TÍTULO DEL TRABAJO:

RED PRIVADA REMOTA MONTADA EN RASPBERRY PI PARA LA GESTIÓN SEGURA DE LOS RECURSOS INFORMÁTICOS ENTRE LAS OFICINAS DE BUILDERECUADOR CIA.LTDA.

LÍNEA DE INVESTIGACIÓN:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

MODALIDAD:

PROPUESTA TECNOLÓGICA

CARRERA:

INGENIERÍA EN SISTEMAS

TÍTULO POR OBETENER:

INGENIERÍA EN SISTEMAS CON ÉNFASIS EN ADMINISTRACIÓN DE REDES

AUTOR:

LUIS ALBERTO RIVERA MORLA

TUTORA:

MGTR. DIANA MARÍA LÓPEZ ÁLVAREZ

SAMBORONDÓN 2022

DEDICATORIA

A mis padres y hermanas, quienes son el pilar fundamental en mi vida y que con su esfuerzo y sacrificio me brindaron su apoyo incondicional para continuar en mis estudios y creyeron en mí hasta el final.

AGRADECIMIENTO

A la directiva de la empresa BUILDERECUADOR CIA.LTDA. conformada por el Mgtr. Arq. Jasmany Romero Espinoza y el Mgtr. Arq. Ronald Torres Ortiz, quienes me brindaron su confianza para desarrollar mi trabajo de titulación en sus instalaciones y por apostar a ideas innovadoras en beneficio de las empresas en crecimiento.

A mi tutora de tesis, la Mgtr. Diana María López Álvarez, por la orientación y ayuda que me brindó durante la realización de mi trabajo de titulación.

A mis amigos, quienes han estado presentes durante mis años de universidad y que con su ayuda y consejos han aportado significativamente a este logro.

CERTIFICACIÓN DE REVISIÓN FINAL

ANEXO N°16

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL

Samborondón, 8 de noviembre de 2022

Magíster
Mgrt. Erika Ascencio Jordán
Decana de la Facultad
Facultad de Ingenierías
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **RED PRIVADA REMOTA MONTADA EN RASPBERRY PI PARA LA GESTIÓN SEGURA DE LOS RECURSOS INFORMÁTICOS ENTRE LAS OFICINAS DE BUILDERECUADOR CIA.LTDA.** según PROPUESTA TECNOLÓGICA; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **RIVERA MORLA LUIS ALBERTO** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

DIANA MARIA LOPEZ ALVAREZ

Firmado digitalmente por DIANA MARIA LOPEZ ALVAREZ
Nombre de reconocimiento (DN): cn=DIANA MARIA LOPEZ ALVAREZ, serialNumber=0210222020356, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, o=SECURITY DATA S.A. 2, c=EC
Fecha: 2022.11.08 08:41:06 -05'00'

Mgtr. Diana Lopez Alvarez

Tutora

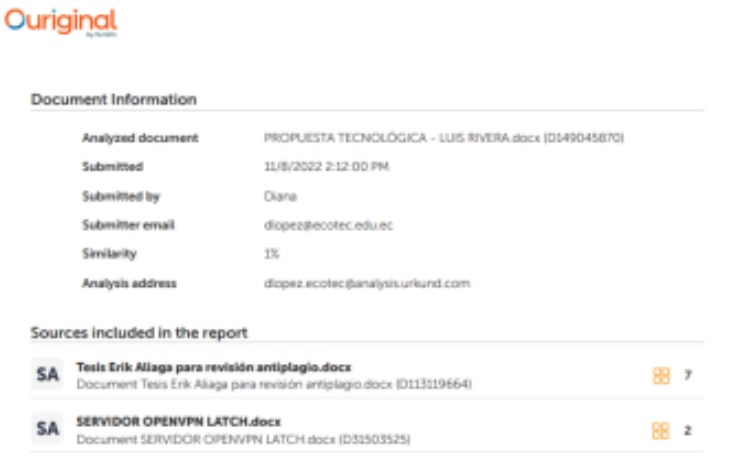
CERTIFICADO DE PORCENTAJE DE COINCIDENCIAS DE PLAGIO

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado LOPEZ ALVAREZ DIANA MARIA, tutor del trabajo de titulación "RED PRIVADA REMOTA MONTADA EN RASPBERRY PI PARA LA GESTIÓN SEGURA DE LOS RECURSOS INFORMÁTICOS ENTRE LAS OFICINAS DE BUILDERECUADOR CIA.LTDA." elaborado por LUIS ALBERTO RIVERA MORLA, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN SISTEMAS.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 1% mismo que se puede verificar en el siguiente link https://secure.urkund.com/view/142062627-133018-899695#/exported. Adicional se adjunta print de pantalla de dicho resultado.



Ouriginal

Document Information

Analyzed document	PROPUESTA TECNOLÓGICA - LUIS RIVERA.docx (D149045870)
Submitted	11/8/2022 2:12:00 PM
Submitted by	Diana
Submitter email	dlopez@ecotec.edu.ec
Similarity	1%
Analysis address	dlopez.ecotec@analysis.urkund.com

Sources included in the report

SA	**Tesis Erik Aliaga para revisión antiplagio.docx** Document Tesis Erik Aliaga para revisión antiplagio.docx (D113119664)	7
SA	**SERVIDOR OPENVPN LATCH.docx** Document SERVIDOR OPENVPN LATCH.docx (D31503525)	2

DIANA MARIA LOPEZ ALVAREZ

FIRMA DEL TUTOR
DIANA LOPEZ A.

RESUMEN

En la presente propuesta tecnológica se desarrolló una red privada remota, basada en la tunelización de información mediante el hardware Raspberry Pi para la gestión segura de los recursos informáticos entre las oficinas de BUILDERECUADOR CIA.LTDA.

Para lo cual, previamente se analizó la problemática que presentó la empresa y se propuso una alternativa de solución tecnológica que logre solventar sus requerimientos. Para buscar una solución tecnológica en el capítulo 1 se realizó una revisión general de conceptos generales entorno a la Red Privada Virtual (VPN), sus características, diferentes protocolos y ventajas de implementar OpenVPN, también se analizó los beneficios de la utilización del Raspberry Pi 4, así como también se analizó los roles y características de Windows Server 2019. En el capítulo 2 se desarrolló la metodología del proceso de la propuesta tecnológica con un enfoque de tipo cualitativo. En el capítulo 3 se efectuó un análisis e interpretación de los resultados de la entrevista que se realizó al presidente de la empresa BUILDERECUADOR CIA.LTDA.

Finalmente, en el capítulo 4 se detalló la implementación de la solución tecnológica que se dividió en 3 partes: la primera corresponde a la comunicación encriptada por medio de VPN, la segunda consiste en el almacenamiento de información confidencial de la empresa en un servidor de archivos y la tercera contempla la administración de usuarios y equipos. Una vez finalizado la implementación de esta propuesta tecnología, se comprobó su correcta operación la cual fue recibida a satisfacción de la empresa.

Palabras Claves: VPN, Raspberry Pi, Windows Server, file server, directorio activo

ABSTRACT

In this technological proposal, a remote private network was developed, based on the tunneling of information through Raspberry Pi hardware for the secure management of computer resources between the offices of BUILDERECUADOR CIA.LTDA.

For which, the problems presented by the company were previously analyzed and an alternative technological solution was proposed to solve their requirements. To find a technological solution in chapter 1, a general review of general concepts around the Virtual Private Network (VPN), its characteristics, different protocols and advantages of implementing OpenVPN was carried out, the benefits of using the Raspberry Pi 4 were also analyzed. , as well as the roles and characteristics of Windows Server 2019 were analyzed. In chapter 2, the methodology of the technological proposal process was developed with a qualitative approach. In chapter 3, an analysis and interpretation of the results of the interview with the president of the company BUILDERECUADOR CIA.LTDA.

Finally, in chapter 4, the implementation of the technological solution was detailed, which was divided into 3 parts: the first corresponds to encrypted communication through VPN, the second consists of the storage of confidential information of the company in a file server. and the third contemplates the administration of users and equipment. Once the implementation of this technology proposal was completed, its correct operation was verified, which was received to the satisfaction of the company.

Keywords: VPN, Raspberry Pi, Windows Server, file server, active directory

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

A través del tiempo, la tecnología de información y comunicación se ha desarrollado según las necesidades de los usuarios y las demandas del mundo actual. El concepto de redes ha alcanzado su importancia en la intercomunicación a nivel corporativo con la implementación de la Red Privada Virtual (VPN) que permite compartir información importante, sensible y privada, entre los colaboradores de una empresa, de forma encriptada, rápida y confiable (Carpentier, 2018).

Cada vez más la VPN es implementada en empresas públicas y privadas por sus facilidades y ventajas para los equipos de trabajo multidisciplinarios de las empresas. El acceso a contenido de forma remota en cualquier lugar y hora, mejora la saturación de tráfico de datos por ser una red privada. Tiene un control único de conexión y ajustes para sus dispositivos, además es flexible en cuanto a incorporar o disminuir usuarios a la red. Pero lo relevante es que permite mantener la privacidad de la información en la red y que su acceso sea únicamente para los trabajadores de la empresa.

La VPN de una empresa también puede extender su aplicabilidad hacia sus diferentes oficinas ubicadas en cualquier parte del mundo que requieran de una interconectividad permanente. Como es el caso de la empresa constructora BUILDERECUADOR CIA.LTDA. que fue creada en el 2021 y demanda de un servidor privado que le proporcione un servicio de conexión entre sus oficinas ubicadas en las ciudades de Loja y Guayaquil.

El presente trabajo de titulación propone una Red Privada Virtual (VPN) en la empresa constructora BUILDERECUADOR CIA.LTDA. La empresa cuenta con un equipo de trabajo especializado en el ámbito de la construcción y ligados a las nuevas plataformas digitales de trabajo, por lo que requieren un sistema de transferencia y almacenamiento de información de sus proyectos de forma ágil, efectiva y segura a través de una red privada encriptada.

Contexto histórico

En su momento, las empresas públicas y privadas cuya información era de carácter reservada y confidencial, temían sobre las vulnerabilidades informáticas que podrían existir al utilizar conexiones abiertas a Internet (Tanenbaum, 2012).

Por tal motivo, se creó la Red Privada Virtual (en lo adelante VPN) para que las conexiones fueran más seguras de lo que eran y que los usuarios remotos pudieran acceder y usar los archivos de la empresa sin filtrar su documentación reservada.

Los protocolos de tunelización que son implementados en las conexiones seguras utilizan encriptación de alto nivel, por lo que los datos transferidos no podrán ser utilizados sin autorización, aunque éstos hayan sido sustraídos. Es por ello, que la utilización de la VPN se ha difundido entre los usuarios por los beneficios que brinda ante las amenazas informáticas en conexiones y dispositivos.

Las necesidades actuales hacen que las empresas se reinventen y busquen mecanismos de defensa y protección ante cualquier vulnerabilidad informática que se presente; es por ello que el presente trabajo de titulación está enfocado a la implementación de una Red Privada Virtual en la empresa constructora BUILDERECUADOR CIA.LTDA., para la transferencia y almacenamiento de datos y reemplazar los medios convencionales e inseguros que actualmente utiliza, con el fin de manejar la información que se genera de cada proyecto de forma coordinada y confiable.

Antecedentes

En esta sección se demuestra la efectividad de la propuesta tras exponer los argumentos y conclusiones de proyectos relacionados con la gestión segura de los recursos informáticos empleando servidores VPN.

Pallo & Reyes (2015) señalan que su implementación de una Red Privada Virtual que utiliza una solución de conectividad segura basada en OpenVPN para un sistema de telemedicina, mejoró la comunicación entre el Hospital Provincial General Docente Ambato y sus centros de salud, beneficiando la atención médica. (Pallo & Reyes, 2015)

Además del sector de la salud, la red de comunicación VPN sobre internet puede aplicarse a un distribuidor autorizado de una telefónica. Como indica Martel (2019) que aseguró que las Redes Privadas Virtuales son una solución flexible y económica para las organizaciones de telefonía, como Claro Perú, que necesiten tener una comunicación segura con sus proveedores, clientes y sucursales sin invertir en redes costosas y que son utilizadas para el mismo propósito. (Martel, 2019)

De igual forma coincide Quishpe (2021) donde señala que su implementación de una VPN utilizando herramientas de software libre para la Comisión Fullbright del Ecuador, se realizó con poca inversión económica a diferencia de otras soluciones que requieren de equipos y licencias de uso. (Quishpe, 2021)

De lo expuesto, se concluye que la implementación de una Red Privada Virtual es óptima para la comunicación entre dependencias de una misma empresa, cuya inversión económica es asequible comparada con otras soluciones que ofrece el mercado.

El presente trabajo de titulación analiza el diseño e implementación de una VPN (Red Privada Virtual) en la empresa constructora BUILDERECUADOR CIA.LTDA para la comunicación entre sus oficinas ubicadas en las ciudades de Loja y Guayaquil con sus usuarios remotos, basados en los requerimientos de la empresa.

La empresa lleva a cabo varios proyectos inmobiliarios, los cuales son planificados entre el equipo de trabajo de ambas oficinas y requieren de una comunicación constante para acordar diseños, presupuestos, cronogramas, citas con proveedores, entre otros. Es por ello, que la empresa necesita un medio común de transferencia y almacenamiento de datos para el intercambio de información y revisión de avances de los proyectos en curso.

Planteamiento del problema a resolver

Tras una revisión de las necesidades de la empresa constructora BUILDERECUADOR CIA.LTDA., se constató la utilización de medios convencionales para la transferencia de datos como son los correos electrónicos corporativos, dispositivos externos como discos duros y memorias externas, y el uso de páginas web como WeTransfer para enviar y recibir archivos de gran tamaño.

Para el almacenamiento de la información crean carpetas dentro de las computadoras de escritorio o computadoras portátiles y utilizan plataformas de almacenamiento en la nube como Google Drive.

Los sistemas informáticos de la empresa están protegidos por un antivirus y el firewall que incluyen las computadoras.

Así mismo, se constató que la empresa opera desde la ciudad de Loja y Guayaquil, y su equipo de trabajo labora en oficina o se movilizan a los sitios de las obras en distintos puntos del país; por lo que se requiere de una conexión remota segura para que puedan acceder a la información de la empresa, con el fin de mantener una base de datos compartida que se actualice de acuerdo con las actividades diarias de la empresa.

Para lograr esta interconexión se necesitará un hardware que actúe como servidor, por lo que se utilizará un sistema simplificado de computación llamado Raspberry Pi, el cual reducirá los costos y tiempo de implementación del sistema.

Una vez puesta en operación, se creará un túnel seguro entre el cliente y la red protegida. Esta conexión segura permite que el usuario trabaje en su computadora

como si estuviera dentro de su puesto de trabajo en la oficina (Vega, 2021). Lo que es más importante, sirve como un medio seguro para acceder y contribuir a los archivos almacenados en el servidor de la empresa (Perez, 2020).

Esta continuidad de datos es vital para respaldar un plan integral de recuperación ante desastres. Según Carpentier (2018), un plan de recuperación de datos es necesario en las empresas, el cual debe incluir copias de seguridad periódicas de los servidores y los archivos que contienen. (Carpentier, 2018)

El túnel creado permite que todo el tráfico de Internet se dirija desde la computadora del usuario; y a pesar de que puede generar tiempos de carga más largos, garantiza que los usuarios estén protegidos contra una amplia gama de ataques informáticos

Por lo general, las empresas suelen utilizar una Red Privada Virtual (VPN) para brindar a sus colaboradores accesos remotos a las aplicaciones y datos internos, o para crear una única red compartida entre varias oficinas. En ambos casos, el objetivo final es evitar que el tráfico web, en particular el tráfico que contiene datos importantes, quede expuesto en la internet abierta o cuando el usuario se conecte a redes públicas, lo cual puede comprometer la filtración de información a través de ciberataques (Ezra, 2021).

Los resultados esperados en el presente trabajo de titulación es que se establezca una conexión segura que encripte la comunicación entre las oficinas de BUILDERECUADOR CIA.LTDA., lo cual facilitará a su equipo que trabajan en las instalaciones y permitirá que puedan conectarse desde su computadora o dispositivo móvil directamente a la red interna de la empresa. Como indica Kanich (2018), un trabajador que realiza sus funciones de manera remota y dicha conexión de red interna debe realizarse a través de la internet pública, puede ocasionar la exposición de su tráfico a ataques en ruta y otros métodos de espionaje en datos confidenciales, por lo que encriptar ese tráfico con una VPN puede contribuir a su seguridad.

De lo expuesto, se detallan los siguientes problemas: la empresa no cuenta con un medio para poner en práctica una comunicación segura para el traslado de

información; no se tiene acceso remoto a recursos que se encuentran en las oficinas de Loja y Guayaquil; no existe un medio informático para realizar la actualización o aportación de la información de los proyectos ejecutados o en ejecución de forma simultánea entre las dos oficinas. Bajo esta perspectiva se plantea la pregunta problémica.

Pregunta problemática

¿Cómo mejorar la gestión segura de recursos informáticos entre las oficinas de BUILDERECUADOR CIA.LTDA?

Alcance

El alcance de esta propuesta tecnológica es proponer a la empresa constructora BUILDERECUADOR CIA.LTDA un diseño e implementación de Red Privada Remota para la gestión segura de sus recursos informáticos, es por esta razón que se sugiere utilizar la tecnología de Raspberry Pi para el alojamiento de un servidor VPN basado en el protocolo OpenVpn, y además implementar de un file server y directorio activo para la gestión segura de los archivos.

OBJETIVOS

Objetivo general

Desarrollar una Red Privada Remota, basada en la tunelización de información mediante el hardware Raspberry Pi para la gestión segura de los recursos informáticos entre las oficinas de BUILDERECUADOR CIA.LTDA.

Objetivos específicos

1. Identificar referentes tecnológicos de seguridad basada en tunelización sobre Raspberry Pi.

2. Analizar la situación actual de la red de la empresa en el manejo de transferencia y almacenamiento de información.

3. Determinar los requerimientos de la empresa para la solución tecnológica propuesta.

4. Diseñar una red privada remota que ayuden a la seguridad del manejo de la información de la empresa BUILDERECUADOR CIA.LTDA. de acuerdo con las necesidades y requerimientos planteados.

JUSTIFICACIÓN

Según Chávez (2019), las empresas adoptan avances tecnológicos como un requisito fundamental para lograr sus objetivos. La utilización de la tecnología para establecer comunicación y almacenamiento de datos puede vulnerar su seguridad por los delitos informáticos que pueda existir. De allí surge la necesidad de las empresas por proteger su data digital. (Chavez, 2019)

Por tal motivo, es necesario mejorar el tráfico y almacenamiento de la información de la empresa BUILDERECUADOR CIA.LTDA. ya que con su correcto manejo y funcionamiento se mejorará la comunicación entre sus oficinas y representará un ahorro en tiempo, costo y recurso humano.

Esta propuesta tratará sobre el análisis e implementación de OpenVPN en una Raspberry Pi, el cual se diferencia de otros tipos de VPN, ya que es un protocolo de cifrado de código abierto. Esto significa que los usuarios podrán utilizar de una red Fuenteblemente segura gracias a la biblioteca OpenSSL que no tiene ningún propietario; además de la implementación de un file server configurado en Windows Server 2019 y un directorio activo.

Conforme al requerimiento de la empresa el file server servirá para el almacenamiento de archivos como planos arquitectónicos, imágenes y renders, presupuestos entre otros.

MARCO TEORICO

CAPITULO 1

1. CAPÍTULO 1: MARCO TEÓRICO

Este capítulo consta de un compendio teórico asociado con los distintos conceptos esenciales para el desarrollo de esta propuesta tecnológica.

1.1. Seguridad en redes informáticas

Según Valencia (2020) la circulación de la información confidencial en las redes es motivo de preocupación para los usuarios y empresas, por lo que se busca proteger contra el uso fraudulento de sus datos o contra intrusiones malintencionadas en los sistemas informáticos. (Valencia, 2020)

Los virus proporcionados por el atacante informático se propagan en los archivos descargados sin el conocimiento de los usuarios y destruyen documentos e incluso provocan la pérdida total de la información almacenada en las computadoras.

La tendencia actual es implementar mecanismos de control de acceso y protocolos seguros que brinden varios servicios como:

- La autenticación que consiste en pedir a un usuario que demuestre su identidad (proporcionando una contraseña o datos biométricos)
- La confidencialidad que garantiza a los usuarios que un tercero malicioso no podrá leer ni explotar ningún dato.
- La integridad que asegura a los usuarios que sus datos no han sido modificados indebidamente durante la transmisión en la red, por lo que el cifrado evita que los datos sean leídos por usuarios no autorizados.

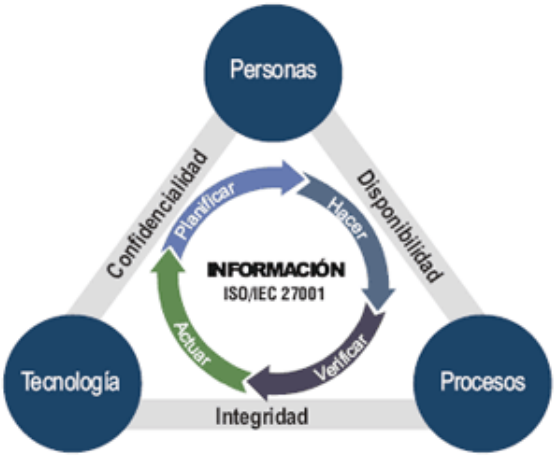
El cifrado de la información y la firma digital utilizan sofisticados algoritmos de cálculo que funcionan con claves. El algoritmo es simétrico si la clave que cifra el mensaje es idéntica a la utilizada para el descifrado; es asimétrica cuando se utilizan claves diferentes para las dos operaciones (Gutierrez & Tena, 2013).

El proceso simétrico se conoce desde la Antigüedad ya que era necesario poseer o conocer la clave secreta elegida por el remitente para decodificar el mensaje al recibirlo. En este caso, la seguridad del sistema se basa en la seguridad de

transmisión de la clave secreta. Con el aumento del poder de cómputo de las computadoras actuales, las claves utilizadas son secuencias de datos binarios son cada vez más largos y más complejas.

La figura 1 representa la relación que tiene la confidencialidad, disponibilidad e integridad con los procesos.

Figura 1. *Confidencialidad, disponibilidad e integridad*



Fuente: Tomado de (Gutierrez & Tena, 2013)

1.1.1. Amenazas en redes informáticas

La seguridad de las redes implica controles de protección específicos agregados a una red. Estos controles han evolucionado a lo largo de los años y seguirán evolucionando a medida que se investigue más sobre la defensa de una red y los atacantes informáticos descubran nuevos métodos de ataque.

Vega (2021) recalca que comprender el entorno de amenazas actual y las vulnerabilidades de la red es esencial para tener los mejores controles para brindar protección. También es importante comprender qué tipos de controles están disponibles, de modo que pueda utilizar los proveedores, las soluciones y las configuraciones adecuadas para la red.

1.1.2. Entorno de amenazas actuales

Según Colina & Espinoza (2021), el uso masivo de la tecnología de la información y comunicaciones ha provocado que la sociedad sea dependiente de ella y que su información esté expuesta a los ataques o amenazas informáticas por la ausencia de controles eficientes. (Colina & Espinoza, 2021)

Las amenazas son violaciones potenciales que afectan la confidencialidad, disponibilidad o integridad de los recursos. Las amenazas pueden incluir la divulgación de datos confidenciales, la manipulación de datos o incluso la denegación de acceso a un servicio (Colina & Espinoza, 2021). El contexto de amenazas actual consiste en información sobre amenazas, actores maliciosos y el vector de amenazas a través del cual puede ocurrir un ataque.

El actor malicioso es una persona o un grupo de personas que quieren causar daño usando amenazas existentes. Perez (2020) realiza un símil con el robo de un computador portátil, indica que el ladrón es el actor malicioso y el vector de amenaza es la ruta que permite que se lleve a cabo el ataque.

Una vulnerabilidad es una debilidad o falla que los actores maliciosos pueden usar para violar las políticas de seguridad. Retomando el ejemplo del computador portátil, el diseño de éste es ligero y es fácil de transportar, por lo que son características que atraen a muchos clientes. Al mismo tiempo, estas características son puntos débiles que aumentan la probabilidad del robo del computador portátil, por lo que los controles de seguridad, como cerraduras de puerta, ralentizan al delincuente y reducen la probabilidad de que se produzca un robo, lo que reduce el riesgo general.

La confidencialidad, integridad y disponibilidad son los atributos principales que definen el propósito de un proceso de seguridad de la información. Este proceso involucra muchas estrategias y actividades, y cada uno pertenece a una de estas tres fases: prevención, detección y remediación (Vega, 2021).

1.1.3. Normativa legal sobre la seguridad informática en el Ecuador

Según el Código Orgánico Integral Penal (2014) los delitos contra la seguridad de los activos de los sistemas de información y comunicación, se sancionan en el

Ecuador con los siguientes artículos y que son concordantes con la seguridad informática en las redes:

Esta tabla muestra los diferentes crímenes informáticos que puede haber con años que el individuo puede pasar privativo de la libertad por cometer aquellos delitos.

Tabla 1. *Normativa legal según el código orgánico penal*

No. Artículo	**Concepto**	**Contenido**	**Pena privativa de libertad**
229	Revelación ilegal de base de datos	Este artículo señala que una persona que, en provecho propio o de un tercero, revele información registrada en archivos, base de datos, entre otros, a través de un sistema informático o de telecomunicaciones y materialice de forma voluntaria o intencional la acción de violación de la privacidad de las personas.	3 a 5 años
230	Interceptación ilegal de datos	Este artículo señala que: 1. La persona, en provecho propio o de un tercero intercepte, escuche, desvíe, grabe u observe, un dato informático en el interior de un sistema informático con la finalidad de obtener información registrada o disponible.	3 a 5 años
231	Transferencia electrónica de activo patrimonial	Este artículo señala que la persona que, con ánimo de lucro, manipule o modifique el funcionamiento de un sistema informático para asegurar la transferencia o apropiación no consentida de un activo patrimonial de otra persona.	3 a 5 años
232	Ataque a la integridad de sistemas informáticos	Este artículo señala que la persona que destruya, dañe, borre, altere, cause mal funcionamiento o suprima datos informáticos de sistemas de	3 a 5 años

No. Artículo	Concepto	Contenido	Pena privativa de libertad
		información o telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen	
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	Este artículo señala que la persona que, sin autorización acceda en todo o parte a un sistema informático o de telecomunicaciones para explotar ilegítimamente el acceso logrado, desviar o redireccionar de tráfico de datos o voz que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos.	3 a 5 años

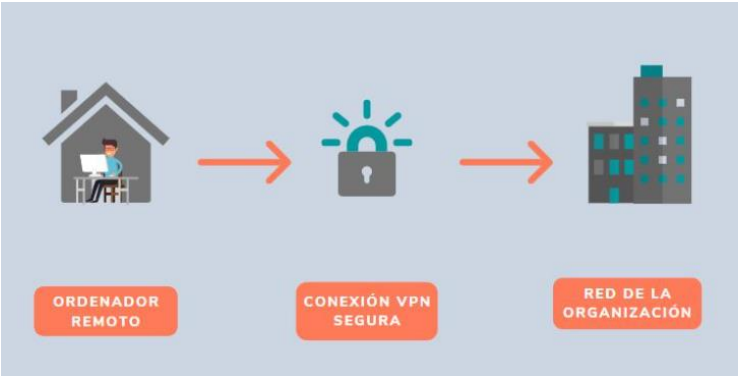
Fuente: Elaboración propia

1.2. Red remota

Según Dordoigne (2015) cualquier tecnología de red puede brindar a los usuarios acceso a servicios de red esenciales desde ubicaciones remotas.

La figura 2 muestra lo que básicamente consiste una conexión remota hacia la red de una organización.

Figura 2. *Red remota*



Fuente: Tomado de (Hubspot, 2019)

El acceso remoto generalmente brinda a los usuarios remotos acceso a los siguientes servicios en la red de una empresa:

- Servicios de archivo e impresión
- Aplicaciones cliente/servidor como aplicaciones de base de datos
- Aplicaciones para la administración remota de redes

Dordoigne (2015) propone las siguientes funciones principales de un acceso remoto:

Control remoto: Se utiliza un programa para tomar el control de la consola de una computadora de forma remota. Los administradores suelen utilizar este método para solucionar problemas del servidor de forma remota. Sin embargo, debido a que la conexión remota a menudo se realiza a través de un módem analógico, la restricción del ancho de banda a menudo hace que el acceso al control remoto sea lento y entrecortado.

Nodo remoto: Se utiliza un dispositivo de acceso remoto para proporcionar una puerta de enlace para que los usuarios accedan a archivos, impresión y otros servicios en la red de una empresa desde ubicaciones remotas, como desde una computadora portátil mientras están de viaje.

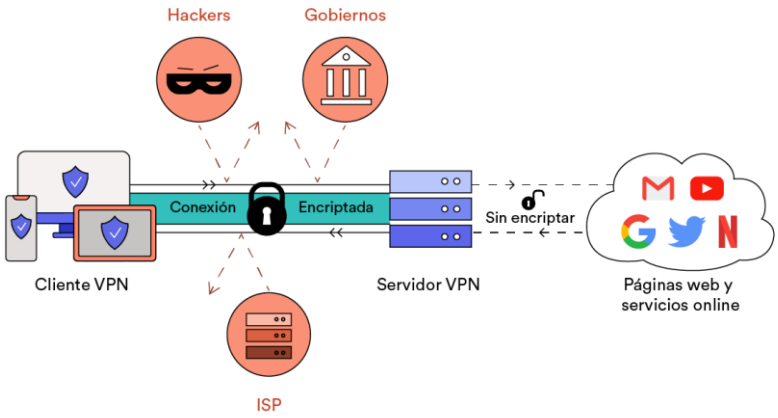
1.2.1. Cifrado de información en la tunelización

El cifrado es un término utilizado para describir los métodos que ocultan el verdadero significado de los mensajes mediante código, especialmente para evitar el acceso no autorizado a la información de los mensajes (Chavez, 2019).

