UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

# Metodología para evaluar el rendimiento de software de redes privadas virtuales.

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

Ingeniero de Sistemas


**AUTORES:**

Corpus Giraldo, Cheyer Marcelino (ORCID:0000-0002-4024-8065)

Cuentas Turpo, Anthony Santiago (ORCID:0000-0003-4230-8647)

**ASESOR:**

Dr. Liendo Arevalo, Milner David (ORCID:0000-0002-7665-361X)


**LÍNEA DE INVESTIGACIÓN:**

Auditoría de Sistemas y Seguridad de la Información

LIMA – PERÚ

2020

## Dedicatoria

Este trabajo está dedicado a mi madre Francisca Giraldo Torres y a mi padre Marcelino Julián Corpus Arias que fueron el apoyo necesario para la culminación de esta investigación. De igual modo, agradecer a mis hermanos que fueron motivo para superar las adversidades y poder cumplir mi meta. Sin ustedes nada de esto sería posible.

**CORPUS GIRALDO CHEYER MARCELINO**

Este trabajo está dedicado a mis padres y hermanos quienes me enseñaron a trazarme metas y seguirlas hasta concluirlas. De igual manera, a mis docentes, compañeros y amistades quienes me apoyaron constantemente de manera emocional y académicamente para la culminación de la investigación.

**CUENTAS TURPO, ANTHONY ANTIAGO**

**Agradecimiento**

Agradecemos cordialmente a nuestra universidad por haber permitido formarnos en sus instalaciones, asimismo, estamos agradecidos principalmente de nuestros profesores, quienes nos guiaron y apoyaron de manera continua para la realización de la presente investigación: **Dr. Liendo Arévalo, Milner David y Dr. Alfaro Paredes Emigdio Antonio**. De igual modo, **Lic. Hurtado Calvillo, Wilmer Daniel** por ofrecernos su sabiduría y experiencia en el ámbito de la ciberseguridad.

## ÍNDICE DE CONTENIDOS

## Índice de tablas

## Índice de figuras

## Índice de abreviaturas

Descripción sobre las abreviaturas o siglas con su significado y autores correspondiente al documento.

| Sigla | Significado | Pág. |
|---|---|---|
| VPN | Red Privada Virtual (Jangid y Trivedi, 2016; Lipp et al., 2019). | 19 |
| PYMES | Pequeña o mediana empresa (Wu y Xiao, 2019; Raymond, 2019; Torres y Alfaro, 2018; De la rosa, 2019; Sharma y Kaur; 2020). | 5 |
| MEPVPNS | Methodology to evaluate the performance of virtual private network software (Corpus y Cuentas, 2022). | 8 |
| L2TP | Protocolo de tunelización de capa 2 (Wu y Xiao, 2019; Aung y Thein, 2020; ExpressVPN, 2020). | 21 |
| IPSEC | Protocolo de seguridad de internet (Gunleifsen et al., 2019; Raymond, 2019; Narayan et al., 2015; Al-fannah, 2017; Aung y Thein, 2020; Juma et al., 2020; ExpressVPN, 2020). | 23 |
| PPTP | Protocolo de tunelización de punto a punto (Narayan et al., 2015; Aung y Thein, 2020; ExpressVPN, 2020). | 21 |
| TLS | Seguridad en capaz de transporte (Raymond, 2019). | 14 |
| SSTP | Protocolo de túnel de sockets seguros (Wu y Xiao, 2019; Lawas, et al., 2016; Narayan et al., 2015). | 16 |
| IKEv2 | Intercambio de claves de internet versión 2 (Lawas et al., 2016) | 16 |
| D-ITG | Generador de tráfico de internet distribuido (Wu y Xiao, 2019) | 14 |
| UDP | Protocolo de datagrama de usuario (Lawas et al., 2016; Narayan, et al., 2015) | 17 |
| TCP | Protocolo de control de transmisión (Lawas, et al., 2016; Narayan, et al., 2015) | 17 |
| VPN Remote Access | VPN de acceso remoto (Sharma y Kaur, 2020). | 22 |
| VPN site to site | VPN de sitio a sitio (Sharma y Kaur, 2020). | 22 |

| Sigla | Significado | Pág. |
|---|---|---|
| MPLS | Conmutación de etiquetas multiprotocolo (Zhipeng et al., 2018). | 23 |
| SSL | Capa de sockets seguros (Zhipeng et al., 2018). | 23 |
| HTTP | Protocolo seguro de transferencia de hipertexto (Zhipeng et al., 2018). | 124 |
| CCITT | Comité Consultivo Internacional Telegráfico y Telefónico (Wang et al., 2019). | 25 |
| ACK | Acuse de Recibo (Tamariz, et al., 2017). | 25 |
| DNS | Sistema de nombres de dominio (Oramas, p. 2, 2020; Fakis et al., 2020; Gordillo, 2017; Saras, 2015). | 35 |
| WebRTC | plataforma de código libre, capaz de facilitar la intercomunicación (audio y video) en tiempo real (Acebedo et al., 2017; Guimarey, 2017; Bhalerao et al., 2020). | 36 |
| ATM | Modo de transferencia asíncrono (Al-fannah, 2017; Li et al., 2017). | 27 |
| SONET | Red óptica síncrona (Li et al., 2017). | 27 |
| IP | Protocolo de internet (Li, et al., 2017). | 27 |
| DoS | Denegación de servicio (Biswas y Wu, 2019). | 32 |
| DDoS | Denegación de servicio distribuido (Jones et al., 2020; Salim et al., 2020) | 32 |

## Resumen

La presente investigación se desarrolló con el propósito de determinar cuáles seránlos procesos de una metodología que permitirán realizar la evaluación de los softwares de redes privadas virtuales. El tipo de investigación que se utilizará es aplicado con un diseño de investigación no experimental transversal-descriptivo. Asimismo, el enfoque fue cuantitativo, por lo que se ha hecho la utilidad de recursosestadísticos para el análisis de los resultados clave en busca de las aprobaciones de las hipótesis.

Por consiguiente, para el desarrollo de la presente investigación se eligió como muestra tres (03) softwares de redes privadas virtuales, tales como: (i) software licenciado (NordVPN), (ii) software libre (ProtonVPN), (iii) software gratuito (TunnelBear) las mismas que fueron comparadas mediante los criterios: (a) rendimiento del software (throughput, jitter), (b) administración de recursos (uso delCPU, uso de Memoria RAM, uso del Disco Duro) y (c) desempeño en la red (latencia, velocidad de descargas de archivos, velocidad de subida de archivos, ancho de banda, filtro y marcado de trafico de red, velocidad de encriptamiento dedatos, velocidad de desencriptamiento de datos, fugas de servidores DNS, fugas de dirección IP, fugas de dirección IP por WebRTC, tiempo de conexión al servidor).En consecuencia, se cumplió con todas las metas planteadas y se aceptó todas las hipótesis. En síntesis, se afirma que la aplicación de los procesos de la metodología MEPVPNS permitió determinar la evaluación de rendimiento de los softwares de redes privadas virtuales en cuanto a: (i) rendimiento del software, (ii) administración de recursos y (iii) desempeño en la red. Finalmente, se recomendóvalidar la metodología MEPVPNS ampliando sus procesos o desarrollando una nueva para entidades proveedores de medios informáticos, etc.



**Palabras claves:** MEPVPNS, metodología, evaluación de rendimiento, software vpn, redes privadas virtuales.

## Abstract

This research was developed with the purpose of determining which will be the processes of a methodology that will allow the evaluation of the virtual private network software. The type of research that will be used is applied with a non-experimental, cross-sectional-descriptive research design. Likewise, the approach was quantitative, so statistical resources have been made useful for the analysis of key results in search of hypothesis approvals.

Therefore, for the development of this research, three (03) virtual private network software was chosen as a sample, such as: (i) licensed software (NordVPN), (ii) free software (ProtonVPN), (iii) free software (TunnelBear) the same ones that were compared using the criteria: (a) software performance (throughput, jitter), (b) resource management (CPU usage, RAM memory usage, Hard Disk usage) and (c) performance over the network (latency, file download speed, file upload speed, bandwidth, network traffic filtering and marking, data encryption speed, data decryption speed, DNS server leaks, address leaks IP, IP address leaks through WebRTC, connection time to the server) Consequently, all the goals set were met and all the hypotheses were accepted. In summary, it is stated that the application of the MEPVPNS methodology processes allows determining the performance evaluation of virtual private network software in terms of: (i) software performance, (ii) resource management and (iii) performance in the net. Finally, it was recommended to validate the MEPVPNS methodology by broadening its processes or developing a new one for providers of computer media, etc.



**Keywords:** MEPVPNS, methodology, performance evaluation, vpn software, virtual private networks.

# I. INTRODUCCIÓN

En la actualidad las personas viven un aislamiento social forzado por la expansión de la enfermedad coronavirus Covid-19 a nivel mundial, haciendo que el uso de la red de internet aumente mucho más de lo que se esperaba hasta unos años en adelante (Katz, Jung y Callorda, 2020, p.3-4). Al respecto CNN (2020) manifestó que en Estados Unidos y Latinoamérica se observó un incremento considerable de usuarios conectados en el ciberespacio, debido al problema que sufre el mundo entero, presionados a realizar sus labores diarias desde casa para prevenir el contagio del Covid-19 (párr. 1). Además, los últimos estudios en base al uso de la red de internet, arrojaron como resultados que cerca del 60% de las personas en el mundo se encuentran en línea (4,5 billones de usuarios) y los especialistas indicaron que este porcentaje se incrementará a mayores proporciones en los siguientes meses del año 2020 (Wearesocial, 2020, párr. 2).

Asimismo, Reolid, Flores, Alcantud, Ayuso y Escobar (2016) mencionaron que navegar por internet haciendo uso de las redes sociales, juegos en línea y los smartphones han logrado cambiar radicalmente las maneras de intercambiar información e ideas entre las personas (p. 6). No obstante, los beneficios que brindael ciberespacio del internet no son seguros, pues la información que es transmitidadiariamente por las personas puede ser vigiladas o sustraídas sin consentimientodel usuario (Reolid et al., 2016, p. 6). Al respecto, los llamados ciberdelincuentes desarrollan técnicas y métodos capaces de sacar ventaja de las acciones que los usuarios realizan cotidianamente, vulnerando sus controles de seguridad internos, tomando provecho sobre el poco conocimiento y la insuficiente preparación para manipular las tecnologías que protegen su privacidad (Pons, 2017, p. 81).

El uso constante de la red de internet acompañado de la falta de cultura en ciberseguridad que tiene el público en general, ocasiona que los riesgos en sus diferentes actividades en línea aumenten en cantidades desproporcionadas en estos últimos tiempos; tales como: compras en línea, pagos de servicios en línea, visitas a diferentes páginas web, entre otros (Ramos, López y Torrecillas, 2018). Espor ello, que la gran mayoría de ataques en línea se atribuyen al comportamiento ydescuido del mismo usuario al navegar por la internet (como hacer clic en un enlaceo abrir un archivo adjunto) (Cyber, 2019). En síntesis, las

personas en general quemantienen un problema de dependencia indirecta a estar conectados a la red de Internet en su vida diaria; ya sea mediante un ordenador, laptop y/o diversos dispositivos móviles con el fin distraerse, comunicarse, estudiar y/o trabajar; puedenterminar siendo víctimas de fraudes o estafas, apoderándose de la información personal y confidencial del usuario (Jingyao, Chandel, Yunnan, Jingji y Zhipeng, 2019).

En consecuencia, los ordenadores y los dispositivos de comunicación manejan información confidencial y personalizada de cada individuo, esto ha hechoque la ciberdelincuencia incremente y encuentren nuevas formas de robar nuestrainformación personal o bancaria (Jingyao et al., 2019). De acuerdo a lo anterior mencionado, Jingyao et al. (2019) manifestaron que los usuarios jamás habían mostrado tanta importancia acerca de la seguridad en el ciberespacio hasta la actualidad, esto se debe al uso constante de la red de internet para realizar sus labores diarias (p. 1050) Además, Jingyao et al. (2019) indicaron que hay diversospeligros y riesgos en el espacio cibernético, capaces de afectar la estabilidad de lared privada a gran escala (p. 1050). Ciertamente, la inseguridad cibernética es un problema que afecta a todos los ciudadanos, comunidades y países enteros debidoa que se encuentran en una alta dependencia hacia las herramientas digitales pararealizar sus actividades tanto laborales, sociales y económicos (Pons, 2017).

Por otro lado, el peligro de expansión de la enfermedad Covid-19 ha generado la necesidad de implementar y monitorear protocolos, normas y políticasde trabajo con el propósito de garantizar condiciones óptimas de salud para los trabajadores de todas las organizaciones (De Lima, Chaves, Meyer, Lancman y Barroso, 2020, p. 2). En síntesis, el estado de emergencia a nivel nacional, ha forzado que cientos de establecimientos de trabajo, organizaciones y entidades a adoptar el teletrabajo haciendo uso de la red de internet y herramientas poco confiables (Katz, et al., 2020). Sin embargo, mantenerse comunicado muestra ser de vital importancia para el crecimiento de las personas u organizaciones generando competitividad y desarrollo económico. Por lo tanto, es inaceptable permanecer aislado o incomunicado con otras entidades y menos aúncon nuestras propias sucursales u oficinas (Martel, 2019, p. 4).

Al respecto, Martel (2019) recalcó que las entidades desean tener imagen como prestigio en el mundo, por lo que comúnmente se alinea y expande a nuevos puntos de acceso de diferentes distritos en nuestro país, originando necesidades de mantenernos interconectados de manera segura y manteniendo costos aceptables en el mercado con el objetivo de intercambiar información para agilizarlas tomas de decisiones en las empresas (Martel, 2019, p. 4). En otras palabras, asegurar la información que es transmitida mediante el ciberespacio es parte fundamental para las organizaciones, pues a medida que las redes transportan unamayor cantidad de información personal y bancaria; estas deben desempeñar mejorsus cualidades, como: seguridad, confidencialidad, integridad, disponibilidad yescalabilidad (Carrión, 2018, p. 15). Por ello, es infalible que todas las entidades tomen razón en la importancia de la implantación de herramientas de seguridad capaces de proteger la información que se transfiere desde el servidor central hasta las tecnologías de información del usuario, esencialmente las entidades que manipulan datos económicos y estratégicos (De la Rosa, 2019, p. 7).

En consecuencia, las organizaciones presentan problemas realizando sus labores remotas, aumentando los riesgos de seguridad de información transmitidapor internet, debido a que no hubo una correcta capacitación de información y herramientas a los colaboradores que manejan la información (Ovalle, 2019, p. 57).Por otro lado, la creciente necesidad de las empresas por realizar sus labores remotas, ha generado que los administradores de redes se interesen en tecnologíascapaces de transportar información a través de internet manteniendo la integridad, confiabilidad y accesibilidad de los datos (Ovalle, 2019). En relación con lo anterior,Sharma y Kaur (2020) enfatizó que la VPN permitirá brindar la máxima seguridad y confidencialidad de los datos que se encamina por Internet hacia o desde una oficina remota logrando el máximo de beneficios de las líneas de transporte e integrando los diferentes servicios empresariales como telefonía, data, videoconferencia etc., desarrollando soluciones que permitan usar más eficientemente los canales de comunicación (p. 2337)**.**

Dicho en otras palabras, los softwares VPN permiten mantener la privacidady estabilidad de los datos en el intercambio de información por medio del

ciberespacio de punto a punto (Martel, 2019). Además, los softwares de redes privadas virtuales tienen como finalidad mantener la privacidad de sus clientes, mediante túneles de seguridad encriptados entre la tecnología empleado por el usuario remoto, organización y el proveedor del servicio (Pandasecurity, 2017, párr.7).

No obstante, existen diferentes organizaciones que brindan el servicio de VPN gratuitos/libres como: *TunnelBear, ProtonVPN, VPNLite, Librewan VPN, OpenConnect, OpenVPN, Openswan,* etc (Av comparatives, 2020). Asimismo, otras organizaciones brindan el servicio de VPN licenciados como: *ExpressVPN, NordVPN, VyprVPN, Cyberghost, IPVanish, PrivateVPN,* etc. (Av comparatives, 2020). Se ha encontrado estudios relacionados al presente tema de investigación con criterios muy importantes que buscan examinar, evaluar y establecer los softwares de redes privadas virtuales, pero con un enfoque diferente (Pacotaype, 2018; Torres y Alfaro, 2018). Sin embargo, no existe una metodología capaz de evaluar el rendimiento de los softwares VPN y permitan disminuir considerablemente el proceso y tiempo de evaluación (Av comparatives, 2020; Pacotaype, 2018). Por ende, este estudio busca aportar en la toma de decisiones para las pymes (pequeña o mediana empresa) y grandes organizaciones acerca de la evaluación de rendimiento de los softwares VPNs, además, busca proporcionar información actualizada sobre las herramientas tecnológicas de seguridad de información en las redes privadas virtuales (Wu y Xiao, 2019; Raymond, 2019; Torres y Alfaro, 2018).

Por ello, la formulación del **problema general** es: ¿Cuáles serán los procesos de una metodología que permitirá realizar la evaluación de los softwares de redes privadas virtuales?, los problemas específicos fueron los siguientes:

- PE1: ¿Cuáles serán los procesos de una metodología que permitirá la evaluación de los softwares de redes privadas virtuales en cuanto al rendimiento del software?
- PE2: ¿Cuáles serán los procesos de una metodología permitirán realizar la evaluación de los softwares de redes privadas virtuales en cuanto a la administración de recursos?

- PE3: ¿Cuáles serán los procesos de una metodología permitirán realizar la evaluación de los softwares de redes privadas virtuales en cuanto al desempeño en la red?

La presente investigación pretende aportar al ***poco conocimiento existente***sobre una metodología para evaluar el rendimiento de los softwares VPNs, cuyos resultados podrán servir como información importante para los usuarios en general,estudiantes y profesionales relacionados con las tecnologías de información, para diferenciar entre la gran variedad de softwares VPNs que existen en la actualidad (Pacotaype, 2018; Torres y Alfaro, 2018 Martinasek, Blazek, Silhavy y Smekal, 2017). Además, adquiririnformación de las tecnologías de software VPN es de utilidad para el administrador de redes y telecomunicaciones, pues son ellos quienes deben plantear una tecnología de información capaz de agilizar y optimizar el traslado de información entre las áreas de la organización de manera segura y eficiente (Capuñay, 2016, p.39). Por otro lado, para reducir el proceso y trabajo requeridos en la implementaciónde los exámenes de rendimiento, se cuenta con tecnologías capaces de automatizar gran parte del proceso de cálculo (Verona, Pérez, Torres, Delgado y Yáñez, 2016). En síntesis, es importante manejar metodologías para evaluar el rendimiento del software y así gestionar la toma de decisiones referente a la tecnología adecuada para la entidad, por el tiempo y dificultad que implica implementarlas (Verona et al., 2016).

Aunque existen algunas fuentes de información respecto al tema, no se ha registrado una ***metodología*** de evaluación de rendimiento de software de redes privadas virtuales (VPNs) concreta y sintetizada; lo cual hace que la toma de decisiones respecto a una tecnología de VPN sea de acuerdo a la popularidad o costo de implementación, mas no en cualidades técnicas del software (De la Rosa,2019; Shim, 2020). Una metodología de evaluación de rendimiento analiza de manera exhaustiva y coordinada una serie de procedimientos sistemáticos a desarrollarse para obtener resultados más exactos (Geraldo, Soria y Tito, 2020, p.14). De igual modo, es necesario que haya conocimiento sobre las herramientas deevaluación de rendimiento para obtener resultados precisos y detallados al momento de ejecutar o lanzar un programa (Verona et al., 2016). Por ello, es necesario desarrollar una metodología en conjunta ayuda de la aplicación

de estándares, para evaluar el rendimiento de las VPNs según los indicadores tomados en la presente investigación tales como: (a) throughput, (b) jitter, (c) uso del CPU, (d) uso de la Memoria RAM, (e) uso del Disco duro, (f) latencia, (g) velocidad de descarga de archivos, (h) velocidad de subida de archivos, (i) ancho de banda, (j) filtro y marcado de tráfico, (k) velocidad de encriptamiento de datos, (l) velocidad de desencriptamiento de datos, (m) fugas de servidores DNS, (n) fugasde dirección IP, (o) fugas de dirección IP por WebRTC y (p) conexión al servidor; en búsqueda de respuestas condicionadas a situaciones y estímulos que brinden resultados con un mayor grado de precisión por ser medibles estadísticamente (Acebedo, Aznar e Hinojo, 2017, p. 108).

Por otro lado, es necesario analizar el rendimiento las VPNs gratuitas, libresy licenciadas, para poder comparar y precisar si mantienen una diferencia mayor o igual de rendimiento entre ambas categorías, posterior a ello se obtendrá opcionesde implementación de seguridad en las ***PyMES a bajo costo*** (De la Rosa, 2019). Al respecto, la información es significativa para brindar utilidades competitivas y sonmayormente las grandes organizaciones quienes manipulan enormes cantidades de datos e información de sus clientes (Sharma y Kaur, 2020, p. 2336; Chappa, 2018). Por ello, las empresas deben invertir en tecnologías de información capaz de asegurar la integridad, confidencialidad y accesibilidad a la información; en cambio las pymes no cuentan con los recursos suficientes, limitándolos a implementar tecnologías de seguridad personalizadas, simples y económicas (De la Rosa, 2019, p. 6). En síntesis, esta investigación podrá ayudar todas las empresas independientemente del tamaño de su organización, pues evitará el usode recursos económicos en tecnologías VPN costosas, mediante propuestas de software de VPN para pymes hasta grandes organizaciones a un precio razonable,manteniendo la eficiencia y seguridad en el transporte de información a través de la red de internet siendo un principio crucial para el avance social y económico (De la Rosa, 2019; Sharma y Kaur, 2020).

La metodología propuesta en la presente investigación permitirá evaluar las***tecnologías de software de redes privadas virtuales***, la misma que será capaz de favorecer el incremento de ventajas competitivas en la empresa, logrando avances importantes después de ponerlo en marcha, facilitando las

labores de sus colaboradores e innovando en el mercado competitivo (Chappa, 2018, p. 26). Al respecto, Chappa indicó que en los últimos años las tecnologías de información han logrado una mayor adopción en las organizaciones debido a las ventajas competitivas que estas brindaban como resultado (Chappa, 2018, p. 26). Asimismo, los equipos y componentes desusados fueron sustituidos por nuevas tecnologías capaces de optimizar los procesos del negocio, para innovar y liderar en el mercado(Chappa, 2018, p. 26). En síntesis, la falta de información respecto al software VPNhace que las personas no puedan explotar al máximo esta tecnología, en la mayoríade las ocasiones las aplicaciones y/o programas son usadas e implementadas sin entender o comprender las bases y las funciones que estas pueden realizar o se destacan del resto (Khan, Deblasio, Voelker, Snoeren, Kanich y Vallina, 2018, p. 454; Marqués, 2016).

**El objetivo general** de la investigación fue determinar cuáles serán los procesos de una metodología que permitirá la evaluación de rendimiento de los softwares de redes privadas virtuales. De acuerdo a ello, Acosta, Espinel y García (2017) mencionaron para identificar un software de calidad es fundamental tener un marco metodológico en base a estándares con el fin de estimar las capacidadesy características, para luego seleccionar un software acorde a las necesidades y requerimientos de los usuarios (p. 83).Teniendo en cuenta lo antes mencionado y al no existir una metodología capaz de evaluar el rendimiento de los softwares VPNs, se propondrá "*MEPVPNS*" una metodología para evaluar el rendimiento de los softwares de redes privadas virtuales en base a estándares.

No obstante, para dar respuesta al objetivo general, se desarrollaron previamente los **objetivos específicos** de la investigación, las mismas que fueronlos siguientes:

- OE1: Determinar cuáles serán los procesos de una metodología que permitirá la evaluación de los softwares de redes privadas virtuales en cuanto al rendimiento del software.
- OE2: Determinar cuáles serán los procesos de una metodología que permitirá la evaluación de los softwares de redes privadas virtuales en cuanto a la administración de recursos.
- OE3: Determinar cuáles serán los procesos de una metodología que

permitirá la evaluación de los softwares de redes privadas virtuales en cuanto al desempeño en la red.

Por ello, **la hipótesis general** planteada en la presente investigación fue: La aplicación de los procesos de la metodología MEPVPNS permitirá determinar la evaluación de rendimiento de los softwares de redes privadas virtuales. Al respecto, Pacotaype (2018) indicó que la aplicación de una metodología para la evaluación de rendimiento del firewall llamada MERF, permitió determinar que los cortafuegosen base a hardware cuentan con un mejor rendimiento que los cortafuegos en basea software (p. 106). Asimismo, Bravo (2015) manifestó en su investigación que el uso de la metodología Cisco (Top-Down Network Design) permitió organizar, detallar y ejecutar los procesos necesarios para alcanzar los objetivos planteados en el proyecto de su organización, mediante un diseño de red en conjunto de políticas de seguridad e incremento del nivel de rendimiento (p. 76). Como resultado de las pruebas desarrolladas en las máquinas virtuales se pudo demostrar satisfactoriamente que el uso de la metodología permitió disminuir el tráfico de red(de 59% a 18%) logrando demostrar la efectividad de una metodología para la gestión y monitoreo de un proyecto (Bravo, 2015, p. 76; Segura y Ramírez, 2018, p. 48).

León (2018) al implementar un software gratuito en una entidad indicó como resultados que la disponibilidad, velocidad y fluidez en el traslado de información dentro y fuera de la organización no registraba un alto índice de latenciao retardos al momento de consultar, compartir o descargar archivos de la organización (León, 2018, p. 168-169; Kumar y Majeed, 2018). Sin embargo, los especialistas de la revista MacWorld mencionaron que los servicios que ofrecen lossoftwares de redes privadas virtuales gratuitas/libres son inferiores en comparacióndel software de redes privadas virtuales licenciados (Macworld, p. 74, 2020; Wolfinbarger, 2018, p. 14).

En referencia a lo anterior mencionado, el software de redes privadas virtuales gratuitas y/o libres no son recomendables para organizaciones de gran escala, debido a su baja seguridad y privacidad de los datos que viajan a través deinternet. Además, se debe considerar que existen opciones de VPN licenciadas que ofrecen el mismo servicio con tarifas estándar con soporte y actualizaciones continuas (Shim, 2020, párr. 133; Phelan, 2019, p. 40; Macworld,

p. 72, 2020). Asimismo, para dar respuesta a la hipótesis general, se desarrollaron previamente las **hipótesis específicas** de la investigación, las mismas que se presentan a continuación:

La aplicación de los procesos de la metodología MEPVPNS permitirá la evaluación de los softwares de redes privadas virtuales en cuanto al **rendimiento del software**. En relación a ello, Lucena (2019) manifestó que el rendimiento de software se calcula con los resultados que arroja un sistema al ser sometido un estrés por la sobrecarga de trabajo al mismo tiempo, con el fin de calcular: (a) velocidad, (b) tiempo (Lucena, 2019, párr. 2). Al respecto, Wolfinbarger (2018) indicó que los proveedores de redes privadas virtuales (ExpressVPN y NordVPN) sobresalen en cuanto a la velocidad de transferencia de datos y desempeño en la red (p. 14). Por otro lado, el número de servidores es un aspecto fundamental cuando se dispone a elegir un servicio de redes privadas virtuales, debido a que el usuario no estará en la obligación de establecer una conexión a un servidor saturado donde el traslado de información muestra retrasos (Wolfinbarger, p. 73, 2018; Ian, p. 77, 2021; PCMag, 2020; Phelan, 2019, p. 40,).

En relación a ello, los especialistas de Av comparatives (2020) realizaron una comparación de 35 software de redes privadas virtuales para Windows indiscriminadamente, concluyendo que los softwares de redes privadas virtuales licenciadas (Trust.Zone VPN, SaferVPN y Surfshark) tuvieron un rendimiento superior y demostraron una gran diferencia en las velocidades de descarga en comparación al resto (Av comparatives, 2020). En síntesis, la experiencia que te ofrece el software de redes privadas virtuales gratuitos en cuanto al desempeño en la red es poco rentable en comparación a las redes privadas virtuales licenciadas por la velocidad en la transferencia de datos en tiempos cortos, a través de protocolos que aseguran la privacidad de información (Phelan, 2019; Wu y Xiao, 2019, Lawas, Vivero y Sharma, 2016; Ian, p. 77, 2021).

La aplicación de los procesos de la metodología MEPVPNS permitirá evaluarlos softwares de redes privadas virtuales en cuanto a la **administración de recursos**. Al respecto, Gunleifsen, Kemmerich y Gkioulos (2019) mencionaron que,para el análisis y administración de recursos, es necesario medir el consumo de la CPU con la herramienta nmon y el consumo de la memoria RAM con la

herramientafstab. Asimismo, en el estudio realizado en el sistema operativo Windows en base al protocolo IKE SA (IKEv1) mantiene un alto índice frente al uso de recursos de SD-SA con una diferencia de 28.5% (Gunleifsen et al., 2019). Por otro lado, en el sistema operativo Linux (kernel) enfocado a monitorear el rendimiento del CPU ante el tráfico de datos encriptados, muestra como resultados que en el proceso de cifrado y descifrado de paquetes el consumo de CPU alcanza un nivel mayor al 90% (Gunleifsen et al., 2019).

Referente a lo anterior mencionado, exponer una máquina que hace uso delos canales VPNs ante un ataque DDoS incrementara el uso de los recursos (CPUy memoria RAM) afectando a los protocolos: (a) IPSEC/IKE, (b) IPSEC/SD-SA entre otros medios de cifrado y autenticación de información IPSEC (Gunleifsen et al., 2019). En relación a ello, Caprolu, Raponi, Oligeri y Di Pietro (2019) realizaron un estudio cuyo propósito fue detectar y determinar las actividades de cifrado confiando únicamente en el tráfico de la red, utilizando software de redes privadasvirtuales (NordVPN v. 1.2.0 y ExpressVPN v. 1.5.0), demostrando el alto consumo de recursos, tanto en CPU, GPU y memoria de una máquina de destino al momento de intento de ser víctima de ataques cibernéticos/robo de información. Asimismo, recomendaron gestionar el acelerador del CPU y requerir privilegios para ejecutar procesos con un índice elevado del consumo de CPU (Caprolu et al., 2019; Martinasek et al., 2017; Lawas, et al., 2016).

La aplicación de los procesos de la metodología MEPVPNS permitirá evaluar los softwares de redes privadas virtuales en cuanto al **desempeño en la red**. En relación a ello, los especialistas de la ISO/IEC 27033-5:2013 tiene como objetivo detallar las normas y políticas de selección, ejecución y verificación de la gestión técnica imprescindible para ofrecer seguridad en la red a través de una red privada virtual para permitir la comunicación entre diferentes puntos del mundo de manera segura y remota (ISO, 2019; Sennewald y Baillie, 2020).

Por otro lado, Rob (2019) mencionó que los principales problemas al elegir un software VPN son: (a) no ser capaces de asegurar la privacidad de sus clientes, (b) rastrear rutinas de navegación de sus clientes y comercializar los datos para conseguir ingresos, (c) no especificar los protocolos y políticas de cifrado de información y (d) no ofrecer soporte ante problemas de seguridad (p.

23). Por ello, la seguridad queda comprometida frente a los fraudes tanto de proveedores como ciberdelincuentes que buscan obtener ganancia a falta de conocimiento de los cibernautas (Rob, 2019).

Wolfinbarger (2018) indicó que la seguridad incompleta y la falta de cifrado hacen que la información que se envía a través de los softwares de redes privadasvirtuales gratuitas/libres puedan quedar expuestas en la red. Además, Wolfinbarger(2018) mencionó que al emplear software VPN licenciados pueden asegurar la trasferencia de información, por medio de conexiones seguras y estables (Wolfinbarger, 2018, p. 14; Rob, 2019, p. 23). Sin embargo, los proveedores de software VPN tanto libres, gratuitos y licenciados buscan satisfacer constantemente los requerimientos de seguridad para sus clientes (Phelan, 2019; De la Rosa, 2019,p. 45).

# II. MARCO TEÓRICO

En esta parte del trabajo de investigación, se mencionaron los trabajos anteriores que muestran similitud sobre el tema presente de investigación. Para encontrar dicha información se consultaron diversos estudios entre artículos, tesis, revistas, entre otros.

Wu y Xiao (2019) estudiaron el impacto del rendimiento con diferentes topologías de red VPN formada entre servidores para demostrar el efecto en la calidad del servicio VPN en Chengdu, China. Wu y Xiao (2019) estructuraron la metodología en: (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). Empleado en cuatro criterios: rendimiento, latencia de red, fluctuación de fase y tasa de pérdida de paquetes (PLR). Para construir la red privada virtual se aplicó la herramienta de código abierto Softether, proyecto de investigación de la Universidad de Tsukuba en Japón. El software se compone de dos partes: concentradores virtuales y adaptadores virtuales; capaz de enviar y recibir flujos de datos para obtener datos de prueba relacionados con el rendimiento que se aplicó con la herramienta D-ITG (Generador distribuido de tráfico de Internet). Asimismo, Wu y Xiao (2019) concluyeron que el rendimiento del Softether y el SSTP/L2TP son básicamente el mismo en términos de rendimiento. Además, Wu y Xiao (2019) recomendaron que en el futuro se adopte una topología de estrella o una topología de árbol, y el número de capas de la topología del árbol no exceden las tres capas. De este antecedente se tomó la funcionalidad de las herramientas para la evaluación y la topología de red.

En Estados Unidos, Raymond (2019) estudió el efecto de determinar un protocolo óptimo para su uso en la protección de redes privadas virtuales, para que las empresas entiendan qué protocolos funcionan en el software de seguridad comercial. Raymond (2019) estructuró la metodología en: (i) metas, (ii) protocolos: descripción, ventajas y desventajas, (iii) resultados. Esta no es una evaluación del funcionamiento funcional del protocolo, instalación, mantenimiento y rendimiento, sino que es un análisis de la fortaleza de la defensa de la red. Asimismo, Raymond (2019) concluyó que todos los protocolos revisados proporcionan soluciones de seguridad y son producidos en entorno de red de producción. Además, los protocolos IPsec y OpenVPN operan en la capa

3 del modelo OSI, el TLS opera en la Capa 4 del modelo OSI. Sin embargo, el IPsec no puede proporcionar un túnel físico y lógico, un requisito para las redes privadas virtuales, el L2TP requiere autenticación/login, por lo que está operando una Capa 5 del Modelo OSI y no proporciona seguridad a nivel de máquina. Esto hace que OpenVPN sea una clara elección en esta dimensión. Raymond (2019) recomendó que en el futuro se debe comprender las consecuencias de la retirada de TLS e IPsec, cuando consideren la implementación de OpenVPN.

En México, León (2018) estudió el efecto de una implementación de una VPN y monitoreó su rendimiento con el objetivo de consolidar la estabilidad y evitar DoS de usuarios ajenos a la organización capaz de vulnerar la integridad de la información de los involucrados. León (2018) estructuró la metodología en: (i)Requisitos Técnicos, (ii)Análisis de costos, (iii)Factibilidad, (iv) Proceso general del Proyecto y (v) Proceso de Desarrollo. Para evaluar el rendimiento, auditoria y gestión de redes se utilizó las herramientas OpenVPN y el sistema Pfense con el fin de establecer redes estables entre diferentes puntos externos a la organización y al área principal de la empresa por medio del internet. Asimismo, León (2018) concluyó que al implementar redes privadas virtuales generó equilibrio en su productividad mediante el transporte de información segura. De este antecedente se tomó la metodología de recolección de datos para evaluar el rendimiento y desempeño de las redes virtuales privadas.

En Múnich, Alemania. Martinasek et al. (2017) estudió el impacto de la implementación de una metodología para el análisis de registro de seguridad para detectar un incidente y generar una respuesta adecuada para mitigar las pérdidas. Martinasek et al. (2017) estructuraron la metodología en dos bloques básicos: proceso de análisis de riesgo y proceso de identificación de registros. Para evaluar el proceso de riesgo es necesario: (a) análisis del sistema, (b) identificación de los activos, (c) análisis de la amenaza, (d) análisis de los ataques y (e) análisis de las vulnerabilidades. Para evaluar el proceso de identificación de registros es necesario: (i) determinar las categorías de mecanismo de amenaza, (ii) definiciones de vectores de ataque, (iii) identificación de eventos y sus correlaciones, (iv) propuesta de registros. Asimismo, Martinasek et al. (2017) concluyeron que la metodología propuesta puede ser empleado para ayudar a la correcta implementación del SIEM o para identificar los eventos específicos que se desean para el análisis de seguridad

del dispositivo criptográfico. De este antecedente se tomó procesos metodológicos de análisis de riesgo e identificación de ataques en las redes virtuales privadas para el desarrollo de la tesis.

En Latacunga, Ecuador. Oña (2016) estudió el efecto de una implementación de una red privada virtual donde analizó e implementó un prototipo de estabilidad en la red y la seguridad de los datos ante usuarios no autorizados que podrían alterar o eliminar la información que maneja la entidad. Oña (2016) estructuró la metodología en: (i) estudio de factibilidad, (ii) requerimiento, (iii) implementación y (iv) fase de diseño. Para demostrar la seguridad, estabilidad y costo se aplicó las tecnologías de información de redes privadas virtuales. Asimismo, Oña (2016) concluyó que las redes privadas virtuales proporcionan seguridad en la navegación y datos creando un túnel de seguridad el cual está compuesto por certificados que ayuda a que los intrusos existentes dentro de la nube se mantengan al margen de la red. De esta investigación se rescató la observación y los resultados arrojados para el desarrollo del presente trabajo de tesis.

En Hyderabad, India. Lawas et al. (2016) estudiaron el efecto de evaluación del rendimiento de los protocolos VPN, principalmente el Protocolo de túnel de sockets seguros (SSTP) y el (IKEv2). Lawas, et al. (2016) estructuraron la metodología en: (i) requerimientos del sistema, (ii) roles, (iii) herramienta e (iv) implementación. Empleado en tres criterios: (i) rendimiento, (Ii) fluctuación de fase y (iii) retraso. Para evidenciar la medición del rendimiento y generar el tráfico de la red se aplica herramientas tecnológicas como el Generador de Tráfico de Internet Distribuido (D-ITG). Además, puede generar tanto el tráfico del Protocolo de Control de Transmisión como el del Protocolo de Datagrama Usado, que da resultados de prueba de rendimiento, fluctuaciones, demoras y pérdida de paquetes. Asimismo, Lawas, et al. (2016) concluyeron que el rendimiento de TCP de IKEv2 es ligeramente mayor que SSTP mientras está en UDP, mientras que IKEv2 es ligeramente menor que SSTP, con una diferencia de menos del 1%. El rendimiento de TCP SSTP varía de 9Mbps a 89Mbps, mientras que IKEv2 varía de 10Mbps a 90Mbps. El rendimiento UDP de SSTP varía de 5Mbps a 90Mbps, mientras que IKEv2 varía de 6Mbps a 89Mbps. De este antecedente se tomó el análisis para medir el rendimiento de

los protocolos VPN y la funcionalidad de la herramienta D- ITG para medir latencia y jitter.

En Coimbatore, India. Narayan, Williams, Hart y Qualtrough (2015) estudiaron el impacto de evaluación de rendimiento de tres protocolos de VPN (PPTP, IPSec, y SSTP) en un entorno de red cliente/servidor de Windows 7 y Windows 2012 sobre medios alámbricos e inalámbricos (Ethernet e IEEE802.11ac) usando ambas versiones de IP y observar su desempeño. Narayan et al. (2015) estructuraron 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 (Protocolo de Control de Transmisión) como el UDP (Protocolo de Datagrama de Usuario). Asimismo, Narayan et al., (2015) 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.

Carrión (2018) estudió el efecto de la implementación de una metodología adaptiva a base de la seguridad informática en redes privada virtual en la Universidad Nacional Pedro Ruiz Gallo. Carrión (2018) utilizó como muestra un total de 32 empleados de la Universidad Nacional Pedro Ruiz Gallo y del área Académica del Centro Pre Universitario. La metodología es denominada adaptiva y propone una metodología de investigación cuantitativa explicativa. Como resultado del estudio se concluyó que la determinación del proceso de estabilidad tecnológica, argumentó que las entidades necesitan protección en la red que transfieren sus datos. Asimismo, Carrión (2018) recomendó que en el futuro se evalué el método para el transporte de información por medio de VPNs asegurando los datos de la organización que viajan a través de ella. De esta investigación se tomó la información explicita y la metodológica para el desarrollo de la tesis.

Pacotaype (2018) estudió el efecto de la implementación de una metodología para la evaluación de rendimiento de Firewall para determinar que los Firewalls de hardware tienen mayor rendimiento que los Firewalls de software. Pacotaype (2018) utilizó como muestra cuatro firewalls, dos firewalls son de hardware y dos firewalls son de software y sus marcas respectivamente son Paloalto, Fortinet, Endian y Sophos. La metodología se estructuro en (a) objetivo, (b) alcance, (c) comparación de metodologías existentes, (d) fases de la metodología. De igual modo, se propusieron tres criterios de evaluación: desempeño de red (i), eficacia de los resultados (ii) y consumo de recursos (iii). El estudio concluyó que la aplicación de una metodología para la evaluación de rendimiento de Firewalls sí permitió determinar que los Firewalls de hardware (Paloalto y Fortinet) tienen mayor rendimiento que los Firewalls de software (Endian y Sophos). Asimismo, Pacotaype (2018) recomendó que en el futuro se evalué el throughput utilizando herramientas de hardware que generan gran volumen de tráfico de red, con la finalidad de evaluar equipos Firewalls de mayor performance. De este antecedente se tomó los procesos metodológicos para el desarrollo de la investigación, debido a los procesos de normalidad de Kolmogorov-Smirnov y Shapiro-Wilk para muestras de datos.

Torres y Alfaro (2018) estudiaron el efecto de la implementación de una metodología para la evaluación de rendimiento de los servidores de correo electrónico y comparar el rendimiento del correo electrónico. Torres y Alfaro (2018) utilizó como muestra cuatro servidores, dos servidores de correo electrónico con licencia gratuita (Sendmail y Postfix) y dos servidores de correo electrónico con licencia de pago (Microsoft Exchange y Lotus Domino). La Metodología se describió considerando los siguientes aspectos: (a) propósito de la metodología, (b) alcance de la metodología, (c) comparación con las metodologías existentes, (d) procedimientos de la metodología y (e) prueba de la metodología. Empleado en tres criterios: (i) capacidad antispam, (ii) filtro antivirus y (iii) consumo de recursos del servidor contra gran volumen de mensajes, con un diseño experimental. Torres y Alfaro (2018) concluyeron que la aplicación de una metodología permitió efectuar la comparación de los resultados obtenidos en lo que concierne a consumo de recursos del servidor ante gran volumen de mensajes, de esta manera se determinó que los servidores de correo electrónico basados en software libre (Sendmail y Postfix) tienen

mayor rendimiento que los servidores de correo licenciados (Microsoft Exchange y Lotus). Asimismo, Torres y Alfaro (2018) recomendaron que en el futuro se evalué los indicadores de rendimiento con múltiples conexiones a los servidores de correo electrónico implementados. De este antecedente se tomó las medidas de los indicadores para el desarrollo de la tesis.

En este apartado del documento, se brindó una definición de los términos que fueron utilizados a lo largo del presente trabajo de investigación. Asimismo, estas definiciones fueron presentadas con sus respectivas bases teóricas fundamentadas por autores acerca de las redes privadas virtuales.

**Metodología**

La metodología es el conjunto ordenado de métodos, procedimientos y normas correctamente definidas para lograr los objetivos, apoyadas en base a estándares referentes al tema elegido (Pacotaype, 2018; Acosta, Espinel y García, 2017). En síntesis, se denomina metodología a la serie de pautas, acciones y técnicas estandarizadas orientadas a lograr identificar el problema o resolverlo directamente para obtener conocimiento (Pacotaype, 2018, p. 123; Acosta, Espinel y García, 2017).

**Redes privadas virtuales**

Jangid y Trivedi (2016) definiendo la VPN como arquitecturas de red más seguras y escalables, puesto que proporcionan más utilidades a las entidades en sus sistemas, para interconectar trabajadores remotos de una manera más sencilla y económica (p. 97). La seguridad que mantiene las redes privadas virtuales usa protocolos de identificación y encriptado de datos e información al ser transportado de un punto a otro, brindando acceso únicamente a los usuarios autorizados (Jangid y Trivedi, 2016, p. 98).

Jahan, Rahman y Saha (2017) infirieron “la red privada virtual (VPN) se usa ampliamente en redes empresariales y domésticas” (p. 41). Es por ello, que las VPN tienen la funcionalidad de poder alojarte en distintas plataformas por medio de servidores que trabajan a nivel mundial (Jahan, et al., 2017). Asimismo, Lipp,

Blanchet y Bhargavan (2019) infirió que transportar datos por un canal público haciendo uso de las redes privadas virtuales garantizaran la integridad y confidencialidad la información mediante protocolos de seguridad (p. 231). Dicho en otras palabras, se considera que las VPNs tienen protocolos que cumplen las políticas para cuidar la información de cada usuario (Lipp, et al., 2019, p. 232).

**A. Direccionamiento**

El direccionamiento es parte fundamental en el transporte de información a través de Internet hacia un punto específico, haciendo uso de los protocolos TCP/IP para encubrir los datos (Florea, Rughinis, Ruse y Dan, 2017). Al respecto, Florea et al. (2017) mencionó que el protocolo IP proporciona información del punto de cohesión con la interfaz física. Las tecnologías de información mantienen interfaces físicas que comúnmente son distintas, pero estas pueden ser capaces de dividirse y distribuir interfaces lógicas para cada uno de ellos, haciendo uso de su misma dirección IP (Florea, et al., 2017). En conclusión, el direccionamiento es la función principal de los protocolos que permite el traslado de datos a través de la red (Florea, et al., 2017).

**B. Funcionalidad**

La funcionalidad de las VPN son procesos esenciales para permitir el manejo de transferencia de datos sin latencias o retardos con el objetivo de enlazar una red a otra de manera segura y protegida (Wu y Xiao, 2019). Al respecto, Redžović, Smiljanic y Savic (2016) explicó que la información que viaja por medio de una red privada virtual realizan los siguientes procedimientos: (a)enviar la información a través de la red de la empresa al Firewall, (b) el Firewall admite la salida de información y la traslada a la red de internet, (c) el servidor de la VPN genera un túnel para trasladar los paquetes de datos encriptados mediante el internet de manera estable y veloz hacia el punto destino, (d)descifra y lee los datos para garantizar una entrega integra de información al usuario remoto (Wu y Xiao, 2019; Redžović, Smiljanic y Savic, 2016, p. 2).

Por lo tanto, indicó las redes privadas virtuales son capaces de unir las agencias corporativas con los interesados, proveedores y trabajadores remotos a través protocolos como Internet, IP, IPSec, Frame Relay, ATM (Al-fannah, 2017, p. 3). Además, se considera que las redes privadas virtuales están capacitadas para

mantener una conexión rápida y segura para el traslado de datos haciendo uso de cifrados robustos (Al-fannah, 2017, p. 3).

### Protocolos de redes privadas virtuales

Respecto a la clasificación de protocolos de redes privadas virtuales (VPN), existen 3 protocolos de VPN: IPSEC, PPTP/MPPE y L2TP/IPsec (Aung y Thein, 2020, p. 5). En el párrafo posterior se realizó una breve descripción de cada una de ellas para identificar algunas ventajas y características individualmente.

### A. Protocolo de seguridad de internet

El protocolo IPsec permite aumentar la estabilidad de la información por medio de encriptamiento fuerte y un sistema de identificación más completo (Juma, Monem y Shaalan, 2020). Al respecto, Juma, et al. (2020) indicaron que el Protocolo de seguridad de Internet emplea dos maneras de encriptación, como: (i) modo transporte y (ii) modo túnel (p. 5). Además, el Protocolo de seguridad de Internet garantiza la comunicación y seguridad en el intercambio de información sobre el protocolo de internet (ExpressVPN, 2020).

### B. Protocolo de tunelización de punto a punto

El protocolo PPTP es una tecnología capaz de mantener diversos protocolos de redes privadas virtuales con encriptaciones (40 bits a 128 bits) empleando el protocolo MPPE, pues el protocolo de tunelización de punto a punto no es capaz de encriptar por sí mismo la información (Narayan, Ishrar, Kumar, Gupta y Khan, 2016, p. 3). Sin embargo, el PPTP es vulnerable a diversos ataques de seguridad, pues sus etiquetas para la identificación (MS-CHAP) son inestables por la falta de mantenimiento de sus sistemas (ExpressVPN, 2020, párr. 3).

### C. Protocolo de tunelización de capa 2

El protocolo L2TP brinda el servicio de envió de información por un túnel haciendo uso del protocolo IPsec para encriptar los datos durante el transporte IPsec, pues al igual que PPTP, L2TP no es capaz de encriptar por sí mismo la información (Aung y Thein, 2020, p. 2). En conclusión, el protocolo de tunelización de capa 2 está definido en diversos paquetes de datos para asegurar la comunicación, sin embargo, mantiene reiterados incidentes con el

firewall bloqueando su entrada y salida, pues utilizan el puerto UDP 500 (Aung y Thein, 2020, p. 2; ExpressVPN, 2020).

## Tipos de Redes Privadas Virtuales (VPN) comunes

Respecto a la clasificación de VPN, Sharma y Kaur (2020) indicó que existen 2 tipos de redes privadas virtuales comunes: (a) remote access, (b) site to site (Sharma y Kaur, 2020, p. 2337). En el párrafo posterior se realizó una breve descripción de cada una de ellas para identificar algunas ventajas y características individualmente.

