UNIVERSIDAD NACIONAL DE CAJAMARCA
FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL
DE INGENIERÍA DE SISTEMAS

"IMPACTO DE LA IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL EN LA GESTIÓN DE INFORMACIÓN DE LA EMPRESA DEYFOR E.I.R.L."

INFORME DE TESIS:
PARA OBTENER EL TÍTULO DE INGENIERO DE SISTEMAS

AUTOR:
Bach. Araceli Yoselín Cueva Mendoza

ASESOR:
MANUEL ENRIQUE MALPICA RODRÍGUEZ
Ingeniero de Sistemas

CAJAMARCA-PERÚ
Marzo 2018

AGRADECIMIENTO

En primer lugar, dar las gracias infinitas a Dios; por haberme dado la fuerza necesaria para culminar este proyecto tan importante de mi vida.

Agradezco también el apoyo y confianza brindados por mis padres Ofelia y Elmer; que; a pesar de las circunstancias adversas, me han demostrado su amor y cariño al haber corregido mis faltas y celebrado mis triunfos, y al encaminarme en este proyecto que significa la culminación de mi etapa universitaria.

A mis hermanos Mary, César y Kely que han sido una fuente de inspiración y apoyo constante para sobrellevar los obstáculos.

A mis amigos incondicionales Americo Cueva Bernal y Eugenia Villanueva Villena, por su ayuda desinteresada, los cuales hicieron posible esta presentación.

Agradecer al ingeniero Manuel Malpica Rodríguez por la asesoría, la guía, la colaboración y sobre todo la amistad brindada a mi persona; que, con los consejos, el apoyo intelectual, académico; me encaminó e hizo posible la culminación de este proyecto.

DEDICATORIA

A Dios, por permitirme llegar a este momento tan importante de mi vida. Por los triunfos y los momentos difíciles que me han enseñado a tenerlo presente cada día de mi vida.

A mis padres, por ser el principal impulso para lograr cerrar esta universitaria y encaminarme en mi vida profesional, al haberme acompañado y orientado en todo momento.

A mis hermanos y amigos, que han sido un gran aliciente para poder sobrellevar este proceso.

Al ingeniero Manuel Malpica, por mostrarme el camino a seguir para la realización de la presente tesis.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

El presente proyecto de investigación se enrumba tras el objetivo de determinar el impacto de implementación de una VPN sobre la gestión de información en la empresa Deyfor E.I.R.L. Tras haber realizado un estudio detallado y consciente de la forma en que se gestiona la información dentro de ésta, se encuentra evidencia de la innegable necesidad de implementar una VPN para gestionar la información, puesto que, actualmente se manejan elevados volúmenes de información tanto dentro como fuera de la organización y ha superado el tamaño de archivos aceptados en el servidor de correos con los que cuenta la organización y viene siendo manejada través de aplicaciones gratuitas y externas como Wetransfer y/o Google Drive que, por ende, no garantiza integridad y seguridad en los accesos a la información.

Como medida inmediata para dar solución a los problemas encontrados en el estudio situacional previo, se plantea la implementación de una Red Privada Virtual en la organización con la finalidad que facilite y simplifique el acceso, transmisión y gestión de la información. Como primer paso después de que la solución planteada es aceptada por parte de la alta gerencia, se recogen muestras de los tiempos que tardan las ejecuciones de los procesos y/o actividades relacionadas al manejo de información antes de implementar la VPN, lo que constituye los datos de pre prueba y, que servirá para comparar con los tiempos tomados después de que la VPN se ha implementado. Posteriormente, se realiza la implementación de la VPN como tal, y, debido a que no existe una metodología mundialmente aceptada para implementar VPN, se siguen una serie de pasos que usan la mayoría especialistas en el tema. Como medida inicial se forma el equipo de trabajo, luego se fija el alcance del proyecto para después realizar el estudio y análisis de la solución, se elige la plataforma de implementación, se proponen un conjunto de soluciones, se establecen las consideraciones de seguridad, se crean los planes de contingencia, se estiman los costos de implementación, se realiza la implementación de la VPN (instalación y configuraciones), se establecen planes de mantenimiento y, finalmente se realizan las mediciones para determinar el impacto positivo o negativo de la implementación de la VPN.

Al culminar esta investigación se concluye que la implementación de una VPN impacta de manera positiva sobre la gestión de información en la empresa Deyfor E.I.R.L.

Palabras clave: Red, Red Privada Virtual, Seguridad, Gestión, Gateway, Router

ABSTRACT

This research project is based on the objective of determining the impact of implementing a VPN on information management in the Deyfor E.I.R.L company. After having made a detailed and conscious study of the way in which information is managed within Deyfor, there is evidence of the undeniable need to implement a VPN to manage the information, since currently high volumes of information are handled both inside and outside of the organization and has exceeded the size of accepted files on the mail server that the organization has and has been managed through free and external applications such as WeTransfer and/or Google Drive, which, therefore, does not guarantee integrity and security in information.

As an immediate measure to solve the problems found in the previous situational study, the implementation of a Virtual Private Network within the facilities of the organization is proposed in order to facilitate the access, transmission, and management of the information. As a first step after the proposed solution is accepted by top management, samples are collected of the times that the executions of the processes and/or activities related to the handling of information take before implementing the VPN, which constitutes the Pre-test data, which will be used to compare with the times taken after the VPN has been implemented. Subsequently, the implementation of the VPN is performed as such, and, because there is no globally accepted methodology for implementing VPN, a series of steps are followed that are used by most people who specialize in the subject. As an initial measure, the work team is formed, then the scope of the project is set to the study and analyze the solution, the implementation platform is chosen, a set of solutions are proposed, security considerations are established, create the contingency plans, estimate the implementation costs, implement the VPN (installation and configurations), establish maintenance plans and, finally, perform the measurements to determine the positive or negative impact of the implementation of the VPN.

At the end of this investigation, it is concluded that the implementation of a VPN positively impacts on the information management in the Deyfor E.I.R.L. Company.

Keywords: Network, Virtual Private Network, Security, Management, Gateway, Router

CAPÍTULO I. INTRODUCCIÓN

En las últimas décadas, la información se ha convertido en el activo con mayor importancia dentro de las organizaciones, principalmente para aquellas que manejan grandes cantidades de información, sucursales, clientes y socios que están distribuidos en diferentes ciudades y países. Esto trae consigo altos costos, y diversos problemas en torno a la conexión de usuarios para la realización de sus labores; así como el acceso fuera de tiempo a la información, además de correr el riesgo de que la información sea alterada o modificada de manera indebida [1]. Asimismo, las organizaciones requieren establecer una comunicación efectiva a sus redes locales, de tal manera que ésta sea eficiente y productiva entre los elementos que la componen para lograr buenas interacciones dentro y fuera de su negocio; reduciendo costos, ofreciendo un mejor servicio tanto a los usuarios locales como externos, buscar e implementar nuevas formas de trabajo y tener información más oportuna, rápida y acertada [2].

La existencia de infinitas fuentes de información, obligan a las organizaciones a sistematizarla de tal forma que se garantice su coherencia y contribución al logro de los objetivos a corto, mediano y largo plazo. En medio de este contexto surgen riesgos potenciales inherentes a un mundo globalizado tales como el acceso no autorizado a información que es de vital importancia para la organización, fuga de datos hacia organizaciones establecidas como competencia directa, mala gestión del conocimiento que posee el recurso humano, etc. Todos estos riesgos obligan a la alta gerencia organizativa a la adquisición de medidas que mengüen al máximo estos riesgos al nivel de ser casi imperceptibles [3].

Esta tesis tiene como foco de ejecución la empresa Deyfor E.I.R.L. ubicada en la ciudad de Cajamarca, Perú; Deyfor cuenta con varios puntos de trabajo establecidos en Minera Yanacocha S.R.L. y otros dentro y fuera del departamento de Cajamarca, además de manejar una gran cantidad de información distribuida de manera desorganizada, transferencia insegura de la información, vulnerabilidad de la integridad; debido a esto surge la necesidad de dar respuesta a la interrogante ¿cuál es el impacto de la implementación de una red privada virtual para gestión de información?; asimismo, persigue el objetivo primordial que es evaluar el impacto de la implementación de una red privada virtual para gestión de información y, por otro lado se busca fijar el alcance que va a tener la VPN, estudiar y analizar los requisitos de implementación, elegir plataformas que se utilizarán en la implementación, establecer un diseño para la VPN, establecer la Política de seguridad de la VPN; un cifrado de datos, para no permitir

intrusiones y garantizar la entrega de información solo a usuarios correctamente autentificados, implementar la red VPN, entre otros; finalmente se pretende demostrar la hipótesis general de que la implementación de una red privada virtual mejorará la gestión de información de la empresa Deyfor E.I.R.L.

La ejecución de este proyecto de tesis, responde de manera directa al sentido de urgencia que presenta la empresa Deyfor E.I.R.L de contar con una herramienta y/o solución con la capacidad suficiente para gestionar de manera correcta y eficaz el manejo de su información; asimismo, pretende satisfacer la necesidad de que todos sus equipos estén conectados, puedan tener acceso a la información en tiempo real y de manera continua (varios usuarios a la vez puedan utilizar un mismo recurso de información); disminuyendo errores en la presentación de la información y logrando integrar la misma. Por otro lado, el trabajo contenido en este documento, puede en ser tomado como punto de partida, para la elaboración de otros proyectos futuros; una vez que este sea terminado y validado directamente, ya que se presentará los pasos y secuencias que se seguirán para la implementación de una red privada virtual. Una vez concluido el proyecto, el proceso de la gestión de información en la empresa mejorará en cuanto a orden y manejo de la misma.

La principal motivación del uso y difusión de la VPN Red Virtual Privada en Deyfor E.I.R.L. es la reducción de costos directos en implementación de canales privados como en hardware y servicios de telecomunicaciones sin importar la ubicación de sus oficinas. Cada usuario remoto puede comunicarse de manera segura y confiable utilizando internet para conectarse a la red privada local. Las VPNs pueden adaptarse a más usuarios y en diferentes lugares gracias al nivel de escalabilidad con el que cuentan. Otras ventajas de esta tecnología para la empresa Deyfor E.I.R.L. son la reducción de tiempos y costos de transporte para los usuarios remotos, mejora de la productividad de la empresa, simplificación de la topología empresarial, proveer a los usuarios remotos facilidades de telecomunicaciones, permitir un mejor uso de las redes con un buen ancho de banda y la posibilidad de encontrar oportunidades de negocio a nivel global. También se garantiza que los supervisores puedan tener acceso a los sistemas informáticos empresariales desde cualquier punto donde se encuentren, para que se pueda facilitar la salida de estas herramientas y/o materiales con más rapidez de almacén y la respectiva utilización en los puntos de trabajo.

Al culminar la ejecución de la tesis, se habrá fijado una IP pública para la red de Deyfor E.I.R.L., se habrá instalado un sistema operativo de red que permita el despliegue de un dominio de red. Asimismo, se habrá creado Unidades Organizativas con sus

respectivos usuarios debidamente diferenciados en cuanto a permisos y restricciones dentro de la red. Por otro lado, se garantizará la entrega de información solo a usuarios correctamente autentificados, se asegurará la integridad de los datos evitando que puedan ser alterados en algún punto del recorrido sin que el receptor lo detecte, se establecerá una correcta emisión de Información para que si sufre transformación de cualquier tipo se pueda rastrear el origen de estas modificaciones. Finalmente, se establecerá mecanismos para que la información se maneje de manera clara, puntual y en tiempo real; los usuarios podrán acceder al sistema Odoo implementado en servidor a través de cualquier dispositivo tanto móvil como pc de escritorio y/o laptop, con solo acceder a red privada virtual y contando como una dirección IP, y, lo más importante, no se permitirá el acceso a la red VPN de usuarios no autorizados.

El presente trabajo de tesis consta de cinco capítulos debida y cuidadosamente diferenciados: en el capítulo I se encuentra la sección que define la parte introductoria al proyecto y, es en este apartado, donde se puede encontrar el problema, los objetivos, la justificación e hipótesis planteados; en el capítulo II se referencian un conjunto de investigaciones que sirven como punto de partida para la presente investigación y ayudan a justificar su ejecución, además se conceptualiza de manera clara las bases teóricas que respaldan y sientan las bases para el proyecto, también se puede encontrar la definición de términos básicos que ayudarán a entender la terminología utilizada; en el capítulo 3 se detallan los materiales y métodos utilizados para el desarrollo del proyecto, cabe mencionar que se realiza una breve descripción y situación actual de la empresa dentro de la cual se ejecuta la investigación, además, es en este capítulo donde se detalla el desarrollo e implementación de la red privada virtual; en el capítulo IV se encuentra el análisis y discusión de los resultados obtenidos mediante la ejecución de pruebas que sirven para realizar la contrastación de hipótesis y determinar si lo que se ha implementado cumple debidamente con las expectativas del cliente; finalmente, en el capítulo V se encuentran las conclusiones a las que se llegó al finalizar la ejecución del presente proyecto de tesis, además de un conjunto de recomendaciones que servirán como punto de partida para trabajos futuros o mejoras que se puedan hacer al software implementado. En el apartado final se pueden encontrar los anexos que ayudan al correcto desarrollo del proyecto.

CAPÍTULO II. MARCO TEÓRICO

2.1 ANTECEDENTES TEÓRICOS

2.1.1 Antecedentes internacionales

Hostos y Zambrano [4], en su tesis “Diseño de una Topología de Red VPN y VoIP para la Universidad Católica Andrés Bello”, buscaban modernizar los servicios de telecomunicaciones de la Universidad Católica Andrés Bello, y brindar una solución que genere ahorro, para lo cual implementaron una topología de red VPN y VoIP en donde integran por medio de dispositivos Gateways FXO y Firewalls en las sedes de la universidad. Hicieron un análisis de la situación en la que se encontraba la red para luego establecer el diseño de la red VPN; con el fin de ofrecer seguridad en las comunicaciones por medio de protocolos de encriptamiento y llaves compartidas, servicio de antivirus, anti-spam, anti-hacker, etc. Este documento es importante puesto que ayudará para ver impacto del proyecto al ofrecer una solución integral y convergente, sobre la situación de los procesos de la universidad antes de la implementación de la red privada virtual, además de evaluar la seguridad de esta red mediante el uso de firewalls.

Rodríguez y Gonzáles [5], en su tesis “Diseño y construcción de una Red Privada Virtual (VPN) para la Universidad Tecnológica de Bolívar”, plantean una solución para compartir información y proteger los datos; creando intercambio de ideas, para que puedan ser fácilmente capturas y transformadas a través de internet; manteniendo la información a salvo de intrusiones. El desarrollo de este trabajo de investigación les permitió profundizar en conocimientos y experimentar físicamente con las Redes Privadas Virtuales (VPN), principalmente con las implementaciones en el sistema operativo Windows. Esta tesis se considera importante ya que implementa una red privada virtual funcional para un entorno Windows, con la cual se va a comparar este trabajo.

Paillier y Arzuaga [6], en su trabajo “Guía Práctica sobre Redes Privadas Virtuales Virtual Private Network (VPN)” manifiestan que la integración de los servicios en las empresas hacen evidente una búsqueda de nuevas formas para mantener la comunicación constante entre cada uno de los miembros de su organización, proveedores y clientes, estas necesidades de comunicación son suplidas satisfactoriamente por la implementación de la tecnología VPN, esta, permite hacer extensión de la red privada corporativa mediante el uso de técnicas criptográficas a

más bajo costo ya que utiliza un medio público (Internet) como estructura física. Este trabajo ayuda a entender cuáles son los pasos a seguir, cuando se pretende apoyar a las empresas a implementar soluciones integrales como redes privadas virtuales para la gestión de información, y el apoyo en la toma de decisiones organizacionales.

Trujillo [7] en su tesis “Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPSEC”, diseña alternativas de implementación VPN en una empresa comercializadora y construye un prototipo demostrativo; logra evidenciar que una VPN de acceso remoto es la herramienta ideal para las personas que viajan constantemente o que se conectan desde su hogar hacia la oficina central, tienen mayores facilidades y esto aumenta la productividad de los empleados ya que pueden acceder a la red desde cualquier punto en el que estén. Esta tesis muestra a las redes privadas virtuales como una solución total y confiable para integrar a la empresa comercializadora con sus sucursales, tal como se quiere hacer en el presente trabajo.

Limari [8], en su tesis “Protocolos de Seguridad para Redes Privadas Virtuales (VPN)”, analiza las diferentes formas que hacen posible crear túneles a través de estos medios considerados como poco seguro para quien necesite que sus datos no sean dañados, leídos o tergiversados; estudia tanto los modelos como la estructura que adopta la información al momento de considerarse listo para viajar por un medio inseguro, hace un énfasis en el protocolo de seguridad sobre IP llamado IPSec, el cual reúne la mayoría de las características que hacen que un modelo sea seguro sobre un medio masivo como lo es la Internet. Esta investigación se tomará como base para evaluar las diferentes formas de implementación de una red privada virtual.

Peña [9], es su trabajo especial de grado “Diseño e Implementación de una Red Privada Virtual (VPN-SSL) Utilizando el Método de Autentificación LDAP en una empresa privada”, tuvo como propósito diseñar e implementar una Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada, con el objetivo de proteger las conexiones de acceso remoto hacia la organización a través del contenido cifrado, garantizando la integridad, confidencialidad y seguridad de los datos. Este trabajo documenta aspectos teóricos de una VPN, seguridad y protocolos que se utilizan actualmente para las conexiones seguras de acceso remoto en la implementación de una red privada virtual, los mismos que se tendrá en consideración para el desarrollo de la presente tesis.

