,

UNIVERSIDAD ESTATAL DE MILAGRO

FACULTAD CIENCIAS DE LA INGENIERIA

TRABAJO DE TITULACIÓN DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

PROPUESTA PRÁCTICA DEL EXAMEN DE GRADO O DE FIN DE CARRERA (DE CARÁCTER COMPLEXIVO)

INVESTIGACIÓN DOCUMENTAL

TEMA: Análisis de Software en la Implementación de VPN en LAN Inalámbrica

Autores:

Mendoza Guanoquiza Freddy Geovanny

Ortega Quiñonez Adrián Marcel

Acompañante:

Ing. Freddy Lenin Bravo Duarte Mgti.

Milagro, Mayo 2019

ECUADOR

DERECHOS DE AUTOR

Ingeniero.
Fabricio Guevara Viejó, PhD.
RECTOR
Universidad Estatal de Milagro
Presente.

Yo, **MENDOZA GUANOQUIZA FREDDY GEOVANNY** en calidad de autor y titular de los derechos morales y patrimoniales de la propuesta práctica de la alternativa de Titulación – Examen Complexivo: Investigación Documental, modalidad presencial, mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor de la propuesta practica realizado como requisito previo para la obtención de mi Título de Grado, como aporte a la Línea de Investigación **ANÁLISIS DE SOFTWARE EN LA IMPLEMENTACIÓN DE VPN EN LAN INALÁMBRICA** de conformidad con el Art. 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, concedo a favor de la Universidad Estatal de Milagro una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Milagro para que realice la digitalización y publicación de esta propuesta practica en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Milagro, a los 8 días del mes de Mayo del 2019

Firma del Estudiante
MENDOZA GUANOQUIZA FREDDY GEOVANNY
CI: 0941604183

DERECHOS DE AUTOR

Ingeniero.
Fabricio Guevara Viejó, PhD.
RECTOR
Universidad Estatal de Milagro
Presente.

Yo, **ORTEGA QUIÑONEZ ADRIÁN MARCEL** en calidad de autor y titular de los derechos morales y patrimoniales de la propuesta práctica de la alternativa de Titulación – Examen Complexivo: Investigación Documental, modalidad presencial, mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor de la propuesta practica realizado como requisito previo para la obtención de mi Título de Grado, como aporte a la Línea de Investigación **ANÁLISIS DE SOFTWARE EN LA IMPLEMENTACIÓN DE VPN EN LAN INALÁMBRICA** de conformidad con el Art. 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, concedo a favor de la Universidad Estatal de Milagro una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Milagro para que realice la digitalización y publicación de esta propuesta practica en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Milagro, a los 8 días del mes de Mayo del 2019

Adrian Ortega

Firma del Estudiante
ORTEGA QUIÑÓNEZ ADRIÁN MARCEL
CI: 0940724396

APROBACIÓN DEL TRIBUNAL CALIFICADOR

El tribunal calificador constituido por:

Bravo Duarte Freddy Lenin

Cordova Martinez Luis Cristobal

Correa Peralta Mirella Azucena

Luego de realizar la revisión de la Investigación Documental como propuesta practica, previo a la obtención del título (o grado académico) de **INGENIERO EN SISTEMAS COMPUTACIONALES** presentado por el señor **MENDOZA GUANOQUIZA FREDDY GEOVANNY**.

Con el tema de trabajo de Titulación: **ANÁLISIS DE SOFTWARE EN LA IMPLEMENTACIÓN DE VPN EN LAN INALÁMBRICA**.

Otorga a la presente Investigación Documental como propuesta práctica, las siguientes calificaciones:

Investigación documental	[56]
Defensa oral	[14]
Total	[70]

Emite el siguiente veredicto: (aprobado/reprobado) Aprobado

Fecha: 8 de Mayo del 2019.

Para constancia de lo actuado firman:

	Nombres y Apellidos	Firma
Presidente	Bravo Duarte Freddy Lenin	
Secretaria	Correa Peralta Mirella Azucena	
Integrante	Cordova Martinez Luis Cristobal	

APROBACIÓN DEL TRIBUNAL CALIFICADOR

El tribunal calificador constituido por:

Bravo Duarte Freddy Lenin

Cordova Martinez Luis Cristobal

Correa Peralta Mirella Azucena

Luego de realizar la revisión de la Investigación Documental como propuesta practica, previo a la obtención del título (o grado académico) de **INGENIERO EN SISTEMAS COMPUTACIONALES** presentado por el señor **ORTEGA QUIÑÓNEZ ADRIÁN MARCEL**.

Con el tema de trabajo de Titulación: **ANÁLISIS DE SOFTWARE EN LA IMPLEMENTACIÓN DE VPN EN LAN INALÁMBRICA**.

Otorga a la presente Investigación Documental como propuesta práctica, las siguientes calificaciones:

Investigación documental	[56]
Defensa oral	[14]
Total	[70]

Emite el siguiente veredicto: (aprobado/reprobado) Aprobado

Fecha: 8 de Mayo del 2019.

Para constancia de lo actuado firman:

	Nombres y Apellidos	Firma
Presidente	Bravo Duarte Freddy Lenin	
Secretaria	Correa Peralta Mirella Azucena	
Integrante	Cordova Martinez Luis Cristobal	

DEDICATORIA

MENDOZA GUANOQUIZA FREDDY GEOVANNY

El presente trabajo lo dedico principalmente a Dios, porque me dio la fuerza para seguir día a día en todo este proceso, a mi familia por sus oraciones, palabras de aliento y todo el apoyo incondicional que me brindaron en especial a mi madre por todo el esfuerzo que ha hecho por nosotros, a mi esposa y mi pequeño vástago Jared que son mi motivo para seguir luchando cada día.

ORTEGA QUIÑONEZ ADRIAN MARCEL

Este trabajo de titulación se lo dedico a mis padres que me han apoyado incondicionalmente durante todos mis años de estudio universitarios y con su esfuerzo, unión he logrado culminar mi meta de ser un profesional.

A Dios que a pesar de muchas circunstancias me ha guiado todo este tiempo en mis estudios y por siempre darme las fuerza de seguir adelante.

AGRADECIMIENTO

MENDOZA GUANOQUIZA FREDDY GEOVANNY

Agradezco a Dios por estar conmigo y no desampararme a lo largo de toda mi carrera universitaria, en los momentos de debilidad él fue mi fortaleza, por darme el entendimiento y sabiduría para culminar exitosamente esta etapa de mi vida.

Le doy gracias a toda mi familia que fueron quienes estuvieron ahí en este proceso, siempre me apoyaron, gracias madre por el amor que nos brindas, desde pequeños nos inculcaste la palabra de Dios por habernos enseñado lo importante que es la unión en la familia, todo tu sacrificio no ha sido en vano.

ORTEGA QUIÑONEZ ADRIAN MARCEL

Agradezco a Dios por darme la fortaleza necesaria diariamente para poder cumplir con mis metas académicas.

A mis padres por darme el apoyo necesario en todo momento, son el pilar fundamental en mi vida, gracias a ellos he podido culminar mis estudios académicos y lograr cumplir mi meta de ser un profesional.

Agradezco especialmente a mi tutor Ing. Freddy Bravo por su ayuda y colaboración, quien nos orientó durante el desarrollo de este trabajo de Investigación.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ANÁLISIS DE SOFTWARE EN LA IMPLEMENTACIÓN DE VPN EN LAN INALÁMBRICA

RESUMEN

Las Redes De Área Local Inalámbricas (WLAN) son sistemas de transferencia de datos, los cuales permiten acceso a una red independiente a la ubicación del dispositivo y la información requerida, mediante el uso de ondas de radio en vez de una infraestructura cableada.

Existen problemas de seguridad las cuales se debe resolver antes de que se transmita información de gran valor en un gobierno u organización dentro de una red inalámbrica.

Hay graves problemas de seguridad que deben resolverse antes de que todos estén dispuestos a transmitir información corporativa valiosa en una red inalámbrica.

Las Redes Privadas Virtuales (VPN) actualmente es el método más común para acceder de forma remota, se habilita un proveedor de servicios y se proporciona un túnel privado a través de la nube pública para así obtener ahorro de costos y mejor productividad de las aplicaciones de acceso remoto

Las VPN es una extensión de una red privada (intranet) de una empresa por medio de una red pública (internet) para crear una conexión segura, ya que las VPN sirven como un transmisor de información de forma segura a través del internet, o una red corporativa extendida

Esta investigación se centra en el uso de software para implementar redes privadas virtuales dentro de LANs inalámbrica y conocer como estas funcionan y ver cuál de los recursos utilizados es el más óptimo al momento de su implementación y ejecución, comparando los resultados obtenidos una vez culminadas las pruebas.

PALABRAS CLAVE: redes inalámbricas, vpn, wlan.

ANÁLISIS DE SOFTWARE EN LA IMPLEMENTACIÓN DE VPN EN LAN INALÁMBRICA

ABSTRACT

Wireless Local Area Networks (WLAN) are data transfer systems, which allow access to a network independent of the location of the device and the information required, through the use of radio waves instead of a wired infrastructure.

There are security problems that must be resolved before valuable information is transmitted to a government or organization within a wireless network.

There are serious security problems that must be resolved before everyone is willing to transmit valuable corporate information over a wireless network.

Virtual Private Networks (VPN) is currently the most common method to access remotely, a service provider is enabled and a private tunnel is provided through the public cloud in order to obtain cost savings and better productivity of applications remote access

The VPN is an extension of a private network (intranet) of a company through a public network (internet) to create a secure connection, since the VPNs serve as a transmitter of information in a secure way through the internet, or an extended corporate network

This research focuses on the use of software to implement virtual private networks within wireless LANs and know how they work and see which of the resources used is the most optimal at the time of implementation and execution, comparing the results obtained once the tests.

KEY WORDS: wireless networks, vpn, wlan

INTRODUCCIÓN

Una de las tendencias tecnológicas más transformadoras de la última década es la disponibilidad y la creciente expectativa de conectividad. Ya sea para revisar el correo electrónico, llevar una conversación de voz, navegar por la web o un sinnúmero de otros casos de uso, ahora esperamos poder acceder a estos servicios en línea sin importar la ubicación, la hora o la circunstancia: en la carrera, mientras estamos en la cola, en la oficina, en un metro, en vuelo, y en todas partes. Hoy en día, todavía nos vemos forzados a ser proactivos a la hora de encontrar conectividad (por ejemplo, buscar un punto de acceso WiFi cercano) pero, sin lugar a dudas, el futuro se trata de la conectividad ubicua donde el acceso a Internet es omnipresente.