### A. Conexión "remote access"

Respecto a las VPN de acceso remoto, Sharma y Kaur (2020) mencionaron que permite enlaces estables y encriptados, entre los usuarios externos y el servidor central de la organización desde un servicio mediador externo (p. 2337). En otras palabras, la conexión de acceso remoto admite el emparejamiento de los usuarios ubicados en cualquier parte del mundo y la red privada de la empresa (Sharma y Kaur, 2020, p. 2337).

### B. Conexión "site to site"

Respecto a las VPN de sitio a sitio, Sharma y Kaur (2020) expresó que una red privada virtual implementada para la interconexión entre las áreas de una misma organización es también llamada intranet, sin embargo, una red privada virtual desarrollada para enlazar la organización con su colaborador o usuario interesado es nombrado extranet (Sharma y Kaur, 2020, p. 2337). Además, al utilizar hardware exclusivo y encriptamiento de un mayor nivel, una entidad es capaz de vincular diferentes puntos fijos mediante redes públicas (Sharma y Kaur, 2020, p. 2337).

## Tipos de redes privadas virtuales

Respecto a la clasificación de tipos VPN, Zhipeng, Chandel, Jingyao, Shilin, Yunnan y Jingji (2018) mencionaron que existen 3 tipos de VPN: VPN MPLS, VPN SSL y VPN IPsec (p. 511). En el párrafo posterior se realizó una breve

descripción de cada una de ellas para identificar algunas de sus ventajas y desventajas individualmente.

### A. VPN MPLS

Es la agrupación de la IP VPN (Red Privada Virtual IP) con el mecanismo de transporte de datos estándar MPLS, para el direccionamiento e interconexión de los equipos mediante la red; VPN MPLS es capaz de reducir las rutas de los equipos centrales encargados del enrutamiento haciendo uso de los distintivos del enrutamiento tradicional (Zhipeng et al., 2018). Al respecto, Zhipeng et al. (2018) expresaron que lo mejor de MPLS es que utiliza una combinación de tecnología de comunicación y direccionamiento que proviene de las capas (2 y 3) de la tecnología OSI que produce un alto rendimiento al abordar los problemas importantes de VPN, como la clasificación de servicios e ingeniería de tráfico. (p. 511). Dicho en otras palabras, son procesos flexibles para la manipulación y enrutamiento de transferencia de datos permitiendo la comunicación entre diferentes puntos (Zhipeng et al., 2018).

### B. VPN SSL

De acuerdo a VPN SSL, Zhipeng et al. (2018) definieron: “SSL (Secure Sockets Layer) VPN es una tecnología VPN basada en HTTPS (Secure HTTP que admite el protocolo SSL HTTP) y se ejecuta entre la capa de transporte y la capa de aplicación de las capas OSI” (p. 511). En otras palabras, se refiere a una VPN (Red Virtual Privada) capaz de utilizar el protocolo cifrado SSL (Secure Sockets Layer) con el propósito de asegurar el traslado de información mediante la red de Internet (Zhipeng et al., 2018). En relación a lo anterior mencionado, “el uso de SSL VPN se realiza principalmente en el acceso de seguridad remoto basado en la web. Se asegura de que los usuarios obtengan seguridad remota al acceder a la red privada de la entidad” (Zhipeng et al., 2018, p. 511).

### C. VPN IPsec

En cuanto a la VPN IPsec, Zhipeng et al. (2018) señalaron “La base de IPSec VPN es el protocolo IPSec (Internet Protocol Security), que proporciona la seguridad del túnel. IPSec es un enfoque integral diseñado por IETF (Internet Engineering Task Force)” (p. 511). Asimismo, “proporciona un paquete de

protocolos como el Protocolo de administración e intercambio de claves IPsec (ISAKMP) para la administración de claves, que especifica la negociación y el establecimiento de la seguridad" (Raymond, 2019, p. 41).

### Encapsulamiento en las VPN

Sharma y Kaur (2020) manifestaron "algunas alternativas de VPN encapsulan todos los paquetes antes de cifrarlos, otras cifran solo los contenidos de los paquetes encapsulados y no las cabeceras. De cualquier manera, es la encriptación, no el tunneling la que añade seguridad" (p. 2339). Asimismo, Sharma y Kaur (2020) comentaron que existen procedimientos simétricos capaces de agilizar el cifrado y descifrado de enormes cantidades de información de manera segura y confiable (Sharma y Kaur, 2020, p. 2339). En síntesis, la encriptación permitirá que la información transmitida a través del software VPN pueda mantenerse segura ante posibles DDoS (Sharma y Kaur, 2020, p. 2339).

### Definición de roles

A continuación, se definirán roles para la correcta implementación del escenario de pruebas en la metodología MEPVPNS propuesta en el anexo 1 del presente trabajo de investigación.

### Rendimiento del software

El rendimiento del software es importante para evaluar el producto de manera amplia y especifica en base a criterios previamente seleccionados (Verona et al., 2016, p. 284). Al respecto, Verona et al. (2016) mencionó que los exámenes de rendimiento en cualquier producto de software, pueden variar según el tiempo y/o las situaciones que se ejecutan sus funcionalidades (p. 282). Asimismo, Verona et al. (2016) detallaron "para calcular los criterios de rendimiento de un software, es necesario que las funcionalidades del software se encuentren en ejecución" (p. 282). Sin embargo, para la ejecución de una funcionalidad del software se necesita la intervención de muchas otras ejecuciones al mismo tiempo y en segundo plano (Verona et al., 2016, p. 282).

Por otro lado, Lucena (2019) manifestó que el rendimiento de software se calcula con los resultados que arroja un sistema al ser sometido un estrés por la sobrecarga de trabajo al mismo tiempo, con el fin de calcular: (a) velocidad, (b)

fiabilidad y (c) estabilidad del software (Lucena, 2019, párr. 2). Es por ello, que los individuos llevan a cabo evaluaciones de rendimiento esperando obtener respuestas sencillas y fáciles de entender como: “funciona” o “no funciona” (Lucena, 2019, párr.5).

**Dimensión de velocidad de transferencia de datos**

La transferencia de datos es básicamente la rapidez en la transferencia de información donde se pueda establecer una comunicación entre dos dispositivos a través de un sistema de transmisión de data (Wang, Wang, Singh, Wang, Wu, Zhang, Liu, Zou, He y Meng, 2019). Del mismo modo, Wang, et al. (2019) indicaron que la velocidad de transferencia de datos simboliza la medida de datos transportada en un tiempo dado, además, CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) declaró que esta es capaz de calcularse por medio de: (a) bits, (b) caracteres o (c) bloques (p. 6). Sin embargo, se debe considerar que al utilizar las herramientas para calcular la velocidad de transporte de información debe optar por verificar que capte toda información para obtener resultados eficientes (Wang, et al., 2019).

**A. Throughput**

El throughput es un parámetro clave para evaluación de las redes privadas virtuales en la red, ya que es la cantidad real de información útil transmitida en un canal de comunicaciones en un tiempo determinado y su unidad de medida es bits/seg (Pacotaype, 2018). Pacotaype (2018) explicó que la finalidad primordial de la medición del rendimiento es identificar el mayor índice de envió de datos sin merma de tramas que el que la red privada virtual puede controlar (p. 33). Asimismo, la manera de evaluar el throughput es iniciar el cotejo de tramas enviadas transmitidas exitosamente con la totalidad de velocidad en intervalos de tiempo, luego se aminora la velocidad si se extravía al menos una trama; esta operación se repite hasta que no haya ninguna trama perdida (Tamariz, Coyotecatl, Torrebalba y Ambrosio, 2017, p. 4; Wu y Xiao, 2019, p. 52). De acuerdo a lo anterior mencionado, el throughput se define como la tasa promedio de éxito en la entrega de un mensaje sin considerar los encabezados del paquete, ACK (Acuse de Recibo), retransmisiones, etc., por lo que quedan

sólo los datos puros del usuario (Tamariz, Coyotecatl, Torrebalba y Ambrosio, 2017, p. 4).

**B. Jitter**

Respecto al jitter, Torreblanca, de la Cruz, Carranza y Gutiérrez (2017) mencionaron que es la variación de tiempo promedio en el retraso que hay para la transferencia de datos desde un punto a otro (p. 6582). Además, el jitter es el cálculo del tiempo que tarda en transmitir paquetes dentro de una red, asimismo, jitter puede representar la desviación del canal de comunicación causada por las alteraciones de la frecuencia en la red (Torreblanca et al., 2017; Andreadis, Rizzuto y Zambon, 2016, p. 2). Además, el jitter contempla la variación en el retraso de datos a lo largo del tiempo, siendo un inconveniente para las empresas que emplean herramientas de comunicación en tiempo real (voz/video) (Andreadis, Rizzuto y Zambon, 2016, p. 2; Sahu, Damle y Kherani, 2019, p. 232; Nurhaida, Putra, Zen y Wei, 2020, p. 4).

**Administración de recursos**

Torres, Guevara, Hernández, García y Ramírez (2018) mencionaron que en la actualidad las empresas deben considerar utilizar herramientas de almacenamiento beneficiando a la administración de recursos, considerando los protocolos de seguridad en la red (p. 3). Asimismo, Torres et al. (2018) explicaron que, si el uso previo del recurso de red y la cantidad que se utilizará para completar la operación de red supera un umbral, se puede advertir al usuario y se le puede dar la oportunidad de cancelar la operación o ajustar la forma en que se realizará la operación. Si se desconoce la cantidad de recursos de red que consumirá una operación de red, se determina una tasa de uso del recurso de red y se estima un tiempo hasta que se alcanza el presupuesto (p. 1).

Dicho en otras palabras, se proporciona una herramienta para administrar los recursos de red y establecer presupuestos para el consumo de recursos por parte de usuarios, dispositivos o aplicaciones (Sharma y Kaur, 2020, p. 2336). Hong, Lee, Kang, Yoo (2018) explicaron “la gestión de recursos de red se centran principalmente en el desarrollo de sistemas de organización que tengan en cuenta la calidad del servicio” (p. 18). Además, la administración de recursos

mide todo lo que compromete al sistema, desde que un computador enciende ya está en desarrollo los procesos (Hong, et al.,2018).

Li, Casellas, Landi, De la oliva, Costa, Garcia y Vilalta (2017) comentaron “la gestión de recursos en las redes de transporte sigue presentando un desafío para los operadores de redes” (p. 128). Asimismo, Li et al. (2017) dijeron “el Protocolo de Internet (IP), el modo de transferencia asíncrono (ATM), la red óptica síncrona (SONET) y las redes ópticas se gestionan utilizando sistemas separados” (p. 128). En síntesis, actualmente existen herramientas capaces de ayudar a gestionar los recursos y brindando resultados satisfactorios (Li, et al., 2017).

**Dimensión de consumo de recursos**

Agah (2017) indicó que el consumo de recursos implica todas las funcionalidades del sistema por la gran escala de tráfico adicional en función a los nodos del sistema. En el invento patentado por Tormasov, Beloussov y Protassov (2010) demostraron que los usuarios al emplear procesos de magnitud alta, logran saturar el sistema y la red, este resultado se obtuvo al ser monitoreado por herramientas tecnológicas para recolectar el uso del CPU, memoria RAM, procesos de los sistemas operativos, tráfico de red.

Agregando a lo explicado por Tormasov, et al. (2010) los grupos de procesos, servicios del sistema, servidores privados virtuales y usuarios se les denominan como consumidores de recursos de mayor nivel (Tormasov, et al., 2010, p. 1). El indicador de consumo de recursos en los sistemas es esencial para obtener respuestas al verificar los servicios de otros sistemas que ayudaran a mantener un control sobre los procesos en desarrollo (Zhou y Zhang, 2020). Asimismo, Zhou y Zhang, 2020) mostraron dada a las nuevas actualizaciones de los sistemas es necesario una gestión de recursos dado por las funcionalidades distribuidas, tales como: (i) administración de recurso (uso de CPU, Memoria RAM y discos), (ii) transferencia de paquetes de punto a punto y (iii) calidad del servicio del software considerándose la seguridad, privacidad y confiablidad dentro de la red (p. 3).

Dicho en otras palabras, los sistemas deben mantener la coordinación de funciones para que el consumo de recurso sea minino, puesto que el consumo

de recursos mide todas las interconexiones que tiene el computador (Zhou y Zhang, 2020).

### A. Uso del CPU ante el ataque de denegación de servicios distribuidos

Con respecto al consumo de recurso del CPU ante DDoS, Jati, Hartadi, Putra, Nurul, Iqbal y Yazid (2016) determinaron que el consumo de CPU fue un criterio fundamental para calcular el peligro y efecto en la red de una entidad a través de DDoS. Al respecto, Jati et al. (2016) determinaron que el uso del CPU con un nivel bajo por inactividad puede forzar a realizar un trabajo mayor desgastando su rendimiento con el paso del tiempo. El uso del CPU se evalúa en un rango 0% a 100% según su tasa de inactividad. Además, los resultados de Jati et al. (2016) arrojaron un promedio de inactivad de CPU ante DDoS, oscilando entre un 40% y 80% antes y después de realizar las pruebas de ataques referido al sujeto de prueba (Jati et al., 2016; Aguirre, 2016).

Precisando lo explicado por Jati et al. (2016), se muestra que las herramientas de evaluación de rendimiento son las que consumían los recursos al momento de realizar ataques simultáneos viéndose afectado el CPU y las capacidades del sistema (Aguirre, 2016).

### B. Uso de memoria RAM ante el ataque de denegación de servicios distribuidos

Con respecto al consumo de recurso de la memoria RAM ante los ataques DDoS, Aguirre (2016) determinaron que el consumo de memoria RAM fue un criterio fundamental para calcular el peligro y efecto en la red de una entidad a través de DDoS. Al respecto, Aguirre (2016) en su investigación concluyeron que mediante el ataque DDoS a una máquina de prueba, la memoria RAM se satura al 100% en un intervalo de tiempo menor a 7 minutos (p. 47-49). Sin embargo, El uso de Memoria RAM en base a los enrutadores es más complejo debido al nivel que debe obtener las vpn frente al proceso de ejecución; es decir, que al utilizar en exceso el sistema se verá obligado a tener retardos en sus procesos, además es autónomo frente a la cantidad de VPN pre especificadas a través de las características técnicas (López y Grampín, 2017, p. 4).En conclusión, las herramientas de simulación de ataque de denegación de servicios distribuidos

ayudaron a demostrar que la memoria RAM es el criterio más perjudicado, saturando los procesos e incrementando su consumo (Aguirre, 2016)

### C. Uso del Disco Duro ante el ataque de denegación de servicios distribuidos

Con respecto al disco duro es un hardware capaz de almacenar y recuperar grandes volúmenes de datos, además, de ser un elemento fundamental del ordenador (Aguirre, 2016). Asimismo, el consumo de disco duro ante los ataques DDoS son paquetes de datos infectados y estas están propensos a expandirse, provocando varios problemas como: (i) eliminación total de datos del disco duro, (ii) destrucción de información alojada en la memoria, (iii) infección a los archivos, (iv) suspensión de los principales procesos en la computadora y (v) perdida de dinero en el soporte del computador (Aguirre, 2016; Chilcañán, Navas y Escobar, 2017).

Además, el consumo de disco duro cuenta con encriptamiento de datos, transformando datos comprensibles a complejos y fuera del entendimiento humano, dificultando la interpretación en su totalidad al momento de cifrar datos: (a) carpetas, (b) archivos, (c) subcarpetas y (d) documentos de texto, además, haciendo uso de componentes adicionales y/o instalando driver o paquetes complementarios para incrementar la facilidad en los procesos de ejecución del equipo y evitar comprometer datos del usuario (Quemba, 2020, p. 52; Chilcañán et al., 2017).

### Desempeño en la red

El desempeño en la red es la facultad para hacerle frente a la sobrecarga de red sin generar retrasos o acumulaciones de transporte de la información a través de la red (Lawas, et al., 2016, p. 1; Pacotaype, 2018). Asimismo, es una dimensión fundamental, para evaluar el rendimiento de una VPN y lograr comparar una tecnología con otra. Además, se debe tener en cuenta que el throughput, latencia y ancho de banda son indispensables para identificar las necesidades de tráfico de red actual y futuro de la organización evitando perdida y/o retraso de información en la red de internet (Lawas, et al., 2016, p. 2; Pacotaype, 2018). En otras palabras, es crucial analizar sus indicadores de las VPNs con el objetivo de evaluar sus capacidades y evitar afectar su desempeño

en la red a través de simulaciones que podrán determinar la calidad de servicio que brindan los softwares VPNs (Martinasek, et al., 2017; Pacotaype, 2018).

**Dimensión de conectividad de red**

De acuerdo a la conectividad de red, Amorim, Kovacs, Wigard, Pocovi, Sorensen y Mogensen (2019) lo definieron como la probabilidad de que el origen se conecte con el destino bajo ciertas probabilidades de interrupción del enlace. Sin embargo, para ello se requiere enumerar todas las rutas posibles para calcular la confiabilidad de la conectividad, y el resultado puede depender de la precisión de la probabilidad de interrupción del enlace (Amorim et al., 2019, p. 4; Dong y Kim, 2017, p. 1). En

conclusión, se debe lograr definir la ruta y todos los parámetros desde el sitio inicial hasta el sitio objetivo, para evaluar con mayor efectividad la conectividad en la red (Amorim, et al., 2019). Además, cabe recalcar que son los conmutadores, módems y/o puntos de acceso inalámbricos partes cruciales para la conectividad entre equipos físicos, dispositivos móviles, laptops, otras redes, entre otros (Cisco, 2019, párr. 1).

**A. Latencia**

En relación con la latencia, Sigcha (2020) señalo que es el tiempo que tarda un paquete mínimo de datos en llegar de un punto a otro de una red, es un valor que mide el desfase temporal entre esos dos puntos" (p. 2) Asimismo, hace alusión a los atrasos en la transferencia de información entre la red, concretamente es el aplazamiento entre las tramas de información al momento de ser trasladados desde un punto inicial hacia un punto final (Fujiki, Ishii, Fujiwara, Matsutani, Amano, Casanova y Koibuchi, 2017, p. 470). En otras palabras, la latencia es el tiempo total de retrasos que tiene la información al viajar a través de una red (Sigcha, 2020; Fujiki, et al., 2017, p. 474).

**B. Velocidad de descargas / subidas de archivos**

De acuerdo a la velocidad de descargas/subidas de archivos, Balladares (2017) indicó que la rapidez de transferencia de datos se evalúa por separado para descargar y cargar archivos entre un sitio web remoto y el ordenador de un usuario" (p. 45). Esto quiere decir, que la velocidad de transmisión de datos entre

ordenadores depende si se desea descargar o subir información a la red de internet. Además, en el estándar ETSI EG2020 057-4 V1.2.1 mencionaron que la rapidez en la transferencia de datos se mide por: tamaño de dato a través del tiempo de transferencia requerida para obtener una conmutación integra y exento de fallos. Por otro lado, el administrador de redes obtiene márgenes estadísticos sobre los resultados de las evaluaciones hechas a la velocidad transferencia de archivos (descarga/subida) de manera separada (Balladares, 2017, p. 45-46). Dicho en otras palabras, la rapidez en el intercambio de información es medible por el tamaño del paquete de datos y el tiempo de demora en transportar los datos completamente (Balladares, 2017).

### C. Ancho de Banda

Es la magnitud de transferencia de datos que puede ser enviada a través de una red, independientemente de la velocidad que esta posea (Mercado y Ortiz, 2020, p. 20-21; Sheng, Wang, Li, Liu, Zhou y He, 2017). Además, el ancho de banda es un requisito crucial en un software de redes privadas virtuales, puesto que es el indicador que gestiona el tráfico de una red (Mercado y Ortiz, 2020, p. 21; Sheng, et al., 2017, p. 3). De igual modo, Sheng, et al. (2017) indicó que la calidad de servicio es una particularidad muy significativa de una red privada virtual. Además, la red privada virtual no brindará un servicio de calidad si no tiene capacidades para controlar y gestionar correctamente el ancho de banda (p. 3). En síntesis, el ancho de banda es una cualidad significativa para medir el volumen de transmisión de información mediante de una red, y es un criterio decisivo para diagnosticar la calidad y la rapidez de interconexión (Paessler, 2015, párr. 2).

### Dimensión de seguridad

Referente al indicador de seguridad, Oña (2016) indicó que son los procedimientos e indicadores (llaves cifradas) que normalmente se utilizan para encriptar, desencriptar la información que va a ser redirigida al personal autorizado (p. 35). Asimismo, Nico (2018) manifestaron que una forma segura de intercambiar datos por medio de canales de comunicación, es realizando las siguientes acciones, tales como: (a) autentificar y autorizar, (b) integridad, (c) confidencialidad y (d) no repudiar la información enviada (Nico, 2018, p. 260).

En relación a lo anterior mencionado, el enlace de redes privadas virtuales mantiene políticas de filtro para su correcto funcionamiento. Asimismo, las políticas de filtro funcionan mejor con determinadas conexiones VPN y del ancho de banda que se necesite gestionar (Oña, 2016). En síntesis, cada conexión maneja un filtro de normas específico para realzar su funcionalidad, asimismo, el filtro de normas se puntualiza como procedimientos, protocolos y puertos que se requieran manipular, para una correcta y segura transmisión de información a través del software VPN (IBM, 2021, párr. 2).

**Ataque de denegación de servicio**

Es un ataque cibernético en el que el intruso trata de vulnerar una tecnología de información o un componente de red temporalmente para sus usuarios (Biswas y Wu, 2019). Además, se consideran un delito federal en virtud de la Ley de Fraude y Abuso Informático con penas que incluyen años de prisión (Biswas y Wu, 2019, p. 537). Sin embargo, los ataques actualmente están en un crecimiento por las coyunturas del país, hacer caer plataformas como zoom y recientemente el caso de una de las organizaciones de seguridad de china (Qihoo 360) conocida a nivel mundial (Biswas y Wu, 2019).

**Ataque de denegación de servicio distribuido**

Los ataques DDoS pueden causar el consumo de recursos de las víctimas y la congestión de los enlaces, aun en los tiempos actuales estos ataques siguen planteando un importante desafío tanto en redes públicas como privadas (Jones, Wimmer y Haddad, 2020, p. 4). Por otro lado, Jones, et al. (2020) comentaron que protegerse de los ataques de denegación de servicios distribuidos es una manera eficiente de mitigar los riesgos de comunicaciones contra dos ataques: (a) consumo de recursos y (b) obstrucción de conexiones (p. 4). No obstante, los filtros existentes para gestionar los DDoS no emplean las cualidades indispensables para evitar contingencias en la red, como: (a) identificar las zonas vulnerables de ataque, (b) implementar los filtros de seguridad en las principales ubicaciones y (c) ejecutar diversos filtros de políticas para aumentar la eficiencia de seguridad (Jones, et al., 2020, p. 4).

Por otro lado, Salim, Rathore y Park (2020) mencionaron que los DDoS han vuelto a ser peligrosos nuevamente, debido a las potentes tecnologías y

procedimientos automatizados de ataques simultáneos (p. 21). Los intrusos que manipulan estas herramientas para realizar ataques tienen diferentes fines, como: (a) extorsión, (b) spam, (c) hacking a páginas web, (d) información política, (e) entre otros (Salim, et al., 2020, p. 21). Además, Salim, et al. (2020) indicaron "los atacantes envían una gran cantidad de paquetes de ataque utilizando direcciones IP de origen falsificadas a un servidor víctima que finalmente se queda sin recursos y degrada el rendimiento de los paquetes legítimos" (p. 21). Sin embargo, utilizando el rastreo IP, los atacantes pueden ser identificados y castigados mediante el rastreo de sus ubicaciones físicas (Salim, et al., 2020, p. 21).

### A. Filtro y marcado de tráfico de red

En relación con las políticas de filtro y marcado de tráfico, Basile, Valenza, Lioy, López y Perales (2019) definieron "un conjunto de reglas de gobierno del sistema" (p. 6). Asimismo, Basile, et al. (2019) indicaron "[la política es la] meta o curso de acción para guiar decisiones presentes y futuras de la red. Más concisamente, la política es conjunto de normas para administrar, gestionar y monitorear la autorización a productos, información y servicios en el ciberespacio." (p. 6). Es otras palabras, se debe seguir las pautas y estar bajo ciertas condiciones tecnológicas para mantener la seguridad en la red (Basile, et al., 2019, p. 6). Por otro lado, en el invento patentado por Chauca (2016) manifestaron "es necesario un mecanismo que integre las aplicaciones en un sistema de red basado en políticas y permita que las aplicaciones participen en la decisión de aplicar una QoS determinada a un flujo de tráfico generado por la aplicación" (p. 4; Ariza y Vargas, 2020, p. 4). En síntesis, las políticas existen para poder lograr acceder a parámetros específicos en la red, para mantener la seguridad y estar fuera de ataques (Chauca, 2016; Carvajal, 2019, p. 4). Por otro lado, Gai y McCloghrie (2007) mencionaron que para implementar políticas de administración de tráfico de alto nivel e independientes del dispositivo dentro de una red informática que tenga múltiples dispositivos de red diferentes, el método que comprende los pasos son:

- selección de una o más políticas de alto nivel (p. 20).

- traducir una o más políticas de alto nivel en una pluralidad de reglas ejecutables (p .20).
- recibir una solicitud de directivas de administración de tráfico desde un dispositivo intermedio que admita un conjunto de servicios de red (p. 20).
- seleccionar, en respuesta a la solicitud, una o varias reglas que sean compatibles con los servicios de red admitidos por el dispositivo intermedio (p. 21).
- reenviar una o más reglas seleccionadas al dispositivo intermedio; y utilizando una o más reglas para configurar el conjunto de servicios de red en el dispositivo intermedio para realizar las directivas de alto nivel seleccionadas (p. 21).

Con respecto a las Políticas de filtro y marcado de tráfico, Basile, et al. (2019) expresaron que proporciona un mecanismo flexible y sólido para asignar recursos y servicios de red como la asignación de ancho de banda, la calidad de servicio, los derechos de acceso, la priorización del tráfico y la seguridad en la red (p. 6). Por eso mismo, los servicios de red conllevan políticas para que se pueda priorizar la seguridad y el intercambio de datos sin errores (Basile, et al., 2019, p. 6; Carvajal, 2019; Chauca, 2016).

**B. Encriptamiento de datos**

El encriptamiento de datos es el procedimiento de transformar la información de una forma legible solo para los sistemas y de una forma ilegible para el entendimiento humano, además, permite asegurar la información que es transmitida a través de la red, imposibilitando la visualización y alteración de esta por parte de terceros (usuarios maliciosos) (Saber, Fergani y Abbas, 2018, p. 1385; Pérez, 2017; Quemba, 2020). Al respecto, Quemba (2020) mencionó que el cifrado/encriptamiento de datos se puede realizar por medio de software y/o hardware (equipos móviles, computadoras, componentes técnicos, dispositivos de almacenamiento, programas, redes de telecomunicación, derivador de carpetas y subcarpetas) (p. 26). En otras palabras, el encriptamiento de datos hace uso de algoritmos lógicos para codificar y decodificar los datos que son transmitidos de un punto a otro (Quemba, 2020, p. 26-27).

### C. Desencriptamiento de datos

El Desencriptamiento de datos es el procedimiento capaz de traducir la información de manera legible para el usuario que tenga acceso a la clave del cifrado (Bucșă, 2020, p. 80; Pérez, 2017). Asimismo, los especialistas de Microsoft indicaron que el desencriptamiento es el proceso inverso del cifrado de datos, para el desencriptamiento se debe conocer de las claves que el mismo sistema o usuario impone al momento de cifrar información privada o pública para darle seguridad a través de la red, además, cuenta con dos formas de desencriptar los datos: (a) desencriptamiento simétrico y (b) desencriptamiento asimétrico (Microsoft, 2017, párr., 1).

Por otro lado, al desencriptar un archivo cifrado no debería perder la integridad y confidencialidad de la información dentro del paquete y en caso contrario se debería verificar la configuración del encriptado (FileMaker, 2017). Por ello, asegurarse de una correcta encriptación de datos y una conexión segura a la red es crucial para mantener la seguridad y privacidad de la información que envía el usuario de un lugar a otro, teniendo en cuenta, las vulnerabilidades existentes en la ejecución de los scripts para descifrar la información trasmitida (Gallegos y Mayorga, 2019; Méndez, 2020).

### D. Fugas de servidores DNS – dirección IP – dirección IP por WebRTC

Al respecto, el DNS (sistema de nombres de dominio) es ampliamente utilizado para reducir el tiempo de acceso a las aplicaciones web por medio de algoritmos capaces de traducir los nombres de dominio a sus propias direcciones IP para una búsqueda rápida y ordenada (Oramas, 2020, p. 2; Fakis, Karopoulos y Kambourakis, 2020, p. 10; Saras, 2015; Gordillo, 2017; VpnMentor, 2019, párr. 3). Sin embargo, la función principal del DNS de registrar direcciones IP de las páginas web para facilitar la navegación del usuario en la red puede ser contraproducente para la privacidad, además, si la IP del servidor DNS es filtrada quedará expuesta la dirección IP publica del usuario, convirtiéndose en una víctima más de los ciberdelincuentes (ExpressVPN, 2015, párr., 2). Por ello, aunque utilicemos una red privada virtual para enviar información a través de un túnel VPN, esta no es capaz de asegurar en su totalidad la privacidad de las peticiones DNS en sus dispositivos, ocasionando **fugas de servidores DNS**

(ExpressVPN, 2015, párr., 1; Fakis, et al., 2020; Saras, 2015; Gordillo, 2017; Pérez, 2017).

Al respecto, la dirección IP es un grupo numérico singular y exclusivo, capaz de identificar un dispositivo de comunicación conectado a la red del internet desde un celular, Tablet hasta servidores globales (Hostgator, 2019, párr. 3; Oramas, 2020, p. 2). Por ello, es necesario indagar si el proveedor VPN que utilizas muestra **fugas de dirección IP** durante la navegación en internet y la reconexión a esta, debido a que no todos los servicios VPN brindan protección contra este problema durante la reconexión a internet (Al-fannah, 2017, p. 4; VpnMentor, 2019, párr. 8). Además, la autenticación operativa de los ciberdelincuentes es complejo debido a la capacidad de bloquear los enrutadores/interruptores de internet. Por lo tanto, es importante y desafiante hacer el rastreo de IP (Salim, et al., 2020, p. 28). Es por ello, que se debe cumplir con las políticas de seguridad, optando por mantener los servicios de red sin problemas y así evitando fugas de dirección IP salientes. (Salim, et al., 2020, p. 28; Segura y Ramírez, 2018, p. 47; Salim, et al., 2020).

Además, la WebRTC es una plataforma de código libre, capaz de facilitar la intercomunicación (audio y video) en tiempo real entre usuarios de navegación por medio de computadora y dispositivos, con la ayuda de un servidor de conferencias web (Guimarey, 2017, p. 23; Bhalerao, Pal, Chatterjee, 2020). Respecto al webRTC, Fakis, et al. (2020) indicaron que permite en intercambio audio video y archivos en tiempo real, sin optar por aplicaciones o extensiones complementarias, esta plataforma permite la comunicación entre usuarios por medio de un navegador genérico como: Google, Mozilla, Opera, Internet Explorer, entre otros. Por otro lado, las **fugas de dirección IP por WebRTC** son capaces de revelar las direcciones IP (públicas como privadas) ocasionando riesgos a la privacidad y seguridad de los involucrados (Fakis, et al., 2020; Ezell y Yoakum, 2020).

### E. Conexión al servidor

La conectividad en base al software vpn tienen la finalidad de mantener tus datos seguros y poder ocultar tu IP con el fin de poder establecer conexión a diferentes plataformas sin ser rastreado por tu ISP, redes de publicidad o motores de

búsqueda (Netspotapp, 2020). Al respecto, Hauser, Haberle, Schmidt y Menth (2020) infirieron que la conectividad del software VPN es a través de los protocolos de tunelización en la red, es decir, que la privacidad de navegación, archivos y procesos realizados con los softwares vpn serán de manera anónima y segura ante la transferencia de datos por la red (p. 1). En síntesis, el tiempo de conexión al servidor vpn es un punto importante a considerar, debido a que los servidores se encuentran en diferentes puntos geográficos generando retrasos al establecer una conexión con los servidores del software vpn (Hauser et al., 2020; Netspotapp, 2020; Abril y Cuzco, 2019).

# III. METODOLOGÍA

### 3.1 Tipo y diseño de investigación

El tipo de investigación que se utilizará es aplicado con un diseño de investigación no experimental transversal-descriptivo. Por ende, es necesario la recolección de datos mediante el empleo de tecnologías digitales, índices y lógica para evaluar el rendimiento de software de las VPNs según los criterios planteados (Hernández y Mendoza, 2018). Respecto a la investigación aplicada, los especialistas del Concytec (2017) argumentaron que está orientada a cubrir la necesidad de información examinada y delimitada por medio del razonamiento científico, metodologías, procedimientos, normas, y/o herramientas (p. 5). En conclusión, el presente trabajo hace uso de la investigación aplicada porque apoya a incrementar al conocimiento científico de las VPNs con un fin práctico y concreto de desarrollar una metodología de rendimiento evaluando criterios indispensables de la tecnología VPN. Además, contribuyen al conocimiento científico con un fin práctico concreto. Aplicando los resultados de las investigaciones básicas (Vivanco y Chilán, 2019, p. 12).

Asimismo, en el presente trabajo de investigación se empleará un enfoque cuantitativo. Al respecto Hernández y Mendoza (2018) indicaron el enfoque cuantitativo sigue un paradigma previsible y ordenado de procesos para alcanzar el objetivo de la investigación; se debe discutir las medidas cruciales antes de la recolección de los datos (p. 6). Esto debido a que es necesario recopilar datos e información con el objetivo de comprobar la hipótesis planteada con el apoyo de la evaluación estadística y el análisis para determinar procedimientos, métodos o comprobar teorías" (Hernández y Mendoza, 2018, p. 4).

Hernández y Mendoza (2018) mencionaron que en la investigación no-experimental es imposible la manipulación, alteración o impacto en las variables independientes, debido a que ya ocurrieron, al igual que sus resultados ya sean positivos o negativos (p. 152). Además, el estudio no-experimental se ejecuta sin operar deliberadamente las variables, es decir, no se altera de manera premeditada las variables independientes para observar su impacto sobre diferentes variables (Hernández y Mendoza, 2018; Alva y Domínguez, 2015, p. 94; Vásquez y Guevara, 2020; Hagopian, 2016, p. 50).

Hernández y Mendoza (2018) argumentaron que un diseño transversal-descriptivo recopila información en un único tiempo determinado para describir las variables, y observar los incidentes y su interrelación en un tiempo dado" (p. 94-154). Por lo tanto, es descriptivo porque registra los rasgos y cualidades de los individuos, masas, ciudades, procedimientos, componentes o cualquier otro objetivo que se desea analizar (Hernández y Mendoza, 2018; Alva y Domínguez, 2015, p. 94).

Por otro lado, Gallardo (2017) indicó que el nivel descriptivo tiene como objetivo detallar las características, condiciones y los aspectos de individuos, grupos, categorías, procedimientos, componentes o cualquier otro acontecimiento que se imponga a una evaluación, con el propósito de identificar su organización o conducta, asimismo, puntualiza tendencias de una cantidad menor o mayor (p. 53). En otras palabras, se utiliza un nivel descriptivo para detallar que software de redes privadas virtuales arrojan mejores resultados en base las pruebas de evaluación de rendimiento en el presente estudio (Hernández y Mendoza, 2018; Gallardo, 2017).

### 3.2 Variables y operacionalización

En este apartado del documento se enuncia la variable estudiada y el impacto de la metodología para evaluar el rendimiento de los softwares de redes privadas virtuales, y especificando todos los aspectos que se van a tocar a lo largo del presente estudio.

#### V1: Rendimiento del software

*A. Definición Conceptual:* El rendimiento de las redes privadas virtuales son pruebas de rendimiento que tiene como propósito estresar el software, realizando exámenes fuera del alcance para los que fue implementado. Además, los softwares redes privadas virtuales son túneles virtuales encriptados entre el usuario y un servidor remoto operado por un servicio VPN (Verona et al., 2016; Lucena 2019; Pacotaype, 2018, Torres y Alfaro, 2018; Carrión, 2018; Wang et al., 2019).

*B. Definición Operacional*: El rendimiento de evaluación de las redes privadas virtuales es el resultado obtenido al evaluar de forma organizada y metódica estas tecnologías de comunicación privada a través de dimensiones de 41 evaluación (rendimiento del software, administración de recursos y desempeño en la red). Asimismo, el rendimiento se calcula como la amplitud del software, al emplear los componentes físicos de manera eficaz. Además, el rendimiento se puede medir con métricas de calidad en el intercambio de información, usando los servicios de internet, etc.; mediante herramientas para evaluar los indicadores planteados en la presente investigación (Verona et al., 2016; Lucena 2019; Pacotaype, 2018, Torres y Alfaro, 2018; Carrión, 2018; Wang et al., 2019).

**V2: Administración de recursos**

*A. Definición Conceptual:* La administración de recursos son procesos o subprocesos que se ejecutan en un sistema informático, que requieren recursos compartidos de tiempo de CPU, memoria, objetos del sistema operativo, semáforos, acceso a disco, acceso a la red, entre otros para el correcto funcionamiento del sistema (Torres et al., 2018; Sharma y Kaur, 2020; Hong et al., 2018; Li et al., 2017; Agah, 2017; Tormasov et al., 2010; Zhou y Zhang, 2020).

*B. Definición Operacional:* El indicador de administración de recursos en los sistemas es esencial para obtener respuestas al verificar los servicios de otros sistemas que ayudaran a mantener un control sobre los procesos en desarrollo (Torres et al., 2018; Sharma y Kaur, 2020; Hong et al., 2018; Li et al., 2017; Agah, 2017; Tormasov et al., 2010; Zhou y Zhang, 2020).

**V3: Desempeño en la red**

*A. Definición Conceptual:* El desempeño en la red es la facultad para hacerle frente a la sobrecarga de red sin generar retrasos o acumulaciones de transporte de la información a través de la red (Lawas et al., 2016; Pacotaype, 2018; Martinasek et al., 2017; Amorim et al., 2019; Dong y Kim, 2017; Cisco 2019; Oña,2016; Nico, 2018; IBM, 2021).

*B. Definición Operacional:* La evaluación del desempeño en la red es una dimensión fundamental, para evaluar el rendimiento de una VPN y lograr comparar una tecnología con otra. Además, se debe tener en cuenta que el

throughput, latencia y ancho de banda son indispensables para identificar las necesidades de tráfico de red actual (Lawas et al., 2016; Pacotaype, 2018; 42 Martinasek et al., 2017; Amorim et al., 2019; Dong y Kim, 2017; Cisco 2019; Oña,2016; Nico, 2018; IBM, 2021).

D. *Dimensiones:*

- Velocidad de transferencia de datos (Wang et al., 2019)
- Consumo de recursos (Agah, 2017; Tormasov et al., 2010; Zhou y Zhang, 2020)
- Conectividad de red (Amorim et al., 2019; Dong y Kim, 2017; Cisco 2019).
- Seguridad (Oña,2016; Nico, 2018; IBM, 2021)

*E. Indicadores*

- Throughput: Velocidad real en Mb/s (megabits por segundo) en que el software VPN envía los paquetes de punto a punto (Tamariz et al., 2019; Wu y Xiao, 2019).
- Jitter: Variación de retrasos en que el software VPN envía los paquetes (Torreblanca et al., 2017; Andreadis et al., 2016; Sahu et al., 2019; Nurhaida et al., 2020).
- Uso del CPU: Porcentaje de uso del CPU ante DDoS (Jati et al., 2016; Aguirre, 2016).
- Uso de Memoria RAM: Porcentaje de uso de RAM ante DDoS (Aguirre, 2016; López y Grampín, 2017).
- Uso del Disco Duro: Porcentaje de consumo de Disco Duro ante DDoS (Aguirre, 2016; Chilcañán et al., 2017; Quemba, 2020).
- Latencia: Tiempo de retrasos total (milisegundos) en que el software VPN envía los paquetes de punto a punto (Sigcha, 2020; Fujiki et al., 2017).
- Velocidad de Descargas de archivos: Velocidad para descargar un archivo mediante el uso del software VPN (Balladares, 2017).
- Velocidad de Subidas de archivos: Velocidad para subir un archivo mediante el uso del software VPN (Balladares, 2017).
- Ancho de banda: Consumo de ancho de banda por IP ante descarga/subida de archivos (Mercado y Ortiz, 2020; Sheng et al., 2017; Paessler, 2015).

- Porcentaje de filtro y marcado de tráfico de red: Porcentaje de protocolos registrados ante el encriptamiento y desencriptamiento de datos (Basile et al., 2019; Chauca, 2016; Carvajal, 2019; Gai y McCloghrit, 2007)
- Velocidad de encriptamiento de datos: Tiempo de encriptamiento de datos ante el uso del software (Saber et al., 2018; Pérez, 2017; Quemba,2020)
- Velocidad de desencriptamiento de datos: Tiempo de desencriptamiento datos ante el uso del software (Bucșă, 2020; Pérez, 2017; Microsoft, 2017; FileMaker, 2017; Gallegos y Mayorga, 2019; Méndez, 2020).
- Porcentaje de fugas de DNS: Filtrado de DNS ante el uso del software VPN y reconexión del ISP (Oramas, 2020; Fakis et al., 2020; Saras, 2015; Gordillo, 2017; VpnMentor, 2019; ExpressVPN, 2020).
- Porcentaje de fugas de dirección IP: Filtrado de direcciones IP ante el uso del software VPN y reconexión del ISP (Hostgator, 2019; Oramas, 2020; Al-fannah, 2017; VpnMentor, 2019; Segura y Ramirez, 2018; Salim et al., 2020).
- Porcentaje de fugas de dirección IP por webRTC: Filtrado de webRTC ante el uso del software VPN y reconexión del ISP (Guimarey, 2017; Bhalerao et al., 2020, Fakis et al., 2020; Ezell y Yoakum, 2020).
- Tiempo de conexión al servidor: Tiempo de conexión del software vpn (milisegundos) ante la ubicación del servidor (Netspotapp, 2020; Hauser et al., 2020; Abril y Cuzco, 2019).

F. *Instrumento:* Técnica de observación, Tabulación de datos y fichas de registro.

G. *Escala de Medición*: Razón

H. *Unidad de Medida*: Megabytes/Sec, Gigabits/Sec, Porcentaje; Segundos; Bit/Sec; Milisegundos.

### 3.3 Población, muestra y muestreo

A continuación, se detalla la población, muestra y muestreo, para evaluar el rendimiento de los softwares de redes privadas virtuales.

Hernández y Mendoza, 2018 definieron la población como el grupo de todos los incidentes, individuos o componentes que se asemejan en descripciones específicas. En consecuencia, la presente investigación tiene una población delimitada por (39) treinta y nueve VPNs: (18) dieciocho VPNs

gratuitos/libres - (21) veintiuno VPNs licenciados y sus marcas respectivamente son: SocialVPN, OpenConnect, ProtonVPN, SoftEther VPN, OpenSwan, strongSwan, Tinc VPN, Vpnunlimitedapp, VPN Lite, HotSpot Shield FREE VPN, TunnelBear, PrivateTunnel, Freelan, Hide.me, Tcpcrypt, LibreSwan OpenVPN, ProtonVPN, ExpressVPN, Cyberghost, Nordvpn, Surfshark, PIA, PureVPN, HydeMyAss, PrivateVPN, AstrillVPN, WindScribe, VyprVPN, IPVanish, Private Internet Access, Hidden24, SaferVPN, Zen Mate, Norton LifeLock, UltraVPN, Norton Secure VPN, Panda Security y Hotspot Shield.

La **muestra** es un subgrupo de la población, también puede ser entendido como un pequeño grupo pertenecientes a la agrupación ligada por características similares, también denominada población (Hernández y Mendoza, 2018). Asimismo, Hernández y Mendoza (2018) indicó que a partir de la muestra se recopilan información precisa y crucial para el desarrollo del objetivo del presente estudio (p. 173). La muestra para el presente estudio está conformada por (03) tres VPNs: (01) un VPN gratuito - (01) un VPN de código libre - (01) un VPN licenciado y sus marcas respectivamente son TunnelBear, ProtonVPN, NordVPN. Los mismos que serán evaluados en los siguientes aspectos: (a) rendimiento del software, (b) administración de recursos y (c) desempeño en la red para determinar cuál de las categorías muestra mayor rendimiento.

El **muestreo** es el procedimiento que se utiliza para elegir los sujetos de la muestra de una población establecida (Hernández y Mendoza, 2018). Asimismo, las muestras no probabilísticas se orientan a la selección de los sujetos por las cualidades necesarias para el estudio. De igual modo, la ventaja de emplear este tipo de muestreo esta enfocados seleccionar rigurosamente los sujetos a base de características específicas necesario para responder al problema (Hernández y Mendoza, 2018). En el presente estudio es no probabilístico, pues la elección de los softwares de redes privadas virtuales fue seleccionada por conveniencia de los investigadores, asimismo, la muestra fue elegida sin necesidad de emplear fórmulas o métodos de selección (Pacotaype, 2018, p. 72; Hernández y Mendoza, 2018; Posada, 2016).

### 3.4 Técnicas e instrumentos de recolección de datos

En el presente estudio se adoptó la técnica de la observación. Con respecto a ello, Hernández y Mendoza (2018) indicaron que esta técnica de recolección de datos se centra en el registro metódico, verídico y confiable de conductas y escenarios perceptibles, a través de un grupo de tipos y subtipos. Además, Pulido (2015) mencionó que la técnica de observación forma parte de los métodos capaces de recolectar información paulatina y específicamente en el desarrollo del sucedo a estudiar (p. 1149). Asimismo, la observación metódica supone que los hechos que se perciben son identificados, recopilados y documentados de modo que, previamente se debe determinar los criterios a observar y el lapso del tiempo que se tomara en las observaciones (Pulido, 2015, p. 1149).

Por otro lado, el instrumento que se adoptó para el presente estudio de investigación fue la tabulación de datos, debido a que es necesario recolectar la información de manera ordenada de las herramientas empleadas (Jperf, Test de velocidad Speedy, panel de monitoreo /Administrador de tareas, Wireshark, Camtasia, Leak Test para fugas, Software VPN) para efectuar las pruebas (Throughput, Jitter, uso del CPU, uso de la Memoria RAM, uso del disco duro, latencia, velocidad de descarga de archivos, velocidad de subida de archivos, ancho de banda, filtro y marcado de trafico de red, velocidad de encriptamiento de datos, velocidad de desencriptamiento de datos, fugas de servidores DNS, fugas de dirección IP, fugas de dirección IP por webRTC, conexión al servidor) en la metodología MEPVPNS (Pacotaype, 2018). Es conveniente señalar que la tabulación de datos es el procedimiento por el cual se busca describir los distintos valores o cualidades de la variable, según los criterios seleccionados por los investigadores para obtener resultados precisos y confiables mediante pruebas con intervalos o grados numéricos (Posada, 2016, p. 34; Pacotaype, 2018).

#### Validez

La validez hace referencia al nivel de cumplimiento de una herramienta designada para medir la variable con los criterios establecidos, asimismo, esta puede mantener diferentes clases de evidencia (Hernández y Mendoza, 2018). Al respecto, Ventura (2017) consideraron que los detalles técnicos,

contemplaciones de diseño de la validez y la eficacia de las herramientas de medición son muy importantes en las pruebas (p. 955). Del mismo modo, la validez de contenido es el nivel de la herramienta en cuanto al control particular de contenido de lo que se quiere evaluar, asimismo, la variable que se desea medir debe estar definido o comprobado en los antecedes y marco teórico (Hernández y Mendoza, 2018). Es decir, la validez es considerado como la prueba de que una herramienta adquirida, desarrollada e implementada permita calcular lo que se espera medir (Li y Takakuwa, 2016, p. 88).

**Confiabilidad**

La confiabilidad de una herramienta de evaluación hace referencia al nivel en que su utilidad repetitiva hacia un mismo sujeto u objeto produzca resultados similares, además, esta establece mediante múltiples técnicas, las mismas que se describirán concisamente luego de considerar los conocimientos de validez y confiabilidad (Hernández y Mendoza, 2018). Además, la confiabilidad en las pruebas se muestra en la estabilidad de los resultados extraídos por el mismo individuo u objetos puestos a prueba en diferentes situaciones (Hernández y Mendoza, 2018). Asimismo, los resultados de la investigación son considerados verídicos mientras se obtenga un alto índice de validez, es decir, arrojando resultados de tasa mínimas de errores (Villasís, Márquez, Zurita, Miranda y Escamilla, 2018, p. 416). En esta investigación no será necesario medir la confiabilidad pues se empleará tabulación de datos (hojas de cálculo) como herramienta para recolectar información, es por ello, que se brinda el **95% de grado de confianza** en los resultados estadísticos (Hernández y Mendoza, 2018; Pacotaype, 2018; Villasís et al., 2018, p. 416).