2.1.2 Antecedentes nacionales

Alva [10], en su tesis “Desarrollo e Implementación de una herramienta gráfica para la configuración remota de una VPN con routers CISCO” plantea el uso de la tecnología como las redes privadas virtuales, para mantener un orden y comunicación entre locales, y así mantener su crecimiento de las pymes que están en plena expansión, y se basa en esto para plantear el principal objetivo que se quiere alcanzar con el desarrollo de su tesis. Usa la red privada virtual implementada para facilitar a los usuarios el uso de una herramienta que cuenta con interfaz gráfica amigable, logrando reducir tiempos y así invertir el tiempo ahorrado en otras tareas críticas. Este autor recomienda tener mucho énfasis en las etapas de análisis y diseño para evitar tener que realizar grandes cambios en la etapa de desarrollo; lo que implica, un gran costo mayor al que hubiera costado corregirlo en la etapa de análisis y diseño; lo que se debe tener en cuenta para el desarrollo de la presente tesis.

Díaz y Vieyra [11], en su tesis “Diseño de una Red Privada Virtual para Interconectar las sucursales de la empresa Terracargo SAC” explican cómo se realiza el mejoramiento de la interconexión entre las sucursales de la empresa Terracargo SAC, la cual cuenta con sucursales en distintas ciudades del Perú. Esta mejora se realizó a través de la implementación de una VPN, permitiendo la intercomunicación en tiempo real entré las sucursales, de manera eficiente y segura. Esta tesis presenta todo el proceso detallado de la implementación de una red privada virtual en un entorno Windows; sirviendo como punto de partida inequívoca para la realización de esta tesis, ya que se trabajó en entornos con gran similitud.

Amenero [12], en su tesis “Implementación de una red Privada Virtual (VPN) bajo software libre para optimizar el manejo de información entre los locales de la corporación educativa ADEU, de la ciudad de Chiclayo” buscó la optimización del acceso a la información entre los locales de la Corporación Educativa ADEU, ubicada en Chiclayo; a través de la implementación de una VPN, bajo software libre, nos explica que se utiliza este tipo de software ya que no incurre en gastos económicos excesivos y constituye un canal de comunicación seguro. Esta tesis presenta el proceso de la implementación de una red privada virtual en un entorno de software libre, la cual servirá para hacer comparaciones con la presente tesis.

2.2 BASES TEÓRICAS

2.2.1 Gestión de información

2.2.1.1 *Definición*

Ponjuan [13] considera a la gestión de la información como una triple hélice. En primer lugar considera que, lo importante de la información es su contenido y no tanto su soporte, en segundo lugar, considera que los gastos para sistemas y tecnologías de la información son un gasto para recursos y no deben ser considerados como gastos generales de funcionamiento, y la tercera parte de la filosofía de la gestión de la información es la exacta coordinación del recurso dentro de la propia organización, ya que en la actualidad este recurso está muy disperso en diversas empresas.

2.2.1.2 *Elementos de la gestión de información*

Los elementos involucrados con la gestión de información, tal cómo se muestra en la figura 1 [13] son:

- Los que competen a la información como fuente/recurso (procesos productivos al interior de las organizaciones)
- Los relacionados con el usuario de productos y servicios de información
- Los que conforman el canal de comunicación entre el usuario y la fuente.

Fig. 1: Elementos de la gestión de información

2.2.1.3 *Funciones de los gestores de Información*

Los gestores de información tienen funciones que cumplir, dentro y fuera de la institución en la que se ejecutan. Estas funciones se describen a continuación: [14]:

- Posicionar el rol del profesional como gestor de información, consolidando políticas organizacionales internas coherentes, eficientes y eficaces.
- Gestionar la eficaz adquisición, tratamiento, almacenamiento y difusión de información dentro de la organización y en relación con su entorno.
- Proponer tecnologías adecuadas para el tratamiento de la información.
- Armonizar los requerimientos de los distintos usuarios
- Coordinar y supervisar el funcionamiento de los recursos informáticos.
- Evaluar los productos y servicios de información utilizados por la organización.

2.2.1.4 *Dimensiones de los sistemas de información*

Las dimensiones de los sistemas de información, tal y como se aprecia en la Figura 2 [15], son los siguientes [13]:

2.2.1.4.1 Organizaciones

Las organizaciones tienen una estructura compuesta de diferentes niveles y especialidades. Los sistemas de información son un elemento de la organización misma, se acoplan a la estructura de la organización, reflejan y reproducen las mismas líneas de comunicación, así como los niveles y divisiones del trabajo dentro de la organización.

2.2.1.4.2 Personas (administración)

Una organización es tan buena como las personas que la conforman y trabajan dentro de ella; las personas son el recurso más importante de cualquier organización, ya que estas son las que fabrican y producen la sinergia que finalmente se convertirá en utilidades para la empresa.

2.2.1.4.3 Tecnología

La tecnología está compuesta por todos los recursos de hardware, software, redes y telecomunicaciones que la empresa implementa para soportar la comunicación y producción de la información, Figura 2 [15].

Fig. 2: Dimensiones de los Sistemas de Información

2.2.1.5 *Rendimiento y acceso a la información*

El rendimiento proporciona información no solo sobre los ingresos que se obtienen, sino también de lo que les afecta. Incluye gráficos para que pueda ver las tendencias y comparar las métricas más fácilmente. También ofrece muchas formas de segmentar las estadísticas [14].

El acceso a la información se refiere al conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema: bases de datos, bibliotecas, archivos, Internet. Así mismo, el acceso a la Información involucra a muchos otros temas, como los derechos de autor, el Código abierto, la privacidad y la seguridad.

2.2.2 Redes de computadoras

2.2.2.1 *Definición de redes de computadoras*

Una red de computadoras es un grupo de computadoras interconectadas entre sí las cuales comparten información y recursos. La interconexión se puede realizar de diferentes maneras, ya sea cable de cobre, fibra óptica, rayos infrarrojos o microondas. Los recursos y la información que se pueden compartir pueden ser: archivos, aplicaciones correo electrónico e impresoras, etc. [16].

2.2.2.2 *Clasificación de redes de computadoras*

El mundo de las redes de computadoras es muy complejo, por lo que es necesario clasificarlas para facilitar su estudio, ya que existen muchos tipos de redes. Las redes pueden ser clasificadas en cuanto a cobertura, topología y propiedad [16].

2.2.2.2.1 Cobertura

La clasificación de las redes en cuanto a cobertura se refiere a la extensión que tiene una red dentro de un área geográfica. Utilizando este criterio, las redes de computadoras se pueden clasificar de la siguiente manera:

Red de Área Local (LAN): Es aquella red donde todas las computadoras conectadas en red están dentro de una habitación, un edificio e incluso varios edificios dentro de una localidad pequeña. Las LAN realizan lo siguiente:

- Operan dentro de una zona geográfica limitada.
- Permiten a los usuarios acceder a medios de gran ancho de banda.
- Proporcionan conectividad de tiempo completo a los servicios locales.
- Conectan físicamente dispositivos adyacentes.

Las principales tecnologías LAN son las siguientes:

- Ethernet
- Token Ring[1]
- FDDI

Siendo Ethernet la más popular y más difundida de todas ellas. Una LAN puede intercomunicarse por medio de un cableado que transmita señales punto a punto; o bien, por medio de una zona de influencia de un punto de acceso (access point) inalámbrico. La velocidad que se puede alcanzar en este tipo de red abarca desde los 10 Mbps hasta los 10 Gbps y se están desarrollando normas para 40 Gbps, 100 Gbps y 160 Gbps.

Red de Área Amplia (WAN): Es aquella red que está formada por la interconexión de varias LAN (vea la figura 3 [17] para un mejor entendimiento). Una WAN abarca una gran área geográfica de varios kilómetros.

Las WAN realizan lo siguiente:

- Operan sobre grandes áreas geográficamente separadas
- Permiten que los usuarios mantengan comunicación en tiempo real con otros

[1] Una red de anillo token (token ring) es una red de área local (LAN) en la que todos los ordenadores están conectados en una topología de anillo o estrella y pasan uno o más tokens lógicos de host a host

- Proporcionan acceso a los recursos remotos de una LAN
- Ofrecen servicios de correo electrónico, web, transferencia de archivos y comercio electrónico, figura 3 [17].

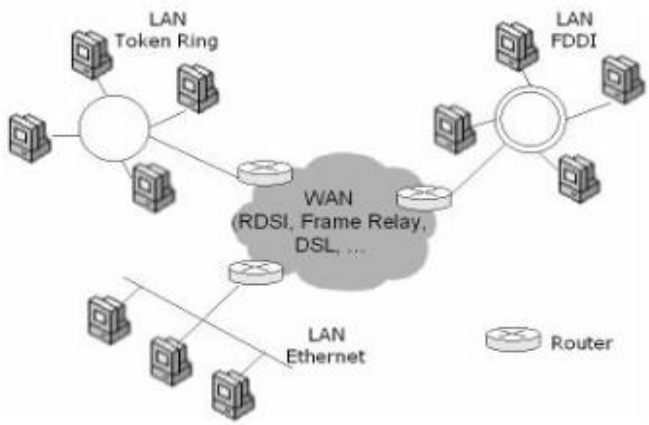


Fig. 3: Redes LAN y WAN

2.2.2.2.2 Topología

En cuanto a la topología, existen básicamente cuatro tipos de redes de las cuales se desprenden varias combinaciones. Estas topologías son:

Red tipo bus

En esta topología se utiliza un cable o serie de cables como eje central al cual se conectan todas las computadoras (vea la figura 4 [18]). En este conductor se efectúan todas las comunicaciones entre las computadoras. Esta red conviene usarse si no son muchas las computadoras que se van a conectar.

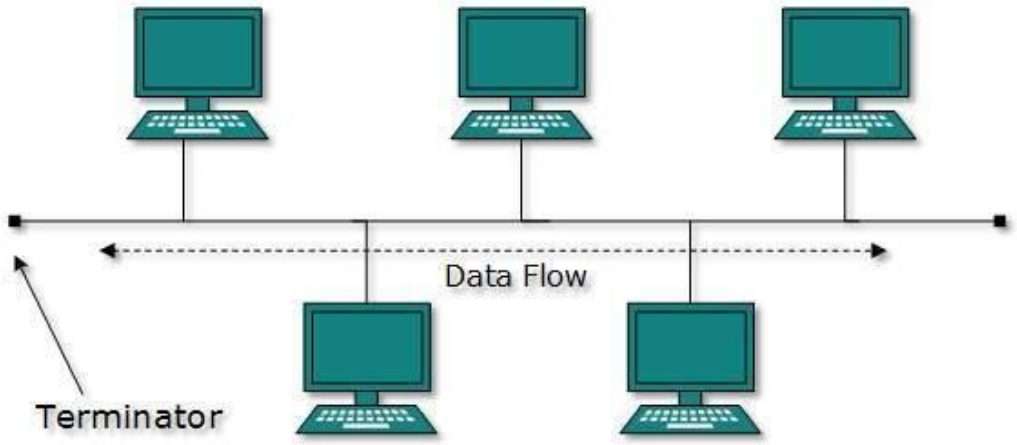


Fig. 4: Topología de red bus

Red tipo estrella

Se caracteriza por tener un núcleo del cual se desprenden líneas guiadas a varios terminales (vea la figura 5 [19]). Fueron las primeras en utilizarse en el mundo de la computación. Esta topología es útil cuando se tiene una computadora central muy potente rodeada de máquinas de menor potencia. Esta topología es la más común porque es la que más utilizan las redes Ethernet.

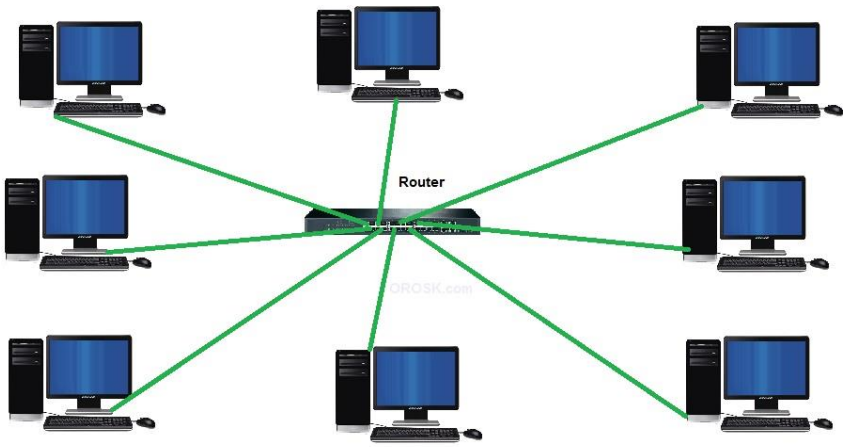


Fig. 5: Topología de red estrella

Red tipo anillo

Aquí también se utiliza un bus como eje central para conectar todos los equipos, sin embargo, como se puede apreciar en la figura 6 [20], dicho bus forma un anillo. Esta topología es utilizada en redes Token Ring y FDDI[2] además de que es favorecida por los principales proveedores de acceso a Internet.

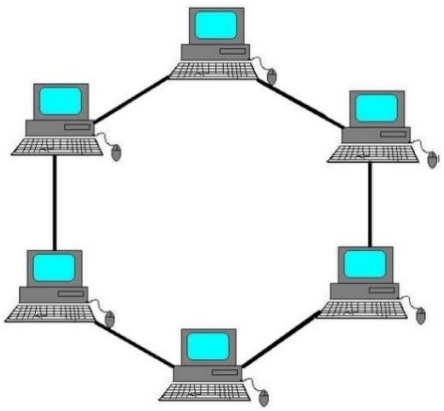


Fig. 6: Topología de red anillo

[2] FDDI (Fiber Distributed Data Interface) es un conjunto de estándares ANSI e ISO para la transmisión de datos en lineas de fibra óptica en redes de área local (LAN) que se pueden extender hasta un radio de unos 200km.

Red tipo malla

En esta topología, como se muestra en la figura 7 [21], todos los dispositivos o algunos de ellos son conectados con todos los demás con el fin de conseguir redundancia y tolerancia a fallos. Si un enlace falla, la información puede fluir por otro enlace. Las redes de malla suelen implementarse solamente en redes WAN.

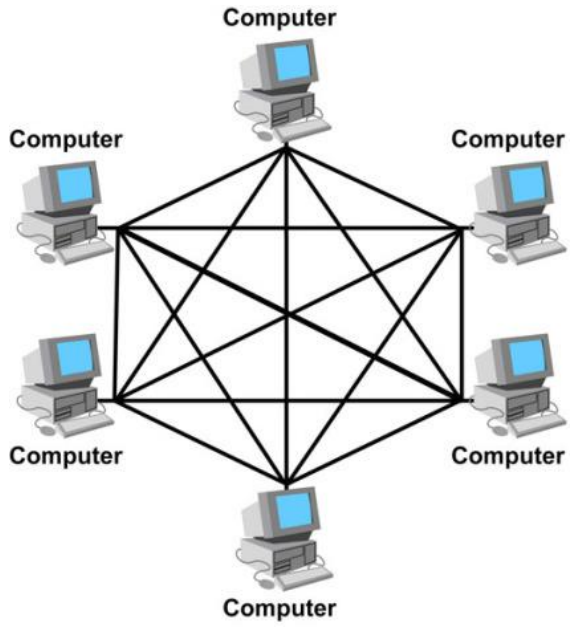


Fig. 7: Topología de red malla

Red tipo híbrida

La topología híbrida es una red que utiliza combinaciones de las topologías anteriores (vea la figura 8 [22]).

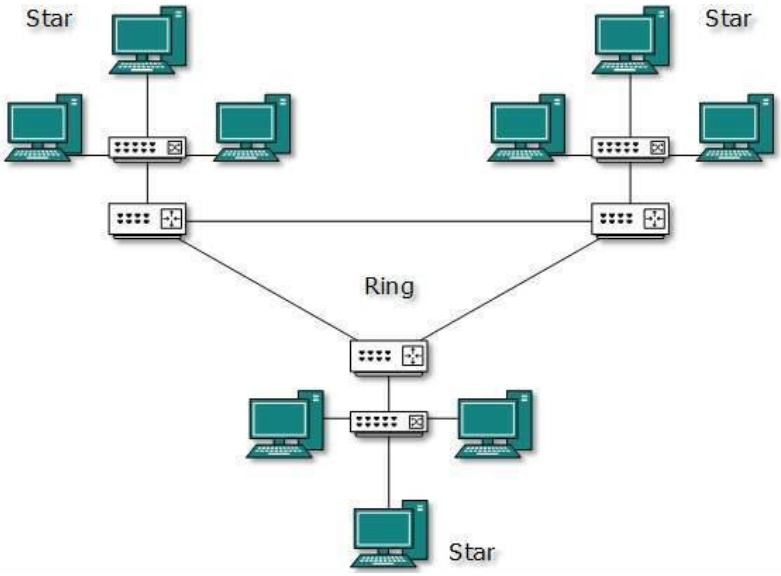


Fig. 8: Topología de red híbrida

2.2.2.2.3 Propiedad

La clasificación de las redes en cuanto a propiedad se refiere a la forma de administración de la red. Así pues, las redes de computadoras se pueden clasificar de la siguiente forma (vea figura 9 [16]):

Red privada

Es aquella red exclusiva de una sola compañía u organización en particular. La información no se comparte con otras compañías u organizaciones. En una red privada la información estará protegida, se puede tomar el control acerca del uso que se le da a la red y se podrá predecir el ancho de banda disponible.

