UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTORES:

Luna Huaman, Alan (ORCID: 0000-0001-5933-1670)

Zeta Nuñez, Cristhian Dany (ORCID: 0000-0002-2576-7596)

ASESOR:

ING. Rivera Crisostomo, Renee (ORCID: 0000-0002-5496-7036)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de servicio de redes y comunicaciones

LIMA – PERÚ

2021

Dedicatoria

Dedicamos el presente trabajo a nuestro forjador, al que guía nuestro camino y padre celestial, al que nos acompaña y no permite que caigamos jamás. A nuestro creador, creador de nuestros padres y padres de ellos, así como de las personas que amamos y admiramos. Gracias Dios.

Agradecimiento

A Dios en primera instancia, quien decidió por nuestros padres para que estemos presentes en este mundo.

Agradecemos al asesor Ing. Rivera, por brindarnos de sus conocimientos con paciencia y manera siempre correcta en la realización de este trabajo de titulación, asimismo a todos y cada uno de los docentes que han hecho posible llegar.

A todas las personas, familia y amistades cercanas, alentándonos a culminar esta etapa.

.

Índice de contenidos

Índice de tablas

Índice de figuras

Índice de anexos

Índice de abreviaturas

WAN: Red de Área Amplia

IPV6: Protocolo de Internet Versión 6 (IP, Internet Protocol)

IPV4: Protocolo de Internet Versión 4 (IP, Internet Protocol)

LAN: Red de Área Local (Local Área Network)

RAM: Memoria de Acceso Aleatorio (Random Access Memory)

VPN: Red Privada Virtual (Virtual Prívate Network)

Resumen

Proporciona una herramienta una herramienta, con bases fundamentadas de lo provechoso y útil que puede resultar, el realizar conexiones u enlaces VPN de acceso remoto usando equipos MIKROTIK. Este hardware de monitoreo permite mejorar el rendimiento y darle la oportunidad al técnico o especialista en tomar una decisión más adecuada en base a criterios que determinaran la efectividad tanto de la metodología como de las herramientas

Las entidades al no tener disponibilidad de implementación con conexiones VPN que emplea herramientas de monitoreo pierden costos, recursos y la calidad del producto.

El problema del estudio se entorna obteniendo información actualizada seleccionada, pero no se detalla sobre la implementación con conexiones VPN empleando herramientas de monitoreo. Por ello, esta conexión prioriza lo confidencial del tránsito de la información, tanto de ida y vuelta, evitando que agentes no autorizados puedan vulnerar o capturar paquetes en el tráfico y sustraer la información que a través de esta VPN se envíe y reciba

Este tipo de solución bien implementada y configurada es usada para transmitir información considerada sensible, data de conexión y accesos remotos en industrias grandes, pequeñas, medianas y microempresas. Las empresas con la nueva normalidad se han visto obligados a buscar y usar diversas soluciones de acceso remoto, tanto para enlazar sedes, acceder a servidores y/o facilitar a los colaboradores puedan acceder a las aplicaciones de la empresa para seguir realizando sus actividades sin movilizarse de sus domicilios.

Palabras clave: Implementación, Mikrotik, desempeño en la red, consumo de recursos técnicos y conectividad en la red.

Abstract

To provide a tool, with a well-founded basis of how profitable and useful it can be, to make connections or remote access VPN links using MIKROTIK equipment. This monitoring hardware allows to improve performance and give the technician or specialist the opportunity to make a more appropriate decision based on criteria that will determine the effectiveness of both the methodology and the tools.

By not having implementation availability with VPN connections that uses monitoring tools, entities lose costs, resources and product quality.

The study problem is ameliorated by obtaining selected updated information, but it is not detailed about the implementation with VPN connections using monitoring tools. For this reason, this connection prioritizes the privacy of the information that is transmitted back and forth, preventing unauthorized agents from violating or capturing packets in traffic and stealing the information that is sent and received through this VPN.

This type of well-implemented and configured solution is used to transmit information considered sensitive, connection data and remote accesses in large, small, medium and micro-enterprises industries. Companies with the new normal have been forced to seek and use various remote access solutions, both to link offices, access servers and / or facilitate collaborators to access the company's applications to continue carrying out their activities without mobilizing from their homes.

Keywords: Implementation, Mikrotik, network performance, consumption of technical resources and network connectivity.

I. INTRODUCCIÓN

La presente investigación se lleva a cabo consciente de la necesidad y el reto tecnológico al que estamos enfrentando. Por ello, frente a las adversidades tecnológicas no hay implementación enfocada a la conexión de redes VPN de punto a punto a base de servidores. Además, la implementación permitirá beneficiar tanto al administrador de redes, especialistas técnicos o personas que se enfocan al área de Tecnologías de Información a base de: (a) desempeño en red, (b) El consumo de recursos y (c) conectividad en la red, para permitir la transferencia de datos seguros y permitir una conexión sin problemas de red, optar por procesos que puedan permitir él envió de paquetes de punto a punto sin tráfico de tunelización de la red VPN a medida de la herramienta Mikrotik.

En la actualidad todo el mundo vive un aislamiento forzado, logrando sobresalir de los desafíos y adversidades cotidianas que se presentan a base de creatividad e innovación tecnológica en niveles donde la solución al trabajo se gestiona remotamente con software y/o conexiones de redes VPN a base de un modelo distribuido de empleado-maquina permitiendo tener alta disponibilidad en servicios (Bargados 2021; Oszlak 2020; Vílchez, Gómez y González 2020; p. 24).

Además, se debe tener en cuenta que, para un administrador de red, un informático, especialista técnico, encargado o líder de los servicios mencionados, es un punto clave (Coan 2020; Santisteban 2020) Asimismo, toda organización debe mantener un entorno de TI dado que es vital para la continuidad de procesos y operaciones, siendo estratégico para los cambios de: (a) conectividad, (b) producción y (c) tecnología (Mendoza 2020; Arias, Milián y Dominguez 2020).

De acuerdo a lo anterior mencionado, Morán (2020) manifestó que al implementar una plataforma de un nivel alto de disponibilidad a través de una conexión VPN de una entidad financiera con los procedimientos de la metodología PPDIOO de Cisco enfocándose a poder asegurar la calidad del servicio Morán (2020). Además, Marín, Patiño y Acevedo (2020) implementaron un servicio completo enfocada a la seguridad de la transferencia de datos a base de: (a) servidor VPN, (b) firewall y (c) sistema IDS con procesos de la metodología de bloques: (i) análisis, (ii) desarrollo e (iii) implementación Marín,

Patiño y Acevedo (2020). En síntesis, las organizaciones están tomando como interés y centro de proyectos y servicio a la tecnología, aquellas instituciones que gestionan y administrar los recursos para optar por un servicio de calidad y excelencia siendo objetivo el usuario final Useche Aguirre et al. (2021).

Por otro lado, Vargas, Gómez y Garzón (2020) desarrollan un marco metodológico enfocado a virtualizar en la nube todos los datos de los usuarios de ingeniería de UNAD a base de un software VPN libre (open VPN) con los siguientes procedimientos: (i) Simulación y virtualización, (ii) Conectividad VPN de las virtualizaciones y (iii) Topología general montada (Carroll, Diaz y Sanchez 2020). Además, Rosero (2021) propuso la implementación de una conexión de red VPN enfocada a una institución educativa para mantener la seguridad de datos por medio de la tecnología a través de procedimientos, tales como: (a) identificar características de protocolos de seguridad, (b) funcionalidad, (c) análisis de los protocolos IPSec, (d) Contextualización del software VPN mediante firewall o hardware de alta gama (e) instalación y configuración Rosero (2021). Para concluir, es necesario seguir procesos/procedimientos de implementación para obtener resultados de calidad que puedan beneficiar al administrador, técnico o especialista de red (Carroll, Diaz y Sanchez 2020).

No obstante, existen diferentes entidades que brindan el servicio de emplear herramientas como Mikrotik con el fin de adaptar un computador a un servidor local para manipular las redes de datos para gestionar el firewall y los enrutamientos de todas las conexiones (Quinte y Ushiña 2020; Arrieta y Guallpa 2021). Se ha hallado investigaciones relacionadas al presente tema de estudio con indicadores muy importantes que buscan escrutar, tasar y disponer de herramientas de monitoreo y gestión de red a base de conexiones VPN (redes privadas virtuales), pero con una perspectiva diferente (Morán 2020; Marín, Patiño y Acevedo 2020; Carroll, Diaz y Sanchez 2020; Rosero 2021). Sin embargo, no existe una metodología de implementación capaz de evaluar las conexiones de redes VPN a base de la herramienta de monitoreo Mikrotik con servidores permitiendo declinar los recursos y tiempos en la investigación (Carroll, Diaz y Sanchez 2020). Por ende, esta investigación busca contribuir en la toma de control para las entidades pequeñas, medianas o grandes acerca de

la implementación de conexiones de redes privadas virtuales con herramientas sofisticadas de monitoreo, además, examinar sobre información actualizada de criterios y herramientas de TI para mantener la seguridad, calidad y recursos técnicos necesarios (Torres y Alfaro 2018; Useche et al. 2021).

En consecuencia, se ha observado muchos problemas cibernéticos últimamente en los trabajos remotos, dado que se hay una tasa alta y en aumento sobre los riesgos de la seguridad de datos que es originaria y transmitida por el servicio de internet, debido a que no hay especialistas que capaciten al personal o técnicos sobre la utilización de herramientas e información sobre criterios de seguridad de estas tecnologías (Borda 2020). Sin embargo, hay un nivel alto de incremento de trabajo remoto y gestiones en la red, es donde el administrador o técnico de redes debe implementar tecnologías que pueda brindar seguridad de datos desde el remitente hasta el destinatario con el objetivo de mantener la integridad, confiabilidad, utilidad y disponibilidad de información (Domínguez 2020).

Es muy importante que se justifique el desarrollo que se hace para una investigación, de manera que se pueda dimensionar la importancia, así como lo verás, en el planteamiento que se hizo al problema, los objetivos y también la hipótesis, todo esto implica presentar las razones por lo cual es importante precisar realizarlo y en consecuencia los beneficios que se darán (Hernández y Mendoza 2018).

La justificación tecnológica de este proyecto de investigación metodológica, para la Implementación de una conexión VPN usando equipos de la tecnología MIKROTIK entre servidores, se fundamenta en el reto que tenemos día a día y de manera incremental, cada vez más agresiva, en poder comunicarnos y conectarnos a las redes de datos que administramos de manera eficiente y segura (Marín, Patiño y Acevedo 2020). A manera personal sirve para demostrar la admiración y sentido de apreciación que me merece los avances que tiene la tecnología en el mundo cada segundo, se puede decir que vivimos a la par de la tecnología y en el futuro, quizás en muchos aspectos dependamos de ella, por tanto, se hace íntimamente y de manera urgente indispensable, que todos tomemos la conciencia, directa o indirectamente en temas de seguridad (Marín, Patiño y Acevedo 2020).

Asimismo, como justificación teórica de esta tesis, para la implementación de una conexión de red VPN usando equipos de la tecnología MIKROTIK entre servidores, se realiza teniendo como principal propósito, el poder agregar información y aportar al conocimiento ya existente, sobre el uso de estos equipos como herramientas de conexión remota, a través de un túnel seguro, cuyos parámetros podrán sistematizarse en una propuesta, para ser incorporado como conocimiento a las ciencias de la tecnología, investigación metodológica, para la implementación de una conexión de red VPN usando equipos de la tecnología MIKROTIK entre servidores deberá demostrar eficiencia y performance (Marín, Patiño y Acevedo 2020).

Además, La justificación práctica, es que, en la misma línea de ideas de la justificación teórica, el proyecto de investigación metodológica, para la Implementación de una conexión VPN usando equipos de la tecnología MIKROTIK entre servidores, es realizado, porque existe la necesidad de mejorar el nivel de conexiones remotas, optimizando el desempeño de la red, consumo de recursos y disminuyendo los riesgos de la integridad de la información, para ello nos sirve de modelo el tener casos prácticos y ejecutable, como lo menciona (Pacotaype 2018).

En síntesis, la justificación metodológica de este proyecto de investigación es que no hay una metodología de implementación enfocada a las conexiones de redes VPN empleado la herramienta MIKROTIK considerando la información del tema de estudio; permitiendo tomarse decisiones a base de costos bajos o por ser una herramienta conocida en el mercado tecnológico mas no por sus características y recursos técnicos tanto del software y hardware de la red VPN (Pauzhi 2016; Muñoz 2017). Una implementación determina de manera íntegra y sistemática serie de procesos ordenados para obtener deducciones más concisas (Carrasco et al. 2015). Además, debemos conocer a profundidad sobre las herramientas de monitoreo de conexiones de redes para obtener derivaciones exactas y poder saber que programas se aplica para diferente criterio de evaluación tales como: (a) desempeño en la red, (b) consumo de recursos técnicos y (c) conectividad en la red (Pacotaype 2018; Torres y Alfaro 2018).

Teniendo presente el caso problemático, planteamos en nuestra indagación el problema general y además los inconvenientes. Nuestro problema general ha sido ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco? Los problemas específicos de la investigación fueron:

- **PE1:** ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK en desempeño en la red para los servidores entre ciudades de Lima y Pisco?
- **PE2:** ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK en el consumo de recursos para los servidores entre ciudades de Lima y Pisco?
- **PE3:** ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK en la conectividad en la red para los servidores entre ciudades de Lima y Pisco?

Por lo tanto, el objetivo general en la investigación tiene la finalidad de Determinar el proceso de la Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco. Los objetivos específicos fueron:

- **OE1:** Determinar el proceso de la Implementación de redes VPN MIKROTIK en el desempeño en la red para los servidores entre ciudades de Lima y Pisco.
- **OE2:** Determinar el proceso de la Implementación de redes VPN MIKROTIK en el consumo de recursos para los servidores entre ciudades de Lima y Pisco.
- **OE3:** Determinar el proceso de la Implementación de redes VPN MIKROTIK en la conectividad en la red para los servidores entre ciudades de Lima y Pisco.

La hipótesis general es La Implementación de redes VPN MIKROTIK incrementó el desempeño de la red, mejoró el consumo de recursos y la conectividad en la red de los servidores entre ciudades de Lima y Pisco. Las hipótesis específicas fueron los siguientes:

- **HE1:** La Implementación de redes VPN MIKROTIK incrementó el desempeño en la red de los servidores entre ciudades de Lima y Pisco (Vesga, Granados y Vesga 2016; Pacotaype 2018; Julca y Tapia 2020).
- **HE2:** La Implementación de redes VPN MIKROTIK mejoró el consumo de recursos de los servidores entre ciudades de Lima y Pisco (Julca y Tapia 2020; Aguirre 2016; Pacotaype 2018).
- **HE3:** La Implementación de redes VPN MIKROTIK mejoró la conectividad en la red de los servidores entre ciudades de Lima y Pisco (Chilcañán, Navas y Escobar 2017; Davila 2019).

II. MARCO TEÓRICO

Este capítulo, se puede validar de investigaciones previas relacionados a nuestro proyecto de investigación, se encontraron e investigaron antecedentes nacionales e internacionales, se describieron las teorías y los enfoques conceptuales de los temas necesarios a conocer para realizar nuestra metodología de monitoreo para la implementación de redes VPN MIKROTIK hacia servidores entre ciudades de Lima y Pisco. Para nuestra información se realizó una extensa búsqueda y revisión selectiva de la literatura, de investigaciones en diferentes bases de datos, repositorios, libros, revistas, artículos indexados entre otros (Hernández y Mendoza 2018).

Tuvimos en cuenta antecedentes nacionales que sustentan nuestro proyecto tales como:

Santisteban (2020) analizó una revisión de los materiales de impulso para la red definida, la arquitectura y las métricas definidas por software. Se ha utilizado en una población de 288 personas para actividades de investigación. Por lo tanto, se probó en la muestra 17 con una cantidad seleccionada para evaluación analítica. Por otro lado, la investigación que obtuvieron se centró en el análisis cualitativo y cuantitativo del controlador SDN para medir el rendimiento de la red. Por lo tanto, se publicará una revisión de la literatura del artículo SDN Software-Defined Networking, en particular una interpretación de la evaluación comparativa del rendimiento del controlador. En resumen, se muestran el comportamiento, los componentes, los subcomponentes, la funcionalidad, las características y las métricas de la arquitectura SDN

Muñoz (2017) se planteó una implementación de balanceo de carga de Internet usando Mikrotik para asegurar el cumplimiento de las políticas definidas en Health Network director. Este estudio se realizó de acuerdo con un diseño de estudio ab initio. La población es una encuesta de satisfacción de los usuarios de la web, con una muestra de 60 trabajadores. Por tanto, es comprensible que el 83,33% de los trabajadores encuestados sientan que necesitan implementar el balanceo de carga de Internet. El 16,67% dijo que no era necesario optimizar el equilibrio de carga en Internet. En resumen, si existe un alto nivel de conciencia sobre la necesidad de realizar optimizaciones a través del balanceo de carga de Internet utilizando Mikrotik, se ha recopilado, interpretado y analizado. En esta investigación se tiene como aporte el uso de la metodología de redes para distintos proyectos y teniendo en cuenta el uso de la matriz FODA.

Pacotaype (2018) explicó el impacto de la elaboración de la metodología del rendimiento del firewall, para mantener según su estudio, los equipos firewalls en hardware superan a los firewalls en software. Con este estudio se utilizó el diseño de investigación preexperimental. En la población se consideró cuatro firewalls de las cuales dos son software y dos de hardware, de tal manera, la muestra es de cuatro firewalls. Asimismo, la metodología en la que se toma esta investigación se basa en las siguientes fases: (a) planeamiento, (b) implementación y pruebas y (c) análisis de resultados, estos son la metodología de evaluación de rendimiento firewall. Este estudio concluye que, aplicando la metodología de evaluación en el desempeño del firewall, ya que, es posible medir el desempeño en los firewalls en hardware en cuanto a marca Palo Alto y Fortinet más alto que los basados en software tales como Endian y Sophos. En este estudio se aporta a la investigación en una metodología donde permitirá medir el procedimiento normal de Kolmogórov-Smirnov y Shapiro-Wilk sobre datos de la muestra.

Julca y Tapia (2020) en su investigación tienen como propósito, diseñar una metodología que sea integral y para evaluación del rendimiento de los Switches. Como muestra utilizaron 3 Switches (Cisco, Extreme y Fortinet) por lo tanto, se ejecutaron 100 interacciones, como metodología utilizaron la MEIRS (Planear, Hacer, Verificar y actuar). Concluyeron que es importante utilizar la metodología MEIRS ya que sirve para evaluar y medir los dispositivos de red. Recomendaron profesionales en redes y comunicación, primero tener en cuenta las características técnicas necesarias y aplicando la metodología MEIRS.

De la Cruz y Vera (2019) estudiaron el propósito del uso de la VPN en la gestión de aplicación de intranet en la Universidad Nacional Pedro Ruiz Gallo tiene como objetivo permitir el acceso remoto a los datos y aplicaciones internas, mediante un software libre. Como muestra utilizaron 2 servidores configurados (Active Directory Windows 2000), como metodología utilizaron UNPRG. Concluyeron que utilizando la metodología UNPRG demuestra seguridad en los datos VPN permitiendo un software libre ofreciendo seguridad y confidencialidad. Recomendaron utilizar una herramienta Softether VPN Client Manager por ser de entorno gráfico y fácil acceso.

Santisteban (2020) explico que la revisión bibliográfica de redes definidas por software, su estructura y los factores para su evaluación. Esta investigación

se centra en proporcionar a los administradores de red un marco completamente repetible. Se basa en la arquitectura de redes definidas por software, lo que facilita las decisiones de gestión de redes informáticas. Además, la base de datos proporciona 288 coincidencias. Asu vez en la combinación de información en las redes definidas por software, debemos ser más específicos, elegir temas y elegir artículos que puedan respaldar nuestro trabajo y objetivos. Como conclusión, este trabajo presenta una revisión actualizada, compacta y experimental del análisis de desempeño del controlador SDN y presenta un desafío, ya que proporciona conocimientos útiles para el proceso de visualización. Consulte el directorio con atención. Los resultados son muchos.

Tal cual, se detalla el tiempo de respuesta grado LAN en la Red, en la cual se mejoró de 78 milisegundos de la red presente a 17 milisegundos con el Modelo de administración de servicios de red utilizando RouterOS Mikrotik (Davila 2019; p. 74). Sin embargo, se tiene los tiempos de contestación grado WAN de la Red, donde se mejoró de 78 milisegundos de la red presente a 40 milisegundos con el Modelo de administración de servicios de red con RouterOS Mikrotik (Davila 2019; p. 74).

Por otra parte, los tipos de VPN son: (a) Sistemas basados en hardware, (b) Sistemas basados en firewall y (c) Sistemas basados en software. De tal manera, las conexiones VPN, que han sido basadas en Hardware tienen al borde del Server de la compañía un Router, el que tiene la labor de encriptación de data, además de apertura y cierre de los túneles VPN cuando este funciona como recepción (Cueva 2018; p. 37). Por otro lado, estos sistemas aprovechan las bondades del firewall como restringir el acceder a la red o crear posibles registros de amenazas, y también ofrecen otras opciones, como la traducción y autenticación de direcciones muy fuerte (Cueva 2018; p. 37). Asimismo, estos sistemas de software son ideales cuando dos extremos que no forman parte de la misma organización desean comunicarse de forma remota y privada (Cueva 2018; p. 38).

Se considera los siguientes antecedentes internacionales que sustentan nuestro proyecto:

Marín, Patiño, Acevedo (2020) mencionaron brindar a las empresas soluciones asequibles para mitigar el riesgo de ataques de seguridad de TI con el fin de mejorar la disponibilidad y la integridad de la información. Se tuvo como

enfoque de investigación cuantitativo. De tal forma, permite evaluar el riesgo del ataque. Como resultado, se decidió la implementación del sistema, donde se probó continuamente durante ocho horas y se llevaron a cabo varios ataques de intrusión a través de múltiples Linux Kali que admiten ocho máquinas zombis. Como conclusión, esto significa que puede acceder a su VPN para una conexión más segura desde prácticamente cualquier lugar del mundo. Este estudio muestra que se pueden utilizar VPN potentes para determinar la seguridad y la inocuidad de los ciberataques.

Rosero (2021) propone establecer una red privada para utilizar y proteger adecuadamente los datos sensibles evitando los riesgos de ciberataques se realizan en el estudio de la propuesta teniendo en cuenta factores de adaptación a la infraestructura. Se adoptó un enfoque de investigación cuantitativa / cualitativa para validar el rendimiento basado en el VPN. Por lo tanto, la solución VPN más fácil de implementar y más fácil de usar es SSL VPN. Esto se debe a que no se expone la integridad de la configuración. De hecho, solo necesita configurar pares, puertos y autenticación de firewall con FortiClient. En conclusión, se tiene el comportamiento de las VPN en la actualidad, se ha recopilado información sobre el comportamiento de varios protocolos de seguridad y los conceptos de operación IPSec y SSL / TLS utilizados principalmente. Tipos y contextos de VPN disponibles.

Realpe (2016) implementa un sistema web de monitoreo de redes y conjuntos Networking, configurando la herramienta MRTG (Multi Router Traffic Grapher) y la tecnología Mikrotik (compañía letona proveedora de tecnología disruptiva de hardware y software para la construcción de redes), en un servidor CentOS para la compañía J&STECHNOLOGY. Asimismo, este análisis se fundamenta en la metodología RUP, tal cual, se desarrolló las siguientes fases de implementación: (a) inicio, (b) preparación, (c) creación y (d) transición. Como consecuencia, el sistema de monitoreo a través de MRTG comprueba que los servicios ofrecidos se encuentren funcionando y tanto los consumidores como técnicos logren entrar a ellos. Como conclusión, El desarrollo de esta aplicación permitirá a la empresa J&STECHNOLOGY contar con un instrumento de monitoreo de su red inalámbrica en tiempo real.

Wu y Xiao (2019) estudiaron el impacto en la calidad del servicio VPN en Chengdu, China, investigamos el impacto en el rendimiento utilizando varias

topologías de red VPN formadas entre servidores. Asimismo, construyen una metodología a partir de una arquitectura experimental que consta de (a) indicadores de prueba, (b) remitente y receptor, (c) arquitectura experimental estructurado en: cascada de cadenas (i), de la cascada (ii) y para la cascada (iii). Se utiliza para cuatro criterios: rendimiento, retardo de la red, fluctuación y tasa de pérdida de paquetes (PLR). Por lo tanto, construimos una red privada virtual utilizando Softether, una herramienta de código abierto proyectos de la Universidad de Tsukuba. El software consta de dos partes: un concentrador y un adaptador virtuales. Puede utilizar la herramienta D-ITG (Generador de tráfico de Internet distribuido) para enviar y recibir flujos de datos para obtener datos de prueba relevantes relacionados con el rendimiento. En conclusión, el rendimiento del software y SSTP / L2TP es básicamente el mismo en términos de rendimiento. En esta hipótesis se utilizaron las funciones de las herramientas de evaluación y topología de redes.

Narayan et al. (2015) estudiaron el rendimiento y observación de tres protocolos VPN (PPTP, IPSec y SSTP) en entornos de red cliente / servidor de Windows 7 y Windows 2012 a través de medios alámbricos e inalámbricos (Ethernet e IEEE802.11ac) utilizando dos instancias de IP. Se estructuro la metodología en: (i) requerimientos del sistema, (ii) roles, (iii) herramienta e (iv) implementación. La red ha sido probada tanto con IPv4, como IPv6, con solo un protocolo habilitado en el adaptador NIC a la vez. Para demostrar el rendimiento consistente, productividad de red, facilidad y capacidad de producir la métrica requerida se aplica herramientas tecnológicas como el Iperf, que genera tanto el protocolo TCP como el UDP. Asimismo, concluyeron que el IPSec tuvo el menor rendimiento de los tres VPNs para UDP y TCP; SSTP tuvo el rendimiento más consistente, así como el mejor rendimiento de todas las VPN para los tipos de tráfico UDP, además no sufre en la pérdida de paquetes que plaga tanto el PPTP como el IPSec en los tamaños de buffer más grande. De este antecedente se tomó la herramienta ejecutada para la evaluación de rendimiento de los protocolos de los VPNs

Según, Balladares (2017) indicó que las tasas de transferencia de datos se evalúan por separado para descargas entre sitios remotos y computadoras y descargas de archivos (p. 45). Por otro lado, Los administradores de red obtienen resultados estadísticos sobre los resultados de la evaluación ejecutados por la

velocidad de transferencia de archivos individuales (descarga/subida) (Balladares 2017; p. 45-46). Asimismo, bajo la premisa de que el límite de ancho de banda debe mejorar las capacidades de descarga y carga de archivos de su sistema de programación informática científica y tecnológica, mejorar la velocidad de descarga y descargar los archivos.

Con respecto un disco duro es una pieza de hardware que puede almacenar y restaurar grandes cantidades de datos y también es una parte básica de una computadora (Aguirre 2016). Asimismo, el consumo de disco duro frente a los ataques DDoS tiende a aumentar con los paquetes de datos infectados, lo que causa varios problemas que incluyen: (I) borrar datos del disco duro; (ii) destruir información almacenada en la memoria; iii) infectar archivos; (iv) terminar los procesos principales de la computadora; (v) pérdida de costos de soporte informático (Aguirre 2016; Chilcañán, Navas y Escobar 2017).

Jaramillo (2018) estudiaron el análisis que comparaba la VPN IPSEC y DMVPN como objetivo principal de renovar el desarrollo de redes privadas del internet. Como muestra realizaron 208 pruebas, los seguimientos se dividieron en 104 túneles IPSEC y 104 túneles DMVPN. De las 104 pruebas se lograron ejecutar 26 pruebas por túnel Spoke. Llego a una conclusión que IPSEC resulta que fácil de configurar, pero al incrementar los Spoke el control y administración se vuelve muy complejo, en cambio DMVPN muestra un desempeño rápido en configuración al ingresar los Spoke.

Nuñez (2020) investigo la agilización de los dispositivos RouterOS, mediante la implementación y diseño de la aplicación, esto va a permitir que aprovechemos la capacidad de conexión a través API (Appliction Programmada Interface) Mikrotik a fin de mejorar el rendimiento manejo y velocidad. Uso como muestra 10 RouterOS por lo cual ejecutaron solo 3 actividades (Configuración, verificación y Auditoria).

VPN es una abreviatura de Virtual Prívate Network, que es una red privada (pública inaccesible) que conecta de forma segura ubicaciones remotas utilizando medios no personales como el Internet (Musyaffa y Ryansyah 2020; p. 49). Por otra parte, esta es una técnica común para construir redes para estudiantes y administradores. También puede conectarse a una ubicación remota a través de una red pública (generalmente Internet) (Marín, Patiño y Acevedo 2020; p. 88).

Pauzhi (2016) elaborar e implementar una política de seguridad en función de los requerimientos de empresas WISP para la mitigación y prevención de ataques informáticos. Asimismo, se ha utilizado el método inductivo para la detección de los distintos tipos de ataques muy vulnerable. Para ello, en este estudio se tomó tres fases como: (a) reconocimiento de la estructura de red, (b) auditoria de red inalámbrica y (c) analizar e implementar. Como resultado, se hizo una prueba de penetración para obtener la clave de autenticación donde los clientes puedan enlazarse al punto de acceso de dicha empresa. Como conclusión, se somete a la evaluación para lograr invalidar los ataques que se pueda tener en las vulnerabilidades, hombre en medio, wardriving y puntos de acceso no autorizados, teniendo así las detecciones más comunes en la empresa WISP. Esta investigación tiene como aporte a brindar una propuesta de analizar todos los ataques preventivos así dichas empresas.

