simulación se ejecutó con la petición de data de la notaria 1 a la PC3 de Colegio de Notarios y viceversa con el mensaje de retorno, donde se ejecutó de forma exitosa.
- De acuerdo al anexo 01 se ve el instrumento de validación de los riesgos posibles, instrumento que fue determinado de acuerdo a las visitas de inspección visual por parte del autor de la presente tesis realizadas a las notarías de Cajamarca y Colegio de Notarios de Cajamarca, antes de iniciarse los estados de restricción de estado de emergencia por pandemia COVID19.
- Al realizar las pruebas pre prueba y post prueba, se realizó la medida de los KPI´s de tiempo de latencia del servicio de comunicación de 24 pruebas. Siendo

el tiempo promedio de latencia fue de 1183.25 sin la aplicación del sistema y con sistema el tiempo de latencia es de 9.21.

- Al realizar las pruebas pre prueba y post prueba, se realizó la medida de los KPI´s de N° de saltos que desplaza el paquete de datos de 24 pruebas. Siendo el número de saltos promedio de saltos de 7.46 sin la aplicación del sistema y con sistema el número de saltos es de 5.25.
- Al realizar las pruebas pre prueba y post prueba, se realizó la medida de los KPI´s de Tiempo de carga en el ingreso al sistema informático de 24 pruebas. Siendo el tiempo de carga promedio de saltos de 4.76 sin la aplicación del sistema y con sistema el tiempo de carga es de 0.07.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La conclusión general a la que se llega es de afirmar que las redes privadas virtuales (RPV) modelo MPLS es un sistema de redes de comunicación virtual, al aplicarla a nuestras necesidades del proyecto hace que se introduzca al campo de análisis y estudio del caso, lo cual implica diseñar a nuestro criterio la red, y a la vez introducir paradigmas íntegramente nuevos, los cuales no presenten un análogo directo con las redes físicas existentes. Por lo tanto que se tiene mecanismos comunes de redes físicas y virtuales, lo cual nos aporta a la introducción de redes privadas virtuales en las redes públicas existentes, siendo esto un beneficio por que nos aminora esfuerzos para crear estándares y el flujo de información en ambos sentidos, donde las soluciones al problema pueden ser asimiladas.
2. Se realizó el diseño de un modelo de red privada virtual por medio de un MPLS packet tracer con la interconexión notarial, Podemos afirmar que el diseño y el uso de redes privadas virtuales son una solución muy flexible y de costos bajos en las empresas e instituciones que requieren mantener una comunicación fluida de intercambio de información de datos confidenciales y seguros entre las notarías y el Colegio de Notarios de Cajamarca, evitándose costos altos en la implementación de redes que cumplan los mismos objetivos.

Las implementaciones de redes privadas virtuales cuentan con ventajas de bajas y eficientes necesidades de infraestructura y bajos costes de implementación de RPV que permitirían conseguir el mismo fin. Por lo tanto es una de las mejores alternativas para cumplir con los fines cometidos de las notarías. Las bondades más considerables son los bajos costos de implementación, la confidencialidad y seguridad en el envío de información, del mismo modo características de escalabilidad, porque a futuro de puede acceder a implementar otras notarias, cuando así se desee.

3. Se desarrolló un esquema de simulación, para esto se desarrolló la configuración VPN nos da la garantía de privacidad del flujo de comunicación, información y velocidad de la información concluimos que VPN nos respalda de manera directa confidencialidad y entereza en el flujo de documentos, mensajes e instructivos éntrelas notarías y el Colegio de Notarios de Cajamarca. Ventajas que fortalecen la gestión. toma de buenas decisiones inmediatas por la información confidencial, integra y segura, de modo indirecto si tenemos una RPV segura se accede a implementar en ella mecanismos de autenticación y dominio en el ingreso de usuarios aceptados.

4. Para determinar la inter conexión se procedió a realizar la simulación de funcionamiento de la red privada virtual fueron satisfactorias, con lo que confirmamos que las VPN son una alternativa de solución, la cual accede a una topología de red centralizada entre las notarías y el Colegio de Notarios; en la red se accede a los recursos TI en tiempo real, lo que nos permite disponer de la

información requerida en el breve plazo de envío y poder desarrollar las actividades notariales eficientemente en menores tiempos y costes.