Red pública

Es una red a través de la cual circula información de muchas compañías y organizaciones. Una red pública siempre será menos segura que una red privada, pero resultan ser más económicas y no se requiere que un administrador de red local de mantenimiento a una de estas redes. Como ejemplo de red pública tenemos a Internet. Para una mejor comprensión de estas consideraciones vea la siguiente figura:

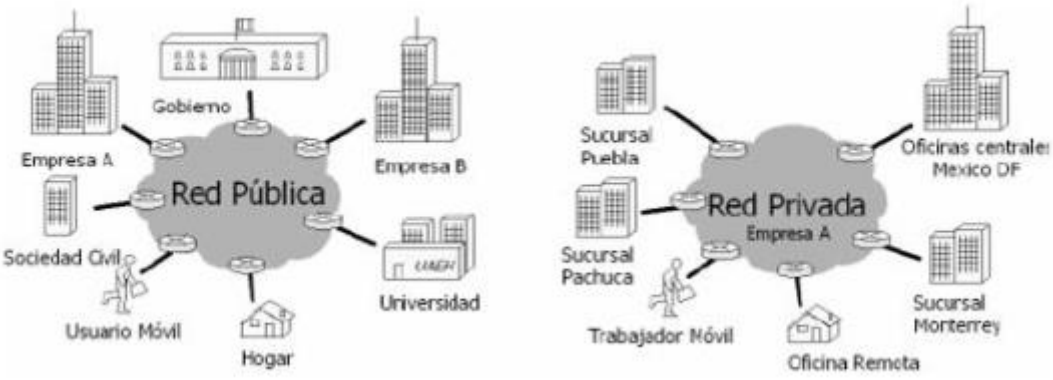


Fig. 9: Red pública y red privada

2.2.2.3 *Conexiones WAN y acceso remoto*

2.2.2.3.1 Internet, Intranet y Extranet

Internet, intranet y extranet son conceptos muy importantes en el mundo de las VPN y no puede hablarse de una VPN sin antes conocer en qué consisten dichos conceptos.

2.2.2.3.1.1 Internet

Internet conecta decenas de millones de computadoras en todo el mundo, permitiéndoles comunicarse entre sí y compartir recursos. Internet es una colección de redes organizada en una estructura multinivel las cuales usan toda una variedad de tecnologías para interconectarse. En el nivel más bajo se encuentra algunas decenas o cientos de computadoras conectadas a un router, formando una LAN.

La base de Internet es TCP/IP. El éxito de las redes basadas en IP se debe precisamente a Internet. Dos conceptos definen la tecnología de Internet: los paquetes y la forma de direccionamiento.

A. Paquetes

Internet transporta toda la información en unidades llamadas paquetes. Un paquete consta de dos partes: la información que contiene, la cual se llama carga útil y la información acerca de la información, llamada cabecera. La cabecera contiene información acerca de las direcciones origen y destino, longitud de los datos y tipo de éstos.

B. Direccionamiento

Las direcciones de la cabecera permiten el envío de la información a través de Internet. Los routers se encargan de realizar esto. Los paquetes recorren diferentes caminos para llegar a su destino y eventualmente pueden ser almacenados dentro del router.

Intranet

Una intranet es una Internet orientada a una organización en particular. Los servidores web intranet difieren de los servidores web públicos en que estos últimos no tienen acceso a la intranet de la empresa sin los permisos y las contraseñas adecuadas. Una intranet está diseñada para que accedan a ellas sólo los usuarios con los debidos permisos de acceso a una red interna de una empresa. Una intranet reside dentro de un firewall y éste impide el acceso a los usuarios no autorizados.

Extranet

Una extranet es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se le permite

el acceso a este contenido adicional, siempre bajo un sistema de autenticación y control de acceso.

La diferencia entre una intranet y una extranet es el método de acceso, siendo similares en cuanto a las facilidades y funciones, el tipo de recurso que utiliza y su filosofía general, de proporcionar acceso fácil, rápido y seguro a la información requerida.

El concepto extranet nace cuando una empresa quiere dar acceso a unas determinadas personas o grupos de personas a una determinada información de su intranet. Sin hacerla pública, la hace accesible a otras personas que puedan necesitarla o con quien mantienen relaciones comerciales. El ejemplo más claro es la accesibilidad que una empresa da a una parte de sus clientes o proveedores.

2.2.2.3.2 Acceso remoto

La necesidad del acceso remoto ha sido la causa principal del auge de las redes privadas virtuales, por lo que es preciso analizarlo un poco antes de verlo desde el punto de vista de las VPN.

2.2.2.3.2.1 Necesidades de acceso remoto

Con el incremento de las relaciones comerciales a nivel internacional, la movilidad geográfica de puestos de trabajo está llevando a las redes privadas a una situación bastante complicada. Los usuarios precisan conexiones que les permitan el acceso a las corporaciones desde cualquier lugar del mundo. Estas necesidades, unidas a las surgidas como consecuencia de la demanda de telecomunicaciones a tiempo completo, están aumentando drásticamente el número de oficinas remotas que una compañía debe interconectar. Como resultado, muchas redes privadas están convirtiéndose en redes muy complicadas de administrar.

Existen diferentes tipos de usuarios dependiendo de las necesidades de una organización y esto hará que las soluciones de acceso remoto también varíen de acuerdo a dichas necesidades. Los usuarios pueden ser clasificados de la siguiente forma:

- **Usuarios móviles**

Son aquellos que necesitan realizar viajes de trabajo a otro estado o país. Estos usuarios requieren de acceder a los recursos de la red de la oficina principal tales como su correo electrónico o sus archivos desde esa ubicación distante. Si el usuario viaja a

otro país, entonces tiene que lidiar con diferentes sistemas telefónicos y compañías de telecomunicaciones, complicando la conexión a la red corporativa.

- ***Usuarios de oficina remota***

Son aquellos que acceden a la red corporativa desde una ubicación fija distante como puede ser una pequeña oficina o el hogar.

El teletrabajo es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional en el domicilio del trabajador. Engloba una amplia gama de actividades, e implica el uso de computadoras y la conexión permanente entre el trabajador y la empresa. El usuario que trabaja desde su casa tiene su computadora conectada a la red privada y desde ahí tienen acceso al correo electrónico o algunas aplicaciones de la empresa (vea la figura 10 [16]).

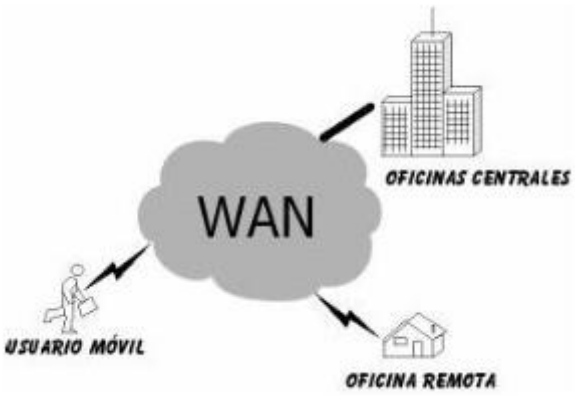


Fig. 10: Acceso remoto

Si una compañía requiere de un sistema de acceso remoto lo primero que se tiene que evaluar es que tipo de usuarios tiene, ya sea móviles, de oficina remota o ambos. Una vez hecho esto, lo que debe hacerse es definir las necesidades de estos usuarios que se deben satisfacer. Estas necesidades pueden ser:

- Acceso remoto al correo electrónico
- Acceso remoto a los archivos del usuario
- Acceso remoto a una aplicación centralizada
- Acceso remoto a aplicaciones personalizadas o programas groupware
- Acceso remoto a la intranet o extranet

Después de examinar estas necesidades, el siguiente paso es estimar los requerimientos del ancho de banda para los diferentes usuarios. Esto es necesario para determinar qué tipo de conexión es necesaria para establecer el acceso remoto.

También es importante determinar si dicha conexión es económicamente rentable para la empresa.

- **Acceso remoto antes de las VPN**

Antes de que las VPN fueran tomadas como opción para el acceso remoto, era común que una corporación instalara módems desde los cuales el usuario remoto hacía una llamada para estar en conexión con la red corporativa. En redes donde no hay muchos usuarios remotos se pueden agregar sólo uno o dos módems a una computadora configurada como Servidor de Acceso Remoto (RAS, Remote Access Server). En el caso de organizaciones que mantienen muchos usuarios remotos, es preciso instalar desde decenas hasta cientos de módems y formar bancos o pilas de módems como se puede ver en la figura 11 [16]:

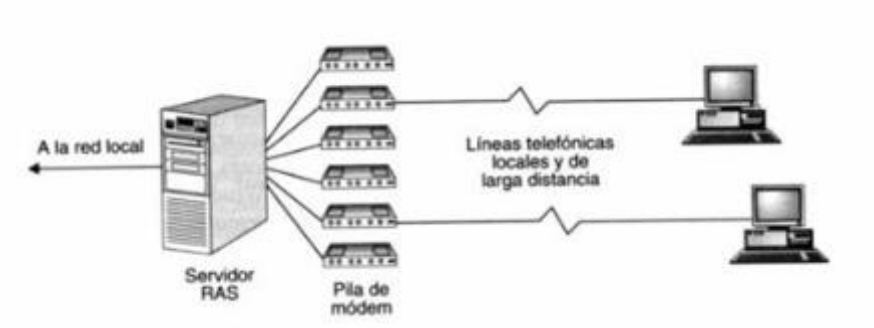


Fig. 11: Acceso remoto sin una VPN

El acceso remoto así resulta ser caro y requiere de un gran soporte por parte de las empresas. Frecuentemente, los usuarios se encuentran muy alejados de las oficinas centrales de la compañía y tienen que realizar llamadas de larga distancia o llamada 0-800. Esto resulta ser especialmente caro si las llamadas son internacionales y si los teletrabajadores requieren estar conectados durante un tiempo largo. El acceso remoto requiere también del uso de los RAS que también son muy caros.

El uso de un módem desde otro país causa muchas dificultades ya que las velocidades de conexión son muy lentas, una línea telefónica no es buena y puesto que la mayor parte del tráfico internacional pasa a través de un satélite se producen muchos retrasos en la comunicación.

2.2.2.4 *Dirección IP*

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente

una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI.

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática). Esta no cambia con el tiempo.

Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Las computadoras se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio.

2.2.2.4.1 Dirección IPV4

Las direcciones IPv4 se expresan por un número binario de 32 bits, permitiendo un espacio de direcciones de hasta 4.294.967.296 () direcciones posibles. Las direcciones IP se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor2^{32} decimal de cada octeto está comprendido en el intervalo de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255.

2.2.2.4.2 Dirección IPV6

La función de la dirección IPv6 es exactamente la misma que la de su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la Tierra tenga asignados varios millones de IPs, ya que puede implementarse con

2^{128}(3.4×10^{38} hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF.

2.2.2.5 *Red Privada Virtual*

2.2.2.5.1 Definición

Una red privada virtual (VPN) es una red privada segura y cifrada que se ha configurado dentro de una red pública para aprovechar la economía de escala y las facilidades administrativas de las grandes redes, como Internet. Una VPN ofrece a su firma comunicaciones seguras y cifradas a un costo mucho menor que las mismas capacidades que ofrecen los proveedores tradicionales que no son de Internet, y que utilizan sus redes privadas para las comunicaciones seguras (vea la figura 12 [23]). Las VPN también proporcionan una infraestructura de red para combinar redes de voz y de datos. Se utilizan varios protocolos competidores para proteger los datos que se transmiten a través de la red Internet pública, como el Protocolo de Tunelización Punto a Punto (PPTP) [23].

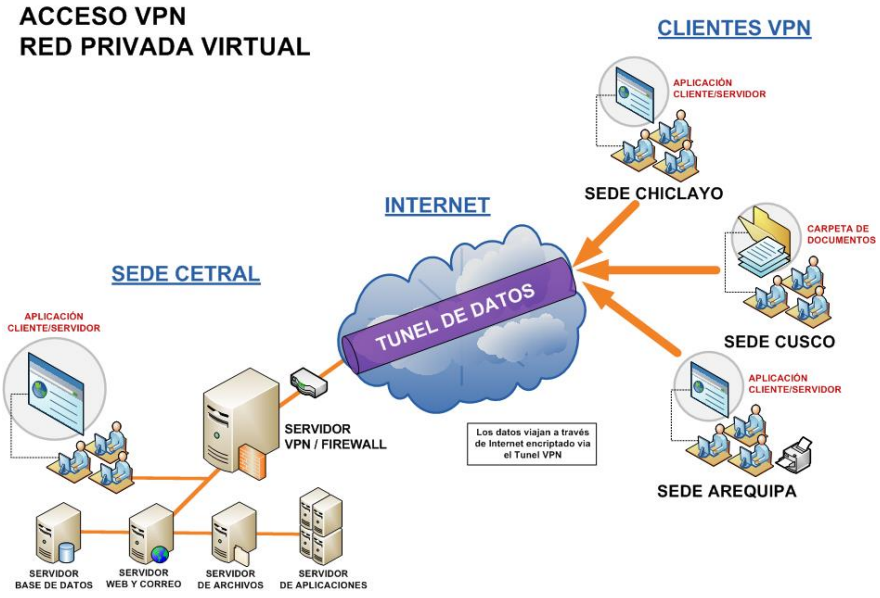


Fig. 12: Ejemplo de una Red Privada Virtual

Se puede utilizar VPN sobre una red pública para realizar dos tipos básicos de conexión [24]:

- ✓ **Acceso remoto**. También llamada Remote Access VPN, Client-Gateway o Usuario-Red. Permite unir virtualmente un equipo remoto a una red.
- ✓ **Interconexión de redes**. También llamada Site to Site VPN, Router to Router VPN, Gateway-Gateway o Red-Red. Permite unir virtualmente dos redes para crear una única red.

De manera similar, se puede utilizar VPN sobre una red privada para acceder a una subred protegida y/u oculta de dos maneras básicas [24]:

- ✓ **Acceso privado**. Permite controlar el acceso a la subred oculta y cifrar el tráfico hacia dicha red.
- ✓ **Interconexión de redes privadas**. Permite unir dos subredes protegidas y/u ocultas cifrando el tráfico entre ellas.

2.2.2.5.2 Razones por las cuales es recomendable Implementar una VPN

Fundamentalmente por las siguientes razones [25]:

Reducción de costos

Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto) de muy alto costo.

Alta seguridad

Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, dando un resultado comparable a una red punto a punto. Protocolos como 3DES (Triple Data Encryption Standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan un alto nivel en seguridad al sistema.

Además, se utilizan varios niveles de autentificación de usuarios para el acceso a la red privada mediante llaves de ingreso, para la asegurar que el usuario es el original y no un tercero que percibe el password de autentificación.

Escalabilidad

Para agregar usuarios a la red no es preciso realizar inversiones adicionales. La provisión de servicios se hace con dispositivos y equipos fáciles de configurar y manejar.

Se usa la infraestructura de alto nivel establecida ya por los proveedores de Internet y no realizar un enlace físico que puede significar una gran inversión monetaria y de tiempo.

Compatibilidad con tecnologías de banda ancha

Una red VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN, lo que implica un alto grado de flexibilidad y reducción de costos al momento de configurar la red. Incluso es posible usar voz sobre IP usando la implementación VPN, y esto implica un significativo ahorro en telefonía de larga distancia.

Mayor productividad

Debido a un mejor nivel de acceso durante mayor tiempo se podría probar que se obtendría una mayor productividad de los usuarios de la red. Además, se fomenta el teletrabajo con la consecutiva reducción en las necesidades de espacio físico.

2.2.2.5.3 Tipos de VPN

Sistemas basados en hardware

Las VPN basadas en Hardware poseen en el extremo del Servidor de la organización un “router” o “enrutador” dedicado el cual tiene la misión de encriptar los datos, además de abrir y cerrar los túneles VPN cuando funciona como receptor. Estos proporcionan facilidades al usuario que administra la implementación VPN, ya que son seguros, rápidos, de fácil instalación y fáciles de usar. Ofrecen un gran rendimiento puesto que no malgastan ciclos en forma tan significativa de procesamiento de operación, y no requieren un sistema operativo que este es configurado para las operaciones que requiera el servicio VPN [24].

Sistemas basados en firewall

Estos sistemas aprovechan las ventajas del “Firewall” o “Cortafuego” como la restricción de acceso a la red o generación de registros de posibles amenazas, y ofrecen además otras opciones como traducción de direcciones o facilidades de autentificación fuerte.

La desventaja de un sistema basado en firewall afecta en mayor o menor medida al rendimiento del sistema general, lo que puede ser un problema para la organización dependiendo de las necesidades que se requieran. Algunos fabricantes de firewalls

ofrecen en sus productos procesadores dedicados a encriptación para minimizar el efecto del servicio VPN en el sistema [24].

Sistemas basados en software

Estos sistemas basados en software son ideales en el caso en que los dos extremos que deseen comunicarse en forma remota y privada no pertenezcan a la misma organización.

Esta solución permite mayor flexibilidad en cuanto a la decisión de que tráfico enviar por el túnel seguro VPN, pudiendo decidir por protocolo y dirección donde en un sistema basado en hardware solo se puede decidir por dirección.

Existen desventajas para un sistema basado en software, las cuales consisten en que estos sistemas son difíciles de administrar, ya que necesitan estar familiarizados con el sistema operativo Cliente, la aplicación VPN y los mecanismos de seguridad adecuados [24].

2.2.2.5.4 Categorías de las VPNS

- ✓ **VPN intranet:** este tipo de red es creado entre una oficina central y una o varias oficinas remotas.
- ✓ **VPN acceso remoto:** es el que se crea entre las oficinas centrales y los usuarios situados remotamente, ya sea a través de dispositivos móviles o terminales fijas. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre.
- ✓ **VPN extranet:** se forma entre dos organizaciones diferentes, o bien entre una corporación y sus proveedores o clientes. Se puede implementar una VPN Extranet mediante acuerdo entre miembros de distintas organizaciones.
- ✓ **VPN internas:** con la migración hacia redes inalámbricas, como 802.11, es necesario incrementar las medidas de seguridad en una corporación. Actualmente se puede implementar una VPN interna cuando se tiene una LAN inalámbrica. En este caso la red pública es el espectro de frecuencia que se ocupa para comunicar un punto de acceso (AP) y un dispositivo [24].

2.2.2.5.5 Seguridad VPN

Un componente principal de las VPN basadas en Internet es la seguridad. Los tres principales protocolos propuestos para VPNs, son IPSec, PPTP y L2TP-cada uno

proporciona diferentes grados de seguridad para sus datos y la facilidad de despliegue. Los esfuerzos de estandarización harán que IPSec y L2TP sean los protocolos preferidos durante los próximos años.