### 3.5 Procedimientos

El procedimiento hace referencia al método regido por el problema general en la investigación que lleva a cabo un conjunto de pasos a seguir y se construye a base un diseño adaptable al problema que se busca solucionar, mediante el uso de diversos componentes, herramientas de recolección de datos y artefactos necesarios para el desarrollo del estudio, esto será evaluado con los recursos esenciales, debiendo el investigador explicar de forma verbal y documentada los 47 resultados obtenidos, permitiendo reorganizar o clasificar la información

(Abeleira, Vázquez y Peña, 2017, p. 1.35). La metodología MEPVPNS se realizó con el enfoque de brindar información tanto a las personas en general, empresas e instituciones públicas para agilizar la toma de decisiones en la selección de software vpn a base de pruebas de estrés para evaluar el rendimiento de los criterios pre-establecidos en el presente estudio de investigación. Para el desarrollo de las pruebas de estrés se utilizó una red LAN con tres hosts (dos hosts para la simulación de pruebas y un solo host para medir el rendimiento) a base de herramientas pre-seleccionados (Jperf, Test de velocidad Speedy, panel de monitoreo/Administrador de tareas, Wireshark, Camtasia, Test de fugas de IP, Fugas de DNS y Fugas de WebRTC, Software VPN) de los antecedentes que brindaran respuestas exactas ayudando a solucionar el objetivo en concreto.

### 3.6 Método de análisis de datos

El método de análisis de datos se centra en la demostración y explicación de los resultados extraídos de las pruebas desarrolladas en la investigación, asimismo, para un correcto análisis de los datos esto es plasmado en una matriz de información utilizando tecnologías de información computacionales (Hernández y Mendoza, 2018). Además, para el estudio de investigación se utiliza la prueba t de Student ya que está enfocada a la evaluación entre dos grupos para identificar las diferencias explicitas entre ellas (medias de variables) (Hernández y Mendoza, 2018). Asimismo, esta es representada en (i): hipótesis, (ii) variables, (iii) nivel de evaluación de la variable a comparar y (iv) análisis y explicación (Hernández y Mendoza, 2018).

Hernández y Mendoza (2018) mencionaron que un fraccionamiento muestral o poblacional de divergencia de medias hace referencia a la **prueba t de Student** que se reconoce por los niveles de autonomía, las mismas que demuestran la cantidad de formas en que los datos pueden diferenciarse (p. 310). Además, la prueba T-Student plantea dos ideas: (a) distribución de normalidad y (b) muestras independientes, además, permite la comparación de muestras (N<= 30) fundamentando la desigualdad entre las medias de los resultados (Sánchez, 2015). De igual modo, se tomará la prueba de Wilcoxon como alternativa. Respecto a ello, Flores, Miranda y Villasís (2017) mencionaron que la prueba de wilcoxon se emplea cuando la repartición de los datos 48 estadísticos no mantiene un fraccionamiento normal, además esta prueba se

aplica con el propósito de comprobar la diferencia entre grupos relacionados (pre y post) (Flores, Miranda y Villasìs, 2017, p. 368; Moreno y Sepúlveda, 2017). **La prueba de normalidad** en el estudio de investigación será de ayuda para la comprobación de que los resultados sigan o no una redistribución normal, considerando importante el volumen de la muestra para seleccionar la prueba adecuada: (a) Kolmogorov-Smirnov y (b) método Shapiro-Wilk (Pacotaype, 2018). Por otro lado, **el método de Kolmogorov-Smirnov** considerado una de las pruebas más significativas para medir el rendimiento en las pruebas de puntuación cuando la cantidad de la muestra es >= (mayor o igual) a 50 (Fang y Chen, 2019, p. 1; Pacotaype, 2018). En el **método Shapiro Wilk** es una prueba capaz de medir el nivel de adaptación a una línea de observaciones representado en un cuadro estadístico de normalidad, rechazando el Ho (hipótesis nula) de normalidad. Esta prueba muestra mejores resultados cuando el volumen de la muestra es < (menor) a 50 y no se cuente con la información necesaria para detallar las variables de distribución (Fang y Chen, 2019; Pacotaype, 2018; Flores, Miranda y Villasís, 2017).

### 3.7 Aspectos éticos

El código de ética busca robustecer la formación y conocimiento de valores en los investigadores, con responsabilidades y derechos en conjunto, manteniendo una comunicación amistosa y comprometida con el desarrollo de la presente investigación. Además, para el estudio de investigación la ética es el instrumento crucial y vital para el entendimiento, incentivación y adopción de principios y virtudes éticos en el progreso de la investigación (Montenegro, 2020; Gómez, 2017).

En el vicerrectorado de investigación de la universidad privada Cesar Vallejo hace mención que el documento de producto observables y líneas de investigación, está enfocada al desarrollo del estudio a base de criterios y artículos vinculados a la UCV (Vicerrectorado de Investigación, Nº011-Nº21, 2020). Además, en el reglamento de propiedad intelectual dispone de artículos que avalan los derechos de los estudiantes, personal educativo y asesores dentro de la universidad Cesar Vallejo (Reglamento de propiedad intelectual, V01, 2020). Asimismo, en el reglamento de investigación busca promover el 49 estudio científico en base a normas, principios y procesos, asimismo, determinar

los roles de los componentes que forman parte de la investigación en la universidad (Reglamento de investigación, 2020). De igual modo, la resolución de directorio mencionó que los reglamentos de los estudiantes ayudaran al investigador a cumplir las normas que regulen sus responsabilidades y privilegios optando por un excelente servicio educacional con profesionales en la materia (Resolución de directorio, N.º 0066, 2018).

En la resolución de consejo universitario hace mención que la ley N.° 30220 describe que el estudio de la investigación es parte fundamental e indispensable para enriquecer o llenar el vacío de conocimiento y el desarrollo de nuevas tecnologías en beneficio de la sociedad (Resolución de consejo universitario, N.º 084-126). De igual modo, el código nacional de integridad científica incentiva la aplicación de buenas prácticas y moralidad en el estudio científico, implementación y proceso tecnológico en el SINACY, asimismo, cuenta con bases legales que fundamenta la importancia de los puntos antes mencionado para el desarrollo de la investigación (Código nacional de integridad científica, 2020; Resolución de consejo universitario N°0126-2017).

# IV. RESULTADOS

En este apartado, se detallan los resultados extraídos por la metodología MEPVPNS aplicada en la presente investigación, referente a las variables “rendimiento del software”, “administración de recursos” y “desempeño en la red” las mismas que fueron seleccionadas para evaluar el rendimiento de las tecnologías de software de redes privadas virtuales. Los datos extraídos de las pruebas fueron procesados y analizadas tanto en Excel como en SPSS v. 25.

## 4.1 Datos descriptivos

Para el siguiente análisis, se realizó la categorización en tres grupos: software libre, gratuito y licenciados, los cuales participaron para la evaluación de softwares de redes privadas virtuales, a través de pruebas de rendimiento. A continuación, se realiza el detalle de estadísticos descriptivos. En los siguientes párrafos se muestra los datos que fueron obtenidos.

**Prueba descriptiva para el indicador throughput de la variable rendimiento del software**.

Tabla 1 Resultados de la prueba descriptiva para el indicador throughput en base a los softwares VPN y sin software VPN.

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_Througput_ ProtonVPN** | Media | | 131,00 | 60,492 |
| | 95% de intervalo de confianza para la media | Límite inferior | -17,02 | |
| | | Límite superior | 279,02 | |
| | Media recortada al 5% | | 119,33 | |
| | Mediana | | 56,00 | |
| | Varianza | | 25615,333 | |
| | Desv. Desviación | | 160,048 | |
| | Mínimo | | 19 | |
| | Máximo | | 453 | |
| | Rango | | 434 | |
| | Rango intercuartil | | 204 | |
| | Asimetría | | 1,709 | ,794 |
| | Curtosis | | 2,619 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv . Error |
| **W_Througput _TunnelBear** | Media | | 2429,43 | 1116,508 |
| | 95% de intervalo de confianza para la media | Límite inferior | -302,57 | |
| | | Límite superior | 5161,43 | |
| | Media recortada al 5% | | 2214,87 | |
| | Mediana | | 1050,00 | |

| | | | | |
|---|---|---|---|---|
| | Varianza | | 8726138,286 | |
| | Desv. Desviación | | 2954,004 | |
| | Mínimo | | 354 | |
| | Máximo | | 8367 | |
| | Rango | | 8013 | |
| | Rango intercuartil | | 3774 | |
| | Asimetría | | 1,703 | ,794 |
| | Curtosis | | 2,593 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_Througput _NordVPN** | Media | | 2710,29 | 1244,784 |
| | 95% de intervalo de confianza para la media | Límite inferior | -335,59 | |
| | | Límite superior | 5756,16 | |
| | Media recortada al 5% | | 2471,26 | |
| | Mediana | | 1171,00 | |
| | Varianza | | 10846410,905 | |
| | Desv. Desviación | | 3293,389 | |
| | Mínimo | | 395 | |
| | Máximo | | 9328 | |
| | Rango | | 8933 | |
| | Rango intercuartil | | 4212 | |
| | Asimetría | | 1,702 | ,794 |
| | Curtosis | | 2,585 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_Througput _SinVPN** | Media | | 2821,71 | 1295,199 |
| | 95% de intervalo de confianza para la media | Límite inferior | -347,52 | |
| | | Límite superior | 5990,95 | |
| | Media recortada al 5% | | 2573,40 | |
| | Mediana | | 1219,00 | |
| | Varianza | | 11742788,238 | |
| | Desv. Desviación | | 3426,775 | |
| | Mínimo | | 411 | |
| | Máximo | | 9702 | |
| | Rango | | 9291 | |
| | Rango intercuartil | | 4396 | |
| | Asimetría | | 1,698 | ,794 |
| | Curtosis | | 2,563 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Througput _ProtonVPN** | Media | | 779,71 | 330,961 |
| | 95% de intervalo de confianza para la media | Límite inferior | -30,12 | |
| | | Límite superior | 1589,55 | |
| | Media recortada al 5% | | 723,74 | |
| | Mediana | | 366,00 | |
| | Varianza | | 766744,238 | |
| | Desv. Desviación | | 875,639 | |
| | Mínimo | | 123 | |
| | Máximo | | 2444 | |
| | Rango | | 2321 | |
| | Rango intercuartil | | 1318 | |
| | Asimetría | | 1,428 | ,794 |
| | Curtosis | | 1,264 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Througput _TunnelBear** | Media | | 959,71 | 360,032 |
| | 95% de intervalo de confianza para la media | Límite inferior | 78,75 | |
| | | Límite superior | 1840,68 | |
| | Media recortada al 5% | | 918,07 | |
| | Mediana | | 512,00 | |
| | Varianza | | 907360,571 | |
| | Desv. Desviación | | 952,555 | |
| | Mínimo | | 172 | |
| | Máximo | | 2497 | |
| | Rango | | 2325 | |
| | Rango intercuartil | | 1846 | |
| | Asimetría | | ,965 | ,794 |
| | Curtosis | | -,867 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Througput _NordVPN** | Media | | 1109,57 | 393,795 |
| | 95% de intervalo de confianza para la media | Límite inferior | 145,99 | |
| | | Límite superior | 2073,15 | |
| | Media recortada al 5% | | 1084,36 | |
| | Mediana | | 514,00 | |
| | Varianza | | 1085520,286 | |
| | Desv. Desviación | | 1041,883 | |
| | Mínimo | | 173 | |
| | Máximo | | 2500 | |
| | Rango | | 2327 | |
| | Rango intercuartil | | 1855 | |
| | Asimetría | | ,414 | ,794 |
| | Curtosis | | -2,447 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Througput _SinVPN** | Media | | 1387,86 | 358,775 |
| | 95% de intervalo de confianza para la media | Límite inferior | 509,97 | |
| | | Límite superior | 2265,75 | |
| | Media recortada al 5% | | 1384,12 | |
| | Mediana | | 1172,00 | |
| | Varianza | | 901036,143 | |
| | Desv. Desviación | | 949,229 | |
| | Mínimo | | 395 | |
| | Máximo | | 2448 | |
| | Rango | | 2053 | |
| | Rango intercuartil | | 1932 | |
| | Asimetría | | ,158 | ,794 |
| | Curtosis | | -2,550 | 1,587 |

Para el caso del indicador throughput, el mayor valor promedio (media) se observó en el software licenciado (NordVPN) con un registro de 2710,29 en comparación con el software gratuito (TunnelBear) que registra una media mayor de 2429,43 en el sistema operativo Windows 10 y por último el software licenciado (NordVPN) con un registro 2429,43 en el sistema operativo Linux – distribución Ubuntu 16.4. De igual modo, en la desviación de error quien aún se mantiene por tener mayor efecto en los resultados es el software licenciado (NordVPN) con un registro de 1244,784 en comparación con el software gratuito (TunnelBear) con un registro de 1116,508 en el sistema operativo Windows 10 y por último el software licenciado (NordVPN) con un registro de 393,795 en el sistema operativo Linux – distribución Ubuntu 16.4.

**Prueba descriptiva para el indicador jitter de la variable rendimiento del software.**

Tabla 2 Resultados de la prueba descriptiva para el indicador jitter en base a los softwares VPN y sin software VPN

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_Jitter_Pro-tonVPN** | Media | | ,70943 | ,310634 |
| | 95% de intervalo de confianza para la media | -,05067 | | |
| | | 1,46952 | | |
| | Media recortada al 5% | | ,65981 | |
| | Mediana | | ,31400 | |
| | Varianza | | ,675 | |

| | | | |
|---|---|---|---|
| | Desv. Desviación | ,821861 | |
| | Mínimo | ,057 | |
| | Máximo | 2,255 | |
| | Rango | 2,198 | |
| | Rango intercuartil | 1,098 | |
| | Asimetría | 1,253 | ,794 |
| | Curtosis | 1,015 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_Jitter_Tunnel-Bear** | Media | | ,05529 | ,009299 |
| | 95% de intervalo de confianza para la media | ,03253 | | |
| | | ,07804 | | |
| | Media recortada al 5% | | ,05443 | |
| | Mediana | | ,04500 | |
| | Varianza | | ,001 | |
| | Desv. Desviación | | ,024602 | |
| | Mínimo | | ,026 | |
| | Máximo | | ,100 | |
| | Rango | | ,074 | |
| | Rango intercuartil | | ,031 | |
| | Asimetría | | ,957 | ,794 |
| | Curtosis | | ,818 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_Jitter_NordVPN** | Media | | ,12986 | ,047284 |
| | 95% de intervalo de confianza para la media | ,01416 | | |
| | | ,24556 | | |
| | Media recortada al 5% | | ,12590 | |
| | Mediana | | ,08400 | |
| | Varianza | | ,016 | |
| | Desv. Desviación | | ,125102 | |
| | Mínimo | | ,021 | |
| | Máximo | | ,310 | |
| | Rango | | ,289 | |
| | Rango intercuartil | | ,276 | |
| | Asimetría | | 1,028 | ,794 |
| | Curtosis | | -1,001 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_Jitter_SinVPN** | Media | | ,24757 | ,144717 |
| | 95% de intervalo de confianza para la media | -,10654 | | |
| | | ,60168 | | |
| | Media recortada al 5% | | ,21397 | |
| | Mediana | | ,07200 | |
| | Varianza | | ,147 | |
| | Desv. Desviación | | ,382884 | |
| | Mínimo | | ,018 | |
| | Máximo | | 1,082 | |
| | Rango | | 1,064 | |
| | Rango intercuartil | | ,284 | |
| | Asimetría | | 2,263 | ,794 |
| | Curtosis | | 5,297 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Jitter_ProtonVPN** | Media | | ,02914 | ,006881 |
| | 95% de intervalo de confianza para la media | ,01230 | | |
| | | ,04598 | | |
| | Media recortada al 5% | | ,02799 | |
| | Mediana | | ,02900 | |
| | Varianza | | ,000 | |
| | Desv. Desviación | | ,018206 | |
| | Mínimo | | ,013 | |
| | Máximo | | ,066 | |
| | Rango | | ,053 | |
| | Rango intercuartil | | ,018 | |
| | Asimetría | | 1,602 | ,794 |
| | Curtosis | | 2,982 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Jitter_TunnelBear** | Media | | ,03014 | ,005462 |
| | 95% de intervalo de confianza para la media | ,01678 | | |
| | | ,04351 | | |
| | Media recortada al 5% | | ,02994 | |
| | Mediana | | ,02600 | |
| | Varianza | | ,000 | |
| | Desv. Desviación | | ,014450 | |
| | Mínimo | | ,013 | |
| | Máximo | | ,051 | |
| | Rango | | ,038 | |
| | Rango intercuartil | | ,028 | |
| | Asimetría | | ,724 | ,794 |
| | Curtosis | | -,972 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Jitter_NordVPN** | Media | | ,03943 | ,004669 |
| | 95% de intervalo de confianza para la media | ,02800 | | |
| | | ,05085 | | |
| | Media recortada al 5% | | ,03903 | |
| | Mediana | | ,03300 | |
| | Varianza | | ,000 | |
| | Desv. Desviación | | ,012354 | |
| | Mínimo | | ,028 | |
| | Máximo | | ,058 | |
| | Rango | | ,030 | |
| | Rango intercuartil | | ,023 | |
| | Asimetría | | ,612 | ,794 |
| | Curtosis | | -1,708 | 1,587 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_Jitter_SinVPN** | Media | | ,07757 | ,023696 |
| | 95% de intervalo de confianza para la media | ,01959 | | |
| | | ,13555 | | |
| | Media recortada al 5% | | ,07491 | |
| | Mediana | | ,05800 | |
| | Varianza | | ,004 | |
| | Desv. Desviación | | ,062695 | |
| | Mínimo | | ,020 | |
| | Máximo | | ,183 | |
| | Rango | | ,163 | |
| | Rango intercuartil | | ,126 | |
| | Asimetría | | 1,030 | ,794 |
| | Curtosis | | -,328 | 1,587 |

Para el caso del indicador jitter, la media de menor valor se observó en el software libre ProtonVPN con un registro de 0,02914 en comparación con el software gratuito (TunnelBear) con un registro de 0,03014 dejando en tercer lugar al software licenciado (NordVPN) con un registro de 0,03943 en el sistema operativo Linux – distribución Ubuntu 6.4. Además, en la desviación de error quien obtuvo el menor efecto del jitter en los resultados es el software licenciado (NordVPN) con un registro de ,004669 en comparación con el software gratuito (TunnelBear) con una media menor a 0,005462 y por último con un registro de 0,006881 el software libre (ProtonVPN) provenientes del sistema operativo Linux – distribución Ubuntu 16.4.

**Prueba descriptiva para el indicador uso del CPU de la variable administración de recursos**

Tabla 3 Resultados de la prueba descriptiva para el indicador uso del CPU en base a los softwares VPN y sin software VPN.

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_ _usoCPU_Pro-tonVPN** | Media | | 23,20 | 5,302 |
| | 95% de intervalo de confianza para la media | 12,10 | | |
| | | 34,30 | | |
| | Media recortada al 5% | | 19,94 | |
| | Mediana | | 14,50 | |
| | Varianza | | 562,274 | |
| | Desv. Desviación | | 23,712 | |
| | Mínimo | | 5 | |
| | Máximo | | 100 | |
| | Rango | | 95 | |
| | Rango intercuartil | | 15 | |
| | Asimetría | | 2,335 | ,512 |
| | Curtosis | | 5,645 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_ _usoCPU_Tun-nelBear** | Media | | 9,55 | 4,437 |
| | 95% de intervalo de confianza para la media | ,26 | | |
| | | 18,84 | | |
| | Media recortada al 5% | | 6,61 | |
| | Mediana | | 3,00 | |
| | Varianza | | 393,734 | |
| | Desv. Desviación | | 19,843 | |
| | Mínimo | | 0 | |
| | Máximo | | 72 | |
| | Rango | | 72 | |
| | Rango intercuartil | | 2 | |
| | Asimetría | | 2,857 | ,512 |
| | Curtosis | | 7,097 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W _usoCPU_Nord VPN** | Media | | 26,85 | 6,370 |
| | 95% de intervalo de confianza para la media | 13,52 | | |
| | | 40,18 | | |
| | Media recortada al 5% | | 25,72 | |
| | Mediana | | 9,50 | |
| | Varianza | | 811,608 | |
| | Desv. Desviación | | 28,489 | |
| | Mínimo | | 0 | |
| | Máximo | | 74 | |
| | Rango | | 74 | |
| | Rango intercuartil | | 57 | |
| | Asimetría | | ,529 | ,512 |
| | Curtosis | | -1,684 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoCPU_sinVPN | Media | | 5,05 | 1,585 |
| | 95% de intervalo de confianza para la media | 1,73 | | |
| | | 8,37 | | |
| | Media recortada al 5% | | 3,89 | |
| | Mediana | | 3,00 | |
| | Varianza | | 50,261 | |
| | Desv. Desviación | | 7,089 | |
| | Mínimo | | 1 | |
| | Máximo | | 30 | |
| | Rango | | 29 | |
| | Rango intercuartil | | 5 | |
| | Asimetría | | 2,812 | ,512 |
| | Curtosis | | 8,413 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoCPU_ProtonVPN | Media | | ,85 | ,274 |
| | 95% de intervalo de confianza para la media | ,28 | | |
| | | 1,42 | | |
| | Media recortada al 5% | | ,67 | |
| | Mediana | | 1,00 | |
| | Varianza | | 1,503 | |
| | Desv. Desviación | | 1,226 | |
| | Mínimo | | 0 | |
| | Máximo | | 5 | |
| | Rango | | 5 | |
| | Rango intercuartil | | 1 | |
| | Asimetría | | 2,410 | ,512 |
| | Curtosis | | 6,785 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoCPU_TunnelBear | Media | | 9,55 | 2,687 |
| | 95% de intervalo de confianza para la media | 3,93 | | |
| | | 15,17 | | |
| | Media recortada al 5% | | 8,78 | |
| | Mediana | | 4,00 | |
| | Varianza | | 144,366 | |
| | Desv. Desviación | | 12,015 | |
| | Mínimo | | 0 | |
| | Máximo | | 33 | |
| | Rango | | 33 | |
| | Rango intercuartil | | 22 | |
| | Asimetría | | 1,000 | ,512 |
| | Curtosis | | -,820 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoCPU_NordVPN | Media | | 4,00 | ,000 |
| | 95% de intervalo de confianza para la media | 4,00 | | |
| | | 4,00 | | |
| | Media recortada al 5% | | 4,00 | |
| | Mediana | | 4,00 | |
| | Varianza | | ,000 | |
| | Desv. Desviación | | ,000 | |
| | Mínimo | | 4 | |
| | Máximo | | 4 | |
| | Rango | | 0 | |
| | Rango intercuartil | | 0 | |
| | Asimetría | | . | . |
| | Curtosis | | . | . |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoCPU_sinVPN | Media | | 1,10 | ,069 |
| | 95% de intervalo de confianza para la media | ,96 | | |
| | | 1,24 | | |
| | Media recortada al 5% | | 1,06 | |
| | Mediana | | 1,00 | |
| | Varianza | | ,095 | |
| | Desv. Desviación | | ,308 | |
| | Mínimo | | 1 | |
| | Máximo | | 2 | |
| | Rango | | 1 | |
| | Rango intercuartil | | 0 | |
| | Asimetría | | 2,888 | ,512 |
| | Curtosis | | 7,037 | ,992 |

Para el caso del indicador uso del CPU, el valor media menor se observó en el software libre (ProntonVPN) con un registro de 0,85 en comparación con el software licenciado (NordVPN) que registra una media menor a 4,00 y por último el software gratuito (TunnelBear) del sistema operativo Windows 10 y el software gratuito (TunnelBear) con un registro de 9,55 en el sistema operativo Linux – distribución Ubuntu 16.4. De igual modo, en la desviación de error quien mantiene un valor mínimo es el software licenciado (NordVPN) con un registro de 0,00E0 en comparación con el software libre (ProtonVPN) con un registro de 0,274 en el sistema operativo Linux – distribución Ubuntu 16.4 y por el último el software gratuito (TunnelBear) con un registro de 4,437 en el sistema operativo Windows 10.

**Prueba descriptiva para el indicador uso de memoria RAM de la variable administración de recursos**

Tabla 4 Resultados de la prueba descriptiva para el indicador uso de memoria RAM en base a los softwares VPN y sin software VPN.

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoMemoriaRAM_ProtonVPN | Media | | 66,10 | 2,234 |
| | 95% de intervalo de confianza para la media | 61,43 | | |
| | | 70,77 | | |
| | Media recortada al 5% | | 66,44 | |
| | Mediana | | 68,50 | |
| | Varianza | | 99,779 | |
| | Desv. Desviación | | 9,989 | |
| | Mínimo | | 43 | |
| | Máximo | | 83 | |
| | Rango | | 40 | |
| | Rango intercuartil | | 12 | |
| | Asimetría | | -,586 | ,512 |
| | Curtosis | | ,194 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoMemoriaRAM_TunnelBear | Media | | 67,95 | 1,321 |
| | 95% de intervalo de confianza para la media | 65,19 | | |
| | | 70,71 | | |
| | Media recortada al 5% | | 68,11 | |
| | Mediana | | 68,00 | |
| | Varianza | | 34,892 | |
| | Desv. Desviación | | 5,907 | |
| | Mínimo | | 56 | |
| | Máximo | | 77 | |
| | Rango | | 21 | |
| | Rango intercuartil | | 8 | |
| | Asimetría | | -,457 | ,512 |
| | Curtosis | | -,026 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoMemoriaRAM_NordVPN | Media | | 67,45 | 1,658 |
| | 95% de intervalo de confianza para la media | 63,98 | | |
| | | 70,92 | | |
| | Media recortada al 5% | | 67,50 | |
| | Mediana | | 69,00 | |
| | Varianza | | 54,997 | |
| | Desv. Desviación | | 7,416 | |
| | Mínimo | | 54 | |
| | Máximo | | 80 | |
| | Rango | | 26 | |
| | Rango intercuartil | | 11 | |
| | Asimetría | | -,363 | ,512 |
| | Curtosis | | -,606 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoMemoriaRAM_sinVPN | Media | | 41,95 | ,170 |
| | 95% de intervalo de confianza para la media | 41,59 | | |
| | | 42,31 | | |
| | Media recortada al 5% | | 41,94 | |
| | Mediana | | 42,00 | |
| | Varianza | | ,576 | |
| | Desv. Desviación | | ,759 | |
| | Mínimo | | 41 | |
| | Máximo | | 43 | |
| | Rango | | 2 | |
| | Rango intercuartil | | 2 | |
| | Asimetría | | ,086 | ,512 |
| | Curtosis | | -1,154 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoMemoriaRAM_Proton VPN | Media | | 69,600 | ,1005 |
| | 95% de intervalo de confianza para la media | 69,390 | | |
| | | 69,810 | | |
| | Media recortada al 5% | | 69,622 | |
| | Mediana | | 69,600 | |
| | Varianza | | ,202 | |
| | Desv. Desviación | | ,4496 | |
| | Mínimo | | 68,8 | |
| | Máximo | | 70,0 | |
| | Rango | | 1,2 | |
| | Rango intercuartil | | ,4 | |
| | Asimetría | | -,989 | ,512 |
| | Curtosis | | -,279 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoMemoriaRAM_Tunnel Bear | Media | | 91,235 | ,8650 |
| | 95% de intervalo de confianza para la media | 89,425 | | |
| | | 93,045 | | |
| | Media recortada al 5% | | 92,100 | |
| | Mediana | | 92,100 | |
| | Varianza | | 14,964 | |
| | Desv. Desviación | | 3,8684 | |
| | Mínimo | | 74,8 | |
| | Máximo | | 92,1 | |
| | Rango | | 17,3 | |
| | Rango intercuartil | | ,0 | |
| | Asimetría | | -4,472 | ,512 |
| | Curtosis | | 20,000 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoMemoria-RAM_NordVPN | Media | | 82,725 | ,1279 |
| | 95% de intervalo de confianza para la media | 82,457 | | |
| | | 82,993 | | |
| | Media recortada al 5% | | 82,822 | |
| | Mediana | | 82,900 | |
| | Varianza | | ,327 | |
| | Desv. Desviación | | ,5720 | |
| | Mínimo | | 80,5 | |
| | Máximo | | 83,2 | |
| | Rango | | 2,7 | |
| | Rango intercuartil | | ,4 | |
| | Asimetría | | -3,340 | ,512 |
| | Curtosis | | 13,113 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| U_usoMemo-ria-RAM_sinVPN | Media | | 31,055 | ,0600 |
| | 95% de intervalo de confianza para la media | 30,929 | | |
| | | 31,181 | | |
| | Media recortada al 5% | | 31,106 | |
| | Mediana | | 31,150 | |
| | Varianza | | ,072 | |
| | Desv. Desviación | | ,2685 | |
| | Mínimo | | 30,0 | |
| | Máximo | | 31,2 | |
| | Rango | | 1,2 | |
| | Rango intercuartil | | ,2 | |
| | Asimetría | | -3,470 | ,512 |
| | Curtosis | | 13,756 | ,992 |

Referente a las tablas anteriores, se evidencia que el software libre (ProtonVPN) muestra una media baja de 66,10 en comparación con el software licenciado (NordVPN) que registra una media de 67,45 y por último el software gratuito (TunnelBear) con una media de 67,95 en base al sistema operativo Windows. De igual modo, quien tiene una tasa mínima de desviación errónea es el software gratuito (ProtonVPN) con un registro de 0,1005 en comparación con el software licenciado (NordVPN) con una tasa mínima de 0,1279 y por último el software gratuito (TunnelBear) con un registro de 0,8650 en el sistema operativo Linux – distribución Ubuntu 16.4.

**Prueba descriptiva para el indicador uso del Disco Duro de la variable administración de recursos**

Tabla 5 Resultados de la prueba descriptiva para el indicador uso del Disco Duro en base a los softwares VPN y sin software VPN.

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoDisco-Duro_ProtonVPN | Media | | 23,20 | 5,302 |
| | 95% de intervalo de confianza para la media | 12,10 | | |
| | | 34,30 | | |
| | Media recortada al 5% | | 19,94 | |
| | Mediana | | 14,50 | |
| | Varianza | | 562,274 | |
| | Desv. Desviación | | 23,712 | |
| | Mínimo | | 5 | |
| | Máximo | | 100 | |
| | Rango | | 95 | |
| | Rango intercuartil | | 15 | |
| | Asimetría | | 2,335 | ,512 |
| | Curtosis | | 5,645 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoDisco-Duro_TunnelBear | Media | | 9,55 | 4,437 |
| | 95% de intervalo de confianza para la media | ,26 | | |
| | | 18,84 | | |
| | Media recortada al 5% | | 6,61 | |
| | Mediana | | 3,00 | |
| | Varianza | | 393,734 | |
| | Desv. Desviación | | 19,843 | |
| | Mínimo | | 0 | |
| | Máximo | | 72 | |
| | Rango | | 72 | |
| | Rango intercuartil | | 2 | |
| | Asimetría | | 2,857 | ,512 |
| | Curtosis | | 7,097 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoDisco-Duro_NordVPN | Media | | 26,85 | 6,370 |
| | 95% de intervalo de confianza para la media | 13,52 | | |
| | | 40,18 | | |
| | Media recortada al 5% | | 25,72 | |
| | Mediana | | 9,50 | |
| | Varianza | | 811,608 | |
| | Desv. Desviación | | 28,489 | |
| | Mínimo | | 0 | |
| | Máximo | | 74 | |
| | Rango | | 74 | |
| | Rango intercuartil | | 57 | |
| | Asimetría | | ,529 | ,512 |
| | Curtosis | | -1,684 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| W_usoDisco-Duro_sinVPN | Media | | 5,05 | 1,585 |
| | 95% de intervalo de confianza para la media | 1,73 | | |
| | | 8,37 | | |
| | Media recortada al 5% | | 3,89 | |
| | Mediana | | 3,00 | |
| | Varianza | | 50,261 | |
| | Desv. Desviación | | 7,089 | |
| | Mínimo | | 1 | |

| | | | |
|---|---|---|---|
| | Máximo | 30 | |
| | Rango | 29 | |
| | Rango intercuartil | 5 | |
| | Asimetría | 2,812 | ,512 |
| | Curtosis | 8,413 | ,992 |

**Descriptivos**

| | | | Estadístico | Desv. Error |
|---|---|---|---|---|
| **U_usoDisco-Duro_ProtonVPN** | Media | | ,85 | ,274 |
| | 95% de intervalo de confianza para la media | ,28 | | |
| | | 1,42 | | |
| | Media recortada al 5% | | ,67 | |
| | Mediana | | 1,00 | |
| | Varianza | | 1,503 | |
| | Desv. Desviación | | 1,226 | |
| | Mínimo | | 0 | |
| | Máximo | | 5 | |
| | Rango | | 5 | |
| | Rango intercuartil | | 1 | |
| | Asimetría | | 2,410 | ,512 |
| | Curtosis | | 6,785 | ,992 |

**Descriptivos**

| | | | Estadístico | Desv. Error |
|---|---|---|---|---|
| **U_usoDisco-Duro_TunnelBear** | Media | | 9,55 | 2,687 |
| | 95% de intervalo de confianza para la media | 3,93 | | |
| | | 15,17 | | |
| | Media recortada al 5% | | 8,78 | |
| | Mediana | | 4,00 | |
| | Varianza | | 144,366 | |
| | Desv. Desviación | | 12,015 | |
| | Mínimo | | 0 | |
| | Máximo | | 33 | |
| | Rango | | 33 | |
| | Rango intercuartil | | 22 | |
| | Asimetría | | 1,000 | ,512 |
| | Curtosis | | -,820 | ,992 |

**Descriptivos**

| | | | Estadístico | Desv. Error |
|---|---|---|---|---|
| **U_usoDisco-Duro_NordVPN** | Media | | 3,80 | ,200 |
| | 95% de intervalo de confianza para la media | 3,38 | | |
| | | 4,22 | | |
| | Media recortada al 5% | | 4,00 | |
| | Mediana | | 4,00 | |
| | Varianza | | ,800 | |
| | Desv. Desviación | | ,894 | |
| | Mínimo | | 0 | |
| | Máximo | | 4 | |
| | Rango | | 4 | |
| | Rango intercuartil | | 0 | |
| | Asimetría | | -4,472 | ,512 |
| | Curtosis | | 20,000 | ,992 |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **U_usoDisco-Duro_sinVPN** | Media | | 1,10 | ,069 |
| | 95% de intervalo de confianza para la media | ,96 | | |
| | | 1,24 | | |
| | Media recortada al 5% | | 1,06 | |
| | Mediana | | 1,00 | |
| | Varianza | | ,095 | |
| | Desv. Desviación | | ,308 | |
| | Mínimo | | 1 | |
| | Máximo | | 2 | |
| | Rango | | 1 | |
| | Rango intercuartil | | 0 | |
| | Asimetría | | 2,888 | ,512 |
| | Curtosis | | 7,037 | ,992 |

Referente a las tablas anteriores, se evidencia que el software libre (ProtonVPN) muestra una media baja de 0,85 en comparación con el software licenciado (NordVPN) que registra una media de 4,00 en base al sistema operativo Linux – distribución Ubuntu 16.4 y por último el software gratuito (TunnelBear) del sistema operativo Windows 10 con el software gratuito (TunnelBear) en base al sistema operativo Linux – distribución Ubuntu 16.4 toman la posición de tercer lugar ante ataques DDoS con una media de 9, 55. De igual modo, quien tiene una tasa mínima de desviación errónea es el software licenciado (NordVPN) con un registro de 0,0E0 en comparación con el software libre (ProntonVPN) con una tasa mínima de 0, 274 y por último el software gratuito (TunnelBear) con un registro de 2,687 en el sistema operativo Linux – distribución Ubuntu 16.4.

**Prueba descriptiva para el indicador conexión al servidor VPN de la variable administración de recursos**

Tabla 6 Resultados de la prueba descriptiva para el indicador conexión al servidor VPN en base a los softwares VPN y sin software VPN.

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_ProtonVPN** | Media | | 12,94833 | ,358032 |
| | 95% de intervalo de confianza para la media | 11,40784 | | |
| | | 14,48882 | | |
| | Media recortada al 5% | | . | |
| | Mediana | | 12,66900 | |
| | Varianza | | ,385 | |
| | Desv. Desviación | | ,620130 | |
| | Mínimo | | 12,517 | |
| | Máximo | | 13,659 | |
| | Rango | | 1,142 | |
| | Rango intercuartil | | . | |
| | Asimetría | | 1,616 | 1,225 |
| | Curtosis | | . | . |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_TunnelBear** | Media | | 12,41600 | ,892753 |
| | 95% de intervalo de confianza para la media | 8,57479 | | |
| | | 16,25721 | | |
| | Media recortada al 5% | | . | |
| | Mediana | | 12,07600 | |
| | Varianza | | 2,391 | |
| | Desv. Desviación | | 1,546294 | |
| | Mínimo | | 11,068 | |
| | Máximo | | 14,104 | |
| | Rango | | 3,036 | |
| | Rango intercuartil | | . | |
| | Asimetría | | ,942 | 1,225 |
| | Curtosis | | . | . |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **W_NordVPN** | Media | | 6,77767 | 2,614237 |
| | 95% de intervalo de confianza para la media | -4,47049 | | |
| | | 18,02582 | | |
| | Media recortada al 5% | | . | |
| | Mediana | | 4,66400 | |
| | Varianza | | 20,503 | |
| | Desv. Desviación | | 4,527992 | |
| | Mínimo | | 3,693 | |
| | Máximo | | 11,976 | |
| | Rango | | 8,283 | |
| | Rango intercuartil | | . | |
| | Asimetría | | 1,643 | 1,225 |
| | Curtosis | | . | . |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **L_ProtonVPN** | Media | | 10,39133 | 1,868203 |
| | 95% de intervalo de confianza para la media | 2,35310 | | |
| | | 18,42956 | | |
| | Media recortada al 5% | | . | |
| | Mediana | | 9,78900 | |
| | Varianza | | 10,471 | |
| | Desv. Desviación | | 3,235822 | |
| | Mínimo | | 7,499 | |
| | Máximo | | 13,886 | |
| | Rango | | 6,387 | |
| | Rango intercuartil | | . | |
| | Asimetría | | ,809 | 1,225 |
| | Curtosis | | . | . |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **L_TunnelBear** | Media | | 4,28433 | ,284742 |
| | 95% de intervalo de confianza para la media | 3,05919 | | |
| | | 5,50948 | | |
| | Media recortada al 5% | | . | |
| | Mediana | | 4,18100 | |
| | Varianza | | ,243 | |
| | Desv. Desviación | | ,493187 | |
| | Mínimo | | 3,851 | |
| | Máximo | | 4,821 | |
| | Rango | | ,970 | |
| | Rango intercuartil | | . | |
| | Asimetría | | ,901 | 1,225 |
| | Curtosis | | . | . |

| Descriptivos | | | | |
|---|---|---|---|---|
| | | | Estadístico | Desv. Error |
| **L_NordVPN** | Media | | 5,08800 | ,979110 |
| | 95% de intervalo de confianza para la media | ,87523 | | |
| | | 9,30077 | | |
| | Media recortada al 5% | | . | |
| | Mediana | | 5,40500 | |
| | Varianza | | 2,876 | |
| | Desv. Desviación | | 1,695868 | |
| | Mínimo | | 3,256 | |
| | Máximo | | 6,603 | |
| | Rango | | 3,347 | |
| | Rango intercuartil | | . | |
| | Asimetría | | -,812 | 1,225 |
| | Curtosis | | . | . |

Referente a las tablas anteriores, se evidencia que el software gratuito (TunnelBear) muestra una media baja 4,28 en comparación con el software licenciado (NordVPN) que registra una media de 5,08 en base al sistema operativo Linux – distribución Ubuntu 16.4 y por último el software licenciado (NordVPN) del sistema operativo Windows 10 toma la posición de tercer lugar con una media de 6,77. De igual modo, quien tiene una tasa mínima de desviación errónea es el software gratuito (TunnelBear) con un registro de 0,284 en el sistema operativo Linux – distribución Ubuntu 16.4 en comparación con el software libre (ProntonVPN) con una tasa mínima de 0, 358 y por último el software gratuito (TunnelBear) con un registro de 0,893 en el sistema operativo Windows 10.

**Prueba de Normalidad**

Se empleó la prueba de normalidad para verificar si los resultados obtenidos de las evaluaciones mantienen una distribución normal, por ello, se debe considerar la cantidad de la muestra al elegir el tipo de prueba adecuada (Shapiro-Wilk o Kolmogorov- Smirnov) (Pacotaype, 2018, p.92). Además, la data es confrontada con el nivel de significancia para aceptar o rechazar las hipótesis planteadas, se identifican de la siguiente forma:

**Ho:** Los datos siguen una distribución normal (Pacotaype, 2018, p.92)

**Ha:** Los datos no siguen una distribución normal (Pacotaype, 2018, p.92)

Nivel de significancia: α=0,05. Entonces, cuando p ≤ α: se rechaza la Ho; o por el contrario p > α: se acepta la Ho (Pacotaype, 2018, p.92).

## 4.2 Prueba de hipótesis

### Variable Rendimiento del software

Se analizó atendiendo dos indicadores, *throughput* y *jitter* en la transferencia de datos al utilizar los softwares de redes privadas virtuales en los sujetos de pruebas, de lo cual los resultados extraídos de las evaluaciones se llevó a cabo el uso de las pruebas de normalidad y dependiendo el resultado se empleaba pruebas paramétricas y no paramétricas para muestras relacionadas, respectivamente. Se determinan las hipótesis con la finalidad de aceptar o rechazar en cada caso con respecto a la media y significancia de los resultados.

### 4. 2.1 Hipótesis específicas HE1

$\mathbf{HE1_0}$: La aplicación de los procesos de la metodología MEPVPNS no permitió la evaluación de los softwares de redes privadas virtuales en cuanto al rendimiento del software.

$\mathbf{HE1_1}$**:** La aplicación de los procesos de la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al rendimiento del software.

A continuación, se especifica los resultados extraídos conforme a las evaluaciones realizadas a través del proceso de la evaluación del rendimiento del software.

**Prueba de normalidad para el indicador throughput de la variable rendimiento del software.**

Para el proceso del indicador throughput para evaluar la prueba de normalidad se utilizó Shapiro-Wilk dado que la cantidad de la muestra es < 50.

Tabla 7 Resultados de prueba de normalidad del indicador throughput.

| | Pruebas de normalidad | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| **W_Througput_ ProtonVPN** | ,259 | 7 | ,171 | ,771 | 7 | ,021 |
| **W_Througput_ TunnelBear** | ,259 | 7 | ,172 | ,772 | 7 | ,022 |
| **W_Througput_ NordVPN** | ,259 | 7 | ,173 | ,773 | 7 | ,022 |
| **W_Througput_ SinVPN** | ,259 | 7 | ,171 | ,773 | 7 | ,022 |
| **U_Througput_ ProtonVPN** | ,253 | 7 | ,195 | ,804 | 7 | ,045 |
| **U_Througput_ TunnelBear** | ,252 | 7 | ,199 | ,823 | 7 | ,069 |
| **U_Througput_ NordVPN** | ,288 | 7 | ,083 | ,789 | 7 | ,031 |
| **U_Througput_ SinVPN** | ,246 | 7 | ,200* | ,815 | 7 | ,057 |

Por ello, los datos de significancia que sean menores α=0,05 se toman como pruebas no paramétricas, es decir, no siguen una distribución normal. No obstante, se han registrado datos mayores y menores α=0,05 evitando aceptar o rechazar la Ho (distribución normal). En síntesis, se utilizaron pruebas paramétricas y no paramétricas para las comparaciones en cuanto al indicador throughput.

Tabla 8 Resultados de prueba de Wilcoxon del indicador throughput en el sistema operativo Windows 10

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| **W_Throughput _ProtonVPN - W_Throughput _NordVPN** | Rangos negativos | 7[a] | 4,00 | 28,00 |
| | Rangos positivos | 0[b] | ,00 | ,00 |
| | Empates | 0[c] | | |
| | Total | 7 | | |
| **W_Throughput _TunnelBear - W_Throughput _NordVPN** | Rangos negativos | 7[d] | 4,00 | 28,00 |
| | Rangos positivos | 0[e] | ,00 | ,00 |
| | Empates | 0[f] | | |
| | Total | 7 | | |
| **W_Throughput _SinVPN - W_Throughput _NordVPN** | Rangos negativos | 0[g] | ,00 | ,00 |
| | Rangos positivos | 7[h] | 4,00 | 28,00 |
| | Empates | 0[i] | | |
| | Total | 7 | | |

Tabla 9 Resultados de prueba estadística de Wilcoxon del indicador throughput en el sistema operativo Windows 10

| Estadísticos de prueba[a] | | | |
|---|---|---|---|
| | **W_Througput_ ProtonVPN - W_Througput_ NordVPN** | **W_Througput_ TunnelBear - W_Througput_ NordVPN** | **W_Througput_Sin VPN - W_Througput_Nor dVPN** |
| Z | -2,366[b] | -2,366[b] | -2,366[c] |
| Sig. Asintótica (bilateral) | ,018 | ,018 | ,018 |

Tal y como se observa en las tablas anteriores, se puede evidenciar que el software licenciado (NordVPN) mantiene un mayor rendimiento frente al software gratuito (TunnelBear) y libre (ProtonVPN) en el sistema operativo Windows 10. Además, quien le sigue en el rango de la prueba de evaluación es el software gratuito (TunnelBear) y dejando al ProtonVPN con el índice más bajo al momento de medir el throughput en la transferencia de datos (**Tabla 8**). De acuerdo a la **Tabla 9,** se observa los niveles de significancia asintótica equivalentes a 0,018 comparando NordVPN con ProtonVPN y TunnelBear.

Tabla 10 Resultados de prueba de wilcoxon del indicador throughput en el sistema operativo Linux- Distribución Ubuntu 16.

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| **U_Througput _ProtonVPN - U_Througput _NordVPN** | Rangos negativos | 7[a] | 4,00 | 28,00 |
| | Rangos positivos | 0[b] | ,00 | ,00 |
| | Empates | 0[c] | | |
| | Total | 7 | | |
| **U_Througput _TunnelBear - U_Througput _NordVPN** | Rangos negativos | 6[d] | 3,50 | 21,00 |
| | Rangos positivos | 0[e] | ,00 | ,00 |
| | Empates | 1[f] | | |
| | Total | 7 | | |
| **U_Througput _SinVPN - U_Througput _NordVPN** | Rangos negativos | 1[g] | 1,00 | 1,00 |
| | Rangos positivos | 6[h] | 4,50 | 27,00 |
| | Empates | 0[i] | | |
| | Total | 7 | | |

Tabla 11 Resultados de prueba estadística de Wilcoxon del indicador throughput en el sistema operativo Linux- Distribución Ubuntu 16.

| Estadísticos de prueba[a] | | | |
|---|---|---|---|
| | U_Througput_Proton VPN - U_Througput_NordV PN | U_Througput_TunnelBear - U_Througput_NordVPN | U_Througput_Sin VPN - U_Througput_NordV PN |
| Z | -2,366[b] | -2,207[b] | -2,197[c] |
| Sig. Asintótica (bilateral) | ,018 | ,027 | ,028 |

De acuerdo a la **Tabla 10**, se puede evidenciar que el software licenciado (NordVPN) mantiene un mayor rendimiento frente al software gratuito (TunnelBear) y libre (ProtonVPN) en el sistema operativo Linux - distribución Ubuntu 16.4. Además, quien le sigue en el rango de la prueba de evaluación es el software gratuito (TunnelBear) y dejando al software libre ProtonVPN con el índice más bajo al momento de medir el throughput en la transferencia de datos. De acuerdo a la **Tabla 11**, se observa los niveles de significancia asintótica equivalentes a 0,018 al comparar NordVPN con ProtonVPN; 0,027 al comparar NordVPN con TunnelBear y 0,028 al comparar NordVPN sin el software VPN.

Tabla 12 Resultados de prueba de rangos con signos de Wilcoxon del indicador throughput – Comparación entre S.O

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| U_Througput _NordVPN - W_Througput _NordVPN | Rangos negativos | 7[a] | 4,00 | 28,00 |
| | Rangos positivos | 0[b] | ,00 | ,00 |
| | Empates | 0[c] | | |
| | Total | 7 | | |

Tabla 13 Resultados de estadísticos de prueba de wilcoxon del indicador throughput – Comparación entre S.O

| Estadísticos de prueba | |
|---|---|
| | U_Througput_NordVPN - W_Througput_NordVPN |
| Z | -2,366[b] |
| Sig. Asintótica (bilateral) | ,018 |

De acuerdo a la **Tabla 12**, comparando las tecnologías de software VPN más resaltantes entre los sistemas operativos se pudo evidenciar que el software licenciado (NordVPN) del sistema operativo Windows 10 mantuvo una mayor media del throughput frente a la transferencia de datos. Además, a la **Tabla 13**, se observa los niveles de significancia asintótica equivalentes a 0,018 al comparar NordVPN de Windows 10 con NordVPN de Linux – Distribución Ubuntu 16.4.