Las redes inalámbricas se encuentran en el epicentro de esta tendencia. En su forma más amplia, una red inalámbrica se refiere a cualquier red no conectada por cables, que es lo que permite la conveniencia y movilidad deseadas para el usuario. No es sorprendente que dada la gran cantidad de aplicaciones y casos de uso diferentes, también deberíamos esperar ver docenas de tecnologías inalámbricas diferentes para satisfacer las necesidades, cada una con sus propias características de rendimiento y cada una optimizada para una tarea y contexto específicos. Hoy en día, ya tenemos más de una docena de tecnologías inalámbricas en uso: WiFi, Bluetooth, ZigBee, NFC, WiMAX, LTE, HSPA, EV-DO, estándares 3G anteriores, servicios satelitales y más.

Como tal, dada la diversidad, no es prudente hacer generalizaciones radicales sobre el rendimiento de las redes inalámbricas. Sin embargo, la buena noticia es que la mayoría de las tecnologías inalámbricas funcionan según principios comunes, tienen concesiones comunes y están sujetas a criterios y restricciones de rendimiento comunes. Una vez que descubramos y comprendamos estos principios fundamentales del rendimiento inalámbrico, la mayoría de las otras piezas comenzarán a encajar automáticamente.

Además, mientras que la mecánica de la entrega de datos a través de la comunicación por radio es fundamentalmente diferente del mundo atado, el resultado experimentado por el usuario es, o debería ser, todo lo mismo: el mismo rendimiento, los mismos resultados. A la larga, todas las aplicaciones son y serán entregadas a través de redes inalámbricas; puede darse el caso de que a algunos se acceda con más frecuencia a través de la red inalámbrica que a otros. No existe tal cosa como una aplicación cableada, y no hay demanda para tal distinción.

Todas las aplicaciones deben funcionar bien independientemente de la conectividad subyacente. Como usuario, no debe preocuparse por la tecnología subyacente en uso, pero como desarrolladores debemos pensar con anticipación y diseñar nuestras aplicaciones para anticipar las diferencias entre los diferentes tipos de redes. Y la buena noticia es que cada optimización que apliquemos a las redes inalámbricas se traducirá en una mejor experiencia en todos los demás contextos.

La presente investigación a elaborar está compuesta por 5 Capítulos que consisten en:

Capítulo 1: Este capítulo abarca el desarrollo de la temática, la descripción del problema de la investigación, sus objetivos y justificación.

Capítulo 2: Es la elaboración del marco teórico de la investigación basados en repositorios científicos, libros para su elaboración.

Capítulo 3: Se describe la metodología a usar en este caso es una investigación de campo-cualitativa.

Capítulo 4: Es la elaboración de desarrollo del tema que es análisis de software en la implementación de VPN en LAN inalámbrica.

Capítulo 5: En este se realiza las conclusiones a las que se llegaron mediante la propuesta de investigación planteada.

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema.

Las redes inalámbricas están obligando a las organizaciones a replantearse por completo cómo protegen sus redes y dispositivos para evitar ataques y mal uso que exponen activos críticos y datos confidenciales. Por su propia naturaleza, las redes inalámbricas son difíciles de implementar, proteger y administrar, incluso para los administradores de redes más inteligentes.

En los últimos cinco años, el mundo se ha vuelto cada vez más móvil. Como resultado, las formas tradicionales de conexión en red del mundo han demostrado ser inadecuadas para enfrentar los desafíos planteados por nuestro nuevo estilo de vida colectivo. Si los usuarios deben estar conectados a una red mediante cables físicos, su movimiento se reduce drásticamente. La conectividad inalámbrica, sin embargo, no presenta tal restricción y permite un movimiento mucho más libre por parte del usuario de la red. Como resultado, las tecnologías inalámbricas están invadiendo el ámbito tradicional de las redes "fijas" o "cableadas". Las redes de telefonía inalámbricas han tenido éxito porque permite que las personas se conecten entre sí independientemente de su ubicación. Las nuevas tecnologías dirigidas a las redes de computadoras prometen hacer lo mismo con la conectividad a Internet. La tecnología de redes de datos inalámbricos más exitosa hasta el momento ha sido 802.11 (Adya, Bahl, Padhye, Wolman, & Zhou, 2004).

(Pérez, Herrera, Uzcátegui, & Bernardo, 2012) Detalla que para la propagación de una red inalámbrica más allá de la seguridad que debe proporcionar este se enfoca en otros aspectos para poder medir la cobertura la red puede alcanzar que también son importantes tales como: morfología, condiciones atmosféricas y topología.

Ahora se puede transmitir a través de redes de transmisión de información archivos multimedia como: video, audios, imágenes. Pero esto a través de una red IP convencional nos permite visualizar una serie de retos, ya que se ajustan a las necesidades de ese tipo de tráfico, para que los elementos de red deban tener las características apropiadas para su correcto funcionamiento. De ser así de complejo en una red por medio de cables, pues se

maximiza la dificultad en una red inalámbrica, ya que el medio es compartido con todo lo que en él se esté transportando (Cruz, Martínez, & Crespo, 2013).

Debido a todos estos problemas que conlleva el uso de una red inalámbrica es necesario conocer cuales con las herramientas necesarias para poder tener mayor seguridad y eficiencia en el tráfico de datos.

1.2 Objetivo General

Determinar la factibilidad de una red inalámbrica local mediante el uso de VPN.

1.3 Objetivos Específicos

- Identificar herramientas para la implementación de VPN en LAN inalámbrica.
- Analizar el funcionamiento de herramientas en la implementación de VPN en LAN inalámbrica.
- Describir los pasos que conlleva el uso de herramientas en la implementación de VPN en LAN inalámbrica.

1.4 Justificación

Los departamentos de TI deben tener un plan de acción preventivo para prevenir ataques maliciosos y el mal uso de los empleados que comprometa la privacidad de los datos de una organización y hacer cumplir las políticas de seguridad para el uso inalámbrico, tanto dentro como fuera de sus instalaciones. Ya sea que una empresa haya autorizado o no el uso de la tecnología inalámbrica o que tenga una política de "no conexión inalámbrica", sus redes, datos, dispositivos y usuarios están expuestos y en riesgo.

Para garantizar una protección de amenazas inalámbricas efectiva y automatizada, las compañías y organizaciones deben implementar una solución de seguridad inalámbrica completa que cubra los activos en toda la empresa que les permita descubrir vulnerabilidades, evaluar amenazas, prevenir ataques y garantizar el cumplimiento continuo, de la manera más segura y fácil Uso y manera rentable disponible.

.

CAPÍTULO 2

MARCO TEÓRICO CONCEPTUAL

2.1 Redes Inalámbricas.

Según (Andreu, Redes inalámbricas (Servicios en red), 2011) son redes que no necesitan de un cableado y que suelen tener una comunicación por medios no guiados a través de ondas electromagnéticas. Tanto la transmisión de datos y la recepción de los mismos de realiza a través de antenas. Comúnmente el emisor posee una antena, pero puede ser que tengas más de una, debido a que hay sistemas que necesitan más de una antena para su funcionamiento. Las antenas son usadas como emisores o como receptores y en algunos casos pueden realizar ambas funciones.

2.2 Red Privada Virtual (VPN)

VPN ha sido una tecnología importante desde su creación a mediados de la década de 1990. PPTP (PPTP) marcó un punto de partida en la capacidad de conectar los equipos remotos a una red común.

Desde entonces, existen muchos avances e innovaciones en el campo, lo que resultó en tecnologías de la competencia. A medida que las tecnologías maduran, es importante centrarse en su comparación y evaluación de sus viabilidades de nuevos casos de uso de redes y paradigmas. Uno de tales paradigma es las funciones de red de virtualización (NFV) según (Esch, 2014). El NFV asume las funciones de red móvil, tal como un servidor de seguridad, punto final de VPN, equilibrador de carga, etc. Actualmente, existen dos tecnologías dominantes utilizadas en los entornos empresariales: IPSec y SSL / TLS OpenVPN base.

(Lacković & Tomić, 2017) Detalla que existen dos tipos de conexiones VPN de capa de red tales como: acceso remoto y de sitio a sitio. Las VPN de acceso remoto se utilizan para conectar teletrabajadores o configurar túneles temporales, y las VPN de sitio a sitio son usadas para estableces túneles de capa de red seguras permanentes entre las redes distantes.

VPN es una tecnología que proporciona a los usuarios una forma de lograr una comunicación segura por medio de un canal de comunicación inseguro, como el internet público. Ha sido aceptado ya que su flexibilidad y disponibilidad en muchas plataformas.

Por lo general se utiliza como una vía alterna a las costosas líneas arrendadas. Para las configuraciones tradicionales, los puntos finales de VPN se instalan en los dispositivos de hardware, entre estos están los firewalls y los routers. En las redes actuales, que usan funciones de red de virtualización (NFV), los puntos finales VPN pueden ser virtualizados en servidores comunes. Ya que el cifrado y descifrado de datos son procesos intensivos del CPU, es necesario conocer los límites de estas configuraciones de modo que la viabilidad de la virtualización de punto final puede ser evaluada (Díaz, Alzórriz, & Sancristóbal, 2014).

(Dhiman, 2014) Y (N, I, & D, 2001) concuerdan que las redes inalámbricas son propensas a sufrir ataques tales como: acceso no autorizado, hombre en el medio (MITM), difusión de la información, degradación de servicios, entre otros. Para (Hoekstra & Musulin, 2011) estos problemas son los que hacen a los usuarios utilizar redes privadas virtuales (VPN) para poder fortalecer la seguridad en la red. Una VPN proporciona confidencialidad e integridad de los datos a través del cifrado y la autenticación del tráfico de un enlace entre dos o más dispositivos de red. Este enlace entre estos dispositivos se realiza por un canal de comunicación denominado túnel, está protegido usando encriptación extremo a extremo. Para (Caldas-Calle, Jara, Huerta, & Gallegos, 2017) la integridad y la autenticación se las obtienen a través de algoritmos de autenticación, mecanismos de intercambio de claves o certificados. Debido a esto, la VPN es usada para conectar dispositivos remotos a redes privadas a través de una red pública.