Una de las principales preocupaciones de cualquier corporación es proteger sus datos; las fortunas se pueden hacer y perder, o reputaciones arruinadas, si la información termina en las manos equivocadas. Proteger los datos contra el acceso ilegal y la alteración es aún más un problema en las redes; transmitir datos entre computadoras o entre LAN puede hacer que los datos sean más vulnerables al espionaje y la interceptación que si hubiera permanecido en una sola computadora.

Muchas de las posibles amenazas a la transmisión de datos a través de las redes actuales son bastante conocidas, y los expertos en seguridad saben cómo contrarrestarlos.

En entornos de red, la seguridad de sus datos y comunicaciones depende de tres cosas: autenticación, confidencialidad e integridad de datos. Autenticación significa que la persona con quien uno se está comunicando realmente es esa persona; es un paso más allá de la identificación porque también se está verificando la identificación. Mantener la confidencialidad de sus comunicaciones es garantizar que nadie puede espiar sus comunicaciones, es decir, nadie puede leer sus datos, incluso si lo interceptan. Por último, garantizar la integridad de sus datos significa que los datos no se han alterado de ninguna manera durante la transmisión.

Protocolos VPN

En este apartado se describen los principales protocolos utilizados para construir VPN's y, que son los preferidos por los encargados de TI en las organizaciones dependiendo de las necesidades que ésta tenga [26].

A. *IPSec*

La seguridad del protocolo de Internet (IPSec) es un marco de estándares abiertos para ayudar a garantizar comunicaciones privadas y seguras a través de las redes de Protocolo de Internet (IP) mediante el uso de servicios de seguridad criptográfica. IPSec admite integridad de datos a nivel de red, confidencialidad de datos, autenticación de origen de datos y protección de reproducción. Como IPSec está integrado en la capa de Internet (capa 3), proporciona seguridad para casi todos los protocolos en el conjunto de TCP / IP, y debido a que IPSec se aplica de forma transparente a las aplicaciones, no hay necesidad de configurar una seguridad separada para cada aplicación que utiliza

TCP / IP [27]. Para un mejor entendimiento de la arquitectura del protocolo IPSec, vea la figura 17 [28].

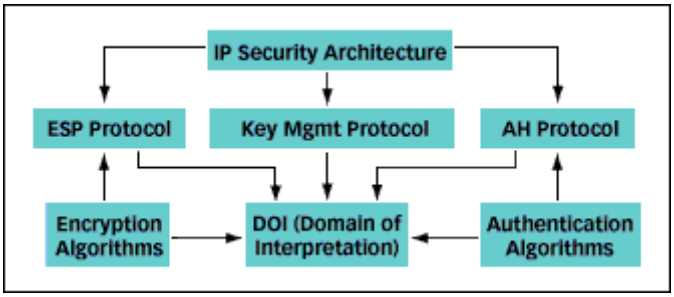


Fig. 13: Arquitectura IPSec

IPSec se basa en una serie de tecnologías criptográficas estandarizadas para proporcionar confidencialidad, integridad de datos y autenticación. IPSec usa lo siguiente:

- Intercambios de claves Diffie-Hellman para entregar claves secretas entre pares en una red pública
- Criptografía de clave pública para firmar intercambios Diffie-Hellman para garantizar las identidades de las dos partes y evitar los ataques de hombre en el medio
- DES y otros algoritmos de cifrado masivo para cifrar datos
- Algoritmos hash con clave (HMAC, MD5 y SHA) para autenticar paquetes
- Certificados digitales para validar claves públicas

El uso de todas estas tecnologías dentro de IPSec ha sido cuidadosamente diseñado en documentos arquitectónicos como RFC 1825. Los tres componentes principales de IPSec son el protocolo AH, el protocolo ESP, y gestión de claves. El diseño de los protocolos AH y ESP son de naturaleza modular, permitiendo diferentes algoritmos criptográficos para ser utilizados como se desee. Si se desarrollan nuevos algoritmos, como el algoritmo de curva elíptica que ahora están volviéndose comercialmente disponibles, los parámetros para su uso pueden ser estandarizado y luego utilizado en conjunto con AH o ESP.

B. *PPTP*

El protocolo de túnel punto a punto fue creado por primera vez por un grupo de compañías que se hacen llamar el Foro PPTP. El grupo estaba formado por 3Com, Ascend Communications, Microsoft, ECI Telematics y US Robotics. La idea básica detrás de PPTP era dividir las funciones de acceso remoto de tal manera que los

individuos y las corporaciones pudieran aprovechar la infraestructura de Internet para proporcionar conectividad segura entre clientes remotos y redes privadas. Los usuarios remotos simplemente se comunican con el número local de su proveedor de servicios de Internet y pueden acceder de forma segura a su red corporativa.

El protocolo más utilizado para el acceso por discado a Internet es el protocolo punto a punto. PPTP se basa en la funcionalidad de PPP para proporcionar acceso por discado que se puede tunelizar a través de Internet a un sitio de destino (vea la figura 18 [29]). Tal como se implementa actualmente, PPTP encapsula paquetes PPP utilizando una versión modificada del protocolo Generic Routing Encapsulation (GRE[3]), que le da a PPTP la flexibilidad de manejar protocolos distintos de IP, como IPX y NETBEUI, por ejemplo.

Debido a su dependencia de PPP, PPTP se basa en los mecanismos de autenticación dentro de PPP, concretamente PAP[4] y CHAP[5]; ya que existe un fuerte vínculo entre PPTP y Windows NT, también se utiliza una versión mejorada de CHAP, MS-CHAP[6]. Esta versión utiliza información dentro de los dominios NT para seguridad. De forma similar, PPTP puede usar PPP para cifrar datos, pero Microsoft también ha incorporado un método de encriptación más fuerte, el Cifrado punto a punto de Microsoft (MPPE[7]) para usarlo con PPTP.

[3] El GRE (Generic Routing Encapsulation) es un protocolo para el establecimiento de túneles a través de Internet

[4] Password Authentication Protocol o PAP es un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet.

[5] CHAP es un protocolo de autenticación por desafío mutuo (CHAP, en inglés: Challenge Handshake Authentication Protocol) y fue definido en la RFC 1994. Es un método de autenticación remota o inalámbrica.

[6] MS-CHAP, en inglés Microsoft Challenge Handshake Authentication Protocol. Es la versión de Microsoft del protocolo de autenticación de contraseñas de cifrado por desafío mutuo, de Microsoft, el cual es irreversible.

[7] Algoritmo de cifrado de claves de 128 bits o claves de 40 bits que utiliza RSA RC4. MPPE garantiza la confidencialidad de los paquetes entre el cliente de acceso remoto y el servidor de acceso remoto o de túnel, y resulta útil cuando no hay IPSec.

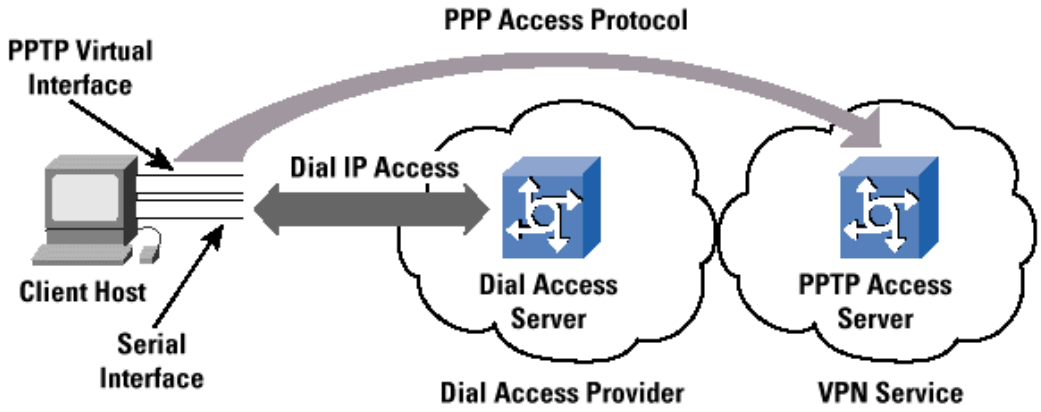


Fig. 14: Modelo de PPP de terminación de túneles de PPTP

Además de la relativa simplicidad del soporte al cliente para PPTP, una de las principales ventajas del protocolo es que PPTP está diseñado para ejecutarse en Capa 2, o la capa enlace, en oposición a IPSec, que se ejecuta en capa 3. Al admitir comunicaciones de datos en capa 2, PPTP puede transmitir protocolos que no sean IP a través de sus túneles. IPSec, por otro lado, está restringido a la transferencia de solo paquetes IP a través de sus túneles.

Con PPTP en una implementación voluntaria de tunelización, el usuario de acceso telefónico puede elegir el destino del túnel PPTP (el servidor PPTP) después de que se haya completado la negociación PPP inicial. Esta característica es importante si el destino del túnel cambia con frecuencia, porque no se necesitan modificaciones en la vista del cliente del acceso base PPP cuando hay un cambio en el servidor y la ruta de tránsito hacia el servidor. También es una ventaja significativa que los túneles PPTP son transparentes para el proveedor de servicios, y no se requiere una configuración previa entre el operador NAS y el acceso de marcado superpuesto VPN. En tal caso, el proveedor de servicios no alberga el servidor PPTP, y simplemente pasa el tráfico PPTP junto con las mismas políticas de procesamiento y reenvío que el resto del tráfico IP. De hecho, esta característica se debe considerar un beneficio significativo de este enfoque. La configuración y el soporte de un mecanismo de tunelización dentro de la red del proveedor de servicios sería un parámetro menos que el proveedor del servicio debe gestionar operacionalmente, y el túnel PPTP puede abarcar de manera transparente múltiples proveedores de servicios sin ninguna configuración explícita del proveedor de servicios [30].

C. *L2TP*

El protocolo de túnel capa 2 se creó como sucesor de dos protocolos de túnel, PPTP y L2F[8]. En lugar de desarrollar dos protocolos en competencia para hacer esencialmente lo mismo, PPTP de Microsoft et al. frente a L2F de Cisco, las empresas acordaron trabajar juntas en un solo protocolo, L2TP, y enviarlo al IETF[9] para su estandarización.

Al igual que PPTP, L2F se diseñó como un protocolo de túnel, utilizando su propia definición de cabecera de encapsulación para transmitir paquetes en capa 2. Una diferencia importante entre PPTP y L2F es que el túnel L2F no depende de IP y GRE, lo que le permite trabajar con otros medios físicos. Como GRE no se usa como protocolo de encapsulado, las especificaciones L2F definen cómo se manejan los paquetes L2F en diferentes medios, con un enfoque inicial en el UDP[10] de IP. Vea la representación de L2TP en la figura 19 [29].

Paralelo al diseño de PPTP, L2F utilizó PPP para la autenticación del usuario de acceso telefónico, pero también incluyó soporte para TACACS + y RADIUS para autenticación desde el principio. L2F difiere de PPTP al definir las conexiones dentro de un túnel, lo que permite que un túnel admita más de una conexión. También hay dos niveles de autenticación del usuario: primero, por el ISP antes de configurar el túnel; segundo, cuando la conexión está configurada en la puerta de enlace corporativa.

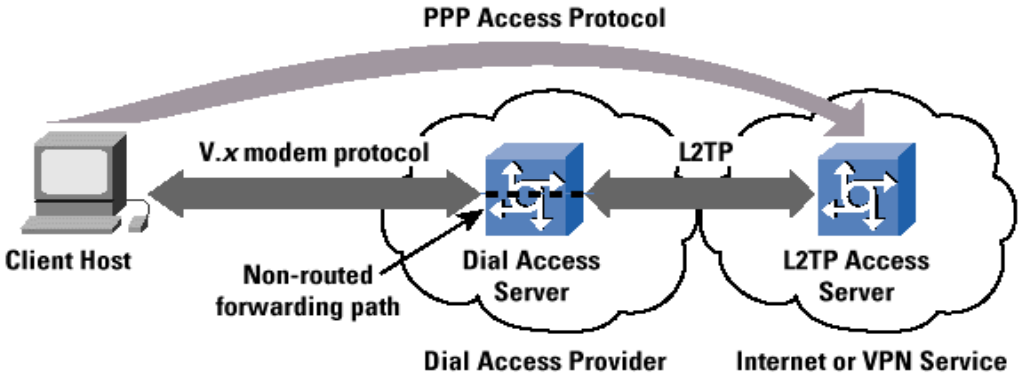


Fig. 15: Modelo de terminación de túnel PPP de L2TP

[8] Protocolo desarrollado por Cisco, a diferencia del PPTP el protocolo L2F no depende de IP con lo cual es capaz de trabajar directamente bajo otros protocolos.
[9] Internet Engineering Task Force (IETF) (en español, Grupo de Trabajo de Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad
[10] Protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 o de Transporte del Modelo OSI)

Con L2TP en una implementación de túnel "obligatoria", el proveedor de servicios controla dónde termina la sesión de PPP. Esta configuración puede ser extremadamente importante en situaciones en las que el proveedor de servicios al que el suscriptor está realmente llamando ("proveedor de grupo de módems") debe transferir transparentemente la sesión PPP del suscriptor a otra red ("proveedor de contenido"). Para el suscriptor, parece que el sistema local está directamente conectado a la red del proveedor de contenido, cuando en realidad la ruta de acceso se ha transmitido de forma transparente a través del proveedor del grupo de módems.

Por supuesto, si todos los suscriptores que se conectan a la red del proveedor del grupo de módems están destinados al mismo proveedor de contenido, entonces hay formas más fáciles de transferir este tráfico a la red del proveedor de contenido, como simplemente agregar todo el tráfico en el local de la Oficina Central y entregarle al proveedor de contenidos un "tubo gordo" de las secuencias de tráfico de la sesión agregada. Sin embargo, en situaciones en las que el proveedor del grupo de módems proporciona un servicio de marcado al por mayor para múltiples redes upstream ascendentes, los métodos para determinar cómo se debe reenviar el tráfico de cada suscriptor a su proveedor de contenido respectivo son algo limitados. Las decisiones de reenvío podrían hacerse en el NAS, según la dirección de origen de la computadora del suscriptor de acceso telefónico. Este escenario permitiría que el tráfico se reenvíe a lo largo de la ruta adecuada a su destino final, a su vez proporciona una conexión virtual intrínsecamente. Sin embargo, el uso de la asignación de direcciones IP estáticas para los suscriptores de acceso telefónico se desaconseja en gran medida debido a las ineficiencias en las políticas de utilización de direcciones IP y al éxito crítico del Protocolo de configuración dinámica de host (DHCP).

D. Open VPN

OpenVPN, una tecnología de código abierto relativamente nueva, utiliza los protocolos SSLv3/TLSv1 y biblioteca OpenSSL junto con una combinación de otras tecnologías para brindar a los usuarios una solución de VPN confiable y potente. El protocolo tiene amplia capacidad de configuración y opera mejor en un puerto UDP, pero se puede configurar para que corra en cualquier otro puerto, lo que hace que sea extremadamente difícil de bloquear para Google y otros servicios similares. Otra de las ventajas importantes de este protocolo es que su biblioteca OpenSSL soporta una variedad de

algoritmos criptográficos, tales como 3DES[11], AES[12], Camellia[13], Blowfish[14], CAST-128[15] y más, aunque Blowfish o AES son utilizados casi exclusivamente por proveedores de VPN. OpenVPN viene con una encriptación Blowfish de 128 bits incorporada. Generalmente se lo considera seguro, pero también tiene algunas debilidades conocidas [31].

En cuanto a la encriptación, AES es la tecnología más reciente disponible y se la considera de un "estándar de oro". Eso es simplemente porque no tiene debilidades conocidas, tanto que ha sido adoptado incluso por el gobierno de los Estados Unidos y sus agencias para proteger datos "confidenciales". Puede manejar archivos pesados comparativamente mejor que Blowfish gracias a su tamaño de bloque de 128 bits comparado con el de 64 bits de Blowfish. Sin embargo, ambos son códigos certificados por el NIST y aunque ahora podrían ser reconocidos ampliamente como un problema, hay algunos inconvenientes con ellos, y los veremos a continuación [31].

En primer lugar, la rapidez con la que se desempeña el protocolo OpenVPN depende del nivel de encriptación utilizado, pero normalmente es más rápido que IPsec. Aunque ahora OpenVPN es la conexión a VPN predeterminada para la mayoría de los servicios, aún no es compatible con cualquier plataforma. Sin embargo, es compatible con la mayoría de los programas de terceros, lo cual incluye a Android y iOS. En cuanto a la configuración, es un poco complicada en comparación con la de L2TP/IPsec y PPTP, particularmente cuando se utiliza el programa genérico OpenVPN [31]. El protocolo OpenVPN se puede observar gráficamente en la figura 20 [32].