La conectividad en la red está bien definida y se basa en estándares abiertos, por el momento no se han desarrollado soluciones basadas en estándares de la capa aplicación(Egas, Viracocha y Rivera 2019; p. 46).

El Throughput tiene una importancia para evaluar el rendimiento es la cantidad real de información útil (segundos / bits / segundo) enviada a través de un canal de comunicación durante un período de tiempo específico, por lo que es importante evaluar la red privada virtual de su red (Vesga et al., citado por Pacotaype 2018; p. 35-36). De acuerdo con lo anterior mencionado, el rendimiento es la tasa de datos que se entregan con éxito al receptor a través de un enlace de comunicación durante un cierto tiempo de observación. El rendimiento se mide en bits por segundo (bps). El mayor rendimiento significa un mejor rendimiento de la red (Tulloh et al. 2020; p. 5).

Es de suma importancia y necesario entender los temas abocados y conceptos iniciales para el desarrollo de nuestro proyecto, de esta manera su comprensión y estructura sea mucho más consistente, por ello se consideraron las siguientes teorías relacionadas:

Jperf: Es un instrumento de programa independiente que posibilita hacer medidas primordiales de Throughput en las conexiones Ethernet de la red LAN (Julca y Tapia 2020; p. 93).

Lan Speed test: una herramienta simple pero poderosa para medir la transferencia de archivos, el disco duro, la unidad USB y las velocidades de la red de área local (LAN) (Pacotaype 2018; p. 130).

Winbox: es una aplicación que posibilita la gestión de Mikrotik RouterOS utilizando un ambiente gráfico de usuario, simple y sencilla (Nuñez 2020).

III. MÉTODO

3.1 Tipo y diseño de investigación

El tipo de investigación que se utilizará en este estudio es aplicado, pues tiene como principal objetivo resolver problemas de conexión y seguridad en micro y pequeñas empresas. Asimismo, un tipo de investigación aplicada es la investigación teórica en la que se prueba la teoría del aprendizaje para analizar las soluciones de un problema (Sáez, 2017, p. 17). Teniendo así en el presente trabajo se tiene la utilización de investigación aplicada apoyándose con una incrementación al conocimiento científico de las VPN con el fin de implementar una conexión.

En el presente estudio de investigación se aplicará el enfoque cuantitativo. Con respecto, Sáez (2017) mencionó que el uso estadístico y cuantitativo de los aspectos observables son identificables en los análisis de datos al utilizar herramientas estadísticas, análisis y el uso de procesos experimental (p. 17). De tal manera, Hernández y Mendoza (2018) mencionaron que los métodos cuantitativos es un proceso de un modelo ordenado y así permitir lograr los objetivos planteados en la investigación. Donde la métrica es importante en obtener antes la recopilación de datos (p. 6). De tal forma, el enfoque de esta investigación es cuantitativa, ya que, se midió la variable de la implementación de conexión VPN MIKROTIK entre servidores.

La investigación es de tipo preexperimental de diseño de preprueba/posprueba con un solo grupo según menciono (Hernández y Mendoza 2018, p. 163).

3.2 Variables y operacionalización

En este proyecto se enuncia la variable la implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco, especificando todos los aspectos que se va a tocar a lo largo del presente estudio. A continuación, se precisa cada aspecto:

Variable Independiente: Redes VPN

A. **Definición conceptual:** VPN es una abreviatura de Virtual Prívate Network, que es una red privada (pública inaccesible) que conecta de

forma segura ubicaciones remotas utilizando medios no personales como el Internet (Jota, Ramirez y Penagos 2018; Cueva 2018).

B. **Definición operacional:** Esta conexión prioriza la privacidad de la información que se transmite, evitando que agentes no autorizados puedan vulnerar o capturar paquetes en el tráfico y sustraer la información. Este tipo de solución bien implementada y configurada es usada para transmitir información considerada sensible, data de conexión y accesos remotos en grandes, pequeñas, medianas y microempresas. Las empresas con la nueva normalidad se han visto obligados a buscar y usar diversas soluciones de acceso remoto, para enlazar sedes, acceder a servidores y/o facilitar a los colaboradores puedan acceder a las aplicaciones de la empresa y seguir realizando sus actividades sin movilizarse de sus domicilios.

Variable Dependiente: Servidores

A. **Definición conceptual:** Los servidores se ejecutan mediante una arquitectura (Cliente-Servidor), a través de una Red. Los servidores dan servicios fundamentales en una Red, así sea usuarios privados, públicos, organizaciones o compañías por medio de internet (Davila 2019; Morán 2020; Castro 2019).

B. **Definición operacional:** Los servidores son artefactos informáticos que proporcionan, distribuye y almacena información y servicios. Por consiguiente, el servidor ejecuta otras labores para beneficio de los consumidores; les da la probabilidad de compartir datos, información y recursos de hardware y programa, para ello consumen recursos de hardware y software, conectándose a una red local y publica, según sé la necesidad.

C. **Dimensiones:**
   - Desempeño en la Red (Chilcañán, Navas y Escobar 2017).
   - Consumo de Recursos (Julca y Tapia 2020; Pacotaype 2018).
   - Conectividad de la Red (Chilcañán, Navas y Escobar 2017; Egas, Viracocha y Rivera 2019).

D. **Indicadores:**
   - Medición de Throughput (Pacotaype 2018; Julca y Tapia 2020; Vesga, Granados y Vesga 2016).

- Consumo de Memoria RAM (Aguirre 2016; Pacotaype 2018).
- Tiempo de Respuesta de la Red Lan (Davila 2019).

E. Escala de medición:

- Ficha de observación (Hernández y Mendoza 2018).

3.3 Población, muestra y muestreo

En esta parte, se menciona las definiciones en relación a población, muestra, muestre y unidad de estudio:

A. Población: Hernández y Mendoza (2018) definieron que la población es un conjunto de todos los incidentes, individuos o componentes que se asemejan en descripciones específicos. En consecuencia, el presente estudio tiene una población delimitada de herramientas tecnologías de monitoreo de red, usando para la presente investigación 2 equipos Mikrotik.

Tabla Nª 1 : *Tabla de Población*

Población	Periodo	Indicador
2 equipos Mikrotik	1 mes	Tiempo de Respuesta de Throughput
		Porcentaje del consumo CPU
		Medición de subida de archivos en la red

B. Muestra: La muestra es un subgrupo de la población; es decir, es una entidad pequeña que pertenece y representa a una población definida y limitada por una característica similar llamada población (Hernández y Mendoza 2018).

Además, el tamaño de una muestra es un número que puede estimar o calcular por mediante de fórmulas matemáticas o programas informáticos para determinar la cantidad de la muestra (Arias, Villasís y Miranda 2016; p. 206)

En este sentido, Las muestras fueron creadas por investigadores como una forma conveniente de garantizar la proximidad y accesibilidad de artículos (Otzen y Manterola 2017; p. 230).

La muestra para la presente investigación está conformada por las herramientas Mikrotik, los mismos que serán evaluados en los siguientes criterios:

(a) Desempeño en la red,

(b) Consumo de recursos y

(c) Conectividad de la red.

los cálculos de las muestras se realizarán mediante la fórmula siguiente:

$$n = \frac{NZ^2(1-p)}{Ne^2 + Z^2p(1-p)}$$

Dónde:

n = Muestra

N =Población

Nivel de Confianza = 95% → Z = 1.96

e (error muestral admisible) = 0.05

p = 0.5

Muestras para la Población que corresponde al nivel de codificación de registros y al porcentaje de cumplimiento de programación.

Debido a que la población asignada es muy reducida para la toma de las muestras, se optó por tomar toda la población como referente para los indicadores. La muestra para el nivel de codificación de registros es de n registros y la muestra para el porcentaje del cumplimiento de programación es de n registros.

Tabla Nª 2 : *Tabla de Muestra*

Población	Muestra	Periodo
2 equipos Mikrotik	N registros	1 mes

C. **Muestreo:** El muestreo es no probabilístico es utilizado en el procedimiento para elegir la muestra de la población, debido a esto la selección de personas o factores a estudiar dependerá de criterios, características y otros factores considerados por el investigador (Otzen y Manterola 2017; p. 228).

De esta manera, la técnica de muestreo no probabilístico es utilizadas en actividades de investigación, muestreo por conveniencia, casos disponibles u objetos alcanzables (Hernández y Mendoza 2018; p. 390).

En el presente estudio es no probabilístico; ya que, elegimos una muestra sin utilizar fórmulas y métodos de selección, no basados en la probabilidad, porque elegimos software de red privada virtual para la conveniencia de los investigadores (Pacotaype 2018; p. 72; Hernández y Mendoza 2018).

D. **Unidad de análisis:** El interés por conocer la unidad de análisis depende de quién o quiénes el individuo de la medida (Hernández y Mendoza 2018; p. 172). En esta investigación, la unidad de análisis son las ciudades (Lima - Pisco).

3.4 Técnicas e instrumentos de recolección de datos

En esta parte se dicen a la técnica y a las herramientas de recolección de datos, explicando ciertos conceptos resaltantes y las herramientas seleccionadas en nuestro análisis. Así mismo, se define la validez y confiabilidad de las herramientas aplicadas.

Las técnicas de recolección de datos

En este estudio se adoptó por la técnica de la observación. Para ello, Hernández y Mendoza (2018) explicaron que este método de recolección de datos se enfoca en registros sistemáticos, auténticos y confiables de comportamientos y escenarios prominentes y verificables.

- **Fichas de observación:** es una técnica que consta de registrar todos los datos que se obtienen de los instrumentos llamados fichas, los cuales apropiadamente son elaborados y ordenados conteniendo la mayor parte de la información que se recolecta en la investigación, está técnica tiene como referencia a Ficha de observación (Hernández y Mendoza 2018).
- **Ficha de Registro:** documento y/o registro, donde se consignan los datos recopilados durante el proceso de pruebas. Usado para anotar los registros generados y resultados. Teniendo como referencia a Ficha de observación (Hernández y Mendoza 2018).

La validez se refiere al grado de cumplimiento de una herramienta diseñada para medir variables frente a criterios establecidos. Asimismo, podemos tener

varios tipos de pruebas (Hernández y Mendoza 2018). Del mismo modo, la eficacia del contenido solo se evalúa mediante una herramienta de control de contenido en particular. Asimismo, las variables medidas deben estar definidas o especificadas en las condiciones previas y marco teórico (Hernández y Mendoza 2018).

La confiabilidad de un instrumento de evaluación se refiere a la utilidad de repetir sobre el mismo tema o temas para producir resultados similares y también se establece mediante varios métodos que se describen brevemente en conocimiento para considerar la validez y fiabilidad (Hernández y Mendoza 2018). Además, la confiabilidad de la prueba se demuestra por la confiabilidad de los resultados extraídos de sujetos dentro de un mismo individuo o en diferentes circunstancias (Hernández y Mendoza 2018). Por ello, se brinda el 95% de grado de confianza ante la recolección de información estadística (Hernández y Mendoza 2018).

3.5 Procedimientos

El procedimiento es una forma basada en el diseño de adaptarse al problema en cuestión mediante la realización de una serie de pasos adecuados para el problema general de investigación y su recopilación utilizando varios objetos y diversas herramientas. Los datos y los entregables necesarios para la investigación y el desarrollo se consideran recursos valiosos. Los investigadores necesitan interpretar y documentar los resultados verbales para permitir que las organizaciones reclasifiquen a la información (Abeleira, Vásquez y Peña 2016; p. 135). La implementación se desarrolló con el propósito de brindar datos e informar a toda persona interesada en las herramientas de monitoreo y redes VPN para analizar sobre la efectividad sobre la gestión o selección de herramienta necesaria para monitorear el tráfico y redes interconectadas a través de pruebas para verificar los requerimientos tecnologías de la herramienta de red WAN con herramientas pare-seleccionadas para las pruebas con antecedentes que brindaran opciones exactas a solucionar el objetivo establecido (Abeleira, Vásquez y Peña 2016; p. 135).

En la implementación propuesta, para crear una vpn a través de protocolos l2tp se usará 2 Router Mikrotik modelos RB450G, que servirán para establecer la extensión de la red Lan, una conexión segura entre 2 locaciones distintas.
El procedimiento por seguir es el siguiente:

1. Se realizará una pre prueba, a los agentes remotos en los indicadores que se requiere medir para una comparación al implementar los Router Mikrotik y realizar una post prueba.
2. Se elije el agente remoto TeamViewer y se realiza la pre prueba de medición de Throughput, consumo de memoria RAM y tiempo de respuesta.
3. Se elige equipos Mikrotik RB 450G que son los que pueden soportar configuraciones vpn. Esta elección se realiza de acuerdo con cuadro comparativo.
4. Se procede a reiniciar y dejar configuración de fábrica, o también conocida como configuración original, en los equipos, accediendo a través de la aplicación Winbox.
5. Finalmente, Se evaluará primero la información técnica cada uno de los equipos, teniendo en consideración, criterios de rendimiento, conexión a red, se determina cuáles son los procedimientos necesarios y se elabora dichos procedimientos para efectuar la evaluación de los Router.

3.6 Método de análisis de datos

Se define mediante la demostración e interpretación de los resultados obtenidos de las pruebas realizadas en el estudio y se refleja en una matriz de información que utiliza tecnologías y técnicas de información para la recolección de datos de precisión (Hernández y Mendoza 2018).
Conforme a la información procesada, se realiza con fichas de observación, de esta manera facilita el manejo de los resultados, por eso (Hernández y Mendoza, 2018) mencionan que se puede recoger conclusiones de las fichas tanto pre observación como post observación procesados en las pruebas estadísticas.

se exponen y explicarán los resultados obtenidos de la tesis de forma detallada para así poder demostrar certeramente los puntos planteados. Asimismo, se han realizado las pruebas Shapiro-Wilk para determinar la normalidad de los datos

con los que estamos trabajando, los cuales fueron recolectados mediante observación y registrados las mencionadas fichas, si los datos no se ajustan a una prueba normal se procederá a realizar la prueba de Wilcoxon para mayor validez y confiabilidad.

3.7 Aspectos éticos

En este punto, se detallará los aspectos éticos profesional según el estilo ISO 690 en el presente trabajo de investigación, donde se respete el código de ética de la investigación.

En este sentido, este proyecto de investigación se ha presentado para consultar artículos sobre el Código de Ética del Instituto Tecnológico del Perú, como el artículo 14, que establece que los ingenieros tienen el deber de vivir de acuerdo con el orden social y traer la felicidad para todo el mundo. Debe demostrarse la importancia del uso de recursos en el desempeño del trabajo profesional (CIP, 1996, p. 3).

Además, el artículo 15 también estipula que los ingenieros deben mantener y proteger no solo el honor y la dignidad de sus carreras, sino también su integridad. De esta manera, podemos observar la lealtad de las personas hacia empleadores, clientes, profesionales e instituciones académicas. Por tanto, sobre los principios contenidos en tratados como la lealtad profesional, la integridad y el honor profesional (CIP, 1996, p. 3).

Por otro lado, las citas de referencias en la redacción son necesarias donde deben identificarse en la bibliografía, por lo que los autores, los años y las páginas deben incluirse como datos relevantes manteniendo el orden correcto de las citas (Universidad César Vallejo, 2017, p. 9).

IV. RESULTADOS

En este capítulo, detallaremos los resultados logrados luego de la aplicación de la técnica del fichaje, mediante cotejaron datos existentes a través del instrumento de la ficha; estos datos sometidos a una mera presentación no soportaran mayores interpretaciones en el presente capitulo; así también debe tenerse presente que se ha empleado el método estadístico Shapiro – Wilk para cada uno de los indicadores (Medición de Throughput, Consumo de Memoria RAM y Tiempo de respuesta Red Lan) debido a que la cantidad de datos recopilados es igual a cincuenta.

Kolmogorov-Smirnov[a] n>50	Shapiro-Wilk n≤50

Figura 1. Condición de empleo estadístico.

Para la realización del análisis estadístico descriptivo, la prueba de normalidad y prueba de hipótesis de los datos obtenidos, se empleó como herramienta el paquete estadístico IBM SPSS Statistics V.26.

Prueba de Hipótesis especifica 1 del Indicador: Medición de Throughput

- **Planteamiento de la hipótesis especifica.**

  $\boldsymbol{HE1_0}$: La Implementación de redes VPN MIKROTIK no incrementó el desempeño en la red de los servidores entre ciudades de Lima y Pisco.

  $\boldsymbol{HE1_A}$: La Implementación de redes VPN MIKROTIK incrementó el desempeño en la red de los servidores entre ciudades de Lima y Pisco.

Tabla Nª 3 : *Indicador Descriptivo de Throughput 64 Bytes*

Descriptivos				
			Estadístico	**Error estándar**
THROUGHPUT AGENTE REMOTO 64 Bytes	Media		81924,28	3956,520
	95% de intervalo de confianza para la media	Límite inferior	73973,36	
		Límite superior	89875,20	
	Media recortada al 5%		82626,08	
	Mediana		83378,00	
	Varianza		782702336,002	
	Desviación estándar		27976,818	
	Mínimo		19008	
	Máximo		140367	
	Rango		121359	
	Rango intercuartil		44414	
	Asimetría		-,342	,337
	Curtosis		-,414	,662
THROUGHPUT VPN 64 Bytes	Media		49921,28	1548,505
	95% de intervalo de confianza para la media	Límite inferior	46809,44	
		Límite superior	53033,12	
	Media recortada al 5%		50825,96	
	Mediana		53600,00	
	Varianza		119893345,593	
	Desviación estándar		10949,582	
	Mínimo		19008	
	Máximo		63040	
	Rango		44032	
	Rango intercuartil		15680	
	Asimetría		-1,225	,337
	Curtosis		,882	,662

En la tabla N.º 3, se puede apreciar los resultados de la aplicación de prueba descriptiva, el Throughput Agente Remoto 64 bytes tiene como media de 81924.28 bytes en 50 muestras realizadas, el Throughput VPN 64 bytes tiene como media 49921.28 bytes.

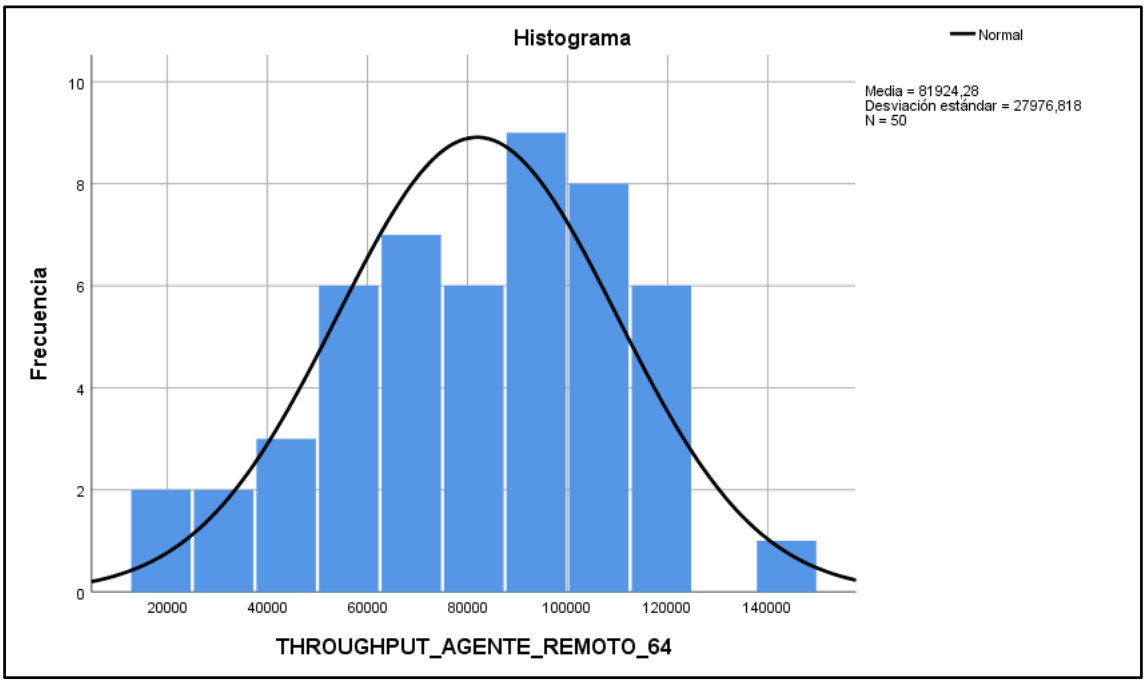

Figura 2. Histograma de Medición de Throughput Agente Remoto 64 Bytes

En la figura N.º 2, se muestra el histograma de medición de Throughput Agente Remoto 64 bytes logramos obtener un promedio de 81924.28 bytes, con una desviación estándar de 27976.818 bytes, de un total de 50 muestras.

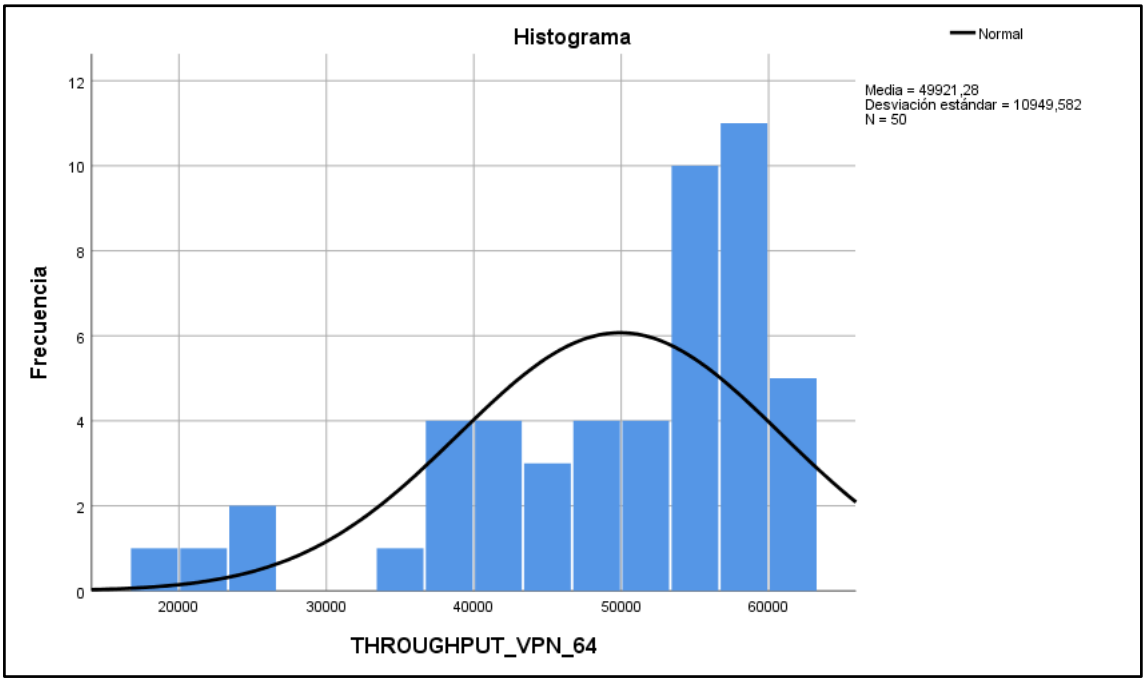

Figura 3. Histograma de Medición de Throughput VPN 64 Bytes

En la figura Nª 3, del histograma de medición de Throughput VPN 64 bytes logramos obtener un promedio de 49921.28 bytes, con una desviación estándar de 10949.582 bytes, de un total de 50 muestras.

Tabla Nª 4 : *Indicador Descriptivo de Throughput 128 Bytes*

Descriptivos				
			Estadístico	**Error estándar**
THROUGHPUT AGENTE REMOTO 128 Bytes	Media		73058,50	1217,509
	95% de intervalo de confianza para la media	Límite inferior	70611,82	
		Límite superior	75505,18	
	Media recortada al 5%		72403,50	
	Mediana		72351,50	
	Varianza		74116456,051	
	Desviación estándar		8609,091	
	Mínimo		59523	
	Máximo		109994	
	Rango		50471	
	Rango intercuartil		9227	
	Asimetría		1,728	,337
	Curtosis		5,815	,662
THROUGHPUT VPN 128 Bytes	Media		69383,68	1218,874
	95% de intervalo de confianza para la media	Límite inferior	66934,26	
		Límite superior	71833,10	
	Media recortada al 5%		68726,04	
	Mediana		68608,00	
	Varianza		74282655,242	
	Desviación estándar		8618,739	
	Mínimo		55936	
	Máximo		106496	
	Rango		50560	
	Rango intercuartil		9344	
	Asimetría		1,743	,337
	Curtosis		5,920	,662

En la tabla N.º 4, se puede apreciar los resultados de la aplicación de prueba descriptiva, el Throughput Agente Remoto 128 bytes tiene como media de 73058.50 bytes en 50 muestras realizadas, el Throughput VPN 128 bytes tiene como media 69383.68 bytes.

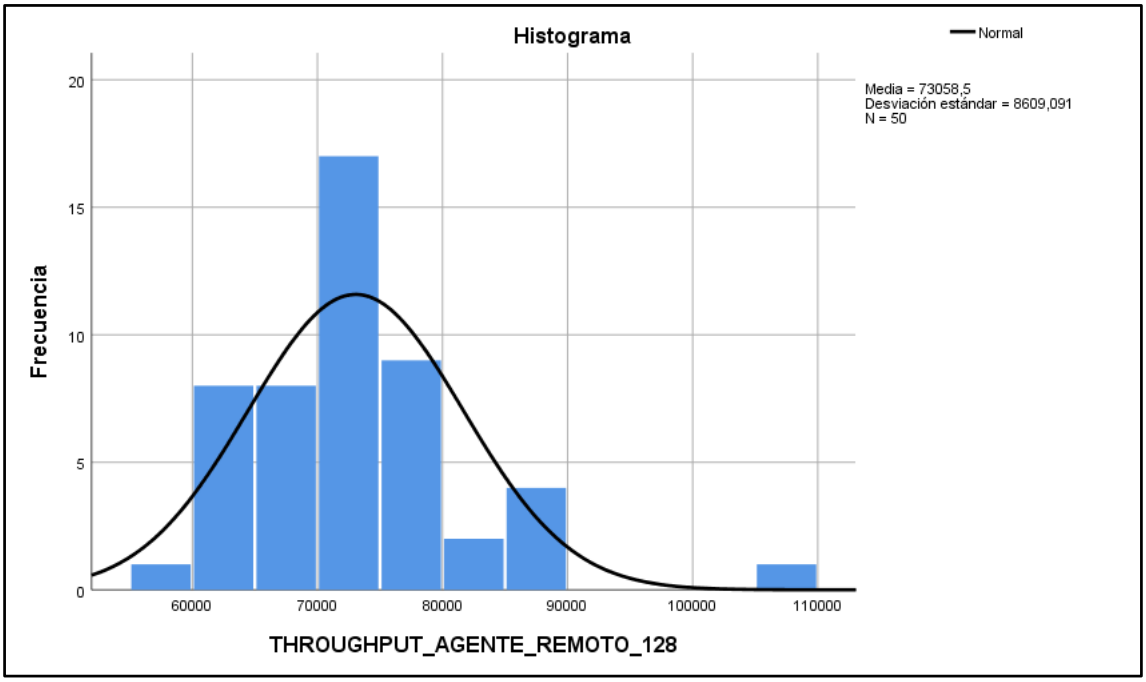

Figura 4. Histograma de Medición de Throughput Agente Remoto 128 Bytes

En la figura N.º 4, del histograma de medición de Throughput Agente Remoto 128 bytes logramos obtener un promedio de 73058.5 bytes, con una desviación estándar de 8609.091 bytes, de un total de 50 muestras.

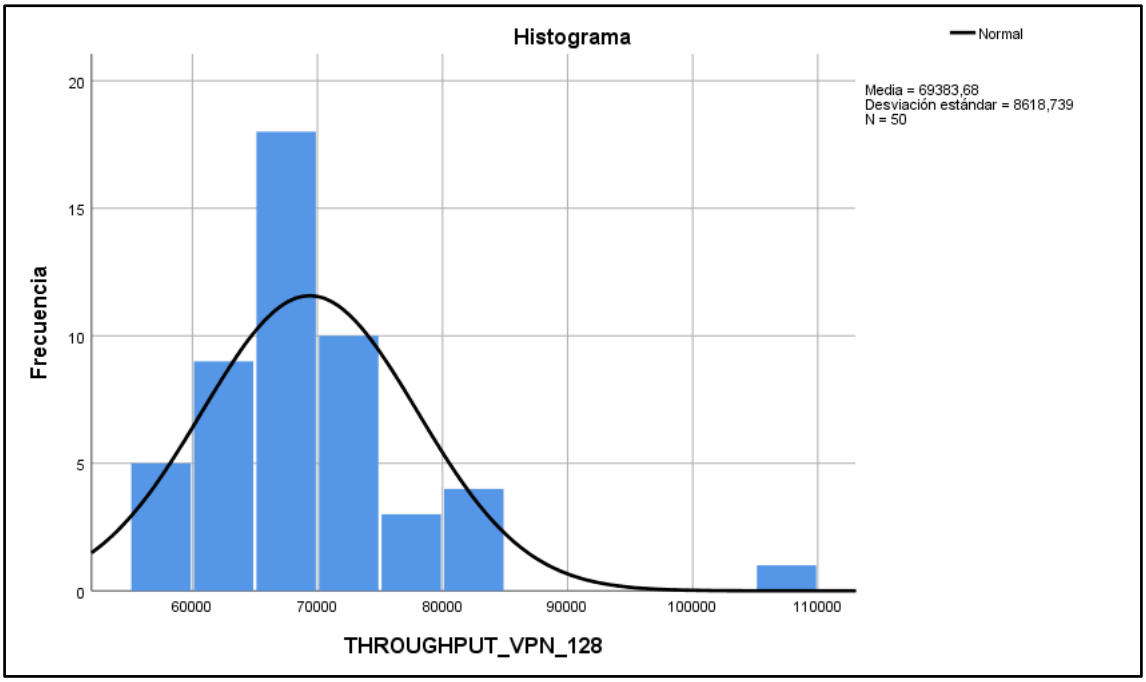

Figura 5. Histograma de Medición de Throughput VPN 128 Bytes

En la figura N.º 5, del histograma de medición de Throughput VPN 128 bytes logramos obtener un promedio de 69383.68 bytes, con una desviación estándar de 8618.739 bytes, de un total de 50 muestras.