Algunos autores estudiaron el comportamiento de los parámetros de calidad de servicio en una VPN a través de una Red Inalámbrica. Por ejemplo (Kolahi, Cao, & Chen, 2016) determina el comportamiento de los parámetros de ida y vuelta y el rendimiento en los protocolos de VPN (IPSec y SSL) con Windows. Para (Likhar, Yadav, & M, 2011) los resultados de las mediciones que realizó determinaron que los parámetros de variación rendimiento, la latencia, tasa de pérdida de tramas y retardo de paquetes disminuyeron la QoS de la red.

(Pena & Evans, 2000) Realizó un análisis de la utilización del CPU cuando se presenta la aplicación de software para la creación de VPN. (Qu, Dang, & Li, 2012) Analizaron el uso de OpenVPN en una tableta con sistema operativo Android.

2.3 Red de Área Local (LAN)

Una red de área local proporciona capacidad de conexión en red a un grupo de computadoras que se encuentran muy cerca unas de otras, como en un edificio de oficinas, escuela u hogar. Las LAN generalmente se crean para permitir compartir recursos y servicios como archivos, impresoras, juegos, aplicaciones, correo electrónico o acceso a Internet (Andreu, Mantenimiento de LAN (Redes locales), 2011).

Una LAN Wi-Fi típica opera uno o más puntos de acceso inalámbrico a los que se conectan los dispositivos dentro del rango de la señal. Estos puntos de acceso, a su vez, administran el tráfico de la red que fluye hacia y desde los dispositivos locales y también puede conectar la red local con redes externas. En una LAN doméstica, los enrutadores de banda ancha inalámbricos realizan las funciones de un punto de acceso (Pongo, 2015).

Una LAN Ethernet típica consiste en uno o más concentradores, conmutadores o enrutadores a los que se conectan los dispositivos individuales a través de cables Ethernet.

Tanto Wi-Fi como Ethernet también permiten que los dispositivos se conecten entre sí directamente (por ejemplo, conexiones entre pares o ad-hoc) en lugar de a través de un dispositivo central, aunque la funcionalidad de estas redes es limitada. Aunque Ethernet y Wi-Fi se usan generalmente en la mayoría de las empresas y hogares, debido a los bajos costos y los requisitos de velocidad, también puede configurar una LAN con conexiones de fibra (Onvural & Nilsson, 2012).

Todos los sistemas operativos de red populares ofrecen soporte integrado para la tecnología TCP / IP requerida.

2.4 Red de Área LocaL Inalámbrica (WLAN)

Una red de área local inalámbrica (WLAN) es una red de área local (LAN) que no se basa en conexiones Ethernet por cable. Una WLAN puede ser una extensión de una red cableada actual o una alternativa a la misma.

Las WLAN tienen velocidades de transferencia de datos que van de 1 a 54 Mbps, y algunos fabricantes ofrecen soluciones propietarias de 108 Mbps. El estándar 802.11n puede alcanzar los 300 a 600Mbps (Vaidya, Dugar, Gupta, & Bahl, 2005) .

Debido a que la señal inalámbrica se transmite para que todos puedan compartirla, se requieren varias precauciones de seguridad para garantizar que solo los usuarios autorizados puedan acceder a su WLAN.

Se puede transmitir una señal WLAN para cubrir un área que varía en tamaño desde una oficina pequeña hasta un campus grande. Más comúnmente, un punto de acceso WLAN proporciona acceso dentro de un radio de 65 a 300 pies (García, 2012).

Según (Korowajczuk, 2011) Las LAN y las WLAN se pueden combinar mediante un puente que conecta las dos redes. Muchos enrutadores inalámbricos también incluyen puertos Ethernet, que proporcionan conexiones para un número limitado de dispositivos inalámbricos. En la mayoría de los casos, los enrutadores inalámbricos actúan como un puente, combinando los dispositivos Ethernet y Wi-Fi conectados en la misma red. Esto permite que los dispositivos cableados e inalámbricos se comuniquen entre sí a través de un solo enrutador.

2.4.1 Ventajas de las WLAN

La ventaja más obvia de una WLAN es que los dispositivos pueden conectarse de forma inalámbrica, eliminando la necesidad de cables. Esto permite que los hogares y las empresas creen redes locales sin cablear el edificio con Ethernet. También proporciona una forma para que los dispositivos pequeños, como teléfonos inteligentes y tabletas, se conecten a la red. Las WLAN no están limitadas por la cantidad de puertos físicos en el enrutador y, por lo tanto, pueden admitir docenas o incluso cientos de dispositivos. El rango de una WLAN se puede ampliar fácilmente agregando uno o más repetidores. Finalmente, una WLAN se puede actualizar fácilmente al reemplazar los enrutadores con nuevas versiones, una solución mucho más sencilla y económica que la actualización de cables Ethernet viejos.

2.4.2 Desventajas de las WLAN

Las redes inalámbricas son naturalmente menos seguras que las redes cableadas. Cualquier dispositivo inalámbrico puede intentar conectarse a una WLAN, por lo que es importante limitar el acceso a la red si la seguridad es una preocupación. Esto se realiza normalmente mediante la autenticación inalámbrica, como WEP o WPA, que cifra la comunicación. Además, las redes inalámbricas son más susceptibles a la interferencia de otras señales o barreras físicas, como las paredes de concreto.

CAPÍTULO 3

METODOLOGÍA

Para (Augusto, 2006) encontrar una estrategia de diseño de investigación es similar al proceso de investigación en su totalidad: primero, busque información general sobre el diseño y los métodos de investigación, luego obtenga conocimientos básicos sobre la metodología que abordaría de manera más apropiada el tipo de datos que recopilará y finalmente elija Una metodología y prueba / medida para utilizar en su investigación.

3.1 Metodología Descriptiva

Para (Hernández Sampieri, 2004) los estudios descriptivos son aquellos que a partir de una variable se pretende medir o recolectar información, ya sea esta de forma independiente o conjunta. Pues se busca conocer y explicar cómo es que se manifiesta el fenómeno o suceso de interés.

3.2 Investigación Documental

"Es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos" (Arias, 2012).

3.3 Extracción de Información

Para esta investigación es necesario extraer la información necesaria de fuentes bibliográficas confiables, en los que se detalle el funcionamiento de las redes inalámbricas.

3.4 Selección de Herramientas

La selección de las herramientas a utilizar para la implementación de VPN se da en base a la obtención de la información de repositorios virtuales, donde se especifique el uso de estas en temas similares.

3.5 Pruebas

Las Pruebas se realizan en base al uso de las herramientas seleccionadas, el cual se procede a verificar cual es el comportamiento de la Tecnología a configurar y se determina cual es la más óptima en base al comportamiento de la red inalámbrica con el uso de la VPN.

CAPÍTULO 4

DESARROLLO DEL TEMA

Realizamos un análisis para demostrar cuales el impacto económico que tendrá una empresa, en este caso un proyecto si la información que se utiliza es plagiada o alterada debido a problemas de seguridad en la Red.

Tomamos como ejemplo la Empresa "Righttek" un proveedor de soluciones informáticas, la cual utiliza 6 computadoras conectadas a una red inalámbrica, para poder realizar un proyecto llamado "Fase de Migraciones". Para eso detallamos la orden de trabajo que se genera para dicho proyecto.

Tabla 1

Orden de Trabajo de Proyecto "Fase de Migraciones"

Recurso	Tipo	Capacidad Máxima	Tasa estándar	Tasa estándar
Líder de Proyecto	Trabajo	100%	$ 6,40/hora	$ 6,40/hora
Analista	Trabajo	100%	$ 5,40/hora	$ 5,40/hora
Programador 1	Trabajo	100%	$ 5,40/hora	$ 5,40/hora
Programador 2	Trabajo	100%	$ 5,40/hora	$ 5,40/hora
Programador 3	Trabajo	100%	$ 5,40/hora	$ 5,40/hora
Programador 4	Trabajo	100%	$ 5,40/hora	$ 5,40/hora
Equipos	Material		3000	3000

Obtenido de Righttek

Ya que se utilizan 6 computadoras las cuales están consideradas como Equipos dentro de la orden de trabajo y 6 Trabajadores los cuales trabajarán al 100% con un sueldo proporcional a cada cargo.

En la siguiente tabla detallamos el flujo de efectivo que tendrá la empresa al usar las diferentes herramientas para implementar una VPN.

Tabla 2

Flujo de efectivo del Proyecto "Fase de Migraciones"

FLUJO DE EFECTIVO	Tunnel Bear	Seed4Me	Windscribe
Contratos Servicios	**99432**	**99432**	**99432**
Descuentos 5% max.	4971,6	4971,6	4971,6
Ventas Netas 100% Capacidad	**94460,4**	**94460,4**	**94460,4**
Costos	**600**	**600**	**600**
Proveedores	600	600	600
Gastos	**1089**	**946**	**1024**
Servicios Básicos	480	480	480
Software	**359**	**216**	**294**
Otros	200	200	200
Depreciación	50	50	50
UAII	**0**	**0**	**0**
Deuda Bancaria			
Capital	**0**	**0**	**0**
Intereses	**0**	**0**	**0**
Flujo Efectivo Neto	**92771,4**	**92914,4**	**92836,4**

Obtenido de Righttek

En la tabla se toma las Ventas netas como el Contrato de Servicio menos el descuento máximo que se puede generar por el servicio, los costos es la suma de los valores correspondientes a proveedores, los gastos serán el total de los servicios básicos, el software como tal será la herramienta para implementar la VPN, en otros se engloban valores de otras licencias de acuerdo a las herramientas o tecnologías a usar para el proyecto y la depreciación de los equipos. Estos valores del alquiler del servicio de la VPN serán tomados como proyección de 1 año.