Tabla 14 Resultados de la prueba t de student para muestras relacionadas del indicador throughput – Individuos paramétricos

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | Media | N | Desv. Desviación | Desv. Error promedio |
| Par 1 | W_Througput_Tunnel-Bear | 2429,43 | 7 | 2954,004 | 1116,508 |
| | U_Througput_SinVPN | 1387,86 | 7 | 949,229 | 358,775 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bi-late-ral) |
| | | Media | Desv. Desvia-ciónn | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | W_Througput _TunnelBear - U_Througput_SinVPN | 1041,571 | 2276,709 | 860,515 | -1064,034 | 3147,176 | 1,210 | 6 | ,272 |

De acuerdo a la **Tabla 14 a**, comparando el throughput con los resultados paramétricos se pudo evidenciar que el software gratuito (TunnelBear) en el sistema operativo Windows 10 tiene una media de 2429,43 ante una media de 1387,86 sin utilizar ninguna tecnología de software VPN en el sistema operativo Linux – Distribución Ubuntu 16.4 con una desviación de error promedio 1116,508 ante una desviación de error promedio de 358,775 correlativamente. Además, en la **Tabla 14 b**, se muestra que el 95% de intervalo de confianza inferior es de -1064,034 y superior es de 3147,176 en comparación con el TunnelBear y sin software VPN, con un intervalo de tiempo 1,210 y una significancia de 0,272**.**

En referencia a las tablas anteriores, se puede evidenciar que el software licenciado (NordVPN) mantiene un mayor rendimiento frente al software gratuito (TunnelBear) del sistema operativo Windows 10. Asimismo, el software licenciado (NordVPN) está posicionado en el tercer lugar en cuanto al rendimiento en el sistema operativo Linux - distribución Ubuntu 16.4. Además, quien le sigue en el rango de la prueba de evaluación es el software gratuito (TunnelBear), el software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 y dejando al software libre (ProtonVPN) en base al sistema operativo Windows 10 con el índice más bajo en cuanto al indicador throughput en la transferencia de datos. En síntesis, ***la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al rendimiento del software. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.***

**Prueba de normalidad para el indicador jitter de la variable rendimiento del software.**

Para el proceso del indicador jitter para evaluar la prueba de normalidad se utilizó Shapiro-Wilk dado que la cantidad de la muestra es < 50.

Tabla 15 Resultados de prueba de normalidad del indicador jitter

| Pruebas de normalidad | | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| **W_Jitter_ProtonVPN** | ,256 | 7 | ,182 | ,827 | 7 | ,075 |
| **W_Jitter_TunnelBear** | ,233 | 7 | ,200* | ,932 | 7 | ,570 |
| **W_Jitter_NordVPN** | ,309 | 7 | ,043 | ,776 | 7 | ,023 |
| **W_Jitter_SinVPN** | ,289 | 7 | ,078 | ,671 | 7 | ,002 |
| **U_Jitter_ProtonVPN** | ,252 | 7 | ,200* | ,823 | 7 | ,068 |
| **U_Jitter_TunnelBear** | ,246 | 7 | ,200* | ,877 | 7 | ,214 |
| **U_Jitter_NordVPN** | ,270 | 7 | ,132 | ,851 | 7 | ,126 |
| **U_Jitter_SinVPN** | ,325 | 7 | ,025 | ,835 | 7 | ,089 |

Por ello, los resultados de la prueba de normalidad del indicador jitter, muestra una significancia mayor de α=0,05 y menor de α=0,05 evitando rechazar o aceptar la Ho manteniendo una distribución normal y no normal, a lo se empleó la prueba t de student para muestras relacionadas paramétricas y prueba de Wilcoxon para pruebas no paramétricas para evaluar el indicador jitter.

Tabla 16 Resultados de prueba de rango con signos de wilcoxon del indicador jitter – entre S.O

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| **U_Jitter_ProtonVPN - W_Jitter_NordVPN** | Rangos negativos | 7[a] | 4,00 | 28,00 |
| | Rangos positivos | 0[b] | ,00 | ,00 |
| | Empates | 0[c] | | |
| | Total | 7 | | |

*Tabla 17 Resultados de prueba estadística de Wilcoxon del indicador jitter – entre S.O*

| Estadísticos de prueba | |
|---|---|
| | **U_Jitter_ProtonVPN - W_Jitter_NordVPN** |
| Z | -2,366[b] |
| Sig. Asintótica (bilateral) | ,018 |

En referencia a las **Tablas 16 y 17**, se pudo evidenciar que el software libre (ProtonVPN) del sistema operativo Linux –distribución Ubuntu 16.4 mantuvo una menor tasa de jitter frente al software licenciado (NordVPN) del sistema operativo Windows 10 con una significancia asintótica 0,018.

Tabla 18 Resultados de la prueba t de student para muestras relacionadas del indicador jitter en base al sistema operativo Windows 10

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | **Media** | **N** | **Desv. Desviación** | **Desv. Error promedio** |
| Par 1 | **W_Jitter_NordVPN** | ,12986 | 7 | ,125102 | ,047284 |
| | **W_Jitter_ProtonVPN** | ,70943 | 7 | ,821861 | ,310634 |
| Par 2 | **W_Jitter_NordVPN** | ,12986 | 7 | ,125102 | ,047284 |
| | **W_Jitter_TunnelBear** | ,05529 | 7 | ,024602 | ,009299 |
| Par 3 | **W_Jitter_NordVPN** | ,12986 | 7 | ,125102 | ,047284 |
| | **W_Jitter_SinVPN** | ,24757 | 7 | ,382884 | ,144717 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bilateral) |
| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la Diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | **W_Jitter_NordVPN - W_Jitter_ProtonVPN** | -,579571 | ,725642 | ,274267 | ,091535 | ,091535 | -2,113 | 6 | ,079 |
| Par 2 | **W_Jitter_NordVPN - W_Jitter_TunnelBear** | ,074571 | ,105962 | ,040050 | ,172570 | ,172570 | 1,862 | 6 | ,112 |
| Par 3 | **W_Jitter_NordVPN - W_Jitter_SinVPN** | -,117714 | ,327829 | ,123908 | ,185477 | ,185477 | -,950 | 6 | ,379 |

En la **Tabla 18,** se observó que el software gratuito (TunnelBear) registra una media baja de 0,05529 posicionándolo como el software con un índice menor de jitter registrado en las evaluaciones, dejando en segundo lugar al software licenciado (Nordvpn) con un registro de media 0,12986 y por último al software libre (ProtonVPN) con una media menor a ,70943 en el sistema operativo Windows 10.

Tabla 19 Resultados de la prueba t de student para muestras relacionadas del indicador jitter en base al sistema operativo Linux – distribución Ubuntu 16.4

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | **Media** | **N** | **Desv. Desviación** | **Desv. Error promedio** |
| Par 1 | **U_Jitter_NordVPN** | ,03943 | 7 | ,012354 | ,004669 |
| | **U_Jitter_ProtonVPN** | ,02914 | 7 | ,018206 | ,006881 |
| Par 2 | **U_Jitter_NordVPN** | ,03943 | 7 | ,012354 | ,004669 |
| | **U_Jitter_TunnelBear** | ,03014 | 7 | ,014450 | ,005462 |
| Par 3 | **U_Jitter_NordVPN** | ,03943 | 7 | ,012354 | ,004669 |
| | **U_Jitter_SinVPN** | ,07757 | 7 | ,062695 | ,023696 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bilateral) |
| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la Diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | **U_Jitter_NordVPN - U_Jitter_ProtonVPN** | ,010286 | ,022896 | ,008654 | -,010890 | ,031461 | 1,189 | 6 | ,280 |
| Par 2 | **U_Jitter_NordVPN - U_Jitter_TunnelBear** | ,009286 | ,013768 | ,005204 | -,003448 | ,022019 | 1,784 | 6 | ,125 |
| Par 3 | **U_Jitter_NordVPN - U_Jitter_SinVPN** | -,038143 | ,056531 | ,021367 | -,090426 | ,014140 | -1,785 | 6 | ,124 |

En la **Tabla 19**, se observó que el software libre (ProtonVPN) registra una media baja de 0,02914 posicionándolo como el software con un índice menor de jitter registrado en las evaluaciones, dejando en segundo lugar al software gratuito (TunnelBear) con un registro de media 0,03014 y por último al software licenciado (NordVPN) con una media menor a 0,03943 en el sistema operativo Linux – distribución Ubuntu 16.4.

Tabla 20 Resultados de la prueba t de student para muestras relacionadas del indicador jitter en base al sistema operativo Linux – distribución Ubuntu 16.4 – Comparación entre S.O

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | **Media** | **N** | **Desv. Desviación** | **Desv. Error promedio** |
| Par 1 | **W_Jitter_TunnelBear** | ,05529 | 7 | ,024602 | ,009299 |
| | **U_Jitter_ProtonVPN** | ,02914 | 7 | ,018206 | ,006881 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bilateral) |
| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la Diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | **W_Jitter_TunnelBear - U_Jitter_ProtonVPN** | ,026143 | ,029650 | ,011207 | -,001279 | ,053565 | 2,333 | 6 | ,058 |

En la **Tabla 20**, comparando las tecnologías de software VPN más resaltantes entre los sistemas operativos se pudo evidenciar queel software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4., con una media menor registrada de 0,02914 en comparación con el software gratuito (TunnelBear) del sistema operativo Windows 10 con una media registrada 0,05529 en referencia al indicador jitter.

En referencia a las tablas anteriores, se puede evidenciar que el software libre (ProtonVPN) mantiene una menor media de jitter frente al software gratuito (TunnelBear) y licenciado (NordVPN) en el sistema operativo Linux - distribución Ubuntu 16.4. Además, quien le sigue en el rango de la prueba de evaluación es el software gratuito (TunnelBear), el software licenciado (NordVPN) y dejando al software libre (ProtonVPN) en base al sistema operativo Windows 10 con el índice más alto al momento de medir el jitter en la transferencia de datos. En síntesis, la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al rendimiento del software. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.

**Variable Administración de recursos**

Se analizó atendiendo tres indicadores, uso del CPU, uso de la Memoria RAM y uso del Disco Duro al momento de ejecutar los softwares de redes privadas virtuales ante ataques de denegación de servicio distribuido en los sujetos de pruebas, de lo cual los resultados extraídos de las evaluaciones se llevó a cabo el uso de las pruebas de normalidad y dependiendo el resultado se empleaba pruebas paramétricas y no paramétricas para muestras relacionadas, respectivamente. Se determinan las hipótesis con la finalidad de aceptar o rechazar en cada caso con respecto a la media y significancia de los resultados.

**IV. Hipótesis Específica HE2**

**$HE2_0$**: La aplicación de los procesos de la metodología MEPVPNS no permitió la evaluación de los softwares de redes privadas virtuales en cuanto a la administración de recursos

**$HE2_1$:** La aplicación de los procesos de la metodología MEPVPNS v evaluar los softwares de redes privadas virtuales en cuanto a la administración de recursos
A continuación, se especifica los resultados extraídos conforme a las evaluaciones realizadas a través del proceso de la evaluación de la administración de recursos

**Prueba de normalidad para el indicador porcentaje de uso del CPU**

Para el proceso del indicador throughput para evaluar la prueba de normalidad se utilizó Shapiro-Wilk dado que la cantidad de la muestra es < 50.

Tabla 21 Resultados de prueba de normalidad del indicador uso del CPU

| | Pruebas de normalidad | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| **W_usoCPU_ProtonVPN** | ,176 | 20 | ,105 | ,913 | 20 | ,072 |
| **W_usoCPU_TunnelBear** | ,168 | 20 | ,143 | ,907 | 20 | ,057 |
| **W_usoCPU_NordVPN** | ,248 | 20 | ,002 | ,864 | 20 | ,009 |
| **W_usoCPU_sinVPN** | ,180 | 20 | ,089 | ,956 | 20 | ,469 |
| **U_usoCPU_ProtonVPN** | ,332 | 20 | ,000 | ,703 | 20 | ,000 |
| **U_usoCPU_TunnelBear** | ,335 | 20 | ,000 | ,641 | 20 | ,000 |
| **U_usoCPU_NordVPN** | ,381 | 20 | ,000 | ,704 | 20 | ,000 |
| **U_usoCPU_sinVPN** | ,094 | 20 | ,200* | ,980 | 20 | ,936 |

Por ello, los datos de significancia que sean menores α=0,05 se toman como pruebas no paramétricas, es decir, no siguen una distribución normal. No obstante, se han registrado datos mayores y menores α=0,05 evitando aceptar o rechazar la Ho (distribución normal).

En síntesis, se utilizaron pruebas paramétricas y no paramétricas para las comparaciones en cuanto al indicador uso del CPU ante DDoS.

Tabla 22 Resultados de prueba de wilcoxon del indicador uso del CPU en el sistema operativo Windows 10

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| **W_usoCPU_ProtonVPN - W_usoCPU_TunnelBear** | Rangos negativos | 3[a] | 11,83 | 35,50 |
| | Rangos positivos | 17[b] | 10,26 | 174,50 |
| | Empates | 0[c] | | |
| | Total | 20 | | |
| **W_usoCPU_NordVP N - W_usoCPU_TunnelBear** | Rangos negativos | 5[d] | 8,20 | 41,00 |
| | Rangos positivos | 13[e] | 10,00 | 130,00 |
| | Empates | 2[f] | | |
| | Total | 20 | | |
| **W_usoCPU_sinVPN -W_usoCPU_TunnelBear** | Rangos negativos | 10[g] | 9,65 | 96,50 |
| | Rangos positivos | 9[h] | 10,39 | 93,50 |
| | Empates | 1[i] | | |
| | Total | 20 | | |

Tabla 23 Resultados de prueba estadística de Wilcoxon del indicador uso del CPU en el sistema operativo Windows 10

| Estadísticos de prueba[a] | | | |
|---|---|---|---|
| | W_usoCPU_ProtonVPN - W_usoCPU_TunnelBear | W_usoCPU_NordVPN - W_usoCPU_TunnelBear | W_usoCPU_sinVPN - W_usoCPU_Tunnel-Bear |
| Z | -2,595[b] | -1,939[b] | -,061[c] |
| Sig. Asintótica (bilateral) | ,009 | ,053 | ,952 |

En las tablas anteriores, se puede evidenciar que el software licenciado (NordVPN) mantiene un menor consumo de CPU frente al software gratuito (TunnelBear) y libre (ProtonVPN) en el sistema operativo Windows 10 (Tabla 22). De acuerdo a la Tabla 23, se observa los niveles de significancia asintótica equivalentes a 0,09 comparando TunnelBear con ProtonVPN y por ultimo, comparando TunnelBear con NordVPN con una significancia asintótica de 0,053.

Tabla 24 Resultados de prueba de Wilcoxon del indicador uso del CPU en el sistema operativo Linux – distribución Ubuntu 16.4

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de Rangos |
| **U_usoCPU_TunnelBear - U_usoCPU_ProtonVPN** | Rangos negativos | 3[a] | 5,33 | 16,00 |
| | Rangos positivos | 14[b] | 9,79 | 137,00 |
| | Empates | 3[c] | | |
| | Total | 20 | | |
| **U_usoCPU_NordVPN - U_usoCPU_ProtonVPN** | Rangos negativos | 1[d] | 1,50 | 1,50 |
| | Rangos positivos | 19[e] | 10,97 | 208,50 |
| | Empates | 0[f] | | |
| | Total | 20 | | |
| **U_usoCPU_sinVPN - U_usoCPU_ProtonVPN** | Rangos negativos | 2[g] | 11,25 | 22,50 |
| | Rangos positivos | 10[h] | 5,55 | 55,50 |
| | Empates | 8[i] | | |
| | Total | 20 | | |

Tabla 25 Resultados de prueba estadística de Wilcoxon del indicador uso del CPU en el sistema operativo Linux – distribución Ubuntu 16.4

| Estadísticos de prueba[a] | | | |
|---|---|---|---|
| | U_usoCPU_Tunnel-Bear - U_usoCPU_Proton-VPN | U_usoCPU_NordVPN -U_usoCPU_Pro-tonVPN | U_usoCPU_sinVPN - U_usoCPU_Pro-tonVPN |
| Z | 2,870[b] | -3,948[b] | -1,359[b] |
| Sig. Asintótica (bilateral) | ,004 | ,000 | ,174 |

En las tablas anteriores, se puede evidenciar que el software gratuito (TunnelBear) mantiene un menor índice de uso de CPU ante DDoS frente al software libre (ProtonVPN) y licenciado (NordVPN) respectivamente en el sistema operativo Linux - distribución Ubuntu 16.4. De acuerdo a la Tabla 25, se observa los niveles de significancia asintótica equivalentes a 0,004 comparando ProtonVPN con TunnelBear y comparando ProtonVPN con NordVPN con una significancia asintótica de 0,000079.

Tabla 26 Resultados de prueba de rangos con signos de Wilcoxon del indicador uso del CPU – Comparación entre S.O

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| U_usoCPU_NordVPN - W_usoCPU_TunnelBearVPN | Rangos negativos | 20[a] | 10,50 | 210,00 |
| | Rangos positivos | 0[b] | ,00 | ,00 |
| | Empates | 0[c] | | |
| | Total | 20 | | |

Tabla 27 Resultados de estadísticos de prueba de wilcoxon del indicador uso del CPU – Comparación entre S.O

| Estadísticos de prueba[a] | |
|---|---|
| | U_usoCPU_NordVPN - W_usoCPU_TunnelBearVPN |
| Z | -3,920[b] |
| Sig. Asintótica (bilateral) | ,000 |

En las tablas anteriores, comparando las tecnologías de software VPN más resaltantes entre los sistemas operativos se pudo evidenciar que el software licenciado (NordVPN) del sistema operativo Windows 10 mantuvo un índice

menor de uso de CPU ante los ataques de denegación de servicio distribuido. Además, se observa los niveles de significancia asintótica equivalentes a 83 0,000089 al comparar NordVPN de Windows 10 con TunnelBear del sistema operativo Linux – Distribución Ubuntu 16.4.

En referencia a las tablas anteriores, se puede evidenciar que el software licenciado (NordVPN) mantuvo un índice menor de uso de CPU ante los ataques de denegación de servicio distribuido frente al software gratuito (TunnelBear) y el software libre (ProtonVPN). Asimismo, el software gratuito (TunnelBear) está posicionado en el cuarto lugar en cuanto al menor uso de CPU ante los ataques de denegación de servicio distribuido. Además, Además, quien le sigue en el rango de la prueba de evaluación es el software libre (ProtonVPN) y dejando al software licenciado (NordVPN) con el índice más alto en cuanto al menor uso de CPU ante los ataques de denegación de servicio distribuido en base al sistema operativo Linux - distribución Ubuntu 16.4. En síntesis, *la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al rendimiento del software. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba de normalidad para el indicador porcentaje de uso de Memoria RAM**

Para el proceso del indicador throughput para evaluar la prueba de normalidad se utilizó Shapiro-Wilk dado que la cantidad de la muestra es < 50.

Tabla 28 Resultados de prueba de normalidad del indicador uso de Memoria RAM

| | Pruebas de normalidad | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| **W_usoMemoriaRAM_ProtonVPN** | ,125 | 20 | ,200* | ,971 | 20 | ,782 |
| **W_usoMemoriaRAM_TunnelBear** | ,109 | 20 | ,200* | ,952 | 20 | ,395 |
| **W_usoMemoriaRAM_NordVPN** | ,133 | 20 | ,200* | ,963 | 20 | ,608 |
| **W_usoMemoriaRAM_NordVPN** | ,226 | 20 | ,009 | ,816 | 20 | ,002 |
| **U_usoMemoriaRAM_ProtonVPN** | ,300 | 20 | ,000 | ,753 | 20 | ,000 |
| **U_usoMemoriaRAM_TunnelBear** | ,538 | 20 | ,000 | ,236 | 20 | ,000 |
| **U_usoMemoriaRAM_NordVPN** | ,320 | 20 | ,000 | ,572 | 20 | ,000 |
| **U_usoMemoriaRAM_sinVPN** | ,319 | 20 | ,000 | ,538 | 20 | ,000 |

Por ello, los datos de significancia que sean < α=0,05 se toman como pruebas no paramétricas, es decir, no siguen una distribución normal. No obstante, se han registrado datos > α=0,05 que evitan rechazar la Ho (distribución normal). En síntesis, se utilizaron pruebas paramétricas y no paramétricas para las comparaciones en cuanto al indicador uso de Memoria RAM ante DDoS.

*Tabla 29 Resultados de la prueba t de student para muestras relacionadas del indicador uso de memoria RAM en base al sistema operativo Windows 10*

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | **Media** | **N** | **Desv. Desviación** | **Desv. Error promedio** |
| Par 1 | **W_usoMemoria-RAM_ProtonVPN** | 66,10 | 20 | 9,989 | 2,234 |
| | **W_usoMemoria-RAM_TunnelBear** | 67,95 | 20 | 5,907 | 1,321 |
| Par 2 | **W_usoMemoria-RAM_ProtonVPN** | 66,10 | 20 | 9,989 | 2,234 |
| | **W_usoMemoria-RAM_NordVPN** | 67,45 | 20 | 7,416 | 1,658 |
| Par 3 | **W_usoMemoria-RAM_ProtonVPN** | 66,10 | 20 | 9,989 | 2,234 |
| | **W_usoMemoria-RAM_sinVPN** | 41,95 | 20 | ,759 | ,170 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bilateral) |
| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | **W_usoMemoriaRAM_ProtonVPN - W_usoMemoriaRAM_TunnelBear** | -1,850 | 12,733 | 2,847 | -7,809 | 4,109 | -,650 | 19 | ,524 |
| Par 2 | **W_usoMemoriaRAM_ProtonVPN- W_usoMemoriaRAM_NordVPN** | -1,350 | 11,713 | 2,619 | -6,832 | 4,132 | -,515 | 19 | ,612 |
| Par 3 | **W_usoMemoriaRAM_ProtonVPN - W_usoMemoriaRAM_sinVPN** | 24,150 | 10,132 | 2,266 | 19,408 | 28,892 | 10,659 | 19 | ,000 |

En referencia a las tablas anteriores (29), se observó que el software libre (ProtonVPN) registra una media baja de 66,10 posicionándolo como el software con un índice menor en el uso de la Memoria RAM registrado en las evaluaciones, dejando en segundo lugar al software licenciado (Nordvpn) con un registro de media 67,45 y por último al software gratuito (TunnelBear) con una media menor a 67,95 enel sistema operativo Windows 10.

Tabla 30 Resultados de prueba de wilcoxon del indicador uso de la Memoria RAM en el sistema operativo Linux – distribución 16.4

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de Rangos |
| **U_usoMemoriaRAM_ TunnelBear - U_uso-MemoriaRAM_ Pro-tonVPN** | Rangos negativos | 0[a] | ,00 | ,00 |
| | Rangos positivos | 20[b] | 10,50 | 210,00 |
| | Empates | 0[c] | | |
| | Total | 20 | | |
| **U_usoMemoriaRAM_ NordVPN - U_usoMe-moriaRAM_ Proton-VPN** | Rangos negativos | 0[d] | ,00 | ,00 |
| | Rangos positivos | 20[e] | 10,50 | 210,00 |
| | Empates | 0[f] | | |
| | Total | 20 | | |
| **U_usoMemoria-RAM_sinVPN - U_usoMemoriaRAM_ ProtonVPN** | Rangos negativos | 20[g] | 10,50 | 210,00 |
| | Rangos positivos | 0[h] | ,00 | ,00 |
| | Empates | 0[i] | | |
| | Total | 20 | | |

Tabla 31 Resultados de prueba estadística de Wilcoxon del indicador uso de la memoria RAM en el sistema operativo Linux – distribución 16.4.

| Estadísticos de prueba[a] | | | |
|---|---|---|---|
| | **U_usoMemoriaRAM_ TunnelBear - U_usoMemoriaRAM_ ProtonVPN** | **U_usoMemoriaRAM_ NordVPN - U_usoMemoriaRAM_ ProtonVPN** | **U_usoMemoriaRAM_ sinVPN - U_usoMemoriaRAM_ ProtonVPN** |
| Z | -3,972[b] | -3,955[b] | -3,940[c] |
| Sig. Asintótica (bilateral) | ,000 | ,000 | ,000 |

Tal y como se observa en las tablas anteriores, se evidencia que el software libre (ProtonVPN) muestra una media baja de uso de Memoria RAM ante DDoS frente al software licenciado (NordVPN) y software gratuito (TunnelBear) en el sistema operativo Linux – distribución Ubuntu 16.4. De acuerdo a la Tabla 28, se observa los niveles de significancia asintótica equivalentes a 0,000071 comparando ProtonVPN con TunnelBear, asimismo, ProtonVPN con NordVPN con una significancia asintótica de 0,000076.

Tabla 32 Resultados de prueba de rangos con signos de Wilcoxon del indicador uso de la memoria RAM – Comparación entre S.O.

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de Rangos |
| **W_usoMemoria-RAM_ProtonVPN - U_usoMemoriaRAM _ProtonVPN** | Rangos negativos | 10[a] | 12,60 | 126,00 |
| | Rangos positivos | 9[b] | 7,11 | 64,00 |
| | Empates | 1[c] | | |
| | Total | 20 | | |

Tabla 33 Resultados de estadísticos de prueba de wilcoxon del indicador uso de la memoria RAM – Comparación entre S.O.

| Estadísticos de prueba[a] | |
|---|---|
| | U_usoMemoriaRAM_ProtonVPN - W_usoMemoriaRAM_ProtonVPN |
| Z | -1,248[b] |
| Sig. Asintótica (bilateral) | ,212 |

De acuerdo a la **Tabla 32**, comparando las tecnologías de software VPN más resaltantes entre los sistemas operativos se pudo evidenciar que el software libre (ProtonVPN) muestra un índice bajo en el uso de la Memoria RAM ante DDoS en el sistema operativo Windows 10 en comparación con el software libre (ProtonVPN) del sistema operativo Linux – Distribución Ubuntu 16.4. Además, a la **Tabla 33**, se observa los niveles de significancia asintótica equivalentes a 0,212 al comparar el software libre (ProtonVPN) de Windows 10 con el software libre (ProtonVPN) de Linux – Distribución Ubuntu 16.4.

En referencia a las tablas anteriores, se puede evidenciar que el software libre (ProntonVPN) mantiene un índice bajo en el uso de la Memoria RAM ante DDoS frente al software licenciado (NordVPN) del sistema operativo Windows 10. Asimismo, el software libre (ProtonVPN) está posicionado en el tercer lugar, sin embargo, el software gratuito (TunnelBear) se encuentra en un escalón inferior en base al sistema operativo Linux - distribución Ubuntu 16.4 y dejando al software licenciado (NordVPN) del sistema operativo Linux - distribución Ubuntu 16.4 y software gratuito (TunnelBear) del sistema operativo Windows 10 con el índice más alto en cuanto al indicador Uso de la Memoria RAM ante DDoS. En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto a la **administración de recursos**. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.

**Prueba de normalidad para el indicador porcentaje de uso del Disco Duro**

Para el proceso del indicador throughput para evaluar la prueba de normalidad se utilizó Shapiro-Wilk dado que la cantidad de la muestra es < 50.

Tabla 34 Resultados de prueba de normalidad del indicador uso del Disco Duro

| | Pruebas de normalidad | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| **W_usoDiscoDuro_ProtonVPN** | ,287 | 20 | ,000 | ,703 | 20 | ,000 |
| **W_usoDiscoDuro_TunnelBear** | ,411 | 20 | ,000 | ,451 | 20 | ,000 |
| **W_usoDiscoDuro_NordVPN** | ,311 | 20 | ,000 | ,780 | 20 | ,000 |
| **W_usoDiscoDuro_sinVPN** | ,292 | 20 | ,000 | ,606 | 20 | ,000 |
| **U_usoDiscoDuro_ProtonVPN** | ,351 | 20 | ,000 | ,652 | 20 | ,000 |
| **U_usoDiscoDuro_TunnelBear** | ,348 | 20 | ,000 | ,734 | 20 | ,000 |
| **U_usoDiscoDuro_NordVPN** | ,538 | 20 | ,000 | ,236 | 20 | ,000 |
| **U_usoDiscoDuro_sinVPN** | ,527 | 20 | ,000 | ,351 | 20 | ,000 |

En la Tabla 31 se han registrados datos < α=0,05, por ello, se infiere que no siguen una distribución normal y utilizaran pruebas no paramétricas para el indicador del uso del Disco Duro ante DDoS.

Tabla 35 Resultados de prueba de Wilcoxon del indicador uso del Disco Duro en el sistema Windows 10

| Rangos | | | | |
|---|---|---|---|---|
| | | **N** | **Rango promedio** | **Suma derangos** |
| **W_usoDiscoDuro_ ProtonVPN - W_usoDiscoDuro_ TunnelBear** | Rangos negativos | 3[a] | 11,83 | 35,50 |
| | Rangos positivos | 17[b] | 10,26 | 174,50 |
| | Empates | 0[c] | | |
| | Total | 20 | | |
| **W_usoDiscoDuro_ NordVPN - W_uso-DiscoDuro_Tun-nelBear** | Rangos negativos | 5[d] | 8,20 | 41,00 |
| | Rangos positivos | 13[e] | 10,00 | 130,00 |
| | Empates | 2[f] | | |
| | Total | 20 | | |
| **W_usoDiscoDuro_ sinVPN - W_uso-DiscoDuro_ TunnelBear** | Rangos negativos | 10[g] | 9,65 | 96,50 |
| | Rangos positivos | 9[h] | 10,39 | 93,50 |
| | Empates | 1[i] | | |
| | Total | 20 | | |

Tabla 36 Resultados de prueba estadística de Wilcoxon del indicador uso del Disco Duro en el sistema operativo Windows 10.

| Estadísticos de prueba[a] | | | |
|---|---|---|---|
| | W_usoDisco-Duro_ProtonVPN - W_usoDisco-Duro_TunnelBear | W_usoDisco-Duro_NordVPN - W_usoDisco-Duro_TunnelBear | W_usoDisco-Duro_sinVPN - W_usoDisco-Duro_TunnelBear |
| Z | -2,595[b] | -1,939[b] | -,061[c] |
| Sig. Asintótica (bilate-ral) | ,009 | ,053 | ,952 |

Tal y como se observa en las tablas anteriores, se evidencia que el software gratuito (TunnelBear) muestra una media baja de uso del Disco Duro ante DDoS frente al software licenciado (NordVPN) y software libre (ProtonVPN) en el sistema operativo Linux – distribución Ubuntu 16.4. De acuerdo a la Tabla 34, se observa los niveles de significancia asintótica equivalentes a 0,009 comparando TunnelBear con ProtonVPN, asimismo, TunnelBear con NordVPN con una significancia asintótica de 0,053.

Tabla 37 Resultados de prueba de wilcoxon del indicador uso del Disco Duro en el sistema Linux –distribución Ubuntu 16.4.

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| U_usoDiscoDuro_Tun-nelBear - U_usoDisco-Duro_ProtonVPN | Rangos negativos | 3[a] | 5,33 | 16,00 |
| | Rangos positivos | 14[b] | 9,79 | 137,00 |
| | Empates | 3[c] | | |
| | Total | 20 | | |
| U_usoDisco-Duro_NordVPN -U_uso-DiscoDuro_ProtonVPN | Rangos negativos | 1[d] | 1,50 | 1,50 |
| | Rangos positivos | 19[e] | 10,97 | 208,50 |
| | Empates | 0[f] | | |
| | Total | 20 | | |
| U_usoDisco-Duro_sinVPN -U_usoDis-coDuro_ProtonVPN | Rangos negativos | 2[g] | 11,25 | 22,50 |
| | Rangos positivos | 10[h] | 5,55 | 55,50 |
| | Empates | 8[i] | | |
| | Total | 20 | | |

Tabla 38 Resultados de prueba estadística de Wilcoxon del indicador uso del Disco Duro en el sistema Linux –distribución Ubuntu 16.4

| Estadísticos de prueba[a] | | | |
|---|---|---|---|
| | U_usoDiscoDuro_TunnelBear - U_usoDiscoDuro_ProtonVPN | U_usoDiscoDuro_NordVPN - U_usoDiscoDuro_ProtonVPN | U_usoDiscoDuro_sinVPN - U_usoDiscoDuro_Proton-VPN |
| Z | -2,870[b] | -3,948[b] | -1,359[b] |
| Sig. Sintótica (bilateral) | ,004 | , 000079 | ,174 |

Tal y como se observa en las tablas anteriores, se evidencia que el software libre (ProtonVPN) muestra una media baja de uso del Disco Duro ante DDoS frente al software gratuito (TunnelBear) y software licenciado (NordVPN) respectivamente en el sistema operativo Linux – distribución Ubuntu 16.4. Además, se observa los niveles de significancia asintótica equivalentes a 0,004 comparando ProtonVPN con TunnelBear, asimismo, ProtonVPN con NordVPN con una significancia asintótica de 0,000079.

Tabla 39 Resultados de prueba de rangos con signos de Wilcoxon del indicador uso del Disco Duro – Comparación entre S.O.

| Rangos | | | | |
|---|---|---|---|---|
| | | N | Rango promedio | Suma de rangos |
| U_usoDiscoDuro_Proton-VPN - W_usoDisco-Duro_TunnelBear | Rangos negativos | 17[a] | 9,62 | 163,50 |
| | Rangos positivos | 1[b] | 7,50 | 7,50 |
| | Empates | 2[c] | | |
| | Total | 20 | | |

Tabla 40 Resultados de estadísticos de prueba de wilcoxon del indicador uso del Disco Duro – Comparación entre S.O.

| Estadísticos de prueba[a] | |
|---|---|
| | U_usoDiscoDuro_ProtonVPN - W_usoDiscoDuro_TunnelBear |
| Z | -3,411[b] |
| Sig. Asintótica (bilateral) | ,001 |

De acuerdo a la **Tabla 39**, comparando las tecnologías de software VPN más resaltantes entre los sistemas operativos se pudo evidenciar que el software libre (ProtonVPN) muestra un índice bajo en el uso del Disco Duro ante DDoS en el sistema operativo Linux – Distribución Ubuntu 16.4 en comparación con el software gratuito (TunnelBear) del sistema operativo Windows 10. Asimismo, en la **Tabla 40**, se observa los niveles de significancia asintótica equivalentes a 0,001 al comparar el software gratuito (TunnelBear) con el software libre (ProtonVPN) de Linux – Distribución Ubuntu 16.4.

En referencia a las tablas anteriores, se puede evidenciar que el software libre (ProntonVPN) mantiene un índice bajo en el uso del Disco Duro ante DDoS frente al software gratuito (TunnelBear) del sistema operativo Linux - distribución Ubuntu 16.4. Asimismo, el software gratuito (TunnelBear) del sistema operativo Windows 10 está posicionado en el tercer lugar, sin embargo, el software licenciado (NordVPN) se encuentra en un escalón inferior en base al sistema operativo Linux - distribución Ubuntu 16.4 y dejando al software licenciado (NordVPN) y software libre (ProtonVPN) del sistema operativo Windows 10 con el índice más alto en cuanto al indicador uso del Disco Duro ante DDoS. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto a la* ***administración de recursos****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Variable Desempeño en la red**

Se analizó atendiendo dos indicadores, Latencia, Velocidad de descarga y subida y ancho de banda de descarga de archivos al utilizar los softwares de redes privadas virtuales en los sujetos de pruebas, de lo cual los resultados extraídos de las evaluaciones. Se determinan las hipótesis con la finalidad de aceptar o rechazar en cada caso con respecto al promedio de los resultados.

**IV. Hipótesis Específica HE3**

**$HE3_0$**: La aplicación de los procesos de la metodología MEPVPNS no permitió evaluar los softwares de redes privadas virtuales en cuanto al desempeño en la red.

**$HE3_1$:** La aplicación de los procesos de la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al desempeño en la red.

A continuación, se especifica los resultados extraídos conforme a las evaluaciones realizadas a través del proceso de la evaluación del rendimiento del software.

**Prueba descriptiva para el indicador latencia de la variable Rendimiento del Software.**

Tabla 41 Resultados del indicador Latencia

| | Latencia | | | | | |
|---|---|---|---|---|---|---|
| | N° | Software VPN | Test de velocidad | Latencia (ms) | Promedio latencia (ms) | |
| SISTEMA OPERATIVO: WINDOWS 10 | 1 | Sin VPN | Speedtest Minedu | 10 | 48 | |
| | | | Speedtest Media Commerce Perú | 123 | | |
| | | | Speedtest Ookla | 11 | | |
| | 2 | Softwareli-bre | Speedtest Minedu | 154 | 158 | |
| | | | Speedtest Media Commerce Perú | 162 | | |
| | | | Speedtest Ookla | 160 | | |
| | 3 | Software gratuito | Speedtest Minedu | 205 | 205 | |
| | | | Speedtest Media Commerce Perú | 217 | | |
| | | | Speedtest Ookla | 193 | | |
| | 4 | Software li-cenciado | Speedtest Minedu | 171 | 157 | |
| | | | Speedtest Media Commerce Perú | 138 | | |
| | | | Speedtest Ookla | 162 | | |
| SISTEMA OPERA-TIVO: LINUX(DIS-TRIBUCION UBUNTU) | 1 | Sin VPN | Speedtest Minedu | 10 | 47 | |
| | | | Speedtest Media Commerce Perú | 124 | | |
| | | | Speedtest Ookla | 8 | | |
| | 2 | Softwareli-bre | Speedtest Minedu | 255 | 326 | |
| | | | Speedtest Media Commerce Perú | 327 | | |
| | | | Speedtest Ookla | 396 | | |
| | 3 | Software gratuito | Speedtest Minedu | 174 | 199 | |
| | | | Speedtest Media Commerce Perú | 249 | | |
| | | | Speedtest Ookla | 174 | | |
| | 4 | Software li-cenciado | Speedtest Minedu | 75 | 117 | |
| | | | Speedtest Media Commerce Perú | 138 | | |
| | | | Speedtest Ookla | 138 | | |

Respecto al indicador Latencia, en la **tabla 41** se utilizó tres tipos de test de velocidad (Speedtest Ookla, Speedtest Minedu, Speedtest Media Commerce Perú) para obtener los promedios de latencia en la conexión al servidor de internet. En consecuencia, se puede observar que el promedio de latencia de menor valor está en el software licenciado NordVPN con un registro de 157 ms (milisegundos) en comparación con el software libre (ProtonVPN) con un registro de 158 ms dejando en tercer lugar al software gratuito (TunnelBear) con un registro de 205 ms en el sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 respecto al indicador Latencia, se

puede observar que el promedio de latencia de menor valor se encuentra en el software licenciado NordVPN con un registro de 117 ms (milisegundos) en comparación con el software gratuita (TunnelBear) con un registro de 199 ms dejando en tercer lugar al software libre (ProtonVPN) con un registro de 326 ms.

En referencia a la tabla anterior, se puede evidenciar que el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 mantiene un promedio bajo de latencia en la conexión al servidor de internet frente al software licenciado (NordVPN) del sistema operativo Windows 10. Asimismo, el software libre (ProtonVPN) está posicionado en el tercer lugar, sin embargo, el software gratuito (TunnelBear) se encuentra en un escalón inferior en base al sistema operativo Linux - distribución Ubuntu 16.4, dejando al software gratuito (TunnelBear) del sistema operativo Windows 10 y software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 con el índice más alto en cuanto al indicador latencia en la conexión al servidor de internet. En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al desempeño en la red. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.

**Prueba descriptiva para el indicador velocidad de descargas/subidas de archivos de la variable Rendimiento del Software.**

Tabla 42 Resultados del indicador velocidad de descarga

| | Velocidad de descargas | | | | | |
|---|---|---|---|---|---|---|
| | **N°** | **Software VPN** | **Test de velocidad** | **Velocidad de descarga (Mbps)** | **Promedio velocidad de descarga (Mbps)** | |
| **SISTEMA OPERATIVO:WINDOWS 10** | **1** | **Sin VPN** | Speedtest Minedu | 39,9 | 38,88 |  |
| | | | Speedtest Media Commerce Perú | 39,5 | | |
| | | | Speedtest Ookla | 37,24 | | |
| | **2** | **Software libre** | Speedtest Minedu | 12,01 | 12,06 |  |
| | | | Speedtest Media Commerce Perú | 11,1 | | |
| | | | Speedtest Ookla | 13,08 | | |
| | **3** | **Software gratuito** | Speedtest Minedu | 12,2 | 17,47 |  |
| | | | Speedtest Media Commerce Perú | 16,2 | | |
| | | | Speedtest Ookla | 24,02 | | |
| | **4** | **Software licenciado** | Speedtest Minedu | 16,24 | 16,86 |  |
| | | | Speedtest Media Commerce Perú | 17,14 | | |
| | | | Speedtest Ookla | 17,2 | | |

| | Velocidad de descargas | | | | | |
|---|---|---|---|---|---|---|
| | N° | Software VPN | Test de velocidad | Velocidad de descarga (Mbps) | Promedio velocidad de descarga (Mbps) | |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU) | 1 | Sin VPN | Speedtest Minedu | 39,1 | 40,38 | |
| | | | Speedtest Media Commerce Perú | 39,5 | | |
| | | | Speedtest Ookla | 42,55 | | |
| | 2 | Software libre | Speedtest Minedu | 1,7 | 1,82 | |
| | | | Speedtest Media Commerce Perú | 1,9 | | |
| | | | Speedtest Ookla | 1,85 | | |
| | 3 | Software gratuito | Speedtest Minedu | 32,8 | 34,40 | |
| | | | Speedtest Media Commerce Perú | 38 | | |
| | | | Speedtest Ookla | 32,41 | | |
| | 4 | Software licenciado | Speedtest Minedu | 38 | 38,85 | |
| | | | Speedtest Media Commerce Perú | 38 | | |
| | | | Speedtest Ookla | 40,56 | | |

Respecto al indicador velocidad de descarga/subida, en la **tabla 42** se utilizó tres Speedtest (Speedtest Minedu, Speedtest Media Commerce Perú y Speedtest Ookla) para obtener los promedios de velocidad de descarga en la conexión al servidor de internet. En consecuencia, se puede observar que el promedio de velocidad de descarga de mayor valor se encuentra en el software gratuito (TunnelBear) con un registro de 17,47 Mbps (Megabit/sec) de descarga en comparación con el software licenciado (NordVPN) con un registro de 16,86 Mbps de descarga, dejando en tercer lugar al software libre (ProtonVPN) con un registro de 12,06 Mbps de descarga en el sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 respecto al indicador velocidad de descarga, se puede observar que el promedio de velocidad de descarga de mayor valor se encuentra en el software licenciado (NordVPN) con un registro de 38,85 Mbps (Megabit/sec) de descarga en comparación con el software gratuito (TunnelBear) con un registro de 34,40 Mbps de descarga, dejando en tercer lugar al software libre (ProtonVPN) con un registro de 1,82 Mbps de descarga.

En referencia a la tabla anterior, se puede evidenciar que el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 mantiene un promedio mayor de velocidad de descargar frente al software gratuito (TunnelBear) en base al sistema operativo Linux - distribución Ubuntu 16.4. Asimismo, el software gratuito (TunnelBear) del sistema operativo Windows 10 está posicionado en el tercer lugar, sin embargo, el software licenciado

(NordVPN) se encuentra en un escalón inferior en base al sistema operativo Windows 10, dejando al software libre (ProntonVPN) del sistema operativo Windows 10 y software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 con el promedio más bajo en cuanto al indicador de velocidad de descarga. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

Tabla 43 Resultados del indicador velocidad de subida

| | Velocidad de subida | | | | | |
|---|---|---|---|---|---|---|
| | **N°** | **Software VPN** | **Test de velocidad** | **Velocidad de subida (Mbps)** | **Promedio velocidad de subida (Mbps)** | |
| **SISTEMA OPERATIVO: WINDOWS 10** | **1** | **Sin VPN** | Speedtest Minedu | 16,3 | 11,72 |  |
| | | | Speedtest Media Commerce Perú | 3 | | |
| | | | Speedtest Ookla | 15,86 | | |
| | **2** | **Softwareli-bre** | Speedtest Minedu | 7,06 | 7,03 |  |
| | | | Speedtest Media Commerce Perú | 6,45 | | |
| | | | Speedtest Ookla | 7,57 | | |
| | **3** | **Software gratuito** | Speedtest Minedu | 1 | 1,47 |  |
| | | | Speedtest Media Commerce Perú | 2 | | |
| | | | Speedtest Ookla | 1,41 | | |
| | **4** | **Software licenciado** | Speedtest Minedu | 4,03 | 4,37 |  |
| | | | Speedtest Media Commerce Perú | 5,07 | | |
| | | | Speedtest Ookla | 4,01 | | |
| **SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU)** | **1** | **Sin VPN** | Speedtest Minedu | 16,5 | 16,43 |  |
| | | | Speedtest Media Commerce Perú | 16,4 | | |
| | | | Speedtest Ookla | 16,4 | | |
| | **2** | **Softwareli-bre** | Speedtest Minedu | 2,1 | 1,26 |  |
| | | | Speedtest Media Commerce Perú | 0,6 | | |
| | | | Speedtest Ookla | 1,07 | | |
| | **3** | **Software gratuito** | Speedtest Minedu | 2 | 2,04 |  |
| | | | Speedtest Media Commerce Perú | 2,9 | | |
| | | | Speedtest Ookla | 1,22 | | |
| | **4** | **Software licenciado** | Speedtest Minedu | 15,7 | 15,70 |  |
| | | | Speedtest Media Commerce Perú | 15,7 | | |
| | | | Speedtest Ookla | 15,69 | | |

Respecto al indicador velocidad de subida, en la **tabla 43** se utilizó tres Speedtest (Speedtest Minedu, Speedtest Media Commerce Perú y Speedtest

Ookla) para obtener los promedios de velocidad de subida en la conexión al servidor de internet. En consecuencia, se puede observar que el promedio de velocidad de subida de mayor valor se encuentra en el software libre (ProtonVPN) con un registro de 7,03 Mbps (Megabit/sec) de subida en comparación con el software licenciado (NordVPN) con un registro de 4,37 Mbps de subida, dejando en tercer lugar al software gratuito (TunnelBear) con un registro de 1,47 Mbps de subida en el sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 respecto al indicador velocidad de subida, se puede observar que el mayor promedio se encuentra en el software licenciado (NordVPN) con un registro de 15,70 Mbps (Megabit/sec) de subida en comparación con el software gratuito (TunnelBear) con un registro de 2,04 Mbps de subida, dejando en tercer lugar al software libre (ProtonVPN) con un registro de 1,26 Mbps de subida.

En referencia a la tabla anterior, se puede evidenciar que el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 mantiene un promedio mayor de velocidad de subida frente al software libre (ProtonVPN) del sistema operativo Windows 10. Asimismo, el software licenciado (NordVPN) del sistema operativo Windows 10 está posicionado en el tercer lugar, sin embargo, el software gratuito (TunnelBear) en base al sistema operativo Linux - distribución Ubuntu 16.4 se encuentra en un escalón inferior, dejando al software gratuito (TunnelBear) del sistema operativo Windows 10 y software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 con el promedio más bajo en cuanto al indicador de velocidad de subida. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador ancho de banda de la variable Rendimiento del Software.**

Tabla 44 Resultados del indicador ancho de banda en base descargas de archivos

| | Ancho de banda | | | | | |
|---|---|---|---|---|---|---|
| | N° | Software VPN | Test de velocidad | Promedio velocidad de descarga (Mbps) | Ancho de banda de descarga de archivos (KB/s) | |
| SISTEMA OPERATIVO: WINDOWS 10 | 1 | Sin VPN | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 38,88 | 4976 |  |
| | 2 | Software libre | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 12,06 | 1544 |  |
| | 3 | Software gratuito | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 17,47 | 2236 |  |
| | 4 | Software licenciado | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 16,86 | 2158 |  |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU) | 1 | Sin VPN | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 40,38 | 5169 |  |
| | 2 | Software libre | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 1,82 | 232 |  |
| | 3 | Software gratuito | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 34,40 | 4403 |  |
| | 4 | Software licenciado | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 38,85 | 4973 |  |

Respecto al indicador ancho de banda de descarga de archivos, en la **tabla 44** se utilizó tres Speedtest (Speedtest Minedu, Speedtest Media Commerce Perú y Speedtest Ookla) para obtener los promedios de ancho de banda de descargas de archivos en la conexión al servidor de internet. En consecuencia, se puede observar que el promedio de ancho de banda de descarga de archivos de mayor valor se encuentra en el software gratuito (TunnelBear) con un registro de 2236 KB/s (Kilobyte/sec) en comparación con el software licenciado (NordVPN) con un registro de 2158 KB/s de ancho de banda de descarga, dejando en tercer lugar al software libre (ProtonVPN) con un registro de 1544 KB/s de ancho de banda de descarga en el sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 respecto al indicador ancho de banda de descarga de archivos, se puede observar que el promedio de ancho de banda

de descarga de mayor valor se encuentra en el software licenciado (NordVPN) con un registro de 4973 KB/s (Kilobyte/sec) en comparación con el software gratuito (TunnelBear) con un registro de 4403 KB/s, dejando en tercer lugar al software libre (ProtonVPN) con un registro de 232 KB/s de ancho de banda de descarga.