Tabla Nª 5 : *Indicador Descriptivo de Throughput 256 Bytes*

Descriptivos				
			Estadístico	**Error estándar**
THROUGHPUT AGENTE REMOTO 256 Bytes	Media		246122,98	2374,657
	95% de intervalo de confianza para la media	Límite inferior	241350,93	
		Límite superior	250895,03	
	Media recortada al 5%		244603,06	
	Mediana		240547,00	
	Varianza		281949851,244	
	Desviación estándar		16791,362	
	Mínimo		224996	
	Máximo		302823	
	Rango		77827	
	Rango intercuartil		17583	
	Asimetría		1,417	,337
	Curtosis		2,194	,662
THROUGHPUT VPN 256 Bytes	Media		242448,16	2378,900
	95% de intervalo de confianza para la media	Límite inferior	237667,58	
		Límite superior	247228,74	
	Media recortada al 5%		240916,80	
	Mediana		236928,00	
	Varianza		282958217,117	
	Desviación estándar		16821,362	
	Mínimo		221440	
	Máximo		299264	
	Rango		77824	
	Rango intercuartil		17344	
	Asimetría		1,422	,337
	Curtosis		2,210	,662

En la tabla N.º 5, se puede apreciar los resultados de la aplicación de prueba descriptiva, el Throughput Agente Remoto 256 bytes tiene como media de 246122.98 bytes en 50 muestras realizadas, el Throughput VPN 256 bytes tiene como media 242448.16 bytes.

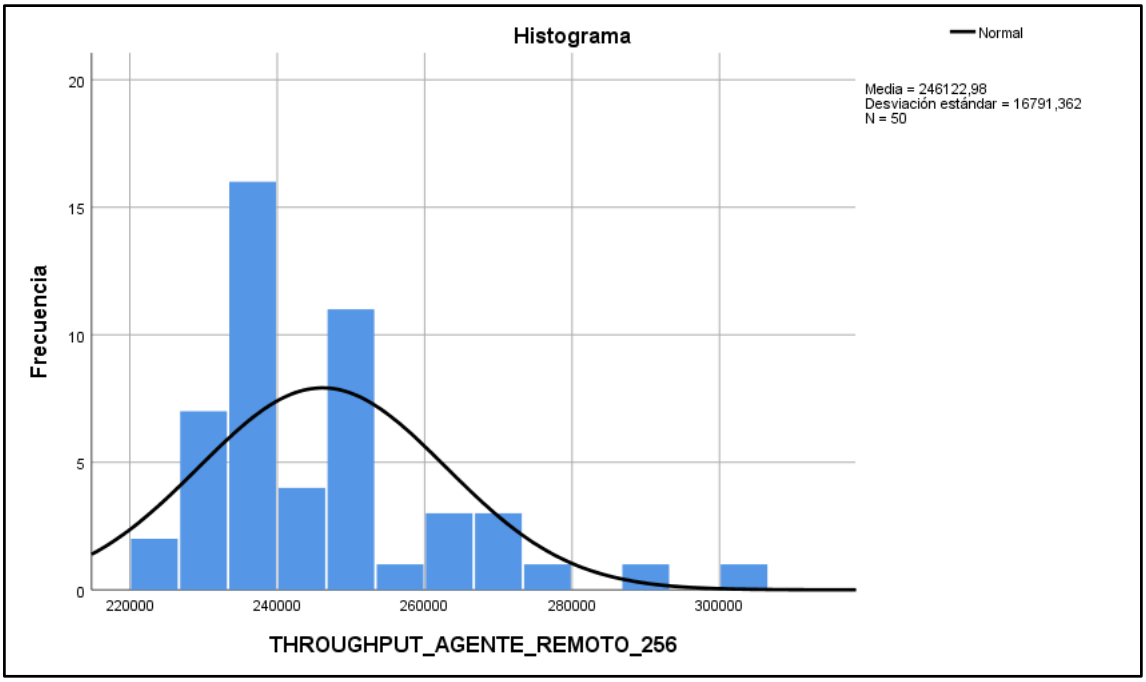

Figura 6. Histograma de Medición de Throughput Agente Remoto 256 Bytes

En la figura N.º 6, del histograma de medición de Throughput Agente Remoto 256 bytes logramos obtener un promedio de 246122.98 bytes, con una desviación estándar de 16791.362 bytes, de un total de 50 muestras.

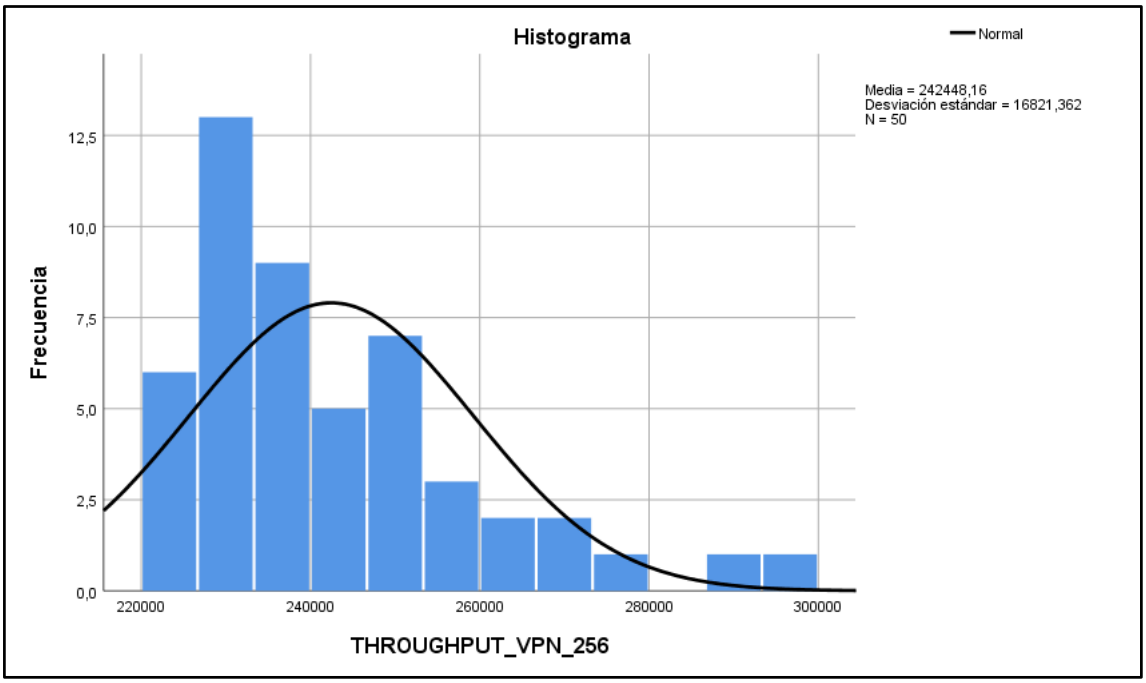

Figura 7. Histograma de Medición de Throughput VPN 256 Bytes

En la figura N.º 7, del histograma de medición de Throughput VPN 256 bytes logramos obtener un promedio de 242448.16 bytes, con una desviación estándar de 16821.362 bytes, de un total de 50 muestras.

Tabla Nª 6 : *Indicador Descriptivo de Throughput 512 Bytes*

Descriptivos				
			Estadístico	**Error estándar**
THROUGHPUT AGENTE REMOTO 512 Bytes	Media		553292,52	9217,184
	95% de intervalo de confianza para la media	Límite inferior	534769,90	
		Límite superior	571815,14	
	Media recortada al 5%		548067,32	
	Mediana		545260,00	
	Varianza		4247823619,398	
	Desviación estándar		65175,330	
	Mínimo		449521	
	Máximo		750786	
	Rango		301265	
	Rango intercuartil		65485	
	Asimetría		1,400	,337
	Curtosis		2,349	,662
THROUGHPUT VPN 512 Bytes	Media		549611,52	9207,883
	95% de intervalo de confianza para la media	Límite inferior	531107,59	
		Límite superior	568115,45	
	Media recortada al 5%		544392,53	
	Mediana		541696,00	
	Varianza		4239255918,132	
	Desviación estándar		65109,569	
	Mínimo		445952	
	Máximo		747008	
	Rango		301056	
	Rango intercuartil		65280	
	Asimetría		1,400	,337
	Curtosis		2,352	,662

En la tabla Nª 6, se puede apreciar los resultados de la aplicación de prueba descriptiva, el Throughput Agente Remoto 512 bytes tiene como media de 553292.52 bytes en 50 muestras realizadas, el Throughput VPN 512 bytes tiene como media 549611.52 bytes.

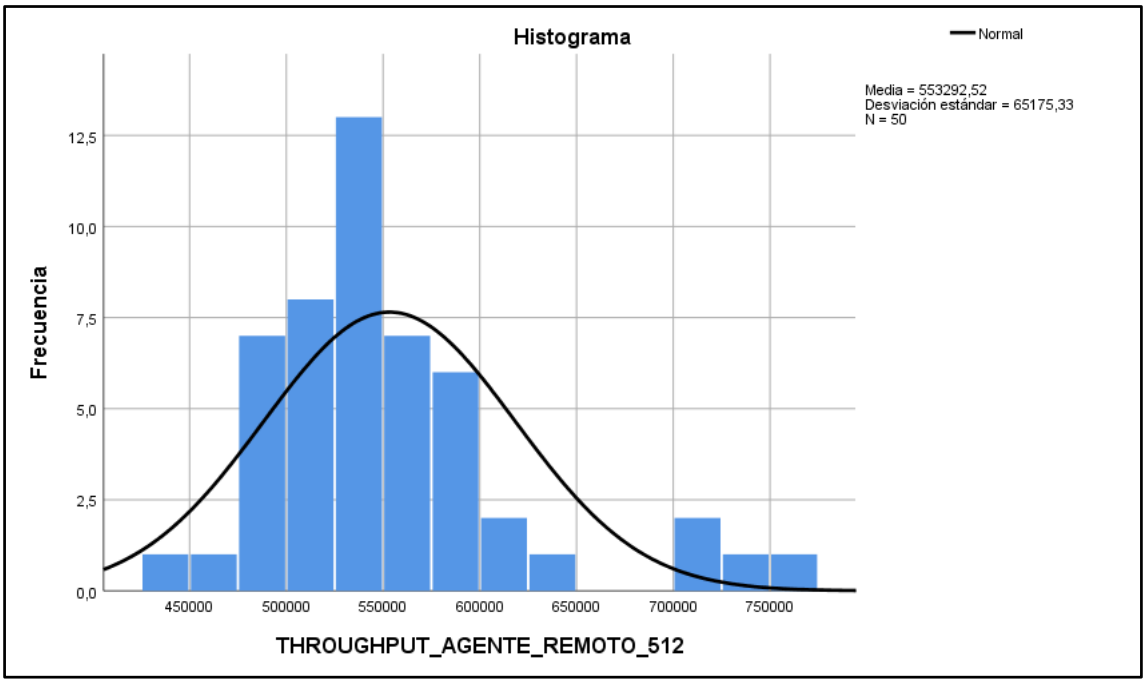

Figura 8. Histograma de Medición de Throughput Agente Remoto 512 Bytes

En la figura N.º 8, del histograma de medición de Throughput Agente Remoto 512 bytes logramos obtener un promedio de 553292.52 bytes, con una desviación estándar de 65175.33 bytes, de un total de 50 muestras.

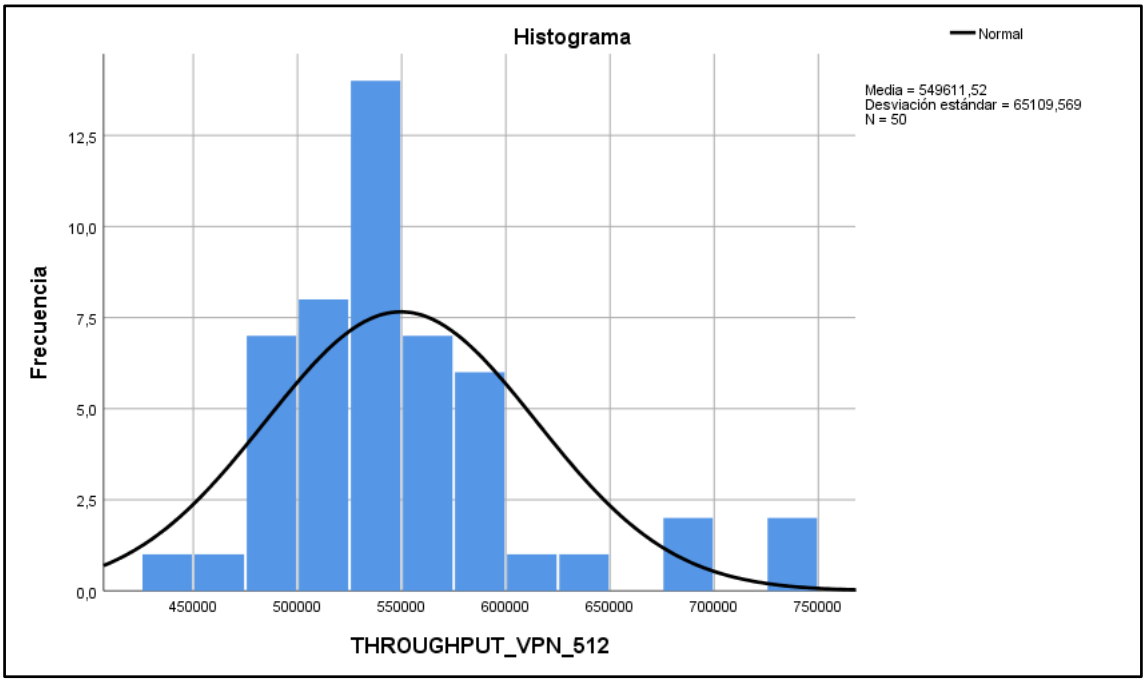

Figura 9. Histograma de Medición de Throughput VPN 512 Bytes

En la figura N.º 9, del histograma de medición de Throughput VPN 512 bytes logramos obtener un promedio de 549611.52 bytes, con una desviación estándar de 65109.569 bytes, de un total de 50 muestras.

Tabla Nª 7 : *Indicador Descriptivo de Throughput 1024 Bytes*

Descriptivos				
			Estadístico	**Error estándar**
THROUGHPUT AGENTE REMOTO 1024 Bytes	Media		407587,56	5530,937
	95% de intervalo de confianza para la media	Límite inferior	396472,73	
		Límite superior	418702,39	
	Media recortada al 5%		406597,92	
	Mediana		405925,50	
	Varianza		1529563461,435	
	Desviación estándar		39109,634	
	Mínimo		312090	
	Máximo		511790	
	Rango		199700	
	Rango intercuartil		56981	
	Asimetría		,270	,337
	Curtosis		,340	,662
THROUGHPUT VPN 1024 Bytes	Media		403906,56	5536,342
	95% de intervalo de confianza para la media	Límite inferior	392780,86	
		Límite superior	415032,26	
	Media recortada al 5%		402932,62	
	Mediana		402432,00	
	Varianza		1532554170,619	
	Desviación estándar		39147,850	
	Mínimo		308224	
	Máximo		507904	
	Rango		199680	
	Rango intercuartil		57600	
	Asimetría		,263	,337
	Curtosis		,325	,662

En la tabla N.º 7, se puede apreciar los resultados de la aplicación de prueba descriptiva, el Throughput Agente Remoto 1024 bytes tiene como media de 407587.56 Bytes en 50 muestras realizadas, el Throughput VPN 1024 bytes tiene como media 403906.56 bytes.

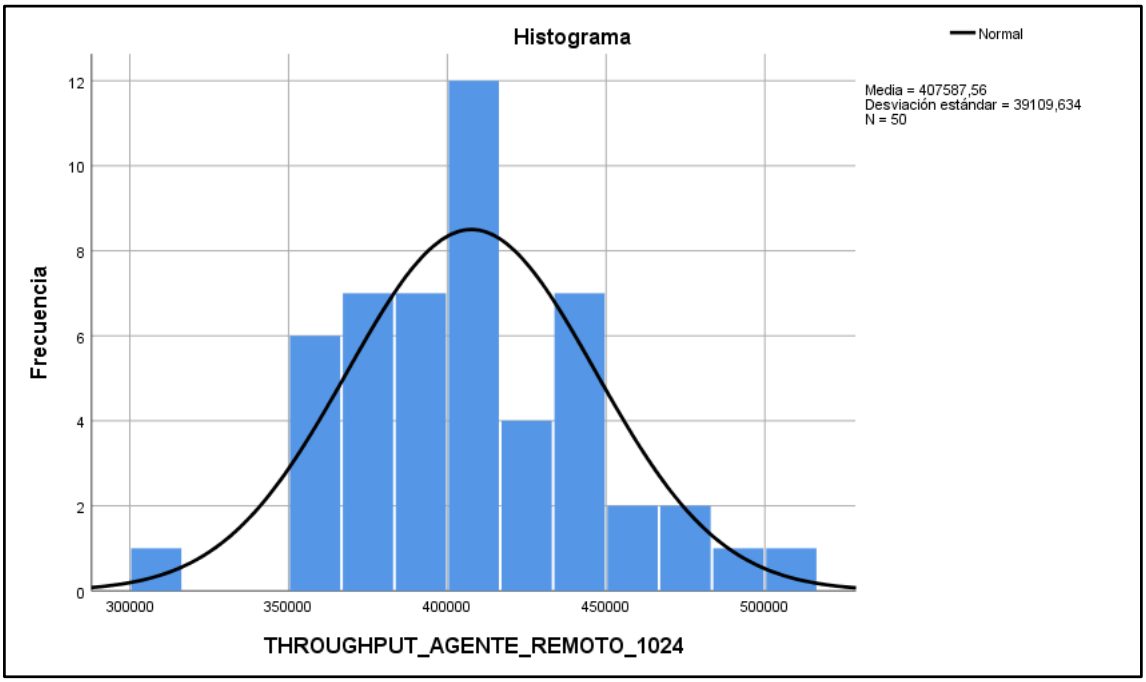

Figura 10. Histograma de Medición de Throughput Agente Remoto 1024 Bytes

En la figura N.º 10, del histograma de medición de Throughput Agente Remoto 1024 bytes logramos obtener un promedio de 407587.56 bytes, con una desviación estándar de 39109.634 bytes, de un total de 50 muestras.

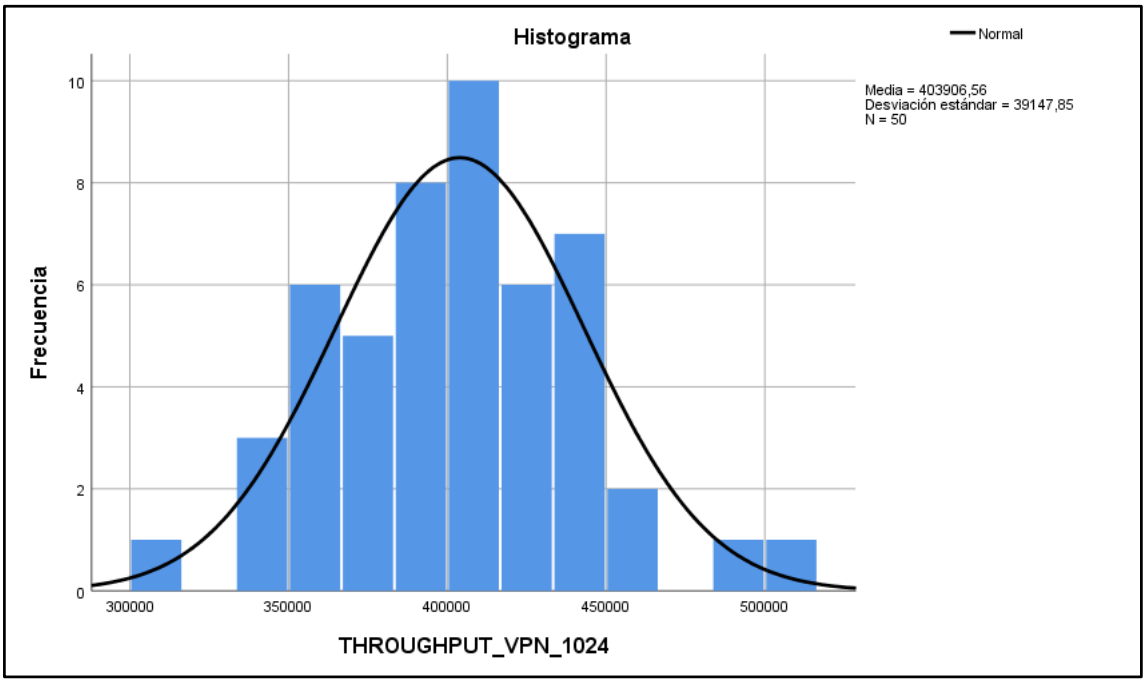

Figura 11. Histograma de Medición de Throughput VPN 1024 Bytes

En la figura N.º 11, del histograma de medición de Throughput VPN 1024 bytes logramos obtener un promedio de 403906.56 bytes, con una desviación estándar de 39147.85 bytes, de un total de 50 muestras.

Tabla Nª 8 : *Indicador Descriptivo de Throughput 1280 Bytes*

Descriptivos				
			Estadístico	**Error estándar**
THROUGHPUT AGENTE REMOTO 1280	Media		128354,60	4602,664
	95% de intervalo de confianza para la media	Límite inferior	119105,20	
		Límite superior	137604,00	
	Media recortada al 5%		128231,23	
	Mediana		131742,00	
	Varianza		1059225730,980	
	Desviación estándar		32545,748	
	Mínimo		44649	
	Máximo		216265	
	Rango		171616	
	Rango intercuartil		31448	
	Asimetría		-,108	,337
	Curtosis		1,446	,662
THROUGHPUT VPN 1280	Media		120473,60	3971,435
	95% de intervalo de confianza para la media	Límite inferior	112492,70	
		Límite superior	128454,50	
	Media recortada al 5%		121472,00	
	Mediana		127360,00	
	Varianza		788614750,041	
	Desviación estándar		28082,285	
	Mínimo		40960	
	Máximo		179200	
	Rango		138240	
	Rango intercuartil		31360	
	Asimetría		-,781	,337
	Curtosis		1,115	,662

En la tabla N.º 8, se puede apreciar los resultados de la aplicación de prueba descriptiva, el Throughput Agente Remoto 1280 bytes tiene como media de 128354.60 bytes en 50 muestras realizadas, el Throughput VPN 1280 bytes tiene como media 120473.60 bytes.

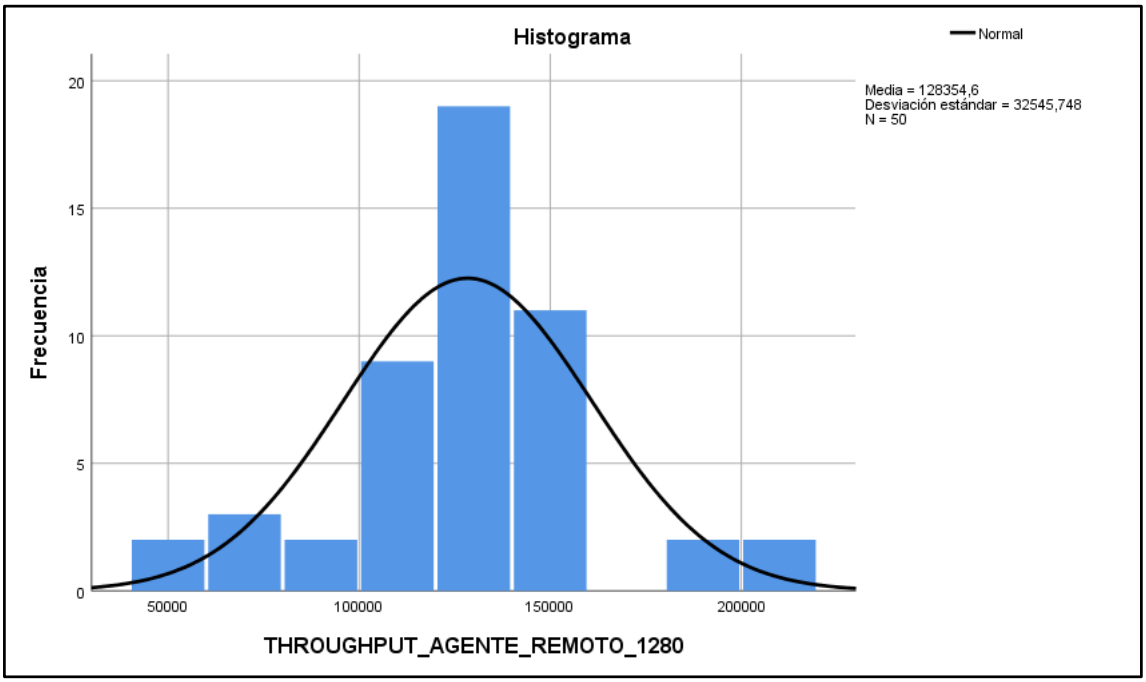

Figura 12. Histograma de Medición de Throughput Agente Remoto 1280 Bytes

En la figura N.º 12, del histograma de medición de Throughput Agente Remoto 1280 bytes logramos obtener un promedio de 128354.6 bytes, con una desviación estándar de 32545.748 bytes, de un total de 50 muestras.

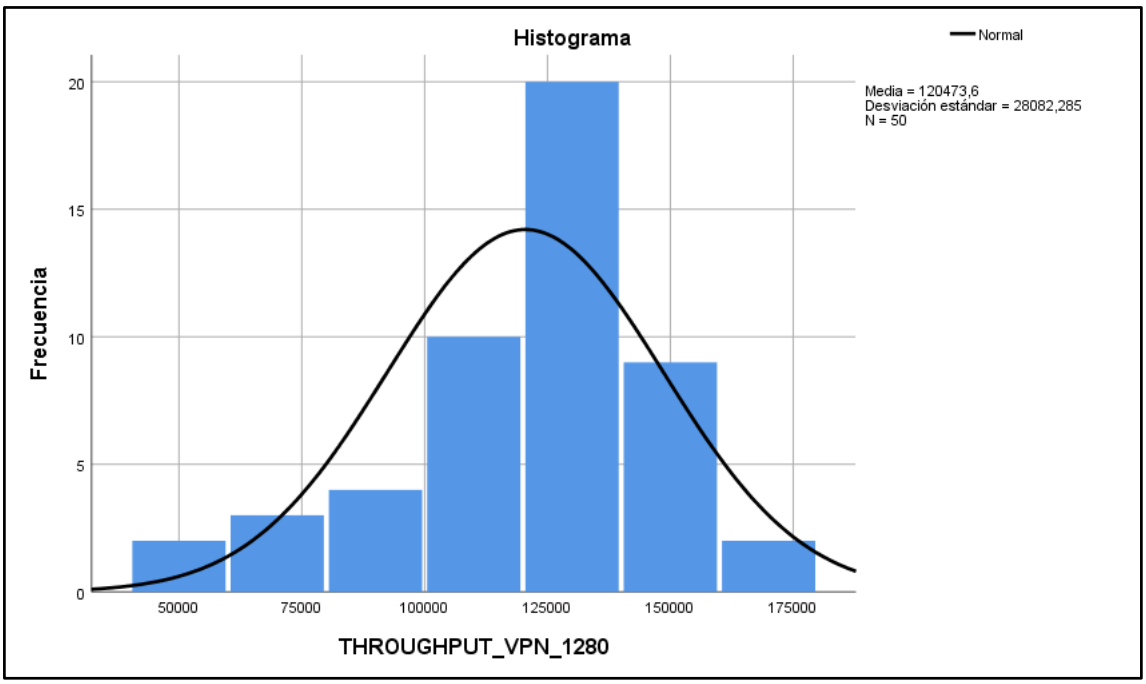

Figura 13. Histograma de Medición de Throughput VPN 1280 Bytes

En la Figura N.º 13, del histograma de medición de Throughput VPN 1280 bytes logramos obtener un promedio de 120473.6 bytes, con una desviación estándar de 28082.285 bytes, de un total de 50 muestras.