No todos los usuarios de Redes Privadas Virtuales (VPN) se preocupan por el cifrado, pero muchos están interesados y se benefician del cifrado sólido de extremo a extremo. Para lograr el cifrado de extremo a extremo, se necesita un proceso llamado tunelización VPN.

En la figura 3 se puede apreciar cómo se crea la tunelización de la información evitando que terceras puedan interceptar la comunicación y traslado de los datos.

Figura 3. *Tunelización de la información*



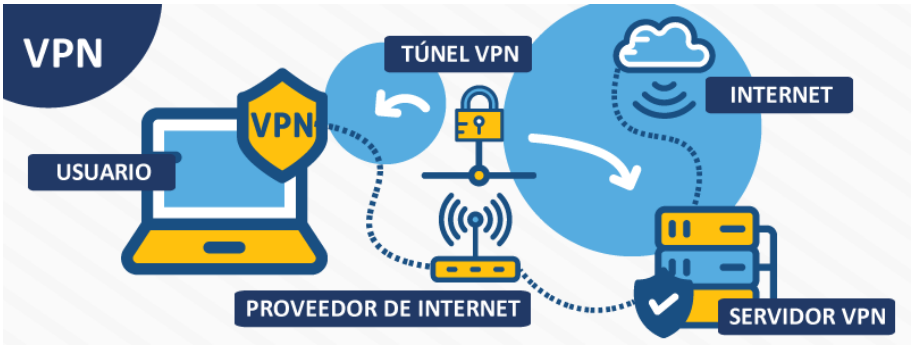
Fuente: Tomado de (Jones, 2022)

1.3. Red Privada Virtual (VPN)

Según NordVPN (2022) una VPN es una herramienta que protege de la conexión durante la navegación por el internet. Además, la VPN oculta la IP y encripta los datos enviados y recibidos a través de la red, por lo que resulta inaccesible por parte de terceros que traten de interceptar la conexión. Es decir, que esta red permite navegar de manera privada y mantener la IP lejos del alcance de posibles ciberataques.

En la figura 4 se puede apreciar la conexión de los clientes VPN a los servidores de red remota.

Figura 4. *Conexión vpn a servidor*



Fuente: Tomado de (NordVPN, 2022).

Las Redes Privadas Virtuales (VPN) crean una conexión con la red desde otro punto final o sitio. Por ejemplo, los usuarios que trabajan desde casa se conectan habitualmente a la red de la empresa a través de una VPN. Los datos entre los dos puntos están cifrados y los usuarios deberán autenticarse para permitir la comunicación entre el dispositivo y la red.

Tanenbaum (2012) afirma que las redes conocidas como VPN se pueden usar para unir las redes individuales, ubicadas en distintos sitios, en una sola red extendida. En otras palabras, el hecho de que un usuario esté a 15 mil kilómetros de distancia de sus datos no lo impide de utilizarlo como si fueran locales.

1.3.1. Características de las VPN

Abundantes ubicaciones de servidores

Una VPN oculta los datos de un usuario cifrándolos con un túnel creado entre el dispositivo del usuario y el servidor web de la VPN. Luego, el usuario toma la dirección IP del servidor web (en lugar de su verdadera IP), y hace que el usuario aparezca en una ubicación geográfica diferente a la que realmente se encuentra, siendo una ventaja de la VPN.

Esto puede tener muchos usos, como poder acceder a servicios de transmisión o sitios de compras específicos de un determinado país, sin pasar por lo que se conoce como bloqueo geográfico. (Ezra, 2021)

Es importante conocer que cualquier proveedor tendrá una distribución de cobertura en una amplia gama de países, lo que le brindará más opciones en general. Además, cuantos más servidores haya disponibles en cada ubicación, es mejor ya que es menos probable que se sobrecarguen, y obtendrá mejores niveles de rendimiento.

Aplicaciones móviles

Cualquier VPN ofrecerá un software de cliente para una PC con Windows. Sin embargo, el valor real de una VPN está en su soporte móvil y en mantener su dispositivo seguro mientras accede a Wi-Fi público cuando se está fuera de la red LAN.

Por lo tanto, al elegir una VPN, el administrador debe asegurar de que sea compatible con las plataformas de los equipos de hardware.

Interruptor de apagado integrado

Ezra (2021) asegura que ningún servicio VPN es completamente seguro y pueden ser susceptibles a filtraciones de IP, lo que expone la verdadera dirección IP del cliente cuando está conectado a internet. Esto puede ocurrir con mayor frecuencia cuando el servicio VPN se sobrecarga.

La solución según Martel (2019) es un interruptor de interrupción de VPN, que puede monitorear la falla de la conexión VPN. Cuando la conexión se cae, es cuando la verdadera IP quedará expuesta y en este caso, un interruptor de interrupción cierra la transferencia de datos.

En conclusión, como sugiere el nombre, elimina la conexión evitando que se transmitan datos no cifrados (y que se filtre la verdadera IP). Si bien no todos los

servicios VPN ofrecen un interruptor de interrupción, algunos sí lo hacen, con la función integrada en el software del cliente.

Servidores DNS anónimos

La resolución de DNS (Sistema de Nombres de Dominio) es el proceso que convierte la dirección que ingresa en la barra de direcciones del navegador web, en la dirección IP que utiliza la red mundial para dirigir el tráfico al usuario. La mayoría de los usuarios realizan la traducción de DNS, de forma predeterminada, a través del ISP, aunque esto se puede cambiar fácilmente.

Por supuesto, cuando se usa una VPN, el objetivo es la privacidad y, por lo tanto, se requiere que la VPN esté configurada para estar protegido de los ataques informáticos también en el proceso de traducción de DNS (manteniendo los datos alejados de las miradas indiscretas del ISP) (Ezra, 2021).

Si bien el traductor de DNS de Google se usa a menudo por su velocidad, no sería la mejor elección desde una perspectiva de privacidad. Más bien, hay servicios de DNS que están diseñados para mejorar de la privacidad.

Política de no registro

Los servicios VPN difieren en sus políticas de registro. Algunas VPN pueden conservar elementos de la actividad de navegación durante meses, por ejemplo, datos potenciales que podrían entregarse a las autoridades, si así lo solicitan.

1.3.2. Tipos de red privada virtual (VPN)

La red privada virtual (en adelante VPN) se compone de dos tipos, los cuales se detallan a continuación:

VPN de acceso remoto

El primer tipo de VPN permite al usuario conectarse a una red privada y acceder a todos los servicios y recursos de forma remota, la cual se produce a través de internet de forma segura y es útil tanto para el usuario doméstico como para usuario comercial.

Este último se lo puede emplear cuando un colaborador que se encuentra fuera de su estación de trabajo, utiliza una VPN para conectarse a la red privada de su empresa y accede de forma remota a archivos y recursos cuando lo requiera.

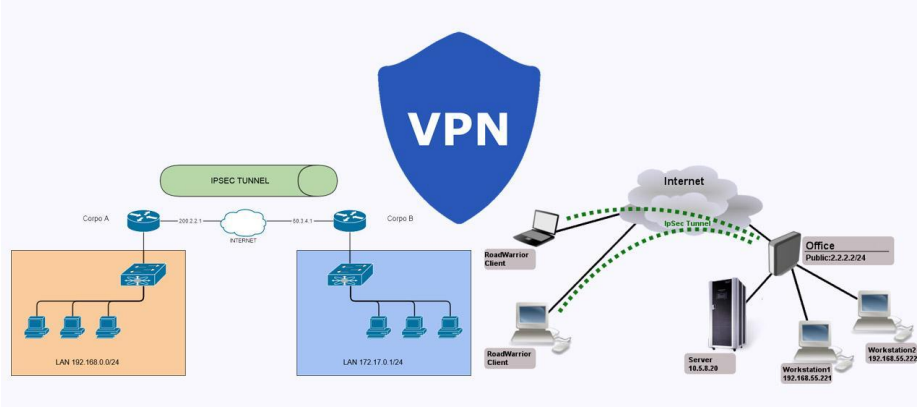
Por otro lado, los usuarios privados o usuarios domésticos de VPN utilizan principalmente su servicio para evitar las restricciones regionales en internet y puedan acceder a sitios web bloqueados, con la seguridad y privacidad que una VPN de acceso remoto les ofrece. (Tanenbaum, 2012)

VPN de sitio a sitio

La VPN de sitio a sitio también se denomina VPN de enrutador a enrutador y se usa comúnmente en las grandes empresas u organizaciones con sucursales en diferentes ubicaciones para conectar la red de una ubicación de oficina a la red en otra ubicación de oficina; lo cual crea un “puente imaginario” entre ellas, a pesar de que se encuentran geográficamente distantes, a través de la conexión de la VPN por la internet, manteniendo una comunicación segura y privada entre las redes. (Tanenbaum, 2012)

La figura 5 muestra la diferencia en el diagrama de conexión entre la VPN de acceso remoto en contraste con el de sitio a sitio.

Figura 5. *Descripción gráfica de VPN acceso remoto y VPN sitio a sitio*



Fuente: Tomado de (Luz, 2022)

Cuando varias oficinas de la misma empresa están conectadas utilizando el VPN de sitio a sitio, se denomina VPN basada en intranet; y cuando las empresas utilizan el tipo de VPN de sitio a sitio para conectarse a la oficina de otra empresa, se denomina VPN basada en extranet. Cuando la autenticación se valida entre los dos enrutadores, es ahí donde comienza la comunicación.

1.3.3. Tipos de protocolos de red privada virtual (VPN)

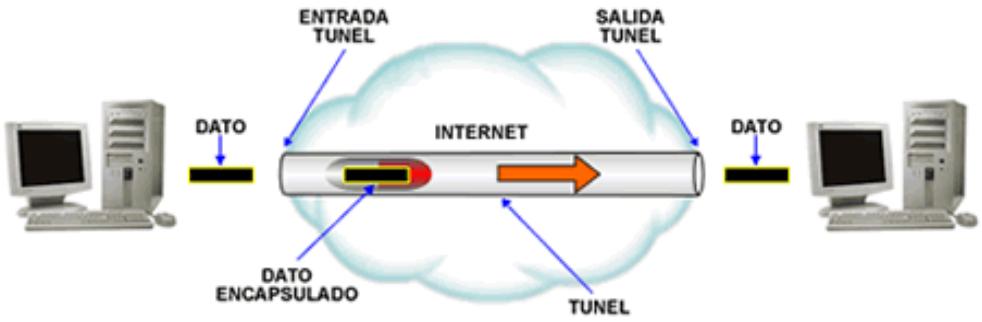
Seguridad del protocolo de Internet (IPSec)

La seguridad del protocolo de Internet (IPSec), se utiliza para asegurar la comunicación de internet a través de una red IP; protege la comunicación del protocolo de internet al verificar la sesión y encripta cada paquete de datos durante la conexión (Katz, 2013).

La IPSec se ejecuta en dos modos: El modo de transporte, que cifra el mensaje en el paquete de datos; y el modo de tunelización, que cifra todo el paquete de datos. También se puede utilizar con otros protocolos para mejorar el sistema de seguridad (Ghanem & Ugwuanyi, 2022).

En la figura 6 se muestra como para establecer un túnel IPSec, dos pasarelas deben autentificarse y definir los algoritmos de seguridad y las claves que utilizarán para el túnel.

Figura 6. *Protocolo IPSEC*



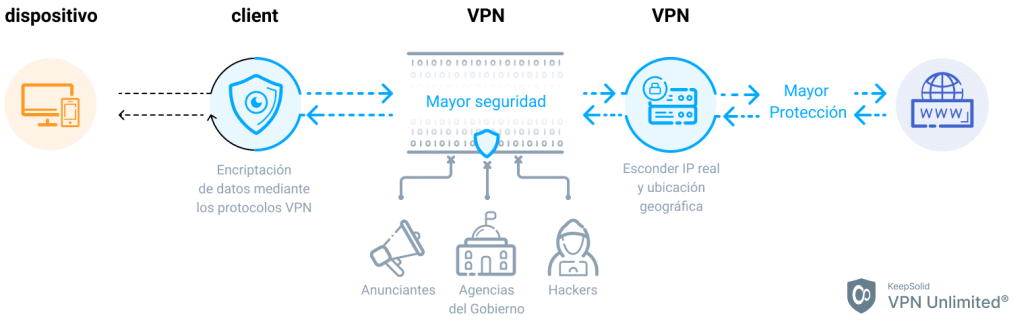
Fuente: Tomado de Huawei, 2018

Protocolo de tunelización de capa 2 o Layer 2 Tunneling Protocol (L2TP)

Es un protocolo de túnel que a menudo se combina con otro protocolo de seguridad VPN como es el IPSec, con el fin de establecer una conexión VPN altamente segura. El L2TP genera un túnel entre dos puntos de conexión; los protocolos L2TP y IPSec cifran los datos y mantienen una comunicación segura entre el túnel (Katz, 2013).

La figura 7 muestra como el protocolo se combina con otro para formar una conexión segura.

Figura 7. *Protocolo L2TP*



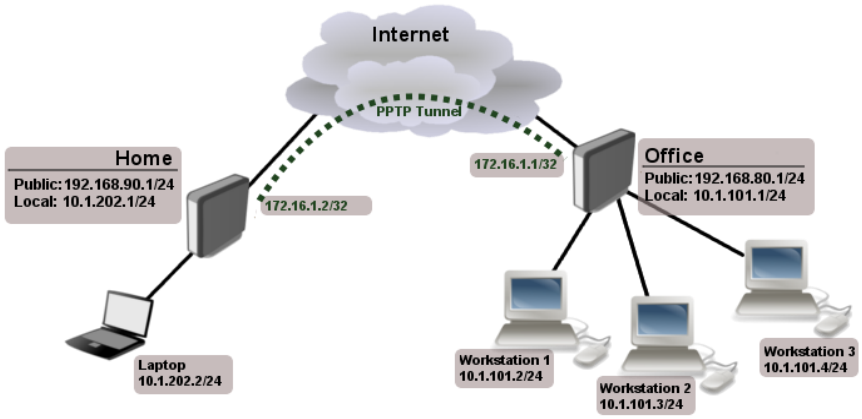
Fuente: Tomado de (VpnUnlimited, 2020)

Protocolo de tunelización punto a punto o Point-to-Point Tunneling Protocol (PPTP)

Este protocolo genera un túnel y confina el paquete de datos; además se utiliza para cifrar los datos entre la conexión. El PPTP es uno de los protocolos VPN más utilizados y ha estado en uso desde el lanzamiento inicial de Windows; también se usa en Mac y Linux. La ventaja de PPTP es su capacidad para brindar soporte multiprotocolo bajo demanda a las infraestructuras existentes en el lugar de trabajo, como internet. Esta capacidad permitiría a las empresas utilizar internet para crear VPN sin pagar líneas alquiladas.

En la figura 8 se muestra la interconexión que existe entre los dos servidores usando protocolo PPTP.

Figura 8. *Protocolo PPTP*



Fuente: Tomado de (Katz, 2013)

Secure Sockets Layer (SSL) y Transport Layer Security (TLS)

Los protocolos SSL y TLS generan una conexión VPN donde el navegador web actúa como cliente y se prohíbe el acceso del usuario a aplicaciones específicas en lugar de toda la red. Los sitios web de compras en línea suelen utilizar los protocolos SSL y TLS. Es fácil cambiar a SSL mediante navegadores web y casi no se requiere ninguna acción por parte del usuario, ya que los navegadores web vienen integrados con SSL y TLS. Las conexiones SSL tienen "https" en la inicial de la URL en lugar de "http" (Katz, 2013).

Se muestra en la figura 9 como al presentar el certificado de autentificación el servidor lee la llave encriptada y establece una sesión segura.

Figura 9. *Protocolo SSL Y TLS*

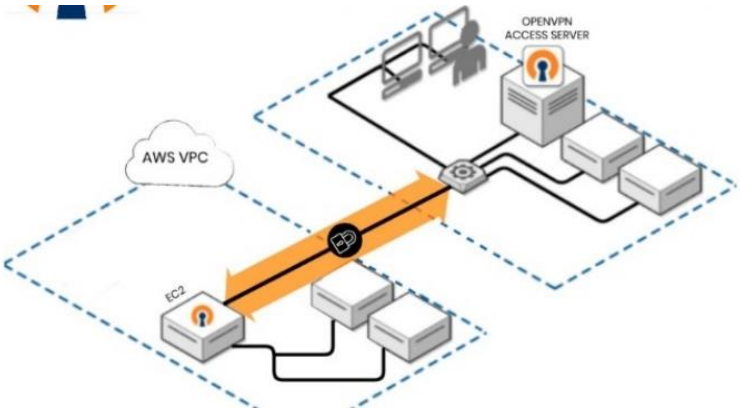
Fuente: Tomado de Informático seguro, 2016

VPN abierta

Es una VPN de código abierto que se usa comúnmente para crear conexiones de punto a punto y de sitio a sitio. Utiliza un protocolo de seguridad tradicional basado en el protocolo SSL y TLS. A continuación se detallará más sobre este protocolo el cual se implementará en la propuesta tecnológica.

En la figura 10 se puede apreciar la conexión encriptada que realiza el protocolo OpenVpn entre dos oficinas.

Figura 10. *Protocolo OpenVpn*



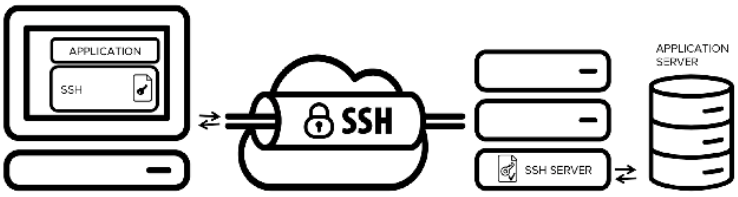
Fuente: Tomado de (Soto, 2021)

Shell seguro o Secure Shell (SSH)

Este protocolo asegura que el túnel VPN, a través del cual ocurre la transferencia de datos, esté encriptado. Las conexiones son generadas por un cliente SSH y los datos se transfieren desde un puerto local al servidor remoto a través del túnel encriptado.

En la figura 11 se puede notar una descripción gráfica de cómo se establece la conexión por medio de SSH.

Figura 11. *Protocolo SSH*



Fuente: Tomado de (Bastify, 2019)

A continuación, se detalla los diferentes protocoles de VPN y sus limitaciones según las características que provee:

En la tabla 2 se puede apreciar que los protocolos OpenVPN e IPSec/IKEv2 tienen mejores rendimientos en cuanto a las características que provee. El protocolo OpenVPN es muy bueno en la encriptación de datos, mientras que el protocolo IPSec/IKEv2 es muy bueno en la estabilidad de la conexión de internet. Fuente:

Tabla 2. Protocolos VPN

Protocolo VPN	Velocidad	Encriptación	Streaming	Estabilidad	P2P
OpenVPN	Rápido	Muy bueno	Bueno	Bueno	Bueno
IPSec/IKEv2	Rápido	Bueno	Bueno	Muy bueno	Bueno
Wireguard	Muy rápido	Bueno	Regular	Pobre	Bueno
SSTP	Regular	Bueno	Regular	Regular	Bueno
L2TP/IPSec	Regular	Bueno	Pobre	Bueno	Pobre
PPTP	Rápido	Pobre	Pobre	Bueno	Pobre

Fuente: Elaboración propia

1.3.4. Ventajas y desventajas de la Red Privada Virtual (VPN)

A continuación, se detallan algunas de las ventajas y desventajas de la implementación de una Red Privada Virtual en las empresas:

En la tabla 3 podemos notar las ventajas y desventajas que tienen las VPN.

Tabla 3. Ventajas y desventajas de las VPN

Red Privada Virtual (VPN)	
Ventajas	**Desventajas**
Seguridad en el traslado de información confidencial y delicada.	Puede llegar a ser compleja la configuración y debe de ser implementado por un administrador en redes
Varios elementos trabajando conjuntamente que proveen una mayor seguridad.	Es dependiente de los servicios del ISP o otras partes del internet. Si existen problemas con el ISP la conexión puede fallar.
Acceso a la información desde cualquier parte.	Requiere un administrador de redes para que genere el cliente VPN y los certificados de autentificación.

Puede hacerse uso de la banda existente de una empresa.	El hardware y software del VPN puede llegar a ser incompatible de diferentes distribuidores.
Provee encriptación de información y firewall para seguridad perimetral.	Consume banda ancha de la red.

Fuente: Elaboración propia

1.4. OpenVPN

La OpenVPN es una aplicación de código abierto para redes privadas virtuales (VPN), donde la aplicación puede crear un túnel de conexión punto a punto que ha sido cifrado. También utiliza claves privadas, certificado o nombre de usuario o contraseña para realizar la autenticación en la creación de conexiones.

1.4.1. Funciones de OpenVPN

La OpenVPN funciona como túnel de capa 2 para que pueda ejecutarse en tramas Ethernet, paquetes IPX y navegación de paquetes de la red de Windows (NETBIOS). Varias de las funciones se detallan a continuación:

- Proteger a los trabajadores de campo con el firewall interno.
- Las conexiones se pueden tunelizar a través de casi todos los túneles de firewall. Puede funcionar en sitios que utilizan el protocolo HTTPS.
- Soporte y configuración de proxy. Este protocolo tiene soporte de proxy y se puede configurar para ejecutarse como un servicio y TCP o UDP como servidor o cliente.
- Las interfaces virtuales permiten reglas de red y firewall muy específicas. Todas las regulaciones, restricciones y conceptos de mecanismos de reenvío como NAT se pueden usar con el túnel OpenVPN.
- Alta flexibilidad con amplias posibilidades de scripting. OpenVPN ofrece muchos puntos de partida para scripts individuales. Este script se puede utilizar para una variedad de propósitos, desde la autenticación hasta la conmutación por error o más.

- Brinda soporte transparente y de alto rendimiento para IP dinámicas. Este protocolo ya no necesita usar IP estáticas a ambos lados del túnel.
- Tanto el servidor OpenVPN como los clientes pueden estar en una red que solo utiliza direcciones IP privadas. Cualquier firewall se puede utilizar para enviar tráfico a otro túnel.
- Dispone de un diseño modular con un alto grado de simplicidad tanto en seguridad como en redes. No hay otras soluciones VPN que puedan ofrecer diferentes posibilidades en el mismo nivel de seguridad.

Según OpenVPN (2022), señala que este protocolo es una tecnología de próxima generación que le permite al usuario una conexión a las redes, dispositivos y servidores privados de una red LAN para construir una red moderna segura y virtualizada.

Sus conectores inteligentes e integrados le permiten enrutar el tráfico en las instalaciones o en la nube y también se puede conectar a cualquier red que el ecosistema de la empresa necesite, ya sea Amazon Web Services (AWS), Azure u otras.

Se incorpora también el filtrado de contenido basado en DNS para monitorear y bloquear nombres de dominio por categoría de contenido y detener amenazas sin necesidad de canalizar el tráfico de internet. Se hace cumplir el acceso a la red de confianza cero definiendo y aplicando políticas basadas en identidad, autenticación y autorización con Cyber Shield (OpenVPN, 2022).

Es importante recalcar que el protocolo depende de SSL/TLS, por lo tanto, se necesitará hacer declaraciones informáticas para la verificación de clientes VPN, es más, también validará con respaldos además de un nombre de usuario/clave secreta que se agrega al marco.

1.4.2. Comparaciones entre OpenVPN e IPSec

En una investigación realizada por Ghanem & Ugwuanyi (2022) se analizó el impacto de emplear OpenVPN e IPsec en el ancho de banda requerido para la

operación de activos de distribución en subestaciones de última generación Unidades Terminales Remotas (RTU). Este análisis mostró que OpenVPN agregó un promedio de 42 bytes a cada paquete dentro del túnel VPN, mientras que Internet Protocol Security (IPsec) contribuyó con una sobrecarga promedio de 64 bytes. Esto demostró que emplear IPsec requeriría más ancho de banda que OpenVPN.

También llegaron a una conclusión de que el protocolo OpenVPN es mucho más intuitivo de diseñar que IPsec, y debido a la extraordinaria compatibilidad con el área local, OpenVPN se puede encontrar en todos los sistemas operativos de área de trabajo, servidores e incluso teléfonos móviles.

La comparación entre OpenVPN e IPSec se señala a continuación:

En la tabla 4 se muestra las notables ventajas que posee OpenVpn sobre IpSec.

Tabla 4. Comparaciones y ventajas de OpenVPN sobre IPSec

OPENVPN	**IPSEC**
Protocolo de mejor rendimiento. Brinda alta velocidad hasta en conexiones con latencias altas que se ubican a grandes distancias.	Requiere más procesamiento de CPU y consume más banda ancha.
Encripta datos con certificados digitales y niveles altos de seguridad.	Verifica integridad de datos y encapsula la información dos veces haciendo de este menos eficiente en cuanto a rendimiento.
Tiene llaves de 160bits + 256bits.	Tiene llaves de 256bits.
Mayor compatibilidad de sistemas operativos	Soporta todos los sistemas operativos.
Usa la biblioteca de OpenSSL que le permite soportar diferentes algoritmos de encriptación.	Es encriptado usando protocolos IPSec estandarizados.
Resulta más estable y rápido sobre conexiones inalámbricas y celulares en las cuales la perdida de paquetes es muy común.	L2TP/PSec es más complejo que OpenVPN y puede ser más difícil para que funcione de forma fiable entre dispositivos detrás de enrutadores NAT

Fuente: Elaboración propia

Del análisis de las ventajas que ofrece el protocolo de OpenVPN sobre otros protocolos de seguridad, se concluye que es la mejor opción de encriptación para implementarlo en la presente propuesta tecnológica.

1.5. Raspberry pi

Raspberry pi es una nano computadora del tamaño de una tarjeta de crédito que se puede conectar a un monitor y usar como una computadora estándar. Su pequeño tamaño y su bajo precio hacen de Raspberry pi un producto ideal para implementar diferentes proyectos y también montar servidores en base a Raspbian que es su sistema operativo basado en Linux.

En la figura 12 se puede apreciar los diferentes elementos electrónicos que posee la placa madre del Raspberry Pi 4.

Figura 12*. Raspberry Pi*

Fuente: Tomado de (Raspberry, 2022)

Raspberry pi es una de las tendencias tecnológicas más usadas en el presente. Su tamaño, facilidad de manejo y mantenimiento, precio económico y bajo consumo energético manteniendo muy buen rendimiento general lo hace uno de los dispositivos más eficientes del mercado. Además, lo hace tan intuitivo que requiere que la utilidad construya poco en su computadora, agregando gradualmente el hardware apropiado para que funcione (Raspberry, 2022).

1.5.1. Características del Raspberry pi 4

Estas son las novedades y características del Raspberry pi 4 Modelo B, el cual se implementó en la propuesta tecnológica realizada:

Memoria RAM

El Raspberry Pi 4 Modelo B es una computadora con pantalla dual 4k completamente actualizada y rediseñada que tiene 2 GB, 4 GB u 8 GB de RAM.

Procesador

Cuenta con un procesador actualizado de cuatro núcleos de 64 bits que funciona a 1,4 GHz.

Puertos

El Pi 4 B cuenta con 2 puertos micro HDMI para admitir pantallas duales 4K. Es más eficiente energéticamente y usa menos energía que otros modelos. Se incluyen dos puertos USB 3 para transferir datos 10 veces más rápido que USB 2.

El Pi 4 B viene con Ethernet Gigabit de 300 mbps, red inalámbrica integrada de doble banda 2.4 y 5 GHz y Bluetooth. La capacidad PoE está disponible a través de un PoE HAT separado. La entrada de alimentación es USB-C con una clasificación de PSU mínima recomendada de 3A. El puerto también está habilitado para OTG.

Dimensión del hardware

La forma y el tamaño básico siguen siendo los mismos, por lo que se puede colocar en proyectos existentes como una actualización. El Raspbrerry Pi 4 B es compatible con versiones anteriores de software como otros modelos de pi (Raspberry, 2022).

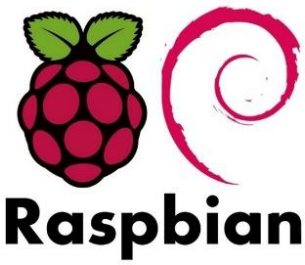
1.5.2. Sistema operativo Raspbian

Raspbian es un sistema operativo gratuito basado en Debian optimizado para el hardware Raspberry pi. Un sistema operativo es el conjunto de programas y utilidades básicos que hacen que el Raspberry pi funcione. Sin embargo, Raspbian proporciona más que un sistema operativo puro, éste viene con más de 35 mil

paquetes, software pre compilado incluido en un formato agradable para una fácil instalación en el Raspberry Pi. (Harrington, 2015)

En la figura 13 se puede observar cómo es el logo del sistema operativo creado para Raspberry Pi el cual se asemeja a una fruta.