La parte sombreada de la tabla indica el valor anual a pagar por el uso de cada herramienta y si nos guiamos a simple vista por los costos reflejados de ganancia en el proyecto en el Flujo Efectivo Neto, podemos definir qué Seed4Me es la más factible, ya que nos generará un margen de ganancia superior al de las otras herramientas, debido a que el costo del software es más económico. Cabe recalcar que esta parte del análisis es solo enfocada en la parte económica, ya que si se usa una VPN es para proteger la información con la que se está trabajando ya que si a esta información una persona o sistema no autorizado llega a tener acceso a ella se perdería, teniendo como consecuencia la pérdida proyecto y las ganancias que se obtienen de ella que en este caso sin usar una VPN la ganancia es de

$93130,4, pero como escogimos Seed4Me debido a que su precio es más bajo estamos protegiendo $**92914,4.**

Una VPN se usa en la red WLAN para transmitir los datos con mayor seguridad, ya que el tráfico que se genera viaja cifrado y es más difícil para que una tercera persona tenga acceso a la información transmitida, existen servicios gratuitos y otros de pago.

En el desarrollo del tema seleccionamos 3 herramientas VPN que son:

- SEED4.ME
- Windscribe
- TunnelBear

Las pruebas se realizaron en una red inalámbrica local con un router de 300mbps y varios ordenadores portátiles, uno de ellos sirvió como servidor y los otros como clientes para ello se utilizó la herramienta Jperf la cual estuvo ejecutándose en todos los computadores implicados en las pruebas, se enviaron varios paquetes por cada ordenador para poder visualizar cómo se comporta el tráfico de la red utilizando una VPN, esto se realizó en diferentes escenarios por ejemplo ciertos ordenadores se encontraban a una distancia entre 2 a 5 metros, también se probó con el servidor dentro de una oficina y el cliente en la parte externa con una distancia aproximada de 6 metros.

4.1 SEED4.ME

Es una herramienta VPN que permitirá la transmisión de datos de forma segura, podemos navegar de forma anónima y privada, esta herramienta está disponible para diferentes plataformas, tiene una versión de prueba que dura 7 días.

Tabla 3

Características de la Herramienta Seed4Me

Conexión wifi cifrada	Elegir país	Navegación privada y anónima.	Reconexión automática de VPN
El túnel de encriptación privado evita que los piratas informáticos roben sus datos a través de redes públicas / abiertas de 'hotspot' de WiFi. Asegure su WiFi y privacidad	Si viaja y necesita acceso a Internet desde diferentes ubicaciones, puede encontrar algunos sitios bloqueados, pero puede desbloquear sitios web. Utilice nuestros servidores ubicados en varios países	Navega por la web de forma anónima y privada. Su conexión a Internet se verá como si se originara en una ubicación diferente. Úselo para desbloquear y anonimizar su acceso a contenido web restringido geográficamente.	No te preocupes por filtrar tus datos. VPN se puede activar en modo automático para establecer una conexión VPN justo antes de que cualquier información se envíe a Internet

Nota. Características de Seed4.Me Tomado de **(seed4.Me, 2019)**

4.2 Windscribe

Es una aplicación para ordenadores y una extensión de navegador que trabajan entre sí para bloquear anuncios, rastreadores, acceder a lugares bloqueados, protege la privacidad en línea.

Características de la Herramienta Windscribe

Red grande	Sin registros de identificación	Cifrado más fuerte
Tiene una de las redes más diversas que hay. Todos los servidores están físicamente en los países en los que se anuncia que están, a diferencia de algunos competidores que tienen la mayoría de sus servidores en Estados Unidos y Europa, y simplemente falsifican la ubicación con datos de WHOIS falsos de IP para que parezca que está en otro lugar.	No almacenamos ningún registro que pueda identificarlo No mantenemos registros de conexión, marcas de tiempo de IP, registros de sesión ni supervisamos su actividad. Almacenamos la última vez que usó Windscribe, así como la cantidad total de ancho de banda utilizada en un período de 30 días para hacer cumplir las limitaciones de nivel gratuito.	En nuestras aplicaciones de escritorio, usamos el cifrado AES-256 con SHA512 auth y una clave RSA de 4096 bits. También apoyamos el secreto hacia adelante perfecto. En nuestras extensiones de navegador utilizamos TLS 1.2, ECDHE_RSA con intercambio de claves P-256 y cifrado AES_128_GCM.

Tabla 4

Nota. Características de Windscribe. Obtenido de (windscribe, 2018)

4.3 TunnelBear

Facilita la protección de su privacidad en línea y disfruta de un internet menos restringido.

Tabla 5

Características de la Herramienta TunnelBear

Diseñado para la velocidad	Conéctate a cualquier parte del mundo	Seguridad en la que puede confiar	Cifrado fuerte
Nuestra red global de servidores está optimizada para permitirle navegar y transmitir rápidamente. Sin limitación, sin amortiguación, sin problemas.	Con un ancho de banda ilimitado y conmutador de servidor, navegue libremente por más de 22 países en nuestra red en constante expansión.	TunnelBear es la única VPN en el mundo que publica auditorías de seguridad periódica e independiente de nuestras aplicaciones.	TunnelBear usa un cifrado AES de 256 bits fuerte por defecto. Un cifrado más débil ni siquiera es una opción.

Características de TunnelBear (TunnelBear, 2019)

4.4 Jperf

Es una herramienta que tiene como objetivo generar uno o más flujos de información desde el cliente hacia el servidor, esta transmisión se puede visualizar gráficamente en la herramienta, posteriormente se obtiene el resultado del total de la carga y el jitter que es la variación del tiempo en la llegada de los paquetes, debido a la congestión de la red, como datos de entrada están el número de flujos TCP o UDP según sea el caso, la carga en unidades de bytes que posee cada flujo y el ancho de banda del canal a evaluar.

4.5 Desarrollo de pruebas

Descargamos los instaladores de las herramientas que se usaron en las pruebas para su posterior instalación.

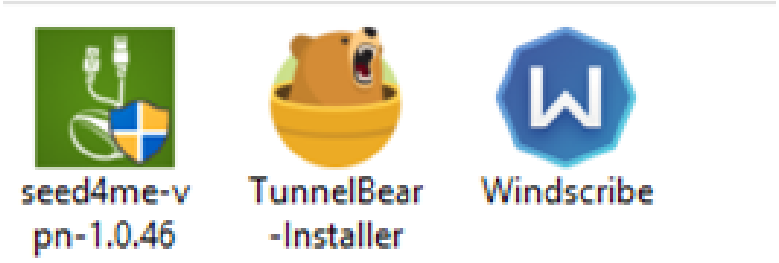

Figura 1 Instaladores de las herramientas VPN que se utilizaron en las pruebas

Las pruebas se realizaron usando ordenadores portátiles con diferentes versiones de sistema operativo entre los cuales se encuentran Windows10, Windows 8.1, Windows 7, unos con arquitectura de 32bits otros de 64 bits. Primero realizamos una prueba sin ninguna herramienta VPN.

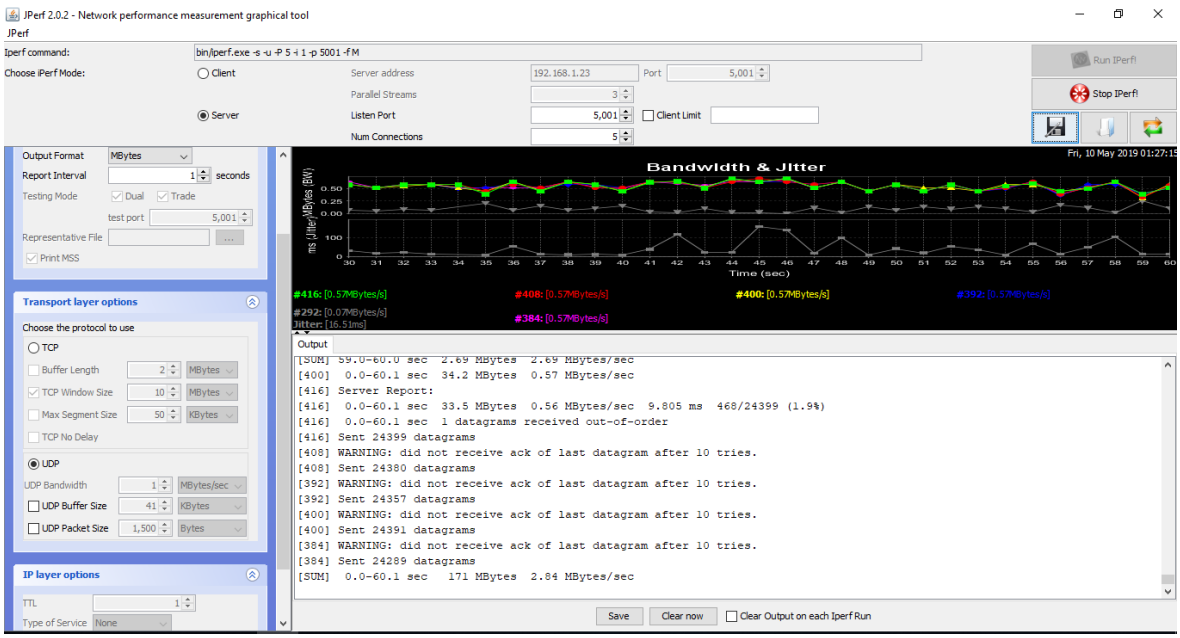

Figura 2 Prueba sin usar VPN

En esta prueba se obtuvo como resultado una transferencia de 34.2 Mb con ancho de banda de 0,56 Mbps y un jitter de 9.81ms.

4.5.1 Pruebas usando SEED4.ME

Una vez instalada la herramienta SEED4.ME la ejecutamos, luego procedemos a enviar paquetes para medir la velocidad del ancho de banda y verificar la variabilidad del tiempo de ejecución de los paquetes.