Tabla Nª 9 : *Indicador Descriptivo de Throughput 1518 Bytes*

Descriptivos				
			Estadístico	**Error estándar**
THROUGHPUT AGENTE REMOTO 1518 Bytes	Media		676968,54	8527,295
	95% de intervalo de confianza para la media	Límite inferior	659832,30	
		Límite superior	694104,78	
	Media recortada al 5%		675300,58	
	Mediana		677750,00	
	Varianza		3635737818,213	
	Desviación estándar		60297,080	
	Mínimo		550149	
	Máximo		879375	
	Rango		329226	
	Rango intercuartil		83627	
	Asimetría		,604	,337
	Curtosis		1,280	,662
THROUGHPUT VPN 1518 Bytes	Media		673293,72	8528,328
	95% de intervalo de confianza para la media	Límite inferior	656155,40	
		Límite superior	690432,04	
	Media recortada al 5%		671613,80	
	Mediana		673992,00	
	Varianza		3636619239,512	
	Desviación estándar		60304,388	
	Mínimo		546480	
	Máximo		875886	
	Rango		329406	
	Rango intercuartil		83870	
	Asimetría		,607	,337
	Curtosis		1,289	,662

En la tabla Nª 9, se puede apreciar los resultados de la aplicación de prueba descriptiva, el Throughput Agente Remoto 1518 bytes tiene como media de 676968.54 bytes en 50 muestras realizadas, el Throughput VPN 1518 bytes tiene como media 673293.72 bytes.

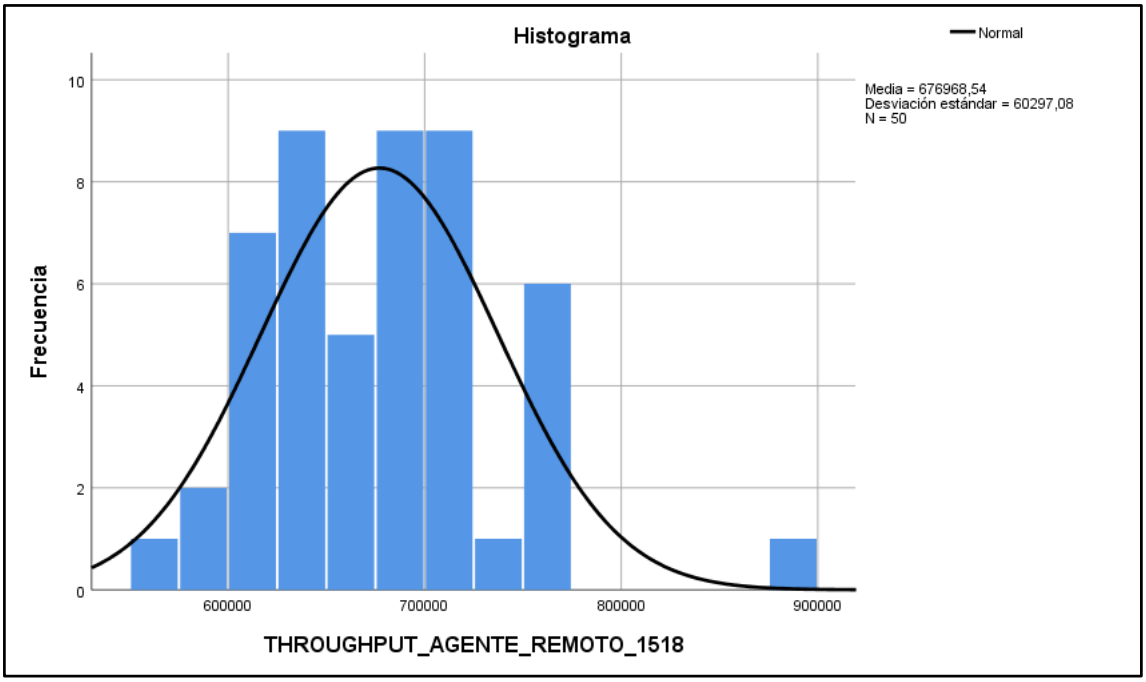

Figura 14. Histograma de Medición de Throughput Agente Remoto 1518 Bytes

En la figura N.º 14, del histograma de medición de Throughput Agente Remoto 1518 bytes logramos obtener un promedio de 676968.54 bytes, con una desviación estándar de 60297.08 bytes, de un total de 50 muestras.

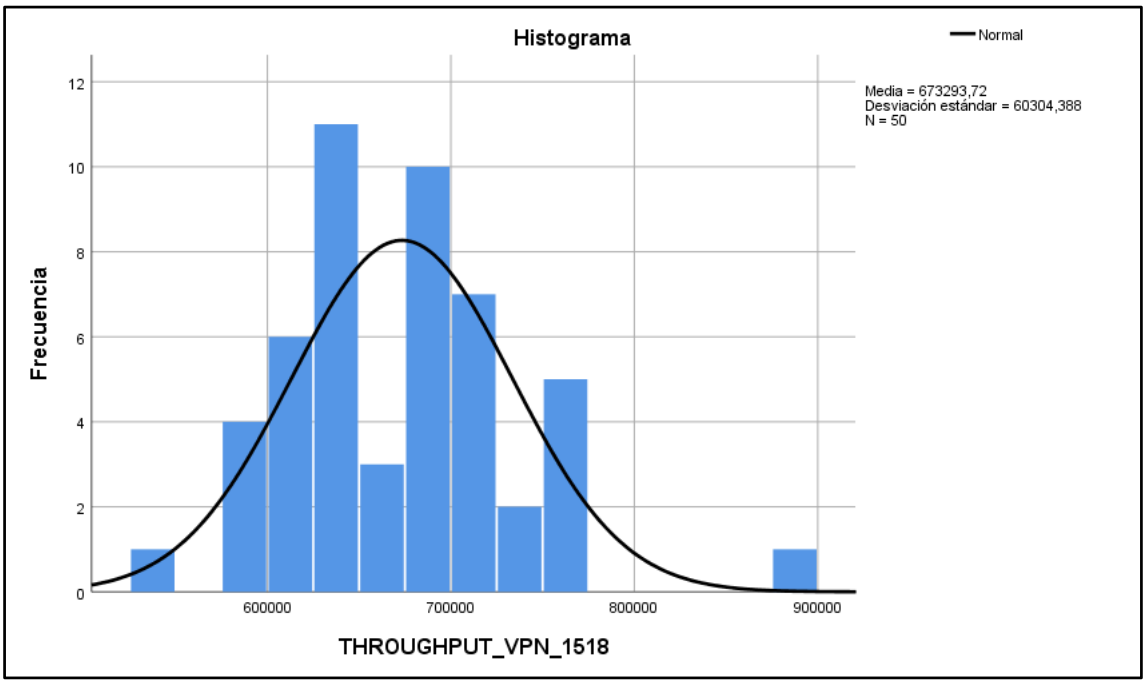

Figura 15. Histograma de Medición de Throughput VPN 1518 Bytes

En la figura N.º 15, del histograma de medición de Throughput VPN 1518 bytes logramos obtener un promedio de 673293.72 bytes, con una desviación estándar de 60304.388 bytes, de un total de 50 muestras.

- **Prueba de Normalidad – Método Shapiro – Wilk**

Tabla Nª 10 : *Prueba de Normalidad de Medición Throughput 64 Bytes*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
THROUGHPUT AGENTE REMOTO 64	,078	50	,200*	,978	50	,457
THROUGHPUT VPN 64	,179	50	,000	,866	50	,000

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

En la tabla N.º 10 de acuerdo con los resultados de valores de significancia son correspondientes a 0.000 son menores p<0.05; no se ajusta a una distribución normal sin embargo existen paquetes mayores p>0.05 que se ajustan a una distribución normal, como tenemos diferencias en los valores de significancia se procederá a realizar la prueba de Wilcoxon.

Tabla Nª 11 : *Prueba de Normalidad de Medición Throughput 128 Bytes*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
THROUGHPUT AGENTE REMOTO 128	,152	50	,005	,876	50	,000
THROUGHPUT VPN 128	,142	50	,013	,875	50	,000

a. Corrección de significación de Lilliefors

En la tabla N.º 11 de acuerdo con los resultados de valores de significancia son correspondientes a 0.000 son menores p<0.05; no se ajusta a una distribución normal, se procederá a realizar la prueba Wilcoxon.

Tabla Nª 12 : *Prueba de Normalidad de Medición Throughput 256 Bytes*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
THROUGHPUT AGENTE REMOTO 256	,159	50	,003	,878	50	,000
THROUGHPUT VPN 256	,157	50	,004	,877	50	,000

a. Corrección de significación de Lilliefors

En la tabla N.º 12 de acuerdo con los resultados de valores de significancia son correspondientes a 0.000 son menores p<0.05; no se ajusta a una distribución normal, se procederá a realizar la prueba Wilcoxon.

Tabla Nª 13 : *Prueba de Normalidad de Medición Throughput 512 Bytes*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			**Shapiro-Wilk**		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
THROUGHPUT AGENTE REMOTO 512	,145	50	,010	,881	50	,000
THROUGHPUT VPN 512	,146	50	,010	,881	50	,000

a. Corrección de significación de Lilliefors

En la tabla N.º 13 de acuerdo con los resultados de valores de significancia son correspondientes a 0.000 son menores p<0.05; no se ajusta a una distribución normal, se procederá a realizar la prueba Wilcoxon.

Tabla Nª 14 : *Prueba de Normalidad de Medición Throughput 1024 Bytes*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			**Shapiro-Wilk**		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
THROUGHPUT AGENTE REMOTO 1024	,073	50	,200*	,986	50	,827
THROUGHPUT VPN 1024	,071	50	,200*	,986	50	,833

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

En la tabla N.º 14 de acuerdo con los resultados de valores de significancia son mayores p>0.05 que se ajustan a una distribución normal, pero para mayor veracidad en los valores de significancia se procederá a realizar la prueba de Wilcoxon.

Tabla Nª 15 : *Prueba de Normalidad de Medición Throughput 1280 Bytes*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
THROUGHPUT AGENTE REMOTO 1280	,138	50	,018	,945	50	,021
THROUGHPUT VPN 1280	,118	50	,080	,939	50	,012

a. Corrección de significación de Lilliefors

En la tabla N.º 15 de acuerdo con los resultados de valores de significancia son correspondientes a 0.000 son menores p<0.05; no se ajusta a una distribución normal, se procederá a realizar la prueba Wilcoxon.

Tabla Nª 16 : *Prueba de Normalidad de Medición Throughput 1518 Bytes*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
THROUGHPUT AGENTE REMOTO 1518	,093	50	,200 *	,970	50	,226
THROUGHPUT VPN 1518	,092	50	,200 *	,970	50	,226

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

En la tabla N.º 16 de acuerdo con los resultados de valores de significancia son mayores p>0.05 que se ajustan a una distribución normal, pero para mayor veracidad en los valores de significancia se procederá a realizar la prueba de Wilcoxon.

- **Prueba de Wilcoxon**

Tabla Nª 17 : *Prueba de rangos con signos - Medición Throughput 64 Bytes*

Rangos				
		N	Rango promedio	Suma de rangos
THROUGHPUT VPN 64	Rangos negativos	43[a]	27,42	1179,00
THROUGHPUT AGENTE	Rangos positivos	7[b]	13,71	96,00
REMOTO 64	Empates	0[c]		
	Total	50		

a. THROUGHPUT_VPN_64 < THROUGHPUT_AGENTE_REMOTO_64

b. THROUGHPUT_VPN_64 > THROUGHPUT_AGENTE_REMOTO_64

c. THROUGHPUT_VPN_64 = THROUGHPUT_AGENTE_REMOTO_64

Tabla Nª 18 : *Estadísticos de prueba[a] Z - Medición Throughput 64 Bytes*

Estadísticos de prueba[a]	
	THROUGHPUT VPN 64 – THROUGHPUT AGENTE REMOTO 64
Z	-5,227[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Tabla Nª 19 : *Prueba de rangos con signos - Medición Throughput 128 Bytes*

Rangos				
		N	Rango promedio	Suma de rangos
THROUGHPUT VPN 128	Rangos negativos	50[a]	25,50	1275,00
THROUGHPUT AGENTE	Rangos positivos	0[b]	,00	,00
REMOTO 128	Empates	0[c]		
	Total	50		

a. THROUGHPUT_VPN_128 < THROUGHPUT_AGENTE_REMOTO_128

b. THROUGHPUT_VPN_128 > THROUGHPUT_AGENTE_REMOTO_128

c. THROUGHPUT_VPN_128 = THROUGHPUT_AGENTE_REMOTO_128

Tabla Nª 20 : *Estadísticos de prueba[a] Z - Medición Throughput 128 Bytes*

Estadísticos de prueba[a]	
	THROUGHPUT VPN 128 – THROUGHPUT AGENTE REMOTO 128
Z	-6,156[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Tabla Nª 21 : *Prueba de rangos con signos - Medición Throughput 256 Bytes*

Rangos				
		N	Rango promedio	Suma de rangos
THROUGHPUT VPN 256 – THROUGHPUT AGENTE REMOTO 256	Rangos negativos	50[a]	25,50	1275,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	50		

a. THROUGHPUT_VPN_256 < THROUGHPUT_AGENTE_REMOTO_256

b. THROUGHPUT_VPN_256 > THROUGHPUT_AGENTE_REMOTO_256

c. THROUGHPUT_VPN_256 = THROUGHPUT_AGENTE_REMOTO_256

Tabla Nª 22 : *Estadísticos de prueba[a] Z - Medición Throughput 256 Bytes*

Estadísticos de prueba[a]	
	THROUGHPUT VPN 256 – THROUGHPUT AGENTE REMOTO 256
Z	-6,156[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Tabla Nª 23 : *Prueba de rangos con signos - Medición Throughput 512 Bytes*

Rangos				
		N	Rango promedio	Suma de rangos
THROUGHPUT VPN 512 – THROUGHPUT AGENTE REMOTO 512	Rangos negativos	50[a]	25,50	1275,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	50		

a. THROUGHPUT_VPN_512 < THROUGHPUT_AGENTE_REMOTO_512

b. THROUGHPUT_VPN_512 > THROUGHPUT_AGENTE_REMOTO_512

c. THROUGHPUT_VPN_512 = THROUGHPUT_AGENTE_REMOTO_512

Tabla Nª 24 : *Estadísticos de prueba[a] Z - Medición Throughput 512 Bytes*

Estadísticos de prueba[a]	
	THROUGHPUT VPN 512 – THROUGHPUT AGENTE REMOTO 512
Z	-6,156[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Tabla Nª 25 : *Prueba de rangos con signos - Medición Throughput 1024 Bytes*

Rangos				
		N	Rango promedio	Suma de rangos
THROUGHPUT VPN 1024 – THROUGHPUT AGENTE REMOTO 1024	Rangos negativos	50[a]	25,50	1275,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	50		

a. THROUGHPUT_VPN_1024 < THROUGHPUT_AGENTE_REMOTO_1024

b. THROUGHPUT_VPN_1024 > THROUGHPUT_AGENTE_REMOTO_1024

c. THROUGHPUT_VPN_1024 = THROUGHPUT_AGENTE_REMOTO_1024

Tabla Nª 26 : *Estadísticos de prueba[a] Z - Medición Throughput 1024 Bytes*

Estadísticos de prueba[a]	
	THROUGHPUT VPN 1024 – THROUGHPUT AGENTE REMOTO 1024
Z	-6,156[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Tabla Nª 27 : *Prueba de rangos con signos - Medición Throughput 1280 Bytes*

Rangos				
		N	**Rango promedio**	**Suma de rangos**
THROUGHPUT VPN 1280 – THROUGHPUT AGENTE REMOTO 1280	Rangos negativos	50[a]	25,50	1275,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	50		

a. THROUGHPUT_VPN_1280 < THROUGHPUT_AGENTE_REMOTO_1280

b. THROUGHPUT_VPN_1280 > THROUGHPUT_AGENTE_REMOTO_1280

c. THROUGHPUT_VPN_1280 = THROUGHPUT_AGENTE_REMOTO_1280

Tabla Nª 28 : *Estadísticos de prueba[a] Z - Medición Throughput 1280 Bytes*

Estadísticos de prueba[a]	
	THROUGHPUT VPN 1280 – THROUGHPUT AGENTE REMOTO 1280
Z	-6,156[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Tabla Nª 29 : *Prueba de rangos con signos - Medición Throughput 1518 Bytes*

Rangos				
		N	**Rango promedio**	**Suma de rangos**
THROUGHPUT VPN 1518 – THROUGHPUT AGENTE REMOTO 1518	Rangos negativos	50[a]	25,50	1275,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	50		

a. THROUGHPUT_VPN_1518 < THROUGHPUT_AGENTE_REMOTO_1518

b. THROUGHPUT_VPN_1518 > THROUGHPUT_AGENTE_REMOTO_1518

c. THROUGHPUT_VPN_1518 = THROUGHPUT_AGENTE_REMOTO_1518

Tabla Nª 30 : *Estadísticos de prueba[a] Z - Medición Throughput 1518 Bytes*

Estadísticos de prueba[a]	
	THROUGHPUT VPN 1518 – THROUGHPUT AGENTE REMOTO 1518
Z	-6,156[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Tabla Nª 31 : *Prueba de Wilcoxon - Medición Throughput*

Estadísticos de prueba [a]							
	THROUGHPUT VPN 64 – THROUGHPUT AGENTE REMOTO 64	THROUGHPUT VPN 128 – THROUGHPUT AGENTE REMOTO 128	THROUGHPUT VPN 256 – THROUGHPUT AGENTE REMOTO 256	THROUGHPUT VPN 512 – THROUGHPUT AGENTE REMOTO 512	THROUGHPUT VPN 1024 – THROUGHPUT AGENTE REMOTO 1024	THROUGHPUT VPN 1280 – THROUGHPUT AGENTE REMOTO 1280	THROUGHPUT VPN 1518 – THROUGHPUT AGENTE REMOTO 1518
Z	-5,227[b]	-6,156[b]	-6,156[b]	-6,156[b]	-6,156[b]	-6,156[b]	-6,156[b]
Sig. asintótica(bilateral)	,000	,000	,000	,000	,000	,000	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

De acuerdo con los resultados de valores de significancia asintótica (Bilateral) son correspondientes a 0.000 son menores a p=0.05; por lo cual se rechaza la $HE1_0$, y se acepta $HE1_A$ que fue la Implementación de redes VPN MIKROTIK incrementó el desempeño en la red de los servidores entre ciudades de Lima y Pisco.

Prueba de Hipótesis Especifica 2 del Indicador Consumo de Memoria RAN

Planteamiento de la hipótesis especifica

- $HE2_0$: La Implementación de redes VPN MIKROTIK no mejoró el consumo de recursos de los servidores entre ciudades de Lima y Pisco.
- $HE2_A$: La Implementación de redes VPN MIKROTIK mejoró el consumo de recursos de los servidores entre ciudades de Lima y Pisco.

Tabla Nª 32 : *Indicador Descriptivo de Consumo de Memoria RAM*

Descriptivos				
			Estadístico	**Error estándar**
CONSUMO DE MEMORIA RAM AGENTE REMOTO	Media		38170,84	147,256
	95% de intervalo de confianza para la media	Límite inferior	37874,92	
		Límite superior	38466,76	
	Media recortada al 5%		38203,42	
	Mediana		38250,00	
	Varianza		1084209,566	
	Desviación estándar		1041,254	
	Mínimo		36120	
	Máximo		39592	
	Rango		3472	
	Rango intercuartil		1864	
	Asimetría		-,372	,337
	Curtosis		-1,035	,662
CONSUMO DE MEMORIA RAM VPN	Media		30411,76	194,865
	95% de intervalo de confianza para la media	Límite inferior	30020,16	
		Límite superior	30803,36	
	Media recortada al 5%		30407,56	
	Mediana		30396,00	
	Varianza		1898616,921	
	Desviación estándar		1377,903	
	Mínimo		28412	
	Máximo		32312	
	Rango		3900	
	Rango intercuartil		2576	
	Asimetría		,036	,337
	Curtosis		-1,839	,662

En la tabla N.º 32, se puede apreciar los resultados de la aplicación de prueba descriptiva, el consumo de memoria RAM Agente Remoto tiene como media de 38170.84 Mb en 50 muestras realizadas, el consumo de memoria RAM VPN tiene como media 30411.76 Mb.

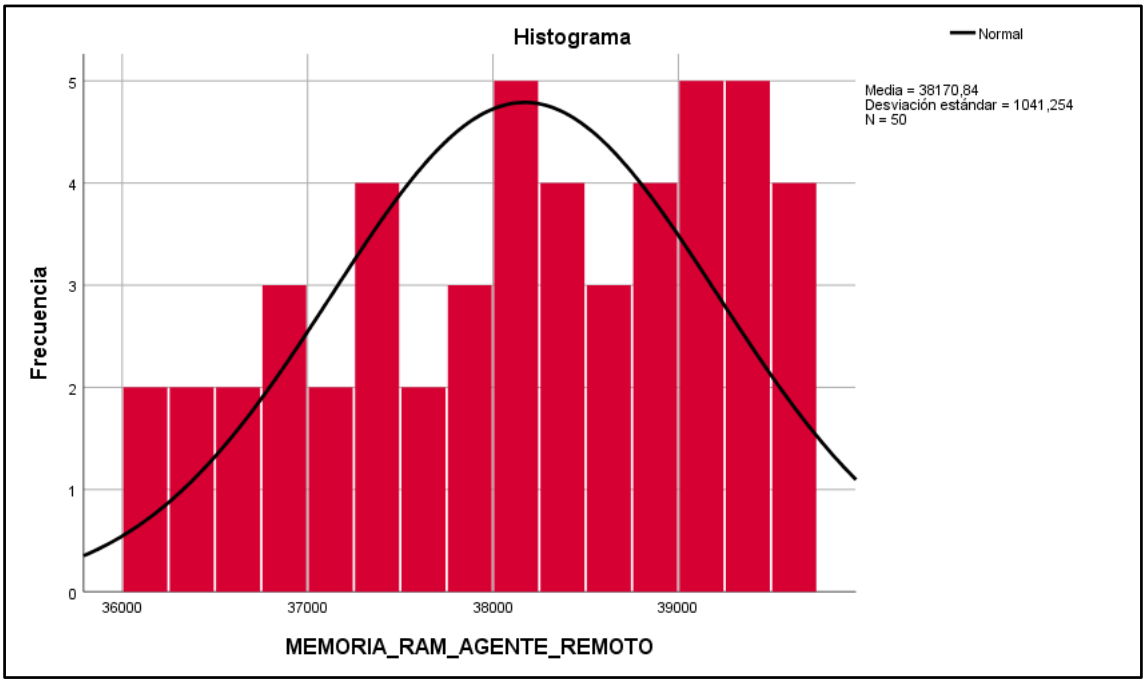

Figura 16. Histograma de Medición de Consumo del Memoria RAM Agente Remoto

En la figura Nª 16, del histograma de medición de consumo de memoria RAM agente remoto logramos obtener un promedio de 38170.84 Mb, con una desviación estándar de 1041.254 Mb, de un total de 50 muestras.

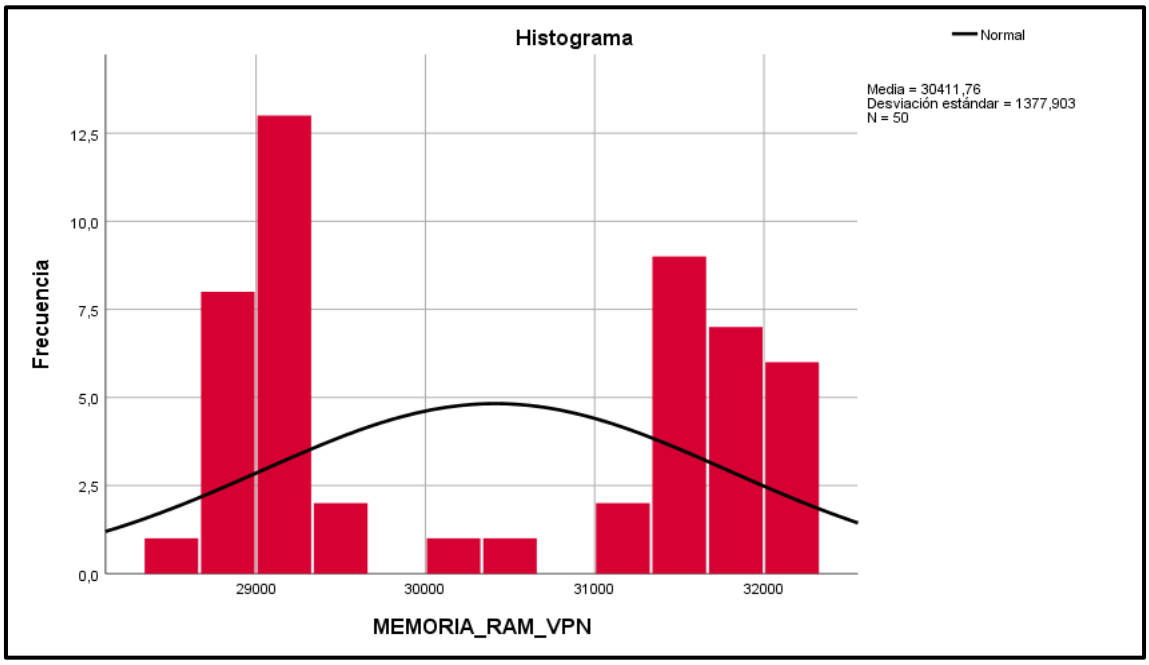

Figura 17. Histograma de Medición del Consumo de Memoria RAM VPN

En la figura Nª 17, del histograma de medición de consumo de memoria RAM VPN logramos obtener un promedio de 30411.76 Mb, con una desviación estándar de 1377.903 Mb, de un total de 50 muestras.

- **Prueba de Normalidad – Método Shapiro – Wilk**

Tabla Nª 33 : *Prueba de Normalidad de Consumo de Memoria RAM*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
MEMORIA RAM AGENTE REMOTO	,101	50	,200*	,938	50	,011
MEMORIA RAM VPN	,259	50	,000	,824	50	,000

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

En la tabla N.º 33 de acuerdo con los resultados de valores de significancia son correspondientes a 0.000 son menores p<0.05; no se ajusta a una distribución normal, se procederá a realizar la prueba Wilcoxon.

- **Prueba de Wilcoxon**

Tabla Nª 34 : *Prueba de rangos con signos – Consumo de Memoria RAM*

Rangos				
		N	Rango promedio	Suma de rangos
MEMORIA RAM AGENTE REMOTO – MEMORIA RAM VPN	Rangos negativos	0[a]	,00	,00
	Rangos positivos	50[b]	25,50	1275,00
	Empates	0[c]		
	Total	50		

a. MEMORIA_RAM_AGENTE_REMOTO < MEMORIA_RAM_VPN
b. MEMORIA_RAM_AGENTE_REMOTO > MEMORIA_RAM_VPN
c. MEMORIA_RAM_AGENTE_REMOTO = MEMORIA_RAM_VPN

Tabla Nª 35 : *Estadísticos de prueba[a] Z – Consumo de Memoria RAM*

Estadísticos de prueba[a]	
	MEMORIA RAM AGENTE REMOTO – MEMORIA RAM VPN
Z	-6,154[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos negativos.

De acuerdo con los resultados de valores de significancia asintótica (Bilateral) son correspondientes a 0.000 son menores a $p = 0.05$; por lo cual se rechaza la $HE2_0$, y se acepta $HE2_A$ que fue la Implementación de redes VPN MIKROTIK mejoró el consumo de recursos de los servidores entre ciudades de Lima y Pisco, porque tenemos una reducción de consumo de memoria RAM.

Prueba de Hipótesis especifica 3 del Indicador: Tiempo de respuesta de Red Lan

Planteamiento de la hipótesis especifica

- $HE3_0$**:** La Implementación de redes VPN MIKROTIK no mejoró la conectividad en la red de los servidores entre ciudades de Lima y Pisco.
- $HE3_A$**:** La Implementación de redes VPN MIKROTIK mejoró la conectividad en la red de los servidores entre ciudades de Lima y Pisco.