Al realizar las pruebas pre prueba y post prueba, se realizó la medida de los KPI´s de tiempo de latencia del servicio de comunicación de 24 pruebas. Siendo el tiempo promedio de latencia fue de 1183.25 sin la aplicación del sistema y con sistema el tiempo de latencia es de 9.21.

El estadígrafo de comprobación de interconexión y acceso de la información antes y después de la simulación del uso de la RPV, se da por contrastación de la variable KPI en el tiempo de latencia en el envío de información, de acuerdo a la técnica mann – Whitney, donde el estadígrafo indica un resultado de 0.000 y el valor de p (Sig. Asintót. (bilateral)) es 0.000, puesto que el valor $p = 0.000 < \alpha = 0.05$, por lo que se acepta la hipótesis que el uso de una RPV reduce el tiempo de latencia en el envío de información (Post – Prueba) con respecto al muestreo donde no se aplica la RPV (Pre – Prueba), con un nivel de significancia del 5%.

En conclusión las VPN son una considerable e importante solución para el conjunto de notarías, ya que brinda confiabilidad, entereza, privacidad y acceso a la información, factores que son preponderantes que representan los tres pilares de la seguridad de la información que toda empresa e institución requiere.

Por los motivos expuestos el presente estudio realizado cumplió a satisfacción el objetivo.

RECOMENDACIONES.

1. la implementación de la Red Privada Virtual para la optimización de los procesos antes mencionados en la investigación en la brevedad posible.

2. Cuando se tenga la implementación se recomienda hacer una base de datos centralizada para que otras entidades como el Ministerio Publico, Poder Judicial, Sunarp y el Colegio de Notarios se puedan comunicar en tiempo real.

3. En la red VPN montada se pueden acceder a desarrollar extensiones y mejoras apropiadas conforme a los requerimientos soporte. Para lo cual incidir en el entorno físico y luego a las redes virtuales. Preceptos por el comportamiento de las redes, como son el direccionamiento, los procesos de reenvío, seguridad, por lo que los inconvenientes que surgen en las VPN tienen análogos directos con los problemas que se dan en las redes físicas.

4. Se recomienda ceñirse a las direcciones IP determinadas, para garantizar la conexión entre los servidores críticos, así como de tener un directorio de control de direcciones IP, para evitar réplicas de las IP, y así evitar conflictos de IP en las notarías y CNC. También nominar cada host con un IP numérico específico y único para poder determinar su ubicación física y lógica.

5. Realizar monitoreos temporales y programados para detectar posibles amenazas de riesgos, para implementar acciones preventivas y correctivas del sistema.

REFERENCIAS BIBLIOGRÁFICAS

Arguedas, H., (2010). Manual de Comandos para Enrutamiento. España: ESIC.

Brollo, Gerardo. (2010). Nuevas Tendencias en Redes Virtuales Privadas (Trabajo de Adscripción para el curso de Teleproceso y Sistemas Distribuidos). Corrientes: Universidad Nacional del Nordeste.

BROWN, Steven R. (2001) Implementación de Redes Privadas Virtuales (RPV) México: McGraw-Hill Interamericana.

CALDERON RODRIGUEZ**,** Calixto (2001) Implementación de una VPN (Virtual Private Network) Usando el estándar IPSEC (Proyecto de fin de carrera como especialista en Informática). Valencia: Universidad Politécnica de Valencia.

CEVALLOS RODRIGUEZ, Mario Roberto (2006) Diseño e Implementación de una Red Virtual Privada entre las oficina de INFONET ubicadas en las ciudades de Quito y Miami (Tesis para el Título de Ingeniero en Electrónica y Telecomunicaciones). Sangolqui: Escuela Politécnica del Ejercito.

CIO Data Center Services (2019). "¿Qué es la interconexión empresarial? México.

García, G., (2009). Propuesta de Migración de la Red NGN de una Operadora Implementada en IP hacia MPLS. Perú: UNIVERSAL.