En referencia a la tabla anterior, se puede evidenciar que el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 mantiene un promedio mayor de velocidad de subida frente al software gratuito (TunnelBear) en base al sistema operativo Linux - distribución Ubuntu 16.4. Asimismo, el software gratuito (TunnelBear) del sistema operativo Windows 10 está posicionado en el tercer lugar, sin embargo, el software licenciado (NordVPN) en base al sistema operativo Windows 10 se encuentra en un escalón inferior, dejando al software libre (ProtonVPN) del sistema operativo Windows 10 y software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 con el promedio más bajo en cuanto al indicador de velocidad de descarga. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red.*** *Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

Tabla 45 Resultados del indicador ancho de banda en base descargas de archivos

| | Ancho de banda de subida | | | | | |
|---|---|---|---|---|---|---|
| | **N°** | **Software VPN** | **Test de velocidad** | **Promedio velocidad de subida (Mbps)** | **Ancho de banda de subida de archivos (KB/s)** | |
| **SISTEMA OPERATIVO:WINDOWS 10** | **1** | **Sin VPN** | Speedtest Minedu | 11,72 | 1500 |  |
| | | | Speedtest Media Commerce Perú | | | |
| | | | Speedtest Ookla | | | |
| | **2** | **Software libre** | Speedtest Minedu | 7,03 | 899 |  |
| | | | Speedtest Media Commerce Perú | | | |
| | | | Speedtest Ookla | | | |
| | **3** | **Software gratuita** | Speedtest Minedu | 1,47 | 188 |  |
| | | | Speedtest Media Commerce Perú | | | |
| | | | Speedtest Ookla | | | |
| | **4** | **Software licenciada** | Speedtest Minedu | 4,37 | 559 |  |
| | | | Speedtest Media Commerce Perú | | | |
| | | | Speedtest Ookla | | | |

| | Ancho de banda de subida | | | | | |
|---|---|---|---|---|---|---|
| | N° | Software VPN | Test de velocidad | Promedio velocidad de subida (Mbps) | Ancho de banda de subida de archivos (KB/s) | |
| SISTEMA OPERATIVO: LINUX(DISTRIBUCION UBUNTU) | 1 | Sin VPN | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 16,43 | 2103 |  |
| | 2 | Software libre | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 1,26 | 161 |  |
| | 3 | Software gratuita | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 2,04 | 261 |  |
| | 4 | Software licenciada | Speedtest Minedu<br>Speedtest Media Commerce Perú<br>Speedtest Ookla | 15,70 | 2009 |  |

Respecto al indicador ancho de banda de subida de archivos, en la **tabla 45** se utilizó tres Speedtest (Speedtest Minedu, Speedtest Media Commerce Perú y Speedtest Ookla) para obtener los promedios de ancho de banda de subidas de archivos en la conexión al servidor de internet. En consecuencia, se puede observar que el promedio de ancho de banda de subidas de archivos de mayor valor se encuentra en el software libre (ProtonVPN) con un registro de 899 KB/s (Kilobyte/sec) en comparación con el software licenciado (NordVPN) con un registro de 559 KB/s, dejando en tercer lugar al software gratuito (TunnelBear) con un registro de 188 KB/s de ancho de banda de subida de archivos en el sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 respecto al indicador ancho de banda de subida de archivos, se puede observar que el promedio de ancho de banda de subida de mayor valor se encuentra en el software licenciado (NordVPN) con un registro de 2009 KB/s (Kilobyte/sec) en comparación con el software gratuito (TunnelBear) con un registro de 261 KB/s, dejando en tercer lugar al software libre (ProtonVPN) con un registro de 161 KB/s de ancho de banda de subidas de archivos.

En referencia a la tabla anterior, se puede evidenciar que el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 mantiene un promedio mayor de velocidad de subida frente al software libre (ProtonVPN) del sistema operativo Windows 10. Asimismo, el software licenciado (NordVPN) del sistema operativo Windows 10 está posicionado en el tercer lugar, sin embargo, el software gratuito (TunnelBear) en base al sistema operativo Linux - distribución Ubuntu 16.4 se encuentra en un escalón inferior, dejando al software gratuito (TunnelBear) en base al sistema operativo Windows 10 y software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 con el promedio más bajo en cuanto al indicador de velocidad de subida. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador Filtro y Marcado de Trafico de red de la variable Rendimiento del Software.**

Tabla 46 Resultados del indicador filtro y marcado de tráfico de protocolos en la red

| | Filtro y Marcado de Trafico de red | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Protocolos de seguridad de datos en la red | | | | | | | | | TOTAL | Protocolos de redes privadas virtuales | | | | TOTAL | TOTAL DE PROTOCOLOS | % | |
| | TCP | ICMP | MDNS | IGMP | UDP | SSDP | NBNS | LLMNR | DNS | | Wireguard | SSL | Openvpn | TLS | | | | |
| SISTEMA OPERATIVO: WINDOWS 10 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 3 | 1 | 0 | 0 | 0 | 1 | 4 | 30.77 | |
| | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 5 | 0 | 0 | 0 | 1 | 1 | 6 | 46.15 | |
| | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 15.38 | |
| | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 6 | 0 | 0 | 0 | 0 | 0 | 6 | 46.15 | |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU 16.4) | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 1 | 1 | 0 | 2 | 5 | 38.46 | |
| | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 4 | 30.77 | |
| | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 | 1 | 3 | 23.08 | |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00 | |

Respecto al indicador filtro y marcado de tráfico de protocolos en la red en base al encriptamiento de datos, en la **tabla 46** se evidencia que en el software gratuito (TunnelBear) registró 5 protocolos de seguridad de datos en la red y 1 protocolo propio del software sumando a 6 protocolos y obteniendo el índice más alto en las evaluaciones en base al sistema operativo Windows con un 46.15%. Además, se evidencia que el software libre (ProtonVPN) registró 4 protocolos de seguridad de datos en la red y 2 protocolos propios del software, con un total de 5 protocolos y obteniendo el índice más alto en las evaluaciones en base al sistema operativo Linux – distribución Ubuntu 16.4 con un 38.46%, entonces, quien destaca en el cumplimiento de protocolos en la red es el software gratuito (TunnelBear) en base al sistema operativo Windows 10.

En referencia a la tabla anterior, se puede evidenciar que el software Gratuito (TunnelBear) en base al sistema operativo Windows 10 cumple con un mayor promedio de protocolos ante el software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4. Asimismo, el software libre (ProtonVPN) y el software gratuito (TunnelBear) están posicionados en el tercer lugar del sistema operativo Windows 10 y sistema operativo Linux - distribución Ubuntu 16.4 respectivamente, sin

embargo, el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 se encuentra en un escalón inferior, dejando al software licenciado (NordVPN) en base al sistema operativo Windows 10 con el promedio más bajo de cumplimiento de protocolo de red en cuanto al indicador filtro y marcado de tráfico de protocolos en la red. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red.*** *Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador Filtro y Marcado de Trafico de red de la variable Rendimiento del Software.**

Tabla 47 Resultados del indicador filtro y marcado de tráfico de red ante el desencriptamiento de datos

| Leyenda |
|---|
| SI = 1 |
| NO = 0 |

| | Filtro y Marcado de Trafico de red | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Protocolos de seguridad de datos en la red | | | | | | | | | TOTAL | Protocolos de redes privadas virtuales | | | | TOTAL | TOTAL DE PROTOCOLOS | % | |
| | TCP | ICMP | MDNS | IGMP | UDP | SSDP | NBNS | LLMNR | DNS | | Wireguard | SSL | OpenVPN | TLS | | | | |
| SISTEMA OPERATIVO: WINDOWS 10 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 1 | 3 | 23.08 | |
| | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 3 | 23.08 | |
| | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 15.38 | |
| | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 3 | 23.08 | |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU 16.4) | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 1 | 3 | 23.08 | |
| | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 5 | 0 | 0 | 0 | 0 | 0 | 5 | 38.46 | |
| | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 7 | 0 | 1 | 0 | 0 | 1 | 8 | 61.54 | |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0 | |

Respecto al indicador filtro y marcado de tráfico de protocolos en la red en base al desencriptamiento de datos, en la **tabla 47** se evidencia que en el software libre (ProntonVPN) registró 2 protocolos de seguridad de datos en la red y 1 protocolo propio del software sumando a tres protocolos y obteniendo el índice más alto en las evaluaciones con un 23.08%, de igual modo, el software gratuito (TunnelBear) registró tres protocolos de seguridad de datos en la red y en ningún protocolo propio del software sumando a tres protocolos e igualando el porcentaje más alto de las evaluaciones con un 23.08% en base al sistema operativo Windows 10. Además, se evidencia que el software licenciado (NordVPN) registró 7 protocolos de seguridad de datos en la red y 1 protocolo propio del software, con un total de 8 protocolos y obteniendo el índice más alto en las evaluaciones en base al sistema operativo Linux – distribución Ubuntu 16.4 con un 61.54% y destacando en el cumplimiento de protocolos en la red ante la comparación de sistemas operativos.

En referencia a la tabla anterior, se puede evidenciar que el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 cumple con un mayor promedio de protocolos ante el software gratuito (TunnelBear) del sistema operativo Linux - distribución Ubuntu 16.4. Asimismo, el software libre (ProtonVPN), el software gratuito (TunnelBear) del sistema operativo Windows 10 y el software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 están posicionados en el tercer lugar, dejando al software licenciado (NordVPN) en base al sistema operativo Windows 10 con el promedio más bajo de cumplimiento de protocolo de red en cuanto al indicador filtro y marcado de tráfico de protocolos en la red. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador velocidad de encriptamiento de datos de la variable rendimiento del software.**

Tabla 48 Resultados velocidad de encriptamiento de datos en una red-LAN

| | Velocidad de encriptamiento de datos | | | | | | |
|---|---|---|---|---|---|---|---|
| | N° | Software VPN | | Tamaño total de paquetes (KiloByte) | Tiempo total de encriptamiento transcurrido (segundos) | Velocidad de encriptamiento KB/s | |
| SISTEMA OPERATIVO: WINDOWS 10 | 1 | Software paga | NordVPN | 862.279 | 119 | 7.25 |  |
| | 2 | Software gratuito | TunnelBear | 862.279 | 110 | 7.84 |  |
| | 3 | Software libre | ProtonVPN | 862.279 | 108 | 7.98 |  |
| | 4 | Prueba sin software | | 862.279 | 154 | 5.60 |  |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU 16.4) | 1 | Software paga | NordVPN | 862.279 | 110 | 7.84 |  |
| | 2 | Software gratuito | TunnelBear | 862.279 | 104 | 8.29 |  |
| | 3 | Software libre | ProtonVPN | 862.279 | 111 | 7.77 |  |
| | 4 | Prueba sin software | | 862.279 | 108 | 7.98 |  |

Respecto al indicador velocidad de encriptamiento de datos en una red-LAN, en la **tabla 48** se evidencia que en el software libre (ProntonVPN) registró un alto índice de velocidad registrado de 7.98 KB/s en base al sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 el software gratuito (TunnelBear) tiene una tasa alta de velocidad con un registro de 8.29 KB/s. En referencia a la tabla anterior, se puede evidenciar que el software gratuito (TunnelBear) en base al sistema operativo Linux - distribución Ubuntu 16.4 cumple con un promedio mayor de velocidad en el encriptamiento de datos ante el software libre (ProtonVPN) del sistema operativo Windows 10. Asimismo, el software gratuito (TunnelBear) del sistema operativo Windows 10 y el software licenciado (NordVPN) del sistema operativo Linux - distribución Ubuntu 16.4 están posicionados en el tercer lugar, sin embargo, el software libre (ProtonVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 se encuentra en un escalón inferior, dejando al software licenciado (NordVPN) en base al sistema operativo Windows 10 con el promedio más bajo de velocidad en el encriptamiento de datos. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red.*** *Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador velocidad de desencriptamiento de datos de la variable rendimiento del software.**

Tabla 49 Resultados velocidad de desencriptamiento de datos en una red-LAN

| | Velocidad de desencriptamiento de datos | | | | | | |
|---|---|---|---|---|---|---|---|
| | N° | Software VPN | | Tamaño total de paquetes (KiloByte) | Tiempo total de encriptamiento transcurrido (segundos) | Velocidad de desencriptamiento KB/s | |
| SISTEMA OPERATIVO: WINDOWS 10 | 1 | Software paga | NordVPN | 862.279 | 96 | 8.98 | |
| | 2 | Software gratuito | TunnelBear | 862.279 | 85 | 10.14 | |
| | 3 | Software libre | ProtonVPN | 862.279 | 83 | 10.39 | |
| | 4 | Prueba sin software | | 862.279 | 93 | 9.27 | |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU 16.4) | 1 | Software paga | NordVPN | 862.279 | 84 | 10.27 | |
| | 2 | Software gratuito | TunnelBear | 862.279 | 98 | 8.80 | |
| | 3 | Software libre | ProtonVPN | 862.279 | 86 | 10.03 | |
| | 4 | Prueba sin software | | 862.279 | 87 | 9.91 | |

Respecto al indicador velocidad de desencriptamiento de datos en una red-LAN, en la **tabla 49** se evidencia que en el software libre (ProntonVPN) registró un alto índice de velocidad de 10.39 KB/s en base al sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 el software licenciado (NordVPN) tiene una tasa alta de velocidad con un registro de 10.27 KB/s. En referencia a la tabla anterior, se puede evidenciar que el software libre (ProtonVPN) en base al sistema operativo Windows 10 cumple con un promedio mayor de velocidad en el desencriptamiento de datos ante el software l licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 16.4. Asimismo, el software gratuito (TunnelBear) del sistema operativo Windows 10 está posicionados en el tercer lugar, sin embargo, el software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 se encuentra en un escalón inferior, el software licenciado (NordVPN) en base al sistema operativo Windows 10 en el penúltimo puesto y dejando al software gratuito (TunnelBear) del sistema operativo Linux

– distribución Ubuntu 16.4., con el promedio más bajo de velocidad en el desencriptamiento de datos. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador velocidad de encriptamiento de datos de la variable rendimiento del software.**

Tabla 50 Resultados velocidad de encriptamiento de datos en una red-WAN

| | Velocidad de encriptamiento de datos | | | | | | |
|---|---|---|---|---|---|---|---|
| | **N°** | **Software VPN** | | **Tamaño total de paquetes (KiloByte)** | **Tiempo de subida de datos encriptados - Punto A (s)** | **Velocidad de encriptamiento KB/s** | |
| **SISTEMA OPERATIVO: WINDOWS 10** | 1 | Software paga | NordVPN | 862.279 | 808.572 | 1.066 | |
| | 2 | Software gratuito | TunnelBear | 862.279 | 573.35 | 1.504 | |
| | 3 | Software libre | ProtonVPN | 862.279 | 486.33 | 1.773 | |
| | 4 | Prueba sin software | | 862.279 | 543.951 | 1.585 | |
| **SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU 16.4)** | 1 | Software paga | NordVPN | 862.279 | 462.927 | 1.863 | |
| | 2 | Software gratuito | TunnelBear | 862.279 | 614.112 | 1.404 | |
| | 3 | Software libre | ProtonVPN | 862.279 | 1538.001 | 0.561 | |
| | 4 | Prueba sin software | | 862.279 | 592.663 | 1.455 | |

Respecto al indicador velocidad de encriptamiento de datos en una red-WAN, en la **tabla 50** se evidencia que en el software libre (ProtonVPN) mantuvo un registro alto de 1.763 KB/s en base al sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 el software licenciado (NordVPN) tiene una tasa alta de velocidad con un registro de 1.863 KB/s. En referencia a la tabla anterior, se puede evidenciar que el software licenciado (NordVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 cumple con un promedio mayor de velocidad en el encriptamiento de datos ante el

software libre (ProtonVPN) del sistema operativo Windows 10. Asimismo, el software gratuito (TunnelBear) del sistema operativo Windows 10 está posicionados en el tercer lugar, no obstante, el software gratuito (TunnelBear) del sistema operativo Linux - distribución Ubuntu 16.4 ocupa el cuarto lugar, sin embargo, el software licenciado (NordVPN) en base al sistema operativo Windows 10 se encuentra en un escalón inferior, dejando al software libre (ProtonVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 con el promedio más bajo de velocidad en el encriptamiento de datos. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red.*** *Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador velocidad del desencriptamiento de datos de la variable rendimiento del software.**

Tabla 51 Resultados velocidad de desencriptamiento de datos en una red-WAN

| | Velocidad de encriptamiento de datos | | | | | | |
|---|---|---|---|---|---|---|---|
| | N° | Software VPN | | Tamaño total de paquetes (KiloByte) | Tiempo de subida de datos encriptados - Punto A (s) | Velocidad de encriptamiento KB/s | |
| SISTEMA OPERATIVO: WINDOWS 10 | 1 | Software paga | NordVPN | 862.279 | 808.572 | 3.374 | |
| | 2 | Software gratuito | TunnelBear | 862.279 | 573.35 | 3.805 | |
| | 3 | Software libre | ProtonVPN | 862.279 | 486.33 | 4.209 | |
| | 4 | Prueba sin software | | 862.279 | 862.279 | 4.652 | |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU 16.4) | 1 | Software paga | NordVPN | 862.279 | 462.927 | 4.977 | |
| | 2 | Software gratuito | TunnelBear | 862.279 | 614.112 | 4.527 | |
| | 3 | Software libre | ProtonVPN | 862.279 | 1538.001 | 0.458 | |
| | 4 | Prueba sin software | | 862.279 | 862.279 | 4.520 | |

Respecto al indicador velocidad de desencriptamiento de datos en una red-WAN, en la **tabla 51** se evidencia que en el software licenciado (NordVPN) mantuvo un registro alto de 4.209 KB/s en base al sistema operativo Windows 10. Además, en el sistema operativo Linux – distribución Ubuntu 16.4 el software libre (ProtonVPN) tiene una tasa alta de velocidad con un registro de 4977 KB/s. En referencia a la tabla anterior, se puede evidenciar que el software libre (ProtonVPN) en base al sistema operativo Linux - distribución Ubuntu 16.4 cumple con un promedio mayor de velocidad en el desencriptamiento de datos ante el software gratuito (TunnelBear) en el sistema operativo Linux – distribución Ubuntu 16.4. Asimismo, el software licenciado (NordVPN) del sistema operativo Windows 10 está posicionados en el tercer lugar, no obstante, el software gratuito (TunnelBear) en base al sistema operativo Windows 10 ocupa el cuarto lugar, sin embargo, el software libre (ProtonVPN) en base al sistema operativo Windows 10 se encuentra en un escalón inferior, dejando al software licenciado (NordVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con el promedio más bajo de velocidad en el desencriptamiento de datos en una red WAN. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Prueba descriptiva para el indicador fugas de dirección IP, fugas de servidores DNS y dirección IP por WebRTC de la variable Rendimiento del Software.**

Tabla 52 Resultados del indicador Fugas de Direcciones IP / Fugas de servidores DNS / Fugas de dirección IP por WebRTC

| | Filtro de Direcciones IP / Filtro de Servidores DNS / Filtro de Direcciones IP por WebRTC | | | | | Leyenda |
|---|---|---|---|---|---|---|
| | N° | Software VPN | Chrome | Firefox | Microsoft Edge | SI = 1 |
| | | | | | | NO = 0 |
| SISTEMA OPERATIVO:WINDOWS 10 | 1 | Sin VPN | 1 | 1 | 1 | |
| | 2 | ProtonVPN | 0 | 0 | 0 | |
| | 3 | TunnelBear | 1 | 1 | 1 | |
| | 4 | NordVPN | 1 | 1 | 1 | |
| SISTEMA OPERATIVO: LINUX (DISTRIBUCION UBUNTU) | 1 | Sin VPN | 1 | 1 | 1 | |
| | 2 | ProtonVPN | 1 | 1 | 1 | |
| | 3 | TunnelBear | 1 | 1 | 1 | |
| | 4 | NordVPN | 0 | 0 | 0 | |

Respecto al indicador Filtro de Direcciones IP / Filtro de Servidores DNS / Filtro de Direcciones IP por WebRTC, en la tabla 49 se utilizó tres navegadores web (Chrome, Firefox y Microsoft Edge) para verificar si filtra paquetes de datos por el túnel del software VPN ante la reconexión de internet. En consecuencia, el software libre (ProtonVPN) no filtra por dirección IP, servidor DNS y dirección IP por WebRTC, dejando al software gratuito (TunnelBear) y licenciado (NordVPN) del sistema operativo Windows 10 como aquellos softwares que filtran datos de paquetes tanto como dirección IP, servidor DNS y dirección IP por WebRTC. Además, el software licenciado (NordVPN) no filtra por dirección IP, servidor DNS y dirección IP por WebRTC, dejando al software gratuito (TunnelBear) y libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 como aquellos softwares que filtran datos de paquetes tanto como dirección IP, servidor DNS y dirección IP por WebRTC. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto al* ***desempeño en la red****. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

**Indicador: Conexión al servidor VPN**

**Prueba de normalidad para el indicador conexión al servidor VPN**

Para el proceso del indicador conexión al servidor VPN para evaluar la prueba de normalidad se utilizó Shapiro-Wilk dado que la cantidad de la muestra es < 50.

Tabla 53 Resultados de prueba de normalidad del indicador conexión al servidor VPN

| Pruebas de normalidad | | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| **W_ProtonVPN** | ,340 | 3 | . | ,848 | 3 | ,235 |
| **W_TunnelBear** | ,254 | 3 | . | ,964 | 3 | ,634 |
| **W_NordVPN** | ,346 | 3 | . | ,837 | 3 | ,205 |
| **L_ProtonVPN** | ,241 | 3 | . | ,974 | 3 | ,691 |
| **L_TunnelBear** | ,250 | 3 | . | ,967 | 3 | ,652 |
| **L_NordVPN** | ,241 | 3 | . | ,974 | 3 | ,689 |

En la **tabla 53**, se han registrado datos > α=0,05 que evitan rechazar la Ho (distribución normal). En síntesis, se utilizaron pruebas paramétricas para las comparaciones en cuanto al indicador conexión al servidor VPN.

Tabla 54 Resultados de la prueba t de student para muestras relacionadas del indicador conexión al servidor VPN del sistema operativo Windows 10.

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | **Media** | **N** | **Desv. Desviación** | **Desv. Errorpro-medio** |
| Par 1 | W_NordVPN | 6,77767 | 3 | 4,527992 | 2,614237 |
| | W_ProtonVPN | 12,94833 | 3 | ,620130 | ,358032 |
| Par 2 | W_NordVPN | 6,77767 | 3 | 4,527992 | 2,614237 |
| | W_TunnelBear | 12,41600 | 3 | 1,546294 | ,892753 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bi-late-ral) |
| | | Media | Desv. Des-via-ciónn | Desv. Error prome-dio | 95% de intervalo de con-fianza de la diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | W_NordVPN -W_Pro-tonVPN | -6,170667 | 3,907948 | 2,256255 | -15,878547 | 3,537213 | -2,735 | 2 | ,112 |
| Par 2 | W_NordVPN - W_Tun-nelBear | -5,638333 | 5,197967 | 3,001048 | -18,550800 | 7,274133 | -1,879 | 2 | ,201 |

Tal y como se observa en las tablas anteriores, se evidencia que el software licenciado (NordVPN) muestra una media baja de tiempo de conexión al servidor VPN frente al software gratuito (TunnelBear) y software libre (ProtonVPN) en el sistema operativo Windows 10. De acuerdo a la **Tabla 54**, se observa los niveles de significancia asintótica equivalentes a 0,112 comparando ProtonVPN con NordVPN, asimismo, TunnelBear con NordVPN con una significancia asintótica de 0,201.

Tabla 55 Resultados de la prueba t de student para muestras relacionadas del indicador conexión al servidor VPN del sistema operativo Linux – distribución Ubuntu 16.4

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | Media | N | Desv. Desviación | Desv. Errorpro-medio |
| Par 1 | L_ProtonVPN | 10,39133 | 3 | 3,235822 | 1,868203 |
| | L_TunnelBear | 4,28433 | 3 | ,493187 | ,284742 |
| Par 2 | L_ProtonVPN | 10,39133 | 3 | 3,235822 | 1,868203 |
| | L_NordVPN | 5,08800 | 3 | 1,695868 | ,979110 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bi-late-ral) |
| | | Media | Desv. Des-via-ciónn | Desv. Error prome-dio | 95% de intervalo de con-fianza de la diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | L_Proton-VPN -L_Tun-nelBear | 6,107000 | 2,742758 | 1,583532 | -,706389 | 12,920389 | 3,857 | 2 | ,061 |
| Par 2 | L_Proton-VPN - L_NordVP N | 5,303333 | 1,715891 | ,990670 | 1,040825 | 9,565842 | 5,353 | 2 | ,033 |

Tal y como se observa en las tablas anteriores, se evidencia que el software gratuito (TunnelBear) muestra una media baja de tiempo de conexión al servidor VPN frente al software licenciado (NordVPN) y software libre (ProtonVPN) en el sistema operativo Linux – distribución Ubuntu 16.4. De acuerdo a la **Tabla 55**, se observa los niveles de significancia asintótica equivalentes a 0,061 comparando ProtonVPN con TunnelBear, asimismo, ProtonVPN con NordVPN con una significancia asintótica de 0,033.

Tabla 56 Resultados de la prueba t de student para muestras relacionadas del indicador conexión al servidor VPN- Comparación de S.O

| Estadísticas de muestras emparejadas | | | | | |
|---|---|---|---|---|---|
| | | Media | N | Desv. Desviación | Desv. Error promedio |
| Par 1 | W_NordVPN | 6,77767 | 3 | 4,527992 | 2,614237 |
| | L_TunnelBear | 4,28433 | 3 | ,493187 | ,284742 |

| Prueba de muestras emparejadas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Diferencias emparejadas | | | | | t | gl | Sig. (bi-lateral) |
| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | | | |
| | | | | | Inferior | Superior | | | |
| Par 1 | W_NordVPN - L_TunnelBear | 2,493333 | 4,943236 | 2,853979 | -9,786346 | 14,773012 | ,874 | 2 | ,474 |

De acuerdo a la **Tabla 56**, comparando las tecnologías de software VPN más resaltantes entre los sistemas operativos se pudo evidenciar que el software gratuito (TunnelBear) del sistema operativo Linux – Distribución Ubuntu 16.4. Muestra un índice bajo en la conexión al servidor en comparación con el software licenciado (NordVPN) del sistema operativo Windows 10. Por ello, en la **Tabla 56**, se observa los niveles de significancia asintótica equivalentes a 0,474 al comparar el software gratuito (TunnelBear) del sistema operativo Linux – Distribución Ubuntu 16.4 con el software libre (ProtonVPN) del sistema operativo Windows 10.

En referencia a las tablas anteriores, se puede evidenciar que el software libre (TunnelBear) del sistema operativo Linux - distribución Ubuntu 16.4 mantiene un índice bajo en la conexión al servidor VPN frente al software licenciado (NordVPN) del sistema operativo Linux - distribución Ubuntu 16.4. Asimismo, el software licenciado (NordVPN) del sistema operativo Windows 10 está posicionado en el tercer lugar, sin embargo, el software libre (ProtonVPN) se encuentra en un escalón inferior en base al sistema operativo Linux - distribución Ubuntu 16.4, dejando al software gratuito (TunnelBear) del sistema operativo Windows 10 en el penúltimo puesto y el software libre (ProtonVPN) del sistema operativo Windows 10 con el índice más alto en cuanto al indicador

conexión al servidor VPN. *En síntesis, se acepta que la metodología MEPVPNS permitió evaluar los softwares de redes privadas virtuales en cuanto a la* ***desempeño en la red.*** *Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.*

### 4. 2.4 Hipótesis General

$\mathbf{HG_0}$: La aplicación de los procesos de la metodología MEPVPNS no permitió determinar la evaluación de rendimiento de los softwares de redes privadas virtuales.

$\mathbf{HG_1}$: La aplicación de los procesos de la metodología MEPVPNS permitió determinar la evaluación de rendimiento de los softwares de redes privadas virtuales.

A continuación, se especifica los resultados extraídos conforme a las evaluaciones realizadas a través del proceso de la evaluación de rendimiento de los softwares de redes privadas virtuales.

Para comprobar la hipótesis general, se presentará el esquema general con los resultados obtenidos por cada indicador de la presente investigación. De esta forma se expresará la decisión de rechazo o aceptación a la formulación de hipótesis general

Tabla 57 Resumen general – Resultados de hipótesis

| N | Resultados | | | | | |
|---|---|---|---|---|---|---|
| | Software VPN | Tipo de software | Sistema Operativo | Indicadores | Valor Promedio | Escala |
| 1 | NordVPN | Licenciado | Windows 10 | Throughput | 2710,29 | Byte/s |
| 2 | ProtonVPN | Libre | Ubuntu 16.4 | Jitter | 0,029 | ms |
| 3 | NordVPN | Licenciado | Windows 10 | Uso del CPU | 26,85 | % |
| 4 | ProtonVPN | Libre | Windows 10 | Uso de Memoria RAM | 66,10 | % |
| 5 | ProtonVPN | Libre | Ubuntu 16.4 | Uso del Disco Duro | 0,85 | % |
| 6 | NordVPN | Licenciado | Ubuntu 16.4 | Latencia | 117 | ms |
| 7 | NordVPN | Licenciado | Ubuntu 16.4 | Velocidad de descargas de archivos | 38,85 | Mbps |
| 8 | NordVPN | Licenciado | Ubuntu 16.4 | Velocidad de subidas de archivos | 15,70 | Mbps |
| 9 | NordVPN | Licenciado | Ubuntu 16.4 D | Ancho de banda | 4973 | KB/s |
| 10 | NordVPN | Licenciado | Ubuntu 16.4 S | | 2009 | KB/s |
| 11 | TunnelBear | Gratuito | Windows 10 E | Filtro y marcado de trafico de red | 46,15 | % |
| 12 | NordVPN | Licenciado | Ubuntu 16.4 D | | 51,54 | % |
| 13 | ProtonVPN | Libre | Windows 10 L | Velocidad de encriptamiento de datos | 7,98 | KB/s |
| 14 | NordVPN | Licenciado | Ubuntu 16.4 W | | 1,863 | KB/s |
| 15 | ProtonVPN | Libre | Windows 10 L | Velocidad de desencriptamientode datos | 10,39 | KB/s |
| 16 | NordVPN | Licenciado | Ubuntu 16.4 W | | 4,977 | KB/s |
| 17 | ProtonVPN | Libre | Windows 10 | Fugas de servidores DNS -Dirección IP - Dirección IP por WebRTC | 0 | ------- |
| 17 | NordVPN | Licenciado | Ubuntu 16.4 | | 0 | ------- |
| 18 | TunnelBear | Gratuito | Ubuntu 16.4 | Conexión al servidor | 4,284 | ms |

De acuerdo con la **tabla 57**, se puede observar los resultados de cada indicador de la investigación. De este modo se afirma que la aplicación de los procesos de la metodología MEPVPNS permitió determinar la evaluación de rendimiento de los softwares de redes privadas virtuales en cuanto a: (i)rendimiento del software, (ii) administración de recursos y (iii) desempeño en la red. Por lo tanto, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.

## IV. Resumen

Tabla 58 Validacion de las hipótesis

| Nº | Detalles de hipótesis | Resultado |
|---|---|---|
| H1 | La aplicación de los procesos de la metodología MEPVPNS permitió la evaluación de los softwares de redes privadas virtuales en cuanto al rendimientodel software | Aceptación |
| H2 | La aplicación de los procesos de la metodología MEPVPNS permitió evaluar lossoftwares de redes privadas virtuales en cuanto a la administración de recursos | Aceptación |
| H3 | La aplicación de los procesos de la metodología MEPVPNS permitió evaluar lossoftwares de redes privadas virtuales en cuanto al desempeño en la red | Aceptación |
| H4 | La aplicación de los procesos de la metodología MEPVPNS permitió evaluar lossoftwares de redes privadas virtuales- | Aceptación |

De acuerdo a la **tabla 58**, se define los resultados de esta investigación fueron muy positivos ante el uso del software VPN. Debido a que se llegó a cumplir con todas las hipótesis planteadas.

# V. DISCUSIÓN

En este apartado, luego de presentar los resultados de la aplicación de la metodología MEPVPNS en los software de redes privadas virtuales (NordVPN, TunnelBear, ProtonVPN) en base a dos sistemas operativos (Windows10 y Linux – distribución Ubuntu 16.4) se procede a comparar los aspectos más importantes con los resultados de las investigaciones previas teniendo en cuenta las hipótesis de estudio, antecedentes y marco teórico en busca de semejanzas, diferencias, comparaciones con la presente investigación. Luego de la recolección de datos se puede llegar a identificar la relación con los resultados de los trabajos previos. De este modo, se llega a demostrar, contrastar y/o justificar la comparación de información extraído de las pruebas de evaluación de rendimiento.

De acuerdo a la hipótesis específica 1, La aplicación de los procesos de la metodología MEPVPNS permitirá la evaluación de los softwares de redes privadas virtuales en cuanto al **rendimiento del software.** De acuerdo a ello, se obtuvo resultados para los indicadores throughput y jitter en la transferencia de datos. Por consiguiente, para el indicador throughput se utilizó RFC-2544 en donde se manifiesta el uso de las tramas: (a) 64, (b) 128, (c) 256, (d) 512, (e) 1024, (f) 1280 y (g) 1518 bytes para la evaluación de throughput, siendo el software libre (ProtonVPN) del sistema operativo Windows 10, el cual mantuvo los resultados más bajos en comparación de todos los softwares, tales como: 453, 226, 113, 56, 28, 22, 19 Bps en base a las tramas de RFC-2544. Sin embargo, el software licenciado (NordVPN) del sistema operativo Windows 10 muestra mejores resultados, tales como: 9328, 4680, 2344, 1171, 586, 468 y 395 Bps. Del mismo modo, muestra similitud la investigación de Pacotaype (2018) porque calculó la velocidad real (throughput) del firewall de hardware y software con los siguientes tamaños de paquetes de red (64, 128, 256, 512, 1024, 1280 y 1518 Kilobytes) demostrando resultados favorables para los firewalls de hardware con los siguientes promedios: 4,4598; 8,9894; 15,5642; 29,0060; 57,2690; 75,9060 y 74,0398 Kilobytes respectivamente.

Sin embargo, estos procesos y resultados se ven contrastados en la investigación de Apolo y Coral (2017) debido a que no empleó ningún tamaño estándar en el desarrollo de su prueba en base a software libre, denominados: (a) Armada, (b) Ejercito y (c) Comaco, obteniendo un decrecimiento notable de 7.4 Mbps en la transferencia de datos de 14.84 Mbps enviados representando

un 49.86% de datos recepcionados satisfactoriamente enfocado al VPN “armada”, de igual modo, en el vpn: (i) Ejército y (ii) Comaco hubo un decrecimiento insignificante de 0,04 Mbps de 9.8 Mbps en la transferencia de datos transferidos siendo los vpn más sobresalientes en las pruebas de rendimiento.

Por consiguiente, para el indicador jitter se utilizó RFC-2544 en donde se manifiesta el uso de las tramas: (a) 64, (b) 128, (c) 256, (d) 512, (e) 1024, (f) 1280 y (g) 1518 bytes para la evaluación de jitter, siendo el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4, mantuvo el índice más bajo en comparación de todos los softwares con un promedio menor de 0,029 milisegundos en base a las tramas de RFC-2544. Sin embargo, el software libre (ProtonVPN) del sistema operativo Windows 10, sostuvo el índice más alto en comparación de todos los softwares con un promedio mayor de 0.709 milisegundos. Este resultado muestra semejanza con el trabajo de Apolo y Coral (2017) debido que utilizaron softwares libres VPN, tales como: (a) Armada, (b) Ejército y (c) Comaco, en el desarrollo de sus pruebas del criterio jitter; donde obtuvieron los siguientes resultados: (i) voz: con una disminución relativa de 27 ms con una superioridad de 33 % en transmisión de voz y (ii) video: con una disminución relativa de 15 ms con una superioridad de 21% en la transmisión de video.

De acuerdo a la hipótesis específica 2, La aplicación de los procesos de la metodología MEPVPNS permitirá la evaluación de los softwares de redes privadas virtuales en cuanto a la **administración de recursos.** Con respecto a ello, se obtuvo resultados para los indicadores uso del CPU, uso de memoria RAM y uso del Disco Duro ante ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuidos (DDoS) mediante el uso del entorno IDPS/IPS Snort para monitorear el tráfico de red, ataques y anomalías dentro del sistema, para ello, se utilizó diferentes tipos de ataques cibernéticos, tales como: Hping, byte-DDoS, DDoS-Anonymous, Hammer, UDP flooder, SMG DOSER, LOIC (Low Orbit Ion Cannon), bats y el Ufonet (Botnet) obteniendo un incremento menor de 34.3% haciendo uso del software licenciado (NordVPN) del sistema operativo Windows 10. Este resultado se diferencia del trabajo de Pudelko, Emmerich, Gallenmáller y Carle (2020) debido a que desarrollaron su

investigación implementando una vpn en base a software libre referido a tres protocolos, tales como: (i) OpenVPN, (ii) Linux IPsec y (iii) Wireguard obteniendo como resultado un incremento de 10% y 20% del total del uso del CPU dependiendo de subprocesos del sistema al momento de emplear enrutamientos con los núcleos del CPU con diferentes tipos de paquetes (1, 4, 64 y 256 registros) en base al sistema operativo Linux – Ubuntu 16.4.

De igual modo, los resultados se ven contrastados con el trabajo de Caprolu et al. (2019) porque implementaron una maquina con canales VPNs ante ataques de denegación de servicio distribuido afectando a los dos protocolos: (a) IPSEC/IKE, (b) IPSEC/SD-SA y obteniendo como resultado un incremento en el uso de recursos (CPU y memoria RAM) en base a softwares de redes privadas virtuales, tales como: (i) NordVPN v. 1.2.0 y (ii) ExpressVPN v. 1.5.0 demostrando el incremento exponencial del CPU, GPU y memoria RAM mientras es víctima de ataques cibernéticos en la red. Asimismo, con el trabajo de Gunleifsen, Kemmerich y Gkioulos (2019) en donde hicieron uso del sistema operativo Linux (kernel) enfocado para monitorear el rendimiento del CPU ante el tráfico de datos encriptados, obtuvo como resultados que en el proceso de cifrado y descifrado de paquetes el consumo de CPU alcanza un nivel mayor al 90%.

Por otro lado, en cuanto al indicador uso de Memoria RAM se obtuvo como resultado que el software libre (ProtonVPN) del sistema operativo Windows 10 muestra un menor índice de incremento del uso de Memoria RAM, con un estado normal de 41.95 % llegando a incrementar hasta un 66.1 % siendo el promedio menor de los softwares seleccionados para la investigación. Estos resultados se asemejan al estudio de Gunleifsen, Kemmerich y Gkioulos (2019) debido a que indicaron que para la evaluación y administración de recursos se empleó la herramienta fstab y el administrador de tareas con el propósito de gestionar el uso de la memoria RAM en base al sistema operativo Windows con el protocolo IKE SA (IKEv1) manteniendo un alto promedio haciendo uso de recursos de SD-SA muestra una diferencia de 28.5% en base a un vpn libre propio.

Por otra parte, en cuanto al indicador uso de Disco duro se obtuvo como resultado que el software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 no muestra un incremento en el uso del disco duro antes DDoS, con un promedio de estado normal de 1.1 % llegando a tener un estado insignificante de 0.85 % siendo el promedio menor de los softwares seleccionados para la investigación sin afectar al sistema en la lectura y escritura de archivos empleando el software, esto fue evaluado en base al panel de nmon. Este resultado es apoyado con el trabajo de Macías (2017) debido a que la investigación a fondo muestra resultados determinantes, pues la institución UNESUM no cuenta con un software de protección ante ataques cibernéticos, ante ello, Macías (2017) recomendó realizar un análisis previo de anomalías al sistema para detectar daños, colapsos al sistema y perdida de información irreparables en el disco duro.

De acuerdo a la hipótesis específica 3, La aplicación de los procesos de la metodología MEPVPNS permitirá la evaluación de los softwares de redes privadas virtuales en cuanto al **desempeño en la red.** En relación a lo anterior mencionado, se obtuvo resultados para los indicadores de latencia, velocidad de subida de archivos, velocidad de descargas de archivos, ancho de banda, filtro y marco de trafico de red, velocidad de encriptamiento de datos, velocidad de desencriptamiento de datos, fugas servidores DNS, fugas de dirección IP y fugas de dirección IP por WebRTC, con respecto al indicador latencia se obtuvo como resultado que el software licenciado (Nordvpn) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 117 milisegundos de 47 ms en un estado normal. Sin embargo, el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 sostuvo el índice más alto en comparación de todos los softwares con un promedio de 326 ms de 47 ms en estado normal.

Este resultado es semejante al trabajo de Fernandez y López (2020) porque indicaron que la implementación de un datacenter definidos por software en base a VPN, muestra un incremento en el promedio de la latencia con un registro de 24.06 milisegundos. Sin embargo, se contrasta con los resultados de Adewale, Adagunodo, John y Ndujiuba (2017) debido a que mantiene un propósito diferente a la investigación, tal como: mejorar el performance de la red

para ofrecer servicios de calidad en base a los siguientes protocolos (a) IP, (b) MPLS VPN y (c) MPLS-TE obteniendo resultados que muestra una clara disminución de latencia y en la perdida de paquetes en la transferencia de datos a través de la red.

Por otro lado, para el indicador velocidad de descarga de archivos en base al uso del software vpn se obtuvo como resultado que el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 1.82 Mbps de 40.38 Mbps en un estado normal. Además, los resultados arrojaron que el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 16.4 sostuvo el índice más alto en comparación de todos los softwares con un promedio de 38.85 Mbps de 40.38 Mbps en estado normal. Este resultado muestra semejanza con el trabajo de Ian (2021) debido a que al utilizar el software licenciado (NordVPN) para realizar pruebas de estrés y saturación, se obtuvo como resultado que la velocidad de descarga no bajo más del 60% del estado normal sin el uso del software.

De igual modo, para el indicador velocidad de subida de archivos en base al uso del software vpn se obtuvo como resultado que el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 1.26 Mbps de 16.43 Mbps en un estado normal. Además, los resultados arrojaron que el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 16.4 sostuvo el índice más alto en comparación de todos los softwares con un promedio de 15.70 Mbps de 16.43 Mbps en estado normal. Este resultado muestra semejanza con el trabajo de Ian (2021) debido a que al utilizar el software licenciado (NordVPN) para realizar pruebas de estrés y saturación, se obtuvo como resultado que la velocidad de subida no bajo más del 40% del estado normal sin el uso del software.

Además, para el indicador ancho de banda para descargas de archivos en base al uso del software vpn se obtuvo como resultado que el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 232

KBs de 5169 KBs en un estado normal. Además, los resultados arrojaron que el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 4973 KBs sostuvo el índice más alto en comparación de todos los softwares con un promedio de 5169 KBs en estado normal. Estos resultados muestran diferencia al trabajo de Mendoza y Ortega (2019) debido a que utiliza la herramienta Iperf y Opnet para evaluar el ancho de banda en base a la unidad de medida de Mbps con un resultado de 0,44 Mbps por parte del software gratuito (TunnelBear) mostrando una diferencia menor de impacto en el ancho de banda en comparación sin el uso de un software VPN.

Por consiguiente, para el indicador filtro y marcado de trafico de red en base al encriptamiento de datos, se utilizó la herramienta de monitoreo wireshark para capturar el tráfico de red en la prueba de evaluación, ante ello, el software licenciado (NordVPN) en base al sistema operativo Windows 10 muestra un índice mínimo de protocolos ante el encriptamiento de datos con un total de 2 registros de protocolos, tales como: (i)UDP, (ii) NBNS con un porcentaje de 15.38 %. Por otro lado, el software gratuito (TunnelBear) registró 5 protocolos de seguridad de datos en la red (TCP, UDP, SSDP, NBNS y DNS) y 1 protocolo propio de redes privadas virtuales (TLS) sumando a 6 protocolos y obteniendo el índice más alto en las evaluaciones en base al sistema operativo Windows 10 con un porcentaje de 46.15%. Este resultado es contrastado con los resultados de Rodríguez (2020) debido a que evaluaron el tráfico de red en base al software Cacti para describir los índices más alto de saturación en la red dando como resultado que la primera entidad CNT manifestó que promedio mínimo es de 41.36%, asimismo como segunda entidad MEGADATOS-NETLIFE ocupa el promedio mínimo de 17.48 % y por último la entidad SETEL con un promedio mínimo de 11.25% en cuanto a tráfico de red en base a vpn.

Además, para el indicador filtro y marcado de trafico de red en base al desencriptamiento de datos, se utilizó la herramienta de monitoreo wireshark para capturar el tráfico de red en la prueba de evaluación, ante ello, el software licenciado (NordVPN) en base al sistema operativo Windows 10 muestra un índice mínimo de protocolos ante el desencriptamiento de datos con un total de 2 registros de protocolos, tales como: (i)UDP, (ii) NBNS con un porcentaje de 15.38 %.Sin embargo, el software licenciado (NordVPN) registró 7 protocolos de

seguridad de datos en la red (TCP, ICMP, MDNS, IGMP, UDP, SSDP, NBNS, LLMNR) y 1 protocolo propio del software de redes privadas virtuales (SSL) con un porcentaje de 61.54 %. Estos resultados muestran semejanza con el trabajo de Tibaduiza (2015) debido a que evaluaron el tráfico de paquetes en la red de la entidad FSD S.A.S en base al software Mikrotik para establecer y/o proveer potenciales fallas para asegurar el intercambio de datos, dando como resultado 0.045% en la transferencia de paquetes de autenticación, asimismo, el 99.955% de paquetes que se transportan por la red mediante los principales protocolos: (a) HTTP (Protocolo Seguro de Transferencia de Hipertexto) y (b) HTTPS. Además, se manifiesta protocolos registrados en las evaluaciones, tales como: (i)TCP, (ii)UDP, (iii)ICMP, (iv)IGMP y (v)GRE.

Por otro lado, para el indicador velocidad de encriptamiento de datos se utilizó la herramienta GoAnywhere Open PGP Studio la misma que permitió determinar la velocidad de encriptamiento de datos ante el uso del software VPN a través del algoritmo RSA y criptografía asimétrica en una red LAN-WAN, ante ello, el software licenciado (NordVPN) en base al sistema operativo Windows 10 muestra una velocidad mínima de 7.25 KB/s en una red LAN, sin embargo, en una red WAN el software libre (ProtonVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con una velocidad mínima de 0.561 KB/s. Por otro lado, el software libre (ProtonVPN) en base al sistema operativo Windows 10 muestra un índice alto de 7.98 KB/s en una red LAN, sin embargo, en una red WAN el software licenciado (NordVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con un índice alto de 1.863 KB/s. Estos resultados son semejantes al trabajo de Velasco, Jiménez y Chafla (2017) porque empleo la herramienta DiskCryptor para evaluar la velocidad de algoritmos (AES, TWOFISH, SERPENT) de encriptamiento de datos a través de disco duros de tamaños (243 GB, 454 GB, 2.03 MB y 7.2 GB) dando como resultados que el algoritmo AES tuvo un índice mayor de velocidad en cuanto a la encriptación por paquetes, tales como: (a)130.55, (b)141.16, (c)137.54 y (d)138.66, respectivamente.

Por otro lado, para el indicador velocidad de desencriptamiento de datos se utilizó la herramienta GoAnywhere Open PGP Studio la misma que permitió determinar la velocidad de desencriptamiento de datos ante el uso del software VPN a través del algoritmo RSA y criptografía asimétrica en una red LAN-WAN, ante ello, el software gratuito (TunnelBear) en base al sistema operativo Linux – distribución Ubuntu 16.4 con una muestra de velocidad mínima de 8.80 KB/s en una red LAN, sin embargo, en una red WAN el software libre (ProtonVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con una velocidad mínima de 0.458 KB/s. Por otro lado, el software libre (ProtonVPN) en base al sistema operativo Windows 10 muestra un índice alto de 10.39 KB/s en una red LAN, sin embargo, en una red WAN el software libre (NordVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con un índice alto de 4.977 KB/s. Estos resultados son semejantes al trabajo de de Velasco, Jiménez y Chafla (2017) porque empleo la herramienta TrueCrypt para evaluar la velocidad de algoritmos (AES, TWOFISH, SERPENT) variando el buffer del desencriptamiento de datos a través de disco duros de tamaños (100KB, 500KB, 1MB, 50MB, 200MB) dando como resultados que el algoritmo AES tuvo un índice mayor de velocidad en cuanto a la desencriptación por paquetes a través de paquetes de 1 KB a 100 KB con una velocidad no mayor a 80 MB/s, demostrando que mientras el tamaño se encuentre en el intervalo de 50 MB y 200 MB habrá un incremento exponencial.

Además, para los indicadores fugas de dirección IP, servidores de DNS y dirección IP por WebRTC, para ello se utilizó LeakTest la misma que permitió evaluar las fugas recurrentes frente a la reconexión de internet en un lapso de tiempo determinado, ante ello, el software libre (ProtonVPN) del sistema operativo Windows 10 y el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 16.4 no muestran fugas ante la reconexión de internet en el lapso de 5 minutos, asimismo, para corroborar las pruebas de evaluación se empleó en 3 navegadores web, tales como: (a) Google Chrome, (b) Firefox y (c) Microsoft Edge. Este resultado es diferente al trabajo de Av comparatives (2020) debido a que los softwares vpn: (a) Nordvpn, (b) ProtonVPN y (c) TunnelBear no muestran fugas ante las pruebas de Leak Kill-switch, sin

embargo, para los softwares gratuitos: (i) Panda Dome VPN y (ii) SaferVPN muestran en sus resultados fugas de servidores DNS y dirección IP.

Sin embargo, para el indicador fugas de servidores DNS el resultado es semejante al trabajo de Ian (2021) debido a que recomienda verificar si el proveedor de software VPN se encuentra filtrando los servidores de DNS haciendo uso de la página LeakTest para mantener la integridad, privacidad, confiablidad y seguridad ante la conexión del software vpn. Además, para el indicador fugas de dirección IP para WebRTC el resultado es semejante al estudio de Al-fannah (2017) debido a que su investigación empleó navegadores web para demostrar que datos privados de sus usuarios filtraban los principales softwares vpn (ZenMate, HMA, ExpressVPN, VyprVPN, TorGuard) en base a 2 criterios: (a) dirección IP y (b) dirección IP por WebRTC, obteniendo como resultado que en el navegador Safari no se filtró datos por ningún criterio, sin embargo, se dedujo que se filtraban datos parcial o totalmente de los usuarios haciendo uso del navegador Edge.