[11] Se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado, empleando una clave criptográfica. 3DES es el algoritmo que hace triple cifrado del DES; se basa en aplicarlo tres veces, con tres claves distintas, por lo que resulta mucho más seguro.
[12] Es uno de los algoritmos más seguros que existen hoy en día. Está clasificado por la National Security Agency (NSA) de EE.UU. para la más alta seguridad de la información secreta.
[13] Es un cifrado simétrico de bloque de clave con un tamaño de bloque de 128 bits y tamaños de clave de 128, 192 y 256 bits.
[14] Cifrado de bloque simétrico que se puede utilizar como un reemplazo directo para DES o IDEA.
[15] Pertenece a la clase de algoritmos de encriptación conocida como cifras Feistel; el funcionamiento general es similar a los datos Estándar de encriptación (DES)

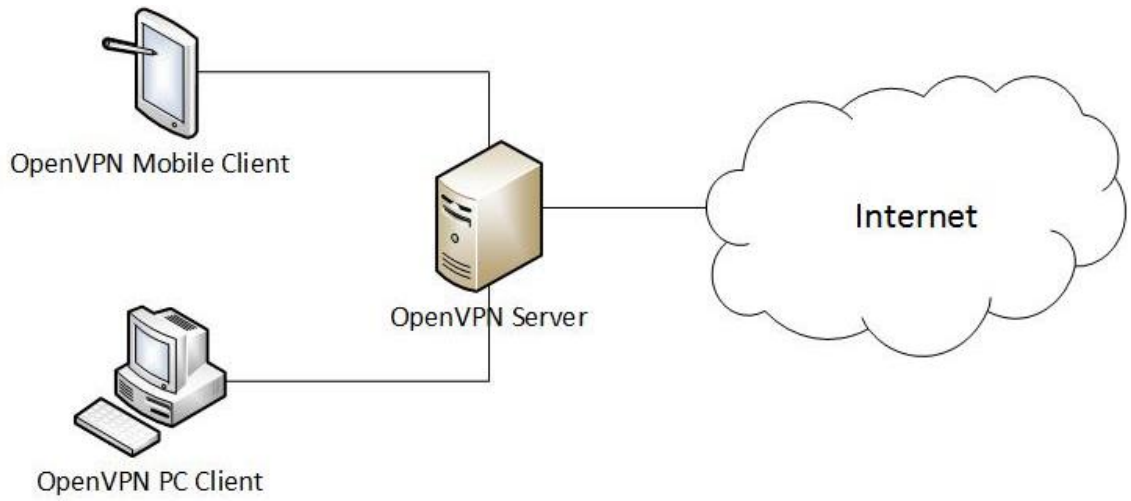


Fig. 16: Funcionamiento Open VPN

E. *SSTP*

Presentado por la Corporación Microsoft en el Service Pack 1 de Windows Vista, el túnel de socket seguro ahora está disponible para SEIL, Linux y RouterOS, pero sigue siendo principalmente una plataforma únicamente para Windows. Como utiliza SSL v3, brinda ventajas que son similares a OpenVPN, tales como la capacidad de prevenir problemas con el cortafuegos NAT[16]. SSTP es un protocolo de VPN estable y fácil de usar, particularmente porque está integrado en Windows. Sin embargo, es un estándar patentado y propiedad de Microsoft [33].

F. *IKEv2*

El protocolo de túnel basado en IPsec, Intercambio de clave de Internet Versión 2, fue desarrollado por Cisco y Microsoft, y está incorporado en la 7ma versión y posteriores de la plataforma Windows. Viene con implementaciones de código abierto compatibles y desarrolladas para Linux y varias otras plataformas, y también soporta dispositivos Blackberry.

Habitualmente conocido como Conexión VPN por la Corporación Microsoft, es bueno para reestablecer conexiones VPN automáticamente cuando se pierde temporalmente. Los usuarios de dispositivos móviles son los más beneficiados con IKEv2 (vea la figura 21 [34]) ya que el protocolo de Movilidad y Multi-Proveedor que se ofrece en forma predeterminada lo hace extremadamente flexible para cambiar de redes. Además, también es genial para usuarios de Blackberry, ya que IKEv2 está entre los pocos

[16] El firewall NAT es una capa adicional de seguridad para su conexión VyprVPN. Bloquea el tráfico entrante no solicitado cuando está conectado a VyprVPN. No se requiere una configuración ni un software adicionales

protocolos de VPN que soportan estos dispositivos. Aunque IKEv2 está disponible en menos plataformas comparado con IPsec, tiene buena reputación en términos de estabilidad, seguridad y rendimiento [35].

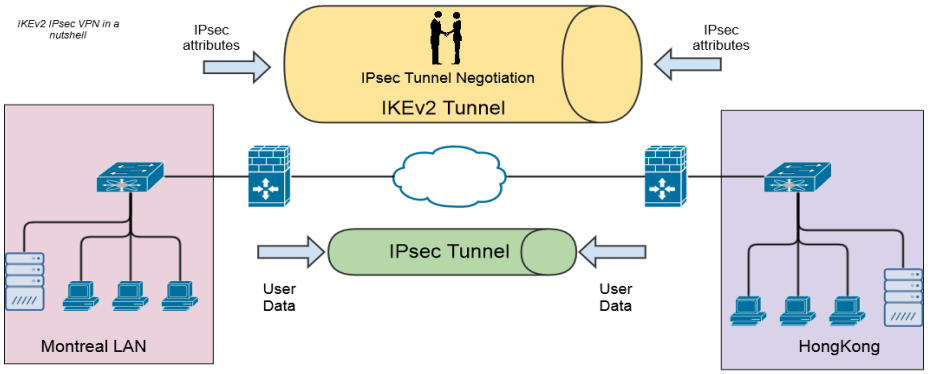


Fig. 17: IKEv2 IPSec VPN

2.2.2.6 *Metodología para la implementación de una VPN*

La metodología que a continuación se va a describir ha sido realizada tomando como experiencia organizaciones pequeñas y tiene como objetivo ayudar al entendimiento y mejor manejo de la teoría y la práctica en el desarrollo de Redes Privadas Virtuales.

Para obtener una Red Privada Virtual exitosa es necesario tomar en cuenta algunos factores que son de vital importancia los mismos que se convertirán en pasos para el análisis y posterior implementación de una Red Privada Virtual, los mismos que se describen a continuación [25]:

2.2.2.6.1 Formación de un equipo de trabajo

Debe ser conformado por un pequeño grupo de especialistas y a este agregar un número pequeño de personal con capacidad de decisión y conocimiento de la organización o empresa, de tal manera que se pueda asignar responsabilidades al personal, además que el equipo debe tener una gran capacidad de liderazgo y responsabilidad para asumir el reto de poner en marcha un proyecto de Redes Privadas Virtuales.

2.2.2.6.2 Fijación del alcance

Temas como los que se describen a continuación deberían ser tomados en consideración:

- ¿Para qué tener una Red Privada Virtual?

- ¿Quiénes serán los usuarios?
- ¿Qué conocimientos, información o datos se van a poner en la Red Privada Virtual?
- ¿Utilizará la Redes Privadas Virtuales para comercio global?
- ¿Instalará una extranet?
- ¿Su organización posee la capacidad técnica adecuada para mantener e instalar una Red Privada Virtual?
- ¿Cómo se integrará la Red Privada Virtual con la Red de la compañía?
- ¿Qué respuesta o resultados se desea obtener?
- ¿Qué tipo de seguridad se utilizará en la red privada virtual?
- ¿Cómo se construirá?
- ¿Su gobierno como considera al cifrado? Se debe tener en cuenta que algunos gobiernos consideran al cifrado como arma, por lo tanto, regula su uso.

2.2.2.6.3 Estudio y análisis

Durante el estudio y análisis se logra identificar los requisitos clave de la Red privada virtual. Se identifica qué información ha de ser procesada, que función y rendimiento se desea, cuál será el comportamiento de la red, que interfaces van a ser establecidas, que restricciones se tendrá, que tipo de seguridad se necesita, que parámetros se sacrificarán a favor de la seguridad y que criterios de validación se necesitan para definir una red privada virtual correcta.

2.2.2.6.4 Elección de la plataforma

Para realizar la elección de qué tipo de Redes Privadas Virtuales instalar es necesario analizar los siguientes puntos:

- Software existente en la empresa.
- Aplicaciones existentes en la empresa.
- Plataforma existente en la empresa.
- Servicios que posee la plataforma.
- Seguridades que brinda la plataforma.
- Soporte técnico que posee la plataforma.
- Tipo de servidores que posee la empresa.
- Costo de la plataforma.

2.2.2.6.5 Propuestas de soluciones

En esta etapa se define la filosofía y enfoque globales; se concibe la estructura lógica de la red privada virtual y se visualiza el conjunto general de la red.

En la propuesta de soluciones se debe tener en consideración los siguientes aspectos:

- ¿Qué aplicaciones van a pasar por la Red Privada Virtual?
- ¿Qué tipo de infraestructura de hardware soporta su organización?
- ¿Cuántos usuarios estima que utilizarán la Red Privada Virtual?
- ¿El tráfico que pasará por la VPN es pesado?
- ¿Qué tipo de seguridades se utilizarán en la Red Privada Virtual?

2.2.2.6.6 Seguridades

Para esto se hace necesario la implantación de una política de Seguridad basándose en los siguientes parámetros:

Fijación de objetivos

Si se toma en cuenta que es lo que se va a proteger, de que va a proteger y si se considera algunas sugerencias del equipo ejecutor (ya que éstos fueron escogidos precisamente para poder realizar un plan de seguridad), se encontrará en la capacidad de establecer cuáles son las prioridades de seguridad corporativa, de tal manera que se pueda obtener una política de seguridad que brinde las mejores condiciones para la red implementada.

Relación costos vs. riesgos

Se debe comparar costo de implantar la seguridad con el costo de la información que se desea proteger, el mismo que brindará un panorama bastante amplio, y se debe tomar la decisión de que es lo que va a proteger, porque realmente sería innecesario proteger algo que tenga menos costo que el valor de la seguridad a implantar.

2.2.2.6.7 Plan de contingencia

Se debe considerar un plan que garantice finalizar con éxito la implementación de la red privada virtual y para ello se debe tener en cuenta los siguientes aspectos:

- ¿El personal encargado de desarrollar las Redes Privadas Virtuales tiene la suficiente capacitación y experiencia en este tema?

- ¿En el medio en el que nos encontramos existen varios proveedores de Internet que puedan brindar soporte para las Redes Privadas Virtuales?
- ¿Todo el proyecto se está documentando?
- ¿Qué acciones se tomarán si el equipo de desarrollo se va?
- ¿Qué riesgos podrían hacer que nuestro proyecto fracasará?
- ¿Qué métodos y herramientas deberíamos emplear?
- ¿Cuánta importancia hay que darle a la calidad?
- ¿Tenemos aplicaciones que entren en conflicto con las Redes Privadas Virtuales?

2.2.2.6.8 Costos

Puesto que la parte económica juega un papel muy importante en el éxito de una Red Privada Virtual, se considera muy importante analizar los siguientes puntos para determinar los costos que involucrados en su implementación: hardware, software, capacitación, contratación de servicios.

2.2.2.6.9 Implementación

En esta fase se configurarán los servidores, los clientes y demás equipos que sean necesarios para la red privada virtual.

2.2.2.6.10 Mantenimiento

El mantenimiento se centra en el cambio que va asociado a la corrección de errores, a las adaptaciones requeridas a medida que evoluciona el entorno de la red privada virtual, y a cambios debidos a las mejoras producidas por los requisitos cambiantes de la organización.

2.2.2.6.11 Medición

Este punto es necesario para poder realizar una evaluación del trabajo realizado en la institución, por tanto, la evaluación se realizará en todo momento, se evaluará a partir de la puesta en marcha del proyecto y se podrá medir como se está avanzando en la ejecución, en lo posterior se evaluará la utilización de los servicios y por defecto se estará evaluando la conformidad, la aceptación por parte de los usuarios hacia la nueva implementación.

2.2.3 Definición de términos básicos

2.2.3.1 *Evaluación de impacto*

Conjunto de estudios y sistemas técnicos que permiten estimar los efectos que la ejecución de un determinado proyecto, obra o actividad causa sobre alguna actividad, proceso, persona, medio ambiente, etc. Las evaluaciones de impacto permiten medir, mediante el uso de metodologías rigurosas, los efectos que un programa puede tener sobre su población beneficiaria y conocer si dichos efectos son en realidad atribuibles a su intervención. El principal reto de una evaluación de impacto es determinar qué habría pasado con los beneficiarios si el programa no hubiera existido [36].

2.2.3.2 *Router*

Un router(enrutador) es un dispositivo de hardware diseñado para recibir, analizar y mover paquetes entrantes a otra red. También se puede usar para convertir los paquetes a otra interfaz de red, soltarlos y realizar otras acciones relacionadas con una red. Un enrutador tiene muchas más capacidades que otros dispositivos de red, como un concentrador o un conmutador que solo pueden realizar funciones básicas de red [37].

2.2.3.3 *Cisco*

Empresa estadounidense que diseña, fabrica y vende productos y servicios de red basados en protocolo de Internet relacionados con la industria de las tecnologías de la información y las comunicaciones. Proporciona una amplia línea de productos para el transporte de datos, voz y video dentro de los edificios y en los campus. La oferta de productos de la empresa se compone de las siguientes categorías: conmutación, enrutamiento de redes de próxima generación (NGN), video del proveedor de servicios, colaboración, centro de datos, inalámbrico, seguridad y otros productos. El cambio es una tecnología de red utilizada en campus, sucursales y centros de datos. Los Switches se usan dentro de edificios en redes de área local y a través de grandes distancias en redes de área amplia. Los productos de conmutación ofrecen muchas formas de conectividad para usuarios finales, estaciones de trabajo, teléfonos IP, puntos de acceso y servidores, y también funcionan como agregadores en redes de área local y redes de área amplia. La tecnología de enrutamiento de red de próxima generación es fundamental para la fundación de Internet [38].

2.2.3.4 *Acces Point*

Dispositivo de conectividad intermedio llamado un punto de acceso inalámbrico. Un punto de acceso inalámbrico, también conocido simplemente como punto de acceso, o un AP, es un dispositivo que acepta señales inalámbricas de múltiples nodos y los retransmite al resto de la red. Los puntos de acceso también se pueden conocer como estaciones base. Los puntos de acceso para su uso en pequeñas oficinas o redes domésticas a menudo incluyen funciones de enrutamiento. Como tal, ellos también se pueden llamar enrutadores inalámbricos o puertas de enlace inalámbricas [39].

2.2.3.5 *Gbps*

Acrónimo usado para establecer las siglas de "Gigabits por segundo". 1 Gbps es igual a 1,000 Megabits por segundo (Mbps), o 1,000,000,000 de bits por segundo. Gbps se usa comúnmente para medir velocidades de transferencia de datos entre dispositivos de hardware. Durante muchos años, las velocidades de transferencia de datos solo se midieron en Mbps y Kbps. Sin embargo, las interfaces de hardware modernas ahora pueden transferir datos a más de un gigabit por segundo, lo que hace que los Gbps sean una unidad de medida necesaria [40].

2.2.3.6 *Gateway*

Un Gateway (puerta de enlace) es un dispositivo con el que podemos interconectar redes con protocolos, así como arquitecturas diferentes, en todos los niveles de comunicación. Se encarga de traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino, actúa como nexo entre dos redes que usan el mismo protocolo, y suele traducir las direcciones IP de ambas redes para que se comuniquen entre ellas [41].

2.2.3.7 *Red*

Una red de datos no es solamente un conjunto de computadoras conectadas entre sí para compartir recursos y servicios. Las redes de datos implican, hoy, conectividad móvil a una infinidad de servicios y de recursos, tanto para las personas individuales como para las empresas. Las organizaciones tienen a su disposición diferentes tecnologías para sus redes de datos. Internet es la base de muchas de ellas. A través de este medio, las empresas pueden comercializar sus productos o tener teletrabajadores que realizan su labor a distancia. Las posibilidades que definen a una red están dadas por su capacidad para implementar nuevas tecnologías [42].

CAPÍTULO III.MATERIALES Y MÉTODOS

La ubicación geográfica donde se realizó la investigación, es la empresa Deyfor E.I.R.L ubicada en el Jr. Antonio Astopilco N°537 – Las Torrecitas de la ciudad de Cajamarca, Perú. Aquí se presenta el procedimiento que se realizó para el desarrollo de la investigación. Por otro lado, se encuentran también las técnicas e instrumentos que fueron necesarios para la selección de información. A la vez se detalla de acuerdo a la metodología utilizada, cada paso en la implementación de la red VPN.

La investigación inicia en junio de 2017 y culmina en marzo de 2018.

2.3 PROCEDIMIENTO

2.3.1 Descripción de la Empresa

Deyfor E.I.R.L. es una empresa dedicada a la prestación de servicios generales (proyectos, obras civiles, metal-mecánica, mantenimiento) en el rubro minero, especialmente en Cajamarca.

Inició sus operaciones desde el 2004, se han constituido como una de las organizaciones cajamarquinas más sólidas y con mayor experiencia. Han desarrollado, a lo largo de su historia, innumerables proyectos en todos los sectores de la construcción, obras electro metalmecánicas, de mantenimiento, entre otros. Deyfor ofrece sus servicios a todas las empresas del departamento de Cajamarca y del resto del país, poniendo a disposición de sus clientes, un equipo de profesionales y técnicos altamente especializados y con pasión por su trabajo. Además, dentro de sus recursos, cuenta con una flota de equipos y maquinaria de última generación con altos estándares de mantenimiento. Con más de 13 años el mercado competitivo, con una magnífica posición de liderazgo, que los conlleva a tener éxito día a día gracias a que mantienen el compromiso, calidad y eficiencia en cada una de sus actividades.

2.3.2 Situación actual de la empresa

Actualmente Deyfor E.I.R.L. se ha convertido en una empresa líder en la prestación de servicios para obras civiles, proyectos, e infraestructuras metálicas; cuenta con alta experiencia en el desarrollo de proyectos para el rubro minero, constructor e industrial. Cada uno de sus colaboradores son altamente valorados ya que conforman el recurso

más preciado e importante que hacen de la familia Deyfor una de las empresas altamente reconocidas en términos de producción en Cajamarca.

Debido al desarrollo sostenido que ha alcanzado esta organización a lo largo del tiempo que viene operando, necesita contar con soluciones innovadoras que contribuyan a un manejo adecuado y eficiente de la información que maneja dentro de todas sus áreas. Frente a estas consideraciones surge la propuesta de implementar una red privada virtual ya que permite el acceso a la red de trabajo de manera remota, especialmente útil si los trabajadores se encuentran fuera de oficinas y necesitan acceder a esta red de trabajo; también permite esconder datos de navegación, para evitar que terceros accedan al contenido o información de la empresa; asimismo, garantiza el acceso a contenido con bloqueo regional, convirtiéndose esta en la mayor ventaja para quienes que pretenden disfrutar del contenido disponible en otros territorios; por otro lado, una VPN permite eludir la censura de Internet mayormente proporcionada por los gobiernos quienes establecen censura sobre algunas páginas. Una VPN funciona en todos los dispositivos y aplicaciones, puesto que enruta todo el tráfico proveniente de Internet.