Ghein, L., (2006). MPLS FUNDAMENTALS. Estados Unidos: CISCO PRESS.

GUZMAN VITE, Marcos (2008) Implementación de una Red Privada Virtual en Presidencia Municipal de Pachuca de Soto Hidalgo (Tesis para el Título de

Ingeniero en Electrónica y Telecomunicaciones). Pachuca de Soto: Instituto de Ciencias de Pachuca de Soto Hidalgo.

Hernández, R., (1997). Metodología de la investigación. México: MCGRAW HILL.

Hernández, R. (2010). Metodología de la investigacion (5ta Ed.) Mexico: Grupo Infagon

Hidalgo, P. & Díaz, A. (2010). Diseño e Implementación de una Red Privada Virtual para la Empresa Eléctrica Quito S.A., Matriz Las Casas, para la Transmisión de Datos y Voz sobre IP. Ecuador. ESCUELA POLITÉCNICA NACIONAL.

Lavado, G., (2010). MPLS – Multiprotocal Label Switching Versión 1.0 Modo Compatibilidad. Estados Unidos: CISCO PRESS.

Limari, V., (2004). Protocolos de Seguridad para Redes Privadas Virtuales (VPN). Chile: AUSTRAL.

MENENDEZ AVILA, Ricardo Armando (2012) Estudio del Desempeño e Implementación de una solución MPLS-VPN sobre Múltiples Sistemas Autónomos. (Tesis para optar el Título de Ingeniero de las Telecomunicaciones). Lima: Pontificia Universidad Católica del Perú.

Morales, L., (2006). Investigaciones de Redes VPN con tecnología MPLS. México: MCGRAW HILL.

Murillo, W. (2008). La investigación científica. Consultado el 18 de abril de 2008 de http//www.monografias.com/ trabajos15/invest-científica/investcientífica.shtm

OROZCO LARA, Fausto Raúl (2014) Diseño de una Red Virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil.

(Tesis para el Título de Magister en Telecomunicaciones). Guayaquil: Universidad Católica de Santiago de Guayaquil.

Pepelnjak, I. & Guichard, J (2002). MPLS and VPN Architectures. Estados Unidos: CISCO PRESS.

REYES MORENO, Enevis Rafael (2005). Lineamientos para la creación de una VPN (Virtual Private Network) Red Privada Virtual (Tesis para el Título de especialista en Telemática). Medellín: Universidad de Antioquia.

SCOTT Ch., WOLFE P. y ERWIN M. (1998) Virtual Private Networks California: O'Reilly Media.

TRUJILLO MACHADO, Edison Rafael (2006) Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPSEC. (Tesis para el Título de Ingeniero en Informática). Quito: Escuela Politécnica Nacional.

VASQUEZ, Jorge (2014) Investigaciones en tecnologías de información informática y computación USA: Palibrio.

ANEXOS

Anexo 01. GUÍA DE LA FICHA DE OBSERVACION PARA EL CONTROL DE TIEMPOS DE LATENCIA

Instrucciones:

1. Número de Observaciones: 24
2. Fecha: El número de días observados fue de 8 días.
3. Hora: Las horas determinadas de controles de tiempo de latencia se desarrollan cada hora, tomando en consideración las horas de atención de las notarías y Colegio de Notarios.
4. Tiempo de latencia: Los tiempos de latencia se contabilizan con la unidad de tiempo de milisegundos para cada una de las tomas de tiempo.
5. Archivos enviados: Determinar la contabilidad de número de archivos enviados origen en el tiempo de latencia determinado.
6. Archivos recibidos: Determinar la contabilidad de número de archivos recibidos en destino en el tiempo de latencia determinado.
7. Archivos perdidos: Determinar la contabilidad de número de archivos perdidos en los envíos o recepciones defectuosos, incompletos, erróneos o sin llegada, en el flujo origen - destino en el tiempo de latencia determinado.
8. Porcentaje de paquetes perdidos: Determinado por la contabilidad total de archivos enviados y recibidos comparados en porcentaje de los archivos perdidos ((Archivos perdidos x 100)/Archivos env.+ arch.perd.).