Además, para el indicador conexión al servidor empleando un cronometro virtual se pudo recepcionar el tiempo de demora para conectar el software vpn con servidores ubicados en diferentes puntos, tales como: Países Bajos, (ii) Japón y (iii) Estados Unidos, ante ello el software libre (ProtonVPN) del sistema operativo Windows 10 obtuvo una media mayor de conexión con un registro de 12.948 segundos. Sin embargo, el software gratuito (TunnelBear) del sistema operativo Linux – distribución Ubuntu 16.4 obtuvo una media menor de conexión con un registro de 4.284 segundos. Estos resultados muestran diferencia al trabajo de Abril y Cuzco (2019) debido a que su investigación busco implementar alertas remotas mediante el uso de softwares libres se evaluó el ancho de banda y el tiempo de conexión al servidor vpn, obteniendo como resultados que registro caídas en un lapso de tiempo de 1 minuto ante la actualización de datos del sistema y llaves de conexión virtual, además el ancho de banda aceptable para la conexión al servidor de la vpn se encuentra en el intervalo de 2 a 2.5 Mbits/s.

En relación a la hipótesis general, la aplicación de los procesos de la metodología MEPVPNS permitió determinar la evaluación de rendimiento de los softwares de redes privadas virtuales, este resultado concuerda con el trabajo de Bravo (2015) que manifestó en su investigación que el uso de la metodología Cisco (Top-Down Network Design) permitió organizar, detallar y ejecutar los procesos necesarios para alcanzar los objetivos planteados en el proyecto de su organización, permitiendo disminuir el tráfico de red (de 59% a 18%) logrando demostrar la efectividad de una metodología para la gestión y monitoreo de un proyecto (Bravo, 2015, p. 76; Segura y Ramírez, 2018, p. 48). De igual modo, es semejante al estudio de Pacotayte (2018) en la cual indicó que la metodología MERF (Metodología de Evaluación de Rendimiento de Firewalls) permitió determinar que los firewalls de hardware tienen mayor rendimiento que los firewalls de software en base a 3 criterios: (a) desempeño en la red, (b) eficacia de la seguridad y (c) consumo de recursos.

Finalmente, se evidencio dado a los resultados obtenidos mediante la aplicación de los procesos de la metodología MEPVPNS permitió corroborar la evaluación de los softwares de redes privadas virtuales en cuanto a: (i)rendimiento del software, (ii) administración de recursos y (iii) desempeño en la red

# VI. CONCLUSIONES

De acuerdo, a lo expuesto en el desarrollo del presente trabajo de investigación permite arribar las siguientes conclusiones:

A. La aplicación de los procesos de la metodología MEPVPNS permitió la evaluación de los softwares de redes privadas virtuales en cuanto al **rendimiento del software**, luego de seguir los términos propuestos en el entorno de pruebas de evaluación de la presente investigación. Es necesario enfatizar que luego de las pruebas en base a los procesos de la metodología MEPVPNS de la variable rendimiento del software, en el **indicador throughput** el software libre (ProtonVPN) del sistema operativo Windows 10 mantuvo el promedio más bajo con 131 Bytes de 2821 Bytes en un estado normal, es decir, sin uso de un software vpn en comparación con todos los softwares de la evaluación. Sin embargo, el software licenciado (NordVPN) del sistema operativo Windows 10 muestra el promedio más alto con 2710 Bytes de 2821 Bytes en un estado normal. Los resultados de Apolo y Coral (2017) fueron semejantes a los de la presente investigación debido a que hubo un decrecimiento notable en la transferencia de datos de punto a punto en las VPN (Ejercito y Comaco) ante la evaluación de rendimiento con un promedio de 7.4 Mbps de un 14.84 Mbps de un estado normal.

B. Respecto al **indicador Jitter**, el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el promedio más bajo con 0.029 ms. Sin embargo, el software libre (ProtonVPN) del sistema operativo Windows 10 muestra el promedio más alto con 0.709 ms. Los resultados de Apolo y Coral (2017) fueron menores a los de la presente investigación debido a que su procedimiento evaluó la transmisión de voz con una disminución considera de 0.027 ms y de video con una disminución de 0.015 ms en la transferencia de datos de punto a punto en las VPN (Ejercito y Comaco) ante la evaluación de rendimiento.

C. La aplicación de los procesos de la metodología MEPVPNS permitió la evaluación de los softwares de redes privadas virtuales en cuanto a la **administración de recursos**, luego de seguir los términos propuestos en el entorno de pruebas de evaluación de la presente investigación. Es necesario enfatizar que luego de las pruebas en base a los procesos de la metodología

MEPVPNS de la variable administración de recursos, en **el indicador uso del CPU**, el software licenciado (NordVPN) del sistema operativo Windows 10 obtuvo un promedio menor de 34.3 % ante las pruebas de estrés. Los resultados de Pudelko, et al. (2020) fueron menores a los de la presente investigación debido a que hubo un incremento de 10% y 20% ante los subprocesos de sistema al momento de emplear enrutamiento con los núcleos del CPU mediante cuatro tipos de paquetes (1, 4, 64 y 256 registros) en base a software libre referido a tres protocolos, tales como: (i) OpenVPN, (ii) Linux IPsec y (iii) WireGuard en el sistema operativo Linux – Ubuntu 16.4.

D. En el **indicador uso de Memoria RAM**, el software libre (ProtonVPN) del sistema operativo Windows 10 muestra un menor índice de incremento de un estado normal de 41.95 % llegando a aumentar hasta un 66.1 % siendo el promedio menor de los softwares seleccionados para la investigación. Los resultados de Gunleifsen, Kemmerich y Gkioulos (2019) fueron mayores a los de la presente investigación debido a que hubo una diferencia de 28.5% porque hicieron uso del protocolo IKE SA (IKEv1) y recursos de SD-SA en base a un vpn libre propio.

E. Para el **indicador uso del Disco Duro**, el software libre (ProtonVPN) del sistema operativo Linux - distribución Ubuntu 16.4 no muestra un incremento en el uso del disco duro antes DDoS, con un promedio de estado normal de 1.1 % llegando a tener un estado insignificante de 0.85 % siendo el promedio menor de los softwares seleccionados para la investigación sin afectar al sistema en la lectura y escritura de archivos empleando el software. Estos resultados se ven apoyados con el trabajo de Macías (2017) debido a que recomienda analizar el sistema previamente para identificar anomalías en el sistema y evitar daños irreparables en el disco duro como la perdida de información.

F. La aplicación de los procesos de la metodología MEPVPNS permitió la evaluación de los softwares de redes privadas virtuales en cuanto a la **desempeño en la red**, luego de seguir los términos propuestos en el entorno de pruebas de evaluación de la presente investigación. Es necesario enfatizar que luego de las pruebas en base a los procesos de la metodología MEPVPNS de la variable desempeño en la red, en el **indicador latencia** el software licenciado

(Nordvpn) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 117 ms de 47 ms en un estado normal. Sin embargo, el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 sostuvo el índice más alto en comparación de todos los softwares con un promedio de 326 ms de 47 ms en estado normal. Este trabajo de Fernandez y López (2020) fueron menores a los de la presente investigación, debido a que implementaron un software VPN en un datacenter obteniendo como resultado un incremento en el promedio de la latencia con un registro de 24.06 milisegundos.

G. En el **indicador velocidad de descarga de archivos**, el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 1.82 Mbps de 40.38 Mbps en un estado normal. Además, los resultados arrojaron que el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 16.4 sostuvo el índice más alto en comparación de todos los softwares con un promedio de 38.85 Mbps de 40.38 Mbps en estado normal. Los resultados de Ian (2021) fueron menores a los de la presente investigación debido a las pruebas de estrés-saturación que empleo para el software licenciado (NordVPN) obteniendo como resultado el 60% de la velocidad de descarga del estado normal sin el uso del software.

H. En el **indicador velocidad de subida de archivos**, el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 1.26 Mbps de 16.43 Mbps en un estado normal. Además, los resultados arrojaron que el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 16.4 sostuvo el índice más alto en comparación de todos los softwares con un promedio de 15.70 Mbps de 16.43 Mbps en estado normal. Los resultados de Ian (2021) fueron menores a los de la presente investigación debido a las pruebas de estrés-saturación que empleo para el software licenciado (NordVPN) obteniendo como resultado el 40% de la velocidad de subida del estado normal sin el uso del software.

I. En el **indicador ancho de banda** para descargas de archivos, el software libre (ProtonVPN) del sistema operativo Linux – distribución Ubuntu 16.4 mantuvo el índice más bajo en comparación de todos los softwares con un promedio de 232 KBs de 5169 KBs en un estado normal. Además, los resultados arrojaron que el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 4973 KBs sostuvo el índice más alto en comparación de todos los softwares con un promedio de 5169 KBs en estado normal. Los resultados de Mendoza y Ortega (2019) fueron menores a los de la presente investigación debido a que hubo una comparación de software VPN donde se midió el impacto del ancho de banda mostrando que el software gratuito (TunnelBear) difiere una diferencia menor de 0.44 Mbps en relación a la velocidad de su ISP.

J. En el **indicador filtro y marcado de tráfico**, el software licenciado (NordVPN) en base al sistema operativo Windows 10 muestra un índice mínimo de protocolos ante el encriptamiento de datos con un total de 2 registros de protocolos, tales como: (i)UDP, (ii)NBNS con un porcentaje de 15.38 %. Por otro lado, el software gratuito (TunnelBear) registró 5 protocolos de seguridad de datos en la red (TCP, UDP, SSDP, NBNS y DNS) y 1 protocolo propio de redes privadas virtuales (TLS) sumando a 6 protocolos y obteniendo el índice más alto en las evaluaciones en base al sistema operativo Windows 10 con un porcentaje de 46.15%.

Sin embargo, los resultados de Rodríguez (2020) fueron diferentes a los de la presente investigación debido al uso del software Cacti para evaluar el tráfico de red ante la saturación la transferencia de datos, dando como resultado que tanto la entidad CNT mantiene un promedio mínimo de 41.36%, seguidamente MEGADATOS-NETFILE con un promedio mínimo de 17.48% y finalmente SETEL con un promedio mínimo de 11.25% en cuanto a tráfico de red en base a vpn. Por otro lado, los resultados de Tibaduiza (2015) fueron mayores a los de la presente investigación debido al software Mikrotik cuya función es monitorear el tráfico de paquetes dando como resultado: 0.045% en la transferencia de paquetes de autenticación, asimismo, el 99.955% de paquetes que se transportan por la red mediante los principales protocolos: (a) HTTP y (b) HTTPS. Además, se manifiesta protocolos registrados en las evaluaciones, tales como: (i)TCP, (ii)UDP, (iii)ICMP, (iv)IGMP y (v)GRE.

K. En el **encriptamiento de datos**, el software licenciado (NordVPN) en base al sistema operativo Windows 10 muestra una velocidad mínima de 7.25 KB/s en una red LAN, sin embargo, en una red WAN el software libre (ProtonVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con una velocidad mínima de 0.561 KB/s. Por otro lado, el software libre (ProtonVPN) en base al sistema operativo Windows 10 muestra un índice alto de 7.98 KB/s en una red LAN, sin embargo, en una red WAN el software licenciado (NordVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con un índice alto de 1.863 KB/s. Los resultados de de Velasco, Jiménez y Chafla (2017) fueron mayores a los de la presente investigación debido al uso de una vpn propia para medir la velocidad de encriptamiento en base a algoritmos (AES, TWOFISH, SERPENT), dando como resultados que el algoritmo AES tuvo un índice mayor de velocidad en cuanto a la encriptación por paquetes, tales como: (a)16318.75 KB/s, (b)17645 KB/s, (c)17192.5 KB/s y (d)17332.5 KB/s, respectivamente.

L. En el **desencriptamiento de datos**, el software gratuito (TunnelBear) en base al sistema operativo Linux – distribución Ubuntu 16.4 con una muestra de velocidad mínima de 8.80 KB/s en una red LAN, sin embargo, en una red WAN el software libre (ProtonVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con una velocidad mínima de 0.458 KB/s. Por otro lado, el software libre (ProtonVPN) en base al sistema operativo Windows 10 muestra un índice alto de 10.39 KB/s en una red LAN, sin embargo, en una red WAN el software libre (NordVPN) en base al sistema operativo Linux – distribución Ubuntu 16.4 con un índice alto de 4.977 KB/s. Los resultados de de Velasco, Jiménez y Chafla (2017) fueron mayores a los de la presente investigación debido al uso de una vpn propia para medir la velocidad de desencriptamiento en base a algoritmos (AES, TWOFISH, SERPENT), dando como resultados que el algoritmo AES tuvo un índice mayor de velocidad en cuanto a la desencriptación por paquetes de 1 KB a 100 KB con una velocidad no mayor a 80 MB/s, demostrando que mientras el tamaño se encuentre en el intervalo de 50 MB y 200 MB habrá un incremento exponencial.

M. Para los **indicadores fugas de dirección IP, servidores de DNS y dirección IP por WebRTC**, el software libre (ProtonVPN) del sistema operativo Windows 10 y el software licenciado (NordVPN) del sistema operativo Linux – distribución Ubuntu 16.4 no muestran fugas ante la reconexión de internet en el lapso de 5 minutos. Los resultados de Av Comparatives (2020) fueron diferentes a los de la presente investigación debido a que el tiempo de reconexión al ISP fue menor en un intervalo de 1 minuto; los softwares vpn: (a) Nordvpn, (b) ProtonVPN y (c) TunnelBear no muestran fugas ante las pruebas de Leak Kill-switch, sin embargo, para los softwares gratuitos: (i) Panda Dome VPN y (ii) SaferVPN muestran en sus resultados fugas de servidores DNS y dirección IP.

N. Por último, para el **indicador conexión al servidor VPN**, el software libre (ProtonVPN) del sistema operativo Windows 10 obtuvo una media mayor de conexión con un registro de 12.948 segundos. Sin embargo, el software gratuito (TunnelBear) del sistema operativo Linux – distribución Ubuntu 16.4 obtuvo una media menor de conexión con un registro de 4.284 segundos. Los resultados de Abril y Cuzco (2019) fueron diferentes a los de la presente investigación debido a que el vpn que implementaron cuya funcionalidad fue generar alertas remotas mediante uso de software libres teniendo como resultado que el tiempo de conexión es de 1 minuto y el ancho de banda aceptable es el intervalo de 2 a 2.5 Mbits/s.

O. En síntesis, la aplicación de los procesos de la metodología MEPVPNS permitió determinar la evaluación de rendimiento de los softwares de redes privadas virtuales desarrollado en esta investigación, obteniendo resultados beneficiosos para minimizar el tiempo en la toma de decisiones, de acuerdo con lo indicado en Pacotaype (2018) quien argumenta que la metodología tiene la finalidad de evaluar de manera ordenada y sistematizada el rendimiento de software, hardware, etc. (Torres y Alfaro, 2018).

# VII. RECOMENDACIONES

En esta investigación se ha aplicado la metodología MEPVPNS a softwares de redes privadas virtuales en base sistemas operativos (Windows - Ubuntu) con entorno virtual, sin embargo, hay factores que deben tenerse en cuenta con un grado más de énfasis para realizar mejores evaluaciones a futuro:

A. Evaluar el throughput empleando vpn de servidor modo empresarial con herramientas tecnologías para medir la transferencia de datos entre diferentes puntos de ubicación, es decir, una red WAN, con el objetivo de simular un entorno de comunicación remota.

B. Considerar a los indicadores en la prueba de evaluación, tales como: filtro de IP local a través de WebRTC, filtro de DNS por Torrent, filtro de IP por Torrent y filtro de solicitudes por HTTP para extender el valor de la metodología a las nuevas características funcionales que obtiene los softwares VPN.

C. Recomendar a toda entidad que requiera realizar procesos de suma prioridad y procesos confidenciales de manera segura y privada, realizar un análisis de las características del software VPN para ver tanto: (i) capacidades, (ii) opciones de configuración, (iii) protocolos, (iv) tipo de algoritmos de cifrado, (v)costos, (vi) ubicación de servidores, (vii) sistemas operativos soportados y (viii) soporte.

D. Determinar si el producto (software vpn) en el cual esté interesado de proveer debe tener en cuenta si mantiene opciones nativas ante la reconexión del ISP, denominada: Kill Switch.

E. Recomendar a las pymes o grandes organizaciones que utilicen software licenciados en particular (NordVPN) por tener efectividad ante la reconexión de internet (ISP) de igual modo por no filtrar fugas de dirección IP, servidores de DNS y dirección IP por WebRTC en base al sistema operativo Linux – distribución Ubuntu 16.4 asegurando la información en la entidad de su red Local brindándole la seguridad y privacidad al usuario.

F. Determinar las pruebas de evaluación de rendimiento en base a otros sistemas operativos, tales como: (i) Mac Os, (ii) Solaris, (iii) FreeBSD, entre otros con la finalidad de enriquecer más la información y obtener resultados más amplios en base al rendimiento del software VPN.

G. MEPVPNS deberá mejorar cada vez que se realice cambios en los procesos de la administración tecnológica debido a las actualizaciones en temas técnicos: modo de conexión, protocolos de envió de datos, protocolos de seguridad en la red, protocolos de encriptación y desencriptación, seguridad, rendimiento, realizar procesos más específicos por navegación web segura, etc.; sin embargo, el modelo se conservaría sin cambios trascendentales.

H. Validar la metodología MEPVPNS ampliando sus procesos o desarrollando una nueva para entidades proveedores de medios informáticos: organizaciones de evaluaciones de rendimiento en software y hardware, organizaciones tecnológicas dedicadas a desarrollo de software, etc.

I. Evaluar los criterios de rendimiento en software de redes privadas virtuales en diversas entidades para elegir los más adecuados de acuerdo a las necesidades.
J. Evaluar los criterios de rendimiento mediante herramientas técnicas más sofisticadas en base al sistema operativo de acuerdo a los requerimientos del software, es decir, se requiere obtener resultados más específicos al emplear el software ya sea en una red LAN, WAN, MAN.

K. Evaluar los criterios de rendimiento en base al desempeño en la red en los softwares licenciados debido a que son necesarios para las entidades privadas y de gestión empresarial.

L. Llevar a cabo la comparación de criterios propios de los softwares de redes privadas virtuales a través de la metodología MEPVPNS para permitir al administrador de red o usuario en tener un software de calidad y sofisticado en su sistema (Celulares, PCs).

M. Ampliar el número de navegadores web necesarios para corroborar al indicador pruebas de fugas de dirección IP por WebRTC con la finalidad de obtener más amplios y precisos para la toma de decisión.

N. Recomendar el uso del protocolo UDP para evaluar el rendimiento del software VPN en base a la transferencia de paquetes de datos recibidos y enviados.

O. Recomendar que el sujeto de prueba no debe ser x32 bits, asimismo, la memoria RAM debe tener mínimo 8 GB para soportar ataques DDoS siendo un aspecto técnico a considerar.

# REFERENCIAS

ABELEIRA, José, VÁZQUEZ, Noelio y PEÑA, Carlos. Metodología para favorecer el desempeño investigativo experimental mediante el análisis de videos con tracker. *Revista Boletín Redipe* [En línea]. Julio 2017, vol. 5, n.° 6. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://revista.redipe.org/index.php/1/article/view/82 ISSN: 2266-1536

ABRIL, Bryam y CUZCO, Patricio. Implementación de un sistema de video vigilancia remoto para hogares, utilizando herramientas de software libre. Tesis (Licenciado ingeniería electrónica). Cuenca: Universidad Politécnica Salesiana, 2019.
Disponible en: https://dspace.ups.edu.ec/handle/123456789/17311

ACEBEDO, Manuel, AZNAR, Inmaculada e HINOJO, Francisco. Instrumentos para la Evaluación del Aprendizaje Basado en Competencias: Estudio de caso. *Información tecnológica* [En línea]. 2017, vol. 28, n.° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.scielo.cl/scielo.php?pid=S0718-07642017000300012&script=sci_arttext&tlng=en
ISSN: 0718-0764

ACOSTA, Néstor, ESPINEL, Luis y GARCÍA Jaime. Estándares para la calidad de software. *TIA Tecnología, investigación y academia* [En línea]. Junio 2017, vol. 5, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://go.gale.com/ps/i.do?id=GALE%7CA568009251&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=23448288&p=IFME&sw=w&userGroupName=anon%7E916fd41c

ADEWALE, Adeyinka, ADAGUNODO, Emmanuel, JOHN, Samuel y NDUJIUBA, Charles. Effect of Increasing Buffer Size on Prioritized Guard Channels with Queue during Call Traffic Congestion. [Efecto del aumento del tamaño del búfer en los canales de protección priorizados con cola durante la congestión del tráfico de llamadas]. *2016 International Conference on Computational Science*

*and Computational Intelligence (CSCI)* [En línea]. 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7881494

AGAH, Seyed. IDS for VPN. *Helix* [En línea]. Abril 2017, vol. 7, n.° 4. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://helix.dnares.in/wp-content/uploads/2017/12/02_Helix_1594-1605.pdf ISSN: 1594-1605

AGUIRRE, Victor. Cloud Computing de modo privado para ofrecer infraestructura como servicio bajo software libre a los estudiantes de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte. Tesis (Licenciado en ingeniería en electrónica y redes de comunicación). Ibarra: Universidad Técnica del Norte, 2016.
Disponible en: http://repositorio.utn.edu.ec/handle/123456789/5345

AL-FANNAH, Nasser, One leak will sink a ship: WebRTC IP address leaks. [Una fuga hundirá un barco: fugas de direcciones IP de WebRTC]. *2017 International Carnahan Conference on Security Technology (ICCST)* [En línea]. Diciembre 2017, vol. 1, n. ° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8167801

ALVA, Jorge y DOMÍNGUEZ, Luz. Clima organizacional y satisfacción laboral en los trabajadores de la universidad san pedro de Chimbote, 2013. *In Crescendo* [En línea]. Junio 2015, vol. 6, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://revistas.uladech.edu.pe/index.php/increscendo/article/view/818.
ISSN: 2307-5260

AMORIM, Rafhael, KOVACS, Istvan, WIGARD, Jeroen, POCOVI, Guillermo, SORENSEN, Troels y MOGENSEN, Preben. Improving Drone's Command and Control Link Reliability through Dual-Network Connectivity. *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)* [En línea]. Junio 2019, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].

Disponible en: https://ieeexplore.ieee.org/abstract/document/8746579

ANDREADIS, Alessandro, RIZZUTO, Sandro y ZAMBON, Riccardo. A cross-layer jitter-based TCP for wireless networks. *EURASIP Journal on Wireless Communications and Networking* [En línea]. Agosto 2016, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-016-0695-0

APOLO, Cristhian; CORAL, Yuliana. Análisis y simulación de tráfico de la red de datos de las Fuerzas Armadas con tecnologías MPLS. Tesis (Titulo para ingeniero electrónico). Quito: Universidad Politécnica Salesiana, 2017. Disponible en: https://dspace.ups.edu.ec/handle/123456789/14289

ARIZA, Edwin y VARGAS, Kevin. Ajuste de políticas de QoS para plataformas de voz, video y aplicaciones compartidas del Banco de Occidente. Tesis (Especialización en Teleinformática). Bogotá: Universidad Distrital Francisco José de Caldas, 2020.
Disponible en: https://repository.udistrital.edu.co/handle/11349/23775

AUNG, Si y THEIN, Thandar. Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks. [Análisis comparativo de redes privadas virtuales de capa 2 de sitio a sitio]. *2020 IEEE Conference on Computer Applications (ICCA)* [En línea]. Marzo 2020, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/9022848

AV Comparatives. VPN Report 2020 – 35 Services. 21 de mayo de 2020. Disponible en: https://www.av-comparatives.org/tests/vpn-report-2020-35-services/

BALLADARES, Jorge. Parámetros de calidad del servicio de acceso a internet en redes convergentes y construcción 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 internet para la

coordinación zonal 4 de la Agencia de Regulación y Control de las Telecomunicaciones. Tesis (Título de magister en redes de comunicaciones). Quito: Pontificia Universidad Católica del Ecuador, 2017.
Disponible en: http://repositorio.puce.edu.ec/handle/22000/13490

BASILE, Cataldo, VALENZA, Fulvio, LIOY, Antonio, LOPEZ, Diego y PERALES, Antonio. Adding Support for Automatic Enforcement of Security Policies in NFV Networks [Adición de soporte para la aplicación automática de políticas de seguridad en redes NFV]. *IEEE/ACM Transactions on Networking* [En línea]. Febrero 2019, vol. 27, n.° 2. [Fecha de consulta: 31 de octubre de 2020]. Disponible en: https://ieeexplore.ieee.org/abstract/document/8637976

BELLIDO, Luis, LÓPEZ, Jorge, GONZÁLEZ, Francisco y LÓPEZ, David. Metodología para la Evaluación de Servicios de Telecomunicación desde la Perspectiva del Usuario. *In Barcelona: Fifth International Workshop on Quality of future Internet Services* [En línea]. 2004, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://web.dit.upm.es/~jlopez/publicaciones/telecomid04lbt.pdf

BHALERAO, Jaydeep, PAL, Biswajyoti y CHATTERJEE, Manish. Mitigation of WebRTC attacks using a network edge system. [Mitigación de los ataques WebRTC utilizando un sistema de borde de red]. U.S., 10.630.717 (21.04.2020). [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://patentimages.storage.googleapis.com/be/c6/80/638e01e8a17f9e/US201 60 337395A1.pdf

BISWAS, Rajorshi y WU, Jie. Filter Assignment Policy against Distributed Denialof-Service Attack. [Política de asignación de filtro contra ataque de denegación de servicio distribuido]. *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)* [En línea]. Febrero 2019, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8644584

BRAVO, Liseth. Modelo diagnóstico y análisis de la red Lan para la mejora del rendimiento y seguridad en la red de salud Valle del Mantaro mediante la metodología Cisco. Tesis (Licenciado en ingeniería de sistemas). Huancayo: Universidad nacional del centro del Perú, 2015.
Disponible en: https://repositorio.uncp.edu.pe/handle/20.500.12894/1460

BUCȘĂ, Radu. Teleworking and Securing Data with VPN Technology. [Teletrabajo y protección de datos con tecnología VPN]. *Economy Transdisciplinarity Cognition* [En línea]. 2020, vol. 23, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://www.ugb.ro/Downloads/Info%20Studenti/20192020/etc2020no1/12_Bucsa.pdf

CAMACHO, Nicolás. Sistema de prevención de intrusos (IPS) para un entorno de red SDN. Tesis (Título de ingeniero electrónico). Bogotá: Pontificia Universidad Javeriana, 2016.
Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6265

CAPROLU, Maurantonio, RAPONI, Simone, OLIGERI, Gabriele y DI PIETRO, Roberto. Cryptomining Makes Noise: A Machine Learning Approach for Cryptojacking Detection. [Cryptomining hace ruido: un enfoque de aprendizaje automático para la detección de Cryptojacking]. *ArXiv* [En línea]. Mayo 2019, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ui.adsabs.harvard.edu/abs/2019arXiv191009272C/abstract

CAPUÑAY, Denys. Análisis comparativo de algoritmos criptográficos para redes privadas virtuales. Tesis (Licenciado en Ingeniería de sistemas). Chiclayo: Universidad Señor de Sipán, 2016.
Disponible en: http://repositorio.uss.edu.pe/handle/uss/2696

CARRIÓN, Gilberto. Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas. Tesis (Doctorado para ciencias de la computación y sistemas) Pimentel: Universidad Señor de Sipán, 2018.
Disponible en: http://repositorio.uss.edu.pe/handle/uss/4723

CARVAJAL, Carlos. La encriptación de datos empresariales: ventajas y desventajas. *Recimundo* [En línea]. 2019, vol. 3, n.° 2. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://salowi.com/~recimund/index.php/es/article/view/487

CHAPPA, Marco. Implementación de una nueva tecnología para mejorar la productividad de una empresa metalúrgica, Lima – 2018. Tesis (Licenciado en ingeniería industrial y de gestión empresarial) Lima: Universidad Norbert Wiener, 2018.
Disponible en: http://repositorio.uwiener.edu.pe/handle/123456789/2072

CHAUCA, Jose. Implementación de calidad de servicio en redes inalámbricas de área local, para la optimización del servicio de telefonía IP en Smart Phones con cliente SIP. Tesis (Maestría en redes de comunicaciones) Quito: Pontifica Universidad Católica del Ecuador, 2016.
Disponible en: http://repositorio.puce.edu.ec/bitstream/handle/22000/11291/Caso%20de%20estudio%20QOS-WLAN.pdf?sequence=1&isAllowed=y

CHILCAÑÁN, David, NAVAS, Patricio y ESCOBAR, Milton. Expert system for remote process automation in multiplatform servers, through human machine conversation. [Sistema Experto para la Automatización de Procesos Remotos en Servidores Multiplataforma, Mediante la Conversación Hombre Máquina]. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI* [En Línea]. Julio 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7975913

CISCO. Aspectos básicos sobre la conectividad de red: qué tiene que saber. 31 de mayo de 2019.
Disponible en: https://www.cisco.com/c/es_es/solutions/small-business/resource-center/networking/networking-basics.html

CNN. Nuestro tráfico de internet aumentó con la cuarentena: ¿puede la red aguantarlo?. CNN. 1 de abril de 2020.
Disponible en: https://cnnespanol.cnn.com/video/incremento-trafico-internet-coronavirus-cuarentenas-pandemia-covid-19-pkg-seg-michael-roa/

CONCYTEC. Proyectos de investigación básica y aplicada. 2017-2. 25 de Julio del 2017.
Disponible en: https://fondecyt.gob.pe/convocatorias/investigacion-cientifica/proyectos-de-investigacion-basica-y-aplicada-2017-02

Cyber. ORR Jeff Enterprise Cyber Security Trends and Predictions 2020. 27 de noviembre de 2019.
Disponible en: https://www.cshub.com/executive-decisions/reports/enterprise-cyber-security-trends-and-predictions-2020?ty-ur

DE LA ROSA, Javier. Ciberseguridad para pymes. Tesis (Licenciado en comercio) Valladolid: Universidad de Valladolid, 2019.
Disponible en: https://core.ac.uk/download/pdf/250406325.pdf

DE LIMA, Bárbara, CHAVES, Marina, MEYER, Marília, LANCMAN, Selma y BARROSO, Víctor. A Saúde do trabalhador em tempos de covid-19: reflexões sobre saúde, segurança e terapia ocupacional. [Salud del trabajador en tiempos covid-19: reflexiones sobre salud, seguridad y terapia ocupacional]. *Cadernos Brasileiros de Terapia Ocupacional* [En línea]. Septiembre 2020, vol. 28, n. ° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.cadernosdeterapiaocupacional.ufscar.br/index.php/cadernos/article/view/2766

DONG, Miaomiao y KIM, Taejoon. Reliability of an Urban Millimeter Wave Communication Link with First-Order Reflections. [Fiabilidad de un enlace de comunicación de ondas milimétricas urbanas con reflejos de primer orden]. *2016 IEEE Global Communications Conference (GLOBECOM)* [En línea]. Febrero 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/document/7842213

DUEÑAS, Jonathan y BERNAL, Christian. Implementación de un sistema de prevención de intrusos en la VLAN de servidores de la empresa Sonda de Colombia S.A. Tesis (Especialización en Seguridad Informática). Bogotá: Universidad Piloto De Colombia, 2019.
Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6265

DUTKOWSKA, Agnieszka, HOUNSEL, Austin, XIONG, Andre, ROBERTS, Molly, STEWART, Brandon, CHETTY, Marshini y FEAMSTER, Nick. (2020). Understanding How and Why University Students Use Virtual Private Networks. [Comprender cómo y por qué los estudiantes universitarios usan redes privadas virtuales]. *arXiv preprint arXiv:2002.11834* [en línea]. Febrero 2020, vol. 1, n° 4. [Fecha de consulta: 29 de octubre de 2020].
Disponible en: https://arxiv.org/abs/2002.11834

EXPRESSVPN. Herramientas de seguridad de ExpressVPN. Prueba de fugas de DNS. 11 de noviembre de 2015.
Disponible en: https://www.expressvpn.com/es/dns-leak-test

EXPRESSVPN. Protocolos VPN: L2TP/IPsec. 2020.
Disponible en: https://www.expressvpn.com/es/what-is-vpn/protocols/l2tp

EZELL, Joel y YOAKUM, John. Providing web real-time communications (WebRTC) media services via WebRTC-enabled media servers, and related methods, systems, and computer-readable media [Proporcionar servicios de medios de comunicaciones web en tiempo real (WebRTC) a través de servidores de medios habilitados para WebRTC y métodos, sistemas y medios legibles por

computadora relacionados]. U.S., 10.581.927 (03.03.2020). [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://patents.google.com/patent/US10581927B2/en

FAKIS, Alexandros, KAROPOULOS, Georgios y KAMBOURAKIS, Georgios. Neither Denied nor Exposed: Fixing WebRTC Privacy Leaks. [Ni denegado ni expuesto: corrigiendo las fugas de privacidad de WebRTC]. *Future Internet* [En línea]. Mayo 2020, vol. 12, n.° 5. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.mdpi.com/1999-5903/12/5/92/htm

FANG, Fang y CHEN, Yuanyuan. A new approach for credit scoring by directly maximizing the Kolmogorov–Smirnov statistic. [Un nuevo enfoque para la calificación crediticia mediante la maximización directa de la estadística de Kolmogorov-Smirnov]. *Computational Statistics & Data Analysis* [En línea]. Mayo 2019, vol. 133, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S0167947318302494

FARÍAS, Jessica y YÉPEZ, Oscar. Diseño de un sistema de detección de intrusos usando SNORT a través del análisis de tráfico en tiempo real y el análisis de protocolos. Tesis (Ingeniero En Networking Y Telecomunicaciones). Guayaquil: Universidad de Guayaquil, 2022.
Disponible en: http://repositorio.ug.edu.ec/handle/redug/59777

FERNANDEZ, Byron y LÓPEZ, Jonnathan. Metodología para el despliegue de un datacenter definido por software.Tesis (Metodología para el despliegue de un datacenter definido por software). Cuenca: Universidad Politécnica Salesiana Sede Cuenca, 2020.
Disponible en: https://dspace.ups.edu.ec/handle/123456789/18870

FILEMAKER. Especialistas de FileMaker. Descifrar un archivo. Enero de 2017. Disponible en: https://fmhelp.filemaker.com/help/18/fmp/es/index.html#page/FMP_Help/decryptin g-files.html

FLOREA, Lulia, RUGHINIS, Razvan, RUSE, Laura y DAN, Dragomir. Survey of Standardized Protocols for the Internet of Things [Encuesta de Protocolos Estandarizados para el Internet de las Cosas]. *2017 21st International Conference on Control Systems and Computer Science (CSCS)* [En línea]. Julio 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7968561

FLORES, Eric, MIRANDA, María y VILLASÍS, Miguel. El protocolo de investigación VI: cómo elegir la prueba estadística adecuada. Estadística inferencial. *Revista Alergia México* [En línea]. Setiembre 2017, vol. 64, n.° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-91902017000300364

FUJIKI, Daichi, ISHII, Kiyo, FUJIWARA, Ikki, MATSUTANI, Hiroki, AMANO, Hideharu, CASANOVA, Henri y KOIBUCHI, Michihiro. High-Bandwidth Low-Latency Approximate Interconnection Networks. [Redes de interconexión aproximada de baja latencia y gran ancho de banda]. *2017 IEEE International Symposium on High Performance Computer Architecture (HPCA)* [En línea]. Mayo 2017, vol. 1, n. ° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7920848

GAI, Silvano y MCCLOGHRIE, Keith. Method and apparatus for defining and implementing high-level quality of service policies in computer networks [Método y aparato para definir e implementar políticas de calidad de servicio de alto nivel en redes informáticas]. U.S. 6.167.445 (26.12.2007). [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://patents.google.com/patent/US7185073B1/en

GALLARDO, Rafael. El Aprendizaje-Servicio como una estrategia inclusiva para superar las barreras al aprendizaje ya la participación. *Revista de Educación Inclusiva* [En línea]. 2017, vol. 5, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://revistaeducacioninclusiva.es/index.php/REI/article/view/222

GALLEGOS, Joan y MAYORGA, Tannia. Automatización de procesos en redes de datos mediante programación en Python [En línea]. 1. ª ed. Colombia: REDIPE, 2019 [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://fdocuments.ec/document/isbn-978-1-951198-25-1-enrique-vinicio-carrera-universidad-de-las-fuerzas-armadas.html?page=15.
ISBN: 978-1-951198-25-1

GARCÍA, Alexander, ESCOBAR, Lina, NAVARRO, Andrés y VÁSQUEZ, Andrés. Evaluation and selection method of network simulation tools [Método de evaluación y selección de herramientas de simulación de redes]. *Sistemas y Telemática* [En línea]. 2011, vol. 9, n.° 16. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/view/1029

GERALDO, Luis, SORIA, Juan y TITO, Pedro. Modelo SEM basado en valores organizacionales y capital intelectual: un estudio realizado en entidades del sistema financiero peruano. *RETOS. Revista de Ciencias de la Administración y Economía* [En línea]. Marzo 2020, vol. 10, n.° 19. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-86182020000100005&script=sci_arttext

GÓMEZ, Aída. Elaboración del guion instruccional mediante la herramienta didáctica del recurso educativo digital. *Via inveniendi et iudicandi* [En línea]. 2017, vol. 12, n.° 2. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.redalyc.org/journal/5602/560259695002/560259695002.pdf

GORDILLO, Sandra. Fuga de información la mayor amenaza para la imagen corporativa. Tesis (Especializada en administración de la seguridad). Bogotá: Universidad Militar Nueva Granada, 2017.
Disponible en: https://repository.unimilitar.edu.co/handle/10654/16649

GUIMAREY, Ruth. Comparativa, análisis y estudio de rendimiento en plataformas de sistemas WebRTC. Tesis (Licenciada en ingeniería de tecnologías de telecomunicación). Vigo: Universidad de Vigo, 2017.
Disponible en: http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/73/TFG_Ruth_Guimarey_Docampo.pdf?sequence=1

GUNLEIFSEN, Håkon, KEMMERICH, Thomas y GKIOULOS, Vasileios. Dynamic setup of IPsec VPNs in service function chaining. [Configuración dinámica de VPN de IPsec en el encadenamiento de funciones de servicio]. *Computer Networks* [En línea]. Septiembre 2019, vol. 160, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1389128619300969

HAGOPIAN, Hrayr. Experimentos en una ciencia no experimental. *Investigación económica* [En línea]. Marzo 2016, vol. 75, n°. 295. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.sciencedirect.com/science/article/pii/S0185166716300029

HAUSER, Frederik, HÄBERLE, Marco, SCHMIDT, Mark y MENTH, Michael. P4-IPsec: Site-to-Site and Host-to-Site VPN with IPsec in P4-Based SDN [P4-IPsec: VPN de sitio a sitio y de host a sitio con IPsec en SDN basado en P4]. *IEEE Access* [En línea]. Julio 2020, vol. 8, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/document/9151942

HENTGES, Ramón y SCHORR, María. Monitoramento de redes de computadores utilizando o protocolo SNMP. *Revista Destaques Acadêmicos* [En línea]. 2020, vol. 13, n.° 4. [Fecha de consulta: 31 de octubre de 2020]. Disponible en: http://www.univates.br/revistas/index.php/destaques/article/view/3037

HERNÁNDEZ, Roberto y MENDOZA, Christian. Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta [En línea]. 1.ª ed. Ciudad de México, México: McGRAW-HILL INTERAMERICANA EDITORES, S.A., 2018 [Fecha de consulta: 31 de octubre de 2020].
ISBN: 978-1-4562-6096-5

HONG, Cheol, LEE, Kyungwoon, KANG, Minko e YOO, Chuck. qCon: QoS-Aware network resource management for fog computing. [qCon: gestión de recursos de red QoS-Aware para la computación en niebla]. *Sensors* [En línea]. Agosto 2018, vol. 18, n.° 10. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.mdpi.com/1424-8220/18/10/3444

HOSTGATOR. Los especialistas de Hostgator. Direcciones IP: para qué sirven y cómo funcionan. 16 de septiembre de 2019.
Disponible en: https://www.hostgator.mx/blog/que-es-una-direccion-ip/

HURTADO, Wilmer y PONCE, Sergio. Estudio del comportamiento de vulnerabilidades de una red privada virtual (VPN). Tesis (Licenciatura de Ingeniero en Telecomunicaciones). Caracas: Universidad Católica Andrés Bello, 2013.

Disponible en: http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAT0210.pdf

IAN, Paul. NordVPN review: Fast and feature-packed. [Revisión de NordVPN: rápido y repleto de funciones]. PCWorld. 30 de octubre 2021. Disponible en: https://www.pcworld.co.nz/review/nordvpn/vpn/693563/

IBM. VPN y filtrado IP. 14 de abril de 2021. Disponible en:https://www.ibm.com/docs/es/i/7.2?topic=concepts-vpn-ip-filtering

ISO. Especialistas de ISO. Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs). [Tecnología de la información. Técnicas de seguridad. Seguridad de la red. Parte 5: Protección de las comunicaciones a través de redes mediante redes privadas virtuales (VPN)]. Agosto de 2019. Disponible en: https://www.iso.org/standard/51584.html ISSN: 2344- 8288

JAHAN, Sohely, RAHMAN, Md y SAHA, Sajeeb. Application specific tunneling protocol selection for Virtual Private Networks. [Selección de protocolo de tunelización específico de la aplicación para redes privadas virtuales]. *2017 International Conference on Networking, Systems and Security (NSysS)* [En línea]. Marzo 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020]. Disponible en: https://ieeexplore.ieee.org/abstract/document/7885799

JANAMPA, Hubner, HUAMANI, Hayde y MENESES, Yudith. Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. *Revista Cubana de Ciencias Informáticas* [En línea]. 2021, vol. 15, n.° 3. [Fecha de consulta: 31 de octubre de 2020].

Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000300055

JANGID, Manoj y TRIVEDI, Prakriti. Improve Performance of Successive Ratio for Virtual Private Network. [Mejorar el rendimiento de la proporción sucesiva para la red privada virtual]. *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)* [En línea]. Octubre 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8082614

JATI, Grafika, HARTADI, Budi, PUTRA, Akmal, NURUL, Fahri, IQBAL, Riza y YAZID, Setiadi. Design DDoS Attack Detector using NTOPNG. [Diseño de un detector de ataques DDoS usando NTOPNG]. *2016 International Workshop on Big Data and Information Security (IWBIS)* [En línea]. Octubre 2016, vol. 1, n°1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7872903

JINGYAO, Sun, CHANDEL, Sonali, YUNNAN, Yu, JINGJI, Zang y ZHIPENG, Zhang. Securing a Network: How Effective Using Firewalls and VPNs Are? [Asegurar una red: ¿Qué tan efectivos son los firewalls y las VPN?]. *Advances in Information and Communication* [En línea]. Febrero 2019, vol. 70, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://link.springer.com/chapter/10.1007/978-3-030-12385-7_71

JONES, Joshua, WIMMER, Hayden y HADDAD, Rami. PPTP VPN: An Analysis of the Effects of a DDoS Attack. [PPTP VPN: análisis de los efectos de un ataque DDoS]. *2019 SoutheastCon* [En línea]. Marzo 2020, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/9020514

JUMA, Mazen, MONEM, Azza y SHAALAN, Khaled. Hybrid End-to-End VPN Security Approach for Smart IoT Objects. [Enfoque de seguridad VPN de extremo a extremo híbrido para objetos de IoT inteligentes]. *Journal of Network and Computer Applications* [En línea]. Mayo 2020, vol. 158, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1084804520300722

KATZ, Raúl, JUNG, Juan y CALLORDA, Fernando. El estado de la digitalización de América Latina frente a la pandemia del COVID-19. *SCIOTECA Espacio de conocimiento abierto* [En línea]. Abril 2020, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://scioteca.caf.com/handle/123456789/1540

KHAN, Mohammad, DEBLASIO, Joe, VOELKER, Geoffrey, SNOEREN, Alex, KANICH, Chris y VALLINA, Narseo. An Empirical Analysis of the Commercial VPN Ecosystem. [Un análisis empírico del ecosistema vpn comercial]. *ACM Digital library* [En línea]. Octubre 2018, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://dl.acm.org/doi/abs/10.1145/3278532.3278570

KUMAR V. y MAJEED K. E-resources sharing through Linux based Virtual Private Network (VPN): a case study. [Uso compartido de recursos electrónicos a través de la red privada virtual (VPN) basada en Linux: un estudio de caso]. *Annals of Library and Information Studies (ALIS)* [En Línea]. 2018, vol. 65, n. ° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://14.139.47.23/index.php/ALIS/article/view/19651

LAWAS, Jay, VIVERO, Allan y SHARMA, Ankit. Network performance evaluation of VPN protocols (SSTP and IKEv2). [Evaluación del rendimiento de la red de protocolos VPN (SSTP e IKEv2)]. *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)* [En línea]. Diciembre 2016, vol. 65, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7759880

LEÓN, Alejandro. Monitoreo de rendimiento para la seguridad de VPN a través de PfSense y OpenVPN. Tesis (Maestro en telemática). Xalapa: Universidad Veracruzana, 2018.
Disponible en: https://cdigital.uv.mx/handle/123456789/48648

LEYVA, Olia y GARCÍA, Milton (2020). Análisis y caracterización de conjuntos de datos para detección de intrusiones. *Serie Científica de la Universidad de las Ciencias Informáticas* [En línea]. 2020, vol. 13, n.° 4. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://publicaciones.uci.cu/index.php/serie/article/view/558

LI, Tania y TAKAKUWA, Rita. Análisis de confiabilidad y validez de un instrumento de medición de la sociedad del conocimiento y su dependencia en las tecnologías de la información y comunicación. *Revista de Iniciación Científica* [En línea]. 2016, vol. 2, n. °2. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://revistas.utp.ac.pa/index.php/ric/article/view/1249/1412

LI, Xi, CASELLAS, Ramon, LANDI, Giada, DE LA OLIVA, Antonio, COSTA, Xavier, GARCIA, Andres, DEISS, Thomas y VILALTA, Ricard. 5G-Crosshaul Network Slicing: Enabling Multi-Tenancy in Mobile Transport Networks. [Slicing de red 5G-Crosshaul: habilitación de la tenencia múltiple en redes de transporte móvil]. *IEEE Communications Magazine* [En línea]. 2017, vol. 55, n. °8. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8004167

LIPP, Benjamin, BLANCHET, Bruno y BHARGAVAN, Karthikeyan. A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol. [Una prueba criptográfica mecanizada del protocolo de red privada virtual WireGuard]. *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* [En línea]. 2019, vol. 1 n. °1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8806752

LÓPEZ, Gustavo y GRAMPÍN, Eduardo. Scalability testing of legacy MPLS-based Virtual Private Networks. [Pruebas de escalabilidad de redes privadas virtuales heredadas basadas en MPLS]. *2017 IEEE URUCON* [En línea]. 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/document/8171874

LUCENA, Carlos. OPENWEBINARS: Qué es una prueba de rendimiento de Software. 14 de junio de 2019.
Disponible en: https://openwebinars.net/blog/que-es-prueba-de-rendimiento-software/

MACÍAS, Luis. Implementación de un módulo basado en el estándar 802.11 n para prácticas en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes. Tesis (Titulo para Ingeniero En Computación Y Redes). Jipijapa: Universidad Estatal Del Sur De Manabí, 2017.
Disponible en: http://repositorio.unesum.edu.ec/handle/53000/991

MACWORLD. Basic Security Tips You Can Use to Protect Your Mac. [Consejos básicos de seguridad que puede usar para proteger su Mac]. Mayo del 2020.
Disponible en:https://es.scribd.com/document/462689547/Basic-Security-Tips-to-Protect-Your-Mac

MARQUÉS, Guillermo, IPsec y redes privadas virtuales [En línea]. 1. ª ed. Editorial Lulu, 2016.
ISBN: 9781329824195

MARTEL, Víctor. Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764. Tesis (Licenciado en ingeniería de redes y comunicaciones) Lima: Universidad Peruana de Ciencias Aplicadas, 2019.
Disponible en: https://repositorioacademico.upc.edu.pe/handle/10757/625693

MARTINASEK, Zdenek, BLAZEK, Petr, SILHAVY Pavel y SMEKAL, David. Methodology for correlations discovery in security logs. [Metodología para el descubrimiento de correlaciones en los registros de seguridad*]. Ninth International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT)* [En línea]. 2017, vol. 11 n. °19. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8255194

MEDINA, Jhonatan y RIVAS, Yonathan. Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos. Tesis (Título Profesional de Ingeniero de Sistemas). Lambayeque: Universidad Nacional “Pedro Ruiz Gallo”, 2020.
Disponible en: https://repositorio.unprg.edu.pe/handle/20.500.12893/8074

MÉNDEZ, Miguel. Análisis de nuevas variantes de Ransomwares. XIV Seminario Iberoamericano de Seguridad en las Tecnologías de la Información [En línea]. 2020, vol. 1 n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://www.informaticahabana.cu/sites/default/files/ponencia-2020/SEG04.pdf

MENDOZA, Freddy y ORTEGA, Adrián. Análisis de software en la implementación de VPN en LAN Inalámbrica. Tesis (Titulo para ingeniero en sistemas). Ecuador: Universidad Estatal de Milagro, 2019.