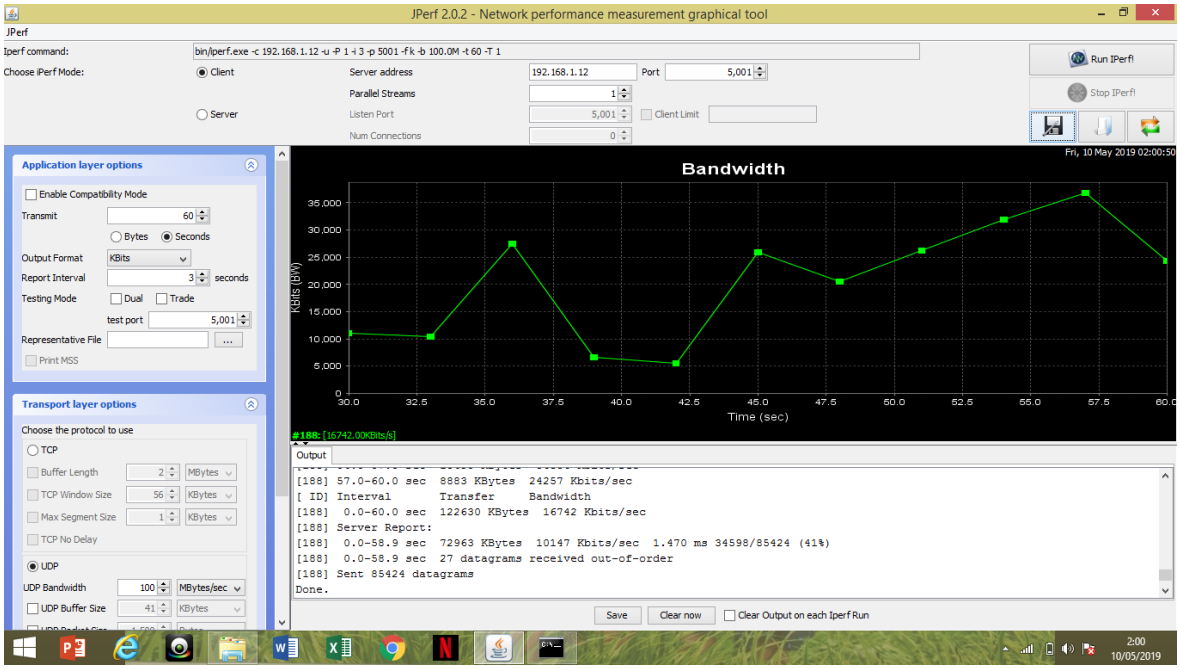

Figura 3 Envío de un paquete desde el cliente con IP 192.168.1.15 usando la herramienta VPN Seed4Me

En este equipo la sumatoria total en una transmisión de datos de 60 segundos dio como resultado una transferencia de 122.63 Mb con un ancho de banda de 0.34 Mbps, y jitter de 2.47ms, el reporte del servidor fue que 27 datagramas se recibieron fuera de orden, cabe mencionar que el ordenador se encontraba a una distancia aproximada de 2 metros del servidor y sin ningún factor que afecte la señal.

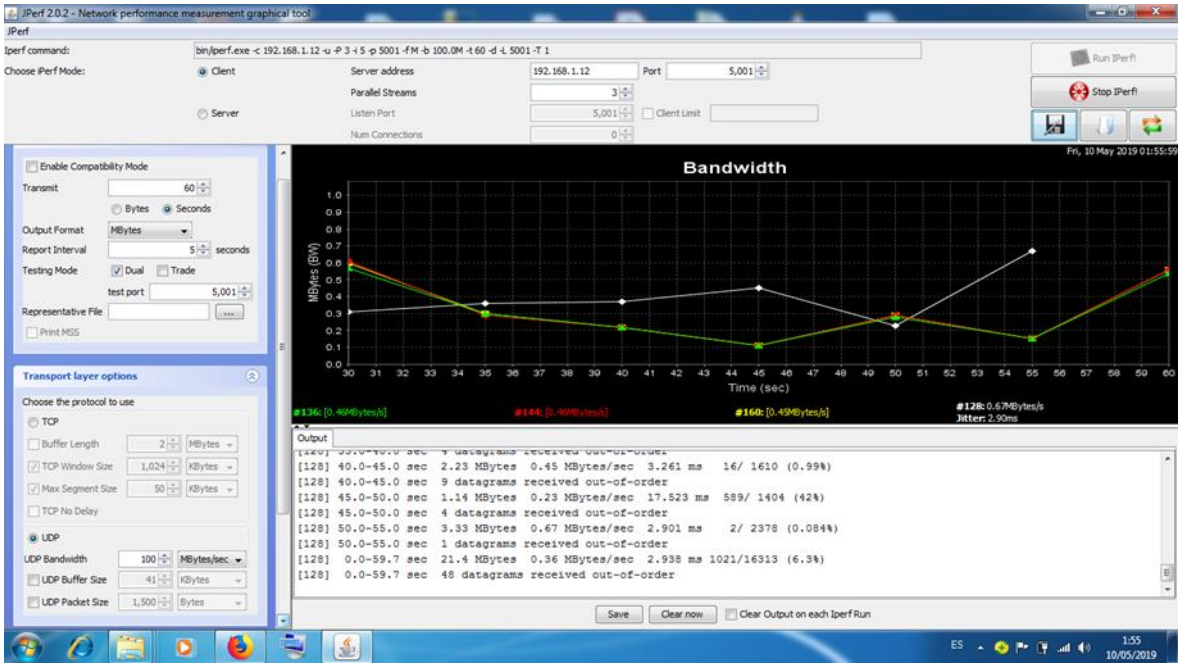

Figura 4 Envío de 3 paquetes desde el cliente con IP 192.168.1.20 usando la herramienta VPN Seed4Me

Las líneas que se observan en la imagen es el comportamiento de cada paquete, este equipo se encontraba a una distancia aproximada de 4 metros del servidor que estaba dentro de la oficina, las paredes interferían en la señal, se obtuvo una media de 21.4 Mb de transferencia con un ancho de banda de 0.36 Mbps, un jitter de 3.90ms y un total de 48 datagramas recibidos fuera de orden.

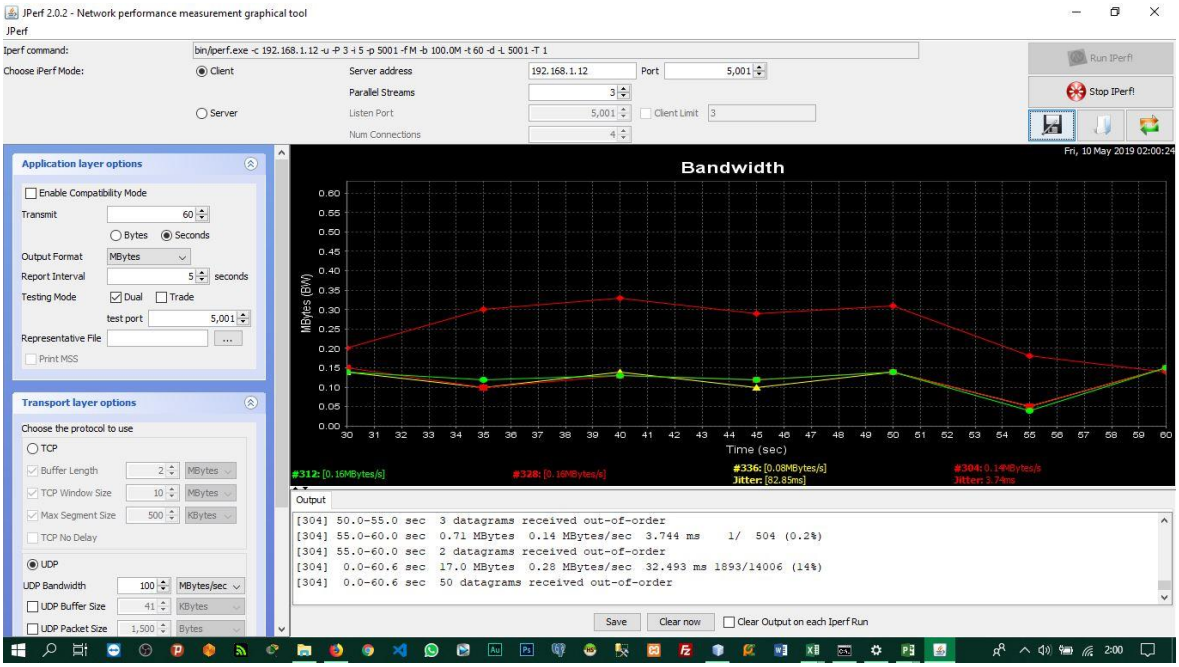

Figura 5 Envío de tres paquetes desde el cliente con IP 192.168.1.23 usando la herramienta VPN Seed4Me

Este equipo se encontraba a una distancia aproximada de 4 metros del servidor que estaba dentro de la oficina, las paredes interferían en la señal, se obtuvo una media de 17.7 Mb de transferencia con un ancho de banda de 0.29 Mbps, un jitter de 10.71ms y un total de 50 datagramas recibidos fuera de orden.

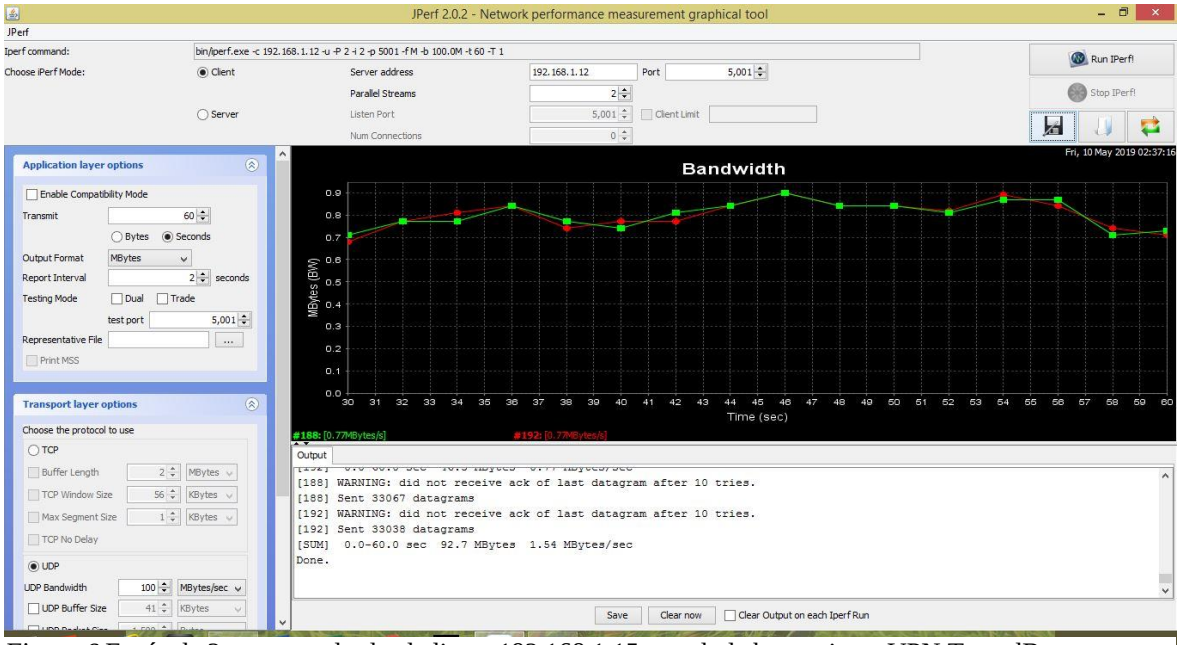

Figura 6 Envío de 2 paquetes desde el cliente 192.168.1.15 usando la herramienta VPN TunnelBear

En esta ocasión el ordenador se encontraba a una distancia aproximada de 3.5 metros sin interferencia en la señal y se obtuvo una suma total de 13.9 Mb de transferencia con ancho de banda de 0.48 Mbps y jitter de 8.38 ms.