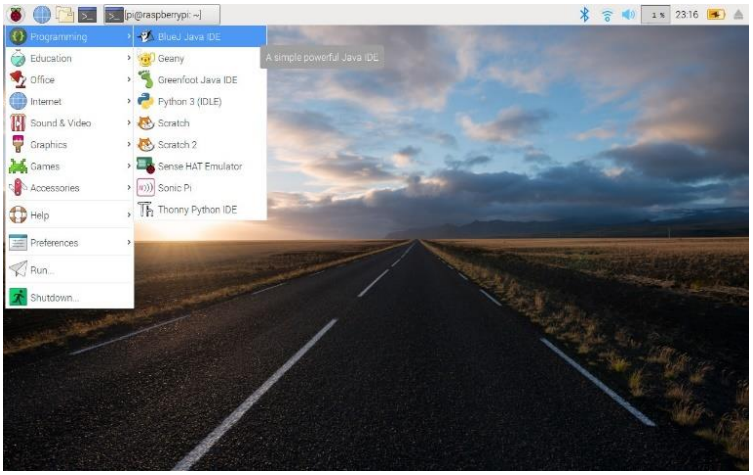
Figura 13. Raspbian



Fuente: Tomado de (Raspberry, 2022)

La compilación inicial de más de 35 mil paquetes de Raspbian, optimizados para obtener el mejor rendimiento en Raspberry pi, se completó en junio de 2012. Sin embargo, Raspbian aún está en desarrollo activo con énfasis en mejorar la estabilidad y el rendimiento de tantos paquetes de Debian como sea posible. Vale señalar que Raspbian no está afiliado a la Fundación Raspberry Pi. Raspbian fue creado por un pequeño y dedicado equipo de desarrolladores del hardware Raspberry pi. (Harrington, 2015)

Figura 14*. Escritorio de Raspbian*



Fuente: Elaboración propia

1.6. Servidor VPN en Linux

Una VPN instalado en un servidor basado en Linux ofrece varias ventajas como:

- Seguridad: una VPN brinda un seguro mejor y más sólido ya que toda la información está codificada. Esto brinda seguridad adicional, en contraste con los firewalls. En un nivel más significativo, una VPN hace que los intercambios de información sean seguros a través del cifrado.
- Acceso remoto: para garantizar una alta seguridad, numerosas asociaciones, gobiernos y lugares de trabajo de protección permiten el acceso remoto solo a través de la VPN.
- Cambio de IP: la configuración de una VPN permite a los clientes cambiar de forma segura sus IP y leer detenidamente. Esto, en casos específicos, se utiliza en áreas que tienen limitaciones basadas en el área.
- Regulación de banda ancha: Ciertos ISP obstruyen la capacidad de transferencia de datos del cliente en vista del contenido.

1.7. Windows server 2019

Windows Server es un sistema operativo desarrollado por Microsoft Corporation que admite la administración de nivel de almacenamiento de datos, aplicaciones y comunicaciones empresariales. Puede actuar como un servidor o centro de datos que desempeña un papel en la gestión de la red de servidores (Microsoft, 2022)

Según Dauti (2022) la tecnología de la información está creciendo más rápido. La tecnología de la información a veces se aplica ampliamente en muchos campos, como la salud, la educación, la industria, los negocios, entre otros. Un producto en este desarrollo es Windows Server.

La construcción de una infraestructura de la Tecnología de la Información (en lo adelante TI) o el desarrollo de un sistema de TI requiere que Windows Server actúe como servidor o centro de datos para proporcionar servicios en una red informática,

como almacenamiento, virtualización de servidores, redes, protección de acceso e información, etc. (Dauti, 2022).

1.7.1. Características de Windows Server 2019

Estas son algunas de las características clave de Windows Server:

- La mayoría de los procesos de servicio del servidor se pueden operar con comandos del sistema operativo basados en la arquitectura del servidor.
- Otorga a los usuarios permiso para acceder y administrar el servidor a través de una interfaz gráfica de usuario (GUI) o una interfaz de línea de comandos (CLI).
- La configuración avanzada del servidor ayuda de dos maneras: configurar hardware, software o servicios de red.
- Las computadoras de administración y monitoreo están conectadas a los sistemas de red del cliente y los sistemas operativos para ejecutar los sistemas de red.
- Proporciona una centralización de interfaz (interfaz) que ayuda a los usuarios (implementadores o administradores de seguridad) a ejecutar varios procesos que son procesos administrativos.

1.7.2. File server

Un servidor de archivos es una característica de servidor central ubicada en una red de computadoras que permite a los clientes conectados acceder a la capacidad de almacenamiento del servidor (IBM, 2021). Cuando se les otorgan los permisos de acceso apropiados, los usuarios pueden acceder a los archivos y la capacidad de almacenamiento del servidor. Los usuarios pueden abrir, leer, cambiar, eliminar una carpeta e incluso cargar sus archivos en el servidor.

1.7.3. Directorio activo

Active Directory (AD) es uno servicio de directorio del sistema operativo Windows que facilita el trabajo unificado con recursos de red interconectados (Dominguez, 2020).

Proporciona una interfaz común para organizar y mantener la información relacionada con los recursos conectados a varios directorios de red. Los directorios pueden ser del sistema (como el sistema operativo Windows), aplicaciones o recursos de red como impresoras. Active Directory sirve como un depósito de datos único para un acceso rápido a los datos para todos los usuarios y controla el acceso de los usuarios según la política de seguridad del directorio. (Dominguez, 2020)

Active Directory proporciona los siguientes servicios de red:

- Protocolo ligero de acceso a directorios (LDAP): un estándar abierto utilizado para acceder a otros servicios de directorio
- Servicio de seguridad que utiliza principios de capa de sockets seguros (SSL) y autenticación basada en Kerberos
- Almacenamiento jerárquico e interno de datos organizacionales en una ubicación central para un acceso más rápido y una mejor administración de la red
- Disponibilidad de datos en múltiples servidores con actualizaciones simultáneas para una mejor escalabilidad

También tiene una estructura interna con una estructura jerárquica. Cada nodo en la estructura de árbol se denomina objeto y está asociado con un recurso de red, como un usuario o servicio. (Castillo, 2018)

Al igual que el concepto de un esquema de tema de base de datos, un esquema de Active Directory se usa para especificar un atributo y tipo para un objeto de Active Directory en particular, lo que facilita la búsqueda de recursos de red conectados en función de los atributos asignados (Microsoft, 2022). Es decir, si el usuario necesita utilizar una impresora capaz de imprimir a color, el atributo del objeto se puede configurar con una palabra clave adecuada para facilitar la búsqueda en toda la red y ubicar el objeto en función de esa palabra clave.

1.7.4. DNS server

El DNS (sistema de nombres de dominio) es un sistema que convierte los nombres de dominio legibles en direcciones IP legibles por máquina. Sin embargo, en DNS, como en toda la web moderna, hay muchos matices. La razón de esto es el número multiplicado de dispositivos que pueden acceder a internet, el esquema mucho más complicado de conectividad de red y las propias tecnologías de internet, que se han desarrollado lejos de la trayectoria establecida por sus desarrolladores (Bravo, 2022).

METODOLOGÍA DEL PROCESO DE LA PROPUESTA TECNOLÓGICA

CAPÍTULO 2

2. CAPÍTULO 2: METODOLOGÍA DEL PROCESO DE DESARROLLO DE LA PROPUESTA TECNOLÓGICA

El presente trabajo de titulación empleará la metodología descriptiva y enfoque cualitativo ya que se validará la condición existente, definirá las necesidades de la empresa, y planteará la solución más viable a través de la recopilación de información sobre la comunicación encriptada a utilizar.

2.1. Enfoque de la investigación

Según Diaz (2013) la entrevista es una técnica de gran utilidad en la investigación cualitativa para recabar datos; se define como una conversación que se propone un fin determinado distinto al simple hecho de conversar. Es un instrumento técnico que adopta la forma de un diálogo coloquial (Diaz, 2013). Hernández (2018) en su libro la define como "la comunicación interpersonal establecida entre el investigador y el sujeto de estudio, a fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto". (Hernandez, 2018)

Después de haber mencionado esto se puede determinar que el enfoque de esta propuesta tecnológica es de tipo cualitativo ya que se conocerá las necesidades de la empresa a partir del análisis de la entrevista realizada a el presidente de la empresa.

2.2. Tipo de investigación

Según Baena (2014) el objetivo principal de la investigación descriptiva es definir las características de un fenómeno particular sin necesariamente investigar las causas que lo producen. La investigación descriptiva es un tipo de análisis que describe las características de la población o los temas en estudio. El investigador no puede influir en las variables en este diseño de investigación, solo puede informar los hechos precisamente como ocurrieron o están ocurriendo. (Baena, 2014)

Los principales métodos utilizados en la investigación descriptiva incluyen observaciones, entrevistas y estudios de casos. (Hernandez, 2018)

La entrevista es muy ventajosa principalmente en los estudios descriptivos y en las fases de exploración, así como para diseñar instrumentos de recolección de datos. (Baena, 2014)

Las entrevistas semiestructuradas son una combinación de las entrevistas estructuradas y no estructuradas. Si bien el entrevistador tiene un plan general de lo que quiere preguntar, las preguntas no tienen que seguir una redacción u orden en particular, estas suelen ser abiertas, lo que permite flexibilidad, pero siguen un marco temático predeterminado, lo que da una sensación de orden. Por esta razón, a menudo se les considera el mejor tipo de entrevista a utilizar. (Baena, 2014)

Después de haber aclarado los diferentes términos se puede determinar que el presente trabajo de titulación empleará el tipo de investigación descriptivo a partir de la realización de una entrevista semiestructurada ya que se validará la condición existente, definirá las necesidades de la empresa, y planteará la solución más viable a través de la recopilación de información sobre la comunicación encriptada a utilizar.

2.3. Periodo y lugar donde se desarrolla la propuesta tecnológica

La presente propuesta tecnológica se desarrolló durante los meses de agosto y septiembre del año 2022, en la oficina de BUILDERECUADOR CIA.LTDA. ubicada en la ciudad de Guayaquil. Durante este periodo se llevó a cabo la revisión tecnológica y bibliográfica para la elaboración de la propuesta.

Se seleccionó a BUILDERECUADOR CIA.LTDA. por ser una empresa en crecimiento, cuya meta establecida es el reconocimiento de su marca en el mercado de la construcción y que apuesta por soluciones tecnológicas innovadoras. Estas características lo convierten en un lugar óptimo para la realización de la presente propuesta tecnológica.

2.4. Métodos empleados

Los métodos utilizados son empíricos ya que pueden recuperar y procesar los datos. El método de recolección de datos de verificación en esta propuesta técnica es una entrevista realizada al presidente de la empresa constructora.

2.5. Proceso de selección de la tecnología usada

Para la selección de la tecnología que se implementará en esta propuesta se determinó que se deben de saber estos puntos clave para el cumplimiento de los objetivos: necesidad de la empresa, alcance, escalabilidad de hardware, presupuesto y la selección de la tecnología.

Necesidad de la empresa

Las oficinas de Guayaquil y Loja requieren de una comunicación diaria para llevar a cabo los diferentes proyectos que realiza la empresa.

Es por ello que es necesario mejorar la seguridad del tráfico y almacenamiento de la información de la empresa BUILDERECUADOR CIA.LTDA. ya que con su correcto manejo y funcionamiento se mejorará la comunicación de la matriz hacia los diferentes puntos donde se encuentre su equipo de trabajo.

Esta propuesta tratará sobre el análisis e implementación de OpenVPN en una Raspberry Pi; además de la implementación de un file server configurado en Windows Server 2019. Conforme al requerimiento de la empresa el file server servirá para el almacenamiento de archivos como planos, bocetos, fotografías, presupuestos entre otros.

Alcance del proyecto

El alcance de esta propuesta tecnológica es proponer a la empresa constructora BUILDERECUADOR CIA.LTDA un diseño e implementación de Red Privada Remota para la gestión segura de sus recursos informáticos, es por esta razón que se sugiere utilizar la tecnología de Raspberry Pi para el alojamiento de un servidor VPN basado en el protocolo OpenVpn, y además implementar de un file server y

directorio activo para la gestión segura de los archivos. Así mismo, la empresa solicitó que la propuesta sea económica la cual no supere los 400 dólares y a la vez cumpla con todas sus necesidades.

Escalabilidad de hardware

Al analizar la proyección de la empresa se determinó que cuentan con un espacio físico suficiente para crecer y contar con más socios, esto significaría el incremento de equipos e información que se almacenará en el servidor. Dicho esto se debe de contar con suficiente memoria de disco duro en el servidor y también tener un switch administrable con varios puertos para cubrir los requerimientos de la red LAN.

Selección de la tecnología en base a las necesidades de la empresa

El equipo Raspberry Pi cumplirá la función de servidor en la cual se alojara los servicios de OpenVPN para que la comunicación entre las dos oficinas sea posible, también se requiere un switch administrable donde se configurara las VLAN de la red LAN y WAN de la red, al igual que una CPU la cual ya contaba la empresa donde se instalara Windows Server 2019, el modem del proveedor al no contar con suficientes puertos se tuvo que adquirir un switch de acceso para la conexión del switch administrable y el router de la empresa. Finalmente se debe de adquirir un UPS para que proteja los equipos ante un posible fallo eléctrico.

A continuación se detalla los modelos del hardware que se utilizará en la propuesta y también el software.

Componentes de hardware

Los componentes de hardware que hará posible la implementación de esta propuesta tecnológico son los siguientes:

- Raspberry Pi 4 Modelo B de 8gb Ram + kit completo
- Switch Administrable L2 8 Pu Gigabit 2 Sfp Tl-sg3210
- Servidor DELL core i3/ 8gb ram / 320gb disco duro+120 disco duro solido
- Switch Desktop TP LINK no administrable

- UPS APC 800VA

Componentes de software

Los componentes de software para la propuesta tecnológica son los siguientes:

- Sistema operativo Linux Raspbian
- Windows server 2019

Presupuesto de la propuesta tecnológica

En la tabla 5 se puede apreciar el presupuesto que se necesitará para adquirir los equipos de hardware, la cual hará posible la implementación de esta propuesta tecnológica.

Tabla 5. Presupuesto de los equipos de hardware

Hardware	Precio (USD.)
Raspberry Pi 4 Modelo B de 8gb Ram + kit completo	**$250,00**
Switch Administrable L2 8 Pu Gigabit 2 Sfp Tl-sg3210	**$50,00**
Switch Desktop TP LINK (acceso)	**$30,00**
UPS APC 800VA	**$40,00**
Precio total de equipos de hardware	**$370,00**

Fuente: Elaboración propia

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

CAPITULO 3

3. CAPÍTULO 3: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

En el presente capítulo de esta propuesta tecnológica se analizará e interpretará las respuestas de la entrevista realizada al presidente de la empresa, con el objetivo de establecer las necesidades de la empresa BUILDERECUADOR CIA. LTDA. y la proyección de la empresa en un futuro.

3.1. Análisis de las respuestas de la entrevista hecha al presidente de la empresa BUILDERECUADOR CIA. LTDA.

3.1.1. Respuestas de la entrevista

Al inicio de la entrevista se preguntó sobre la definición de la empresa BUILDERECUADOR CIA. LTDA. para saber acerca de sus inicios. Se allí se conoció que es una empresa dedicada al diseño y construcción, cuya constitución fue en el año 2021.

En la pregunta número 2 “¿Qué servicios brinda la empresa?” se indicó que la empresa se dedica al desarrollo de proyectos inmobiliarios, así como a la construcción y remodelación de obras civiles de carácter residencial y comercial. También ofrecen servicios de acuerdo a las necesidades del cliente, en donde lo asesoran y buscan que el producto final sea a su satisfacción. Su trabajo implica la subcontratación de proveedores para realizar la ejecución de las obras.

En la pregunta número 3 “¿Cómo está constituida la empresa y dónde se encuentra ubicada?” se señaló que la empresa cuenta con un equipo de trabajo dedicado a las tareas de: diseño y construcción de proyectos, presupuesto y cronogramas de trabajos, equipo de modelamiento 3D, equipo legal e inmobiliario. Así mismo se indicó que cuentan con oficinas en Loja y Guayaquil y que próximamente ubicar

La pregunta número 3 “¿Cómo se realiza la transferencia / almacenamiento de datos dentro de la empresa?” se la formuló con el fin de detectar posibles falencias en la seguridad informática y así poder dar una solución en la propuesta tecnológica. El entrevistado señaló que se utilizan correos electrónicos corporativos para el envío y recepción de información de los proyectos; y en caso de que sea muy pesada la

información, se utiliza dispositivos externos como discos duros, memorias externas o por medio de aplicaciones basadas en la nube como WeTransfer. En el caso del almacenamiento de datos se realiza dentro de las computadoras sean de escritorio o computadora portátil. También crean carpetas en Google Drive para compartir información de interés para el equipo de trabajo.

En las preguntas números 4 “¿Cómo mantiene protegido los sistemas informáticos de su empresa?” y 5 “¿Cuáles son los dispositivos que forman la red de su empresa?”, se indicó que cada una de las computadoras tiene antivirus que lo renuevan anualmente, además del firewall que incluyen en las computadoras. Agregó que las oficinas cuentan con una red WiFi inalámbrica emitida por el modem del ISP y que cuentan con un servicio de internet hogar de la compañía de TV Cable.

La pregunta número 7 “¿Cree usted que la empresa necesita implementar mejoras en su manejo de transferencia y almacenamiento de datos?” se la formuló para conocer su punto de vista de usuario de la red de la empresa e indicó que el tiempo juega un rol esencial en su empresa y su optimización depende de lo ágil y cómodo sea en la realización del fujo de trabajo. Y señaló que la empresa necesita un sistema de transferencia y almacenamiento de información compartido entre las dos oficinas de Guayaquil y Loja como un medio de recopilación documental de cada proyecto que lleva a cabo la empresa.

También agregó que la empresa maneja información gráfica, como archivos de formato dwg, IFC, rtv, tif, skp, psp, entre otros, los cuales ocupan gran capacidad de memoria y se complica un envió a través de plataformas de correo.

Además, indicó que los equipos de Guayaquil y Loja trabajan en proyectos en común y necesitan una carpeta compartida donde se vaya ubicando y guardando los archivos generados, con el fin de tener un mejor control documental por cada obra realizada, y así obtener un expediente digital organizado.

Por último, la pregunta número 6 “¿Cuál es su visión de la empresa en un futuro?”, el entrevistado contestó que su empresa espera llegar a obtener un reconocimiento en el mercado de la construcción, además que tienen proyectos programados a

ejecutar por lo que la empresa necesitará contratar más personal de apoyo para su ejecución y contar con un mejor flujo de trabajo y comunicación.

3.1.2. La empresa y sus necesidades

Tras un análisis de la entrevista se pudo determinar que las oficinas de Guayaquil y Loja requieren de una comunicación diaria para llevar a cabo los diferentes proyectos que realiza la empresa.

Es por ello que es necesario mejorar el tráfico y almacenamiento de la información de la empresa BUILDERECUADOR CIA.LTDA. ya que con su correcto manejo y funcionamiento se mejorará la comunicación de la matriz hacia los diferentes puntos donde se encuentre su equipo de trabajo.

Esta propuesta tratará sobre el análisis e implementación de OpenVPN en una Raspberry Pi; además de la implementación de un file server configurado en Windows Server 2019. Conforme al requerimiento de la empresa el file server servirá para el almacenamiento de archivos como planos, bocetos, fotografías, presupuestos entre otros.

3.3. Evaluación de cambios tecnológicos y realización de propuesta tecnológica en base a la entrevista realizada

3.3.1. Cambios tecnológicos necesarios

Al analizar las respuestas de la entrevista, se sugirió a la empresa el cambio de plan de internet residencial a empresarial debido a que la implementación de una VPN requiere una IP pública.

Tras una consulta con el ISP que tiene contratado la empresa, se conoció las ventajas de tener un plan empresarial, como son:

- Velocidades de carga y descarga más estables
- Conexión dedicada con compartición 2 a 1
- Dirección IP fija
- Servicio al cliente especializado con atención de 24 horas

- Rendimiento optimizado
- Proveen licencias de antivirus empresarial

3.3.2. Propuesta tecnológica

Tras analizar las necesidades de la empresa con relación a la entrevista se determinó que la propuesta tecnológica se conformará en tres partes:

- Primera parte: Comunicación para la gestión segura de los recursos informáticos
- Segunda parte: Almacenamiento de información
- Tercera parte: Administración

En donde se detalla lo siguiente:

En la tabla 5 se puede observar cómo estaría dividida las diferentes partes de la implementación de la propuesta tecnológica.

Tabla 6. Partes de la propuesta tecnológica

	Función	**Propuesta**	**Propósito**
Primera parte	Comunicación	Servidor VPN utilizando el protocolo OpenVPN	Transmisión de información encriptada
Segunda parte	Almacenamiento de información	Configuración de file server en Windows server 2019	Mejorar la eficiencia en el manejo y almacenamiento de la información confidencial
Tercera parte	Administración	Configuración de directorio activo en Windows server 2019	Mejorar la administración de equipos y usuarios

Fuente: Elaboración propia

3.4. Pruebas realizadas a Raspberry Pi

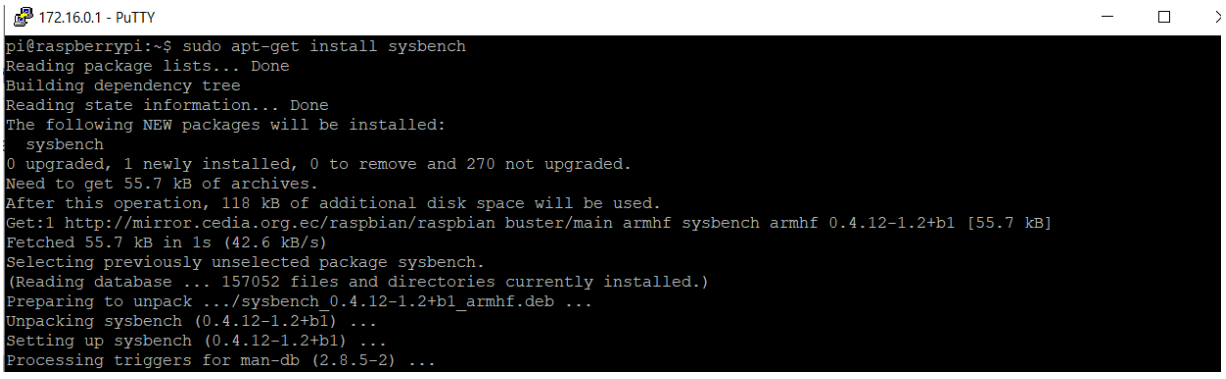
Pruebas de hardware

Las pruebas que se realizaron al hardware se las hizo a través de Benchmark el cual es un procedimiento documentado que medirá el tiempo que necesita un sistema informático para ejecutar una tarea informática bien definida. Este tiempo está relacionado con el rendimiento del sistema informático y que de alguna manera se puede aplicar el mismo procedimiento a otros sistemas, de modo que se puedan realizar comparaciones entre diferentes configuraciones de hardware/software. (Intel, 2014)

Para realizar las pruebas a los componentes de Raspberry se debe de instalar el repositorio de Sysbench, para ello se utilizará el siguiente comando

En la figura 15 se puede visualizar la ejecución del comando sudo apt-get install sysbench

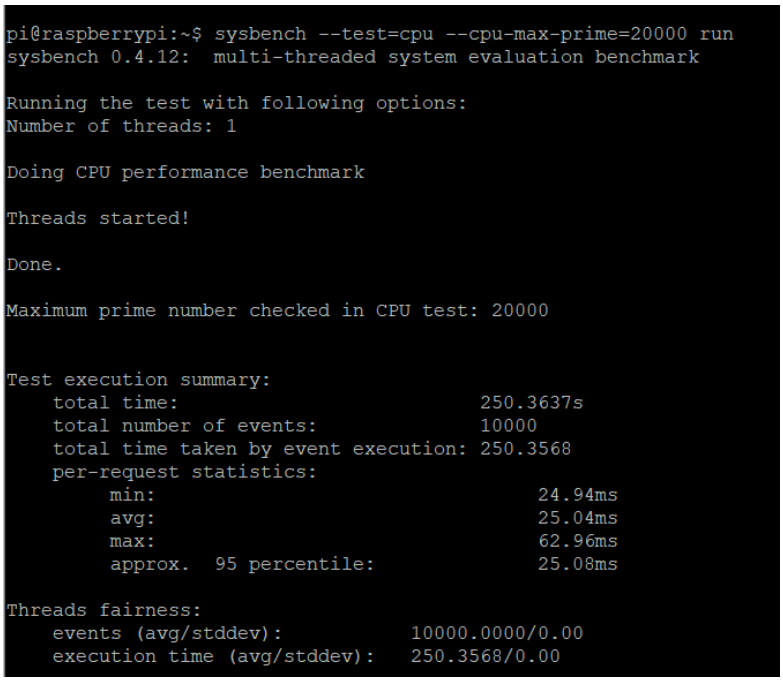
Figura 15. Instalación Sysbench



Fuente: Elaboración propia

Al terminar la instalacion se puede medir el rendimiento de la CPU para determinar si el dispositivo se encuentra en estado optimo para la instalacion de los servicios

Figura 16. Prueba de rendimiento de CPU

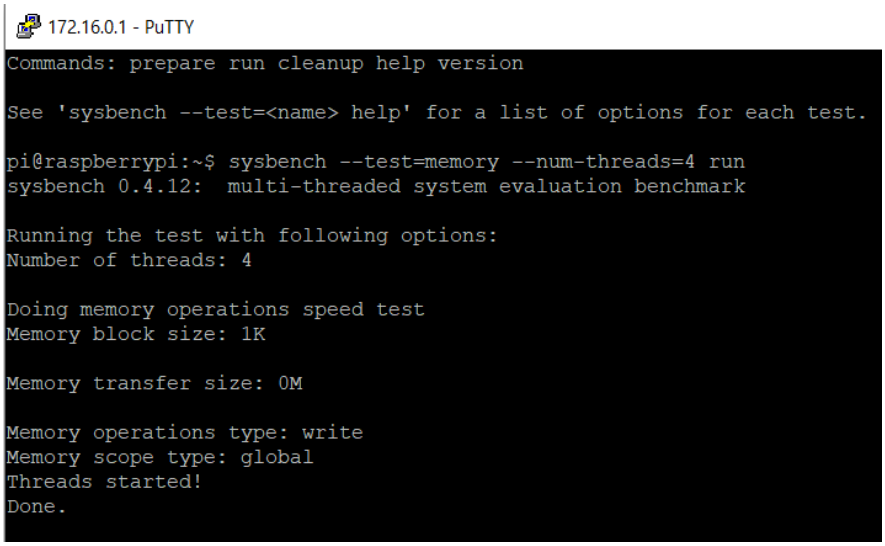


Fuente: Elaboración propia

Cuando se ejecuta con la carga de trabajo de la CPU, sysbench verificará los números primos mediante la división estándar del número entre todos los números entre 2 y la raíz cuadrada del número. Si cualquier número da un resto de 0, se calcula el siguiente número. Esto pondrá algo de estrés en la CPU, pero solo en un conjunto muy limitado de características de la CPU (Intel, 2014).

Al igual que la CPU, tambien se puede realizar pruebas al estado de la memoria en el cual estará alojado el sistema operativo Raspbian.