La proliferación del teletrabajo y de los empleados que viajan con sus equipos portables hace que sea necesario utilizar mecanismos para que esas personas puedan trabajar de forma cómoda y, en especial, muy segura. Las redes privadas virtuales traen una solución a esas cuestiones y presentan una serie de desafíos a la hora de implementarlas y configurarlas, ya que de ello depende, en gran medida, la seguridad de la red que las utiliza.

2.3.2.1 *Servicios*

Deyfor E.I.R.L basa sus operaciones en tres líneas de negocio debidamente diferenciadas con la finalidad de brindar servicios con elevados índices de calidad y que garanticen la satisfacción y fidelización de sus clientes; estas líneas de negocio son: obras y proyectos civiles, metal-mecánicos y de mantenimiento.

2.3.2.2 *Misión y Visión*

2.3.2.2.1 Misión

“Proveer soluciones de la construcción y la prestación de servicios generales con el compromiso de calidad y liderazgo de nuestra gente.”

2.3.2.2.2 Visión

Consolidarnos antes del año 2020 como una empresa líder y sostenible dedicada a la prestación de servicios en obras civiles, proyectos e infraestructuras metálicas con un incremento en la participación año a año mediante procesos eficientes para la satisfacción de las expectativas de los clientes y la sociedad bajo un marco de desarrollo responsable comprometidos con el medio ambiente.

Realizar nuestro trabajo con altos estándares de salud ocupacional y seguridad, siendo efectivos y eficientes en generar las mejores condiciones de seguridad para todos los trabajadores de Deyfor.

2.3.2.3 *Ubicación*

La ubicación respecto al Quinde Shopping Plaza: Jr. Antonio Astopilco N° 537- Oficinas

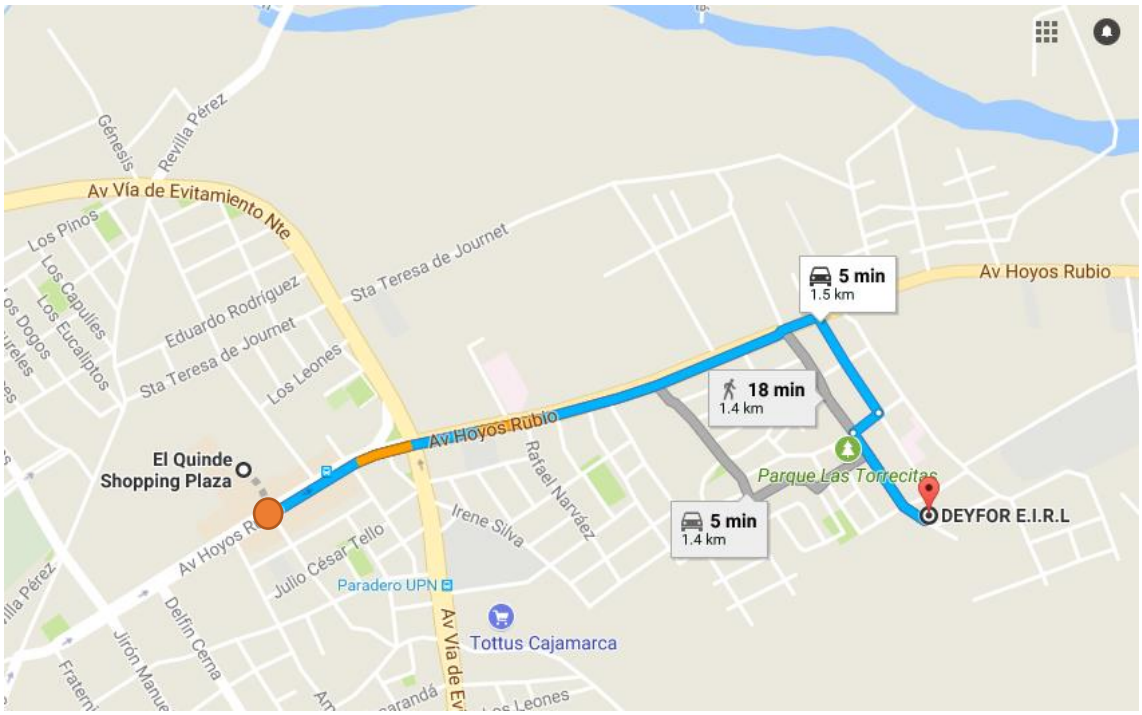


Fig. 18: Ruta de acceso a la empresa Deyfor E.I.R.L. desde el quinde shopping plaza

2.3.2.4 *Estructura General de la Organización Deyfor E.I.R.L.*

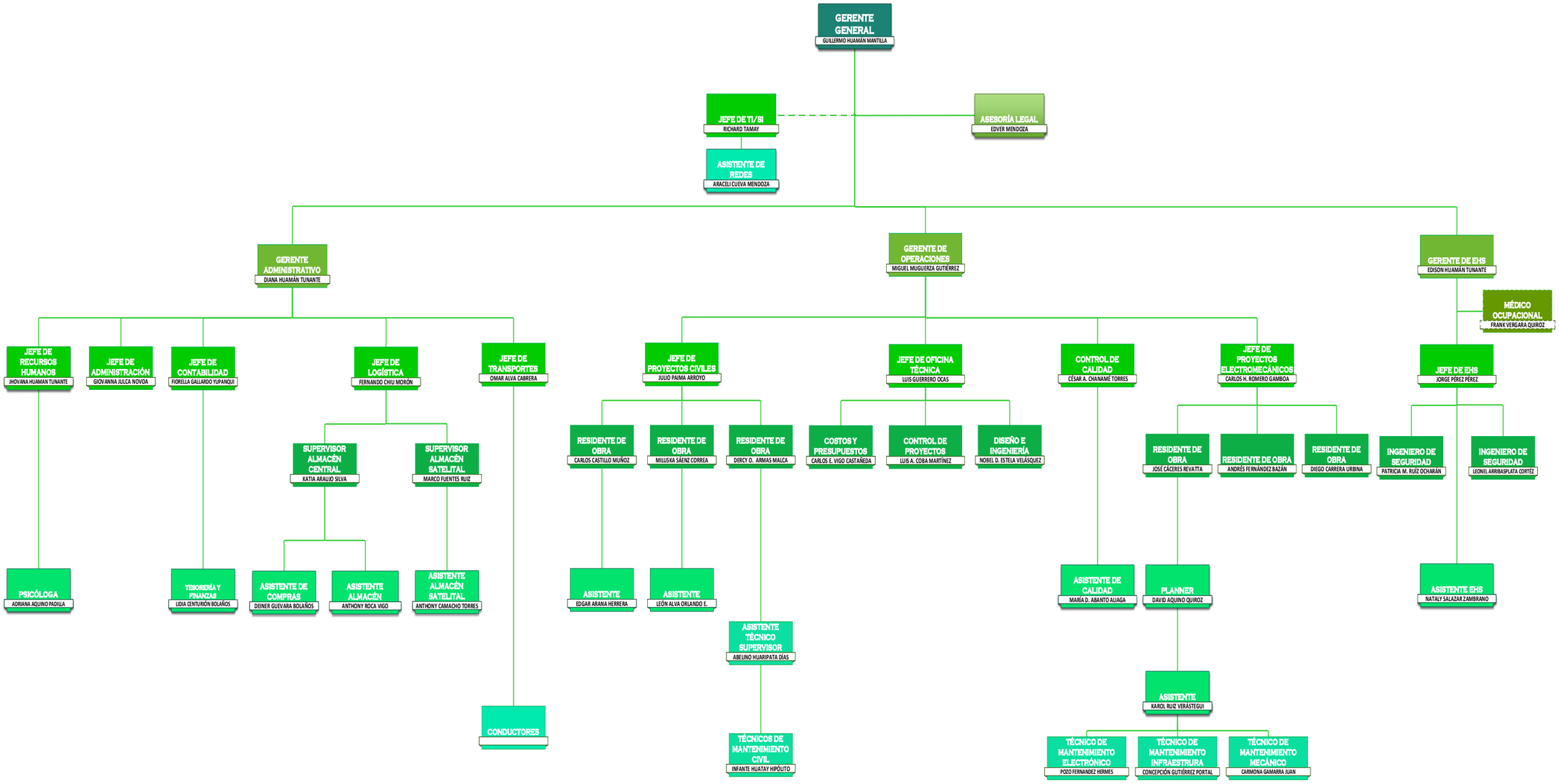


Fig. 19: Estructura Orgánica de la Empresa Deyfor E.I.R.L.

2.3.3 Desarrollo de la solución (Red Privada Virtual)

A continuación, se ha elaborado un gráfico con los pasos establecidos para implementar la VPN, siguen el procedimiento estándar de implementación utilizado por la mayoría de profesionales dedicados a esta actividad, por tanto, se puede afirmar que se ha convertido en prácticamente una metodología que aún no ha sido debidamente aprobada como tal, pero que gracias a su constante adopción no se descarta la posibilidad de que en la posteridad se mejore y se solidifique como una metodología:

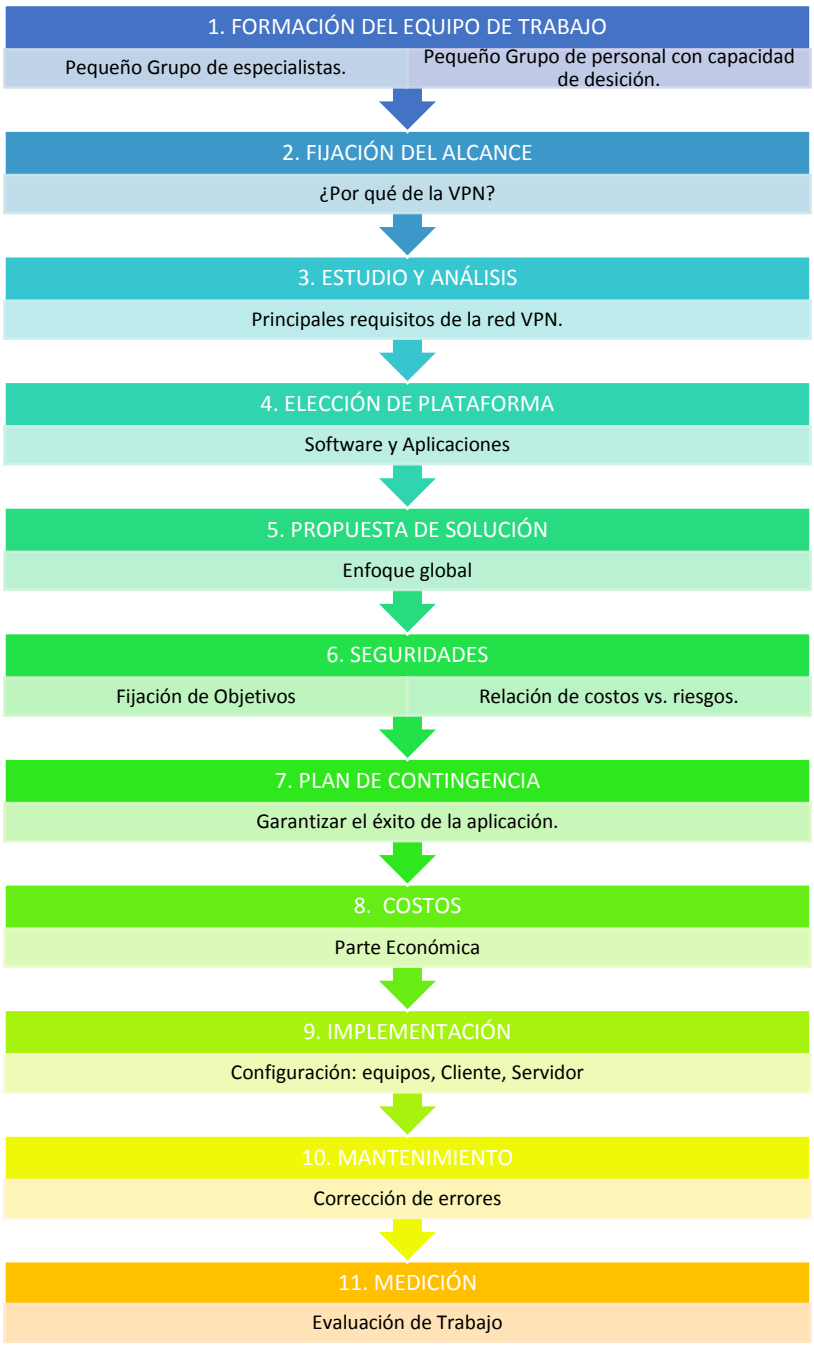


Fig. 20: Pasos para la implementación de una VPN

2.3.3.1 *Formación de un equipo de trabajo*

El equipo estará conformado por profesionales que cuentan con la debida capacidad técnica y científica para respaldar la correcta implementación de la solución dentro de la organización, minimizando al máximo las falencias y, por tanto, garantizar la rápida acción ante cualquier eventualidad o incidencia que pudiera presentarse:

Tabla 1: Equipo de desarrollo para la VPN

Nombre	Área	Apoyo
Guillermo Huamán Mantilla	Gerencia General	Toma de Decisiones
Edison Huamán Tunante	Gerente EHS	Toma de Decisiones
Miguel A. Muguerza Gutiérrez	Gerente Operaciones	Toma de Decisiones
Jhovana Huamán Tunante	Administración	Líder de la Implementación, Toma de Decisiones
Araceli Y. Cueva Mendoza	Tecnologías de Información	Implementador

2.3.3.2 *Fijación del alcance*

2.3.3.2.1 Importancia de tener una Red Privada Virtual

Debido a que la organización cuenta con diversos problemas para la gestión de información, por ejemplo:

- Transferencia insegura de la información a través de servidores de correo y otros servidores externos.
- Manejo de grandes cantidades de información.
- Desorganización de la información.
- Vulnerabilidad de la integridad de la información.
- Acceso a información no actualizada, manejo de información en distintas versiones duplicaciones y modificaciones las cuales generan conflictos al momento de hacer presentaciones formales de la misma.

Por ello el contar con una VPN implica garantizar la seguridad de la información de la organización y además que los colaboradores de la misma puede acceder a prácticamente cualquier lugar de la red sin ningún tipo de restricción geográfica, acceder de manera segura a la información almacenada dentro del servidor local sin importar la ubicación física dónde se encuentren. Los colaboradores tienen la posibilidad de realizar teletrabajo, es decir, realizar labores remotas como si estuvieran presencialmente en la empresa.

Existe un punto vital al momento de considerar la implementación de una VPN en la empresa: la seguridad. Las conexiones VPN tienen un cifrado para los paquetes que se transfieren con ellas, por lo que es la principal opción para conectarse a un Wi-Fi público porque es más seguro mediante una VPN. Es decir, si se utiliza un punto de acceso a Wi-Fi público sin hacer uso de una red privada, seguramente alguien podría acceder a datos personales y de navegación. En cambio, si se hace a través de una VPN de por medio, esta proporcionará los paquetes de cifrado que harán terceras personas no puedan acceder a la información o contenido de navegación.

Por último, y en relación a los anteriores puntos descritos, una VPN ofrece la posibilidad de tener descargas P2P[17]. De igual modo que se puede evitar el bloqueo regional gracias al uso de una VPN, existe la posibilidad de evitar que el proveedor de Internet acceda a las descargas P2P que se realizan.

En Deyfor E.I.R.L. la implementación de una VPN, es necesaria ya que paralelamente al desarrollo del presente proyecto de tesis, se está desarrollando un ERP para brindar el soporte necesario a las actividades empresariales. Al culminar la implementación de esta solución tecnológica (ERP) dentro del servidor institucional, esta será accesible de manera completamente (o casi) segura para los usuarios quienes se encuentren dentro y fuera de la ubicación física del servidor; con lo que, en conclusión, además de la necesidad de que se implemente una red VPN para la gestión de información, también se suma la de facilitar el uso del ERP que está en proceso de implementación.

2.3.3.2.2 Definir los usuarios de la VPN

Lo usuarios de la Red Privada Virtual serán:

Todos los trabajadores de la empresa Deyfor E.I.R.L. que manejen información que pueda ser almacenada y distribuida por el servidor institucional, además de los

[17] Red de ordenadores que actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

colaboradores que hagan uso del sistema ERP en implementación. Estos Trabajadores serían los trabajadores del STAFF de Deyfor, que se presentan en la siguiente lista:

Tabla 2: Listado de usuarios finales de la VPN

N°	ÁREA	APELLIDOS Y NOMBRES	CARGO
1	GERENCIA GENEREAL	Huamán Mantilla, Guillermo	Gerente
2	RECURSOS HUMANOS	Huamán Tunante, Jhovana Yaneth	Jefe de Recursos Humanos
3		Aquino Padilla Adriana	Interna de Psicología
4	ADMINISTRACIÓN	Huamán Tunante Diana Elizabeth	Gerente Administrativo
5		Julca Novoa, Giovanna Elizabeth	Administradora
6	CONTABILIDAD	Gallardo Yupanqui Fiorella	Contadora
7		Centurión Bolaños, Lidia Madeley	Asistente Contable
8	EHS	Huamán Tunante, Edison	Gerente de EHS
9		Pérez Pérez Jorge	Jefe EHS
10		Ruiz Ocharan Patricia	Supervisor de EHS
11		Arribasplata Cortéz Leonel	Supervisor EHS
12		Salazar Zambrano Nataly	Asistente de EHS
13	MEDICINA OCUPACIONAL	Vergara Quiroz Frank Rodolfo	Médico Ocupacional
14	OPERACIONES	Muguerza Gutierrez, Miguel Ángel	Gerente Operaciones
15		Abanto Aliaga María de los Ángeles	Control de Proyectos
16		Paima Arroyo Julio Augusto	Jefe de Proyectos
17		Armas Malca Dercy Omar	Supervisor de Obra
19		Castillo Muñoz Carlos Germán	Supervisor de Obra
20		Arana Herrera Edgar Ulises	Supervisor Residente
21		Fernández Bazán Andrés	Supervisor Residente
22		Cáceres Revata José Manuel	Supervisor Residente
23		Coba Martínez Luis Alberto	Supervisor Residente
24		Carrera Urbina Diego	Supervisor Residente
25		Aquino Quiroz Wilder David	Planner
26		Estela Velásquez Nobel Dereck	Asistente Oficina Técnica
27		Vigo Castañeda Carlos Eduard	Asistente Oficina Técnica
28	LOGÍSTICA	Chiu Morón Fernando Daniel	Jefe Logístico
29		Araujo Silva Katia Janeth	Asistente Logístico
30		Centurión Bolaños Deiner	Asistente de Almacén
31		Vargas Bringas Audiel	Asistente de Almacén
32		Ayala Izquierdo, Emelina	Asistente de Almacén
33		Alva Cabrera Freddy Omar	Asistente Logístico
34	TECNOLOGÍAS DE INFORMACIÓN	Cueva Mendoza Araceli Yoselín	Asistente TI

2.3.3.2.3 Definir los conocimientos, información o datos se van a poner en la VPN

Los conocimientos información o datos que se van a poner en la Red Privada Virtual, está conformada por toda la información que maneja la empresa en sus diferentes áreas y que es de vital importancia para el correcto desarrollo de sus actividades diarias, además, se almacena información que le concierne única y exclusivamente al personal de la alta dirección (cítese, por ejemplo, datos personales del recurso humano). Toda la información estará contenida y disponible dentro del servidor institucional debidamente organizada y con una correcta distribución de acuerdo a cada una de las áreas que forman parte de la organización. La información está sujeta a permisos específicos de acceso con la finalidad de garantizar que cada quien acceda únicamente a los datos que son de su incumbencia.