4.5.2 Pruebas usando TunnelBear

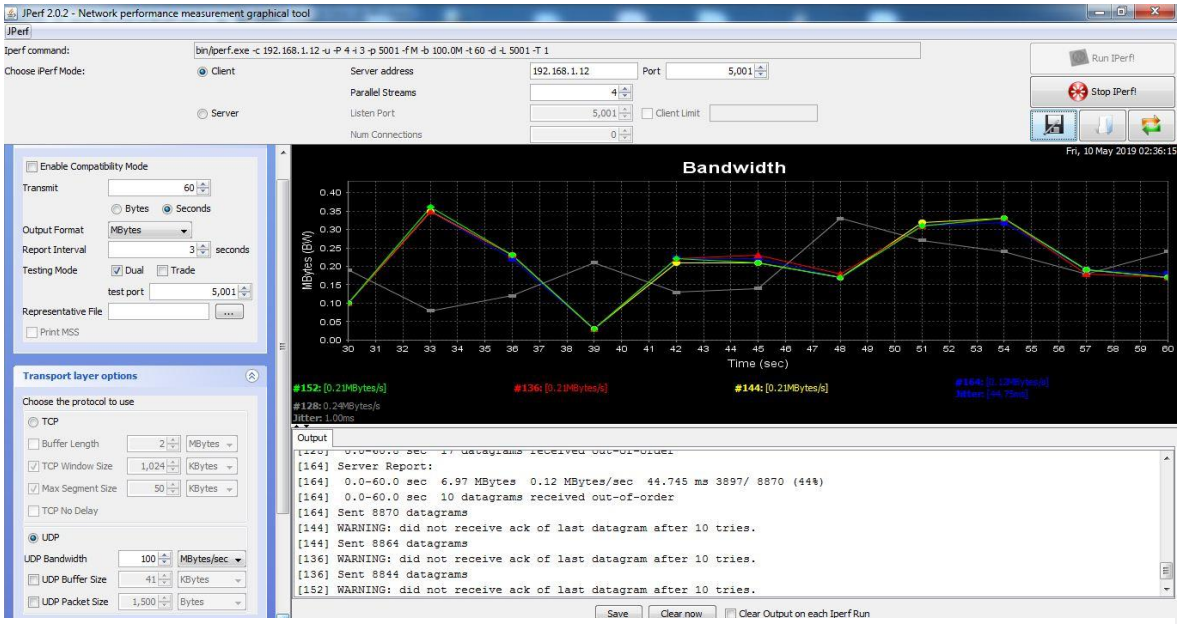

Figura 7 Envío de 4 paquetes desde el cliente con IP 192.168.1.20 usando la herramienta VPN TunnelBear

Este dispositivo se encontraba aproximadamente a 4 metros fuera de la oficina en la cual estaba el servidor, esto interfería la señal, la media de los resultados obtenidos fue una transferencia de 6.97 Mb con ancho de banda de 0.32Mbps, jitter de 8.74ms y 10 datagramas fuera de orden.

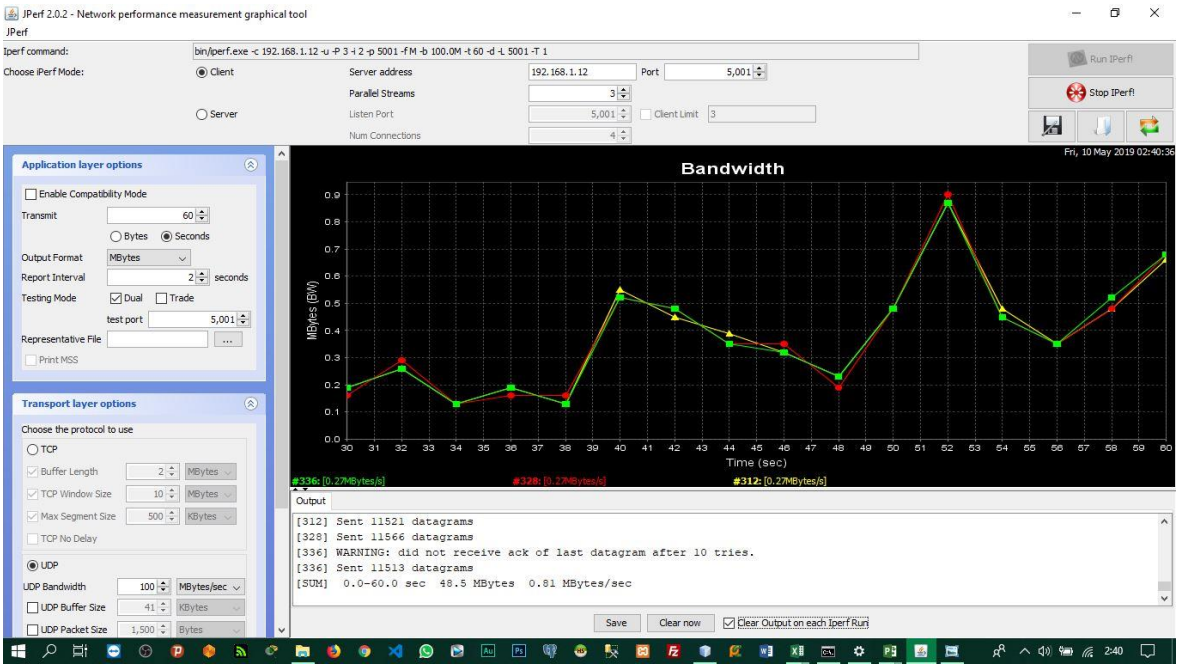

Figura 8 Envío de 3 paquetes desde el cliente con IP 192.168.1.23 usando la herramienta VPN TunnelBear

Este dispositivo se encontraba aproximadamente a 3 metros fuera de la oficina en la cual estaba el servidor, esto interfería la señal, la media de los resultados obtenidos fue una transferencia de 31.3 Mb con ancho de banda de 0.52Mbps, jitter de 6.05ms y 4 datagramas fuera de orden.

4.5.4 Pruebas usando Windscribe

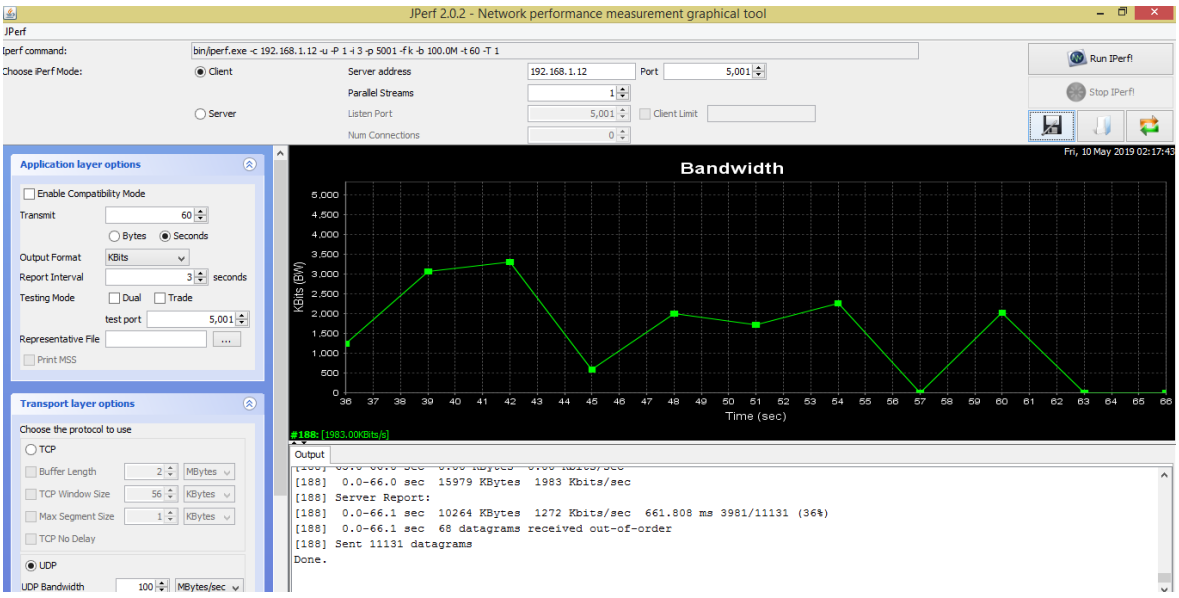

Figura 9 Envío de un paquete desde el cliente con IP 192.168.1.15 usando la herramienta Windscribe

El ordenador se encontraba a una distancia aproximada de 3.5 metros sin interferencia, los resultados obtenidos fueron una transferencia de 10.26 Mb con ancho de banda de 0.16 Mbps y 68 datagramas recibidos fuera de orden.