Figura 17. Prueba de rendimiento de memoria



Fuente: Elaboración propia

Al ejecutar el siguiente script ejecutará 7 test de benchmark al hardware del Raspberry Pi:

curl -L https://raw.githubusercontent.com/aikoncwd/rpi-benchmark/master/rpi-benchmark.sh | sudo bash

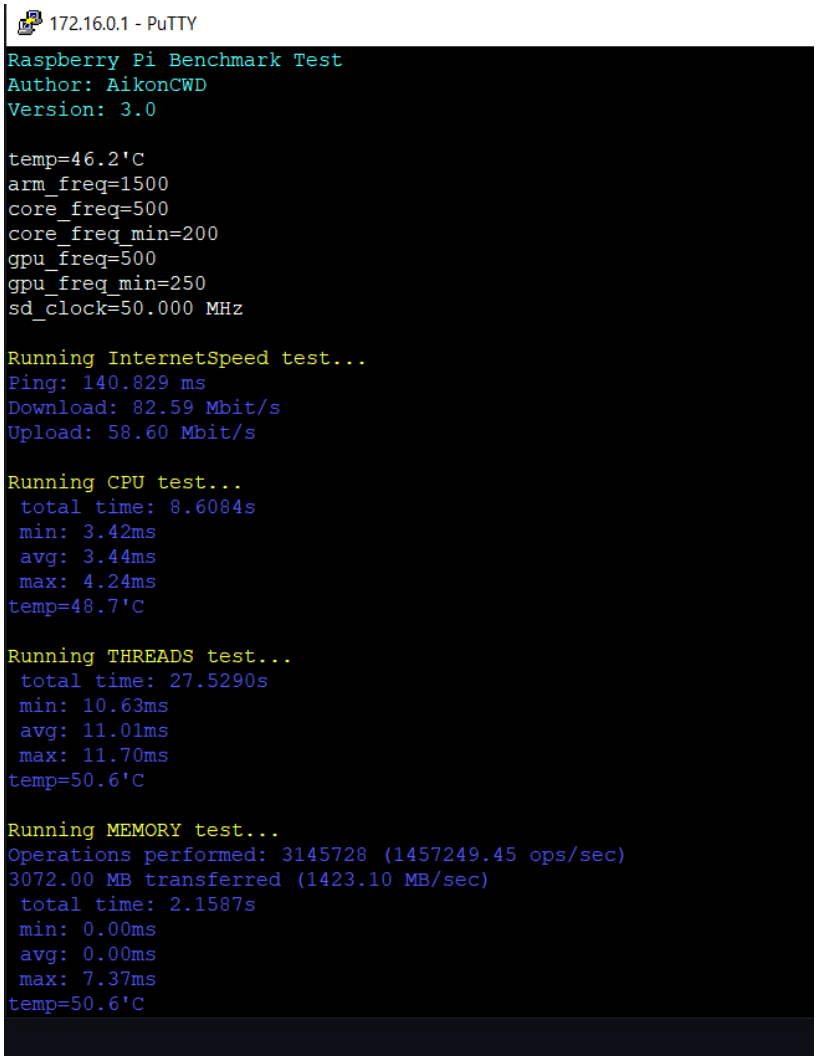
En la figura 18 se aprecia que aparecerá la siguiente información

- Speedtest-cli test: Calcula el ping, velocidad de carga y descarga en Internet
- CPU sysbench test: Calcula 5000 números primos
- CPU sysbench test: Multihilo 4000 rendimientos and 5 bloqueos
- MEMORY RAM test: Acceso sequencial a 3Gb de memoria RAM
- microSD HDParm test: Calcula la velocidad máxima de lectura de la microSD
- microSD DD write test: Calcula la velocidad máxima de escritura con 512Mb de datos

- microSD DD read test: Calcula la velocidad máxima de lectura con 512Mb de datos

Después de cada test, aparecerá la temperatura en ºC de la CPU (Github, 2016)

Figura 18. Script de benchmark

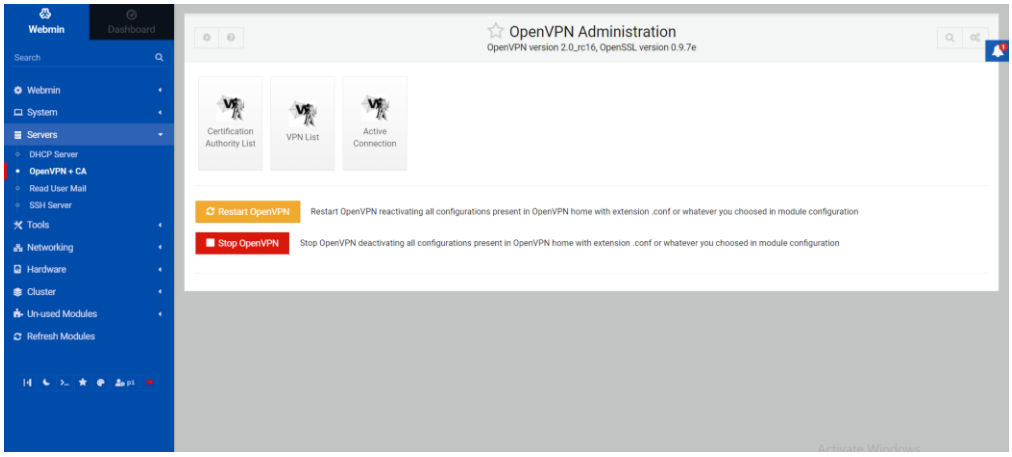


Fuente: Elaboración propia

Pruebas de software

En las siguientes capturas de pantallas se mostrara las pruebas de funcionalidad que se realizó al servidor VPN ya configurado en la Raspberry Pi.

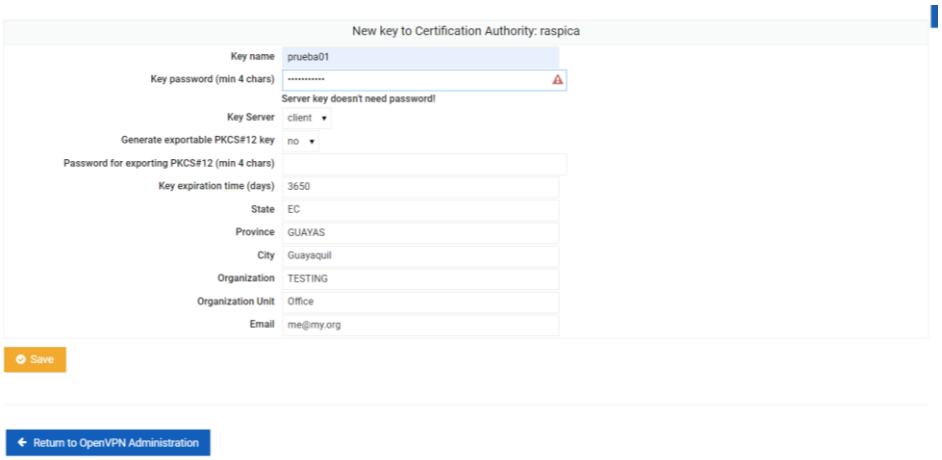
Figura 19. Pantalla de administrador OpenVPN



Fuente: Elaboración propia

Se creo un usuario con el nombre de prueba01 y una clave generica que luego será cambiada por motivos de seguridad.

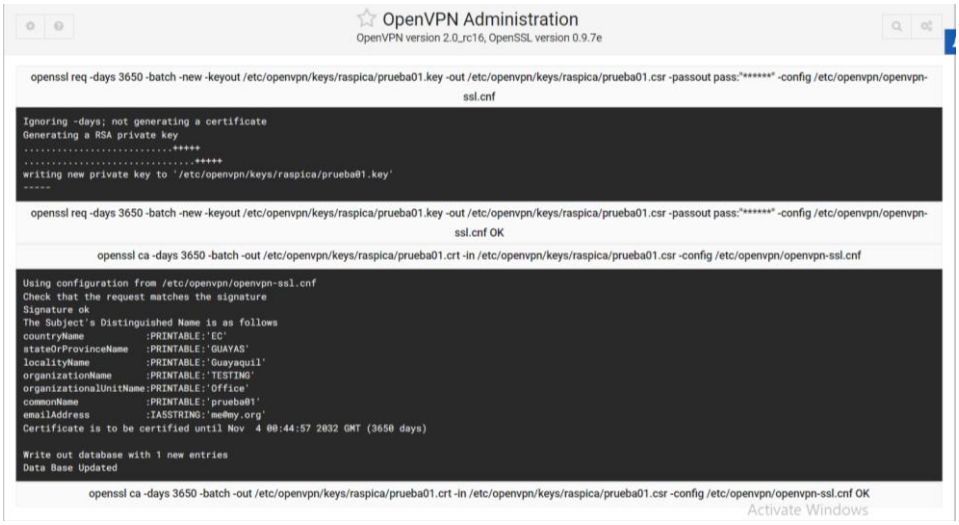
Figura 20. Generación de certificado



Fuente: Elaboración propia

Se puede observar que el certificado se ha creado exitosamente y se verá reflejado en la lista de los clientes.

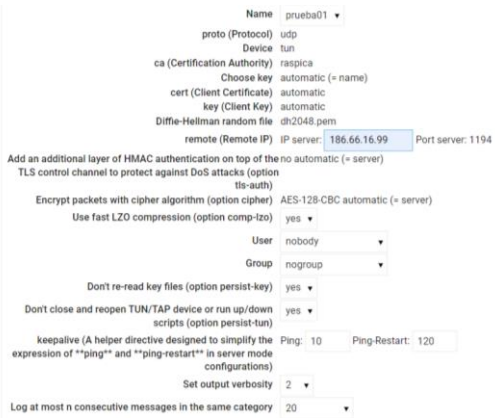
Figura 21. Mensaje de generación exitosa del certificado



Fuente: Elaboración propia

Se selecciona el usuario y se le coloca la ip publica que fue otorgada por el ISP para el funcionamiento de la VPN.

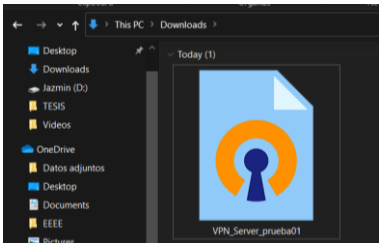
Figura 22. Asignación ip pública al certificado



Fuente: Elaboración propia

Al finalizar se exporta el archivo ovpn el cual permitirá al cliente al acceso a de la red.

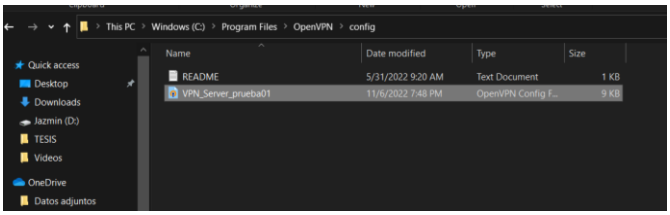
Figura 23. Visualización archivo ovpn



Fuente: Elaboración propia

Se coloca en el archivo destino del software para que reconozca la cliente

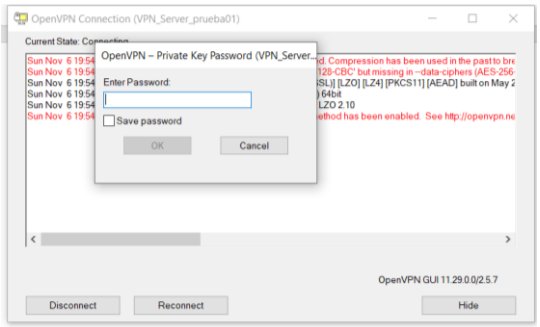
Figura 24. Colocación de archivo ovpn en archivo raíz



Fuente: Elaboración propia

Para poder establecer la conexión se debe de colocar la contraseña que se le asignó anteriormente

Figura 25. Ingreso de contraseña



Fuente: Elaboración propia

Finalmente se logra tener acceso a la red y se determina que se han realizado todas las configuraciones de una manera correcta.

Figura 26. Acceso exitoso a la red

Fuente: Elaboración propia

IMPLEMENTACIÓN DE LA SOLUCIÓN TECNOLÓGICA

CAPITULO 4

4. CAPÍTULO 4: IMPLEMENTACIÓN DE LA SOLUCIÓN TECNOLÓGICA

Este capítulo comprende las diferentes partes para la realización de la propuesta tecnológico como se mencionó en el capítulo 3 de la presente propuesta tecnológica.

4.1. Arquitectura necesaria para la implementación de la solución tecnológica

Tras una inspección de las instalaciones de la empresa BUILDERECUADOR CIA.LTDA, se identificó la falta de algunos componentes de hardware, las cuales eran necesarias para el funcionamiento de la propuesta tecnológica que se detallan a continuación:

Hardware

- Raspberry Pi 4 Modelo B de 8gb Ram + kit completo
- Switch Administrable L2 8 Pu Gigabit 2 Sfp Tl-sg3210
- Servidor DELL core i3/ 8gb ram / 320gb disco duro+120 disco duro solido
- Switch Desktop TP LINK no administrable
- UPS APC 800VA
- 2 memorias Sd Kingston 64gb

Software

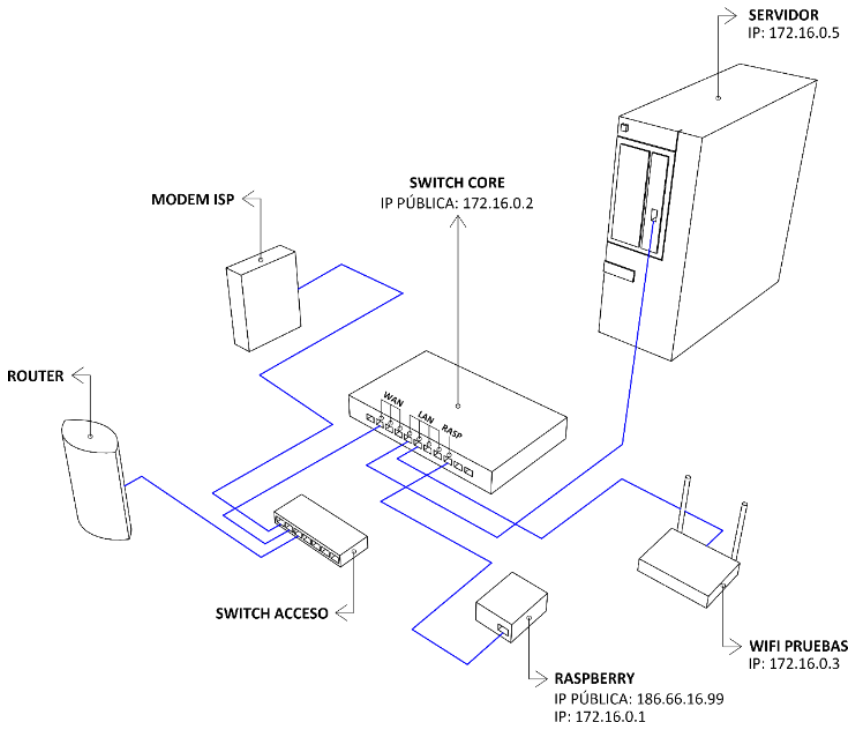
- Sistema operativo Raspbian
- Windows Server 2019

4.2. Diagrama red LAN de implementación en la oficina de la empresa en Guayaquil

A continuación, se muestra una descripción gráfica de cómo se realizó la conexión de los equipos de hardware en la red LAN. Se puede apreciar como los equipos estarían conectados al Switch capa 2 (administrable), en donde encontramos al modem que provee el servicio internet y la ip publica, también el Raspberry pi el cumple la función de servidor en el cual está montado el servicio de OpenVPN, al

igual que el servidor que cumplirá la función de directorio activo y servidor de archivos.

Figura 27. *Red LAN propuesta tecnológica*

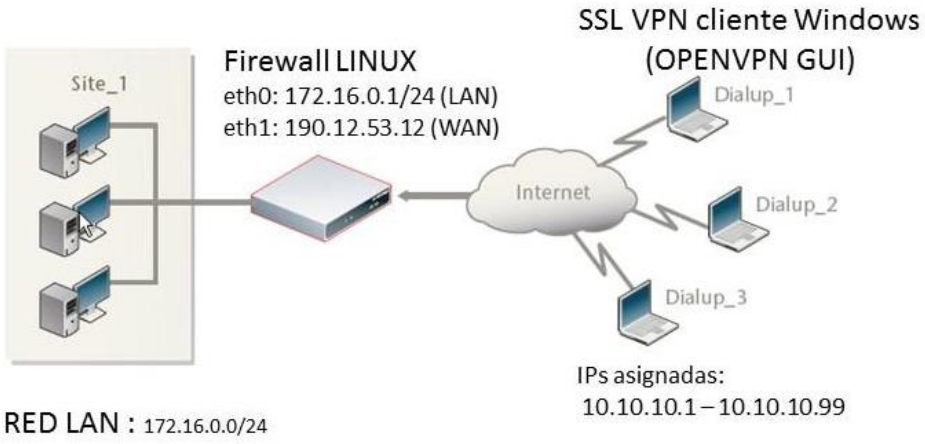


Fuente: Elaboración propia

4.3. Parte 1: Comunicación

Diseño de diagrama de comunicación por VPN entre las dos oficinas

Figura 28. *Diseño de diagrama de comunicación por VPN entre las dos oficinas*



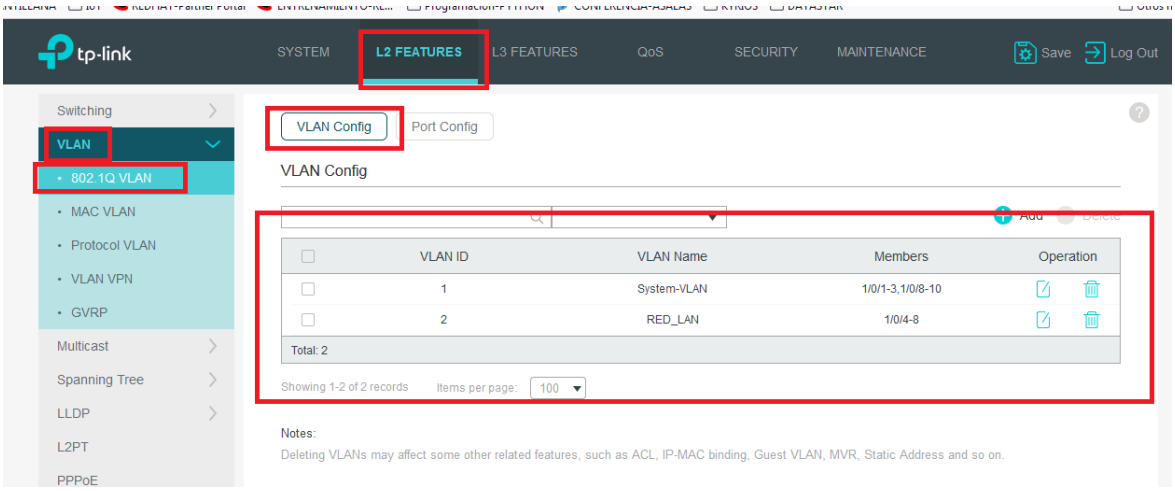
Fuente: Elaboración propia

4.3.1. Configuración switch Tplink:

Para tener acceso al equipo se ingresó por interface WEB a la dirección http://172.16.0.2 y a continuación se configuró las VLAN que dividirá la red LAN y WAN

Configuración CAPA 2 (VLANS):

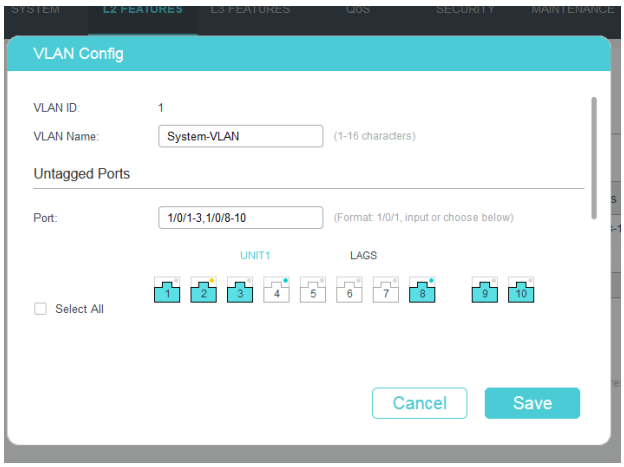
Figura 29. *Configuracion de Switch TpLink capa 2*



Fuente: Elaboración propia

Configuracion VLAN 1

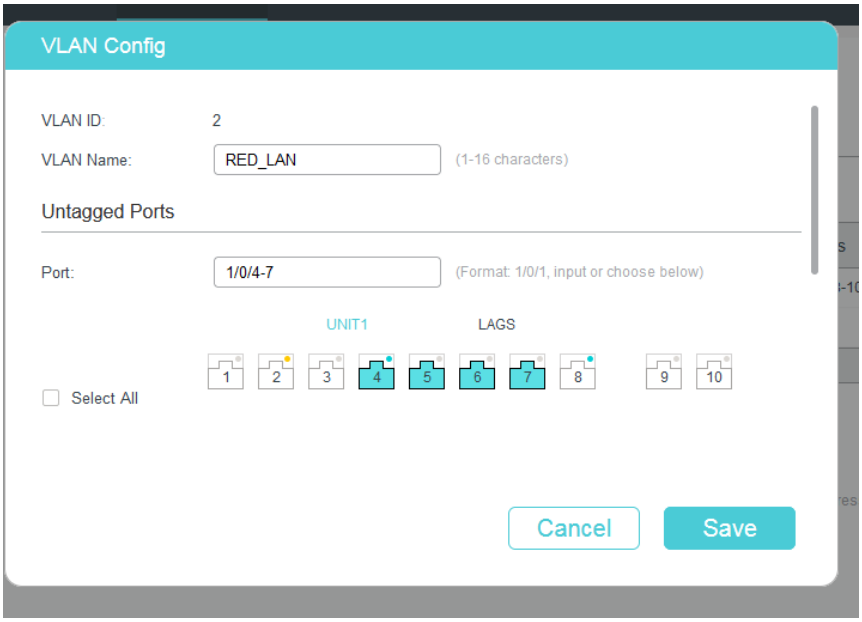
Figura 30. *Configuración de VLAN 1*



Fuente: Elaboración propia

Configuracion VLAN 2

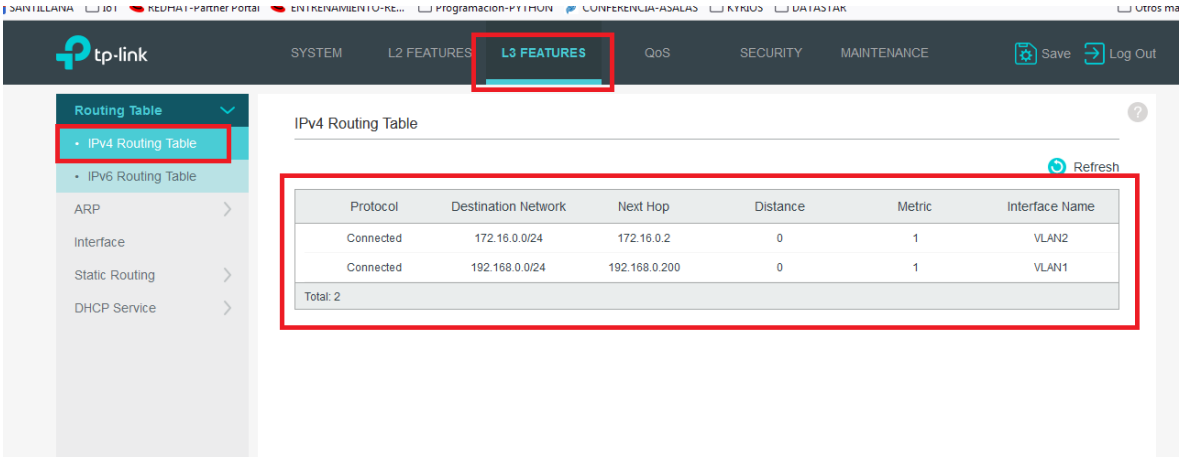
Figura 31. *Configuración VLAN 2*



Fuente: Elaboración propia

Configuración capa 3 (interfaces de red administrativas):

Figura 32. *Configuración capa 2*



Fuente: Elaboración propia

4.3.2. Instalación de Webmin en Raspberry

Como raspbian es una distribucion del sistema operativo GNU/Linux basado en debian, se deben usar los siguientes comandos

Figura 33. *Comandos de instalación librería de Webmin*

```
sudo sh -c 'echo "deb http://ftp.au.debian.org/debian/ buster main non-free" > /etc/apt/sources.list.d/nonfree.list'
sudo apt update
sudo apt install wget
```

Fuente: http://doxfer.webmin.com/Webmin/Installation

Los siguientes comandos agregaron el repositorio de Webmin al sistema e instalaron la última versión de Webmin y todos los paquetes necesarios.

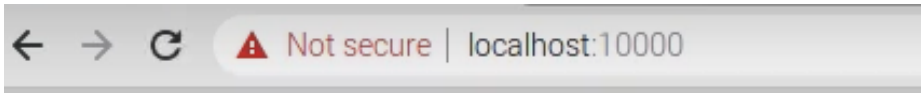
Figura 34. *Comandos de instalación y actualización*

```
wget -qO - http://www.webmin.com/jcameron-key.asc | sudo apt-key add -
sudo sh -c 'echo "deb http://download.webmin.com/download/repository sarge contrib" > /etc/apt/sources.list.d/webmin.list'
sudo apt update
sudo apt install webmin
```

Fuente: http://doxfer.webmin.com/Webmin/Installation

Al terminar la instalación se dirigió al explorador y se colocó localhost: 10000 ya que por defecto el sistema Webmin escucha por el puerto 10000

Figura 35. *Ingreso de URL en la web*



Fuente: Elaboración propia

Para finalizar se colocó las credenciales por defecto que son:

- Usuario: pi
- Clave: raspberry

Figura 36. *Login Webmin*

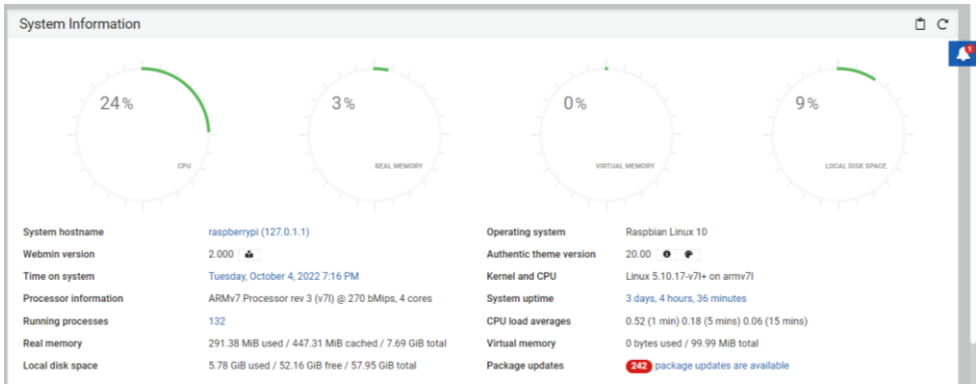
Fuente: Elaboración propia

Esta contraseña predeterminada debió cambiarse inmediatamente por medidas de seguridad.

Una de las ventajas de usar interfaz grafica es que en el dashboard se puede apreciar diferentes estadisticas tales como

- Informacion del estado del servidor tales como CPU, memoria, memoria virtual, espacio en el disco local, etc.

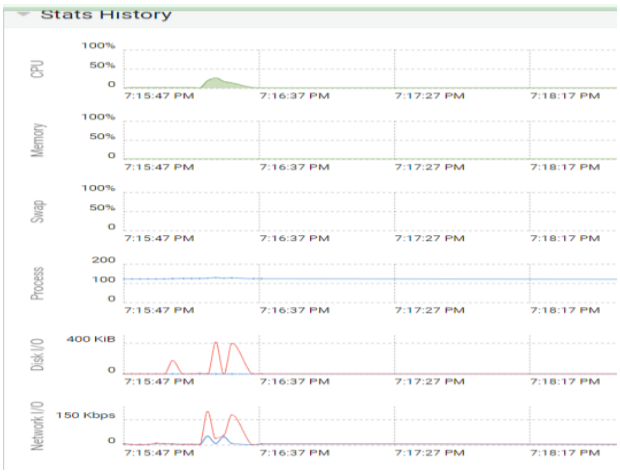
Figura 37. *Graficas de estado del servidor*



Fuente: Elaboración propia

- Historial de estadisticas

Figura 38. *Graficas de estadísticas por fecha*



Fuente: Elaboración propia

4.3.3. Instalación de modulo OpenVpn en webmin

En la línea de comandos del Raspberry pi se colocó lo siguiente:

- **Apt update**
- **Apt install openvpn**

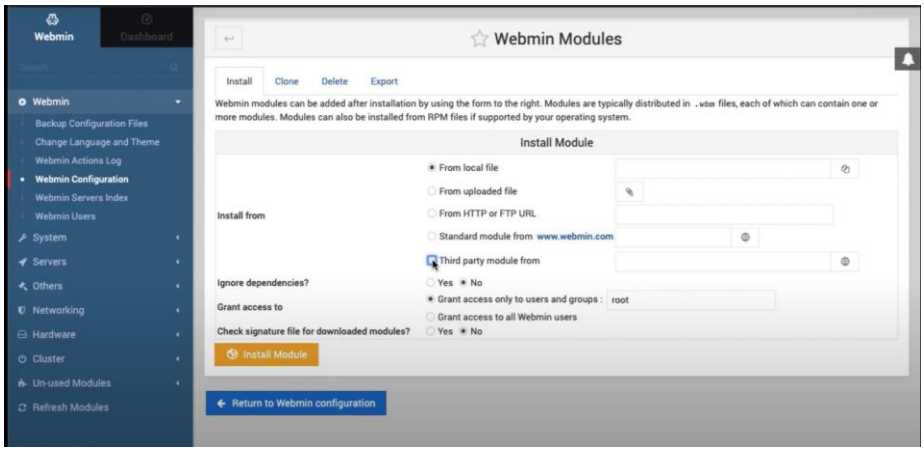
En la configuracion de webmin se dirigió a Webmin configuration – Webmin modules

Figura 39. *Módulos de Webmin*

Fuente: Elaboración propia

En el apartado de la configuracion del Webmin se seleccionó la opción módulo de terceros

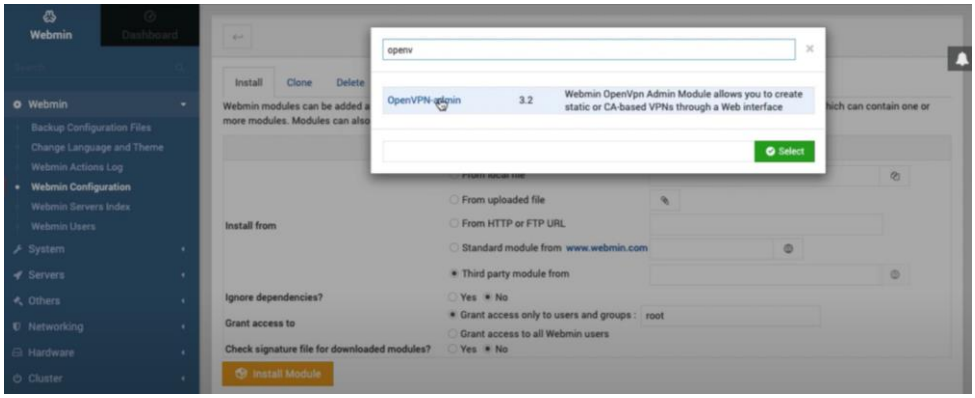
Figura 40. *Selección de módulos de terceros*