Anexo 02. GUÍA DE LA FICHA DE OBSERVACION PARA EL CONTROL DE NÚMERO DE SALTOS RECORRIDOS POR EL PAQUETE DE DATOS DE ORIGEN – DESTINO

Instrucciones:

1. Número de Observaciones: 24
2. Fecha: El número de días observados fue de 8 días.
3. Hora: Las horas determinadas de controles de tiempo de latencia se desarrollan cada hora, tomando en consideración las horas de atención de las notarías y Colegio de Notarios.
4. Traza de saltos sobre caminos de 30 saltos máximos: Determinación de los números de saltos recorridos por el paquete de datos o archivo en la ruta de conexión desde origen a destino, donde se deben tener un máximo de 30 saltos, que son el máximo permisible aceptable de un eficiente flujo de información.
5. Archivos enviados: Determinar la contabilidad de número de archivos enviados origen en el tiempo de latencia determinado.
6. Servicio al que se establece la comunicación: Determinar el tipo de servicio utilizado en el flujo de información, en el caso de estudio se utilizó el servidor Outlook.

Anexo 03. **GUÍA DE LA FICHA DE OBSERVACION PARA EL CONTROL DE NÚMERO DE LAPSO DE TIEMPO EN CARGAR PARA TRANSACCIONES EN EL SISTEMA INFORMÁTICO.**

Instrucciones:

1. Número de Observaciones: 24
2. Fecha: El número de días observados fue de 8 días.
3. Hora: Las horas determinadas de controles de tiempo de latencia se desarrollan cada hora, tomando en consideración las horas de atención de las notarías y Colegio de Notarios.
4. Tiempo de carga del sistema informático: Los tiempos de carga del sistema informático se estiman en minutos, donde se subdividen en dos estimaciones: Sistema de escritorio, el cual está determinado por el equipo y la carga del sistema operativo del procesador y el Sistema Web, que es la carga y configuración del sistema web por calidad de señal en el servicio de internet.
5. Tiempo en minutos en realizar la transacción en el sistema informático: La demora en tiempo de las transacciones del sistema informático se estiman en minutos, donde se subdividen en dos estimaciones: Sistema de escritorio, el cual está determinado por el equipo y la carga del sistema operativo del procesador y el Sistema Web, que es la carga y configuración del sistema web por calidad de señal en el servicio de internet.

Anexo 04. *Ficha de Observación: Tiempo de latencia del servicio de envío de información.*

N°	Fecha	Hora	Tiempo de latencia Ida y Vuelta en milisegundos	Archivos enviados	Archivos recibidos	Archivos perdidos	Porcentaje de paquetes perdidos
1	15/10/2020	09:00 a.m.	980	24	15	9	23%
2	15/10/2020	10:00 a.m.	940	24	16	8	20%
3	15/10/2020	11:00 a.m.	940	24	13	11	30%
4	16/10/2020	12:00 a.m.	950	24	15	9	23%
5	16/10/2020	01:00 p.m.	960	24	11	13	37%
6	16/10/2020	02:00 p.m.	950	24	15	9	23%
7	17/10/2020	03:00 p.m.	1300	24	14	10	26%
8	17/10/2020	04:00 p.m.	1400	24	16	8	20%
9	17/10/2020	05:00 p.m.	940	24	11	13	37%
10	18/10/2020	09:00 a.m.	1510	24	15	9	23%
11	18/10/2020	10:00 a.m.	1500	24	11	13	37%
12	18/10/2020	11:00 a.m.	1500	24	14	10	26%
13	19/10/2020	12:00 a.m.	1350	24	18	6	14%
14	19/10/2020	01:00 p.m.	1350	24	12	12	33%
15	19/10/2020	02:00 p.m.	1450	24	15	9	23%
16	20/10/2020	03:00 p.m.	940	24	15	9	23%
17	20/10/2020	04:00 p.m.	1400	24	13	11	30%
18	20/10/2020	05:00 p.m.	1000	24	12	12	33%
19	21/10/2020	09:00 a.m.	1150	24	11	13	37%
20	21/10/2020	11:00 a.m.	1300	24	15	9	23%
21	21/10/2020	01:00 p.m.	1250	24	11	13	37%
22	22/10/2020	03:00 p.m.	1300	24	14	10	26%
23	22/10/2020	05:00 p.m.	950	24	16	8	20%
24	22/10/2020	07:00 p.m.	1100	24	15	9	23%