Las principales áreas que forman parte de la organización y que sirven como base para distribuir y organizar la información de forma adecuada son:

- Administración
- Contabilidad
- Operaciones
- Logística
- EHS
- Tecnologías de Información
- Medicina Ocupacional
- Sistema Integrado de Gestión

A continuación, se presenta el esquema básico de distribución de información por área:

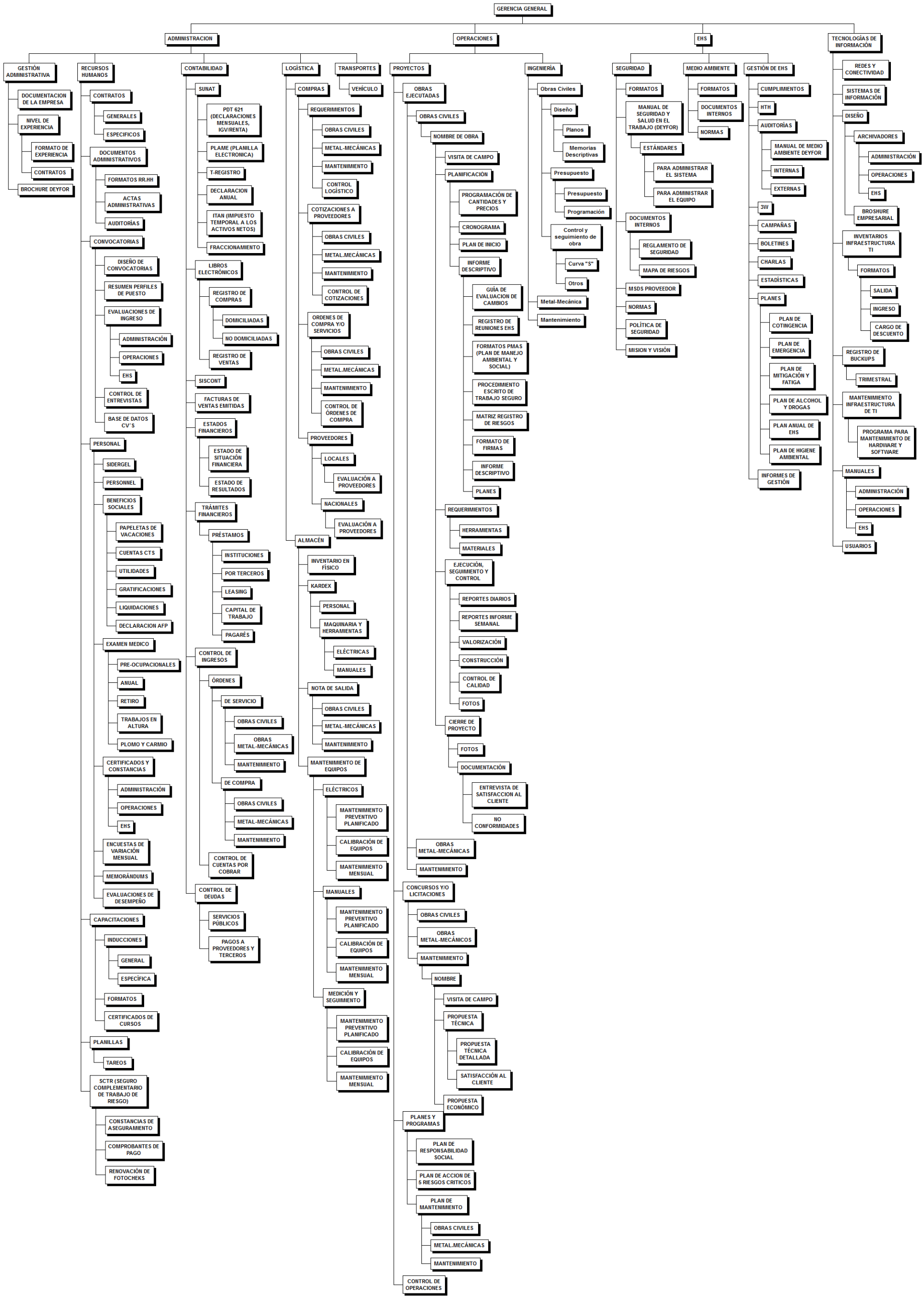


Fig. 21: EDT Información Deyfor E.I.R.L.

2.3.3.2.4 Especificación de si la VPN va a ser utilizada para comercio global

Para el presente proyecto de investigación, la implementación de la VPN no está destinada a fines de comercio global, sino únicamente a garantizar una comunicación efectiva, oportuna y segura entre los involucrados dentro de la organización.

2.3.3.2.5 Definir si se instala o no una extranet

El presente proyecto no contempla por el momento la instalación una extranet; sin dejar de lado, claro está, que se debe considerar la posibilidad que en futuras investigaciones se contemple esta opción como una mejora que repotencie las prestaciones de la VPN.

2.3.3.2.6 Determinar si la organización posee la capacidad técnica adecuada para mantener e instalar una Red Privada Virtual

En la actualidad Deyfor E.I.R.L. cuenta con una infraestructura de red debidamente instalada y correctamente equipada con dispositivos (Servidor, Switch, Router y cableado estructurado) que poseen la capacidad de soportar la implementación de soluciones orientadas a reutilizar la infraestructura pública de red como es el caso de una VPN. Partiendo de esta premisa, se concluye que la organización garantiza la condición ideal que permite la posibilidad de instalar y mantener un Red Privada Virtual; además, la organización cuenta con un equipo de profesionales debidamente capacitados y serán ellos quienes se encarguen de garantizar el correcto uso y funcionalidad a la Red Privada Virtual.

A continuación se muestra un esquema de red de la situación actual de la empresa, dicho esquema ha sido elaborado, para ayudar al entendimiento del estudio ya que no se contaba con documentación alguna.

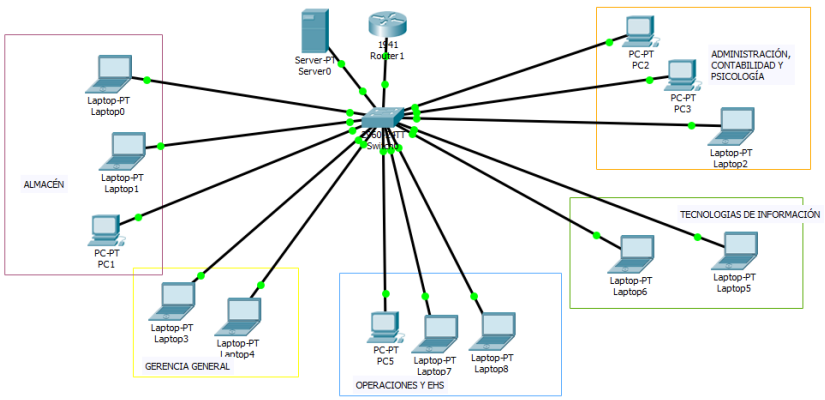


Fig. 22: Esquema de red actual de la empresa Deyfor E.I.R.L

Es importante señalar también que el número de PCs conectados a la red interna de la organización es en la actualidad de 13, estos son los que están conectados de manera fija, y otras 15 PCS que se encuentran en los puntos de trabajo de la organización, para los cuales, se notó la necesidad de la implementación de la red VPN.

2.3.3.2.7 Determinar cómo se integrará la Red Privada Virtual con la red de la compañía

La Red Privada Virtual se integrará a la red de Deyfor E.I.R.L., a través del uso de la infraestructura pública de red. En el caso de los colaboradores que se encuentran fuera de las instalaciones de la sede central organizacional, ya sea en operaciones de minera Yanacocha o desde su casa; estos harán uso del internet, es decir, cualquier usuario que se posee permisos suficientes para acceder a la VPN puede hacerlo desde cualquier punto únicamente ingresando sus credenciales de acceso.

A continuación, se muestra un esquema de la integración, de la actual red con lo que sería la red VPN.

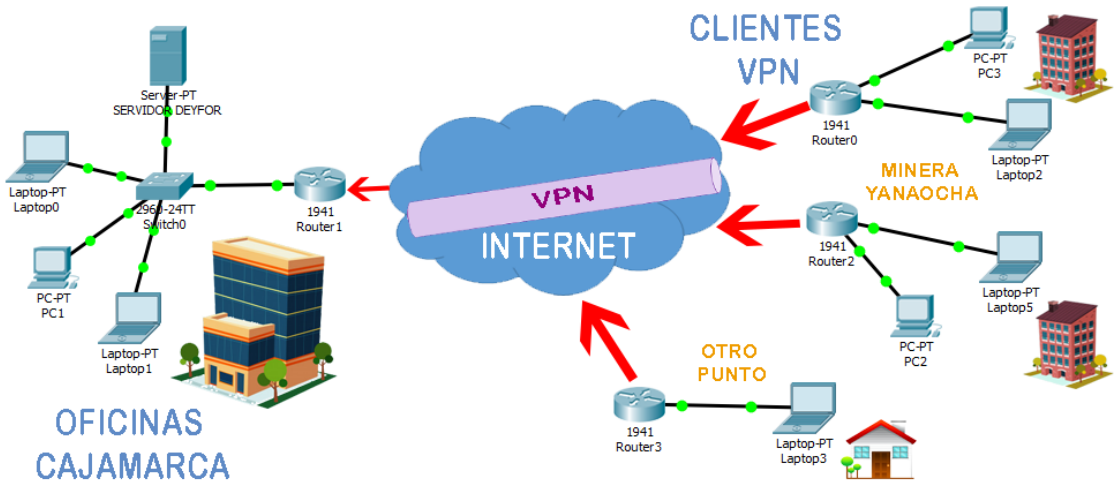


Fig. 23: Esquema de Integración de la Red VPN con la red local de Deyfor E.I.R.L.

2.3.3.2.8 Especificación de resultados esperados

Se desea que todos los usuarios de la red VPN puedan:

1. Acceder simultáneamente a la información almacenada en el servidor de manera segura a través del cifrado de datos.
2. La autenticación obligatoria mediante credenciales con altos niveles de encriptación.
3. Poder obtener y almacenar información de acuerdo a sus necesidades y responsabilidades con la finalidad de facilitar sus tareas diarias sin la necesidad

de estar necesariamente presentes de manera física dentro de las instalaciones de la organización.

4. Proveer a la organización la capacidad de poder controlar el tráfico de la red a la vez que proporciona características de seguridad importantes, como por ejemplo la autenticación y la privacidad de datos.
5. Proporcionar a la organización el control de la mayor cantidad de información que manejan, los colaboradores a diario, en la realización de sus actividades.

2.3.3.2.9 Elección del tipo de seguridad que se utilizará en la red privada virtual

Para la elección del tipo de protocolo a utilizar, se ha elaborado la siguiente tabla, para realizar una comparación de los protocolos existentes y que se pueden tomar en cuenta para la implementación de un red VPN.

Tabla 3: Comparación entre protocolos VPN

Indicadores	PPTP	L2TP	OpenVPN	SSTP	IKEv2
Encriptación VPN	128 bits	256 bits	160 bits 256 bits	256 bits	256 bits
Seguridad	Normal	Seguro	Muy Seguro	Muy Seguro	Extremadamente seguro.
Velocidad	Rápido debido a la encriptación más baja.	Necesita más proceso de la CPU para encapsular los datos dos veces.	Protocolo con mejor rendimiento. Velocidades elevadas, incluso en conexiones con alta latencia y a grandes distancias	Negociar los parámetros entre dos entidades, por ende su proceso es más lento.	Dinámico en volver a conectar durante los momentos de pérdida temporal de conexión a Internet
Compatibilidad	Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	Compatible con la mayoría de los sistemas operativos de ordenadores de sobremesa y dispositivos Android móviles y tabletas.	Solo funciona en plataformas Windows.	Compatibilidad nativa para dispositivos con Windows, iOS y Blackberry.
Estabilidad	Funciona bien en la mayoría de puntos de acceso Wi-Fi, muy estable.	Compatible con dispositivos NAT.	La más fiable y estable, incluso tras routers inalámbricos, en redes no fiables, y en puntos de acceso Wi-Fi.	Este protocolo SSTP ofrece un túnel cifrado mediante el protocolo SSL/TLS, de modo que cuando un cliente establece una conexión VPN basada en SSTP	Los cifrados usados para generar las claves Phase1 son AES-256-GCM para cifrado, junto con SHA2-384 para garantizar la integridad, combinado con PFS (Perfect Forward Secrecy) con claves.
Facilidad de Implementación	PPTP es un protocolo rápido, fácil de usar.	Fácil de implementar.	Requiere software de terceros	Fácil de implementar .	

De la comparación anterior, podemos apreciar varios tipos de protocolos; como se mencionó anteriormente en esta ocasión se ha optado por escoger el protocolo PPTP, sobre los demás en mención; en base a que dicho protocolo cuenta con una encriptación de 128 bits, seguridad normal, compatibilidad con cualquier dispositivo, es estable y tiene facilidad de implementación; y además organización cuenta con los dispositivos (tanto cliente como servidor) que ya cuentan este tipo de protocolo, por otro lado es importante señalar, que no se puede realizar el cambio de protocolo a estos dispositivos, ya que no se puede realizar la manipulación del software con el que cuentan. En esta ocasión lo que no se quiere es incurrir en gastos adicionales para la organización.

Por otro lado se puede proponer la implementación del protocolo SSTP, ya que para los entornos en los que se trabaja que son Windows; este protocolo proporciona seguridad a nivel de transporte con negociación de claves, encriptación y verificación de la integridad del tráfico y tiene soporte nativo solo para Windows.

2.3.3.2.10 Especificar cómo se construirá la VPN

Para la especificación de la construcción de la Red Privada Virtual en Deyfor E.I.R.L. se ha llevado a cabo los siguientes pasos.

1. **Estudio de Red:** Se hizo un estudio detallado de la red, para evaluar el estado de ésta:
   - Se determinó que se cuenta con una conexión de internet de 15 gb. Con una buena velocidad de subida y de descarga como se muestra a continuación.

Fig. 24 Muestra de la velocidad de Internet de Deyfor E.I.R.L.

- Se cuenta también puntos de red con acceso en todas las oficinas de la organización, tanto con la red cableada como con la red wifi.

Fig. 25: Switch que muestra todas las salidas de la red Cableada

Fig. 26: Oficina de Deyfor que muestra la conexión cableada

2. Estudio de la infraestructura de Red:

Se realizó la revisión del router, y se identificó 2 routers:

- 1 router Cisco modelo DPC-3825, instalada por la empresa proveedora de internet.

Tabla 4: Tabla de Características Router Cisco DPC-3825

ROUTER	CARACTERÍSTICAS

	- **Tecnología de conectividad:** wired, Wireless. - **Protocolo de interconexión de datos:** Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n. - **Protocolo Inalámbrico:** 802.11b/g/n - **Protocolo de direccionamiento:** RIP-1, RIP-2, static IP routing. - **Interfáz Proporcionada:** USB 2.0, modem, network. LAN, USB 2.0, antena. F connector, RJ-45.

- 1 router Microtik Routerboard RB 3011 Ui AS–RM.

Tabla 5: Tabla de Características Router Microtik Routerboard RB 3011

ROUTER	CARACTERÍSTICAS
	- **Puertos Ethernet** 10/100/1000: 10. - **Periféricos:** Puerto serial RJ45. - **CPU frecuencia nominal :** 1.4 GHz - **CPU nº de núcleos:** 2 - **Arquitectura:** ARM 32 bits. - **UPC:** IPQ-8064.

Este router cuenta también con un software llamado Winbox, el cual es una pequeña utilidad del router mencionado, para realizar la administración de este por interfaz gráfica; dentro de otra utilidad con la que cuenta éste router, es que a través de la interfaz gráfica, se puede realizar la creación de una red VPN, a través de la configuración de usuarios y el uso del protocolo pptp.