Fuente: Elaboración propia

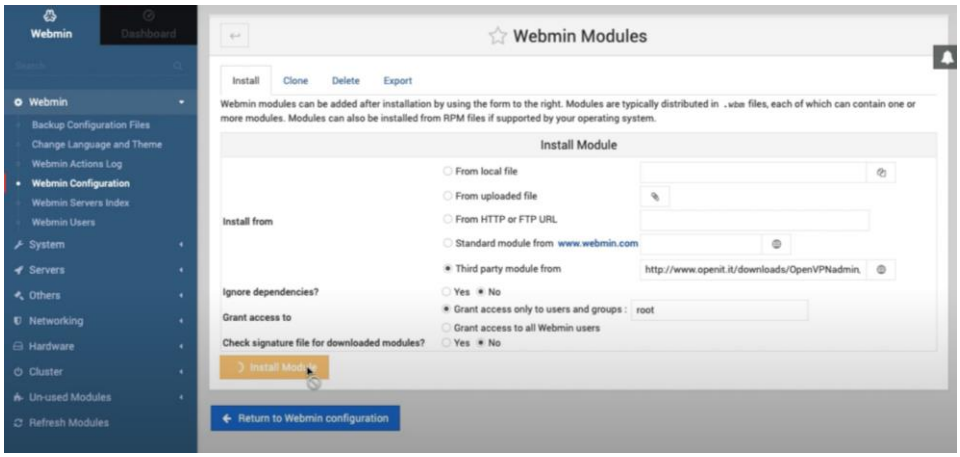
En el buscador se colocó OpenVpn-admin y se lo seleccionó

Figura 41. OpenVpn Admin



Fuente: Elaboración propia

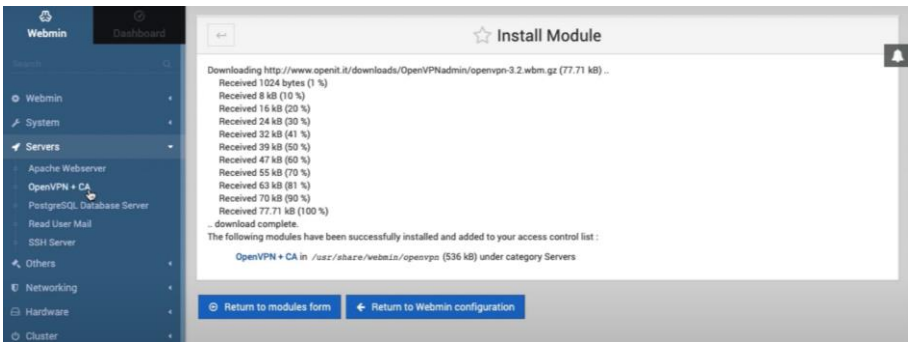
Figura 42. Instalacion de OpenVpn admin



Fuente: Elaboración propia

Una vez instalado se comprobó que se haya añadido en la pestaña de Servers. Debe de salir como OpenVpn+CA

Figura 43. Verificación de instalación del modulo

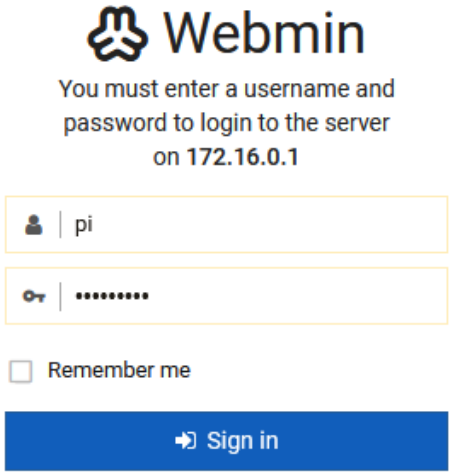


Fuente: Elaboración propia

4.3.4. Acceso al interfaz grafico de Raspberry pi:

Desde la red LAN se abrió el navegador hacia la dirección que se ha asignado al Raspberry Pi que sería la: https://172.16.0.1:10000

Figura 44. Login Webmin

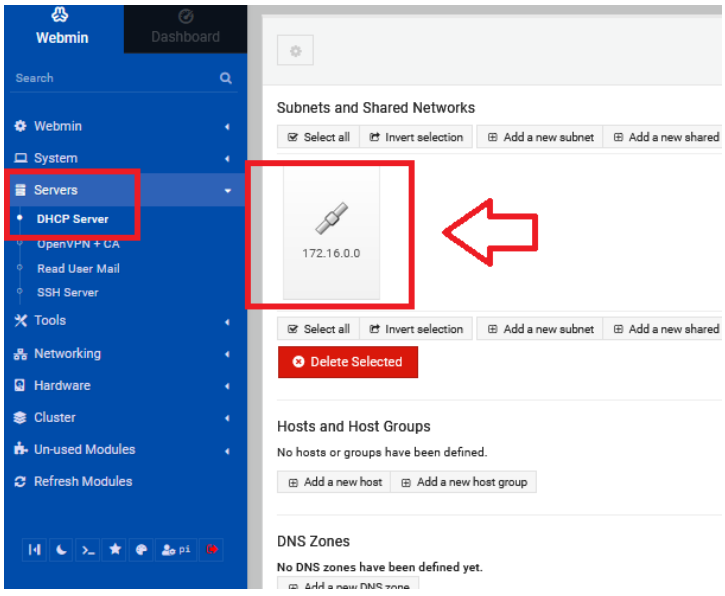


Fuente: Elaboración propia

4.3.5. Servicio de DHCP

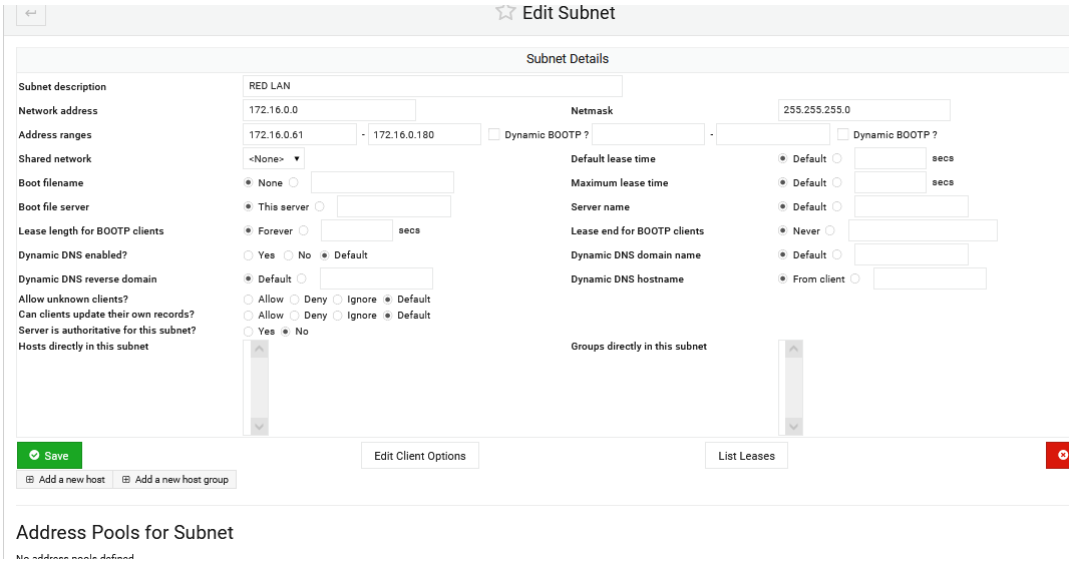
El módulo del DHCP de la VPN tuvo la siguiente configuración:

Figura 45. Configuración DHCP



Fuente: Elaboración propia

Figura 46. Configuración subnet DHCP

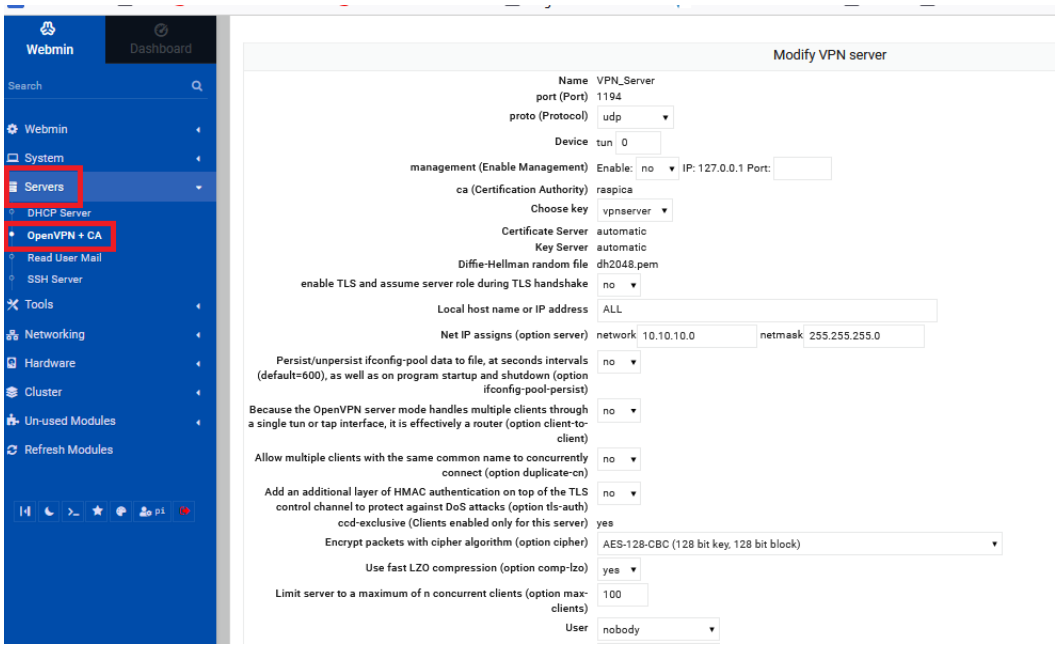


Fuente: Elaboración propia

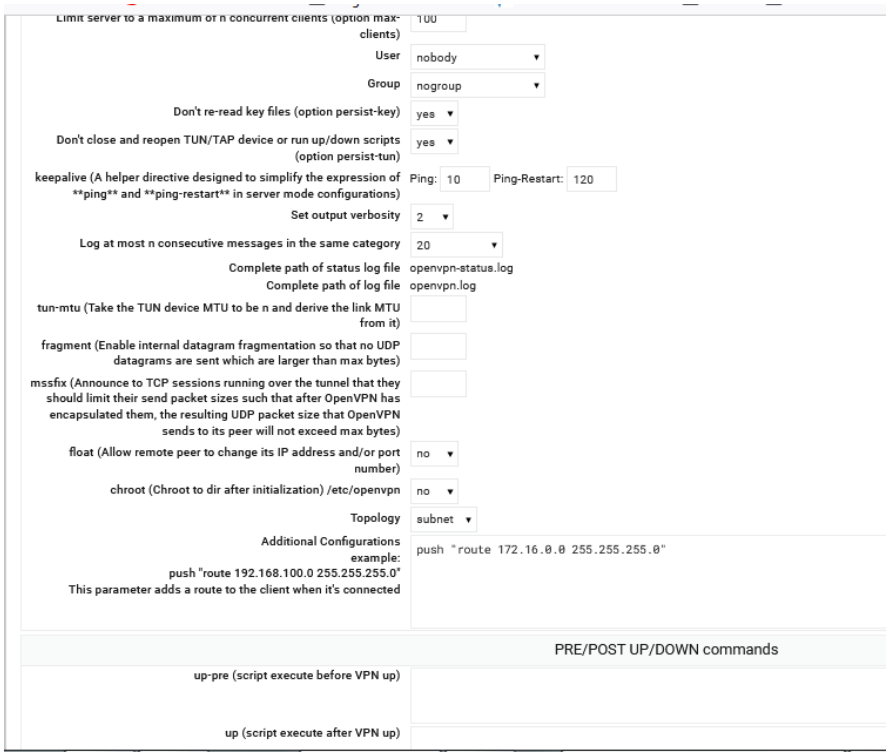
4.3.5. Servicio de OpenVPN

El módulo del servicio de VPN tuvo la siguiente configuración:

Figura 47. Configuración servidor VPN



Fuente: Elaboración propia



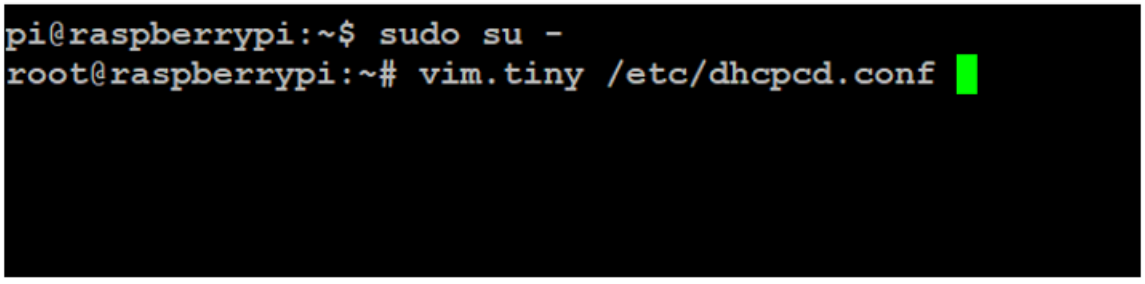
Fuente: Elaboración propia

4.3.6. Cambio de Ip pública en el Raspberry Pi

Tras haber cambiado de plan de internet residencial a plan empresarial se tuvo ingresar la Ip pública contratada.

Primero ingresar como usuario “pi” y luego hacerse “root”. Editar archivo /etc/dhcpcd.conf:

Figura 48. Comandos de cambio de ip pública



Fuente: Elaboración propia

Se cambió las líneas “static ip_address” y “static routers”

```
# fallback to static profile on eth0
#interface eth0
#fallback static_eth0
interface eth0
static ip_address=190.12.53.12/28
static routers=190.12.53.9
#static ip_address=192.168.137.10/24
#static routers=192.168.137.1
static domain_name_servers=4.2.2.2 8.8.8.8
```

Fuente: Elaboración propia

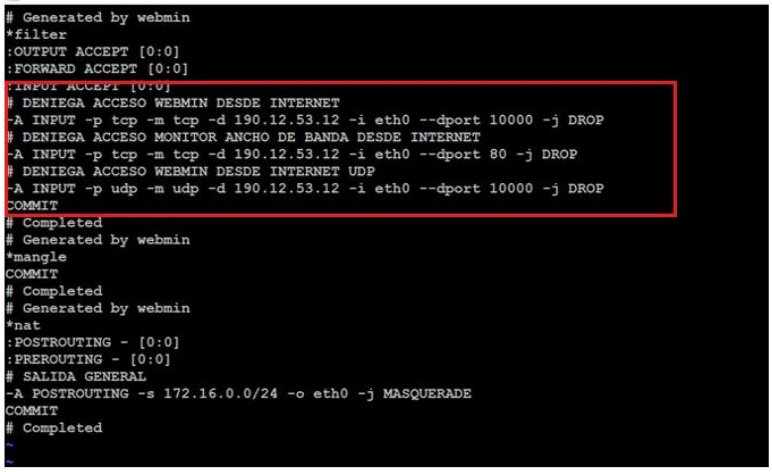
```
# fallback to static profile on eth0
#interface eth0
#fallback static_eth0
interface eth0
static ip_address=186.66.16.99/29
static routers=186.66.16.97
static domain_name_servers=4.2.2.2 8.8.8.8

interface eth0.2
static ip_address=172.16.0.1/24
~
```

Fuente: Elaboración propia

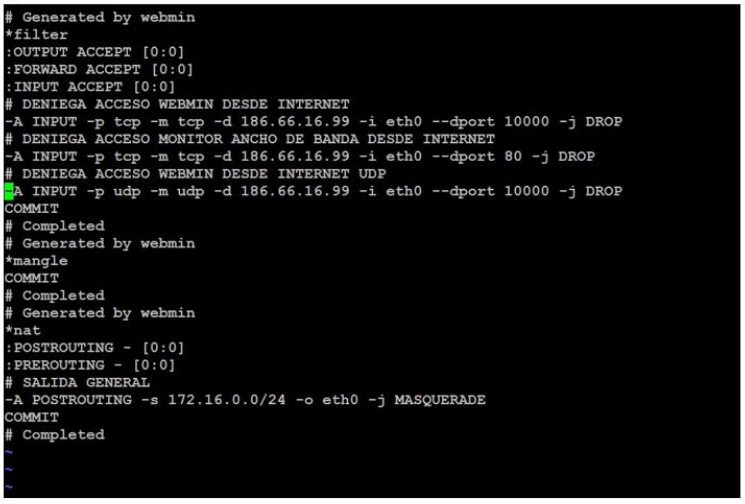
Luego se editó el archivo /etc/iptables.up.rules que contiene las reglas de Firewall:

```
root@raspberrypi:~# vim.tiny /etc/iptables.up.rules
```

Fuente: Elaboración propia



Fuente: Elaboración propia



Fuente: Elaboración propia

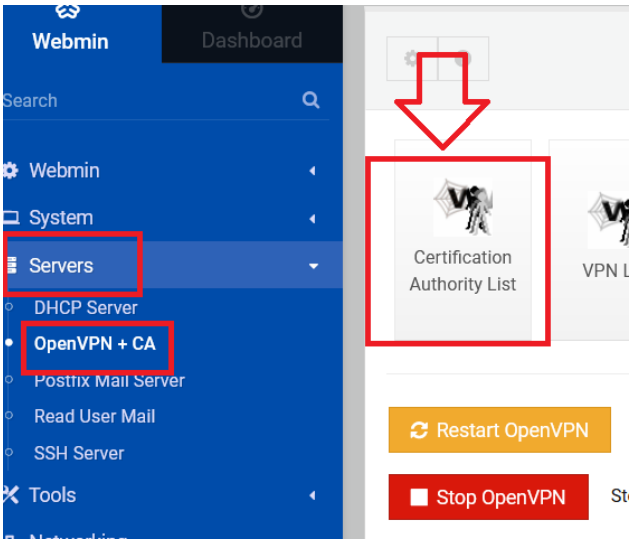
4.3.7. Linux Openvpn server – Administración de usuarios

Para agregar usuarios clientes que se puedan conectar a la red VPN, se deberá crear un certificado digital que contiene a su vez la llave de encriptación que utilizará el cliente para encriptar la información desde su estación de trabajo hacia el servidor VPN. Se recomienda que se utilice el nombre o etiqueta que identifique a cada uno de los certificados que se cree.

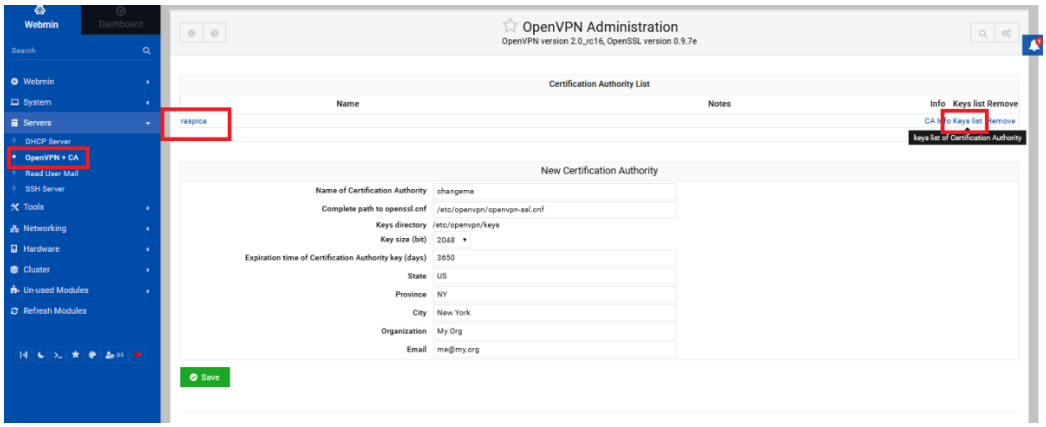
4.3.8. Generación del certificado que será asignado a usuario:

Ingresar a la interfaz Administrativa de Webmin e ingresar al módulo OPENVPN+CA. Alli se selecciona Certification Authority List:

Figura 49. Generación de certificado de autorización



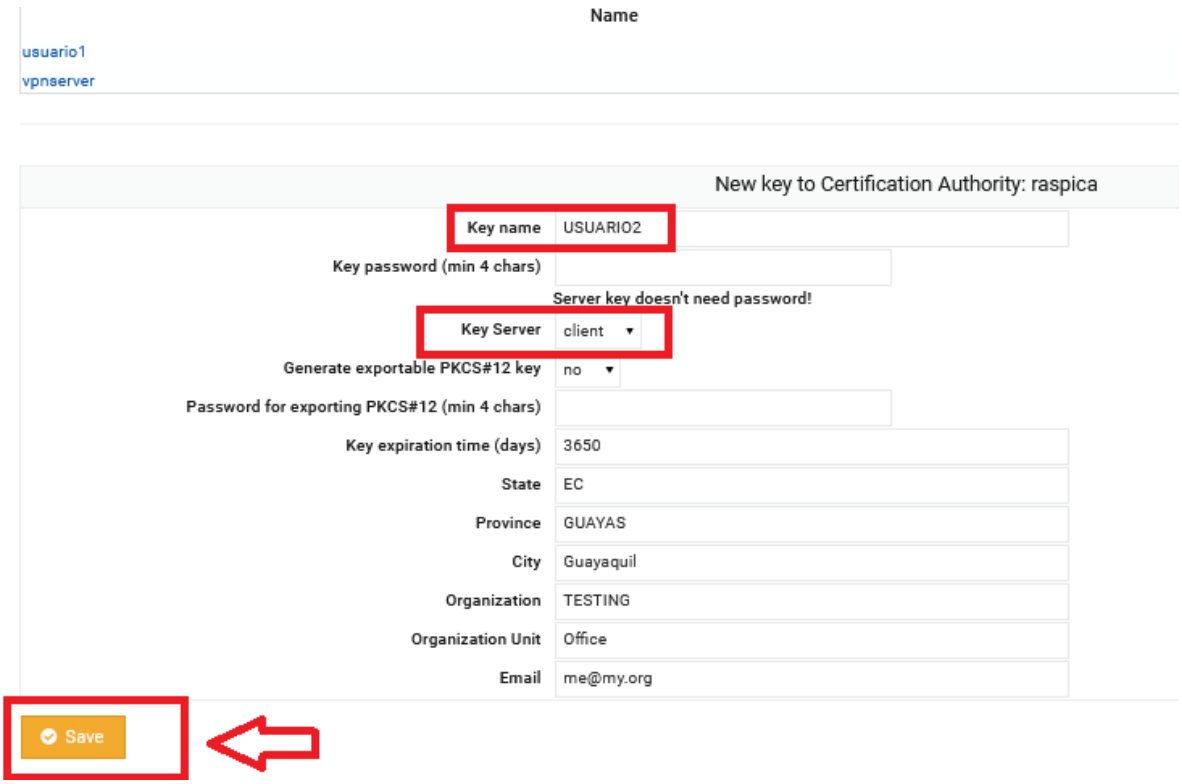
Fuente: Elaboración propia



Fuente: Elaboración propia

En la siguiente pantalla, llenar la forma correspondiente para la creación del certificado del usuario. Llenar el campo “Key name” con el nombre del usuario y seleccionar “Key Server=client”. Finalmente se guarda para generar el nuevo certificado.

Figura 50. Asignación de nombre a cliente VPN



Fuente: Elaboración propia

Posterior a esa acción se mostrará la pantalla de creación exitosa del certificado. El certificado ahora se mostrará listado en la pantalla inicial.

4.3.9. Revocando certificado para un usuario

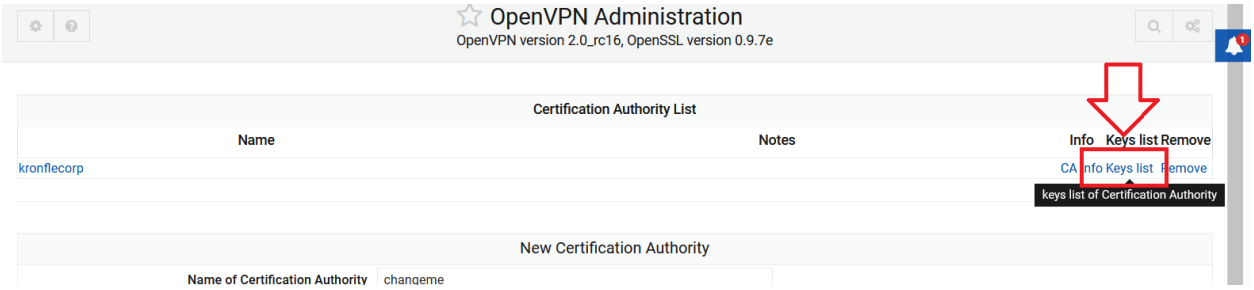
La revocación de un certificado significa invalidar un certificado firmado previamente de modo que ya no se puede utilizar para fines de autenticación.

Las causas más frecuentes por las que desea revocar un certificado incluyen:

- La clave privada asociada con el certificado está en peligro o es robada.
- El usuario de una clave privada encriptada olvida la contraseña de la clave.
- Quiere cancelar el acceso de un usuario VPN.

Para revocar un certificado de un usuario ingrese al software Webmin y se dirige al módulo OPENVPN+CA Allí se coloca sobre el icono Certificación Authority List y a continuación sobre “Keys list”:

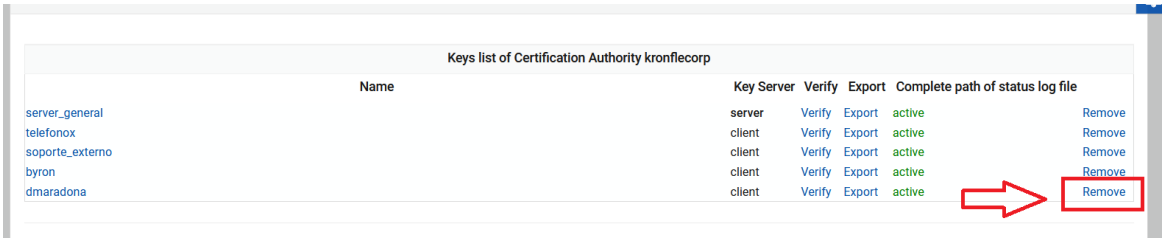
Figura 51. Revocación de certificado de autentificación



Fuente: Elaboración propia

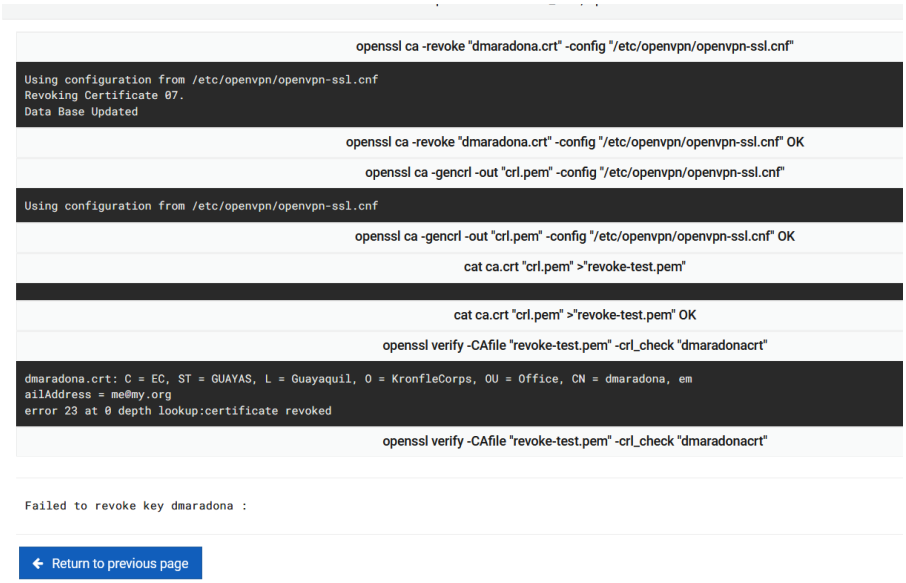
Se listarán los certificados emitidos por el servidor. Se selecciona sobre “Remove” correspondiente al certificado que desea REVOCAR:

Figura 52. Revocación de certificado por usuario

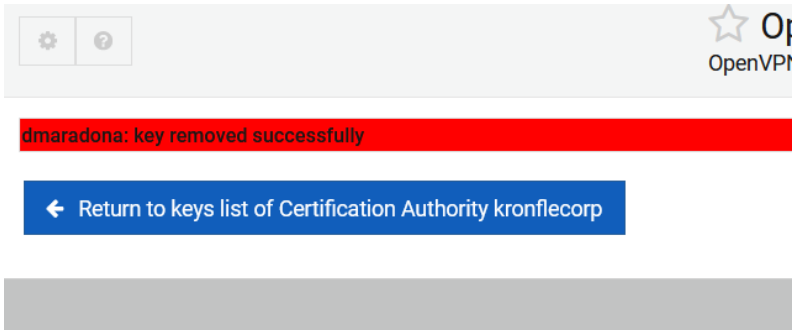


Fuente: Elaboración propia

A continuación, se mostrará la acción de revocación del certificado.