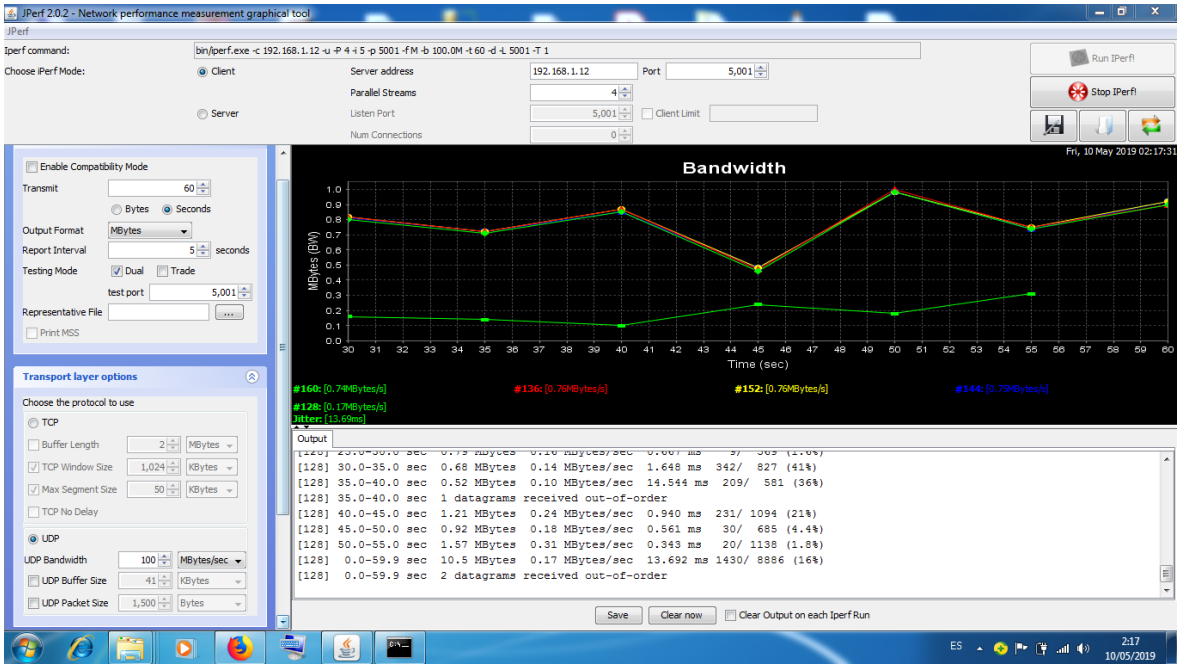

Figura 10 Envío de 4 paquetes desde el cliente con IP 192.168.1.20 usando la herramienta VPN Windscribe

Este dispositivo se encontraba aproximadamente a 4 metros fuera de la oficina en la cual estaba el servidor, esto interfería la señal, la media de los resultados obtenidos fue una transferencia de 15.5 Mb con ancho de banda de 0.27Mbps, jitter de 13.69ms y 2 datagramas fuera de orden.

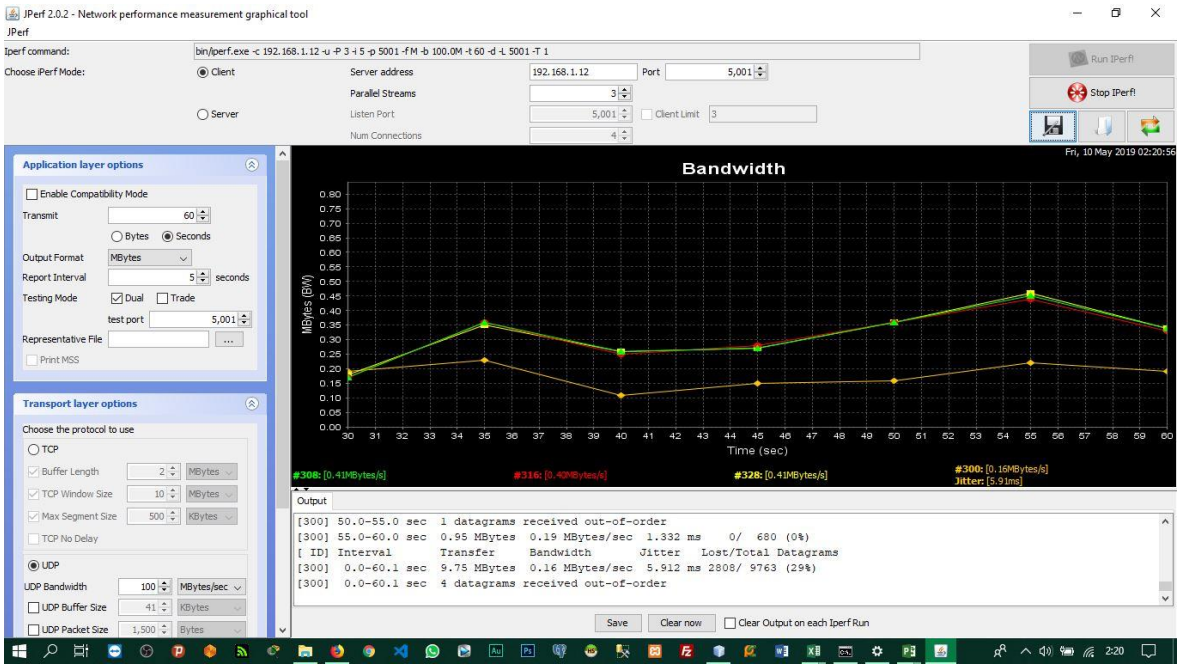

Figura 11 Envío de 3 paquetes desde el cliente con IP 192.168.1.23 usando la herramienta VPN Windscribe

Este dispositivo se encontraba aproximadamente a 4 metros fuera de la oficina en la cual estaba el servidor, esto interfería la señal, la media de los resultados obtenidos fue una transferencia de 9.75 Mb con ancho de banda de 0.16Mbps, jitter de 5.91ms y 4 datagramas fuera de orden.

4.6 Evaluación de los resultados

Una vez realizadas las pruebas pudimos observar que la velocidad de transmisión de datos varia en las diferentes herramientas usadas, se realizó un gráfico para poder determinar cuál es la herramienta más factible.

Tabla 6

Resultados de las Pruebas Realizadas

Herramientas	SEED4.ME	TunnelBear	Windscribe
Ancho de Banda	0,33 Mbps	0,44 Mbps	0,20 Mbps
Jitter	5,6933 ms	7,72 ms	9,3263 ms

Nota. Comparación de resultados obtenidos de las pruebas realizadas con diferentes herramientas VPN

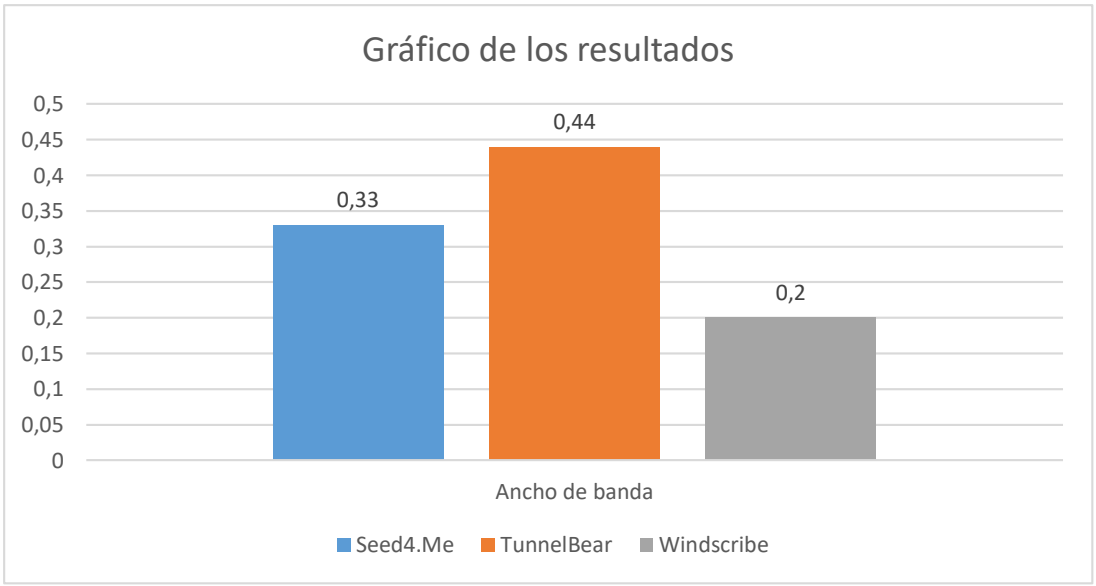

Figure 12 Resultados del ancho de banda

Los valores representados en el grafico están dados en Mbps donde el de mayor valor es el que tiene mayor velocidad en la transmisión de datos por ende el que tiene un mejor rendimiento en la red es la herramienta TunnelBear.

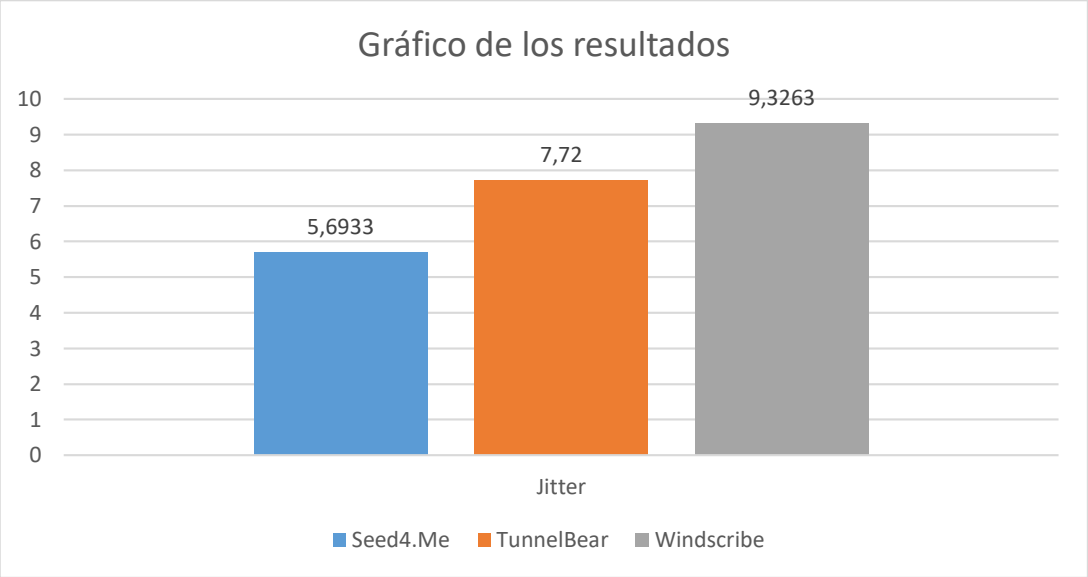

Figure 13 Resultados del Jitter

El grafico esta dado en milisegundos el menor valor indica que tiene menor tiempo de retardo por lo tanto la herramienta Seed4.Me es la que tiene menor tiempo de Jitter.