Tabla Nª 36 : *Indicador Descriptivo de Tiempo de Respuesta de Red LAN*

Descriptivos				
			Estadístico	**Error estándar**
TIEMPO DE RESPUESTA DE LA RED LAN AGENTE REMOTO	Media		201,897764	2,5444801
	95% de intervalo de confianza para la media	Límite inferior	196,784440	
		Límite superior	207,011088	
	Media recortada al 5%		199,463846	
	Mediana		198,049150	
	Varianza		323,719	
	Desviación estándar		17,9921914	
	Mínimo		184,3581	
	Máximo		295,8862	
	Rango		111,5281	
	Rango intercuartil		13,2758	
	Asimetría		3,364	,337
	Curtosis		15,236	,662
TIEMPO DE RESPUESTA DE LA RED LAN VPN	Media		137,549682	1,3774800
	95% de intervalo de confianza para la media	Límite inferior	134,781532	
		Límite superior	140,317832	
	Media recortada al 5%		136,330728	
	Mediana		133,699100	
	Varianza		94,873	
	Desviación estándar		9,7402544	
	Mínimo		129,4346	
	Máximo		170,5666	
	Rango		41,1320	
	Rango intercuartil		7,7225	
	Asimetría		1,917	,337
	Curtosis		3,340	,662

En la tabla N.º 36, se puede apreciar los resultados de la aplicación de prueba descriptiva, el tiempo de respuesta de la red LAN Agente Remoto tiene como media de 201,8977 seg en 50 muestras realizadas, el tiempo de respuesta de la red LAN VPN tiene como media 137,5496 Seg

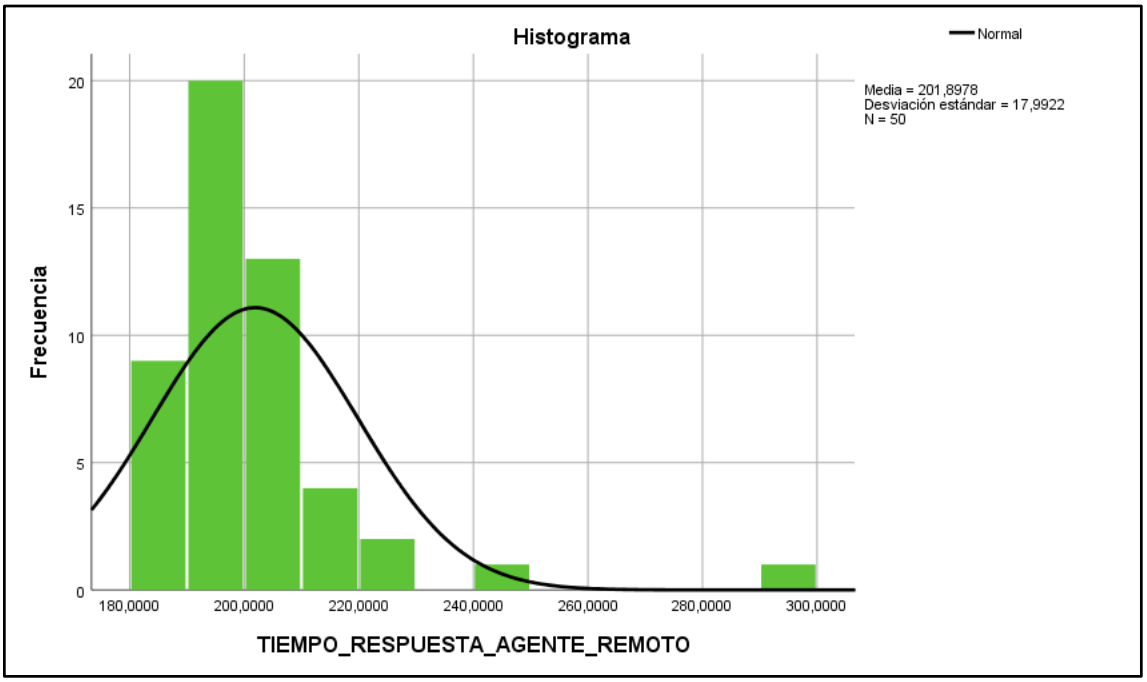

Figura 18. Histograma de Medición de Tiempo de Respuesta Red LAN Agente Remoto

En la figura N.º 18 del histograma de medición de tiempo de respuesta de la red LAN agente remoto logramos obtener un promedio de 201.8978 seg, con una desviación estándar de 17.9922 seg, de un total de 50 muestras.

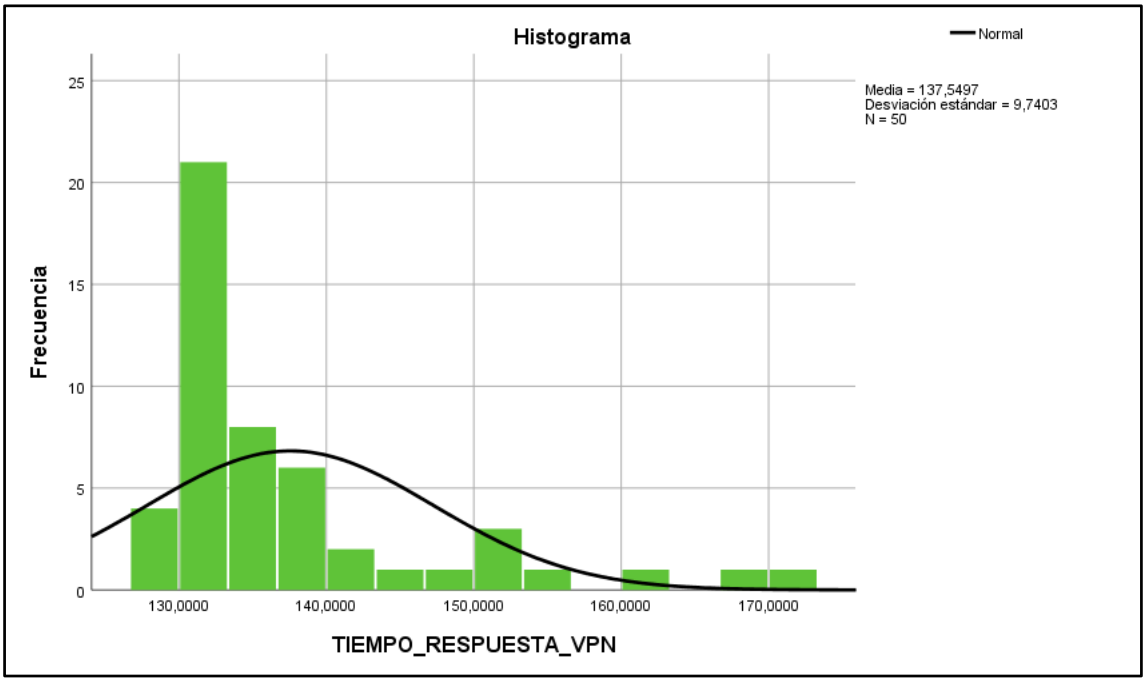

Figura 19. Histograma de Medición de Tiempo de Respuesta Red LAN VPN

En la figura N.º 19 del histograma de medición de tiempo de respuesta de la red LAN VPN logramos obtener un promedio de 137.5497 seg, con una desviación estándar de 9.7403 seg, de un total de 50 muestras.

- **Prueba de Normalidad – Método Shapiro – Wilk**

Tabla Nª 37 : *Prueba de Normalidad de Tiempo de respuesta de la red LAN*

Pruebas de normalidad						
	Kolmogórov-Smirnov [a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
TIEMPO RESPUESTA AGENTE REMOTO	,359	50	,000	,543	50	,000
TIEMPO RESPUESTA VPN	,221	50	,000	,748	50	,000

a. Corrección de significación de Lilliefors

En la tabla N.º 37 de acuerdo con los resultados de valores de significancia son correspondientes a 0.000 son menores p<0.05; no se ajusta a una distribución normal, se procederá a realizar la prueba Wilcoxon.

- **Prueba de Wilcoxon**

Tabla Nª 38 : *Prueba de rangos con signos – Tiempo de respuesta de red LAN*

Rangos				
		N	Rango promedio	Suma de rangos
TIEMPO RESPUESTA AGENTE_REMOTO – TIEMPO RESPUESTA VPN	Rangos negativos	0[a]	,00	,00
	Rangos positivos	50[b]	25,50	1275,00
	Empates	0[c]		
	Total	50		

a. TIEMPO_RESPUESTA_AGENTE_REMOTO < TIEMPO_RESPUESTA_VPN

b. TIEMPO_RESPUESTA_AGENTE_REMOTO > TIEMPO_RESPUESTA_VPN

c. TIEMPO_RESPUESTA_AGENTE_REMOTO = TIEMPO_RESPUESTA_VPN

Tabla Nª 39 : *Estadísticos de prueba[a] Z – Tiempo de respuesta de la red LAN*

Estadísticos de prueba[a]	
	TIEMPO RESPUESTA AGENTE REMOTO – TIEMPO RESPUESTA VPN
Z	-6,154[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

De acuerdo con los resultados de valores de significancia asintótica (Bilateral) son correspondientes a 0.000 son menores a $P = 0.05$; por lo cual se rechaza la $HE3_0$, y se acepta $HE3_A$ que fue la Implementación de redes VPN MIKROTIK mejoró la conectividad en la red de los servidores entre ciudades de Lima y Pisco, porque tenemos una reducción de tiempo de respuesta de la red LAN.

RESUMEN DE HIPÓTESIS GENERAL

Abre.	Hipótesis	Resultado (Aceptada / Rechazado
HE1	La Implementación de redes VPN MIKROTIK incrementó el desempeño en la red de los servidores entre ciudades de Lima y Pisco	Aceptada
HE2	La Implementación de redes VPN MIKROTIK mejoró el consumo de recursos de los servidores entre ciudades de Lima y Pisco	Aceptada
HE3	La Implementación de redes VPN MIKROTIK mejoró la conectividad en la red de los servidores entre ciudades de Lima y Pisco	Aceptada
HG	La Implementación de redes VPN MIKROTIK incrementó el desempeño de la red, mejoro el consumo de recursos y la conectividad en la red de los servidores entre ciudades de Lima y Pisco.	Aceptada

V. DISCUSIÓN

Con los resultados obtenidos en la herramienta de SSPS en esta investigación referida a la que hace mención Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco, por medio de las pruebas de normalidad del método de Shapiro Wilk, prueba de frecuencias y prueba de Poisson, se logró evaluar de manera satisfactoria la variable servidores con sus dimensiones e indicadores para determinar el proceso de la Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco.

De acuerdo a los resultados de la hipótesis especifica 1; en referencia a la dimensión del desempeño de la red mediante el indicador de medición del Throughput, se obtuvo buenos resultados en las medias de los paquetes (64 bytes, 128 Bytes, 256Bytes, 512 Bytes, 1024Bytes, 1280Bytes y 1518Bytes) con los resultados de valores de significancia asintótica (Bilateral) correspondientes a 0.000 son menores a p=0.05; por lo cual se rechaza la $HE1_0$, y se acepta $HE1_A$ con éxito en la entrega de tramas por la VPN usando el equipos MIKTROTIK, en comparación con el estudio de Pacotaype (2018, p. 35) que también obtuvo un rendimiento optimo en el Throughput en las tramas (64 KB, 128 KB, 256 KB, 512 KB, 1024 KB, 1280 KB y 1518 KB) pero fue menor en las tramas de 64 KB, 256 KB y 512 KB respectivamente.

Según los resultados de la hipótesis especifica 2; en referencia a la dimensión del consumo de recursos mediante el indicador de consumo de memoria RAM, los resultados de este estudio fueron semejantes a los resultados de la investigación de Julca y Tapia (2020, p. 66), quienes mencionaron que el consumo promedio de memoria RAM fue de 15419.49 Bytes que fue menor en comparación a nuestra investigación que fue de 30411.76 Bytes como consumo de la memoria RAM. Cabe resaltar que en esta investigación se utilizó un total de Memoria RAM de 256 MB a comparación de 128 MB de la investigación mencionada.

Asimismo, los resultados de la hipótesis especifican 3; en referencia a la dimensión de la conectividad en la red, el indicador de tiempo de respuesta de la red LAN, obtuvimos un promedio de 137,5496 segundos lo que fue mayor con respeto al estudio de Dávila (2019, p. 74) quien obtuvo un incremento de tiempo

de respuesta nivel LAN de la Red que mejoró de 78 milisegundos de la red actual a 17 milisegundos con el Modelo de gestión de servicios de red con RouterOS Mikrotik.

VI. CONCLUSIONES

El desarrollo de la presente implementación de redes VPN MIKROTIK para servidores, nos muestra las siguientes conclusiones:

- En base a los resultados obtenidos, al implementar las redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco, fue favorable en el incremento del desempeño de la red, mejorando el envió de paquetes de Throughput.
- El consumo de recursos con la implementación de redes VPN MIKROTIK fue favorable en reducir el consumo de memoria RAM cuando se ejecuta procesos a diferencia en el uso con agentes remotos que ocasionan mayor consumo de memoria RAM.
- Se logro mejorar la conectividad de la red reduciendo el tiempo de respuesta de la red LAN al implementar las redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco.
- En base al análisis teórico, de otros trabajos relacionados al uso de los equipos Mikrotik en diversas implementaciones de una red, ofrece la mejora del desempeño para el intercambio de todo tipo de tráfico con la debida configuración.
- En el dimensionamiento y diseño, extensión de la red se consideró el uso correcto de los valores l2tp, y el envío y recepción de paquetes, por tal motivo se realiza el cálculo para obtener el valor correcto que permita tener una idea clara de la performance que esta configuración nos puede brindar, determinando que el consumo de recursos usando los equipos elegidos es aceptable.
- Los pasos y procedimientos que estamos presentado, para la presente implementación, busca brindar de manera sencilla y muy concreta los aspectos más relevantes de esta configuración e indica lo que fue desarrollado realmente en la práctica y producción.

Se concluye que la presente implementación, asegura conectividad segura en toda la extensión de la red LAN sobre redes WAN.

VII. RECOMENDACIONES

Realizado el presente trabajo, se puede realizar algunas recomendaciones:

Considerar el uso y aplicación de la misma implementación teniendo como base direcciones con el protocolo IPv6 y evaluar su desarrollo y desempeño, sabiendo que en teoría evitará retardos a causa de la traducción normal en el direccionamiento de redes privadas a públicas que si sucede al usar IPv4.

Para un posterior diseño se puede recomendar dimensionar en paralelo otros direccionamientos, ancho de banda dedicado y probar con equipos Mikrotik más básicos, esto en consideración de soluciones más económicas, pero por el buen ancho de banda ayuden a evitar lentitud que puedan ocasionar con equipos que en la teoría no pueden soporten dichos los procesos implementados.

En la implementación se debe tratar de mantener el uso de equipos de características semejantes para cada prueba, tanto en hardware como firmware, así como iguales protocolos propietarios del enrutamiento que se estén trabajando. Todo esto para evitar que por una diferente configuración parezca que cada equipo arroja diferente resultado.

Lo ideal y recomendable en este tipo de implementaciones, que se realizar con direccionamiento público estático para poder disminuir los procesos del equipo Mikrotik y acelerar los tiempos en el despliegue de las rutas; asimismo, esto permitirá al especialista o administrador encargado de la red un mejor y mayor control ante casuísticas normales o pruebas que desee realizar.

REFERENCIAS

ABELEIRA ORTIZ, J.L., VÁSQUEZ VARGAS, N. y PEÑA DUARTE, C.R., 2016. Metodología para favorecer el desempeño investigativo experimental mediante el análisis de videos con tracker. *Revista Boletín Redipe*, vol. 5, no. 6, pp. 133-138.

AGUIRRE CORONEL, V.H., 2016. *Cloud computing de modo privado para ofrecer infraestructura como servicio bajo software libre a los estudiantes de la facultad de ingenieria en ciencias aplicadas de la universidad técnica del norte* [en línea]. S.l.: s.n. Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/5345/1/04 RED 112 TESIS DE GRADO.pdf.

ALVAREZ ROA, N.J., 2010. *Análisis de rendimiento y calidad de servicio (QoS) en tres arquitecturas de seguridad basadas en firewall*. S.l.: s.n.

ARIAS GÓMEZ, J., VILLASÍS KEEVER, M.Á. y MIRANDA NOVALES, M.G., 2016. The research protocol III. Study population. *Revista Alergia Mexico*, vol. 63, no. 2, pp. 201-206. ISSN 00025151. DOI 10.29262/ram.v63i2.181.

ARIAS HERRERA, D.I., MILIÁN NIEBLAS, I. y DOMINGUEZ HERNÁNDEZ, J.F., 2020. Procedimiento Para Diagnosticar La Gestión De Las Tecnologías De La Información En Empresas. *Tlatemoani*, vol. 11, no. 33, pp. 109-132. ISSN 1989-9300.

ARRIETA SUCUZHAÑAY, E.R. y GUALLPA CAGUANA, D.F., 2021. *Implementacion de seguridad, servicios y protocolos de redes en equipos Mikrotik* [en línea]. S.l.: s.n. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/21485/1/CD 10978.pdf.

BALLADARES FLORES, J.H., 2017. *Parámetros de calidad del servicio de acceso a internet en redes convergentes y construción de una sonda para la medición de parámetros de velocidad de descarga, velocidad de subida, tiempo de ping y latencia para usuarios finales del servicio de acceso a* [en línea]. S.l.: s.n. Disponible en: http://repositorio.puce.edu.ec/bitstream/handle/22000/13490/Tesis final Jorge Balladares.pdf?sequence=1&isAllowed=y.

BARGADOS, A., 2021. Impacto del Covid-19 en las Pymes argentinas: actividad, empleo y condiciones de trabajo. *Trabajo y sociedad*, vol. 21, no. 36, pp. 122-145. ISSN 1514-6871.

BORDA CRUZ, J.A., 2020. *Determinación De Los Riesgos Y Plan Estratégico*

De Seguridad De La Información Del Teletrabajo En Las Organizaciones [en línea]. S.l.: s.n. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/39396/jabordac.pdf?sequence=3&isAllowed=y.

CALLEGATI, F., CERRONI, W. y CONTOLI, C., 2016. Virtual Networking Performance in OpenStack Platform for Network Function Virtualization. *Journal of Electrical and Computer Engineering*, no. 1, pp. 1-15. ISSN 20900155. DOI 10.1155/2016/5249421.

CARRASCO GALLEGO, A., DONOSO ANES, J.A., DUARTE ATOCHE, T., HERNÁNDEZ BORREGUERO, J.J. y LÓPEZ GAVIRA, R., 2015. Diseño y validación de un cuestionario que mide la percepción de efectividad del uso de metodologías de participación activa (CEMPA). El caso del Aprendizaje Basado en Proyectos (ABPrj) en la docencia de la contabilidad. *Innovar*, vol. 25, no. 58, pp. 143-158. ISSN 0121-5051. DOI 10.15446/innovar.v25n58.52439.

CARROLL VARGAS, J., DIAZ GÓMEZ, L. y SANCHEZ GARZÓN, C.C., 2020. Metodología de Cloud Computin VPN con Graphical Network Simulator (GNS3). *Memorias*, DOI 10.22490/25904779.4210.

CASTRO CUBA SAYCO, D.H., 2019. *Diseño e implementación de la interconexión de sucursales de hp-store en las ciudades de arequipa y cusco mediante vpn con mikrotik router* [en línea]. S.l.: Arequipa. Disponible en: http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/8663/IEcsdh.pdf?sequence=1&isAllowed=y.

CHILCAÑÁN, D., NAVAS, P. y ESCOBAR, M.S., 2017. Sistema Experto para la Automatización de Procesos Expert System for Remote Process Automation in Conversation. *CISTI (Iberian Conference on Information Systems & Technologies)*, vol. 1, pp. 1-8.

COAN, L.A., 2020. Implementação do protocolo IPV6 com segurança: Uma análise sobre os desafios e riscos para os administradores de redes internet. *Revista Brasileira em Tecnologia da Informação*, vol. 2, no. 1, pp. 3-16.

CUEVA MENDOZA, A.Y., 2018. *Impacto De La Implementación De Una Red Privada Virtual En La Gestión De Información De La Empresa Deyfor*

E.I.R.L. [en línea]. S.l.: s.n. Disponible en: https://repositorio.unc.edu.pe/bitstream/handle/UNC/2574/Tesis - Impacto de la implemEntacion de una red privada virtual en la gestion de informacion de la empresa DEYFOR E.I.R.L..pdf?sequence=1&isAllowed=y.

DAVILA LLIMPE, Y.T., 2019. *Modelo de gestión de servicios de red con routeros mikrotik en la disponibilidad de información de la red de datos de la escuela profesional de ingeniería de sistemas de la universidad nacional de huancavelica* [en línea]. S.l.: s.n. Disponible en: http://repositorio.unh.edu.pe/bitstream/handle/UNH/2618/TESIS-2019-ING. DE SISTEMAS-DAVILA LLIMPE.pdf?sequence=1&isAllowed=y.

DE LA CRUZ BERNILLA, S.M. y VERA CRUZ, J.R.S., 2019. *Implementación de una VPN con open source para la gestión de la aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo* [en línea]. S.l.: s.n. Disponible en: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/8266/BC-4666 DE LA CRUZ BERNILLA-VERA CRUZ.pdf?sequence=1&isAllowed=y.

DOMÍNGUEZ CHÁVEZ, J., 2020. Entendiendo el teletrabajo. *Universidad Politécnica Territorial del Estado Aragua*, pp. 1-17.

EGAS, C., VIRACOCHA, D. y RIVERA, J., 2019. Implementación de una red inalámbrica de sensores para la gestión de luminarias utilizando IPv6. *Enfoque UTE* [en línea], vol. 10, no. 4, pp. 45-56. ISSN 1390-9363. Disponible en: http://scielo.senescyt.gob.ec/pdf/enfoqueute/v10n4/1390-6542-enfoqueute-10-04-00045.pdf.

HERNÁNDEZ SAMPIERI, R. y MENDOZA TORRES, C.P., 2018. *Metodología de la investigación* [en línea]. S.l.: s.n. ISBN 978-1-4562-6096-5. Disponible en: http://repositorio.uasb.edu.bo:8080/bitstream/54000/1292/1/Hernández-Metodología de la investigación.pdf.

HICKMAN, B., NEWMAN, D., TADJUDIN, S. y MARTIN, T., 2003. Benchmarking Methodology for Firewall Performanc. *The Internet Society*, pp. 1-34.

JARAMILLO ZAMORA, A.W., 2018. *Análisis comparativo entre vpn ipsec y*

dmvpn (dynamic multipoint virtual private network) para mejorar el desempeño de redes privadas sobre internet [en línea]. S.l.: s.n. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/9301/1/20T01119.pdf.

JOTA FONSECA, Y.M., RAMIREZ CASTAÑEDA, D.S. y PENAGOS AREVALO, A.R., 2018. *Diseño De Una Red Privada Virtual (Vpn) Con Seguridad L2Pt Para La Empresa Laboratorios Expofarma s.a.* [en línea]. S.l.: s.n. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/6193/1/2018_Ramirez%2CJota y Penagos_VPN_L2TP_Seguridad..pdf.

JULCA COSCOL, Á.B. y TAPIA PRADO, C.D., 2020. *Metodologia integral para evaluar el rendimiento de swithches*. S.l.: Perú.

KLEPAC, M., HEGR, T. y BOHAC, L., 2015. Enhancing availability of services using software-defined networking. *Advances in Electrical and Electronic Engineering*, vol. 13, no. 5, pp. 522-528. ISSN 18043119. DOI 10.15598/aeee.v13i5.1498.

MARÍN VALENCIA, J.J., PATIÑO VALENCIA, A. y ACEVEDO BEDOYA, J.C., 2020. Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS. *Revista Universitaria Católica Oriente*, vol. 31, no. 45, pp. 84-99.

MENDOZA CARLOS, E.J., 2020. *Modelo de alineamiento de tecnologías de la información para el apoyo de las estrategias del negocio en empresas orientadas a ofrecer servicios de TI del sector pyme en la región Lambayeque*. S.l.: s.n.

MORÁN BARRERA, J.C., 2020. *Implementación de un sistema de alta disponibilidad de un enlace VPN para una entidad financiera* [en línea]. S.l.: s.n. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3116/Julio Moran_Trabajo de Suficiencia Profesional_Titulo Profesional_2020.pdf?sequence=1&isAllowed=y.

MUÑOZ LÓPEZ, J.O., 2017. *Implementación de balanceo de carga de internet con Mikrotik en la dirección de Red de Salud Conchucos Sur - Huari; 2017.* [en línea]. S.l.: s.n. Disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/1978/BALAN

CEO_DE_CARGA_INTERNET_MUNOZ_LOPEZ_JUAN_ORLANDO.pdf?sequence=1&isAllowed=y.

MUSYAFFA, N. y RYANSYAH, M., 2020. Implementation of VPN Using Router MikroTik at Al-Basyariah Education Foundation Bogor. *Jurnal Teknik Informatika CIT Medicom*, vol. 12, no. 2, pp. 49-55.

NARAYAN, S., CAMERON J, W., HART, D.K. y QUALTROUGH, M.W., 2015. Network performance comparison of VPN protocols on wired and wireless networks. *2015 International Conference on Computer Communication and Informatics, ICCCI 2015*, pp. 419-425. DOI 10.1109/ICCCI.2015.7218077.

NUÑEZ AGURTO, A., 2020. FNCS: Propuesta de una plataforma de gestión de dispositivos de Red basados en RouterOS. *Ciencia y Tecnología*, vol. 13, no. 1, pp. 89-96. ISSN 1390-4051. DOI 10.18779/cyt.v13i1.356.

OSZLAK, O., 2020. Trabajo remoto: hacer de necesidad virtud. ,

OTZEN, T. y MANTEROLA, C., 2017. Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, vol. 35, no. 1, pp. 227-232. ISSN 07179502. DOI 10.4067/S0717-95022017000100037.

PACOTAYPE HUAMAN, R.J., 2018. *Metodologia integral para evaluar el rendimiento de firewalls* [en línea]. S.l.: s.n. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/38180/Pacotaype_HR.pdf?sequence=1&isAllowed=y.

PAUZHI IDROVO, W.H., 2016. *Análisis E Implementación De Políticas De Seguridad Para Wisp Mediante Equipos Mikrotik Y Elementos De Red* [en línea]. S.l.: s.n. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/12127/1/UPS-CT006042.pdf.

QUINTE SINCHE, P.I. y USHIÑA TOMALÁ, I.L., 2020. *Implementación de topologías de red utilizando equipos mikrotik* [en línea]. S.l.: s.n. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/20647/1/CD 10150.pdf.

REALPE ROSERO, J.L., 2016. Sistema de monitoreo de redes y equipos networking utilizando la herramienta MRTG y la tecnología Mikrotik para la empresa J & STECHNOLOGY. , vol. 1, no. 1, pp. 1-7.

ROSERO GUTIÉRREZ, J.S., 2021. *Formulación de propuesta para la implementación de una VPN en el Colegio centro Don Bosco* [en línea]. S.l.: s.n. Disponible en:

https://repository.usta.edu.co/bitstream/handle/11634/33538/2021juanroser o.pdf?sequence=1&isAllowed=y.

ROUSSEAU FREY, Á.C., 2013. *Laboratorio de nuevas métricas en ethernet*. S.l.: s.n.

SANTISTEBAN YNGA, B.R., 2020. *Arquitecturas de redes de computadoras definidas por software: revisión bibliográfica*. S.l.: s.n.

TORRES CALDERÓN, P.A. y ALFARO PAREDES, E.A., 2018. MEPES: Methodology for evaluating the performance of e-mail servers. *International Journal of Open Source Software and Processes*, vol. 9, no. 4, pp. 47-64. ISSN 19423934. DOI 10.4018/IJOSSP.2018100103.

TULLOH, R., AMRI GINTING, J.G., MULYANA, A. y LUTFI, M., 2020. Performance Comparison of File Transfer Protocol Service between Link State and Distance Vector Routing Protocol in Software Defined Network. *IOP Conference Series: Materials Science and Engineering*, vol. 982, no. 1. ISSN 1757899X. DOI 10.1088/1757-899X/982/1/012026.

USECHE AGUIRRE, M.C., VÁSQUEZ LACRES, L.M., SALAZAR VÁZQUEZ, F.I. y ORDÓÑEZ GAVILANES, M., 2021. Fórmula Estratégica Empresarial para Pymes en Ecuador ante el Covid-19. *Revista Universidad y Empresa*, vol. 23, no. 40, pp. 1-22.

VESGA FERREIRA, J.C., GRANADOS-ACUÑA, G. y VESGA BARRERA, J.A., 2016. Evaluación del rendimiento de una red LAN sobre power line communications para la transmisión de VOIP. *Iteckne*, vol. 13, no. 1, pp. 83-95. ISSN 1692-1798. DOI 10.15332/iteckne.v13i1.1385.

VÍLCHEZ ESPINOZA, F.A., GÓMEZ PUERTO, M.R. y GONZÁLEZ SEQUEIRA, Y.P., 2020. *Desarrollo de prácticas de laboratorio utilizando Tecnología MikroTik para el apoyo de la docencia de la asignatura Redes de Computadores de la carrera Ingeniería en Telemática* [en línea]. S.l.: s.n. Disponible en: http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/8166/1/245132.pdf.

VONDROUS, O., MACEJKO, P. y KOCUR, Z., 2015. FlowPing - The New Tool for Throughput and Stress Testing. *Information and Communication Technologies and Services*, vol. 13, no. 5, pp. 516-521. DOI 10.15598/aeee.v13i5.1497.

WU, Z. y XIAO, M., 2019. Performance evaluation of VPN with different network topologies. *2019 2nd International Conference on Electronics Technology, ICET 2019*, pp. 51-55. DOI 10.1109/ELTECH.2019.8839611.