Fuente: Elaboración propia

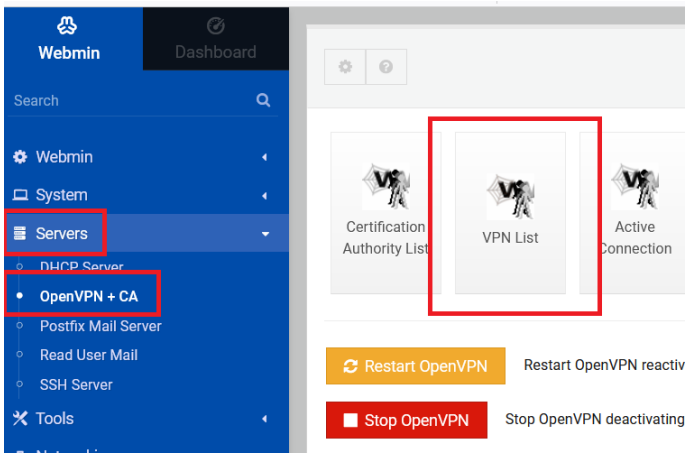


Fuente: Elaboración propia

4.3.10. Generación del archivo de configuración VPN para cliente:

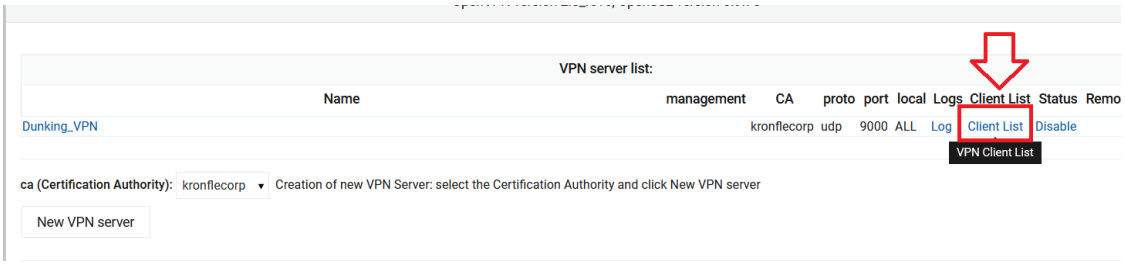
Para generar el archivo de configuración para el cliente OpenVPN, ingresar a la interfaz administrativa del Webmin y dirigirse al menú de Server → OpenVPN+CA y se selecciona VPN list:

Figura 53. Generación de archivo OVPN para el cliente



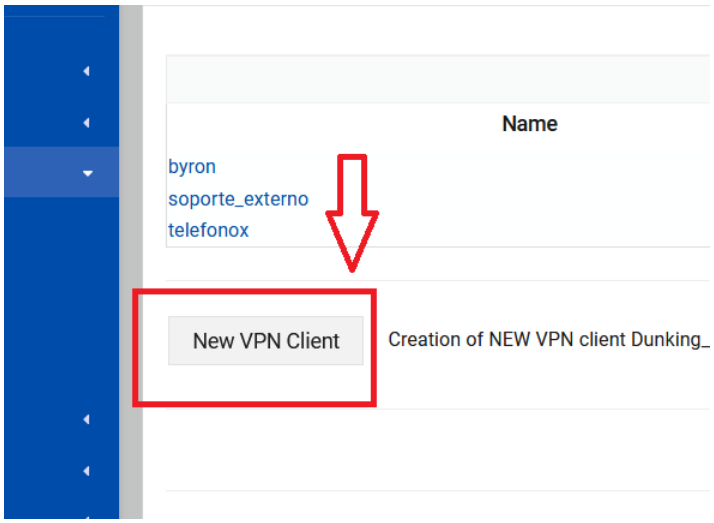
Fuente: Elaboración propia

En la siguiente ventana, se selecciona “Client List”:



Fuente: Elaboración propia

Se crea un nuevo cliente VPN



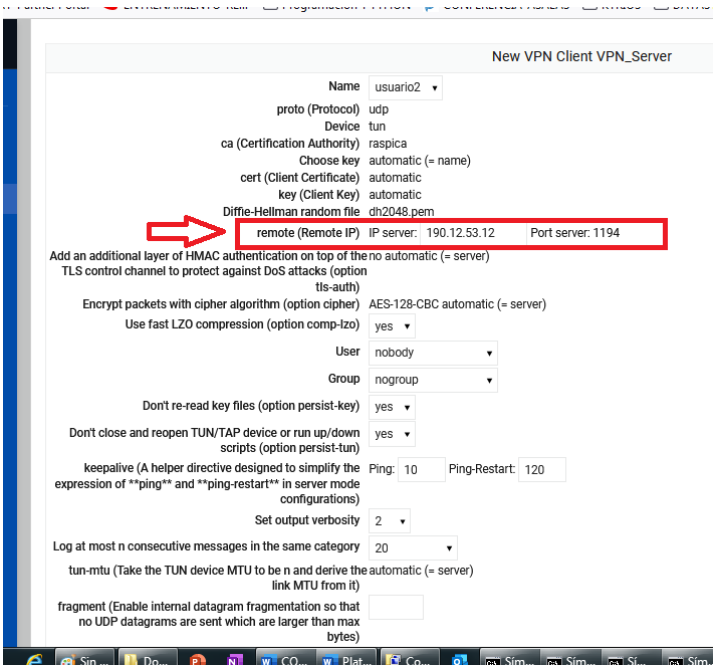
Fuente: Elaboración propia

A continuación, se muestran los campos que se debe configurar para el cliente VPN:

Name: Debe estar seleccionado el certificado del usuario

Remote: Ingresar la IP del Firewall de: 190.12.53.12

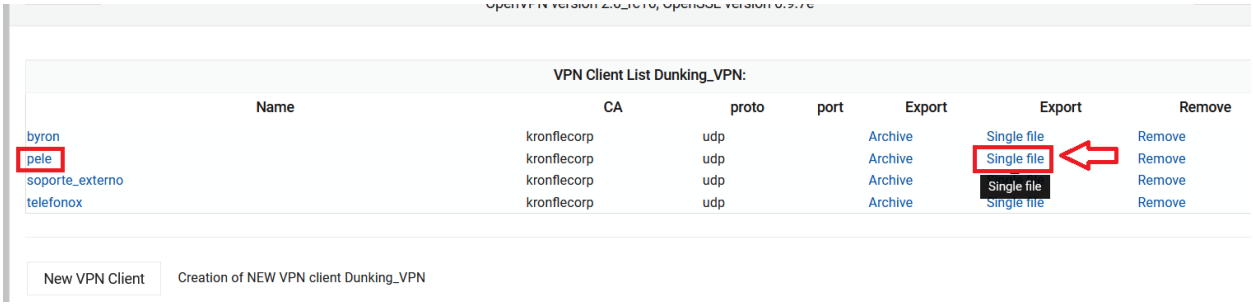
Figura 54. Asignación ip pública al certificado del usuario



Fuente: Elaboración propia

Ahora la configuración del usuario aparecerá listada en la parte superior de la pantalla. Se debe dirigirse a “Single File” para descargar el archivo de configuración. Enviar el archivo de configuración al usuario final.

Figura 55. Exportación de archivo cliente



Fuente: Elaboración propia

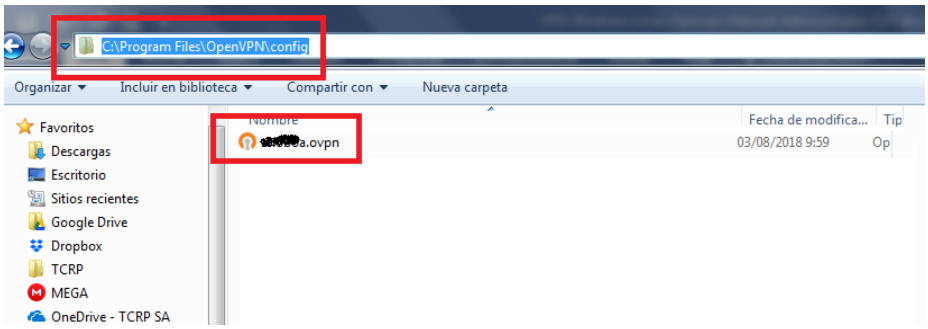
Configuración en Windows del cliente

- Version: Windows 7 o Windows 10
- VPN Client: OpenVPN GUI v2.5

Cada usuario debe recibir un archivo de configuración OPENVPN en formato. ovpn con su configuración específica y claves de encriptación que serán utilizadas en la conexión VPN.

1) Instalar cliente OpenVPN (32 o 64 bits según corresponda) http://openvpn.net/index.php/open-source/downloads.html
2) Copiar archivo USUARIO.ovpn en %programfiles(x86)%\OpenVPN\config o %programfiles%\OpenVPN\config según la version de 32 o 64 bits.

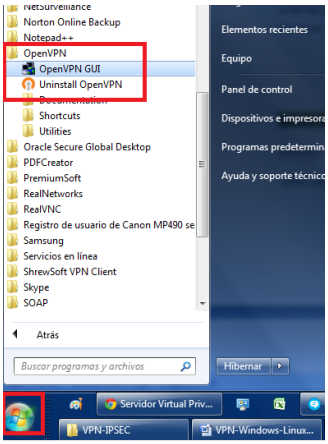
Figura 56. Instalación de archivo cliente



Fuente: Elaboración propia

Para proceder con la conexión VPN, el usuario debe seguir los siguientes pasos:

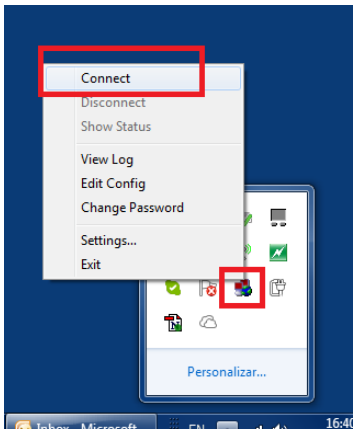
1) Abrir el GUI de la aplicación OpenVPN:



Fuente: Elaboración propia

2) Hacer click derecho sobre el icono del cliente VPN, y escoger la opción “Connect”.

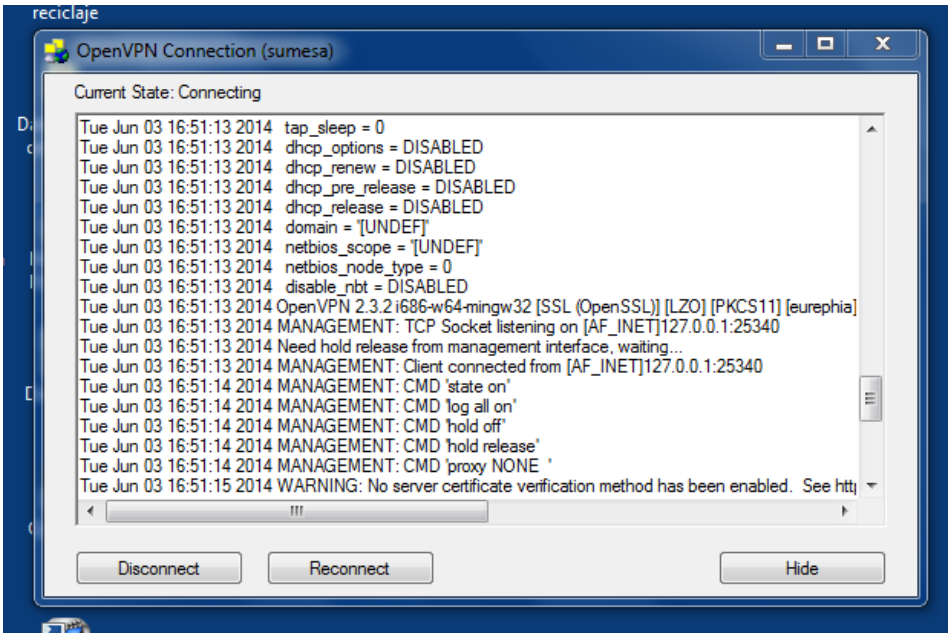
Figura 57. Conexión al servidor VPN



Fuente: Elaboración propia

3) Se mostrará el detalle del proceso de conexión.

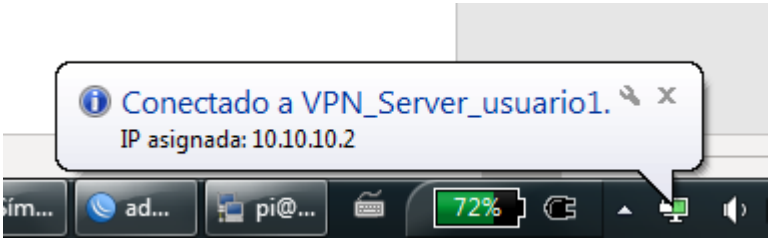
Figura 58. Detalles de conexión al servidor VPN



Fuente: Elaboración propia

4) El proceso de conexión es exitoso cuando se muestre el mensaje “NOMBREUSUARIO is now connected”.

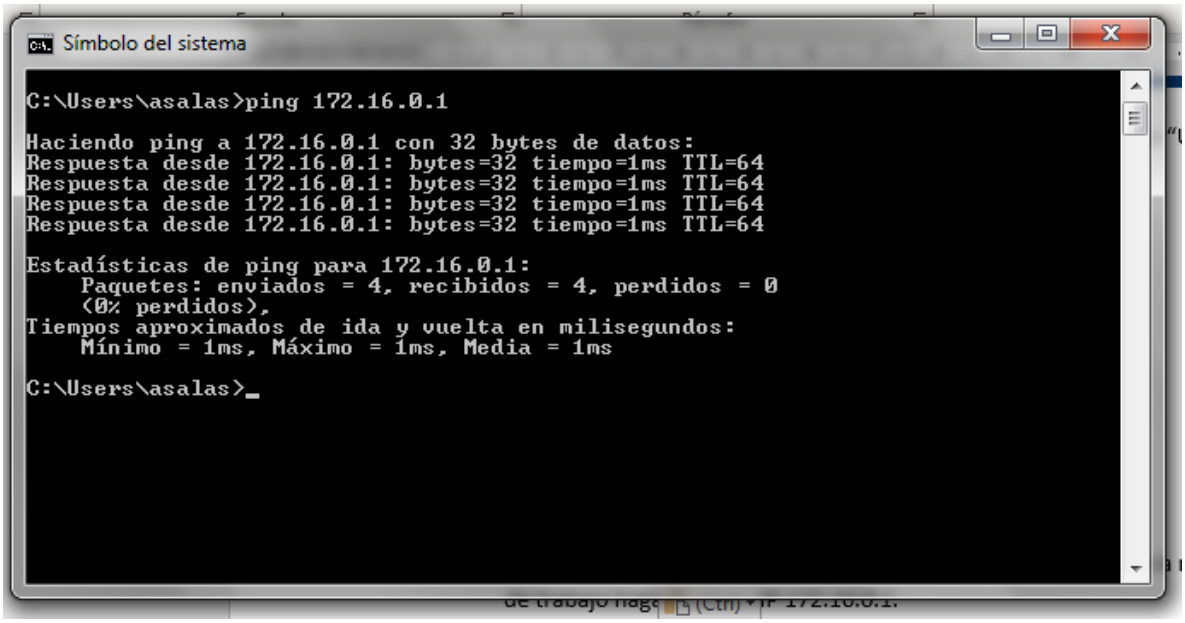
Figura 59. Mensaje de conexión exitosa



Fuente: Elaboración propia

5) Una vez establecida la VPN, para comprobar que tiene acceso a la red, desde la estacion de trabajo haga ping a la IP 172.16.0.1.

Figura 60. Comprobación de comunicación de los equipos

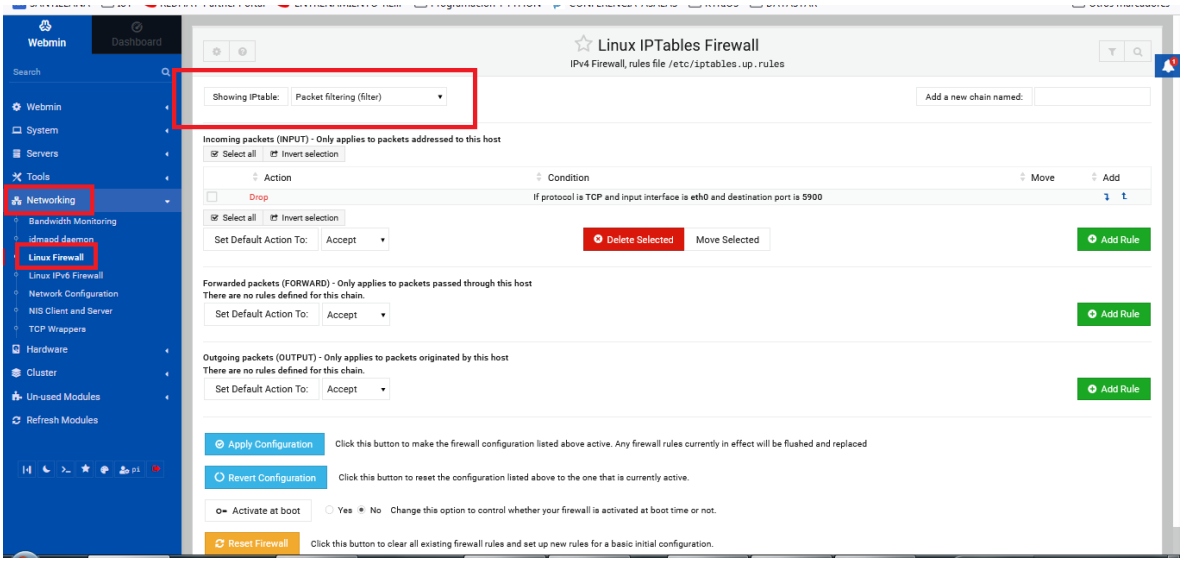


Fuente: Elaboración propia

4.3.11. Servicio de firewall

El servicio de firewall tiene su interfaz de administración en el menú de Networking → Linux Firewall en donde se puede establecer IPTables en las cuales se pone diferentes reglas para definir qué tipo de datos son los que se recibe y transmite.

Figura 61. Servicio de firewall del servidor

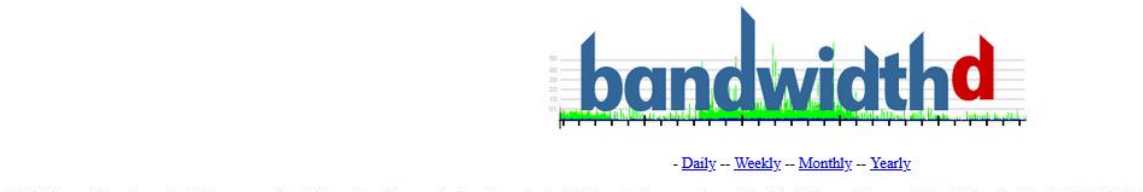


Fuente: Elaboración propia

4.3.12. Servicio de monitoreo de uso de ancho de banda de internet

El sistema cuenta con un monitoreado de uso de ancho de banda de INTERNET. El cual puede ser consultado en esta URL:

Figura 62. Servicio de monitoreo de banda ancha del servidor



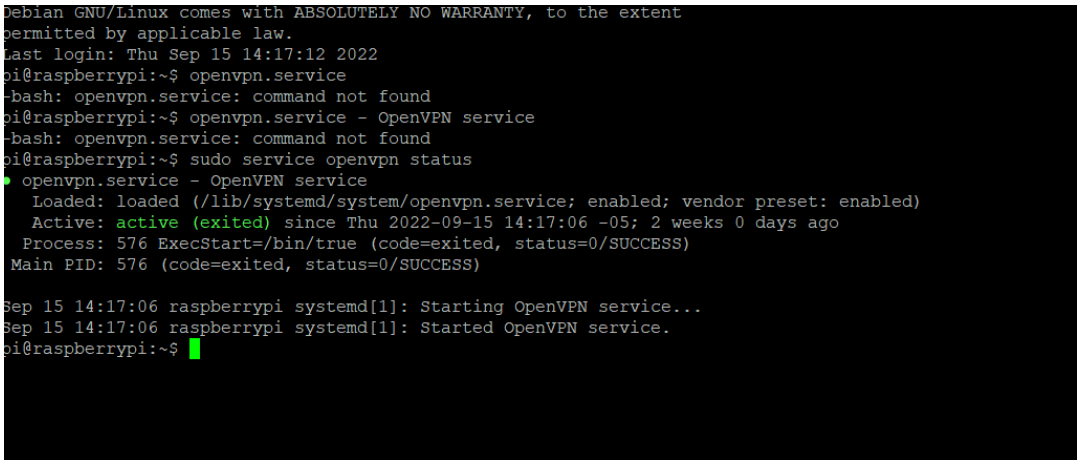
Fuente: Elaboración propia

4.4. Comprobación de correcta funcionalidad de la primera parte de la propuesta tecnológica

- **Ingresando por medio de SSH a Raspberry se puede observar el estado del servicio OpenVPN con el siguiente comando:**

sudo service openvpn status

Figura 63. Estado de servicio VPN



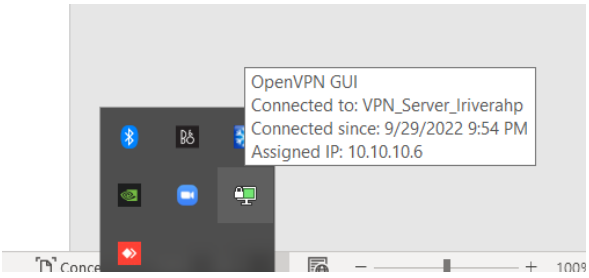
Fuente: Elaboración propia

En este grafico podemos apreciar que los servicios están activos

En la computadora del cliente:

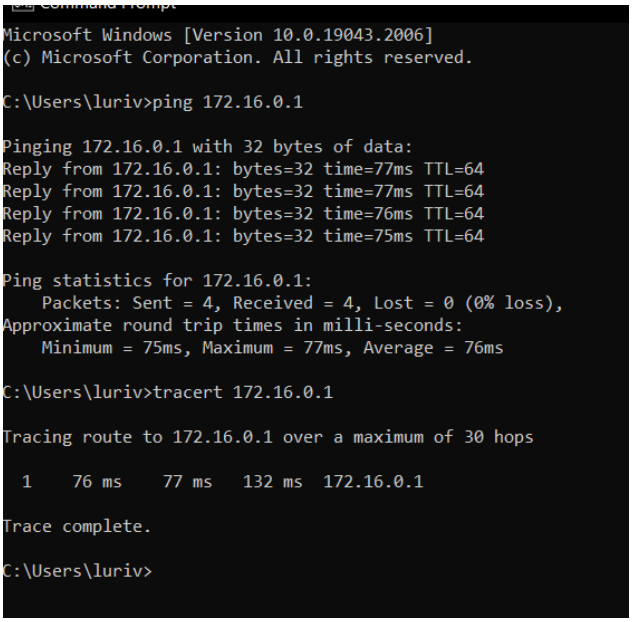
Cada vez que se conecte a la VPN le saldra lo siguiente:

- Al servidor que esta conectado
- La fecha de conexión
- La IP que se le ha sido asignada



Fuente: Elaboración propia

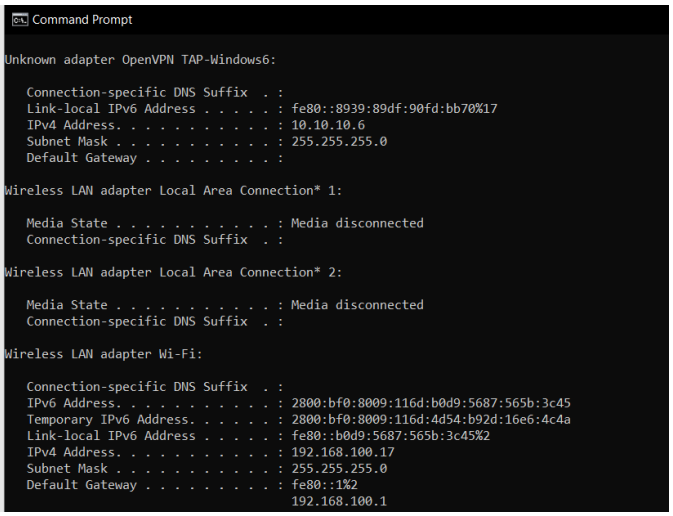
También se puede validar la comunicación ingresando por medio de comando de Windows y haciendo ping a las IP de los equipos de la oficina.



Fuente: Elaboración propia

Al igual con el comando ipconfig en Windows se puede observar la ip que le ha asignado la VPN

Figura 64. Verificación de asignación ip del equipo del cliente



Fuente: Elaboración propia

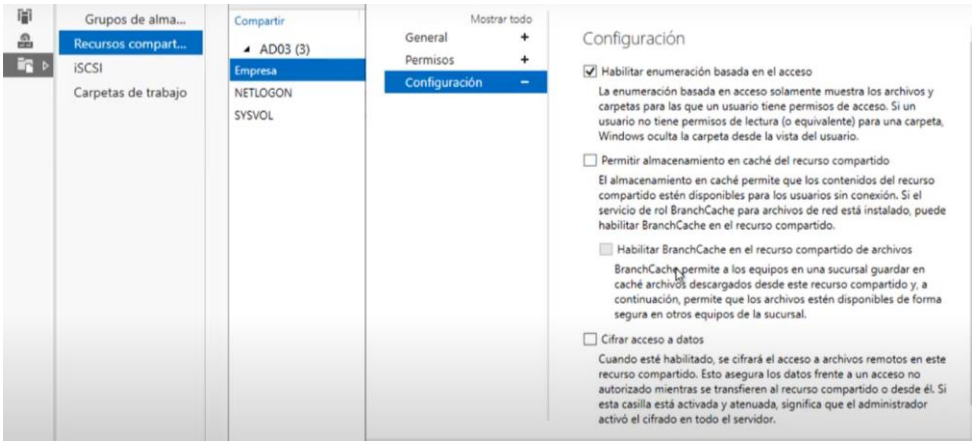
4.4. Parte 2: Almacenamiento

Después de haber instalado Windows Server 2019 se realiza las siguientes configuraciones para el servidor de archivos que requiere la empresa.

Configuración file server en Windows Server 2019

Una vez levantado los servicios de archivos y almacenamiento se ingresa a sus recursos compartidos y se habilita la enumeracion basada en el acceso.