Anexo 05.*Ficha de Observación: Número de saltos recorridos por el paquete de datos de origen - destino*

N°	Fecha	Hora	Traza de saltos sobre caminos de 30 saltos máximos	Servicio al que se establece la comunicación
1	15/10/2020	09:00 a.m.	6	Servidor outlook
2	15/10/2020	10:00 a.m.	11	Servidor outlook
3	15/10/2020	11:00 a.m.	9	Servidor outlook
4	16/10/2020	12:00 a.m.	9	Servidor outlook
5	16/10/2020	01:00 p.m.	11	Servidor outlook
6	16/10/2020	02:00 p.m.	6	Servidor outlook
7	17/10/2020	03:00 p.m.	6	Servidor outlook
8	17/10/2020	04:00 p.m.	8	Servidor outlook
9	17/10/2020	05:00 p.m.	6	Servidor outlook
10	18/10/2020	09:00 a.m.	6	Servidor outlook
11	18/10/2020	10:00 a.m.	8	Servidor outlook
12	18/10/2020	11:00 a.m.	8	Servidor outlook
13	19/10/2020	12:00 a.m.	6	Servidor outlook
14	19/10/2020	01:00 p.m.	6	Servidor outlook
15	19/10/2020	02:00 p.m.	8	Servidor outlook
16	20/10/2020	03:00 p.m.	8	Servidor outlook
17	20/10/2020	04:00 p.m.	11	Servidor outlook
18	20/10/2020	05:00 p.m.	6	Servidor outlook
19	21/10/2020	09:00 a.m.	6	Servidor outlook
20	21/10/2020	11:00 a.m.	6	Servidor outlook
21	21/10/2020	01:00 p.m.	8	Servidor outlook
22	22/10/2020	03:00 p.m.	8	Servidor outlook
23	22/10/2020	05:00 p.m.	6	Servidor outlook
24	22/10/2020	07:00 p.m.	6	Servidor outlook

Anexo 06. *Ficha de Observación: Lapso de tiempo en cargar para transacciones en el sistema informático.*

N°	Fecha	Hora	Tiempo en minutos de carga del sistema informático		Tiempo en minutos en realizar la transacción en el sistema informático	
			Sistemas de escritorio	Sistema Web	Sistemas de escritorio	Sistema Web
1	15/10/2020	09:00 a.m.	3	3	5	4
2	15/10/2020	10:00 a.m.	4	4	3	7
3	15/10/2020	11:00 a.m.	5	3	5	4
4	16/10/2020	12:00 a.m.	3	4	5	4
5	16/10/2020	01:00 p.m.	4	4	7	5
6	16/10/2020	02:00 p.m.	4	5	3	4
7	17/10/2020	03:00 p.m.	5	4	5	4
8	17/10/2020	04:00 p.m.	5	4	3	3
9	17/10/2020	05:00 p.m.	5	3	7	5
10	18/10/2020	09:00 a.m.	3	4	5	4
11	18/10/2020	10:00 a.m.	5	4	3	4
12	18/10/2020	11:00 a.m.	3	5	5	3
13	19/10/2020	12:00 a.m.	5	4	5	4
14	19/10/2020	01:00 p.m.	5	4	7	4
15	19/10/2020	02:00 p.m.	3	3	3	3
16	20/10/2020	03:00 p.m.	3	4	5	4
17	20/10/2020	04:00 p.m.	4	4	3	7
18	20/10/2020	05:00 p.m.	3	5	3	4
19	21/10/2020	09:00 a.m.	3	3	5	4
20	21/10/2020	11:00 a.m.	5	4	5	3
21	21/10/2020	01:00 p.m.	5	4	7	4
22	22/10/2020	03:00 p.m.	4	5	3	7
23	22/10/2020	05:00 p.m.	4	4	5	4
24	22/10/2020	07:00 p.m.	5	3	3	3