MERCADO, Luis y ORTIZ, Daniel. Evaluación de la calidad de enlaces de telecomunicaciones a través de herramientas de estimación del ancho de banda disponible en redes de computadores heterogéneas. Tesis (Licenciado en Ingeniería de Sistemas). Barranquilla: Universidad de la Costa (CUC), 2020.
Disponible en: https://repositorio.cuc.edu.co/handle/11323/7080

MICROSOFT. Especialistas de Microsoft. Descifrar datos. 30 de marzo de 2017.
Disponible en: https://docs.microsoft.com/eses/dotnet/standard/security/decrypting-data

MONTENEGRO, Juan. La calidad en la docencia universitaria. Una aproximación desde la percepción de los estudiantes. *Educación* [En línea]. 2020, vol. 29, n.° 56. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1019-94032020000100116

MOREANO, Roberto. Metodología para evaluar la Calidad de Servicio de las Telecomunicaciones. *Jornadas de Ingeniería Eléctrica y Electrónica (FIEE)* [En línea]. Noviembre 2010, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020]. Disponible en: https://bibdigital.epn.edu.ec/handle/15000/3730

MORENO, Carmen y SEPÚLVEDA, Luz. Conocimientos y prácticas en anticoncepción de los estudiantes de medicina y enfermería de Manizales, Colombia 2015. *Revista chilena de obstetricia y ginecología* [En línea]. Junio 2017, vol. 82, n.° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.scielo.cl/scielo.php?pid=S0717-75262017000300259&script=sci_arttext

MOSTACERO, Nick. Controles y mecanismo en la gestión de seguridad de red basado en Sistemas de Detección de intrusos: Una revisión sistemática de la literatura. Tesis (Bachiller en Ingeniería de Sistemas). Lima: Universidad Peruana Unión, 2020.
Disponible en: https://repositorio.upeu.edu.pe/handle/20.500.12840/3443

NARAYAN, Shaneel, ISHRAR, Salman, KUMAR, Avinesh, GUPTA, Ruchinav y KHAN, Ziafil. Performance analysis of 4to6 and 6to4 transition mechanisms over point to point and IPSec VPN protocols [Análisis de rendimiento de los mecanismos de transición 4to6 y 6to4 sobre protocolos VPN punto a punto e IPSec]. *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)* [En línea]. Diciembre 2016, vol. 1, n. °1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7759027

NARAYAN, Shaneel, WILLIAMS, Cameron, HART, Daniel y QUALTROUGHT, Max. Network performance comparison of VPN protocols on wired and wireless networks. [Comparación del rendimiento de la red de protocolos VPN en redes alámbricas e inalámbricas]. *2015 International Conference on Computer Communication and Informatics (ICCCI)* [En línea]. Agosto 2015, vol. 1, n. °1. [Fecha de consulta: 29 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7218077

NETSPOTAPP. Especialistas de Netspotapp. Las mejores maneras de ocultar mi dirección IP. 10 de marzo de 2020.
Disponible en: https://www.netspotapp.com/es/hide-my-ip.html

NICO, Rino. Secure Portable Virtual Private Network with Rabbit Stream Cipher Algorithm. [Red privada virtual portátil segura con algoritmo de cifrado Rabbit Stream]. *Procedia Computer Science* [En línea]. 2018, vol. 135, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050918314625

NURHAIDA, Ida, PUTRA, Dimas, ZEN, Remmy y WEI, Hong. Interior gateway protocol routing performance comparison of the virtual private network based on multi-protocol label switching and direct-link backupsed on mpls and direct-link backup. [Comparación de rendimiento de enrutamiento de protocolo de puerta de enlace interior de la red privada virtual basada en conmutación de etiquetas multiprotocolo y respaldo de enlace directo en mpls y respaldo de enlace directo]. *Sinergi* [En línea]. Febrero 2020, vol. 24, n. °1. [Fecha de consulta: 29 de octubre de 2020].
Disponible en: https://sinergi.mercubuana.ac.id/publications/297892/interior-gateway-protocol-routing-performance-comparison-of-the-virtual-private24

OÑA, Diego. Análisis e implementación de una red privada virtual VPN con túneles de seguridad en el transporte de datos con un servidor Centos Linux: caso práctico: propuesta de implementación en la unidad de admisión y nivelación de la Universidad Técnica de Cotopaxi. Tesis (Licencia de ingeniero en informática y sistemas computacionales). Latacunga: Universidad Técnica de Cotopaxi, 2016.
Disponible en: http://repositorio.utc.edu.ec/handle/27000/3671

ORAMAS, Guillermo. Importancia de los conocimientos básicos de las tecnologías web en los graduandos de ing. de sistemas. *Revista CECAVI* [En línea]. Enero 2020, vol. 8, n.° 2. [Fecha de consulta: 29 de octubre de 2020].
Disponible en: http://revistas.uam.edu.pa/index.php/revistacecavi/article/view/30

OVALLE, Anggie. Uso de herramientas informáticas para descubrir vulnerabilidades en las redes wifi domésticas. Tesis (Licencia de especialista en seguridad de la información). Bogotá: Universidad Católica de Colombia, 2019.
Disponible en: https://repository.ucatolica.edu.co/handle/10983/24062

PACOTAYPE, Rogelio. Metodología integral para evaluar el rendimiento de firewalls. Tesis (Licencia de ingeniero de sistemas). Lima: Universidad Cesar Vallejo, 2018.
Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/38180

PAESSLER. Especialistas de Paessler. Ancho de banda. Publicado el 16 de octubre de 2015.
Disponible en: https://www.es.paessler.com/itexplained/bandwidth

PANDASECURITY. Especialistas de Pandasecurity. Son seguras las VPNs. Publicado el 3 de abril de 2017.
Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/son-seguras-lasvpns/

PCMAG. Los especialistas de Pcmag. The Best Free VPNs for 2020. [Las mejores VPN gratuitas para 2020]. 5 de octubre de 2020.
Disponible en: https://www.pcmag.com/picks/the-best-free-vpns

PÉREZ, Pablo. Estudio de ataques DDoS basados en DNS. Tesis (Licencia de ingeniero en tecnologías de telecomunicación) Madrid: Universidad Carlos III de Madrid, 2017.
Disponible en: https://e-archivo.uc3m.es/handle/10016/27876

PHELAN, David. Slipping under the Net [Deslizándose bajo la red]. *Business Traveler* [En línea]. 2019, vol. 1, n.° 1. [Fecha de consulta: 29 de octubre de 2020].
Disponible en: https://www.businesstravelerusa-digital.com/articles/slipping-under-the-net?m=66059&i=700506&p=38&ver=html5

PONS, Vicente. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Seguridad Ciudadana* [En línea]. 2017, vol. 20, n.° 1. [Fecha de consulta: 28 de octubre].
Disponible en: https://revistas.flacsoandes.edu.ec/urvio/article/view/2563

POSADA, Gabriel. Elementos básicos de estadística descriptiva para el análisis de datos [En línea]. 1. ª ed. Medellín: Fondo Editorial Luis Amigó, 2016 [Fecha de consulta: 30 de octubre de 2020].
Disponible en: https://www.funlam.edu.co/uploads/fondoeditorial/120_Ebook-elementos_basicos.pdf
ISBN: 978-958-8943-05-3

PUDELKO, Maximilian, EMMERICH, Paul, GALLENMÜLLER, Sebastian, CARLE, Georg. Performance analysis of VPN gateways. [Análisis de rendimiento de puertas de enlace VPN]. *2020 IFIP Networking Conference (Networking*) [En línea]. 2020, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/9142755

PULIDO, Marta. Ceremonial y protocolo: métodos y técnicas de investigación científica. *Opción* [En línea]. 2015, vol. 31, n.° 1. [Fecha de consulta: 30 de octubre de 2020].
Disponible en: https://www.redalyc.org/pdf/310/31043005061.pdf

QUEMBA, Luis. Cifrado de la información y su incidencia actual en la seguridad de la información para pequeñas empresas pymes en Colombia. Tesis (Licenciado en seguridad informática). Bogotá: Universidad nacional abierta y a distancia (UNAD), 2020.
Disponible en: https://repository.unad.edu.co/handle/10596/34350

RAMOS, Irene, LÓPEZ, Carmen y TORRECILLAS, Teresa. Online risk perception in young people and its effects on digital behaviour [Percepción de riesgo online en jóvenes y su efecto en el comportamiento digital]. *Comunicar. Media Education Research Journal* [En línea]. 2018, vol. 26, n.° 56. [Fecha de consulta: 28 de octubre de 2020].
Disponible en: https://www.scipedia.com/public/Ramos-Soler_et_al_2018a

RAYMOND, Angello. Secure protocols and virtual private networks: an evaluation [Protocolos seguros y redes privadas virtuales: una evaluación]. *Issues in Information Systems* [En línea]. 2019, vol. 20, n.° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://iacis.org/iis/2019/3_iis_2019_37-46.pdf

REDŽOVIĆ, Hasan, SMILJANIĆ, Aleksandra y SAVIĆ, Bogdan. Performance evaluation of Software Routers with VPN features [Evaluación del rendimiento de enrutadores de software con funciones de VPN]. *2016 24th Telecommunications Forum (TELFOR)* [En línea]. 2016, vol. 1, n.° 1. [Fecha de consulta: 30 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7818727

REOLID, Ricardo, FLORES, María, LÓPEZ, Mónica, ALCANTUD, Pilar, AYUSO, Candelaria y ESCOBAR, Francisco. Frequency and characteristics of Internet use by Spanish Teenagers a cross-sectional study. [Frecuencia y características del uso de Internet por adolescentes españoles Un estudio transversal]. *Original article* [En línea]. Febrero 2016, vol. 114, n.° 1. [Fecha de consulta: 29 de octubre].
Disponible en: https://www.sap.org.ar/docs/publicaciones/archivosarg/2016/v114n1a03e.pdf

ROB, Abel. Vpn Endgame. SC Magazine: For IT Security Professionals [En línea]. Mayo 2019 [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.scmagazine.com/feature/privacy-compliance/vpn-endgame

RODRÍGUEZ, Walter. Evaluación del tráfico de red ante los episodios de saturación a nivel nacional. Tesis (Titulo en ingeniería de Telecomunicaciones). Guayaquil: Universidad Católica de Santiago de Guayaquil, 2020.
Disponible en: http://repositorio.ucsg.edu.ec/handle/3317/15597

RODRÍGUEZ, Walter. Evaluación del tráfico de red ante los episodios de saturación a nivel nacional. Tesis (Título de ingeniero en telecomunicaciones). Guayaquil: Universidad Católica de Santiago de Guayaquil, 2020.
Disponible en: http://201.159.223.180/handle/3317/15597

SABER, Abid, FERGANI, Belkacem y ABBAS, Moncef. Encrypted Traffic Classification: Combining Over-and Under-Sampling through a PCA-SVM. [Clasificación de tráfico cifrado: combinación de sobre muestreo y submuestreo a través de una PCA-SVM]. *2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS)* [En línea]. 2018, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8598480/

SAHU, Megha, DAMLE, Snigdha y KHERANI, Arzad. Traffic Splitting for End-toEnd Delay Jitter Control in Uplink Multi-Access Systems. [División de tráfico para el control de fluctuación de retardo de extremo a extremo en sistemas de acceso múltiple de enlace ascendente]. *2019 11th International Conference on Communication Systems Networks (COMSNETS)* [En línea]. 2019, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8711198/

SALIM, Mikail, RATHORE, Shailendra y PARK, Jong. Distributed denial of service attacks and its defenses in IoT: a survey [Ataques distribuidos de denegación de servicio y sus defensas en IoT: una encuesta]. *The Journal of Supercomputing* [En línea]. 2020, vol. 1, n.° 76. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://link.springer.com/article/10.1007/s11227-019-02945-z

SÁNCHEZ, Reinaldo. T-Student: Usos y abusos. *Revista mexicana de Cardiología* [En línea]. 2015, vol. 26, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=s0188-21982015000100009

SARAS, Celia. Análisis de vulnerabilidades del DNS. Tesis (Licenciado en Ingeniería de telecomunicación). Madrid: Universidad Politécnica de Madrid, 2015.
Disponible en: http://oa.upm.es/37771/1/PFC_CELIA_SARAS_GONZALEZ_2015.pdf

SEGURA, Paola y RAMÍREZ, Maritza. Informatics Security-VPN [Seguridad informática-VPN]. *Tekhnê* [En línea]. Junio 2018, vol. 15, n.° 1. [Fecha de consulta: 29 de octubre de 2020].
Disponible en: https://revistas.udistrital.edu.co/index.php/tekhne/article/view/16944

SENNEWALD, Charles y BAILLIE, Curtis. International security standards. [Normas internacionales de seguridad]. *Effective Security Management* [En línea]. 2020, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.researchgate.net/publication/339914355_International_security_standards

SHARMA, Yogesh y KAUR, Chamandeep. The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World [El papel vital de la red privada virtual (VPN) para establecer una conexión segura a través del mundo de Internet]. *International Journal of Recent Technology and Engineering (IJRTE)* [En línea]. 2020, vol. 8, n. °6. [Fecha de consulta: 29 de octubre de 2020].
Disponible en: https://www.ijrte.org/wp-content/uploads/papers/v8i6/F8335038620.pdf

SHENG, Min, WANG, Yu, LI, Jiandong, LIU, Runzi, ZHOU, Di y HE, Lijun. Toward a Flexible and Reconfigurable Broadband Satellite Network: Resource Management Architecture and Strategies. [Hacia una red satelital de banda ancha flexible y reconfigurable: arquitectura y estrategias de gestión de recursos]. *IEEE Wireless Communications* [En línea]. 2017, vol. 24, n.° 4. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/7956007/

SHIM, Timothy. Los mejores servicios de VPN de 2020: 10 principales VPN comparadas. 30 de junio de 2020.
Disponible en: https://www.webhostingsecretrevealed.net/es/blog/web-tools/best-vpn/#choose

SIGCHA, Mario. Análisis del desempeño de un sistema de VoIP Asterisk implementado sobre un servidor remoto y sobre un servidor físico. Tesis (Licenciado en ingeniería en electrónica y telecomunicaciones). Sangolquí: Universidad de las fuerzas armadas, 2020.
Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/22405/1/T-ESPE-043760.pdf

SUÁREZ, Lissette. Análisis de vulnerabilidad en la red Lan usando herramientas de hacking ético para una empresa de la provincia de Santa Elena. Tesis (Titulo para ingeniero en tecnologías de la información). La Libertad: Universidad Estatal Península de Santa Elena, 2022.
Disponible en: https://repositorio.upse.edu.ec/handle/46000/7727

TAMARIZ, Edna, COYOTECATL, Miguel, TORREALBA, Richard y AMBROSIO, Roberto. Análisis del parámetro Throughput en una red Ad hoc y MANET en el estándar 802.11 ac. *Revista de Aplicación Científica y Técnica* [En línea]. Enero - marzo 2017, vol. 3, n.° 7. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.ecorfan.org/spain/rj_aplicacion_cyt_vii.php

THAKKAR, Ankit y LOHIYA, Ritika. A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges. [Una revisión sobre las perspectivas de aprendizaje automático y aprendizaje profundo de IDS para IoT: actualizaciones recientes, problemas de seguridad y desafíos]. *Archives of Computational Methods in Engineering* [En línea]. 2021, vol. 28, n.° 4. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://link.springer.com/article/10.1007/s11831-020-09496-0

TIBADUIZA, Jorge. Estudio del tráfico de red por medio de un análisis estadístico de los paquetes de datos que viajan a través de los diferentes nodos y hacia cada uno de los usuarios que posee la empresa "FSD S.A.S.". Tesis (Licenciatura de ingeniería electrónica). Colombia: Universidad Pedagógica Y Tecnológica de Colombia, 2015.
Disponible en: https://repositorio.uptc.edu.co/handle/001/1724

TORMASOV, Alexander, BELOUSSOV, Serguei y PROTASSOV, Stanislav. System, method, and computer program product for group scheduling of computer resources. [Sistema, método y producto de programa informático para la programación grupal de recursos informáticos]. U.S., 7.665.090 (16.02.2010). [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://patents.google.com/patent/US7665090B1/en

TORREBLANCA, Guillermina, DE LA CRUZ, Eduardo, CARRANZA, Jorge Gómez3 y Gutiérrez, Francisco. Un modelo educativo virtual para simular entornos de red móvil. *Memorias del Congreso Internacional de Investigación Académica Journlist Celaya 2017* [En línea]. Noviembre 2017, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://acapulco.tecnm.mx/wp-content/uploads/maestria/repositorio/memoria_congreso/5_Memorias-Academia-Journals-Celaya-2017-Guillermina.pdf

TORRES, Néstor, GUEVARA, Adela, HERNÁNDEZ, José, GARCÍA, Carlos y Ramírez, John. Una alternativa para Pymes GNU/Linux Server como sistema operativo base para servicios de infraestructura Tecnológica. Tesis (Licenciado

en ingeniería de sistemas). Bogotá: Universidad Nacional Abierta y a Distancia, 2018.
Disponible en: https://repository.unad.edu.co/handle/10596/23959

TORRES, Pedro y ALFARO, Emigdio. MEPES: Methodology for Evaluating the Performance of E-Mail Servers. [MEPES: Metodología para evaluar el rendimiento de los servidores de correo electrónico]. *International Journal of Open Source Software and Processes (IJOSSP)* [En línea]. 2018, vol. 9, n.° 4. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.igi-global.com/article/mepes/221363

UCV. Código nacional de la integridad científica [En línea]. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://drive.google.com/drive/u/0/folders/1LN01hkToSuvPbBkNCAp48PljS3tS4v_s

UCV. Reglamento de investigación [En línea]. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://drive.google.com/drive/u/0/folders/1LN01hkToSuvPbBkNCAp48PljS3tS4v_s

UCV. Reglamento de propiedad intelectual de la UCV [En línea]. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://drive.google.com/drive/u/0/folders/1LN01hkToSuvPbBkNCAp48PljS3tS4v_s

UCV. Resolución de consejo universitario N°0126-2017 UCV [En línea]. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://drive.google.com/drive/u/0/folders/1LN01hkToSuvPbBkNCAp48PljS3tS4v_s

UCV. Resolución de consejo universitario N°084-2016 UCV [En línea]. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://drive.google.com/drive/u/0/folders/1LN01hkToSuvPbBkNCAp48PljS3tS4v_s

UCV. Resolución de directorio, N.° 0066-2018 UCV [En línea]. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://drive.google.com/drive/u/0/folders/1LN01hkToSuvPbBkNCAp48PljS3tS4v_s

UCV. Vicerrectorado de investigación, N°011-N°21-VI- UCV [En línea]. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://drive.google.com/drive/u/0/folders/1LN01hkToSuvPbBkNCAp48PljS3tS4v_s

VARGAS, Gabriela, GUARDA, Teresa, MUYÓN, Christian y QUIÑA, Geovanni. Obtención de claves en redes WLAN/WPS usando Wifislax y Denegación de Servicios con Kali Linux. *Revista Ibérica de Sistemas e Tecnologias de Informação* [En línea]. 2019, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.proquest.com/openview/f4b193b46ccb16a2fa7f1e3c633e8dd1/1?pq-origsite=gscholar&cbl=1006393

VÁSQUEZ, Gustavo y GUEVARA, Elia. Evaluación de pacientes adultos mayores con diagnóstico de abdomen agudo quirúrgico. Estudio prospectivo, descriptivo, no experimental. *Revista Venezolana De Cirugía* [En línea]. Octubre de 2020, vol. 73, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.revistavenezolanadecirugia.com/index.php/revista/article/view/288

VELASCO, Paola, JIMÉNEZ, María y CHAFLA, Gustavo. Análisis de los mecanismos de encriptación para la seguridad de la información en redes de comunicaciones. *Ciencias Básicas Y Tecnología* [En línea]. 2017, vol. 12, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://190.15.129.73/index.php/sathiri/article/view/38

VENTURA, José. La importancia de reportar la validez y confiabilidad en los instrumentos de medición: Comentarios a Arancibia et al. *Revista médica Chile* [En Línea]. Julio 2017, vol.145, n.° 7 [Fecha de consulta: 31 de octubre de 2020]. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0034-98872017000700955&lng=es&nrm=iso.%20ISSN%200034-9887

VERONA, Sandra, PÉREZ, Yasiel, TORRES, Lisbán, DELGADO, Martha y YÁÑEZ, Cornelio. Pruebas de rendimiento a componentes de software utilizando programación orientada a aspectos. *Ingeniería Industrial* [En línea]. 2016, vol. 37, n.° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=s1815-59362016000300006%20ISSN%201815-5936

VILLASÍS, Miguel, MÁRQUEZ, Horacio, ZURITA, Jessie, MIRANDA, María y ESCAMILLA, Alberto. El protocolo de investigación VII. Validez y confiabilidad de las mediciones. *Revista alergia México* [En línea]. Octubre 2018, vol. 65, n.° 4. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://dx.doi.org/10.29262/ram.v65i4.560

VIVANCO, Danny y CHILÁN, Ingrid. Desarrollo de un observatorio tecnológico enfocado a la seguridad de la información para instituciones de educación superior (IES). Tesis (Maestría en auditoría en tecnología de la información). Guayaquil: Universidad de especialidades Espíritu Santo UEES, 2019.
Disponible en: http://201.159.223.2/handle/123456789/2990

VPNMENTOR. Kanishk. VPNMentor: Cómo comprobar la seguridad de tu VPN. 22 de mayo de 2019.
Disponible en: https://es.vpnmentor.com/blog/como-comprobar-la-seguridad-de-tu-vpn/

WANG, Wenqi, WANG, Dong, SINGH, Vijay, WANG, Yuankum, WU, Jichun, ZHANG, Jianyun, LIU, Jiufu, ZOU, Ying, HE, Ruimin y MENG, Deqing. Evaluation of information transfer and data transfer models of rain-gauge network design based on information entropy. [Evaluación de modelos de transferencia de información y transferencia de datos de pluviómetro diseño de red basado en la entropía de la información]. *Environmental Research* [En línea]. 2019, vol. 178, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S0013935119304839

WEARESOCIAL. Simón, Kemp. Digital 2020: 3.8 billion people use social media - We Are Social. 30 de enero de 2020.
Disponible en: https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/

WOLFINBARGER, Patrick. A VPN can make public Wi-Fi safe. [Una VPN puede hacer que la conexión Wi-Fi pública sea segura]. *Wyoming Business Report* [En línea]. Julio 2018, vol. 19, n. °4. [Fecha de consulta: 27 de octubre de 2020].
Disponible en: https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=3&sid=aff1058e-1715-4978-b831-6dc920a1b7ff%40redis

WU, Zheng y XIAO, Mingzhong. Performance Evaluation of VPN with Different Network Topologies. [Evaluación de rendimiento de VPN con diferentes topologías de red]. *2019 IEEE 2nd International Conference on Electronics Technology (ICET)* [En línea]. Mayo 2019, vol. 1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/8839611

ZAMBRANO, Silvia y VALENCIA, David. Seguridad en informática: consideraciones. *Dominio de las Ciencias* [En línea]. 2017, vol. 3, n.° 3. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

ZHIPENG, Zhang, CHANDEL, Sonali, JINGYAO, Sun, SHILIN, Yan, YUNNAN, Yu, y JINGJI, Zang. VPN: a Boon or Trap?: A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks. [VPN: ¿una bendición o trampa?: Un estudio comparativo de redes privadas virtuales MPLS, IPSec y SSL]. *In 2018 Second International Conference on Computing Methodologies and Communication (ICCMC)* [En línea]. Noviembre 2018, vol. 1, n. ° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/document/8487653

ZHOU, Yimin y ZHANG, Kai. DoS Vulnerability Verification of IPSec VPN [Verificación de vulnerabilidad DoS de IPSec VPN]. *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)* [En línea]. 2020, vol.1, n.° 1. [Fecha de consulta: 31 de octubre de 2020].
Disponible en: https://ieeexplore.ieee.org/abstract/document/9182437

ANEXOS

# Anexo 1 Matriz de Consistencia

## Tabla 59 Matriz de consistencia

<table>
<tr><th>Problema General</th><th>Objetivo General</th><th>Hipótesis</th><th colspan="3">Variables, Dimensiones e Indicadores</th><th>Método</th></tr>
<tr><td rowspan="2">PG: ¿Cuáles fueron los procesos de la metodología que permitió la evaluación de rendimiento de los softwaresde redes privadas virtuales?</td><td rowspan="2">OG: Determinar cuáles fueron los procesos de la metodología que permitió la evaluación de rendimiento delos softwares de redes privadas virtuales (Acosta, Espinel y García, 2017).</td><td rowspan="2">HG: La aplicación de los procesos de la metodología MEPVPNS permitiódeterminar la evaluación de rendimiento de los softwares de redes privadas virtuales. (Pacotaype, 2018; Bravo, 2015; Segura y Ramírez,2018; León, 2018; Kumar y Majeed, 2018; Macworld, 2020; Wolfinbarger, 2018; Shim, 2020; Phelan, 2019).</td><th>Variables</th><th>Dimensiones</th><th>Indicadores</th><td rowspan="5">➢ Tipo de investigación<br>Aplicada (Hernández y Mendoza, 2018, Concytec, 2017; Vivanco y Chilán, 2019)<br>➢ Diseño de investigación<br>No experimentaltransversal-descriptivo (Hernández y Mendoza, 2018; Alva y Domínguez, 2015, p. 94; Vásquez y Guevara, 2020; Hagopian, 2016)<br>➢ Enfoque delnvestigaciones<br>Cuantitativo (Hernández y Mendoza, 2018).<br>➢ Nivel<br>Descriptivo (Gallardo, 2017; Hernández y Mendoza, 2018)</td></tr>
<tr><td>1. Rendimiento del software (Verona et al., 2016; Lucena 2019; Pacotaype, 2018)</td><td>1. Velocidad de transferencia de datos (Wang et al., 2019)</td><td>1. Throughput (Tamariz et al., 2019; Wu y Xiao, 2019)<br>2. Jitter (Torreblanca et al., 2017; Andreadis et al., 2016; Sahu etal., 2019; Nurhaida et al., 2020)</td></tr>
<tr><td>Problema Específico</td><td>Objetivo Específico</td><td>Hipótesis Específicas</td><td rowspan="2">2. Administración de recursos (Torres et al., 2018; Sharma y Kaur, 2020; Hong et al., 2018; Li et al., 2017)</td><td rowspan="2">2. Consumo de Recursos (Agah, 2017; Tormasov et al., 2010; Zhou y Zhang, 2020)</td><td rowspan="2">3. Uso del CPU (Jati et al., 2016; Aguirre, 2016)<br>4. Uso de la Memoria RAM (Aguirre, 2016; Lopez y Grampín, 2017)<br>5. Uso del Disco Duro (Aguirre, 2016; Chilcañán et al., 2017;Quemba, 2020)</td></tr>
<tr><td>PE1: ¿Cuáles fueron losprocesos de la metodología que permitió la evaluación de rendimiento de los softwaresde redes privadas virtuales en cuanto al rendimiento del software?</td><td>OE1: Determinar cuáles fueron los procesos de la metodología que permitió la evaluación de rendimiento delos softwares de redes privadas virtuales en cuanto al rendimiento del software</td><td>HE1: La aplicación de los procesos de la metodología MEPVPNS permitió la evaluación de los softwares de redes privadas virtuales en cuanto al rendimiento del software (Lucena, 2019; Wolfinbarger, 2018; Ian, 2021; PCMag, 2020; Phelan, 2019; Av comparatives, 2020; Wu y Xiao, 2019; Lawas et al., 2016; Ian, 2021)</td></tr>
<tr><td>PE2: ¿Cuáles fueron losprocesos de la metodología que permitió la evaluación de rendimiento de los softwaresde redes privadas virtuales en cuanto a la administración de recursos?</td><td>OE2: Determinar cuáles fueron los procesos de la metodología que permitió la evaluación de rendimiento delos softwares de redes privadas virtuales en cuantoa la administración de recursos.</td><td>HE2: La aplicación de los procesos de la metodología MEPVPNS permitióevaluar los softwares de redes privadasvirtuales en cuanto a la administración de recursos (Gunleifsen et al., 2019; Caprolu et al., 2020; Martinasek et al., 2017; Lawas, et al., 2016)</td><td rowspan="2">3. Desempeño en la red (Lawas et al., 2016; Pacotaype, 2018; Martinasek et al., 2017).</td><td>4. Conectividad de Red (Amorim et al., 2019; Dong y Kim, 2017; Cisco 2019).</td><td>6. Latencia (Sigcha, 2020; Fujiki et al., 2017)<br>7. Velocidad de Subida (Balladares, 2017)<br>8. Velocidad de Descarga (Balladares, 2017)<br>9. Ancho de banda (Mercado y Ortiz, 2020; Sheng et al., 2017;Paessler, 2015)</td></tr>
<tr><td>PE3: ¿Cuáles fueron los procesos de la metodología que permitió la evaluación de rendimiento de los softwaresde redes privadas virtuales en cuanto al desempeño en la red?</td><td>OE3: Determinar cuáles fueron los procesos de la metodología que permitió la evaluación de rendimiento delos softwares de redes privadas virtuales en cuanto al desempeño en la red.</td><td>HE3: La aplicación de los procesos de la metodología MEPVPNS permitióevaluar los softwares de redes privadasvirtuales en cuanto al desempeño en la red (ISO, 2019; Sennewald y Baillie, 2020; Rob, 2019; Wolfinbarger, 2018; Phelan, 2019; De la Rosa, 2019).</td><td>3. Seguridad (Oña,2016; Nico, 2018; IBM, 2021)</td><td>10. Porcentaje de filtro y marcado de trafico de red (Basile et al., 2019;Chauca, 2016; Carvajal, 2019; Gai y McCloghrit, 2007)<br>11. Velocidad de encriptamiento de datos (Saber et al., 2018; Pérez,2017; Quemba,2020)<br>12. Velocidad de desencriptamiento de datos (Bucşă, 2020; Pérez, 2017; Microsoft, 2017; FileMaker, 2017; Gallegos y Mayorga, 2019;Méndez, 2020)<br>13. Fugas de servidores DNS (Oramas, 2020; Fakis et al., 2020; Saras, 2015; Gordillo, 2017; VpnMentor, 2019; ExpressVPN, 2020)<br>14. Fugas de dirección IP (Hostgator, 2019; Oramas, 2020; Al-fannah,2017; VpnMentor, 2019; Segura y Ramirez, 2018; Salim et al., 2020)<br>15. Fugas de dirección IP por webRTC (Guimarey, 2017; Bhalerao et al., 2020, Fakis et al., 2020; Ezell y Yoakum, 2020)<br>16. Conexión al servidor (Netspotapp, 2020; Hauser et al., 2020; Abril y Cuzco, 2019)</td></tr>
</table>

## Anexo 2 Matriz de operacionalización de variables

### Tabla 60 Matriz de operacionalización de variables

| Variables | Definición conceptual | Definición operacional |
|---|---|---|
| Rendimiento del software **(Verona et al., 2016; Lucena 2019; Pacotaype).** | El rendimiento de las redes privadas virtuales son pruebas de rendimiento que tiene como propósito estresar el software, realizando exámenes fuera del alcance para los que fue implementado. Además, los softwares redes privadas virtuales son túneles virtuales encriptados entre el usuario y un servidor remoto operado por un servicio VPN **(Verona et al., 2016; Lucena 2019; Pacotaype, 2018, Torres y Alfaro, 2018; Carrión, 2018; Wang et al., 2019).** | El rendimiento de evaluación de las redes privadas virtuales es el resultado obtenido al evaluar de forma organizada y metódica estas tecnologías de comunicación privada a través de dimensiones de evaluación (rendimiento del software, administración de recursos y desempeño en la red). Asimismo, el rendimiento se calcula como la amplitud del software, al emplear los componentes físicos de manera eficaz. Además, el rendimiento se puede medir con métricas de calidad en el intercambio de información, usando los servicios de internet, etc.; mediante herramientas para evaluar los indicadores planteados en la presente investigación **(Verona et al., 2016; Lucena 2019; Pacotaype, 2018, Torres y Alfaro, 2018; Carrión, 2018; Wang et al., 2019).** |
| Administración de recursos **(Torres et al., 2018; Sharma y Kaur, 2020; Hong et al., 2018; Li et al., 2017).** | La administración de recursos son procesos o subprocesos que se ejecutan en un sistema informático, que requieren recursos compartidos de tiempo de CPU, memoria, objetos del sistema operativo, semáforos, acceso a disco, acceso a la red, entre otros para el correcto funcionamiento del sistema **(Torres et al., 2018; Sharma y Kaur, 2020; Hong et al., 2018; Li et al., 2017; Agah, 2017; Tormasov et al., 2010; Zhou y Zhang, 2020).** | El indicador de administración de recursos en los sistemas es esencial para obtener respuestas al verificar los servicios de otros sistemas que ayudaran a mantener un control sobre los procesos en desarrollo **(Torres et al., 2018; Sharma y Kaur, 2020; Hong et al., 2018; Li et al., 2017; Agah, 2017; Tormasov et al., 2010; Zhou y Zhang, 2020)** |
| Desempeño en la red **(Lawas et al., 2016; Pacotaype, 2018; Martinasek et al., 2017).** | El desempeño en la red es la facultad para hacerle frente a la sobrecarga de red sin generar retrasos o acumulaciones de transporte de la información a través de la red **(Lawas et al., 2016; Pacotaype, 2018; Martinasek et al., 2017; Amorim et al., 2019; Dong y Kim, 2017; Cisco 2019; Oña,2016; Nico, 2018; IBM, 2021).** | La evaluación del desempeño en la red es una dimensión fundamental, para evaluar el rendimiento de una VPN y lograr comparar una tecnología con otra. Además, se debe tener en cuenta que el throughput, latencia y ancho de banda son indispensables para identificar las necesidades de tráfico de red actual **(Lawas et al., 2016; Pacotaype, 2018; Martinasek et al., 2017; Amorim et al., 2019; Dong y Kim, 2017; Cisco 2019; Oña,2016; Nico, 2018; IBM, 2021).** |

| Dimensiones | Indicadores | Descripción | Instrumento | Unidad de medida |
|---|---|---|---|---|
| Velocidad de transferencia de datos **(Wang et al., 2019).** | Medición del Throughput **(Tamariz et al., 2019; Wu y Xiao, 2019).** | $\boldsymbol{Throughput} = \frac{PTR}{T}$<br>**PTR**: Paquete Total recibidos<br>**T**: Tiempo | Hoja de tabulación de datos | Megabits/segundo ò Gigabits/segundo |
| | Medición del Jitter **(Torreblanca et al., 2017; Andreadis etal., 2016; Sahu et al., 2019; Nurhaida et al., 2020).** | $\boldsymbol{Jitter} = \frac{cantidad\ de\ paquetes\ recibidos}{tiempo\ promedio - variacion\ de\ tiempo}$ | Hoja de tabulación de datos | Milisegundos |
| Consumo de Recursos **(Agah,2017; Tormasov et al., 2010; Zhou y Zhang, 2020)** | Porcentaje del uso de CPU **(Jati et al., 2016; Aguirre, 2016).** | $\boldsymbol{Consumo\ CPU} = \frac{Consumo\ de\ CPU}{Ataque\ de\ denegación\ de\ servicio}$ | Hoja de tabulación de datos | Porcentaje |
| | Porcentaje del uso de Memoria RAM **(Aguirre, 2016; Lopezy Grampín, 2017)** | $\boldsymbol{Memoria\ RAM} = \frac{Consumo\ de\ Memoria\ RAM}{Ataque\ de\ denegación\ de\ servicio}$ | Hoja de tabulación de datos | Porcentaje |
| | Porcentaje del uso del Disco Duro **(Aguirre, 2016;Chilcañán et al., 2017; Quemba, 2020).** | $\boldsymbol{Disco\ Duro} = \frac{Consumo\ de\ disco\ duro}{Ataque\ de\ denegación\ de\ servicio}$ | Hoja de tabulación de datos | Porcentaje |
| Conectividad de Red **(Amorim etal., 2019; Dong y Kim, 2017; Cisco 2019).** | Medición del ancho de banda **(Mercado y Ortiz, 2020;Sheng et al., 2017; Paessler, 2015).** | $\boldsymbol{Ancho\ de\ banda} = \frac{VD}{TT}/8$<br>**VD**: Velocidad de descarga (Megabits)<br>**TT**: Tiempo transcurrido (segundos) | Hoja de tabulación de datos | Kilobyte/sec |
| | | $\boldsymbol{Ancho\ de\ banda} = \frac{VS}{TT}/8$<br>**VS**: Velocidad de subida (Megabits)<br>**TT**: Tiempo transcurrido (segundos) | Hoja de tabulación de datos | Kilobyte/sec |
| | Medición de Latencia **(Sigcha, 2020; Fujiki et al., 2017).** | $\boldsymbol{Latencia} = \frac{Tiempo\ de\ respuesta}{uso\ del\ software\ vpn}$ | Hoja de tabulación de datos | Milisegundos |
| | Velocidad de Subidas de archivos **(Ballada-res, 2017).** | $\boldsymbol{velocidad\ de\ subida} = \frac{TPS}{TTT}$<br>**TPS**: Tamaño de paquetes subidos (Megabits)<br>**TTT**: Tiempo total transcurrido (segundos) | Hoja de tabulación de datos | Bit/Segundos |
| | Velocidad de Descargas de archivos **(Ballada-res, 2017).** | $\boldsymbol{velocidad\ de\ subida} = \frac{TPD}{TTT}$<br>**TPD:** Tamaño de paquetes subidos (Megabits)<br>**TTT:** Tiempo total transcurrido (segundos) | Hoja de tabulación de datos | Bit/Segundos |

| Dimensiones | Indicadores | Descripción | Instrumento | Unidad de medida |
|---|---|---|---|---|
| Seguridad **(Oña,2016; Nico, 2018; IBM, 2021).** | Porcentaje de Filtro y marcado de tráfico de red **(Basile et al., 2019;Chauca, 2016; Carvajal, 2019; Gai y McCloghrit, 2007)** | $\boldsymbol{filtro\ y\ marcado\ de\ trafico\ de\ red} = \frac{TPD}{TP} * 100$<br>**TPD:** Total de protocolos detectados<br>**TP:** Total de protocolos | Hoja de tabulación de datos | Porcentaje |
| | Velocidad de encriptamiento de datos **(Saber et al., 2018; Pérez,2017; Quemba,2020).** | $\boldsymbol{Encriptamiento\ de\ datos} = \frac{CP}{TED}$<br>**CP:** Cantidad de paquetes (Kilobyte)<br>**TED:** Tiempo de encriptamiento de datos (segundos) | Hoja de tabulación de datos | Kilobyte/sec |
| | Velocidad de desencriptamiento de datos **(Bucșă, 2020; Pérez,2017; Microsoft, 2017; FileMaker, 2017; Gallegos y Mayorga, 2019; Méndez, 2020).** | $\boldsymbol{Desencriptamiento\ de\ datos} = \frac{CP}{TDD}$<br>**CP:** Cantidad de paquetes (Kilobyte)<br>**TDD:** Tiempo de desencriptamiento de datos (segundos) | Hoja de tabulación de datos | Kilobyte/sec |
| | Fugas de servidores DNS (**Oramas, 2020; Fakis et al., 2020; Saras, 2015; Gordillo, 2017; VpnMentor, 2019; ExpressVPN, 2020)** | $\boldsymbol{Fugas\ de\ servidores\ DNS} = \frac{CSD}{RI}$<br>**CSD:** Cantidad de servidores detectados<br>**RI:** Reconexión de Internet | Hoja de tabulación de datos | Numérico |
| | Fugas de dirección IP (**Hostgator, 2019; Oramas, 2020; Al-fannah,2017; VpnMentor, 2019; Segura y Ramirez, 2018; Salim et al., 2020)** | $\boldsymbol{Fugas\ de\ dirección\ IP} = \frac{CDIP}{RI}$<br>**CDIP:** Cantidad de direcciones IP detectadas<br>**RI:** Reconexión de Internet | Hoja de tabulación de datos | Numérico |
| | Fugas de dirección IP por webRTC (**Guimarey, 2017; Bhalerao et al.,2020 , Fakis et al., 2020; Ezell y Yoakum, 2020).** | $\boldsymbol{Fugas\ de\ WebRTC} = \frac{CDIWD}{RI}$<br>**CDIWD:** Cantidad de dirección IP por WebRTC detectadas<br>**RI:** Reconexión de Internet | Hoja de tabulación de datos | Numérico |
| | Conexión al servidor **(Netspotapp, 2020; Hauser et al., 2020; Abrily Cuzco, 2019)** | $\boldsymbol{Conexión\ al\ servidor} = \frac{Tiempo\ de\ conexión\ al\ servidor}{uso\ del\ software\ vpn}$ | Hoja de tabulación de datos | Milisegundos |

Anexo 3 Matriz de clasificación de softwares de redes privadas virtuales

Tabla 61 Clasificación de software VPN

| N° | PRODUCTO | | | | PROTOCOLOS | | | | | | | PAGOS | | | | BÚSQUEDA | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Software | Última Versión | Administrador | Servidor Central | OPENVPN | IKEv2/ IPSec | L2TP/ IPSec | PPT | SSTP | SSH | WireGuard | Prueba Libre/Gratuita | Tiempo de utilidad / Limitaciones | Valor del software | Modo de Pago | Sin Búsqueda de trafico | Sin Búsqueda de ancho de banda | Sin Búsqueda de direcciones IP |
| 1 | Avast Secure-Line VPN | 5.5 | Avast Software S.R.O | República Checa | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Gratuita | 7 días | 90 dólares | Tarjeta de crédito/débito, PayPal, Transferencia bancaria | No hay datos registrados | Datos registrados | Datos registrados<br>Recopila la dirección IP asignada a la VPN y la subred solo de la dirección IP de origen |
| 2 | AVG Secure VPN | 1.10 | Avast Software S.R. O | República Checa | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Gratuita | 7dias | 90 dólares | Tarjeta de crédito/débito, PayPal, Transferencia bancaria | No hay datos registrados | Datos registrados | Datos registrados<br>Recopila la dirección IP asignada a la VPN y la subred solo de la dirección IP de origen |
| 3 | Avira Phantom VPN | 2.32 | Avira Operations GmbH & Co. KG | Alemania | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | Sin ubicación en el Reino Unido, datos de 500 MB al mes | 78 dólares | Tarjeta de crédito/débito, PayPal | No hay datos registrados | Datos registrados | No hay datos registrados |
| 4 | Bitdefender VPN | 24.0 | Bitdefender SRL | Rumania | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Gratuita | 30 días | 85 dólares | Tarjeta de crédito/débito, PayPal, Transferencia bancaria | No se establece explícitamente, política poco clara | No se establece explícitamente, política poco clara | Datos registrados pero anónimos |
| 5 | Bull-Guard VPN | 1.3 | BullGuard LTD. | Uk | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 83 dólares | Tarjeta de crédito/débito, PayPal, Transferencia bancaria | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 6 | CyberGhost VPN | 7.2 | CyberGhost S.A. | Rumania | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 72 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda,monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |

| N° | PRODUCTO | | | | PROTOCOLOS | | | | | | | PAGOS | | | | BUSQUEDA | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Software | Última Versión | Administrador | Servidor Central | OPENVPN | IKEv2/ IPSec | L2TP/ IPSec | PPT | SSTP | SSH | WireGuard | Prueba Libre/Gratuita | Tiempo de utilidad / Limitaciones | Valor del software | Modo de Pago | Sin Búsqueda de trafico | Sin Búsqueda de ancho de banda | Sin Búsqueda de direcciones IP |
| 7 | **Express VPN** | 7.8 | Express VPN International LTD. | Islas Vírgenes Británicas | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 100 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda,monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 8 | **F-Secure Freedome** | 2.32 | F-Secure Corp. | Finlandia | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Gratuita | 30 días | 90 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, monederos digitales | Datos registrados pero anónimos | Datos registrados | Datos registrados |
| 9 | **Hide.me VPN** | 3.2 | EVenture LTD. | Malasia | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Libre | Menos ubicaciones, datos de 10 GB al mes | 100 dólares | Tarjeta de crédito/débito, PayPal, criptomoneda de transferencia bancaria | No hay datos registrados | Datos registrados pero anónimos | No hay datos registrados |
| 10 | **HMA VPN** | 5.0 | Privax LTD. | Uk | Protocolo soportado | Protocolo no soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Gratuita | 7 días | 84 dólares | Tarjeta de crédito/débito, PayPal | No hay datos registrados | Datos registrados pero anónimos | No hay datos registrados |
| 11 | **Hotspot Shield** | 9.6 | AnchorFree INC. | E.E.U. U | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | 1 ubicación de EE. UU. solamente, 500 MB de datos por mes, sin optimización de streaming | 96 dólares | Tarjeta de crédito/débito, PayPal | Datos registrados pero anónimos | Datos registrados | Datos registrados pero anónimos |
| 12 | **IPVanish** | 3.4 | Mudhook Media INC. | E.E.U. U | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 78 dólares | Tarjeta de crédito/débito, PayPal | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 13 | **Ivacy** | 5.3 | PMG Pte. LTD. | Singapur | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Gratuita | 7 días | 42 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda,monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |

| N° | PRODUCTO | | | | PROTOCOLOS | | | | | | | PAGOS | | | | BUSQUEDA | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Software | Última Versión | Administrador | Servidor Central | OPENVPN | IKEv2/ IPSec | L2TP/ IPSec | PPT | SSTP | SSH | WireGuard | Prueba Libre/Gratuita | Tiempo de utilidad / Limitaciones | Valor del software | Modo de Pago | Sin Búsqueda de trafico | Sin Búsqueda de ancho de banda | Sin Búsqueda de direcciones IP |
| 14 | **Kaspersky Secure Connection** | 20.0 | AO Kaspersky LAB. | Rusia | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | Selección automática de ubicación, 200 MB pordía | 30 dólares | Tarjeta de crédito/débito, PayPal, Transferenciabancaria | No se establece explícitamente, política poco clara | No se establece explícitamente, política poco clara | No se establece explícitamente, política poco clara |
| 15 | **McAfee Safe Connect** | 2.6 | McAfee LLC | E.E.U. U | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | Datos de 250 MB al mes | 48 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, Monederos digitales | No se establece explícitamente, política poco clara | No se establece explícitamente, política poco clara | No se establece explícitamente, política poco clara |
| 16 | **mySteganos Online Shield VPN** | 2.0 | Steganos Software GmbH | Alemania | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Gratuito | 7 días | 50 dólares | Tarjeta de crédito/débito, PayPal, Transferenciabancaria | No hay datos registrados | Datos registrados pero anónimos | No hay datos registrados |
| 17 | **Nord VPN** | 6.27 | Tefincom & Co. S.A. | Panamá | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 84 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda,monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 18 | **Norton Secure VPN** | 1.9 | NortonLifeLock INC. | E.E.U. U | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 100 dólares | Tarjeta de crédito/débito, PayPal, Transferencia bancaria | No hay datos registrados | Datos registrados pero anónimos | Datos registrados pero anónimos |
| 19 | **Panda Dome VPN** | 20.00 | Panda Security S.L. | España | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | Selección automática de ubicación, datos de 150 MB por día | 77 dólares | Tarjeta de crédito/débito, PayPal | No se establece explícitamente, política poco clara | No se establece explícitamente, política poco clara | No se establece explícitamente, política poco clara |
| 20 | **Private Internet Access** | 1.8 | Acceso privado a Internet INC. | E.E.U.U | Protocolo soportado | Protocolo no soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo soportado | No Gratuita ni Libre | n/a | 40 dólares | Tarjeta de crédito/débito, PayPal, criptomoneda, Monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |

| N° | PRODUCTO | | | | PROTOCOLOS | | | | | | | PAGOS | | | | BUSQUEDA | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Software | Última Versión | Administrador | Servidor Central | OPENVPN | IKEv2/ IPSec | L2TP/ IPSec | PPT | SSTP | SSH | WireGuard | Prueba Libre/Gratuita | Tiempo de utilidad / Limitaciones | Valor del software | Modo de Pago | Sin Búsqueda de trafico | Sin Búsqueda de ancho de banda | Sin Búsqueda de direcciones IP |
| 21 | Private Tunnel | 2.8 | OpenVPN Technologies INC. | E.E.U. U | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Gratuito | 7 días | 48 dólares | Tarjeta de crédito/débito, PayPal, Monederos digitales | No hay datos registrados | Datos registrados | Datos registrados |
| 22 | PrivateVPN | 2.3 | Private Kommunikation Sverige AB | Suecia | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 50 dólares | Tarjeta de crédito/débito, PayPal, criptomoneda | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 23 | ProtonVPN | 1.13 | Proton TechnologiesAG | Suiza | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | 3 ubicaciones, 1 dispositivo, límite de velocidad | 96 dólares | Tarjeta de crédito/débito, PayPal, criptomoneda | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 24 | PureVPN | 7.1 | GZ Systems LTD. | Hong Kong | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 70 dólares | Tarjeta de crédito/débito, PayPal | No hay datos registrados | Datos registrados | No hay datos registrados |
| 25 | SaferVPN | 5.0 | Safer Social LTD. | Israel | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 66 dólares | Tarjeta de crédito/débito, PayPal, criptomoneda | No hay datos registrados | Datos registrados | No hay datos registrados |
| 26 | StrongVPN | 2.4 | Strong Technology LLC | E.E.U. U | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo soportado | Protocolo no soportado | Protocolo soportado | No Gratuita ni Libre | n/a | 70 dólares | Tarjeta de crédito/débito, PayPal, Monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 27 | Surfshark | 2.6 | Surfshark LTD. | Islas Vírgenes Británicas | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 77 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda, monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 28 | TorGuard | 3.98 | VP Networks LLC | E.E.U.U | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Gratuito | 7 días | 60 dólares | Tarjeta de crédito/débito, transferencia bancaria, criptomoneda, monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |

| N° | PRODUCTO | | | | PROTOCOLOS | | | | | | | PAGOS | | | | BUSQUEDA | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Software | Última Versión | Administrador | Servidor Central | OPENVPN | IKEv2/ IPSec | L2TP/ IPSec | PPT | SSTP | SSH | WireGuard | Prueba Libre/Gratuita | Tiempo de utilidad /Limitaciones | Valor del software | Modo de Pago | Sin Búsqueda de trafico | Sin Búsqueda de ancho de banda | Sin Búsqueda de direcciones IP |
| 29 | **Trust.Zone VPN** | 1.1. | Trusted Solutions LTD. | Seychelles | Protocolo soportado | Protocolo no soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 94 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda,monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 30 | **TunnelBear** | 4.1 | TunnelBear INC. | Canadá | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | 500 MB de datos por mes | 60 dólares | Tarjeta de crédito/débito, criptomoneda | No hay datos registrados | Datos registrados | No hay datos registrados |
| 31 | **VPNSecure** | 2.1 | VPNSecure Pty LTD. | Australia | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo soportado | Protocolo no soportado | Protocolo soportado | Protocolo no soportado | Gratis | 30 días, 1 Ubicación en EE. UU. solamente, 2 GB durante el período de prueba | 80 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda,monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 32 | **VPN Unlimited** | 7.0 | KeepSolid INC. | E.E.U.U | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo soportado | Gratuito | 7 días | 60 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda, monederos digitales | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 33 | **VyprVPN** | 3.3 | Golden Frog GmbH | Suiza | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | No Gratuita ni Libre | n/a | 45 dólares | Tarjeta de crédito/débito, PayPal | No hay datos registrados | No hay datos registrados | No hay datos registrados |
| 34 | **Windscribe** | 1.83 | Windscribe LTD | Canadá | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | 10 ubicaciones, 2 GB de datos al mes | 49 dólares | Tarjeta de crédito/débito, PayPal, transferencia bancaria, criptomoneda, monederos digitales | No hay datos registrados | Datos registrados | No hay datos registrados |
| 35 | **ZenMate VPN** | 5.0 | ZenGuard GmbH | Alemania | Protocolo soportado | Protocolo soportado | Protocolo soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Protocolo no soportado | Libre | 4 ubicaciones, límite de velocidad de 2 MB/s, solo extensión del navegador | 40 dólares | Tarjeta de crédito/débito, PayPal, Transferenciabancaria | No hay datos registrados | No hay datos registrados | No hay datos registrados |