Anexo 3: Matriz de operacionalización de variables

Tabla Nª 40 : *Matriz de operacionalización de variable*

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADOR	DESCRIPCIÓN	INSTRUMENTO	UNID. DE MEDIDA
Redes VPN	VPN es una abreviatura de las siglas en inglés virtual Prívate Network, la cual es en síntesis una red privada virtual, que es publica, pero inaccesible, la cual conecta de manera segura, redes en ubicaciones remotas, utilizando para ello medios no personales como el internet. **(Jota, Ramirez y Penagos 2018; Cueva 2018)**	Esta conexión prioriza la privacidad de la información que se transmite, evitando que agentes no autorizados puedan vulnerar o capturar paquetes en el tráfico y sustraer la información. Este tipo de solución bien implementada y configurada es usada para transmitir información considerada sensible, data de conexión y accesos remotos en grandes, pequeñas, medianas y microempresas. Las empresas con la nueva normalidad se han visto obligados a buscar y usar diversas soluciones de acceso remoto, para enlazar sedes, acceder a servidores y/o facilitar a los colaboradores puedan acceder a las aplicaciones de la empresa y seguir realizando sus actividades sin movilizarse de sus domicilios.	Red Privada **(Jota, Ramirez y Penagos 2018; Cueva 2018)**				
Servidores	Los servidores se ejecutan mediante una arquitectura (cliente-servidor), a través del uso de una red. Los servidores brindan servicios fundamentales en una red, así sea usuarios privados, públicos, organizaciones o compañías por medio del internet. **(Davila 2019; Morán 2020; Castro 2019)**	Los servidores son artefactos informáticos que proporcionan, distribuye y almacena información y servicios. Por consiguiente, el servidor ejecuta otras labores para beneficio de los consumidores; les da la probabilidad de compartir datos, información y recursos de hardware y programa, para ello consumen recursos de hardware y software, conectándose a una red local y publica, según sé la necesidad.	Desempeño en la Red **(Chilcañán, Navas y Escobar 2017)**	Medición de Throughput **(Pacotaype 2018; Julca y Tapia 2020; Vesga, Granados y Vesga 2016)**	$throughput = \frac{Paquete\ total\ r}{Tiempo}$	Ficha de observación **(Hernández y Mendoza 2018)**	
			Consumo de Recursos **(Julca y Tapia 2020; Pacotaype 2018)**	Consumo de Memoria RAM **(Aguirre 2016; Pacotaype 2018)**	$Consumo\ Memori = Total\ de\ Memor - Memoria\ RAM\ D$	Ficha de observación **(Hernández y Mendoza 2018)**	
			Conectividad de la Red **(Chilcañán, Navas y Escobar 2017; Egas, Viracocha y Rivera 2019)**	Tiempo de Respuesta de la Red LAN **(Davila 2019)**	$Red\ LAN = \frac{Capacidad\ paq}{Ancho\ de\ ban}$	Ficha de observación **(Hernández y Mendoza 2018)**	

Anexo 4: Matriz de consistencia

Tabla Nª 41 : *Matriz de consistencia*

<table>
<tr><th>Problema General</th><th>Objetivo General</th><th>Hipótesis</th><th>Variable</th><th>Dimensiones</th><th>Indicadores</th><th>Método</th><th>Instrumento</th></tr>
<tr><td>PG: ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco?</td><td>OG: Determinar el proceso de la Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco.</td><td>HG: La Implementación de redes VPN MIKROTIK incrementó el desempeño de la red, mejoro el consumo de recursos y la conectividad en la red de los servidores entre ciudades de Lima y Pisco.</td><td>Redes VPN</td><td></td><td></td><td rowspan="5">Tipo de investigación: Aplicada
(Hernández y Mendoza 2018)
Enfoque de investigación: Cuantitativo
(Hernández y Mendoza 2018)
Diseño de investigación: pre - experimental
(Hernández y Mendoza 2018)
Nivel de la investigación
Descriptivo
(Hernández y Mendoza 2018)</td><td rowspan="5">Ficha de observación
(Hernández y Mendoza 2018)</td></tr>
<tr><td>Problema Especifico</td><td>Objetivo Especifico</td><td>Hipótesis Específicos</td><td rowspan="4">Servidores</td><td></td><td></td></tr>
<tr><td>PE1: ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK en desempeño en la red para los servidores entre ciudades de Lima y Pisco?</td><td>OE1: Determinar el proceso de la Implementación de redes VPN MIKROTIK en el desempeño en la red para los servidores entre ciudades de Lima y Pisco.</td><td>HE1: La Implementación de redes VPN MIKROTIK incrementó el desempeño en la red de los servidores entre ciudades de Lima y Pisco (Vesga, Granados y Vesga 2016; Pacotaype 2018; Julca y Tapia 2020).</td><td>Desempeño en la Red
(Vesga, Granados y Vesga 2016)</td><td>Medición de Throughput
(Pacotaype 2018; Julca y Tapia 2020; Vesga, Granados y Vesga 2016)</td></tr>
<tr><td>PE2: ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK en el consumo de recursos para los servidores entre ciudades de Lima y Pisco?</td><td>OE2: Determinar el proceso de la Implementación de redes VPN MIKROTIK en el consumo de recursos para los servidores entre ciudades de Lima y Pisco.</td><td>HE2: La Implementación de redes VPN MIKROTIK mejoró el consumo de recursos de los servidores entre ciudades de Lima y Pisco (Julca y Tapia 2020; Aguirre 2016; Pacotaype 2018).</td><td>Consumo de Recursos
(Julca y Tapia 2020; Pacotaype 2018)</td><td>Consumo de Memoria RAM
(Aguirre 2016; Pacotaype 2018)</td></tr>
<tr><td>PE3: ¿Cuál es el proceso de la Implementación de redes VPN MIKROTIK en la conectividad en la red para los servidores entre ciudades de Lima y Pisco?</td><td>OE3: Determinar el proceso de la Implementación de redes VPN MIKROTIK en la conectividad en la red para los servidores entre ciudades de Lima y Pisco.</td><td>HE3: La Implementación de redes VPN MIKROTIK mejoró la conectividad en la red de los servidores entre ciudades de Lima y Pisco (Chilcañán, Navas y Escobar 2017; Davila 2019).</td><td>Conectividad en la Red
(Chilcañán, Navas y Escobar 2017)</td><td>Tiempo de respuesta de la Red LAN
(Davila 2019)</td></tr>
</table>

Anexo 5: Captura de Pre pruebas

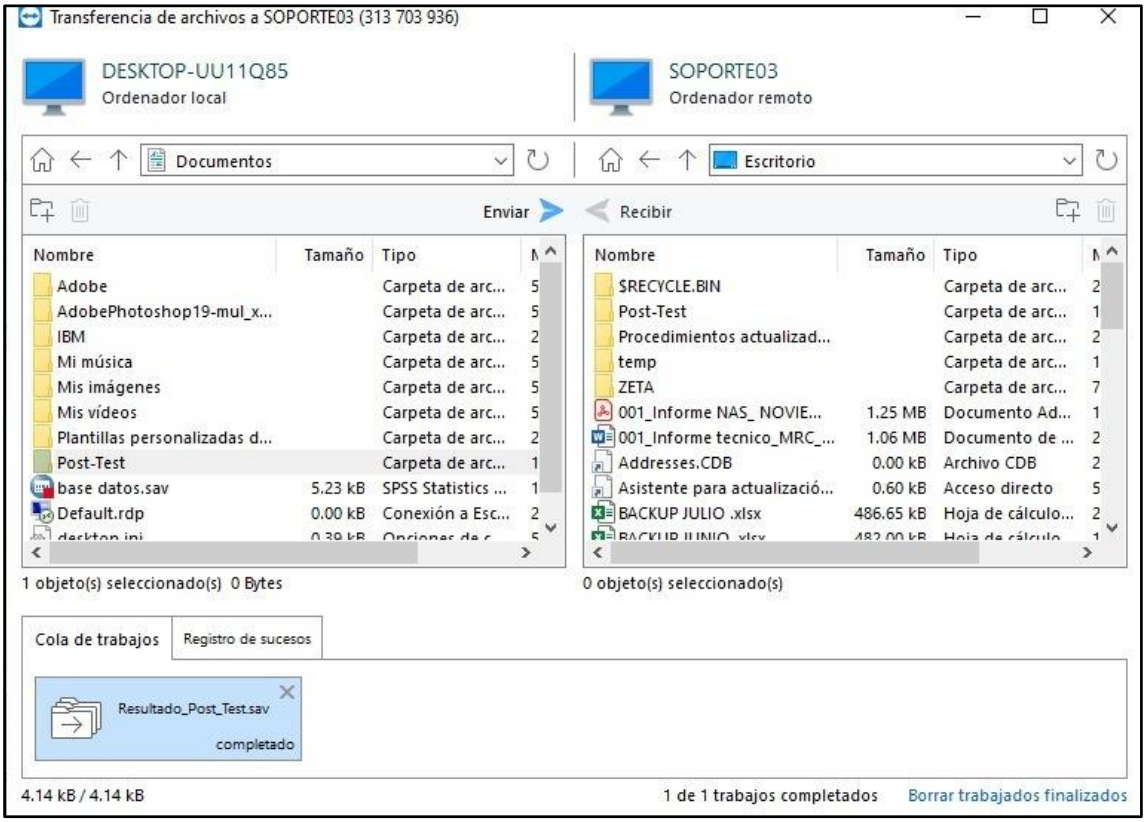

Figura 20.: Pre prueba de medición del Throughput

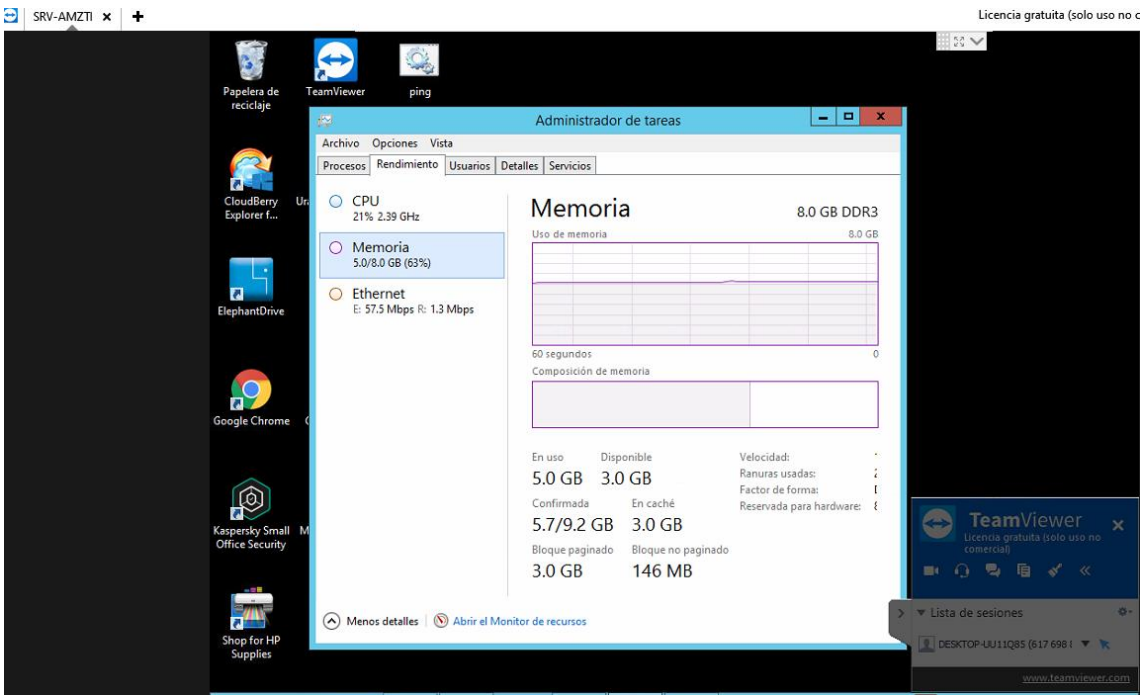

Figura 21.: Pre prueba de medición de consumo de memoria RAM

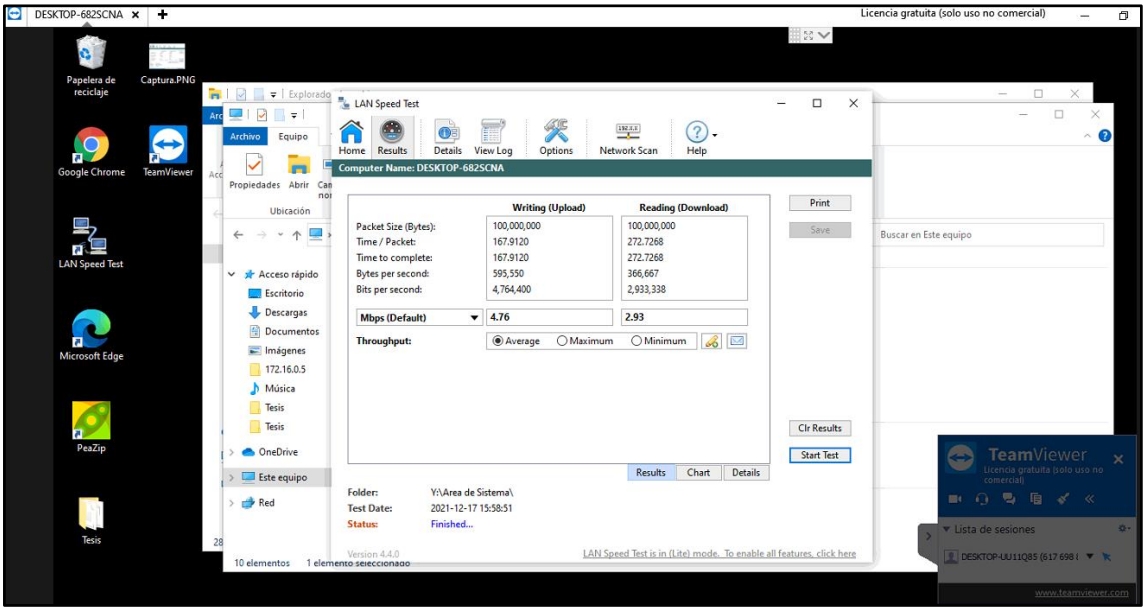

Figura 22.: Pre prueba de medición de Tiempo de respuesta red LAN

Anexo 6: Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco

Implementación de redes VPN Mikrotik para los servidores entre ciudades de lima y pisco está siendo descriptiva tomando en cuenta los próximos puntos

I. Objetivo de la Implementación

El objetivo de la implementación de redes VPN MIKROTIK incrementará la conectividad de los servidores entre ciudades de lima y pisco.

II. Alcance de la Implementación

El alcance de esta implementación encierra la evaluación del rendimiento de la red secundado en los criterios de evaluación: manejo en la red y consumo de recursos. Anterior a comenzar la evaluación se debería conocer las habilidades técnicas y funcionales de los dispositivos, para esto se debería tener en importancia la revisión de lo próximo.

III. Fases de la Implementación

Implementación de redes VPN MIKROTIK

Figura 23. Fases de la Implementación

Imagen del desarrollo de las fases de la implementación

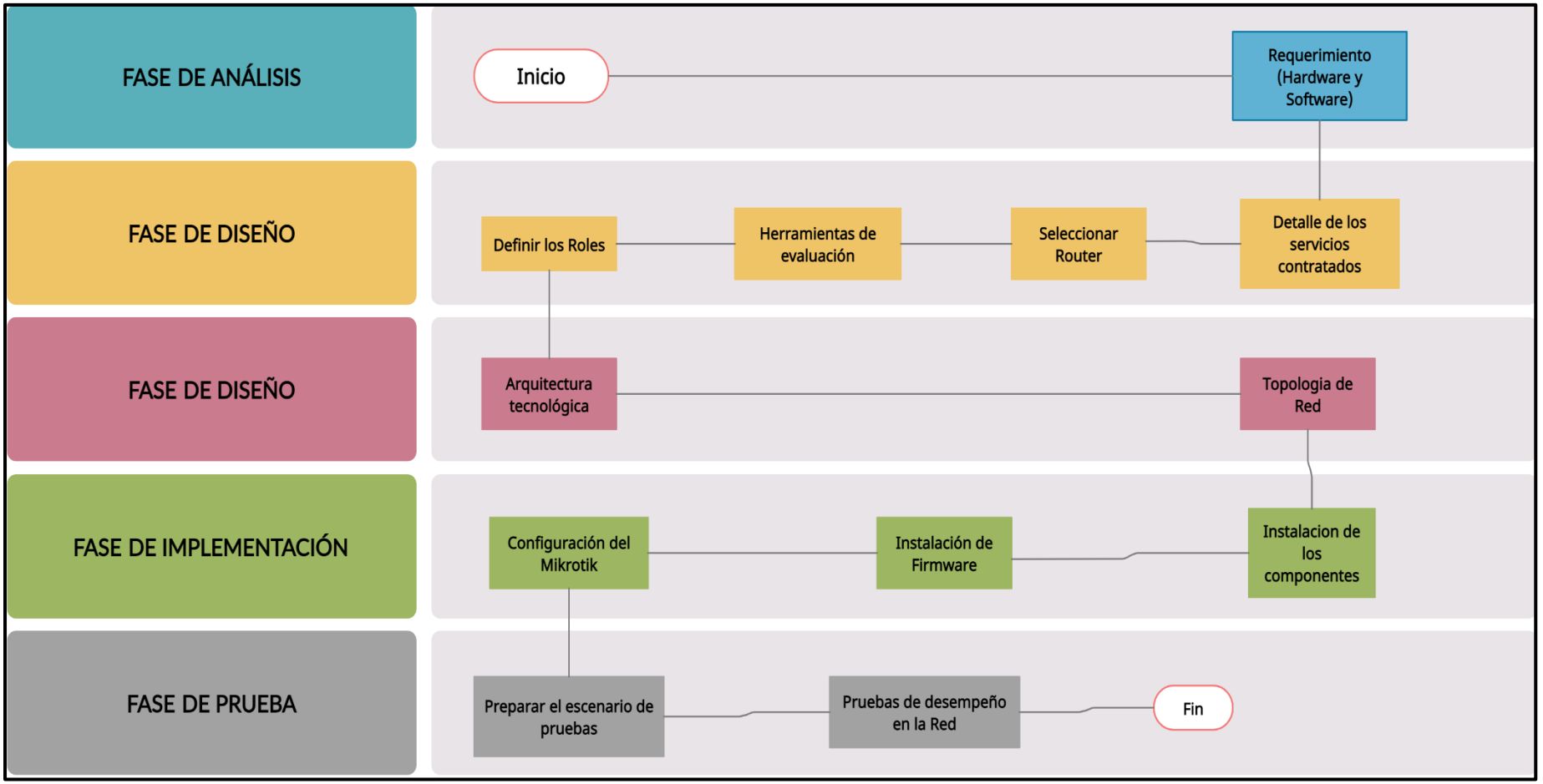

Figura 24. Desarrollo de las fases de la implementación

1. Fase de Análisis

A. Requerimiento (Hardware y Software)

Tabla Nª 42 : *Tabla de Requerimiento*

Equipo	Características	Logo	Cantidad	Disponible
Routerboard Mikrotik RB 450G	• Sistema Operativo: RouterOS • Tamaño RAM 256MB • Almacenamiento 512MB • 5 Puertos Ethernet		2	Si
Laptop	• Intel Core i5 • Windows 10 Pro • Memoria RAM 12GB • ASUS		2	Si
Cable de Red	• Cable De Red Utp RJ45 de 3 mts		4	Si
IP Pública Claro Movistar	• 190.117.66.233 • 179.6.169.95		2	Si

2. Fase de Planeamiento

A. Detalle de los Servicios Contratados

- En la sede de lima se contrató una IP publica estática al proveedor de servicios América Móvil, de 60 MB, la IP publica 190.117.66.233.
- En la sede de pisco se contrató una IP publica estática al proveedor de Movistar, de 60 MB, la IP publica 190.232.131.252.

B. Seleccionar Router

La selección de los Router Mikrotik, se hace a conveniencia por ser accesible a los estudios, por los cuales son las próximas marcas:

- Routerboard Mikrotik

C. Definir las Herramientas de Evaluación

- **Jperf:** Es un instrumento de software libre que posibilita la medición de medir Throughput y redes locales (Julca y Tapia 2020).
- **Lan Speed test:** una herramienta simple pero poderosa para medir la transferencia de archivos, el disco duro, la unidad USB y las velocidades de la red de área local (LAN) (Pacotaype 2018).
- **Winbox:** es una aplicación que posibilita la gestión de Mikrotik RouterOS utilizando interfaz gráfica de usuario, simple y sencilla (Nuñez 2020).

D. Definir los Roles

- **Estación de trabajo:** Son Pc's y Laptop con superiores recursos que la Pc's usual y son usados por los empleados o trabajadores de la compañía u organización.
- **Servicio de monitoreo:** Posibilita al administrador de la red poder ingresar, por medio de la interfaz gráfica.

3. Fase de Diseño

A. Arquitectura Tecnológica

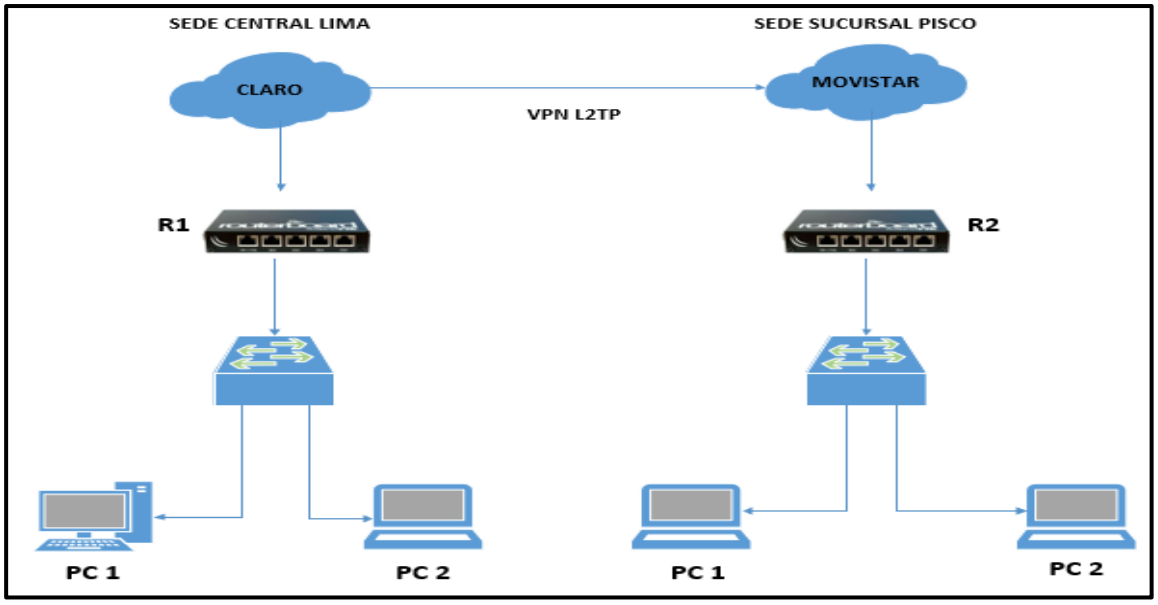

Figura 25. Arquitectura Tecnológica

B. Topología de la Red

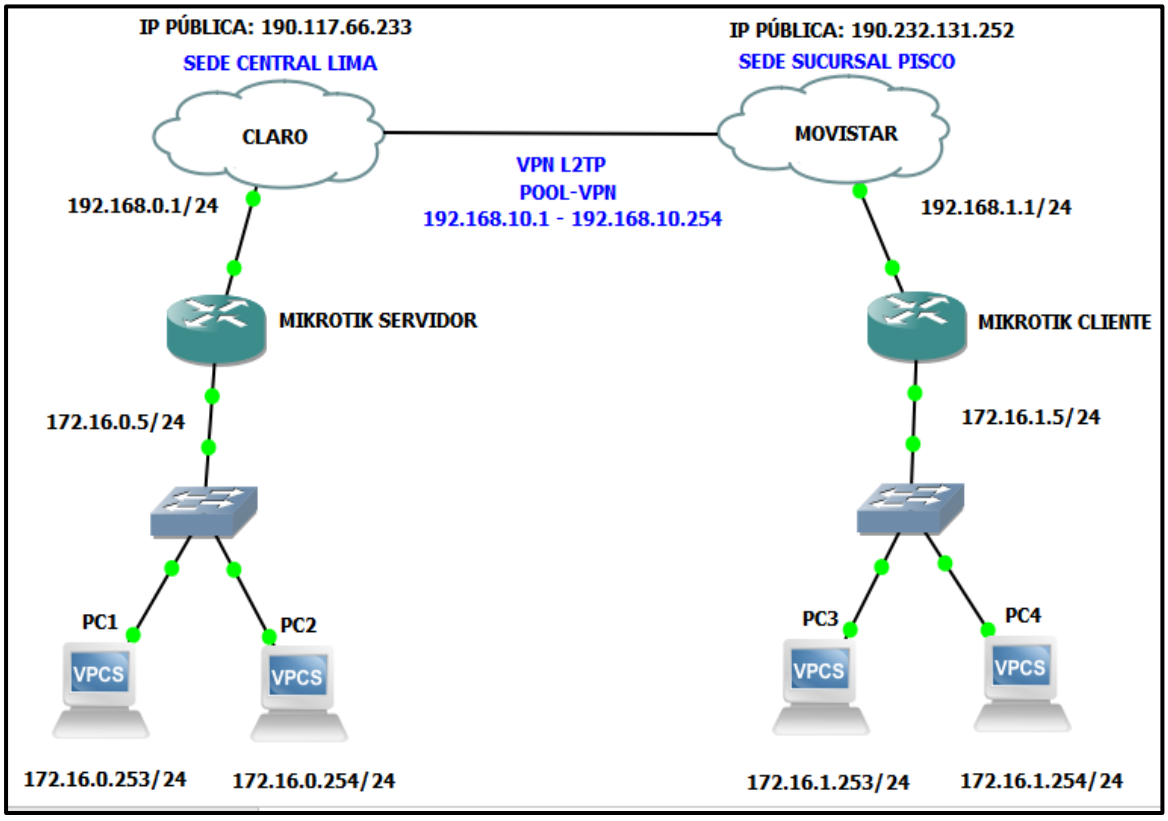

Figura 26. Topología de la Red

4. Fase de Implementación

A. Realizar la instalación de los componentes

Se realizo la instalación de todos los componentes:

- Se procedió a instalar el Router Mikrotik RB 450G en la sede Lima usando dos cables de Red.
- Se procedió instalar el Router Mikrotik RB 450G en la sede Pisco usando dos cables de Red.

B. Realizar la instalación del Firmware

Para actualizar el sistema operativo de Mikrotik por el aplicativo del Winbox. Paso fundamental una vez que ponemos un Mikrotik en administración debido a que frecuentemente la actualización de su firmware soluciona inconvenientes de estabilidad que nos ayudaran a conservar una red segura.