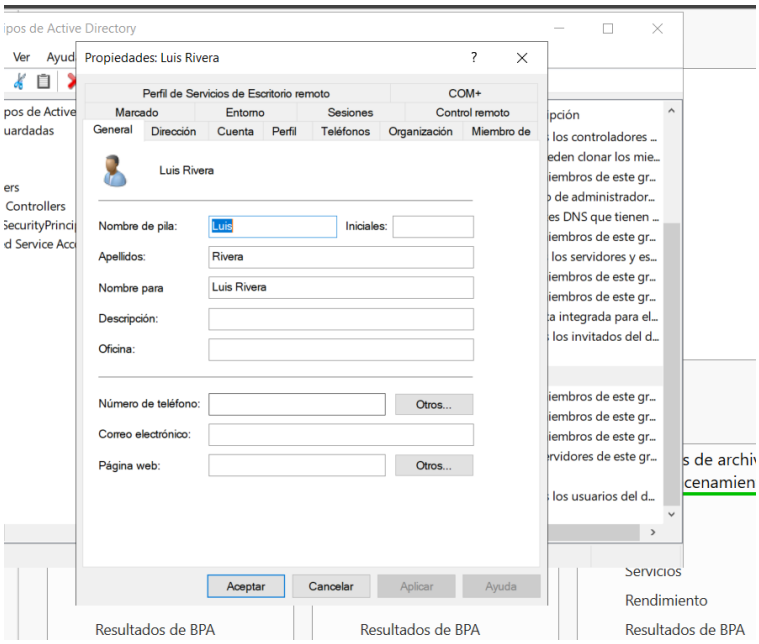
Figura 65. Configuración de file server



Fuente: Elaboración propia

Se crea un perfil del usuario que va a cumplir el rol de administrador

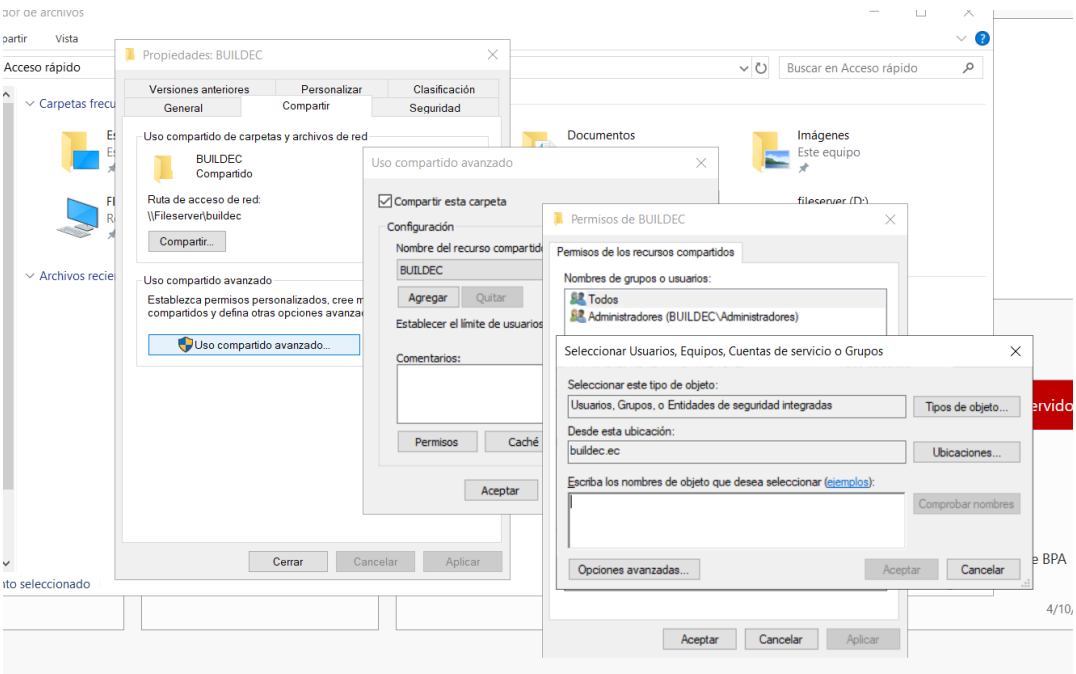
Figura 66. Creación de perfil administrador



Fuente: Elaboración propia

Luego se crea una carpeta de administracion y se concede todos los permisos para el acceso del administrador

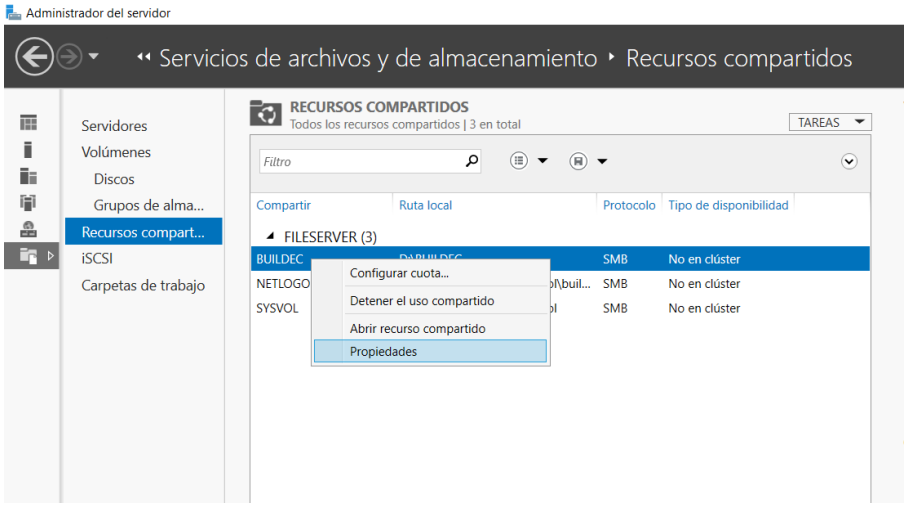
Figura 67. Permisos de usuarios y equipos



Fuente: Elaboración propia

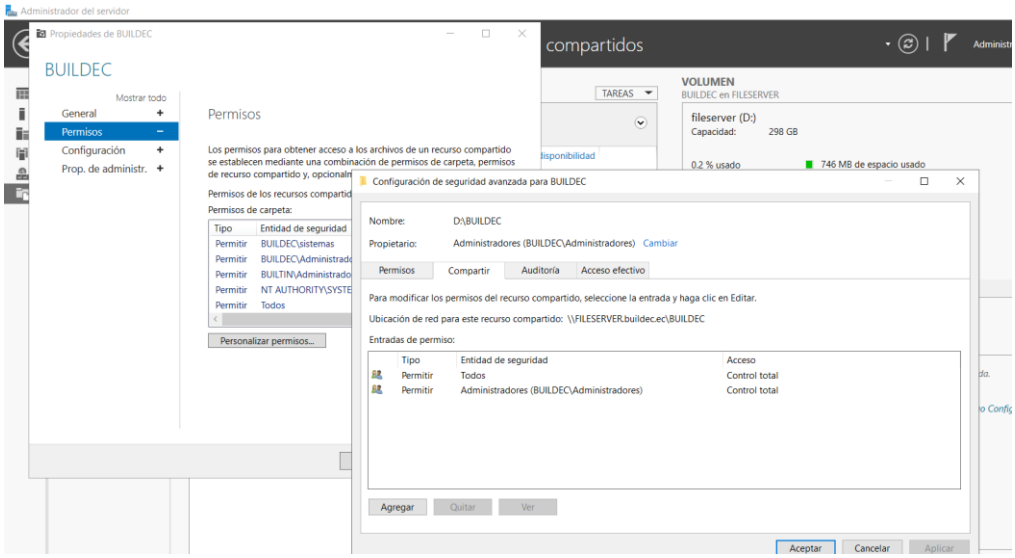
Se busca las propiedades de la carpeta creada en recursos compartidos del servidor

Figura 68. Propiedades de las carpetas del usuario



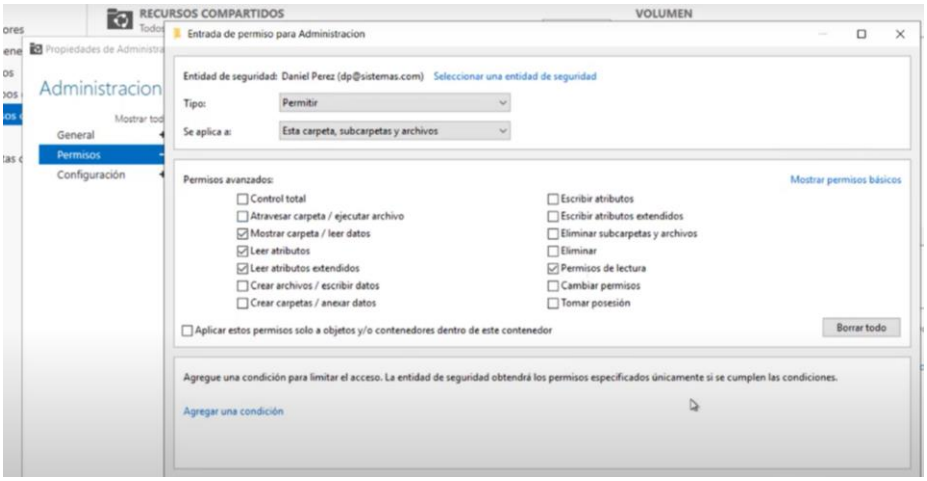
Fuente: Elaboración propia

Se concede los permisos a los diferentes usuarios



Fuente: Elaboración propia

En la opcion de entrada de permiso para administrador se puede observar de manera mas detallada y completa los permisos que puede tener el usuario.

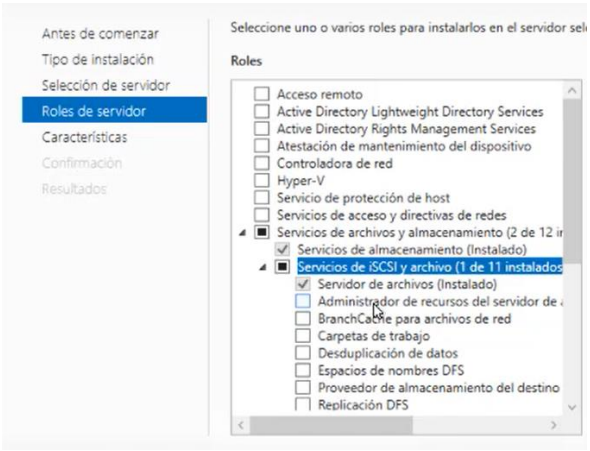


Fuente: Elaboración propia

Adición de consola de administrador del servidor

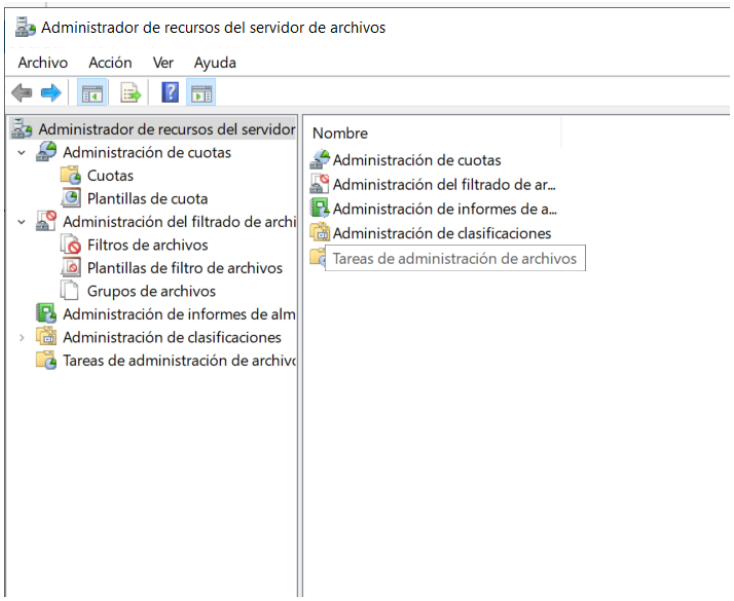
Esta consola administrara el filtrado de archivos y también los recursos de almacenamiento remoto.

Se debe de acceder a los roles del servidor y activar los servicios de administrador de recursos del servidor



Fuente: Elaboración propia

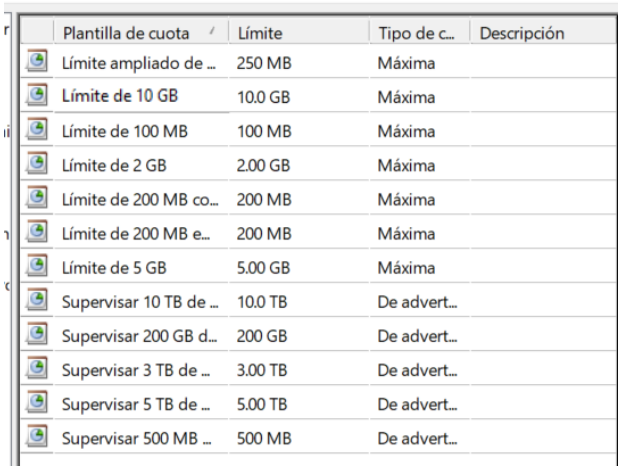
Una vez activado el servicio se habilitará el administrador de recursos en las herramientas



Fuente: Elaboración propia

En el administrador de recursos del servidor de archivos se encuentran las siguientes opciones:

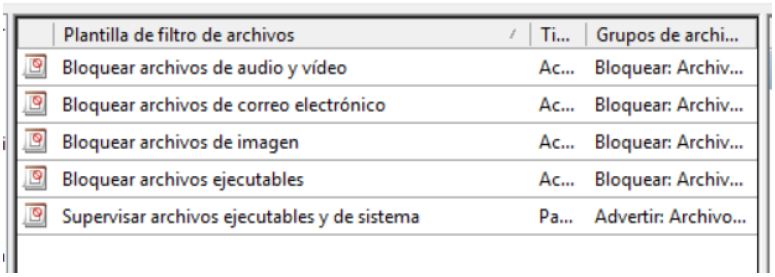
- Administración de cuotas
  Limita y supervisa la capacidad de archivos que se están almacenando en el servidor



Plantilla de cuota	Límite	Tipo de c...	Descripción
Límite ampliado de ...	250 MB	Máxima	
Límite de 10 GB	10.0 GB	Máxima	
Límite de 100 MB	100 MB	Máxima	
Límite de 2 GB	2.00 GB	Máxima	
Límite de 200 MB co...	200 MB	Máxima	
Límite de 200 MB e...	200 MB	Máxima	
Límite de 5 GB	5.00 GB	Máxima	
Supervisar 10 TB de ...	10.0 TB	De advert...	
Supervisar 200 GB d...	200 GB	De advert...	
Supervisar 3 TB de ...	3.00 TB	De advert...	
Supervisar 5 TB de ...	5.00 TB	De advert...	
Supervisar 500 MB ...	500 MB	De advert...	

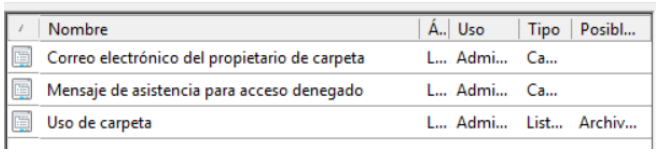
Fuente: Elaboración propia

- Administración de filtrado de archivos
  Bloquea diferentes tipos de archivos



Fuente: Elaboración propia

- Administración de informes de almacenamiento
  Genera reportes del almacenamiento en el servidor.
- Administración de clasificaciones

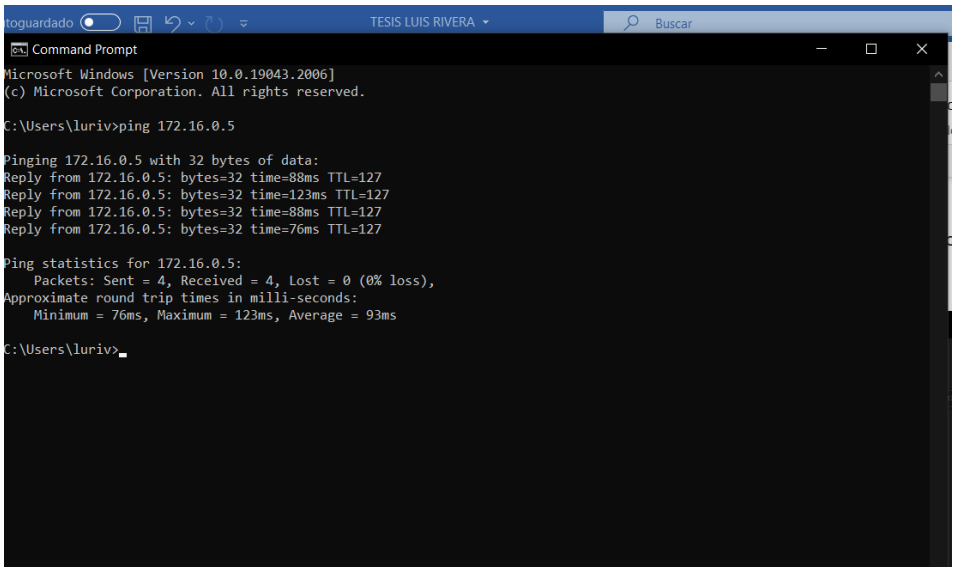


Fuente: Elaboración propia

Este servicio se levantó debido a que el presidente de la empresa indicó que se supervise los archivos ejecutables.

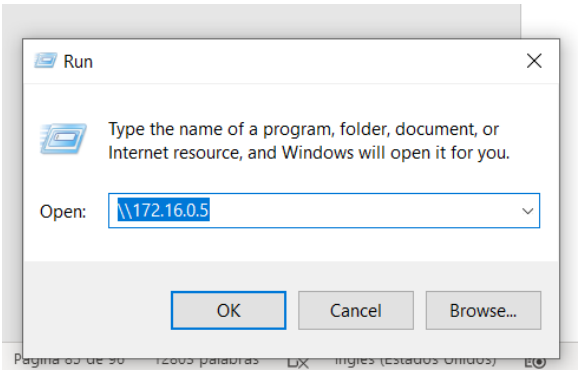
Procedimiento de adición de carpeta compartida en computadora del usuario

Después de haberse conectado por medio de la VPN se comprueba la comunicación con el servidor



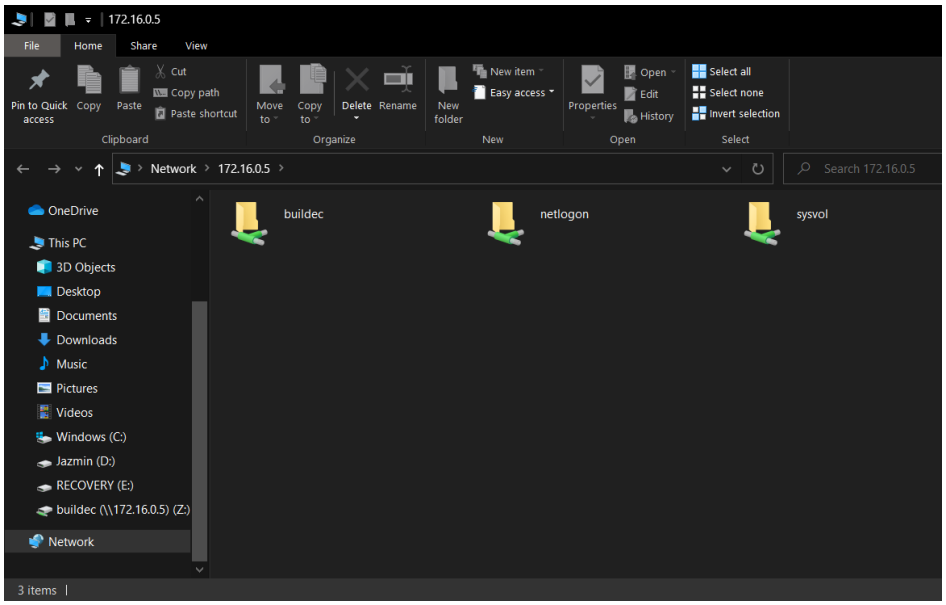
Fuente: Elaboración propia

Luego en ejecutar se escribe la ip del del servidor para acceder a las comparticiones

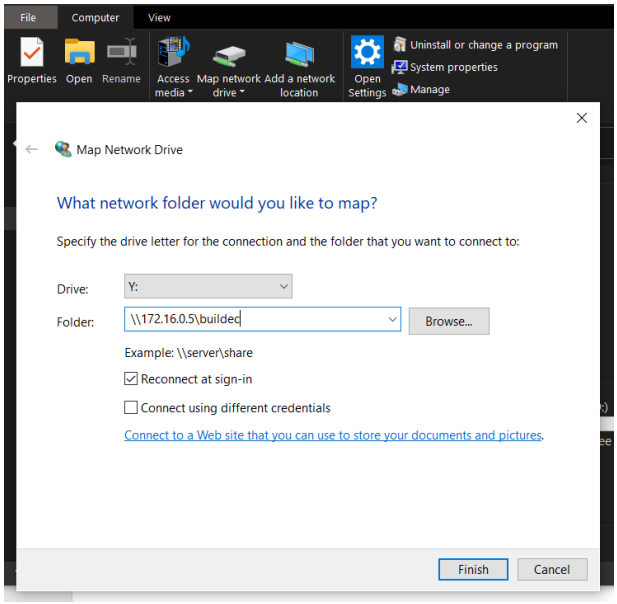


Fuente: Elaboración propia

Al acceder a las comparticiones se copia la direccion de la carpeta que se ha creado los permisos y se pega en el mapeo de unidades

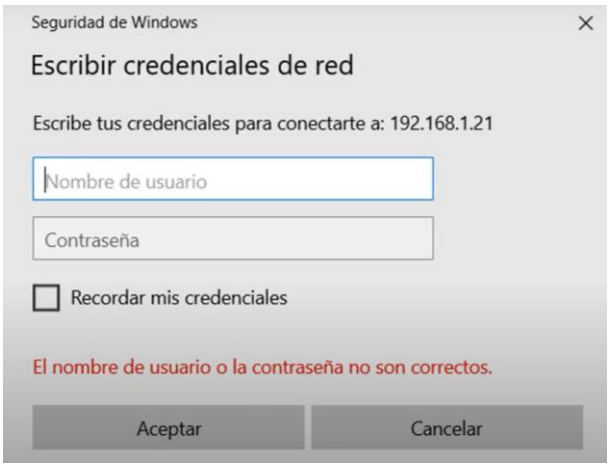


Fuente: Elaboración propia



Fuente: Elaboración propia

El usuario deberá ingresar las credenciales que se le ha asignado

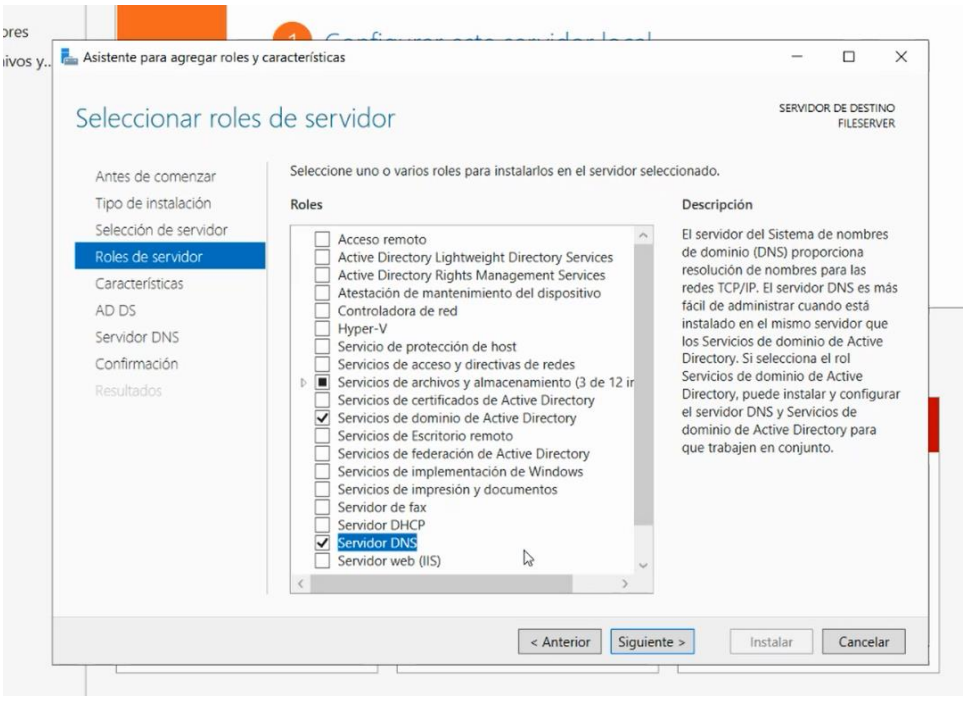


Fuente: Elaboración propia

4.5. Parte 3: Administración de usuarios y equipos

En esta parte del proyecto se detallan los procesos de la instalación de Active Directory en Windows Server 2019.

En los roles y características del servidor se levantan los servicios de Active Directory y el servidor DNS.

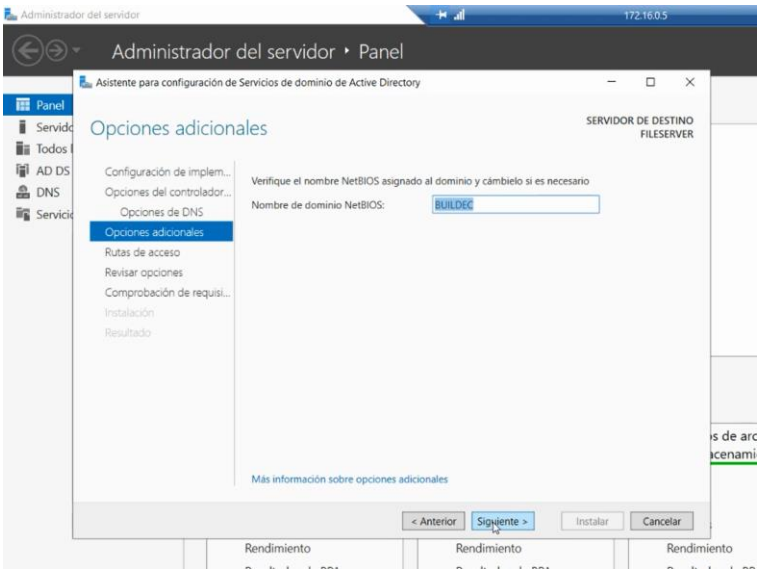


Fuente: Elaboración propia

Al finalizar el levantamiento del servicio se promueve el controlador de dominio.

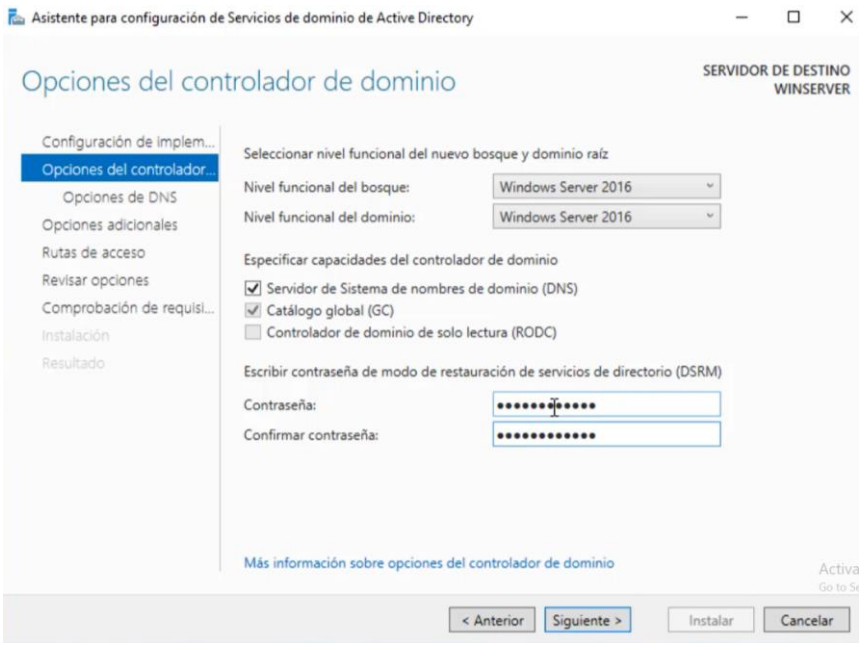
Fuente: Elaboración propia

Se pone como nombre de dominio del NetBIOS el nombre de la compañía.



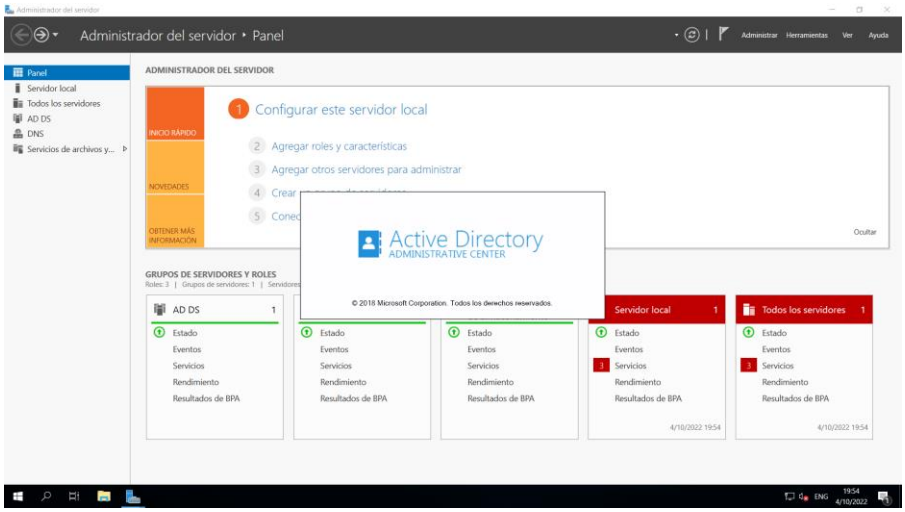
Fuente: Elaboración propia

A continuación, se procede a colocar las contraseñas de administrador que se establecieron anteriormente.



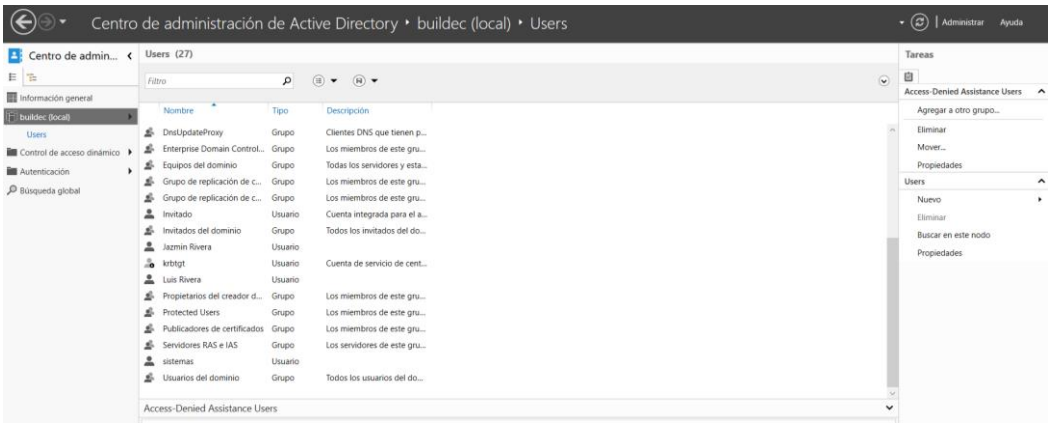
Fuente: Elaboración propia

Despues de unos procedimientos mas de configuracion se genera el directorio acivo.