VPN Report 2020 – 35 Services, Av comparatives, 2020

Anexo 4 Instrumento de recolección de datos

## A) Throughput

Tabla 62 Medición del throughput

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | Fecha / / | 01 |
|---|---|---|---|
| **Responsables** | 1. | | |
| | 2. | | |
| **Especialista** | | | |
| **Titulo** | | | |
| **Indicador a medir** | **Throughput** | | |

| N° | Software VPN | Tamaño total de paquetes (bits) | Tiempo transcurrido (segundos) | Paquetes total recibido (bits) | Resultado |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |

## B) Velocidad de transferencia

Tabla 63 Velocidad de transferencia de datos

| UNIVERSIDAD PRIVADA CESAR VALLEJO | | Fecha / / | 02 |
|---|---|---|---|
| **Responsables** | 1. | | |
| | 2. | | |
| **Especialista** | | | |
| **Titulo** | | | |
| **Indicador a medir** | | | |

| Velocidad de subida | | | | |
|---|---|---|---|---|
| **N°** | **Software VPN** | **Tamaño total de paquetes (bits)** | **Tiempo total transcurrido** | **Resultado** |
| **1** | | | | |
| **2** | | | | |

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | Fecha / / | 03 |
|---|---|---|---|
| **Responsables** | 1. | | |
| | 2. | | |
| **Especialista** | | | |
| **Titulo** | | | |
| **Indicador a medir** | | | |

| Velocidad de descarga | | | | |
|---|---|---|---|---|
| **N°** | **Software VPN** | **Tamaño total de paquetes (bits)** | **Tiempo total transcurrido** | **Resultado** |
| **1** | | | | |
| **2** | | | | |

## C) Evasiones a las políticas de filtro y marcado de trafico

Tabla 64 Porcentaje de evasiones a las políticas de filtro y marcado de tráfico URL

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | Fecha / / | 04 |
|---|---|---|---|
| **Responsables** | 1. | | |
| | 2. | | |
| **Especialista** | | | |
| **Titulo** | | | |
| **Indicador a medir** | **Evasiones a las políticas de filtro y marcado de trafico** | | |

| N° | Software VPN | Total de políticas | Cantidad evasiones detectadas | Cantidad de políticas cumplidas | Resultado |
|---|---|---|---|---|---|
| **1** | | | | | |
| **2** | | | | | |
| **3** | | | | | |
| **4** | | | | | |
| **5** | | | | | |

## D) Fugas DNS

Tabla 65 Porcentaje de fugas DNS

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | | | Fecha / / | 05 |
|---|---|---|---|---|---|
| **Responsables** | 1. | | | | |
| | 2. | | | | |
| **Especialista** | | | | | |
| **Titulo** | | | | | |
| **Indicador a medir** | **Fugas DNS real** | | | | |
| **Fugas DNS real** | | | | | |
| **N°** | **Cantidad de actividades registradas** | **Actividades registradas con DNS real** | | **Resultados** | |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| **Fugas DNS del VPN** | | | | | |
| N° | Software VPN | Cantidad de actividades registradas | Actividades registradas con DNS del VPN | Resultado | |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |

## E) Fugas de direcciones IP

Tabla 66 Porcentaje de fugas de direcciones IP

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | Fecha / / | 06 |
|---|---|---|---|
| Responsables | 1. | | |
| | 2. | | |
| Especialista | | | |
| Titulo | | | |
| Indicador a medir | | | |

| Fugas de Direcciones IP real | | | |
|---|---|---|---|
| N° | Cantidad de actividades registradas | Actividades registradas con dirección IP real | Resultado |
| 1 | | | |
| 2 | | | |
| 3 | | | |

| Fugas de direcciones IP del VPN | | | | |
|---|---|---|---|---|
| N° | Software VPN | Cantidad de actividades registradas | Actividades registradas con dirección IP del VPN | Resultado |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |

## F) Fugas de WebRTC

Tabla 67 Porcentaje de fugas de WebRTC

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | Fecha / / | 07 |
|---|---|---|---|
| **Responsables** | 1. | | |
| | 2. | | |
| **Especialista** | | | |
| **Titulo** | | | |
| **Indicador a medir** | | | |

| Fugas de webRTC | | | |
|---|---|---|---|
| **N°** | **Cantidad de actividades registradas** | **Actividades registradas con webRTC** | **Resultados** |
| 1 | | | |
| 2 | | | |
| 3 | | | |

| Fugas de webRTC del VPN | | | | |
|---|---|---|---|---|
| **N°** | **Software VPN** | **Cantidad de actividades registradas** | **Actividades registradas con webRTC del VPN** | **Resultado** |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |

## G) Encriptamiento de datos

Tabla 68 Velocidad de encriptamiento de datos

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | | | Fecha / / | 08 |
|---|---|---|---|---|---|
| Responsables | 1. | | | | |
| | 2. | | | | |
| Especialista | | | | | |
| Titulo | | | | | |
| Indicador a medir | Velocidad de encriptamiento de datos | | | | |
| **N°** | **Software VPN** | **Tamaño total de paquetes (bits)** | **Tiempo total de encriptamiento transcurrido** | **Velocidad** | |
| 1 | | | | | |
| 2 | | | | | |

## H) Desencriptamiento de datos

Tabla 69 Velocidad de desencriptamiento de datos

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | | | Fecha / / | 09 |
|---|---|---|---|---|---|
| Responsables | 1. | | | | |
| | 2. | | | | |
| Especialista | | | | | |
| Titulo | | | | | |
| Indicador a medir | Velocidad de desencriptamiento de datos | | | | |
| **N°** | **Software VPN** | **Tamaño total de paquetes (bits)** | **Tiempo total de desencriptamiento transcurrido** | **Velocidad** | |
| 1 | | | | | |
| 2 | | | | | |

## I) Consumo de CPU; Consumo de memoria RAM; Consumo de Disco Duro

Tabla 70 Consumo de recursos (CPU, memoria RAM, Disco Duro)

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | | | Fecha / / | 10 |
|---|---|---|---|---|---|
| **Responsables** | 1. | | | | |
| | 2. | | | | |
| **Especialista** | | | | | |
| **Titulo** | | | | | |
| **Indicador a medir** | | | | | |
| **Consumo del CPU** | | | | | |
| **N°** | **Operación realizada** | **Número de registros** | **Tamaño de registro** | **Porcentaje de uso** | |
| 1 | | | | | |
| 2 | | | | | |
| **Consumo de memoria RAM** | | | | | |
| **N°** | **Operación realizada** | **Número de registros** | **Tamaño de registro** | **Porcentaje de uso** | |
| 1 | | | | | |
| 2 | | | | | |
| **Consumo de Disco Duro** | | | | | |
| **N°** | **Operación realizada** | **Número de registros** | **Tamaño de registro** | **Porcentaje de uso** | |
| 1 | | | | | |
| 2 | | | | | |

## J) Ancho de banda

Tabla 71 Ancho de banda

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | | Fecha / / | 11 |
|---|---|---|---|---|
| Responsables | 1. | | | |
| | 2. | | | |
| Especialista | | | | |
| Titulo | | | | |
| Indicador a medir | Ancho de banda | | | |
| N° | Software VPN | Capacidad de ancho de banda | | |
| 1 | | | | |
| 2 | | | | |

## K) Jitter

Tabla 72 Jitter

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | | | | Fecha / / | 12 |
|---|---|---|---|---|---|---|
| Responsables | 1. | | | | | |
| | 2. | | | | | |
| Especialista | | | | | | |
| Titulo | | | | | | |
| Indicador a medir | Jitter | | | | | |
| N° | Software VPN | Tamaño total de paquetes (bits) | Retraso(N1) | Retraso(N2) | Resultado | |
| 1 | | | | | | |
| 2 | | | | | | |

## L) Latencia

Tabla 73 Latencia

| UNIVERSIDAD PRIVADA CÉSAR VALLEJO | | | Fecha / / | 13 |
|---|---|---|---|---|
| **Responsables** | 1. | | | |
| | 2. | | | |
| **Especialista** | | | | |
| **Titulo** | | | | |
| **Indicador a medir** | **Latencia** | | | |
| **N°** | **Software VPN** | **Operación realizada** | **Tiempo de retraso en la conexión** | |
| **1** | | | | |
| **2** | | | | |
| **3** | | | | |
| **4** | | | | |
| **5** | | | | |

## 1. Finalidad de la metodología

La finalidad de la metodología es evaluar el rendimiento de software de redes privadas virtuales gratuitos/libres y licenciadas.

## 2. Limitación de la metodología

La limitación de la metodología establece la evaluación de rendimiento de los softwares de redes privadas virtuales gratuitos/libres y licenciadas en base a criterios, tales como: (a) rendimiento d software, (b) administración de recursos y desempeño en la red. Asimismo, es necesario tener conocimiento sobre las cualidades técnicas y funcionales del software de red privada virtual para realizar correctamente las pruebas de evaluación. La información a indagar será enfocada a la evaluación de software de redes privadas virtuales gratuitos/libres y licenciados a medir y comparar, por ello es necesario los siguientes pasos:

- Analizar modelos de aplicación y gestión de softwares de redes privadas virtuales gratuitos/libres y licenciadas que contemplen: (a) características y descripciones de las redes privadas virtuales, (b) procedimientos necesarios para la instalación de los softwares de redes privadas virtuales, (c) procesos para la gestión de los softwares de redes privadas y (d) configuración básica.

- Revisar los conceptos y procesos de configuración de seguridad en los softwares de redes privadas virtuales.

- Revisar técnicas para determinar la existencia de fugas de datos (DNS – IP - WebRTC) y seguridad de información.

- Revisar las herramientas necesarias para ejecutar las pruebas de rendimiento referente a: (i) rendimiento de software, (ii) administración de recursos y (iii) desempeño en la red las mismas que fueron descritas en el presente estudio de investigación.

- Considerar estándares y/o normas de seguridad de información relacionadaa redes privadas virtuales.

### 3. Clasificar y seleccionar los softwares de redes privadas virtuales

En la implementación de la presente metodología se realizó una tabla de clasificación de los softwares de redes privadas virtuales teniendo en cuenta las investigaciones relacionadas al estudio planteado, las mismas que han sido detalladas en el Anexo 4. Según Phelan (2019) mencionó que los principales softwares VPNs son: ExpressVPN, TunnelBear, NordVPN e Invincibull. Por otro lado, Dutkowska, Hounsel, Xiong, Roberts, Stewart, Chetty y Feamster (2020) indicaron que entre la variedad de softwares VPN licenciados populares destacan: ExpressVPN, Private Internet Access y NordVPN; mientras que entre los softwares VPN gratuitos/libres populares destacan: Hotspot Shield, TunnelBear, Hola y Betternet. (Dutkowska et al., 2020, p. 8). Por ende, se tomó la decisión de elegir los siguientes softwares VPNs: (a) ProtonVPN (libre), (b) TunnelBear (gratuito), (c) NordVPN (licenciado).

### ENTRADAS

En la presente metodología se requiere entradas de información establecidas por los softwares de redes privadas virtuales extraídos de investigaciones, paginas oficiales, revistas, estándares y políticas acerca de los softwares VPNs. Asimismo, para realizar la evaluación es necesario que los procesos se cumplan, tales como: Identificar indicadores/parámetros de evaluación, Determinar las herramientas tecnológicas de evaluación, Detallar especificaciones técnicas y funciones de los sujetos de prueba y Habilitar el escenario de pruebas de la metodología con el fin de poder ejecutar los procedimientos de la metodología MEPVPNS.

A. Para “**Identificar indicadores/parámetros de evaluación**” es necesario las siguientes actividades:

a) Identificar indicadores/parámetros propios del software VPN.
b) Identificar indicadores/parámetros generales de software.
c) Revisar los conceptos de los indicadores.
d) Verificar los indicadores y parámetros en base de estudios de evaluación de rendimiento.
e) Identificar fórmulas para medir el rendimiento de los indicadores.
f) Identificar fórmulas para medir el rendimiento de los indicadores.

g) Verificar la validez de las fórmulas.

B. Para **“Determinar las herramientas tecnológicas de evaluación”** es necesario las siguientes actividades:

a) Identificar sobre los tipos de sistemas de detecciones de intrusos (IDS).
b) Identificar sobre los tipos de sistemas de prevención de intrusos (IDS).
c) Revisar los procesos sniffing.
d) Revisar los procesos SNMP (Protocolo simple de administración de red).
e) Identificar las vulnerabilidades informáticas en los sistemas.
f) Identificar de ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuido (DoSS).
g) Registrar de herramientas tecnológicas en base criterios de evaluación en el sistema y en la red.
h) Verificar la efectividad de las herramientas elegidas para las pruebas de evaluación.

C. Para “**Detallar especificaciones técnicas y funciones de los sujetos de prueba”** las siguientes actividades:

a) Revisar guías técnicas para ensamblaje de los equipos tecnológicos
b) Identificar los componentes hardware de cada sujeto de prueba.
c) Verificar el buen estado de los componentes de hardware.
d) Especificar las funciones a realizar para los sujetos de prueba.

D. Para “**Habilitar el escenario de pruebas de la metodología**” es necesario las siguientes actividades:

a) Asegurar los recursos necesarios para las pruebas de rendimiento.
b) Asegurar que las características técnicas muestren semejanza para los sujetos de prueba.
c) Asegurar que los sistemas operativos y/o herramientas mantengan una funcionalidad correcta.
d) Especificar la topología de red empleada para las pruebas de rendimiento.
e) Realizar pruebas de conectividad entre el IPS (proveedor de internet) y sujetos de prueba.
f) Asegurar la red LAN entre dispositivos en el escenario de pruebas.

**PROCESOS**

En el siguiente grafico muestra resumir la secuencia de procesos para el desarrollo de la metodología MEPVPNS, asociados a subprocesos que permitirán el objetivo del proceso:

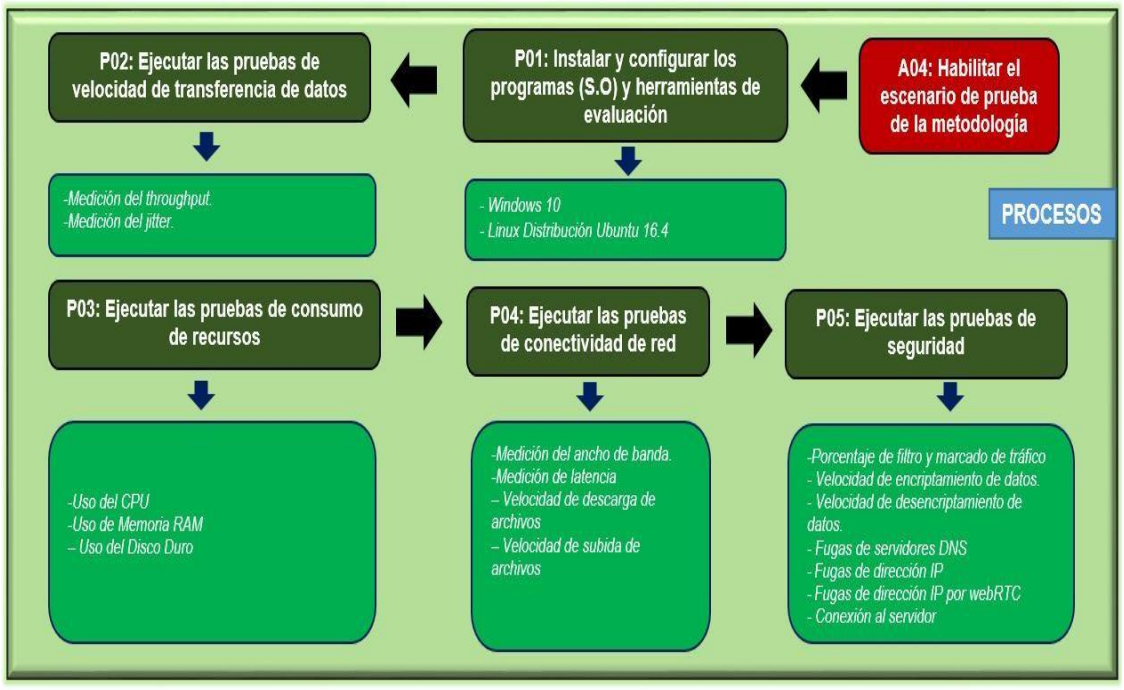


Figura 2 Procesos de la metodología MEPVPNS

Las actividades de la metodología MEPVPNS, son las siguientes:

A. Para el P01, "**Instalar y configurar los programas (S.O) y herramientas de evaluación**", es necesario seguir estas actividades:

a) Revisar las últimas versiones de los sistemas operativos y distribuciones para los sujetos de prueba.
b) Revisar guías, cursos y videos técnicos para la instalación y configuración de los sistemas operativos.
c) Instalación de los sistemas operativos, tales como: Windows, Linux (Ubuntu 16.4).
d) Revisar guías y videos técnicos para la instalación configuración de las herramientas de evaluación de rendimiento.
e) Instalación de herramientas de evaluación, tales como: Jperf, Wireshark, Nessus, Paessler, Snom, etc.

f) Instalación de las herramientas de detección y prevención de intrusos., tales como: Snort, Nessus, etc.

B. Para el P02, "**Ejecutar las pruebas de velocidad de transferencia de datos**", es necesario seguir estas actividades:

a) Revisar guías y/o videos técnicos para la evaluación del throughput.
b) Evaluar los pasos para la medición del throughput, esto engloba implementar los procedimientos P02, del anexo 7.
c) Desarrollar los pasos necesarios para la evaluación del throughput y recolectar los resultados en la herramienta de tabulación de datos
d) Revisar guías y/o videos técnicos para la evaluación del jitter.
e) Evaluar los pasos para la medición del jitter, esto engloba implementar los procedimientos P02, del anexo 7.
f) Desarrollar los pasos necesarios para la evaluación del jitter y recolectar los resultados en la herramienta de tabulación de datos

C. Para el P03, "**Ejecutar las pruebas de consumo de recursos**", es necesario seguir estas actividades:

a) Revisar guías y/o videos técnicos acerca de los ataques informáticos Hping, byte-DDoS, DDoS-Anonymous, Hammer, UDP flooder, SMG DOSER, LOIC (Low Orbit Ion Cannon), bats y el Ufonet (Botnet).
b) Evaluar los pasos para la ejecución de ataques informáticos, esto engloba implementar los procedimientos P03, del anexo 7.
c) Revisar guías y/o videos técnicos para la evaluación del consumo de CPU.
d) Evaluar los pasos para la medición del consumo de CPU, esto engloba implementar los procedimientos P03, del anexo 7.
e) Desarrollar los pasos necesarios para la evaluación del consumo de CPU y recolectar los resultados en la herramienta de tabulación de datos
f) Revisar guías y/o videos técnicos para la evaluación del consumo de memoria RAM.
g) Evaluar los pasos para la medición del consumo de memoria RAM, esto engloba implementar los procedimientos P03, del anexo 7.

h) Desarrollar los pasos necesarios para la evaluación del consumo de memoria RAM y recolectar los resultados en la herramienta de tabulación de datos.
i) Revisar guías y/o videos técnicos para la evaluación del consumo de disco duro.
j) Evaluar los pasos para la medición del consumo de disco duro, esto engloba implementar los procedimientos P03, del anexo 7.
k) Desarrollar los pasos necesarios para la evaluación del consumo de disco duro y recolectar los resultados en la herramienta de tabulación de datos

D. Para el P04, **"Ejecutar las pruebas de conectividad de red"**, es necesario seguir estas actividades:

a) Revisar guías y/o videos técnicos para la evaluación de la latencia.
b) Evaluar los pasos para la medición de la latencia, esto engloba implementar los procedimientos P04, del anexo 7.
c) Desarrollar los pasos necesarios para la evaluación de la latencia y recolectar los resultados en la herramienta de tabulación de datos
d) Revisar guías y/o videos técnicos para la evaluación de la velocidad de descarga/subida de archivos.
e) Evaluar los pasos para la medición de la velocidad de descarga/subida de archivos, esto engloba implementar los procedimientos P04, del anexo 7.
f) Desarrollar los pasos necesarios para la evaluación de velocidad de descarga/subida de archivos y recolectar los resultados en la herramienta de tabulación de datos
g) Revisar guías y/o videos técnicos para la evaluación del ancho de banda real de archivos en la red.
h) Evaluar los pasos para la medición del ancho de banda real de archivos en la red, esto engloba implementar los procedimientos P04, del anexo 7.
i) Desarrollar los pasos necesarios para la evaluación del ancho de banda real de archivos en la red y recolectar los resultados en la herramienta de tabulación de datos.

E. Para el P05, **“Ejecutar las pruebas de seguridad”**, es necesario seguir estas actividades:

a) Revisar guías y/o videos técnicos para la evaluación del filtro y marcado de trafico de red.
b) Evaluar los pasos para la medición del filtro y marcado de trafico de red, esto engloba implementar los procedimientos P05, del anexo 7.
c) Desarrollar los pasos necesarios para la evaluación del filtro y marcado de trafico de red y recolectar los resultados en la herramienta de tabulación de datos
d) Revisar guías y/o videos técnicos para la evaluación de la velocidad de encriptamiento/desencriptamiento de datos.
e) Evaluar los pasos para la medición de la velocidad de encriptamiento/desencriptamiento de datos, esto engloba implementar los procedimientos P05, del anexo 7.
f) Desarrollar los pasos necesarios para la evaluación de la velocidad de encriptamiento/desencriptamiento de datos y recolectar los resultados en la herramienta de tabulación de datos
g) Revisar guías y/o foros técnicos para la evaluación de fugas de servidores DNS – dirección IP – dirección IP por WebRTC.
h) Evaluar los pasos para la medición de fugas de servidores DNS – dirección IP – dirección IP por WebRTC, esto engloba implementar los procedimientos P05, del anexo 7.
i) Desarrollar los pasos necesarios para la evaluación de fugas de servidores DNS – dirección IP – dirección IP por WebRTC y recolectar los resultados en la herramienta de tabulación de datos.
j) Revisar guías y/o videos técnicos para la evaluación del tiempo de conexión al servidor.
k) Evaluar los pasos para la medición del tiempo de conexión al servidor, esto engloba implementar los procedimientos P05, del anexo 7.
l) Desarrollar los pasos necesarios para la evaluación del tiempo de conexión al servidor y recolectar los resultados en la herramienta de tabulación de datos.

Anexo 5 Contrastación de metodologías existentes Tabla 74 Comparación de metodologías existentes

| N° | Estudios | Autores | Finalidad | Características | Etapas | Pruebas | Resultados |
|---|---|---|---|---|---|---|---|
| **1** | Metodología para evaluar la Calidad de Servicio de las Telecomunicaciones **(Roberto Moreano, 2010).** | Roberto Moreano | En la investigación de Moreno (2010) tiene como finalidad desarrollar una metodología para adquirir una afinidad satisfactoria entre el nivel de servicio de calidad del proveedor y el nivel de servicio de calidad apreciada por el usuario.<br><br>**(Roberto Moreano, 2010).** | Tiene como criterio deevaluación:<br>1. Velocidad<br>2. Precisión<br>3. Disponibilidad<br>4. Fiabilidad<br>5. Seguridad<br>6. Simplicidad<br>7. Flexibilidad<br><br>**(Roberto Moreano, 2010).** | 1. Conceptos de calidad de servicio.<br>2. Relación de los cuatro puntos devista sobre calidad de servicio.<br>3. Criterios del servicio de calidad<br>4. resultados<br><br>**(Roberto Moreano, 2010).** | 1. Velocidad<br>2. Precisión<br>3. Disponibilidad<br>4Fiabilidad<br>5. Seguridad<br>6. Simplicidad<br>7. Flexibilidad<br><br>**(Roberto Moreano, 2010).** | El modelo G.1000 es un componente crucial, debido a que facilita la determinación de lasincidencias vinculada alQoS, además, mide las incidencias desde el puntode vista del cliente y del proveedor. Asimismo, seobserva criterios que ayudan en los procesos de calidad de servicio entre ellos destaca los requerimientos de los usuarios. **(Roberto Moreano, 2010).** |
| **2** | Metodología para la Evaluaciónde Servicios de Telecomunicación desde la Perspectiva del Usuario**(Bellido, López, Gonzáles y López, 2004)** | 1. LuisBellido,<br>2. Jorge Lópezde Vergara<br>3. FranciscoGonzález<br>4. DavidLópez | En el estudio de Bellido,Lopez, Gonzáles y López (2004) tiene como finalidad desarrollar una metodología para simplificar la evaluación delos servicios de las TIC desde el punto de vista delusuario **(Bellido, López, Gonzáles y López, 2004).** | Tiene como criterio deevaluación:<br>1. Gestión en la transferencia de datos.<br>2. Administración de los servicios principales.<br>3. Gestión del valor agregado<br>4. Gestión de audio - video digital.<br>**(Bellido, Lopez, Gonzáles y López, 2004).** | 1. Planificación<br>2. Clasificación de servicios.<br>3. Relación de entre usuarios y servicios del proveedor<br>4. Plataforma de medición de calidad de servicio.<br>**(Bellido, Lopez,Gonzáles y López, 2004).** | 1. Marco de datos.<br>2. Recursos terciarios con acceso a la red.<br>3. Puntos de vista acerca de la calidad del servicio<br>**(Bellido, Lopez,Gonzáles y López, 2004).** | Se realizó una comparación entre normalizaciones y propuestas con relación a la evaluación de la calidad de servicio. Además, se llegó a concluir que los clientes optan por sistemas didácticos y de fácil entendimiento<br>**(Bellido, Lopez, Gonzáles y López, 2004)** |

| N° | Estudios | Autores | Finalidad | Características | Etapas | Pruebas | Resultados |
|---|---|---|---|---|---|---|---|
| **3** | Método de evaluación y selección de herramientas de simulación de redes **(García, Escobar,Navarro y Vásquez, 2011)** | 1. Alexander García Dávalos<br>2. Lina Marcela Escobar Paz<br>3. AndrésNavarro Cadavid<br>**4.** Andrés Vásquez Mejía. **(García, Escobar, Navarro yVásquez,2011)** | En el estudio de García,Escobar, Navarro y Vásquez (2011) tiene como finalidad proponer un nuevo método de evaluación y selección basado en dos elementos claves: la norma ISO/IEC 9126-1 **(García, Escobar, Navarro y Vásquez, 2011)** | Tiene como criteriosde evaluación: (a)Funcionalidad, (b)Confiabilidad, (c)Eficiencia, (d)Mantenimiento, (e)Portabilidad **(García, Escobar,Navarro y Vásquez,2011)** | 1. Especificación<br>2. Marco de evaluación para herramientas de prueba<br>3. Evaluación de las herramientas software<br>4. Implementación y seguimiento del cuestionario mediante GoogleDocs.<br>5. Observación y evaluación de los resultados **(García, Escobar, Navarro y Vásquez, 2011)** | 1. Apoyo en elmanejo de las herramientas<br>2. Escalabilidad<br>**3.** Adaptación a múltiples topologías y recursos de red **(García, Escobar, Navarro y Vásquez, 2011)** | En síntesis, la herramientaNS-2 muestra una mejoradopción por parte de los usuarios, debido a queposee un mayor número de modelos disponibles y gran cantidad de información en línea acerca de su configuración y uso. Por otrolado, la herramienta NCTUns es un motor de simulación capaz de ofrecer soportepara la adopción de nuevos modelos y alteración de los protocolos. **(García, Escobar, Navarro y Vásquez, 2011)** |
| **4** | Metodología integral para evaluar el rendimiento de firewalls **(Pacotaype, 2018)** | 1. Rogelio Joseph Pacotaype Huaman **(Pacotaype, 2018)** | Evaluar el rendimiento de Firewalls de hardware y software **(Pacotaype, 2018)** | Tiene como criteriosde evaluación:Desempeño en la red,eficacia de laseguridad (evaluación de políticas) yconsumo de recursos **(Pacotaype, 2018).** | 1. Planeamiento<br>2. Implementación y pruebas<br>**3.** Análisis de Resultados **(Pacotaype, 2018)** | 1. Throughput<br>2. Latencia<br>3. Filtrado web<br>4. Archivos Malicioso<br>5. Consumo de memoria RAM<br>6. Consumo de CPU **(Pacotaype, 2018)** | La aplicación de una metodología para la evaluación de rendimiento de Firewalls sí permite determinar que los Firewalls de hardware (Paloalto y Fortinet) tienen mayor rendimiento que los Firewalls de software (Endian y Sophos) **(Pacotaype, 2018)** |

| N° | Estudios | Autores | Finalidad | Características | Etapas | Pruebas | Resultados |
|---|---|---|---|---|---|---|---|
| 5 | MEPES: Methodology for Evaluating the Performance of E-Mail Servers**(Torres y Alfaro, 2018)** | 1. Pedro Alexis TorresCalderón **2.** Emigdio Antonio AlfaroParedes **(Torres y Alfaro, 2018)** | El propósito del estudio fue desarrollar una metodología integrada para evaluar el rendimiento de los servidores de correo electrónico y aplicarla paradeterminar si dos servidores de correo electrónico basados en software libre funcionan mejor que dos servidores de correo electrónico con licencia de pago **(Torres y Alfaro, 2018)** | Tiene como criterio de evaluación: Mensajes de correo electrónico spam Consumo de RAMConsumo de CPU **(Torres y Alfaro, 2018)** | 1. procedimiento 1: seleccionar servidores de correoelectrónico 2. Procedimiento 2: para identificar criterios de rendimiento paraservidores de correo electrónico y parámetros de medición **3.** Procedimiento 3: para definir las características técnicas del sujetode medición y lasaplicaciones pararealizar las pruebasde rendimiento delos servidores decorreo electrónico **(Torres y Alfaro,2018)** | 1. Mensajes de correo 2. Consumo de CPU **3.** Consumo de RAM **(Torres y Alfaro, 2018)** | se puede concluir, que la aplicación de una metodología para evaluar el desempeño de losservidores de correo electrónico permitió establecer que los dos servidores de correo electrónico implementados con software libre (Sendmaily Postfix) tienen un mayor rendimiento que los dos servidores de correo con licencia (MS Exchange y Lotus) **(Torres y Alfaro, 2018)** |
| 6 | Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas **(Carrión, 2018)** | Gilberto Carrión Barco | Elaborar una metodología adaptativa basada en unmodelo de seguridad informática en redes privadas virtuales para la Universidad Nacional Pedro Ruiz Gallo quepermita mejorar el intercambio de información académica contextualizada en unentorno de conexionespúblicas **(Carrión, 2018)** | Tiene como criterio deevaluación: Tipos deusuarios Requerimientos yservicios de redTopología de Red Componentes de lainfraestructura tecnológica de la redRiesgos. Políticas deseguridad. Protocolosde seguridad **(Carrión, 2018)** | Etapa 1: dimensiónde la gestión de conectividad de la Etapa 2: dimensiónde la gestión deseguridad informática Etapa 3: seguimientoy control **(Carrión, 2018)** | 1- Tipos de usuarios2- Requerimientos y servicios de red 3- Topología de Red 4- Componentes de la infraestructura tecnológica de la red5- Riesgos 6- Políticas de seguridad 7- Protocolos de seguridad **(Carrión, 2018)** | Como resultado de la investigación, se logró determinar que IKEv2 tenía un resultado significativamente mejor conrespecto al SSTP en relación con el rendimiento, la fluctuación de fase y el retardo **(Carrión, 2018)** |

| N° | Estudios | Autores | Finalidad | Características | Etapas | Pruebas | Resultados |
|---|---|---|---|---|---|---|---|
| **7** | Estudio del comportamiento devulnerabilidades de una red privada virtual (VPN) **(Hurtado y Ponce, 2013)** | 1. Hurtado Calvillo, Wilmer Daniel **2.** Ponce Rivas, SergioLuis **(Hurtado y Ponce, 2013)** | Estudios de comportamientos de lasvulnerabilidades de seguridad que puede sufrir una red privada virtual (VPN), tráfico de información, ataques DoS **(Hurtado y Ponce, 2013)** | Tiene como criterios de evaluación: Protocolos de las redes privada virtualesy cifrados seguridad **(Hurtado y Ponce, 2013)** | 1. Investigación derecursos de análisis de redes (VPN).<br>2. Estudiar ataques hacia una VPN teórico/practico.<br>3. Instalación de una red de pruebas con conexiones VPN.<br>4. Observación de vulnerabilidades (VPN)<br>**(Hurtado y Ponce, 2013)** | 1. PPTP<br>2. IPsec/L2TP<br>3. Emisora de certificado<br>4. AH<br>5. ESP<br>6. IKEv2<br>7. ISKAMP<br>8. SSH<br>**(Hurtado y Ponce, 2013)** | Se concluyó queanteriormente se debeconfigurar el firewall, si es elpunto final de VPN, parapermitir solo el tráfico seguroa través del túnel VPN **(Hurtado y Ponce, 2013)** |

La metodología MEPVPNS abarca los siguientes aspectos: Finalidad de la metodología (objetivo), Limitaciones de la metodología (alcance), Entradas (información de los recursos necesarios para las pruebas), Procesos de MEPVPNS (evaluaciones de rendimiento) y Salidas (Reportesy contrastaciones de los resultados). Asimismo, se detalla una tabla comparativa de metodologías existentes con el fin de estructurar los procesos sistemáticamente de la metodología MEPVPNS.

Anexo 8 Metodología para evaluar el rendimiento del software de red privada virtual

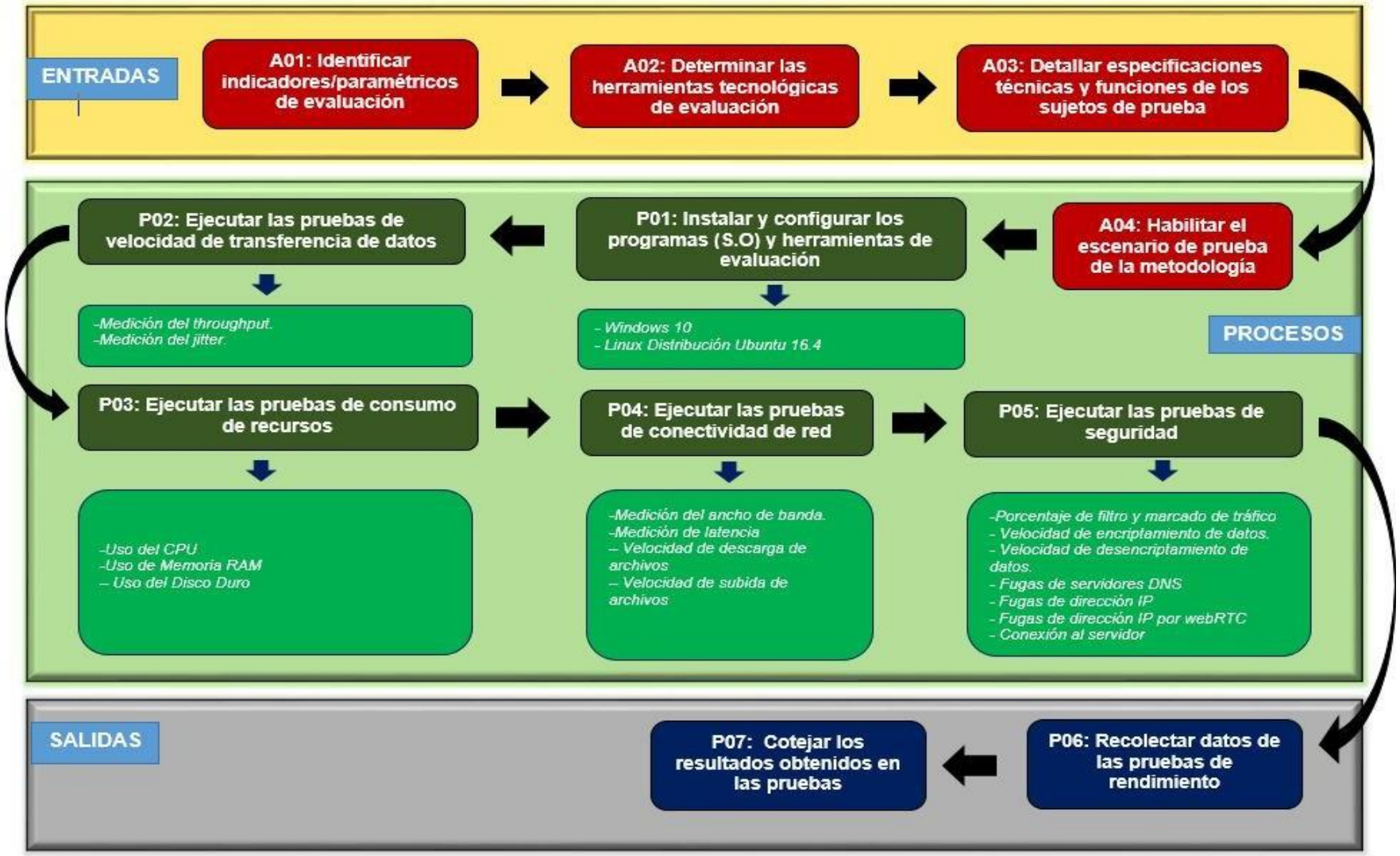


Figura 3 MEPVPNS

## Detección de Intrusos (IDS)

Respecto a las IDS, Thakkar y Lohiya (2021) mencionaron que es capaz de recolectar datos de diferentes partes del sistema de un computador para evaluar la información de la mejor manera, comparando los paquetes de información con enormes bases de datos de ataques cibernéticos y gestionar los incidentes relacionado a los permisos de usuarios autorizados y análisis de variabilidad estadística en datos que demuestre anormalidades que perjudique al sistema (Thakkar y Lohiya, 2021). En síntesis, los IDS son como los firewalls porque detectan retrasos de paquete o incidencias de ataques cibernéticos, analizando las anomalías extraídas de las pruebas de seguridad del sistema (Medina y Rivas, 2020; Leyva y Borroto, 2020; Janampa, Huamani y Meneses, 2021; Mostacero, 2020).

Tabla 75 Clasificación de las Detecciones de Intrusos (IDS)

| PROCESOS IDS | DESCRIPCIÓN |
|---|---|
| **A. Los IDS basados en red** (Dueñas y Bernal, 2019) | Un IDS basado en red controla la información que es transferida a través de la red analizando posibles incidencias en contra delemisor-receptor, además, puede ser ubicado en terminales del sistema, gestionando el tráfico de datos, es por ello que controla a todo sistema relacionado con la red para detectar anomalías o intrusos (Dueñas y Bernal, 2019, p. 19). |
| **B. IDS basados en host** (Dueñas y Bernal, 2019) | Respecto, un IDS basados en host, se enfoca en la seguridad de un solo hardware en base al proceso background mediante los análisis recurrentes para detectar factores que afecte al sistema o se viera afectado por un ciberdelincuente, malware para tomar las estrategias debidas para mantener seguro el sistema (Dueñas y Bernal, 2019, p. 19). |

## Sistema de prevención de intrusos (IPS)

Al respecto, el IPS es una tecnología de seguridad para la trasferencia de datos controlada en la capa 3 y capa 7, con la finalidad de la búsqueda de actividades maliciosas, intrusos o acciones que perjudiquen al sistema, además, realiza un plan de contingencia en base a funciones pre-establecidos en el momento que se logra identificar la anomalía, asimismo, cumple las mismas funciones que un firewall o IDS para mantener el canal de red seguro (Camacho, 2016, p. 15; Farías y Yépez, 2022).

Tabla 76 Clasificación de los Sistemas de prevención de intrusos (IPS)

| CRITERIOS | DESCRIPCIONES |
|---|---|
| **IPS basado en firmas** (Camacho, 2016). | El *IPS basado en firmas* debe disponer de un repositorio de información que contengapautas sobre ataques específicos que puedan afectar al sistema, este procedimiento se desarrolla por medio de una exploración de similitudes para determinar la existencia de una incidencia (Camacho, 2016, p. 15). |
| **IPS basado en** anomalías (Camacho, 2016). | El *IPS basado en anomalías*, también llamado "basado en el perfil" busca reconocer una actividad anormal en la red,tales como: desvió de información o pérdida de datos, asimismo, cabe recalcarque mantiene un enfoque estadístico para encontrar con mayor facilidad anomalías en el sistema (Camacho, 2016, p. 16). |
| **IPS basado en Análisis de Protocolo** (Camacho, 2016). | El *IPS basado en análisis de protocolos,* lleva a cabo un reconocimiento y análisis más exhausto de la información recopiladapara encontrar ataques y alertar al sistema(Camacho, 2016, p. 16). |

### Protocolo Simple de Administración de Red (SNMP)

El SNMP, es aquel protocolo normalizado que gestiona los equipos tecnológicos conectados a una red que emplee el protocolo de internet (IP), además, hay equipos que permiten que el SNMP gestione la red, tales como: conmutador, servidor, fax, impresora, Router y entre otros. Por otro lado, el protocolo simple de administración de red muestra los datos gestionados en forma de parámetros hacia los equipos conectados a la red, que alojan las distribuciones del sistema, asimismo, estos parámetros pueden ser consultados a través de la gestión de los equipos (Hentges y Schorr, 2020).

### Sniffing

Es un procedimiento por el cual el ciberdelincuente extrae datos privados, desde una terminal de red conectado a través de un hardware o software que toma la posición de espía interviniendo la red para sustraer claves, datos, direcciones IP, funciones de los sistemas, email, procesos de ejecución o toda actividad realizada en el computador (Suárez, 2022; Vargas, Guarda, Muyón y Quiña, 2019).

### Vulnerabilidades informáticas

Las vulnerabilidades informáticas son aspectos buscado por los ciberdelincuentes para efectuar estafas y/o robos a través de la red, por lo que un administrador de red siempre debe estar alerta ante anomalías o alteraciones que afecten al sistema. Por ello, los análisis de vulnerabilidades deben ser realizadas por un especialista en redes en conjunta ayuda de herramientas tecnologías para monitorear periódicamente la red y los dispositivos que se encuentran conectados (Zambrano y Valencia, 2017).

## Validez de pruebas de la metodología

Se debe verificar la equidad de los recursos para las pruebas de rendimiento. Con el objetivo de ejecutar las pruebas en un entorno imparcial y ordenado, para la obtención de resultados certeros, asimismo, se empleó software VPN con especificaciones técnicas semejantes.

*Ta*bla 77 Características de software VPN

| Tipo | Software | Compatibilidad | Protocolos |
|---|---|---|---|
| **SOFTWARE GRATUITO** | TunnelBear | Windows, IOS, Android, Mac | OpenVPN, IKEv2/IP-SEC |
| **SOFTWARELI-BRE** | ProtonVPN | Windows, IOS, Android, Mac | OpenVPN, IKEv2/IP-SEC |
| **SOFTWARELI-CENCIADO** | NordVPN | Windows, IOS, Android, Linux, Mac | IKEv2/IPSEC, OpenVPN, Nortlynx |

Los softwares de redes privadas virtuales serán implementados y configurados en los sujetos de prueba (computador) con características similares previamente detallados. La arquitectura del software de redes privadas virtuales que se empleara en la metodología es “RED LAN” la misma que permitirá la simulación de una red compartida entre un mismo entorno. El escenario propuesto será configurado en base a guías, estándares y políticas para la efectividad de las pruebas de software VPN (NIST SP 800-46; Cyber Essentials de CISA; NIST SP 800-113; NIST SP 800-115; NIST SP 800-77; ITL Bulletin; NIST SP 1800; Cyber Security Policy and Standards, 2020; CSA Mitigating Recent VPN Vulnerabilities).

Seguidamente, se detalla el escenario de evaluación donde se llevará a cabo las pruebas de rendimiento para los softwares de redes privadas virtuales. El entorno se encuentra en una red compartida denominada LAN para minimizar el tráfico de datos al momento de realizar dichas pruebas, además todo compartirán el mismo ISP, pero con direcciones IP diferentes empleando el software VPN para medir los indicadores propuesto en el Anexo 4.

Anexo 6 Escenario de pruebas

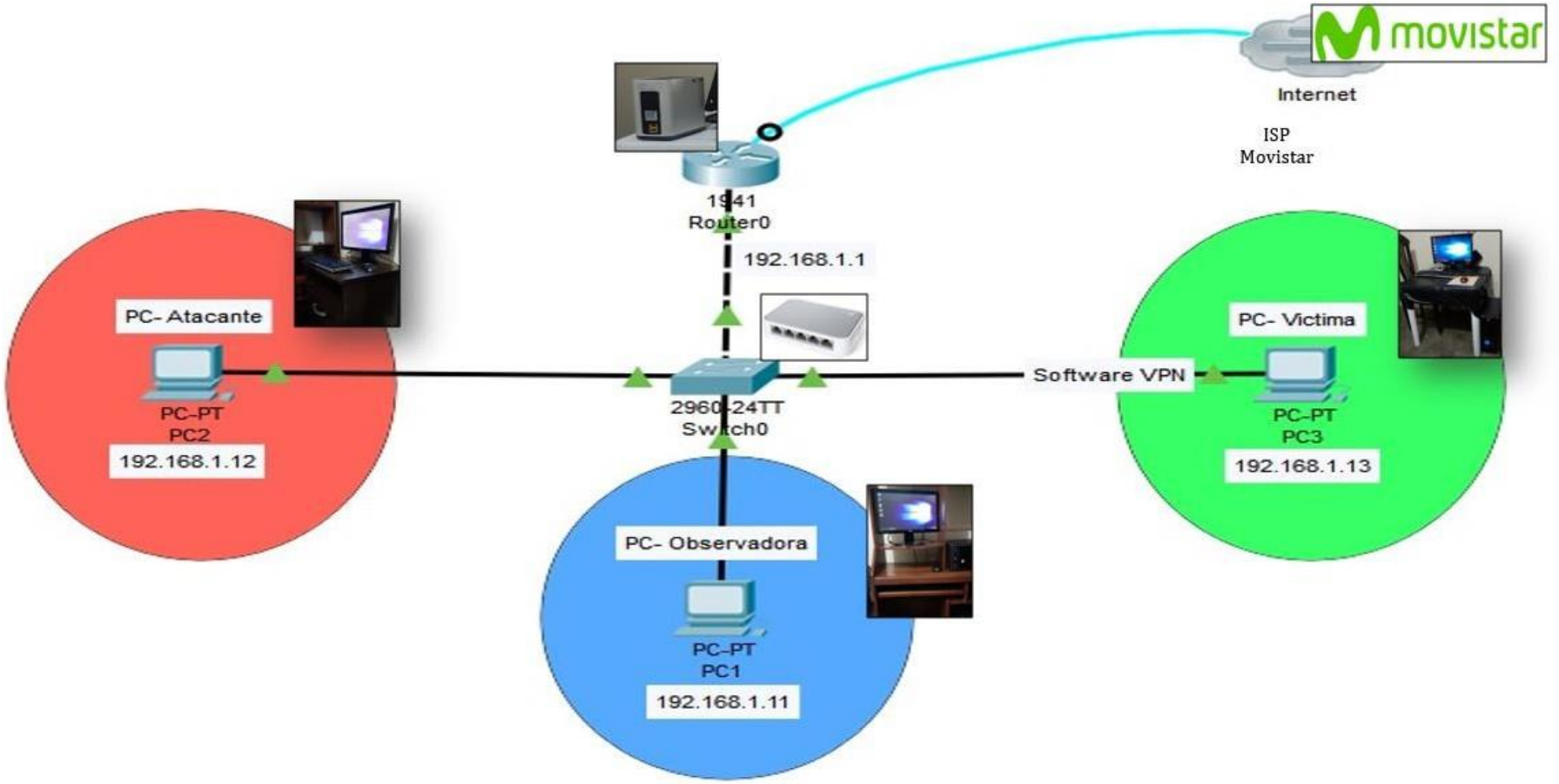


Figura 4 Escenario para las pruebas de rendimiento

El presente diagrama muestra la topología de red LAN que se empleara para evaluar los indicadores de rendimiento enfocado a los softwares de redes privadas virtuales.