- Accedemos al Mikrotik vía Winbox luego vamos al menú lateral izquierdo a la elección **System -> Packages**

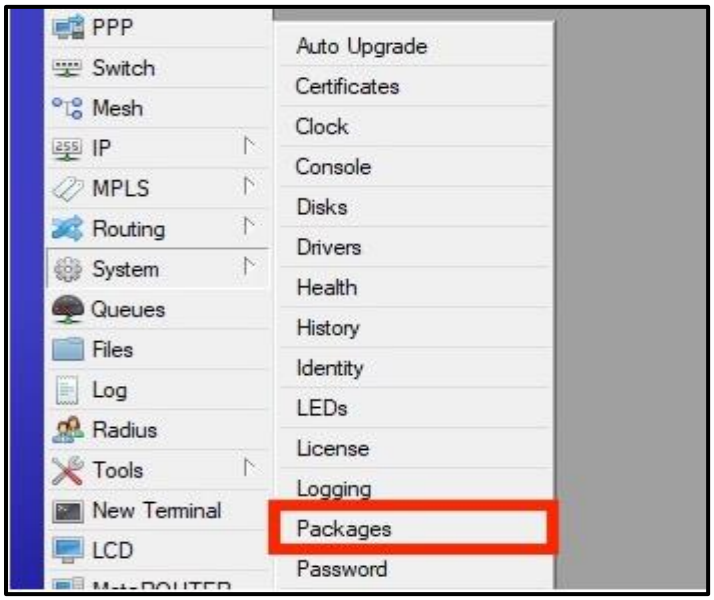

Figura 27. Topología de la Red

- Nos dirigimos al botón **Check For Updates** para revisar las actualizaciones:

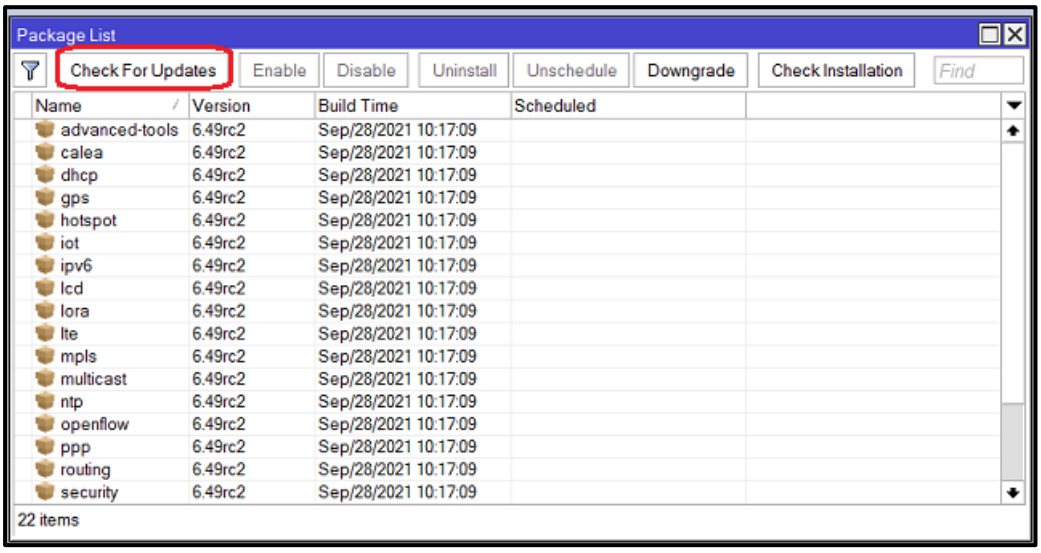

Figura 28. Comprobar si hay actualizaciones nuevas

- Seguimos y seleccionamos en la ventana **Stable** en el parámetro **Channel** y observamos las nuevas versiones **Installed versión** y la **Latest versión**. Y presionamos el botón **Download&Install:**

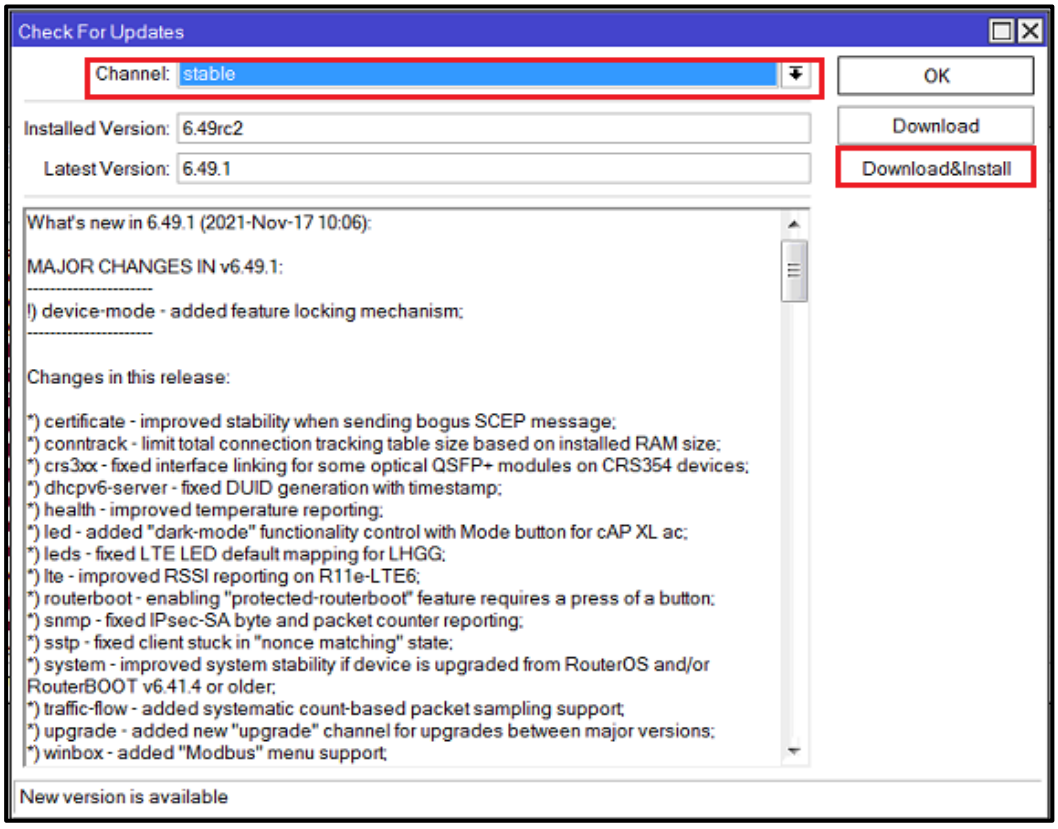

Figura 29. Descarga e instalación (Actualización)

- Si todo es adecuado observaremos **el proceso de descarga en la parte inferior:**

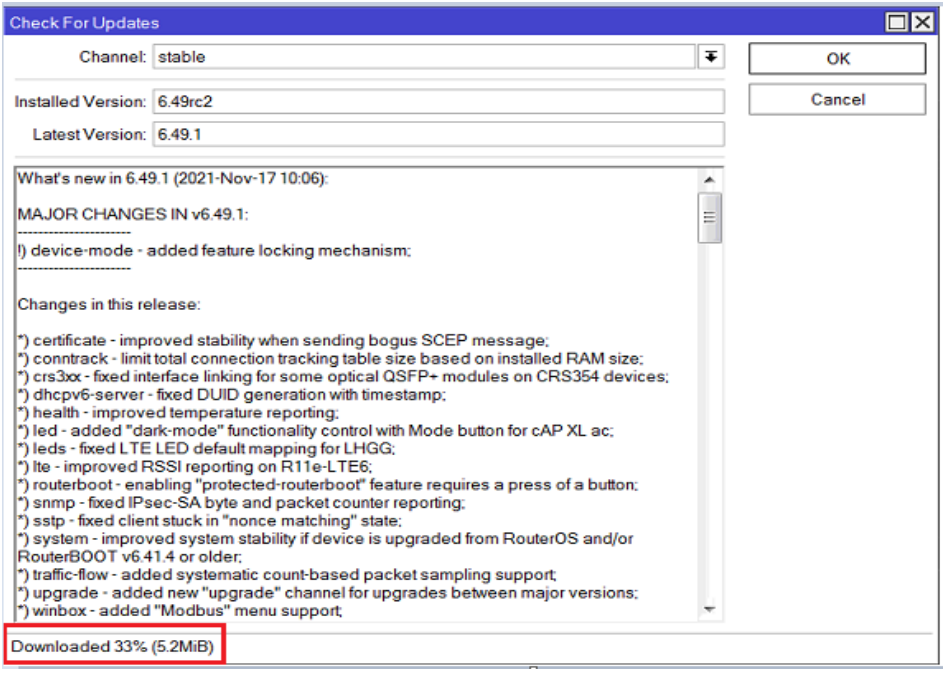

Figura 30. Proceso de descargade la actualización

C. Configuración del Mikrotik (VPN – L2TP)

Para configurar Mikrotik VPN se necesita conocer sobre redes y hacer pasos que iremos explicando en la configuración:

- En el menú primordial del Winbox seleccionamos la alternativa **IP**, luego escogimos la sub-opcion **Firewall:**

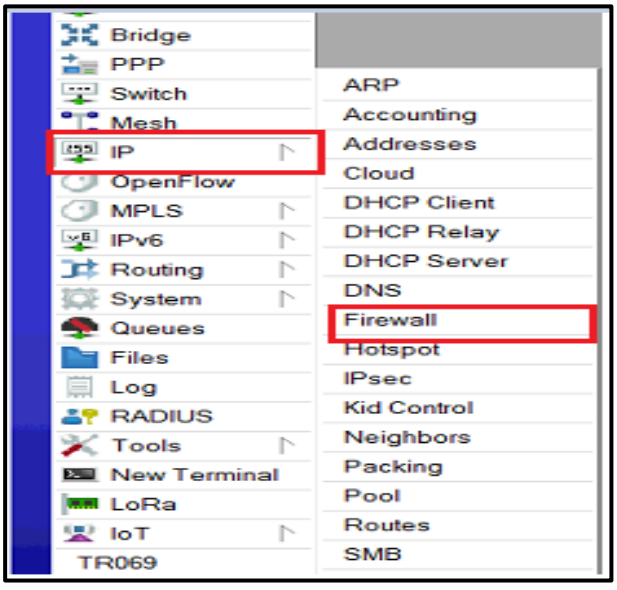

Figura 31. Configuración del Servidor

- Nos dirigimos a el fragmento de firewall y añadimos nuestra regla input para admitir el tráfico entrante de los próximos **puertos UPD 1701: L2TP, UDP: 500**. Utilizado por el protocolo **IPSec el UDP: 4500**: utilizado por IPSec manejo de la **encryptacion** y el **nateo** de nuestro túnel **L2TP/IPSec**.

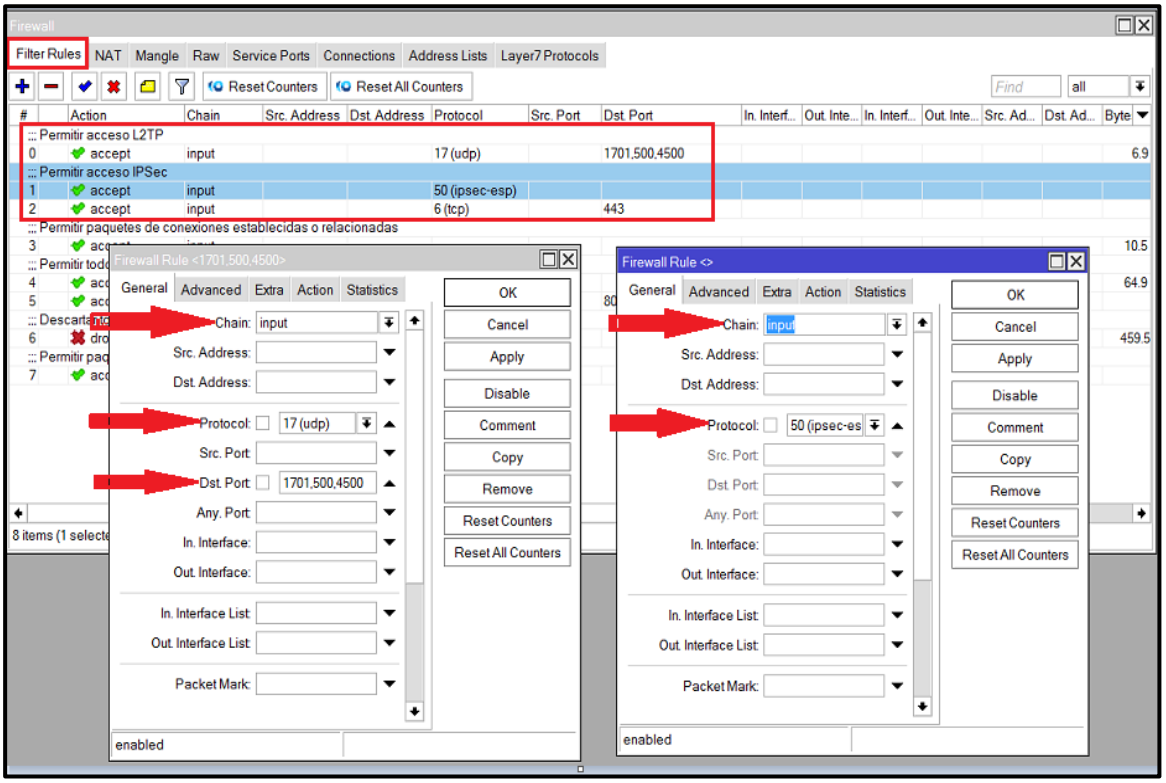

Figura 32. Configuración de Puertos

- Luego realizaremos la activación del servicio de PPP para la configuración de la VPN L2TP ingresamos en la interface, luego le damos clic en la opción L2TP Server:

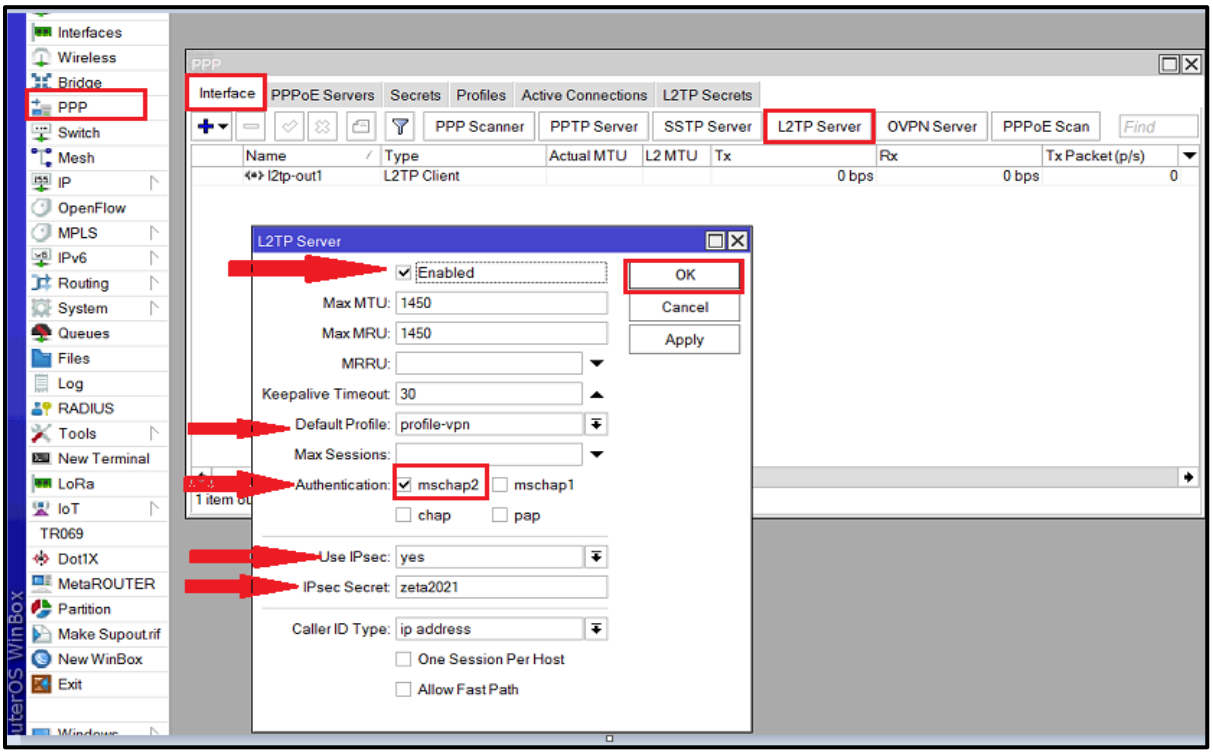

Figura 33. Configuración de Túnel L2TP/IPSec server

- Como siguiente paso vamos a crear los usuarios para la VPN:

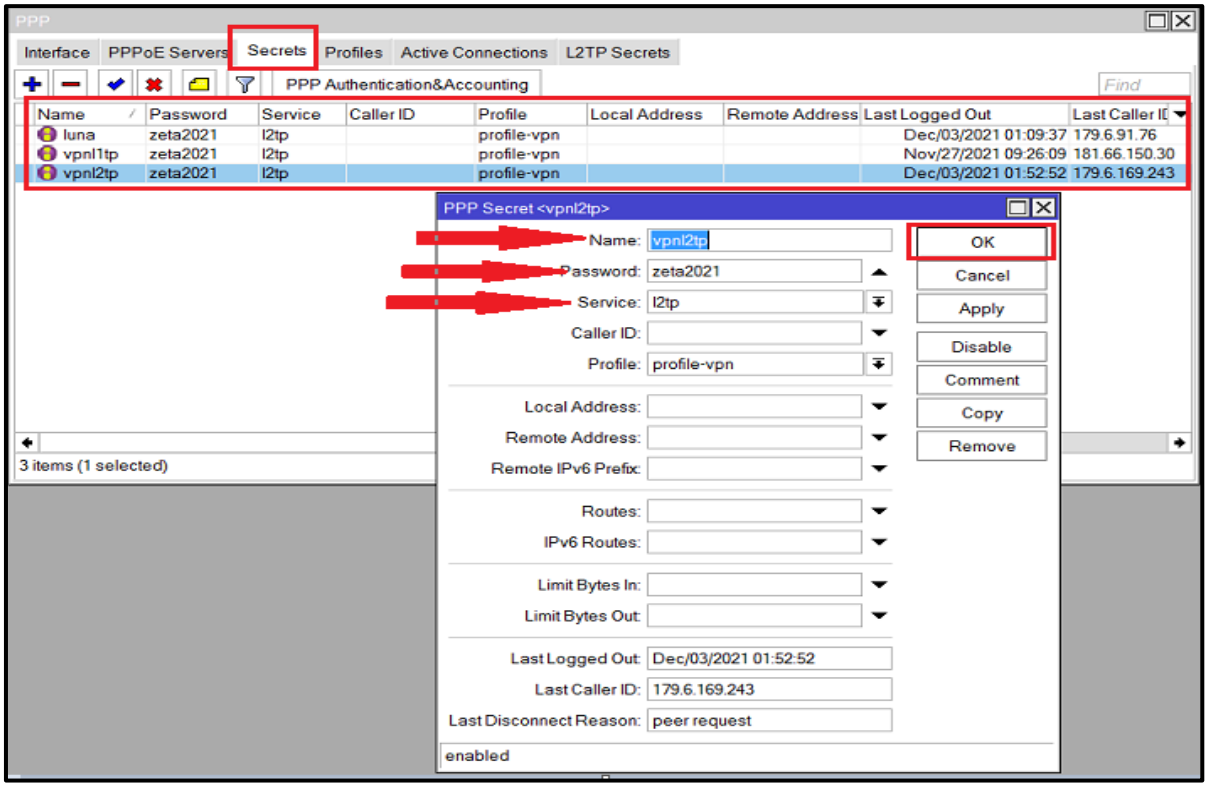

Figura 34. Configuración de los usuarios de la VPN

- Configuramos en nuestro cliente Windows 10 no dirigimos configuraciones y después a Red internet, luego seleccionamos VPN y damos click en añadir conexión VPN

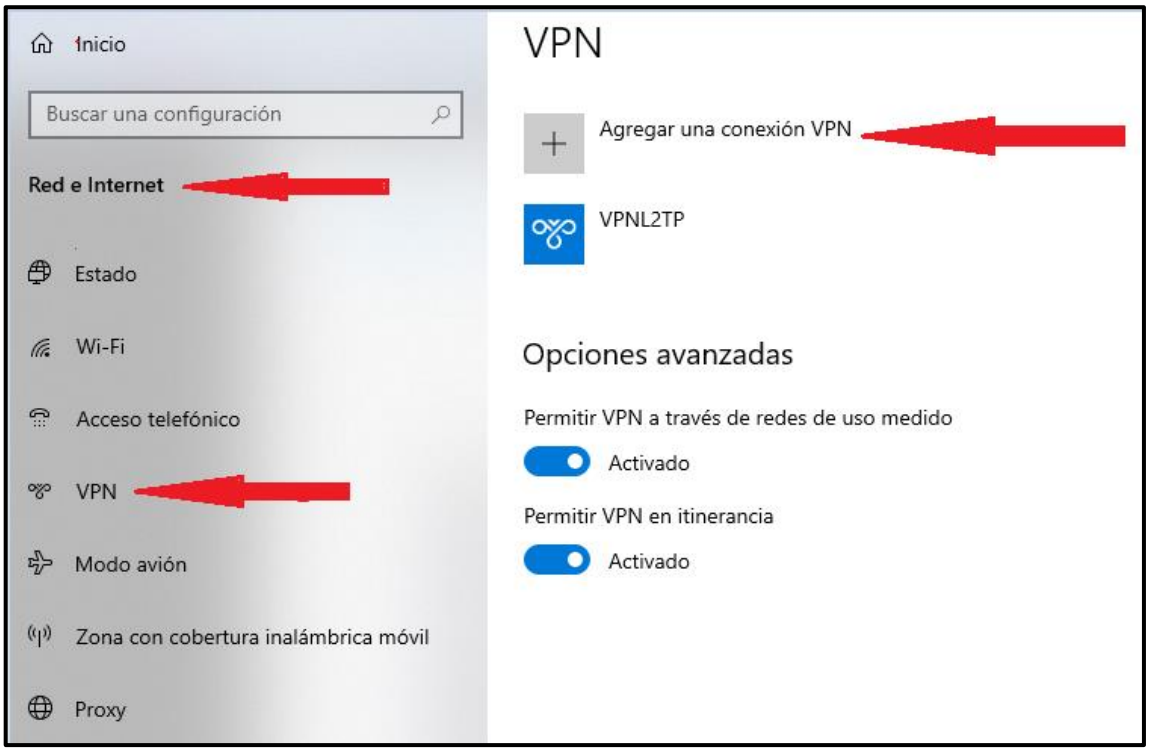

Figura 35. Configuración de VPN al Windows 10 (Cliente)

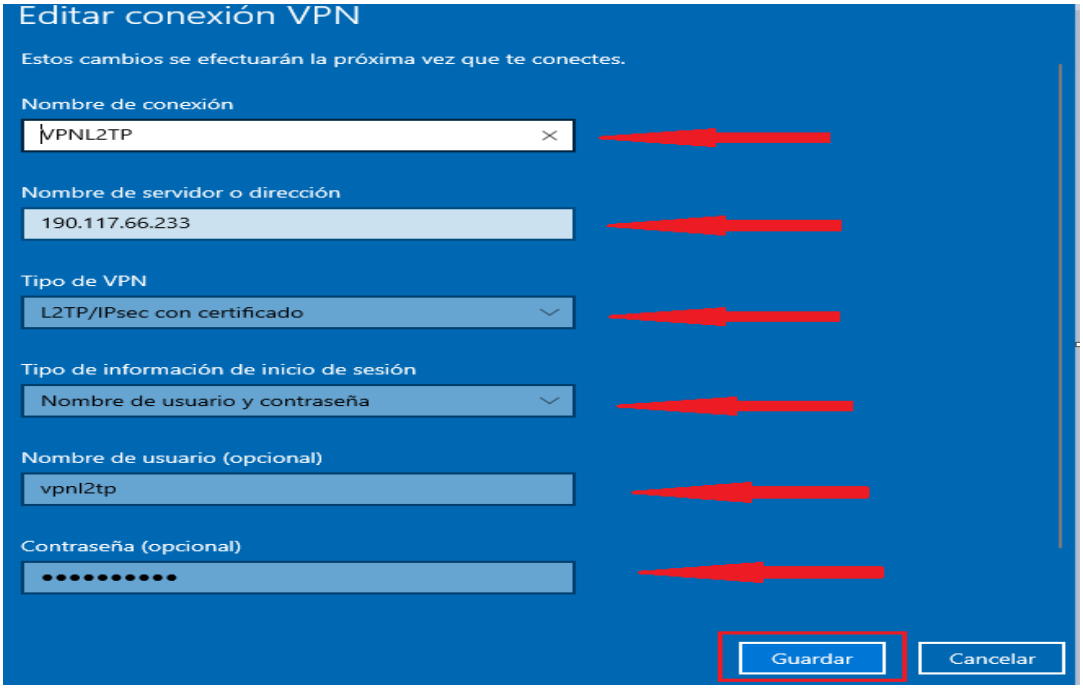

Figura 36. Ingreso de datos a la VPN

- Conexión exitosa de la VPN

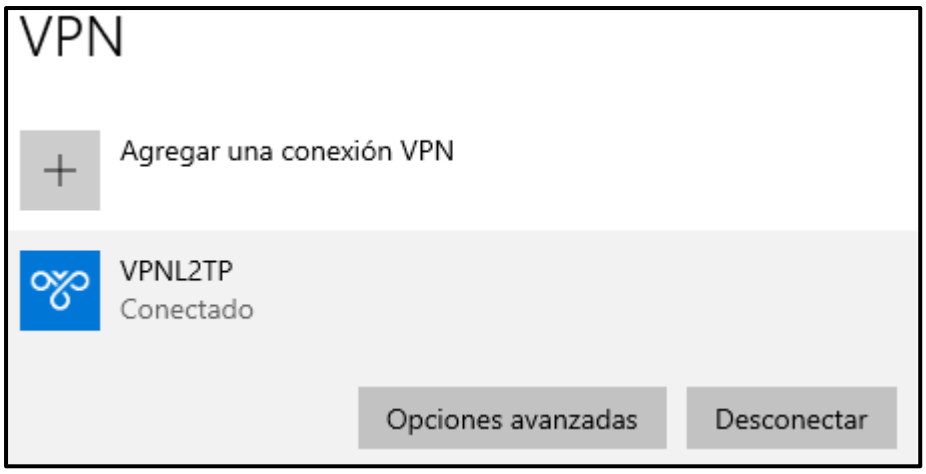

Figura 37. Conexión exitosa de la VPN

5. Fase de Pruebas

En esta etapa de presentación del ambiente de prueba según la topología y ejecutamos las pruebas programadas, de consenso al entorno de la presente implementación.

A. Preparar el escenario de pruebas

Previo a elaborar a las pruebas se debería asegurar el incremento de los recursos de los sujetos de medición. Con el fin de las pruebas se realicen en ámbito igualitario.

La topología de la red que utilizaremos en el presente ataque hacia la estación de trabajo y servidor de monitoreo de red. El escenario postulado va a ser realizado desde la configuración de una LAN.

B. Realizar las pruebas de desempeño en la red

Procedimiento para realizar las pruebas de desempeño en la red

- **Objetivo**

Medir y examinar el incremento de Router de consenso al criterio de evaluación manejo en la red.

Se busca decidir el nivel de predominación que desempeña todos los Router sobre el tráfico de red que le atraviesa y evaluar la rapidez real en la que transmiten los datos (Throughput).

- **Alcance**

  El alcance del procedimiento incluye:

  a. Revisión de los procesos de la etapa de planeamiento de la presente metodología.
  b. Revisión de documentación relacionada a las pruebas de manejo en la red en relación con los indicadores Throughput.
  c. Revisión de la vigencia de las pruebas.
  d. Verificación de idónea ejecución de las pruebas.

- **Entradas**

  Para hacer estas pruebas, es preciso que se haya desarrollado la etapa de planeamiento de la presente metodología (Identificación de criterios de evaluación, definición del individuo de medición, aplicaciones para evaluar el rendimiento y roles) y preparado el ambiente de pruebas según los escenarios propuestos para Routerboard a evaluar.

- **Proceso**

  Las ocupaciones por hacer para calcular el costo del Throughput frente a el envío de paquetes son las próximas:

1. La prueba para encontrar el Throughput se apoya en producir tráfico por medio del envío de paquetes de diferentes tamaños a partir de la estación de trabajo hacia el servidor.
2. La comunicación entre la estación de trabajo (zona LAN) y el servidor (zona DMZ) es directa al quipo evaluado
3. Conceder direcciones IP de host a los dispositivos, conforme con la red que le corresponda:

IP Servidor	: 190.117.66.233
IP estación de trabajo	: 172.16.0.5/24

4. Revisar que exista conectividad entre la estación de trabajo (cliente) y el servidor con ayuda del comando ping (protocolo ICMP).
5. En la estación de trabajo debería presionar la tecla “Windows + R” y aparecerá la herramienta ejecutar.

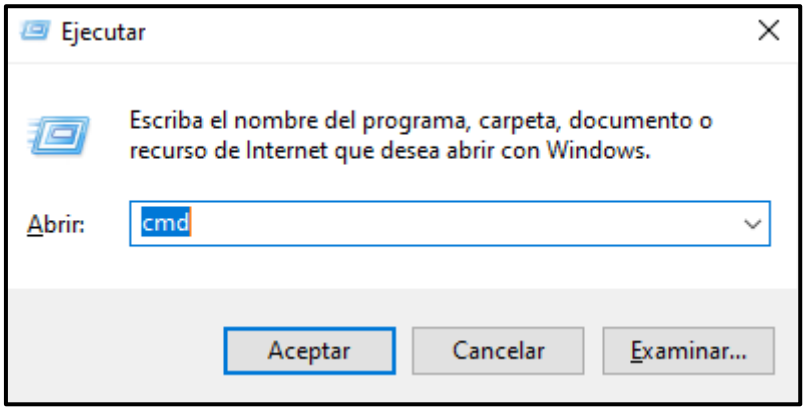

Figura 38. Herramienta Ejecutar

6. De la misma forma que se muestra en la figura anterior, en la herramienta realizar debería redactar el término “CMD” para abrir el signo del sistema.
7. Luego de que cargue la consola del signo del sistema “CMD” debería llevar a cabo el comando ping en compañía de la dirección IP del servidor y/o estación de trabajo. Ejemplificando:

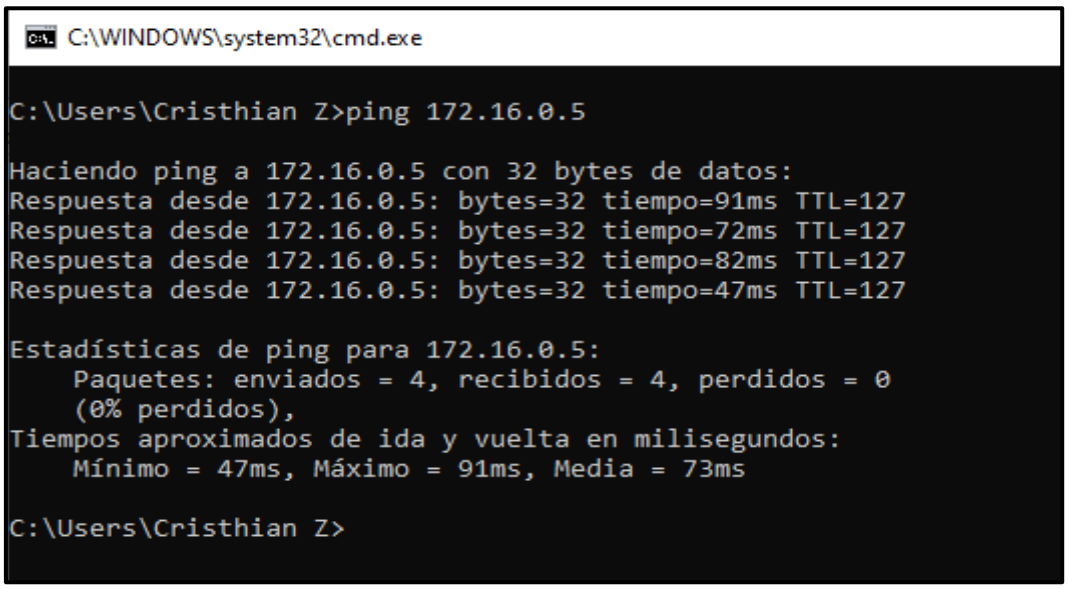

Figura 39. Conectividad con el Servidor

8. Debería obtener contestación del servidor como se observa en la imagen anterior caso opuesto no va a poder hacer la prueba.
9. Nota: La herramienta a usar en la presente prueba es Jperf que es la versión grafica de Jperf, delegada de mandar paquetes de red en porciones y peso según las necesidades de la prueba.