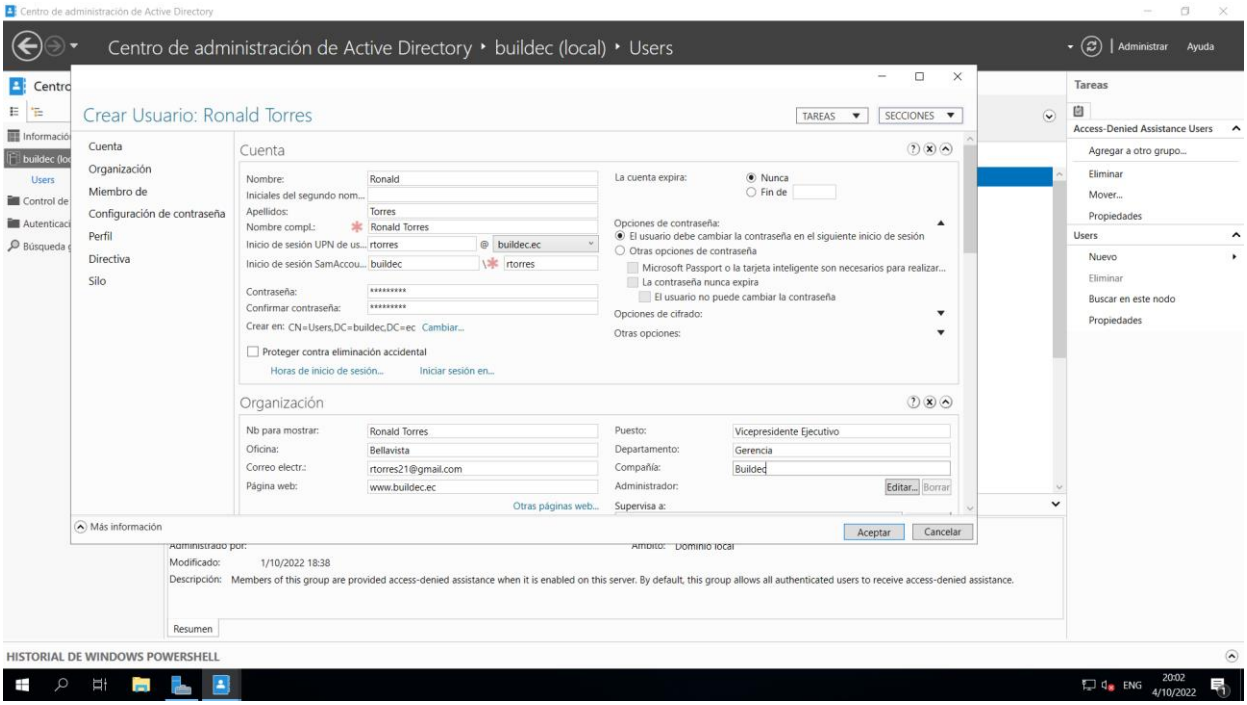
Fuente: Elaboración propia

En el cual se pueden ver detalladamente los usuarios y equipos



Fuente: Elaboración propia

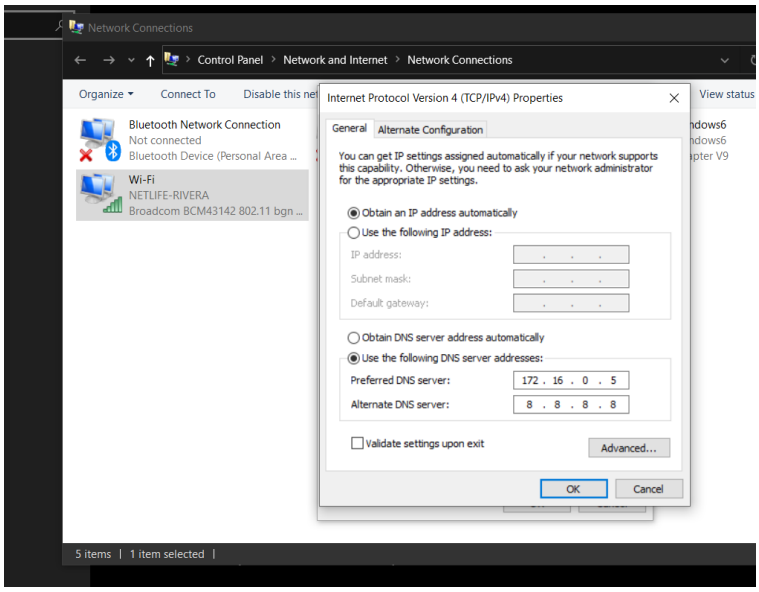
Al finalizar la instalación se procedió a crear el usuario del vicepresidente ejecutivo



Fuente: Elaboración propia

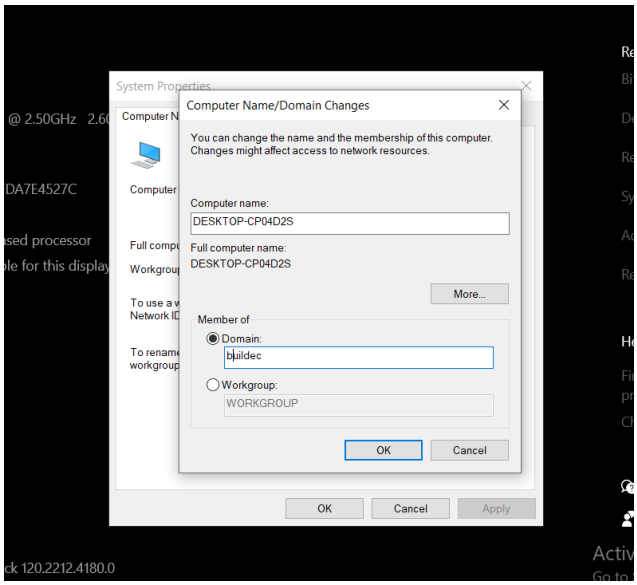
Administración de equipos en directorio activo por medio de VPN

Para conectar la computadora al directorio activo, debe de estar en el mismo segmento de red así que se cambia el DNS del adaptador de red.



Fuente: Elaboración propia

Se debe dirigirse a opciones avanzadas del computador para introducir el dominio de Buildec



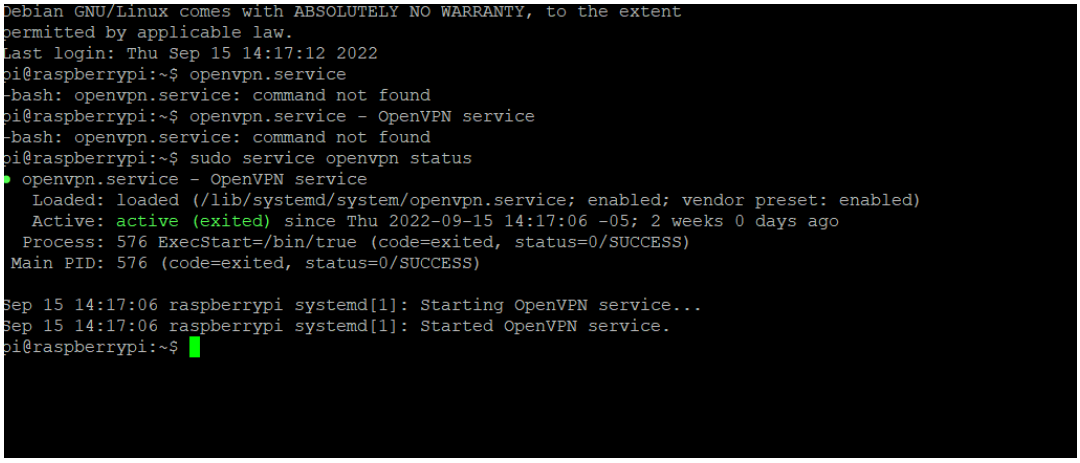
Fuente: Elaboración propia

Validación de la propuesta tecnológica

Ingresando por medio de SSH a Raspberry se puede observar el estado del servicio OpenVPN con el siguiente comando:

sudo service openvpn status

Figura 69. Estado de servicio VPN



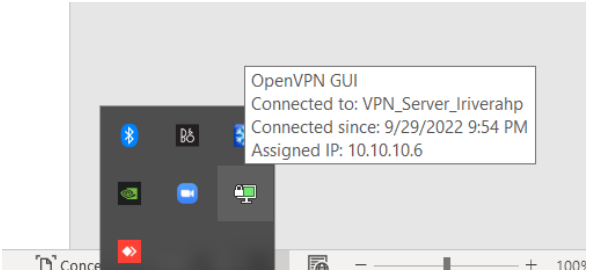
Fuente: Elaboración propia

En este grafico podemos apreciar que los servicios están activos

En la computadora del cliente:

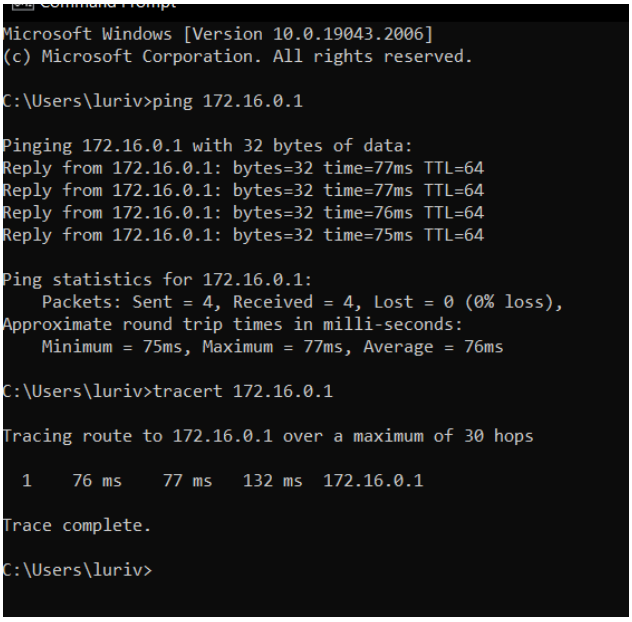
Cada vez que se conecte a la VPN le saldra lo siguiente:

- Al servidor que esta conectado
- La fecha de conexión
- La IP que se le ha sido asignada



Fuente: Elaboración propia

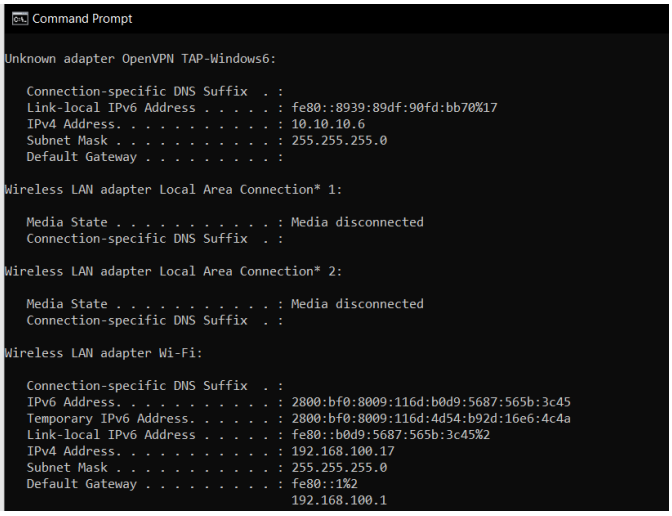
También se puede validar la comunicación ingresando por medio de comando de Windows y haciendo ping a las IP de los equipos de la oficina.



Fuente: Elaboración propia

Al igual con el comando ipconfig en Windows se puede observar la ip que le ha asignado la VPN

Figura 70. Verificación de asignación ip del equipo del cliente

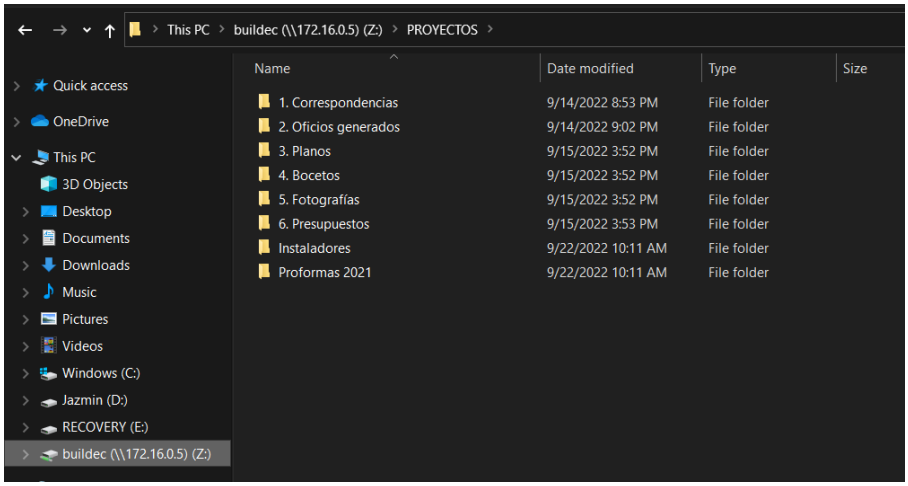


Fuente: Elaboración propia

Resultados de la implementación del servidor de archivos

Tras una consulta realizada a los socios de la empresa, decidieron que la carpeta este organizada de la siguiente forma:

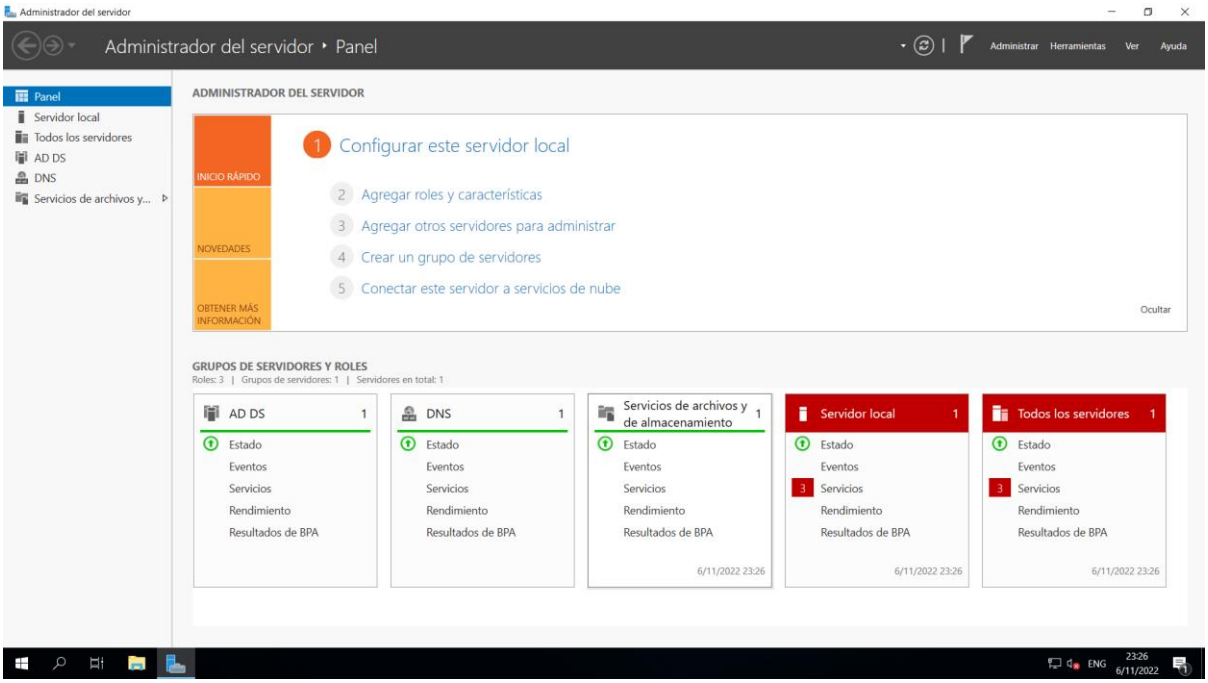
1. Correspondencia
2. Oficios generados
3. Planos
4. Bocetos
5. Fotografías
6. Presupuesto



Fuente: Elaboración propia

Servidores activos en Windows server 2019

A continuación se puede observar los servicios que están activos en Windows Server los cuales son el servidor de archivos, active directory y el servidor DNS.



Fuente: Elaboración propia

Conclusiones

Las empresas públicas y privadas manejan información confidencial, que es de uso exclusivo de sus trabajadores, y que normalmente está expuesta a amenazas informáticas si no se emplea conexiones seguras para su transferencia en la red. En el proceso de la investigación se identificó referentes tecnológicos de seguridad basada en la tunelización sobre Raspberry Pi, y se llegó a la conclusión que el protocolo OpenVPN ofrece mejores beneficios en cuanto a encriptación de datos con altos niveles de seguridad, velocidad, encriptación y estabilidad.

La propuesta del trabajo de titulación se implementó en la red de la empresa constructora BUILDERECUADOR CIA.LTDA, y se analizó su situación actual para proponer mejoras en su transferencia y almacenamiento de datos. La empresa lleva a cabo varios proyectos inmobiliarios, los cuales son planificados entre el equipo de trabajo ubicado en las oficinas de Loja y Guayaquil.

Se constató que para la transferencia y almacenamiento de datos de los proyectos utilizaban medios convencionales como: correos electrónicos corporativos, dispositivos externos como discos duros y memorias externas, uso de páginas web como WeTransfer para enviar y recibir archivos de gran tamaño, creación de carpetas con información dentro de las computadoras de escritorio o computadoras portátiles y utilización de plataformas de almacenamiento en la nube como Google Drive. Dichos medios de transferencia y almacenamiento de información que empleaba la empresa, no contaban con un respaldo seguro de conexión encriptada para las vulnerabilidades informáticas.

Mediante una entrevista al Presidente de la empresa BUILDERECUADOR CIA.LTDA se determinaron los requerimientos necesarios para implementar la propuesta tecnológica del presente trabajo de titulación. Uno de los requerimientos fue el de aplicar un sistema de transferencia / almacenamiento de información compartido entre las dos oficinas de Guayaquil y Loja como un medio de recopilación documental de cada proyecto que lleva a cabo la empresa, así como considerar que la información que maneja la empresa es de carácter gráfico y

requirió que el sistema a implementar tuviera una gran capacidad de memoria para almacenar dicha información. Además se necesitó que exista una carpeta compartida para que los equipos de trabajo de Loja y Guayaquil pudieran trabajar simultáneamente en la información de los proyectos de la empresa y permitir un mejor control documental por cada obra realizada, con el fin de obtener un expediente digital organizado.

Para lo cual, se procedió a realizar la implementación de la solución tecnológica mediante un diseño de red privada remota que ayude a la seguridad del manejo de la información de la empresa BUILDERECUADOR CIA.LTDA. de acuerdo con las necesidades y requerimientos planteados.

Por medio de la investigación y análisis de costo beneficio de acorde a un presupuesto, se puede concluir que el equipo utilizado como Core principal que es el Raspberry Pi 4 es una herramienta de gran ayuda para avanzar en el uso de las tecnologías de la información y comunicación.

Recomendaciones

Se recomienda:

- A los directivos que gestionen su inversión de tecnología de la información de acuerdo a una planificación estratégica que permita evaluar los niveles de impacto de las soluciones tecnológicas que sean implementadas a futuro.
- Cambiar plan de internet residencial a empresarial en oficina ubicada en Loja para gozar de los beneficios que estos poseen y así tener una banda ancha estable capaz de soportar el tráfico de la información que pasara por medio de la VPN implementada.
- Utilizar equipos con sistemas operativos superiores a Windows 8 por posibles problemas de compatibilidad.
- Aprovechar las características proporcionadas por Windows server.
- Arreglar problemas eléctricos para prevenir el daño de los equipos de la compañía.

- Se recomienda también que no se use el mismo cliente OpenVpn en diferentes dispositivos.

Referencias y Bibliografía

Referencias

Baena, G. (2014). *Metodologia de la investigacion.* Ciudad de Mexico: Patria.

Bastify. (1 de Febrero de 2019). *Bastify*. Obtenido de https://www.bastify.com/que-es-ssh-y-como-funciona/

Bravo, G. (16 de Septiembre de 2022). *Hostinger*. Obtenido de https://www.hostinger.es/tutoriales/que-es-dns

Carpentier, J. F. (2018). *La seguridad informatica en la PYME.* Barcelona: ENI.

Castillo, J. (15 de Diciembre de 2018). *Profesionalreview*. Obtenido de https://www.profesionalreview.com/2018/12/15/active-directory/

Chavez, C. A. (2019). La encriptación de datos empresariales: ventajas y desventajas. *Recimundo*, 1.

Colina, A., & Espinoza, M. (2021). Identificación de amenazas informáticas aplicando arquitecturas de Big Data. *INNOVA, 6*(3).

Dauti, B. (2022). *Administracion fundamenta en Windows server.* Birminham: PACKT.

Diaz, L. (2013). La entrevista, recurso flexible y dinámico. *Scielo*.

Diez, M. (2018). *MarthaMDiez*. Obtenido de http://www.marthamdiez.com/las-bases-de-datos-en-las-pymes/

Dominguez, R. (2020). Personalizacion de Windows Server 2016. Lima, Peru.

Dordoigne, J. (2015). *Redes Informarticas: Nociones fundamentales.* ENI.

Ezra, P. J. (2021). *Cyber Security and Digital Forensics.* New York: Springer.

Ghanem, K., & Ugwuanyi, S. (2022). Security vs Bandwidth: Performance Analysis between IPsec and OpenVPN in Smart Grid. Glasgow: Scopus.

Gutierrez, J., & Tena, J. (2013). *Protocolos criptograficos y seguridad de redes.* Editorial de la Universidad de Cantabria.

Harrington, W. (2015). *Learning Raspbian.* Birminham: PACKT.

Hernandez, R. (2018). *Metodologia de la investigacion.* Guadalajara: Mc Graw Hill.

Hubspot. (2019). *Hubspot*. Obtenido de https://blog.hubspot.es/marketing/acceso-remoto

IBM. (14 de abril de 2021). *IBM*. Obtenido de https://www.ibm.com/docs/es/i/7.3?topic=programs-file-server

Jones, J. (14 de septiembre de 2022). *Top10VPN*. Obtenido de https://www.top10vpn.com/es/que-es-una-vpn/como-funciona-una-vpn/

Kanich, C. (2018). An Empirical Analysis of the Commercial VPN Ecosystem. *ACM Digital Library*.

Katz, M. (2013). *Redes y seguridad.* Alfaomega.

Luz, S. d. (01 de Septiembre de 2022). *RedesZone*. Obtenido de https://www.redeszone.net/tutoriales/vpn/openvpn-instalacion-configuracion/

Martel, V. (2019). Diseño de una red de comunicación VPN sobre internet para un Distribuidor. Lima.

Martinez, C. (18 de Junio de 2020). *Likedin*. Obtenido de https://es.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez

Microsoft. (2022). Obtenido de https://www.microsoft.com/es-es/windows-server

NordVPN. (2022). *NORDVPN*. Obtenido de NORDVPN: https://nordvpn.com/es/what-is-a-vpn/

OpenVPN. (2022). *OpenVPN*. Obtenido de https://openvpn.net/

Pallo, J., & Reyes, E. (2015). RED PRIVADA VIRTUAL (VPN) PARA UN SISTEMA DE TELEMEDICINA. Ambato.

Penal, C. O. (10 de febrero de 2014). *Asamblea General del Estado*. Obtenido de https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Perez, D. M. (2020). *Administracion y seguridad en redes de computadoras.* Bogota, Colombia: Alfaomega.

Quishpe, L. (2021). ESTUDIO PARA LA IMPLEMENTACIÓN DE UNA RED PRIVADA. Quito.

Raspberry. (2022). *Raspberry Org*. Obtenido de https://www.raspberrypi.org/

Soto, J. (18 de Marzo de 2021). *Geeknetic*. Obtenido de https://www.geeknetic.es/Guia/1998/Como-usar-y-configurar-OpenVPN.html

Tanenbaum, A. (2012). *Redes de computadoras* (5ta edicion ed.). Mexico: Pearson.

Tanenbaum, A. (2012). *Redes de computadoras.* Pearson.

Valencia, A. (2020). *EVOLUCIÓN Y TENDENCIAS INVESTIGATIVAS EN INGENIERIAS.* Medellin: Sello Editorial Americana.

Vega, E. (2021). *Seguridad de la informacion* (Vol. 1). Medellin: Tres Ciencias.

VpnUnlimited. (2020). *VpnUnlimited*. Obtenido de https://www.vpnunlimited.com/es/help/vpn-protocols/l2tp-protocol

Ghanem, K., Ugwuanyi, S., Hansawangkit, J., McPherson, R., Khan, R., Irvine, J. Security vs Bandwidth: Performance Analysis between IPsec and OpenVPN in Smart Grid (2022) 2022 International Symposium on Networks, Computers and Communications, ISNCC 2022.

Soriano, M. (2014). Seguridad en redes y seguridad de la información. *Obtenido de http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf*.

ANEXOS

ANEXO No. 1

CARTA DE CUMPLIMIENTO DE PROPUESTA TECNOLÓGICA

Buildec
ARQUITECTURA Y CONSTRUCCIÓN

Guayaquil, 4 de octubre del 2022

Magíster
Erika Ascencio Jordán
Decana de la Facultad de Ingenierías
Universidad Tecnológica ECOTEC
Ciudad. -

De mis consideraciones:

A través del presente, comunico que el señor **RIVERA MORLA LUIS ALBERTO**, con cédula de ciudadanía **N° 1718345430**, por motivo del desarrollo de su trabajo de fin de grado en la Universidad ECOTEC, ha implementado un Sistema de Red Privada Virtual y un Servidor de archivos con Directorio Activo en nuestra oficina de Guayaquil, el cual se encuentra en funcionamiento y al servicio de la empresa.

Debo indicar que el recurso tecnológico desarrollado ha contribuido a que las tareas realizadas por el equipo de trabajo sean más eficientes en tiempo y calidad, además de proveer seguridad informática a la documentación que maneja la empresa; por consiguiente, nuestros requerimientos fueron atendidos en la propuesta presentada.

Como empresa apoyamos a la contribución de nuevos conocimientos en el ámbito tecnológico por parte de las nuevas generaciones de profesionales, que son en beneficio de la sociedad y del país.

Atentamente,

Firmado electrónicamente por:
RONALD ARMANDO TORRES ORTIZ

Arq. Ronald Torres Ortiz, MSc.
Presidente de BUILDERECUADOR CIA.LTDA.
Contacto: +593 994886802

J.A. Eguiguren 156-19 entre Sucre y Bolivar
Edificio R&C, Oficina Nro. 8 (Loja- Ecuador)

ANEXO No. 2

FOTOS DE LOS EQUIPOS UTILIZADOS EN LA PROPUESTA TECNOLÓGICA

Red LAN

Dispositivos que lo conforman

Raspberry Pi 4 Modelo B de 8gb Ram + kit completo

Switch Administrable L2 8 Pu Gigabit 2 Sfp Tl-sg3210

Switch Desktop TP LINK no administrable

DELL core i3/ 8gb ram / 320gb disco duro+120 disco duro solido

UPS APC 800VA

ANEXO No. 3

ENTREVISTA AL PRESIDENTE DE LA EMPRESA BUILDERECUADOR CIA. LTDA.

Tecnologías de la Información y Comunicación
Ingeniería en Sistemas con énfasis en Administración de Redes

ENTREVISTA AL PRESIDENTE DE LA EMPRESA BUILDERECUADOR CIA. LTDA.

1. **¿Cómo define a BUILDERECUADOR CIA. LTDA.?**

   BUILDERECUADOR CIA. LTDA. es una empresa constructora que se inició en el año 2021 y que cuenta con un staff de profesionales especializados y de amplia experiencia en las ramas del diseño arquitectónico y construcción. La empresa surgió de la necesidad de contribuir al desarrollo inmobiliario del Ecuador, con base en tres ejes: solidez, innovación y confianza.

2. **¿Qué servicios brinda la empresa?**

   La empresa se dedica al desarrollo de proyectos inmobiliarios, así como a la construcción y remodelación de obras civiles de carácter residencial y comercial. Ofrecemos nuestros servicios de acuerdo con las necesidades del cliente, además de asesorar en cada etapa del diseño con el fin de que el producto final sea a satisfacción del cliente.

   Así mismo, contamos con proveedores que brindan servicios y materiales con altos estándares de calidad, con el fin de que la marca de la empresa se posicione dentro del mercado de la construcción.

   La construcción sostenible es parte de la misión de BUILDERECUADOR CIA. LTDA., ser una empresa responsable con el medio ambiente. De manera que

nos encontramos ligados a la innovación tecnológica dentro de los proyectos de diseño como herramienta para la sostenibilidad y confort térmico.

3. **¿Cómo está constituida la empresa y dónde se encuentra ubicada?**

   Contamos con un equipo de trabajo dedicado a las tareas de: Diseño y construcción de proyectos, presupuesto y cronogramas de trabajos, equipo de modelamiento 3D, equipo legar e inmobiliario.

   Nuestras oficinas están ubicadas en la ciudad de Loja, en la calle J.A. Eguiguren 156-19 entre Sucre y Bolívar, Edificio R&C, Oficina 8; y en la ciudad de Guayaquil, en la Cdla. Bellavista, Mz. 25, villa 26. Además, se espera la apertura de oficinas en la provincial de El Oro.

4. **¿Cómo se realiza la transferencia / almacenamiento de datos dentro de la empresa?**

   Nosotros utilizamos los correos electrónicos corporativos para el envío y recepción de información de los proyectos; y en caso de que sea muy pesada la información utilizamos dispositivos externos como discos duros, memorias externas o por medio de aplicaciones basadas en la nube como WeTransfer.

   En el caso del almacenamiento de datos se lo realizamos dentro de las computadoras sean de escritorio o computadora portátil. También creamos una carpeta en Google Drive para compartir información de interés para el equipo de trabajo.

5. **¿Cómo mantiene protegido los sistemas informáticos de su empresa?**

   Cada una de las computadoras tiene antivirus que lo renovamos anualmente, además del firewall que incluyen en las computadoras.

6. **¿Cuáles son los dispositivos que forman la red de su empresa?**

   Las oficinas cuentan con una red WiFi inalámbrica emitida por un router. Además, contamos con un servicio de internet hogar de la compañía de TV Cable.

7. **¿Cree usted que la empresa necesita implementar mejoras en su manejo de transferencia / almacenamiento de datos?**

   En mi experiencia como arquitecto he comprobado que el tiempo juega un rol esencial en el trabajo; y su optimización depende de lo ágil y cómodo sea en la realización del fujo de trabajo. Por lo cual creo que es necesario que la empresa cuente con un sistema de transferencia / almacenamiento de información compartido entre las dos oficinas de Guayaquil y Loja como un medio de recopilación documental de cada proyecto que lleva a cabo la empresa.

   Es importante recalcar que la empresa maneja información gráfica, como archivos de formato .dwg, IFC, rtv .tif .skp .psp entre otros. Son archivos que ocupan gran capacidad de memoria y se complica un envió a través de plataformas de correo.

   Además, los equipos de Guayaquil y Loja trabajan en proyectos en común y necesitan una carpeta compartida donde se vaya ubicando y guardando los archivos generados. Con ellos nos permitirá tener un mejor control documental por cada obra realizada, con el fin de obtener un expediente digital organizado.

8. **¿Cuál es su visión de la empresa en un futuro?**

   BUILDERECUADOR CIA. LTDA. tiene como meta establecida el reconocimiento de su marca en el mercado de la construcción. Creo firmemente que el éxito la empresa está en su equipo de trabajo y en el sacrificio ligado a la dedicación nos permitirá contribuir al crecimiento de la constructora. Tenemos proyectos en procesos y otros que esperamos iniciar el próximo año, por lo que la empresa necesitará contratar más personal de apoyo para su ejecución y contar con un mejor flujo de trabajo y comunicación.