CAPÍTULO 5

CONCLUSIONES

Las redes inalámbricas locales (WLAN) como cualquier otro tipo de red son vulnerables a diferentes ataques es por eso la propuesta de usar una VPN en la red local esto nos permite tener una mayor seguridad de la información, asegura el flujo de tráfico en la red.

Realizamos pruebas con diferentes herramientas VPN para constatar cual es la más viable y conveniente al momento de usar, con los resultados comprobamos que el tiempo de respuesta y carga varía, se hizo una prueba sin usar ninguna VPN, al momento de conectarnos con una VPN y realizar el test se puede notar la diferencia de velocidad de transmisión de datos uno de los motivos es porque las VPN usan el cifrado de extremo a extremo para evitar que alguien haga captura de nuestro tráfico de red, este proceso de cifrado puede ralentizar la conexión, si presentamos problemas con la velocidad podemos bajar el nivel de cifrado o cambiar el protocolo de VPN aunque esto representaría un riesgo para la integridad de los datos.

Verificamos la velocidad de transmisión de los datos mediante el software Jperf es una herramienta sencilla pero muy útil, el trabajo que realiza esta aplicación es que sigue el modelo cliente servidor, un lado envía datos y el otro recibe dando la opción de visualizar el comportamiento de la red, verificar el ancho de banda y el jitter en la transmisión de datos.

Después de comparar los resultados obtenidos de las pruebas realizadas concluimos que la herramienta VPN mas apta para usar en la red WLAN TunnelBear en cuanto a rendimiento, pero si vemos el factor económico el más factible seria Speed4.Me.

Tabla 7

Comparación de rendimiento de herramientas VPN utilizadas

Herramientas	Ancho de banda	Rendimiento	Porcentaje de impacto
Seed4	0,33Mbps	59%	41%
TunnelBear	0,44Mbps	79%	21%
Windscribe	0,20Mbps	36%	64%

Fuente elaboración propia

La herramienta que tiene menor impacto en la red es TunnelBear con el 21% de perdida en el rendimiento de la red en comparación al ancho de banda sin usar VPN.

REFERENCIAS BIBLIOGRÁFICAS

Adya, A., Bahl, P., Padhye, J., Wolman, A., & Zhou, L. (29 de Octubre de 2004). *ieeexplore.ieee.org.* Obtenido de ieeexplore.ieee.org: https://ieeexplore.ieee.org/abstract/document/1363823

Andreu, J. (2011). *Mantenimiento de LAN (Redes locales).* Madrid: Editex.

Andreu, J. (2011). *Redes inalámbricas (Servicios en red).* Madrid: Editex.

Arias, F. G. (2012). *El Proyecto de Investigación. Introducción a la Metodología Científica.* Fidias G. Arias Odón.

Augusto, B. C. (2006). *sidalc.net.* Recuperado el Febrero de 2019, de sidalc: http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=zamocat.xis&method=post&formato=2&cantidad=1&expresion=mfn=027873

Caldas-Calle, L., Jara, J., Huerta, M., & Gallegos, P. (Junio de 2017). *ieeexplore.ieee.org.* Recuperado el Febrero de 2019, de ieeexplore: https://ieeexplore.ieee.org/document/7959718

Cruz, M., Martínez, R., & Crespo, Y. (2013). *scielo.* Recuperado el 10 de 02 de 2019, de scielo.sld.cu: http://scielo.sld.cu/scielo.php?pid=S2227-18992013000100010&script=sci_arttext&tlng=en

Dhiman, D. (Enero de 2014). *semanticscholar.* Recuperado el Febrero de 2019, de pdfs.semanticscholar.org: https://pdfs.semanticscholar.org/cabd/a6b52dfd269e5e478ddeaa86220ef3abe4ef.pdf

Díaz, G., Alzórriz, I., & Sancristóbal, E. (2014). *Procesos y herramientas para la seguridad de redes.* Madrid: UNED - Universidad Nacional de Educación a Distancia.

Esch, J. (Diciembre de 2014). *ieeexplore.ieee.org.* Recuperado el Febrero de 2019, de ieeexplore: https://ieeexplore.ieee.org/document/6994329?arnumber=6994329

García, N. L. (2012). *Diseño e implementación de una red LAN y WLAN con sistema de control de acceso mediante servidores AAA.* Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería.

Hernández Sampieri, R. F. (2004). *METODOLOGÍA DE LA INVESTIGACIÓN.* Mexico: Mc Graw Hill Interamericana.

Hoekstra, B., & Musulin, D. (Agosto de 2011). *homepages.staff.os3.nl.* Recuperado el Febrero de 2019, de homepages: https://homepages.staff.os3.nl/~delaat/rp/2010-2011/p09/report.pdf

Kolahi, S. S., Cao, Y., & Chen, H. (Julio de 2016). *ieeexplore.ieee.org.* Recuperado el Febrero de 2019, de ieeexplore: https://ieeexplore.ieee.org/document/7574043

Korowajczuk, L. (2011). *LTE, WiMAX and WLAN Network Design, Optimization and Performance Analysis.* West Sussex: John Wiley & Sons.

Lacković, D., & Tomić, M. (Mayo de 2017). *ieeexplore.* Recuperado el Febrero de 2019, de ieeexplore.ieee.org: https://ieeexplore.ieee.org/abstract/document/7973470

Likhar, P., Yadav, R. S., & M, K. R. (Noviembre de 2011). *researchgate.net.* Recuperado el Febrero de 2019, de researchgate: https://www.researchgate.net/publication/51969257_Securing_IEEE_80211g_WLAN_Using_Open_VPN_and_its_Impact_Analysis

N, B., I, G., & D, W. (Julio de 2001). *scopus.* Recuperado el Enero de 2019, de www.scopus.com: https://www.scopus.com/record/display.uri?eid=2-s2.0-0034777649&origin=inward&txGid=5d39a3f9b9b60cf8e672c179bdff7dcd

Onvural, R. O., & Nilsson, A. (2012). *Local Area Network Interconnection.* Springer Science & Business Media.

Pena, C., & Evans, J. (Noviembre de 2000). *ieeexplore.ieee.org.* Recuperado el Febrero de 2019, de ieeexplore: https://ieeexplore.ieee.org/abstract/document/891094

Pérez, N., Herrera, J., Uzcátegui, J., & Bernardo, J. (2012). *scielo.* Recuperado el 10 de 02 de 2019, de scielo.org.ve: http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1316-48212012000100007

Pongo, S. S. (2015). *Instalación y Configuración de una Red Lan con Windows Server 2003 e Internet.* Shang Shing Cutipa Pongo.

Qu, J., Dang, F., & Li, T. (Agosto de 2012). *researchgate.net.* Recuperado el Febrero de 2019, de researchgate: https://www.researchgate.net/publication/261339243_Performance_Evaluation_and_Analysis_of_OpenVPN_on_Android

seed4.Me. (15 de Enero de 2019). *seed4.Me*. Recuperado el 10 de Marzo de 2019, de seed4.Me: https://seed4.me/

TunnelBear. (12 de Enero de 2019). *TunnelBear*. Obtenido de TunnelBear: https://www.tunnelbear.com/

Vaidya, N., Dugar, A., Gupta, S., & Bahl, P. (Octubre de 2005). *ieeexplore.ieee.org.* Recuperado el Febrero de 2019, de ieeexplore: https://ieeexplore.ieee.org/abstract/document/1516110

windscribe. (13 de Junio de 2018). *windscribe*. Recuperado el 10 de Marzo de 2019, de windscribe: https://esp.windscribe.com/features

Revisión URKUND

URKUND

Urkund Analysis Result

Analysed Document: propuesta_version_urkund20194885139.docx (D50493890)
Submitted: 4/11/2019 12:06:00 AM
Submitted By: fbravod@unemi.edu.ec
Significance: 2 %

Sources included in the report:

PROY_PERALTA JOSE28-11.docx (D23864535)
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-74252013000300005

Instances where selected sources appear:

3

Registro de acompañamientos

REPÚBLICA DEL ECUADOR

UNIVERSIDAD ESTATAL DE MILAGRO

UNEMI

Milagro, 13 de mayo del 2019

REGISTRO DE ACOMPAÑAMIENTOS

Inicio: 05-11-2018 **Fin** 30-04-2019

FACULTAD CIENCIAS DE LA INGENIERIA

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

Línea de investigación: DESARROLLO DE SOFTWARE, SEGURIDAD DE LA INFORMACIÓN.

TEMA: ANALISIS DE SOFTWARE EN LA IMPLEMENTACION DE VPN EN LAN INALAMBRICA

ACOMPAÑANTE: BRAVO DUARTE FREDDY LENIN

DATOS DEL ESTUDIANTE			
Nº	**APELLIDOS Y NOMBRES**	**CÉDULA**	**CARRERA**
1	MENDOZA GUANOQUIZA FREDDY GEOVANNY	0941604183	INGENIERÍA EN SISTEMAS COMPUTACIONALES
2	ORTEGA QUIÑONEZ ADRIAN MARCEL	0940724396	INGENIERÍA EN SISTEMAS COMPUTACIONALES

Nº	FECHA	HORA		Nº HORAS	DETALLE
1	2019-31-01	Inicio: 09:00 a.m.	Fin: 11:00 a.m.	2	REVISION CAPITULO 1

BRAVO DUARTE FREDDY LENIN
PROFESOR(A)

REA SANCHEZ VICTOR HUGO
DIRECTOR(A)

MENDOZA GUANOQUIZA FREDDY GEOVANNY
ESTUDIANTE

ORTEGA QUIÑONEZ ADRIAN MARCEL
ESTUDIANTE

Dirección: Cdla. Universitaria Km. 1 1/2 vía km. 26
Conmutador: (04) 2715081 - 2715079 Ext. 3107
Telefax: (04) 2715187
Milagro • Guayas • Ecuador

VISIÓN
Ser una universidad de docencia e investigación

MISIÓN
La UNEMI forma profesionales competentes con actitud proactiva y valores éticos, desarrolla investigación relevante y oferta servicios que demanda el sector externo, contribuyendo al desarrollo de la sociedad.

www.unemi.edu.ec

Anexos