10. Llevar a cabo Jperf en el servidor, realizando doble clic en el icono localizado en el escritorio (Callegati, Cerroni y Contoli 2016; p. 5; Klepac, Hegr y Bohac 2015; p. 525).

Figura 40. Icono de la Herramienta Jperf

11. Configurar la herramienta Jperf en modo server (Servidor) y dejar la configuración por defecto (puerto 5001 y número de conexiones 1), como se muestra en la siguiente imagen (Vesga, Granados y Vesga 2016; p. 90 Rousseau 2013; p. 45).

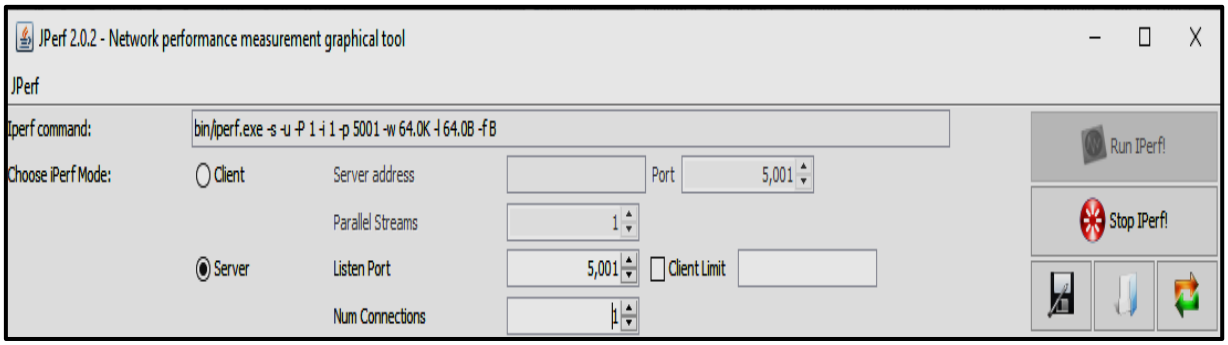

Figura 41. Panel de configuración de la herramienta Jperf modo Server

12. Hacer clic en el botón “Run Jperf” para empezar la herramienta Jperf en modo comprador.
13. Realizar la herramienta Jperf en la estación de trabajo realizando doble clic en el icono del escritorio, de la misma forma que se sugiere en la figura Nª 27.
14. Configurar la herramienta Jperf en modo comprador (Estación de trabajo), ingresar la dirección IP del servidor (172.16.0.5) y situar el puerto activo por defecto (5001), como se muestra en la siguiente imagen (Rousseau 2013; p. 45).

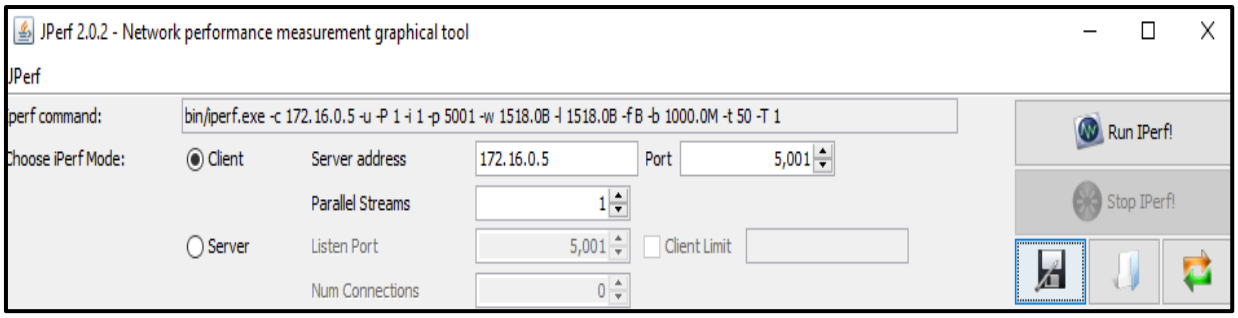

Figura 42. Panel de configuración de la herramienta Jperf modo cliente

15. Configurar el menú “Application layer options” del Jperf (Estación de trabajo) la era de transmisión en 50 segundos, el Output Format en Bytes y el examen test port en 5001, como se muestra en la figura Nª 30.

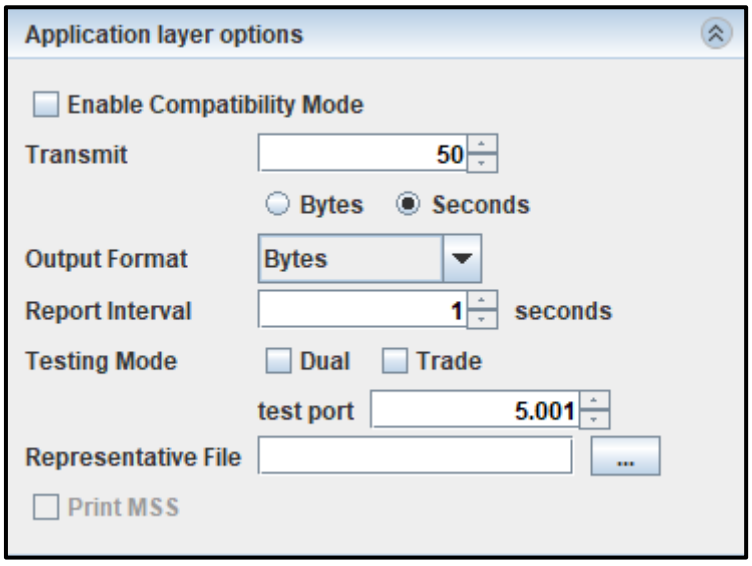

Figura 43. Panel application layer options de la herramienta Jperf

16. Conceptualizar la medida de paquetes en bytes a usar para la ejecución de las pruebas. Según los estándares RFC-2544 e ITU-T Y.1564 se tienen que utilizar los próximos tamaños de paquetes en Bytes (Vondrous, Macejko y Kocur 2015; p. 517; Rousseau 2013; p. 22; Alvarez 2010; p. 25).

Tabla Nª 43 : *Paquetes estándares RFC - 2544*

Estándares RFC – 2544						
A	**B**	**C**	**D**	**E**	**F**	**G**
64	128	256	512	1024	1280	1518

17. Configurar el menú “Transport layer options” del Jperf (Estación de trabajo), para eso debería elegir el protocolo UDP para el envío de paquetes y después debería configurar el “UDP Bandwidth” con los datos de acuerdo con el medio de transmisión usado (1000) cable UTP Giga Ethernet.
18. Posteriormente en las posibilidades del menú “UDP Buffer size” y “UDP Packet size” del Jperf (Estación de trabajo) debería poner los valores definidos en la tabla anterior (64, 128, 256, 512, 1024, 1280, 1518) y al final debería hacer clic en el botón “Run Iperf” para ofrecer inicio a la prueba. En la siguiente figura Nª 31 se muestra cómo debería permanecer el menú “Transport layer options” luego de meter los valores asignados

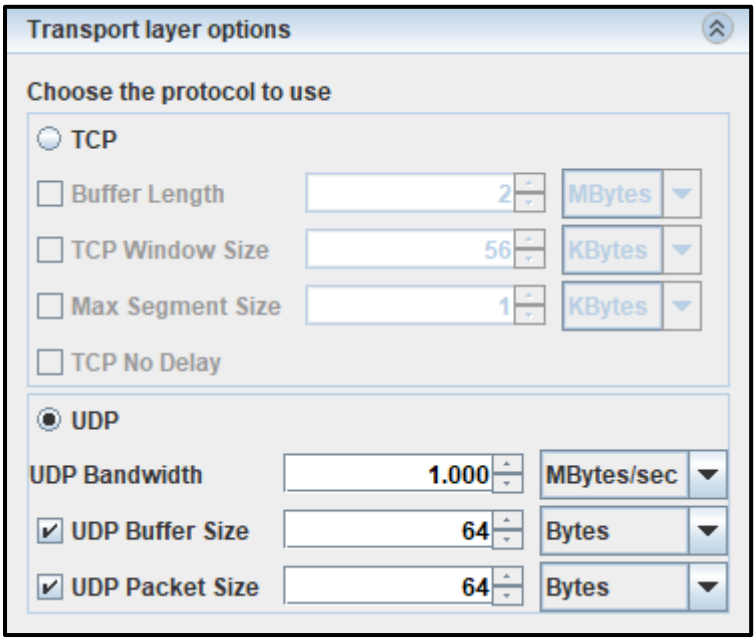

Figura 44. Panel transport layer options de la herramienta Jperf

19. Observar el panel “Output” de la herramienta Jperf que está ejecutándose en el servidor. En la siguiente figura se muestra como aparecerán los resultados de la prueba en el panel.

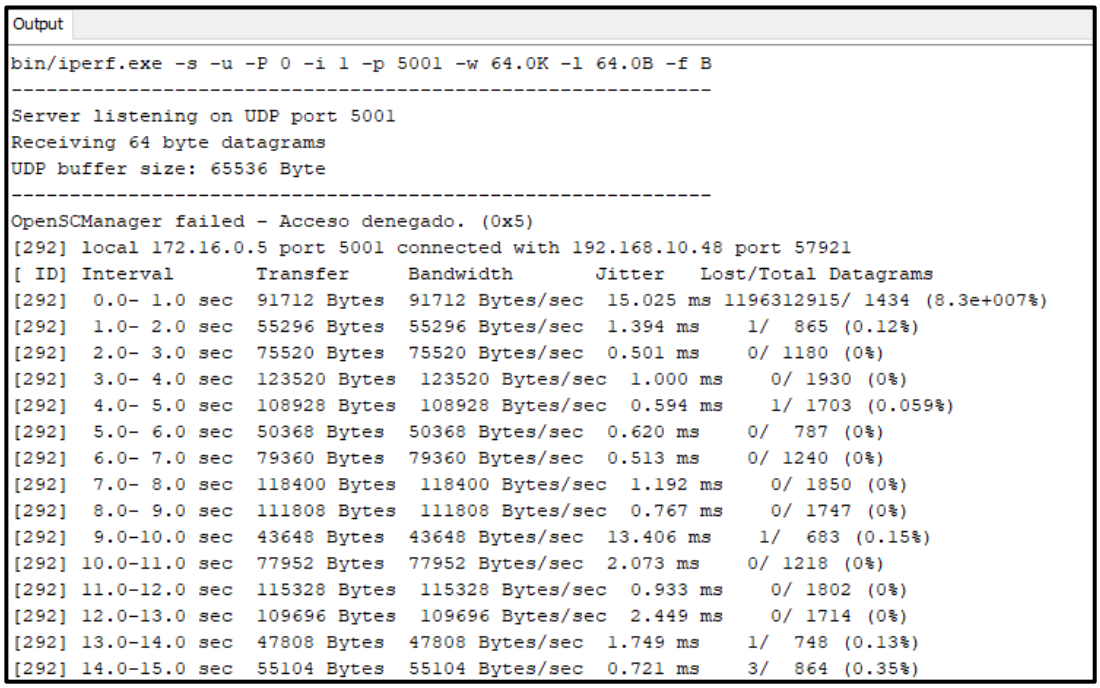

Figura 45. Resultado de prueba de Throughput con la herramienta Jperf

20. Ahora debería tomar nota de los 50 resultados mostrados en la columna “Bandwidth” del Jperf (Servidor) y agruparlos en la tabla de tabulación de datos según las columnas Firewall, tamaño de paquetes y las filas conforme el orden correspondiente.
21. Posteriormente debería repetir el paso 17 hasta el 21 cambiando los valores según la tabla indicada en el paso 17 (64, 128, 256, 512, 1024, 1280, 1518) bytes para ofrecer cumplimiento a los estándares mundiales.
22. La evaluación del Throughput en la presente metodología concluye una vez que se ha llevado a cabo las pruebas a todos los Firewalls con los valores asignados en la tabla.

Procedimiento para realizar las pruebas de consumo de Recursos

Las ocupaciones a hacer para calcular el Consumo de Memoria RAM frente a la descarga de un documento son las próximas:

1. Ejecutamos la herramienta de Winbox, para ingresar remotamente al Router.

Figura 46. Icono de Herramienta Winbox

2. Ingresamos al equipo Router de Mikrotik de Winbox para hacerlo de la forma gráfica y sencilla.

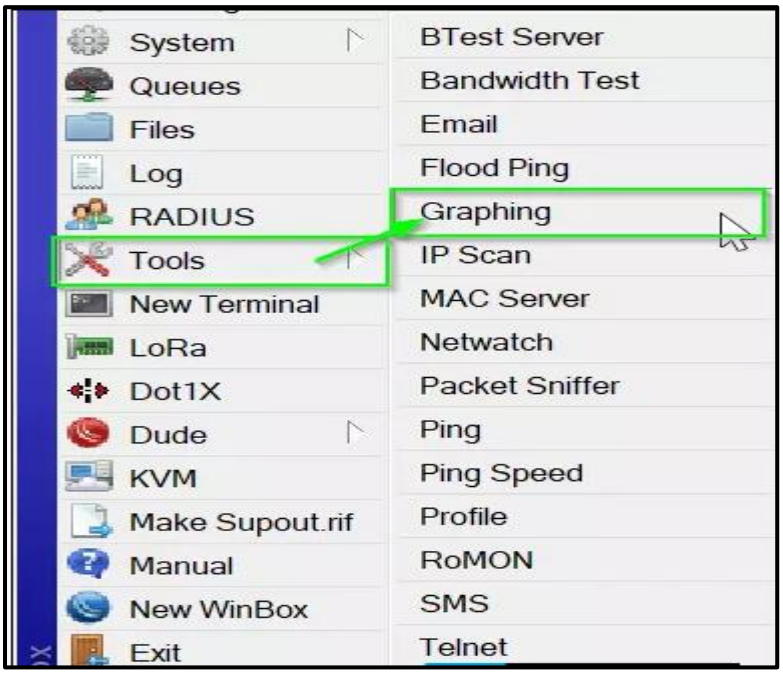

Figura 47.

3. Asignamos las próximas direcciones IP a los dispositivos, conforme con la red a cuál pertenezcan de acuerdo al siguiente detalle:

IP del Servidor : 172.16.0.1/24

4. Para visualizar los gráficos de consumo accederemos desde el navegador Web (Chrome, Microsoft Edge, Firefox…) a http://172.16.0.1/graphs/ram/

Figura 48. Gráficos de Consumo de la Memoria RAM

5. Vemos el resultado por el medio de la herramienta de Winbox

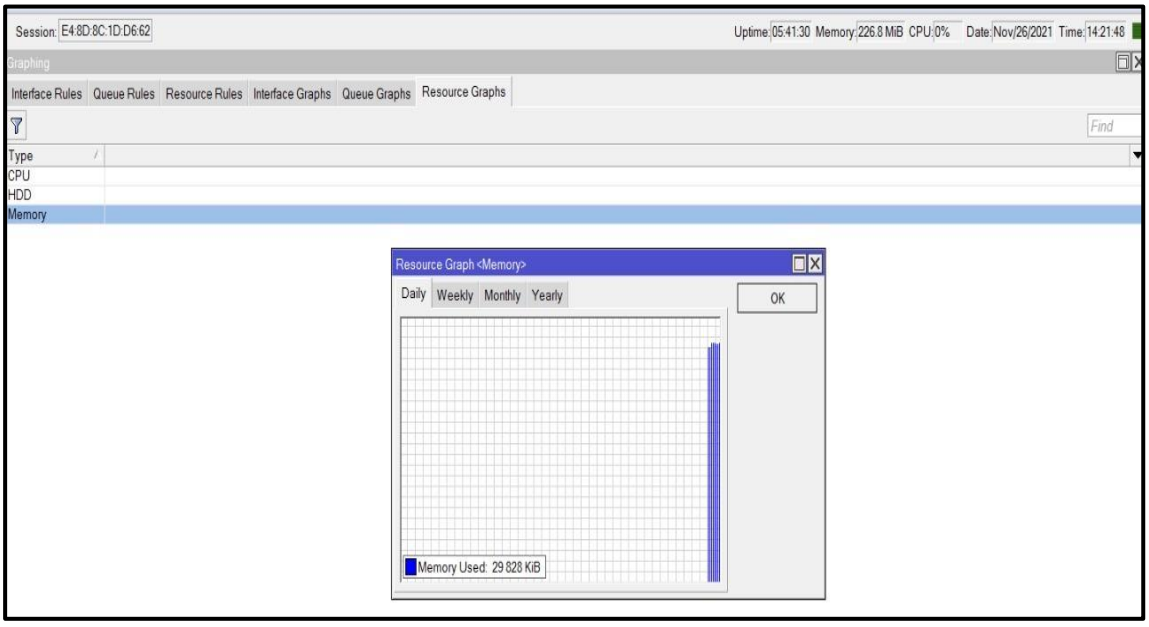

Figura 49. Gráficos de Consumo de la Memoria RAM (Winbox)

Procedimiento para realizar las pruebas de Conectividad de la Red

Las ocupaciones a hacer para calcular el Tiempo de respuesta de la red LAN frente a la descarga de un documento son las próximas:

1. La prueba para encontrar el tiempo de respuesta de la red LAN se basa en bajar en la estación de trabajo un documento situado en el servidor y calcular el tiempo de respuesta de la red LAN.
2. Asignamos las próximas direcciones IP a los dispositivos, conforme con la red a cuál pertenezcan de acuerdo al siguiente detalle:

IP servidor	: 172.16.0.5/24
IP estación de trabajo	: 192.168.10.99/24

3. Verifique que haya una conexión entre la estación de trabajo y el servidos mediante el comando ping.
4. En la estación de trabajo, presione la tecla “Windows R” y aparecerá el ejecutable.

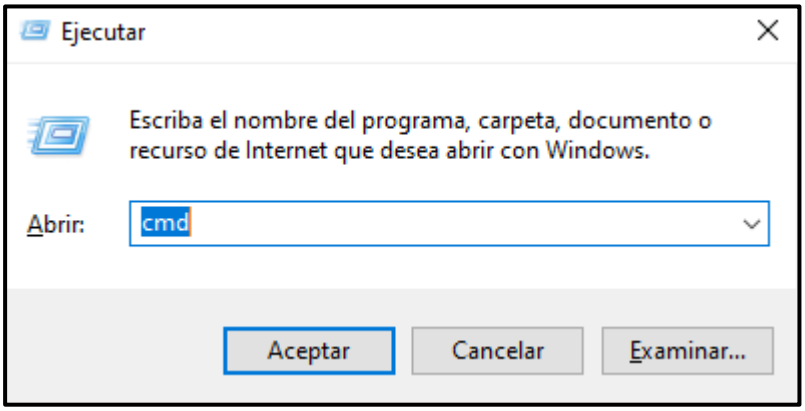

Figura 50. Herramienta Ejecutar

5. De la misma forma que se muestra en la ilustración anterior, en la herramienta de ejecución, debería redactar “CMD” para abrir el símbolo del sistema.
6. Luego de cargar la consola del signo del sistema “CMD”, debería hacer un ping junto con la dirección IP del servidor y/o estación de trabajo. Ejemplificando

7. Debería obtener una respuesta del servidor como se muestra en la ilustración anterior, de caso opuesto no va poder hacer la prueba.

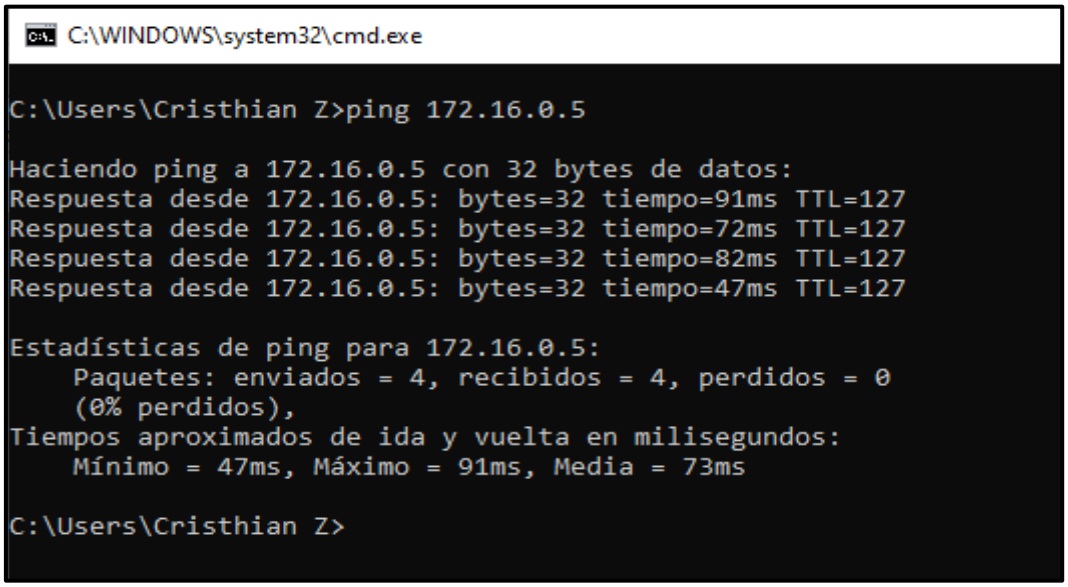

Figura 51. Prueba de conectividad al servidor

8. La herramienta utilizada en esta prueba es LAN Speed Test, esta herramienta es responsable de contar el tiempo que lleva descargar archivos del servidor.
9. Ejecute la herramienta LAN Speed Test en la estación de trabajo, realizando doble clic en el icono del escritorio.

Figura 52. Icono Lan Speed Test

10. Configure la herramienta de prueba de velocidad LAN seleccionando la alternativa “Test Read” para la medida del tiempo de transferencia de archivos a partir del servidor a la estación de trabajo.

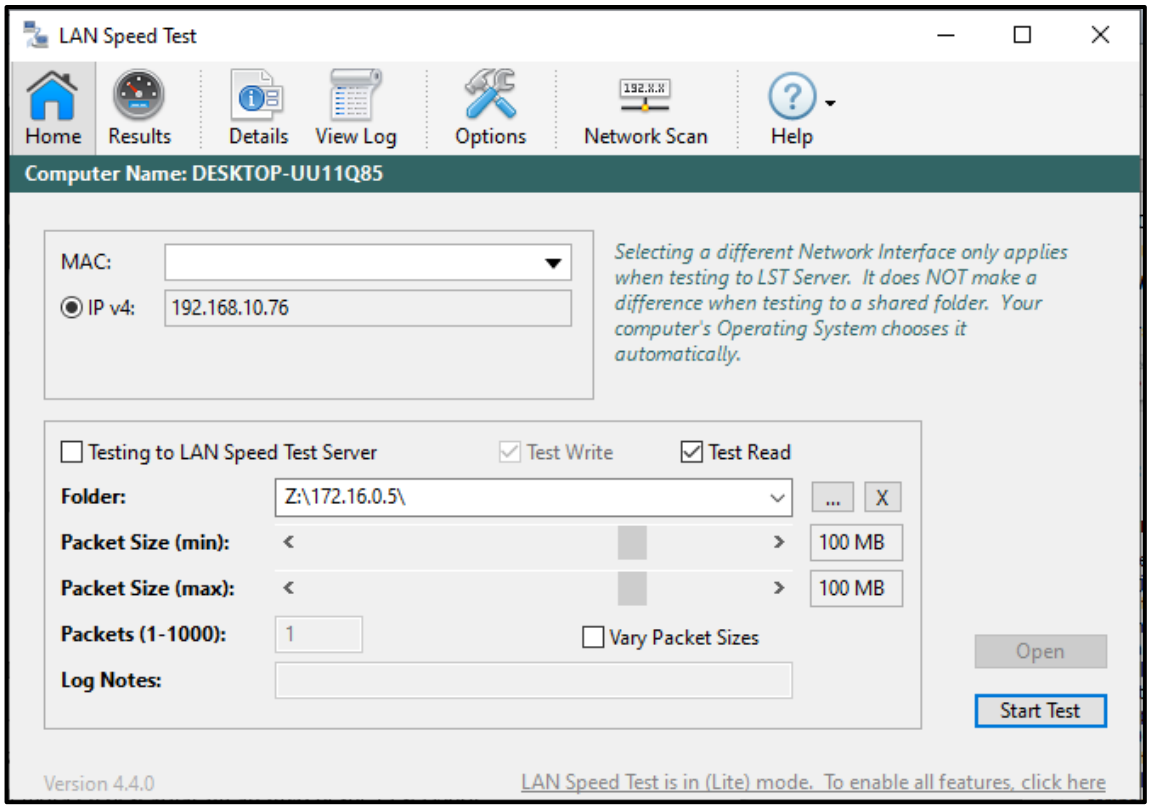

Figura 53. Plataforma Lan Speed Test

11. En el panel de control de la herramienta Lan Speed Test (Workstation), debería configurar la dirección IP del servidor en la elección “IP del servidor LST”, para indicar la localización donde se creará el archivo en el servidor. Ejemplificando \\Z:\172.16.0.5\ de la misma forma que se muestra en la ilustración.
12. Debería elegir la medida del documento a bajar a partir del servidor. En esta prueba, el tamaño de archivo que la magnitud de documento a usar es de 100 Mb (Hickman et al. 2003; p. 16).
13. Haga clic en el botón “Start Test” (Iniciar prueba) para empezar la prueba. Después aparecerá la prueba de transferencia de archivos aparecen de inmediato.

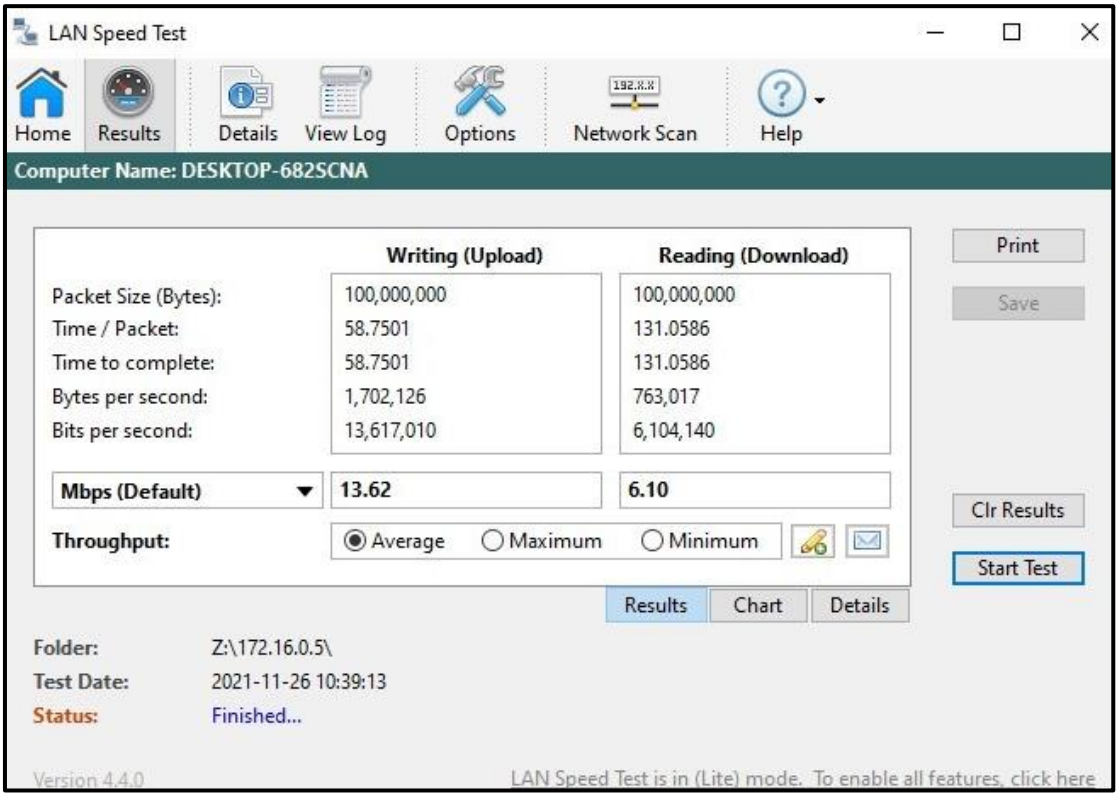

Figura 54. Lan Speed Test Resultado

14. Tomar el tiempo para descargar archivos del servidor lugar de trabajo. Para eso debería mirar la tabla que muestra los resultados de la herramienta de software Lan Speed Test y anotar el tiempo necesario para transferir archivos a partir del servidor a la estación de trabajo (Lectura – Descarga). Como se puede mirar en el ejemplo de la ilustración anterior, el tiempo es de 131.0586 segundos.
15. Hacer 50 descargar de archivos del servidor, estación de trabajo con la herramienta Lan Speed Test.
16. Registre el tiempo de todos los cincuentas (50) descarga y agrúpelas en la tabla de tabulación en la columna de prueba de conectividad.
17. La evaluación del tiempo de respuesta de la red Lan en esta implementación concluye una vez finalice al completar los cincuentas (50) descargas.