Es importante señalar, que se ha aprovechado al máximo os equipos con los que cuenta la organización, pero existen otros routers los cuales

proporcionan una infraestructura más segura para la implementación de un red VPN [43], los cuales se detalla a continuación:

Tabla 6: Tabla de Características Router Linksys WRT3200ACM

ROUTER	CARACTERÍSTICAS
Linksys WRT3200ACM 	- 4x Gigabit Ethernet, 1x USB 3.0, 1 x ESATA/USB 2.0 - Con tecnología MU-MIMO para proporcionar unas velocidades Wi-Fi ultrarrápidas. - Cuenta con un firmware DD-WRT para configurar tu VPN sin mucho problema. Tiene un excelente rendimiento. - Puertos eSATA, USB 3.0 y USB 2.0 para conectar todo tipos de dispositivos y 4 antenas de alto rendimiento para una cobertura inalámbrica máxima

Tabla 7: Tabla de Características Router Asus RT-AC5300

ROUTER	CARACTERÍSTICAS
Asus RT-AC5300 	- 4 x Gigabit Ethernet, 1 x WAN, 1 x USB 2.0, 1 x USB 3.0 - Tecnología Broadcom NitroQAM con hasta 4334 Mbps en las dos bandas de 5 GHz y hasta 1000 Mbps en la de 2,4 GHz. - Tri-Band Smart Connect selecciona automáticamente la frecuencia más rápida disponible para cada dispositivo tomando como referencia la velocidad del dispositivo, la potencia de la señal y cuán ocupada está cada banda. Tiene un

	excelente firmware, también para configurar tu red VPN en todo tu lugar.

Tabla 8: Tabla de Características Router Asus RT-AC86U

ROUTER	CARACTERÍSTICAS
Asus RT-AC86U 	- 5 x Gigabit LAN, 1 x USB 2.0, 1 x USB 3.0 - Seguridad de grado profesional: AiProtection con tecnología Trend Micro protege todos los dispositivos conectados . - Zona de cobertura ampliada: las antenas de alto rendimiento, ASUS AiRadar y Range Boost ayudan a cubrir las zonas difíciles, y MU-MIMO maximiza el rendimiento al conectar múltiples dispositivos. - Para conectarte a tu red VPN, puedes instalar un firmware de terceros, pero el que viene de fabrica es perfecto para usar con tu red VPN.

Tabla 9: Tabla de Características Router D-Link DIR-885L

ROUTER	CARACTERÍSTICAS

D-Link DIR-885L 	- 4x Gigabit Ethernet, 1x USB 3.0. - MU-MIMO: rendimiento WiFi hasta 4 veces superior - Puertos LAN y WAN Gigabit (10/100/1000 Mbps), para aprovechar al máximo la velocidad contratada con el operador de Internet - Con opción también para gaming, y por supuesto para conectarte a tu red VPN.

El contar con algunos de routers citados, establecería una infraestructura con mayor seguridad, y una respuesta ante fallos muchos más efectiva; insistiendo en el motivo de la implementación de esta VPN, se está trabajando con la infraestructura con la que ya cuenta la organización para no incurrir en costos.

Se elaboró un plano de red:

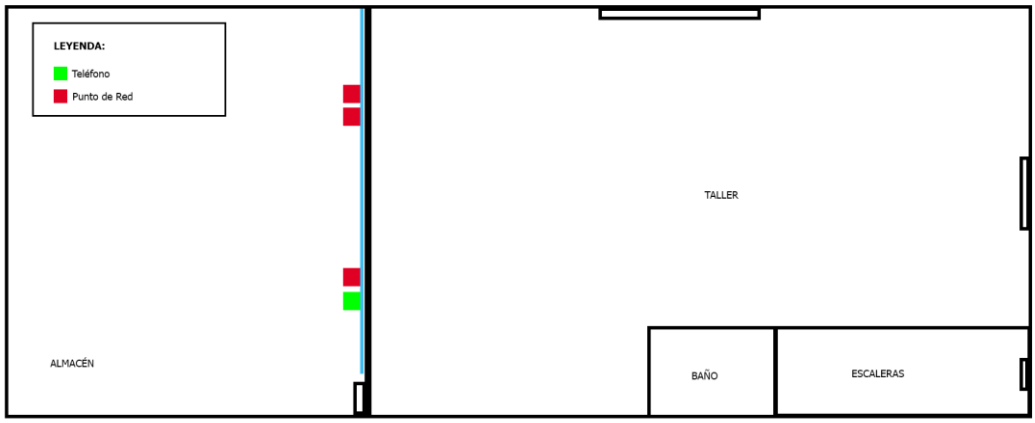


Fig. 27: Plano de Red Primer Nivel de las Oficinas Deyfor E.I.R.L.

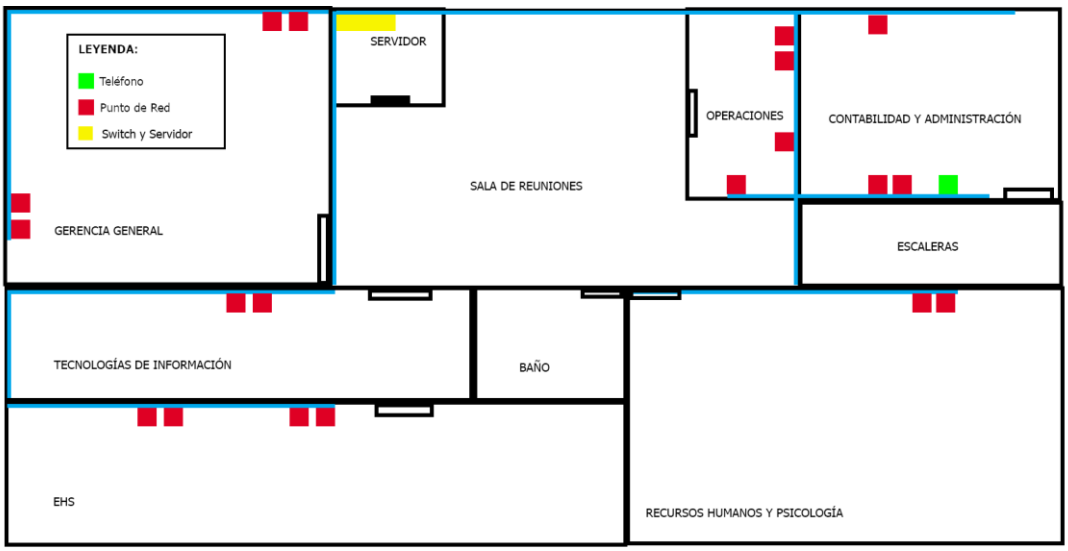


Fig. 28: Plano de Red Segundo Nivel de las Oficinas Deyfor E.I.R.L.

- Después de la elaboración del plano de red, se determinó que Deyfor E.I.R.L. cuenta con 22 puntos de red cableada, y 2 puntos telefónicos; determinando que en todas las oficinas de trabajo de la organización se cuenta con red de conexión por cable, con un número 2 puntos o superior.
- Además de que, en cada oficina de la organización, existe una buena conexión por wifi.
- La red se encuentra en 2 subredes, la red cableada se encuentra distribuida desde la ip 192.168.20.1, y la red por wifi está distribuida desde la ip 192.168.30.1.

3. **Análisis de conectividad desde otro punto:** Para que los usuarios puedan acceder a la red a través de la VPN, es necesario que la red local cuente con una IP pública, para contar con una salida y entrada desde otro punto. Ésta IP tiene que ser proveída por el proveedor de servicio de internet, de la operadora Claro.

2.3.3.2.11 Consideraciones legislativas en cuanto al cifrado de datos

Actualmente en Perú, aún no existe ningún tipo de reglamento, normativa o ley explícitos que regulen el cifrado de datos. No obstante, existe una directiva de seguridad, aprobada por Resolución Directoral Nº 019-2013-JUS/DGPDP, en el año 2013 por la Autoridad Nacional de Protección de Datos Personales (APDP) perteneciente al Ministerio de Justicia y Derechos Humanos que exige a los titulares de los bancos de

datos personales la implementación de medidas de seguridad adecuadas que les permitan el tratamiento de los datos personales que administran, preservando la confidencialidad, disponibilidad e integridad de aquellos, lo que, en buena cuenta, significa dar cumplimiento al marco normativo dado por la Ley de Protección de Datos Personales y su respectivo Reglamento [44].

La directiva orienta sobre las condiciones, los requisitos y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento, aprobado a través del Decreto Supremo Nº 003-2013-JUS, en materia de medidas de seguridad de los bancos de datos personales. Es en el apartado 2.3.4.6 (de la directiva) dónde se menciona que la información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad, asimismo, como complemento a esto, en el apartado 2.3.5.3 de la directiva (sobre el tratamiento no autorizado del banco de datos personales) se hace mención al transporte electrónico de datos personales en forma cifrada, lo cual puede realizarse mediante el cifrado de la información antes de su transmisión o mediante el uso de protocolos de comunicación cifrados (Ejemplo: VPN, correo electrónico cifrado, FTP seguro, entre otros) [44].

2.3.3.3 *Estudio y análisis*

La planificación y diseño de una VPN debe realizarse con cuidado, ya que no solo afecta la conectividad entre las diferentes partes de la organización y la seguridad de sus datos, sino que también puede afectar el tráfico de la red en cada sitio.

En esta etapa de ejecución del presente proyecto de tesis, se recogen los requisitos base que debe cumplir la VPN una vez finalizada su implementación dentro de la empresa Deyfor. Además, se contempla una serie de consideraciones antes de iniciar con la implementación del proyecto. Estas actividades se detallan a continuación.

- El requisito base que cumple la VPN al finalizar su implementación es la transmisión segura y correcta de información (garantizar la seguridad de la información en todo sentido) entre usuarios que pertenecen al recurso humano de Deyfor.
- Cada uno de los usuarios pertenecientes a la VPN cuentan con una clave de acceso debidamente encriptada y que cumpla con las medidas de seguridad

requeridas; y asignada la información apropiada para el uso y necesidad que presente. El acceso a la información de los colaboradores está manejada de acuerdo a un documento, evaluado por la gerencia, el cual distingue el acceso de información entre dichos colaboradores. Este documento no puede ser presentado en dicha tesis, pues cuestiones de seguridad de la organización.

- La VPN permite además de acceso a información clave de la empresa, la posibilidad de realizar teleconferencias, es decir, un usuario que no se encuentra físicamente dentro de las instalaciones, pueda establecer un lazo de comunicación con otros usuarios mediante un canal audiovisual.
- La VPN se configura única y exclusivamente en los equipos pertenecientes a la empresa, quedando terminantemente prohibido el acceso a usuarios mediante el uso de sus dispositivos electrónicos personales.
- En cuanto al rendimiento y la velocidad de la red VPN esta será definida por el ancho de banda del ISP.
- En cuanto a la instalación de la red VPN, se considera factible, ya que la organización cuenta con los recursos necesarios para ello.

El protocolo punto a punto (PPTP) cumple con todos estos requisitos mínimos, es por ello, que se opta por utilizarlo en la implementación de la VPN.

2.3.3.4 *Elección de la plataforma*

Deyfor E.I.R.L cuenta con un servidor HP ProLiant DL380 Gen9.

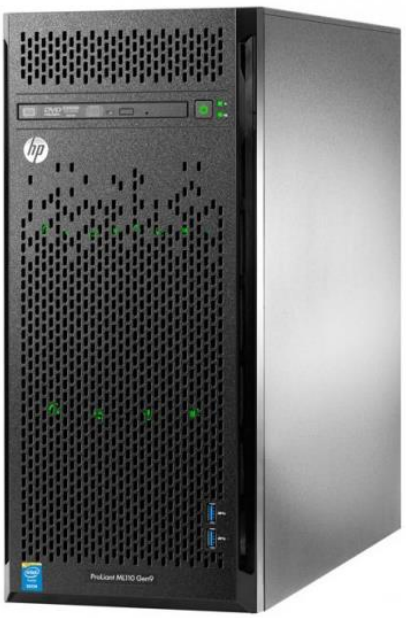


Fig. 29: Imagen Servidor ProLiant DL380 Gen9

Este ofrece lo último en rendimiento y capacidad de expansión. Su fiabilidad, capacidad de servicio y disponibilidad casi continua, junto con el respaldo de una garantía integral, lo hacen perfecto para cualquier entorno de servidores. Diseñado para reducir los costes y la complejidad, aprovecha los procesadores E5-2600 v4 más recientes de Intel con un 21% de aumento del rendimiento, además de la más reciente HPE SmartMemory DDR4 a 2400 MHz, que admite 3 TB y hasta un 23% de aumento del rendimiento. Admite SAS[18] de 12 Gb/s, NIC de 40 Gb con una amplia variedad de opciones informáticas. Memoria persistente HPE, la primera NVDIMM del mundo optimizada en ProLiant que ofrece niveles sin precedentes de rendimiento para bases de datos y cargas de trabajo de análisis. Ejecuta todo, desde las aplicaciones más básicas a las cruciales, y puede implementarse con seguridad [45].

[18] Las unidades de disco duro SAS (Serial Attached SCSI) son las más utilizadas a nivel empresarial por su alto rendimiento. La mejor ventaja de esta interfaz es que ofrece almacenar y leer un gran volumen de datos trabajando a altas velocidades.

Fig. 30: Equipos de la red de la organización

El servidor empresarial opera con Windows Server 2012 R2. Asimismo, todos los equipos (portátiles y desktops) que utiliza el recurso humano para desempeñar sus funciones diarias opera con el Sistema Operativo Windows 10 Profesional; por ende, todo el software y/o aplicaciones que se utiliza es compatible con este SO. Dentro del servidor se encuentra instalado y desplegado el ERP (Odoo V10 [19]) que brinda el soporte necesario a las operaciones logísticas dentro de la empresa.

Windows Server 2012 R2, ofrece algunas novedades dignas de mención, estas se listan a continuación [46]:

[19] Sistema de gestión empresarial (ERP) de código abierto y sin coste de licencias que cubre las necesidades de las áreas de: Contabilidad y Finanzas, Ventas, RRHH, Compras, Proyectos, Almacenes (SGA), CRM y Fabricación entre otras.

- **Carpetas de Trabajo.** Para lidiar con la tendencia Bring You Own Device (Utilice su propio dispositivo móvil en el trabajo), el sistema permite utilizar el servidor corporativo para servir ficheros de una manera unificada, al modo “Dropbox”. De esta manera se obtiene un entorno seguro, y en la empresa, que además de reducir el espacio total de ficheros gracias a la deduplicación, permite el intercambio y el compartir archivos de manera segura y controlada.
- **Estado deseado de Configuración (DSC).** Windows Server 2012 R2 incluye DSC (Desired State Configuration), que auto provisiona y orquesta, ciertas acciones a los servidores y equipos que se le indique de la Organización. DSC permite instalar o eliminar Roles y Características; administrar Entradas del Registro de Windows; administrar Ficheros y Directorios; iniciar, detener o administrar Procesos y Servicios; administrar Grupos Locales y Cuentas de Usuarios; lanzar Scripts; etc.
- **Almacenamiento nativo por niveles**. Mientras se disponga de discos de estado sólido (SSD) y unidades tradicionales de disco duro (HDD), permite unir ambos discos a un espacio global de almacenamiento, donde un motor de almacenamiento diferenciará entre ambos tipos de almacenamiento. Automáticamente, Windows Server 2012 R2 moverá los bloques que se leen con más frecuencia al almacenamiento SSD, mientras que los bloques menos accedidos se mantendrán en el almacenamiento tradicional HDD.
- **Fijación de almacenamiento**. Define qué tipo archivos se ejecutarán siempre sobre almacenamiento SSD y cuáles sobre disco tradicional HDD. También podemos definir configuraciones para que sean pseudo-persistentes, que estén sobre SSD y se muevan a HDD, en caso de no ser usado durante un periodo de tiempo.
- **Almacenamiento en caché por reescritura (Write-Back).** Es la opción de usar una caché writeback persistente, que hará que todas las operaciones de escritura las ejecute sobre SSD, para posteriormente mover a un almacenamiento HDD. Esta configuración ayudará a ganar rendimiento.
- **Hyper-V en Windows Server**. Existen numerosas ventajas y novedades, y también nuevos límites en cuanto a procesadores, memoria, cantidad de máquinas virtuales, etc. Algunas de las funcionalidades agregadas son: disco virtual compartido, calidad de servicio en almacenamiento, nueva generación de máquinas virtuales, modo sesión mejorada, y activación automática de máquinas virtuales.

- **Deduplicación en Windows Server 2012 R2 y Compresión**. La deduplicación[20] de datos es una nueva característica disponible en Windows Server 2012 R2. Con la deduplicación se logra reducir el espacio que se usa en disco guardando únicamente una copia de los datos que son idénticos dentro de un volumen. Por otra parte, son muchas las ventajas que brinda el usar deduplicación en las tareas de backup con soluciones como Veeam Backup & Replication. Se debe tener en cuenta que Windows Server 2012 R2 no deduplica archivos comprimidos. Es por ello que se tiene que configurar bien las tareas de Veeam Backup & Replication para aprovechar esta característica al máximo. No obstante, es interesante saber que los archivos deduplicados tienen al final menor tamaño que uno comprimido. Utilizando deduplicación se logra liberar de las cargas y picos de CPU diarios, a la Infraestructura de Veeam Backup & Replication, ya que se lanza las tareas sin compresión, o con la opción de Dedup-Friendly.

A continuación, se realiza una descripción de las prestaciones esenciales que ofrece Windows 10 en su versión Profesional [47].

- Permite la conexión al dominio de la empresa o escuela, o a Azure Active Directory, para usar archivos de red, servidores, impresoras y mucho más.
- Garantiza un cifrado mejorado. Gracias a la funcionalidad de BitLocker, se tiene la posibilidad de proteger los datos con administración del cifrado y la seguridad.
- Permite el inicio de sesión remoto. Windows 10 te permite establecer conexiones a través de escritorio remoto para iniciar sesión y usar la PC Pro en casa o durante los desplazamientos.
- Ofrece la posibilidad de instalar y ejecutar máquinas virtuales con Hyper-V para que se pueda ejecutar más de un sistema operativo a la vez en el mismo PC.
- Windows 10 te permite crear una sección propia y privada de aplicaciones en la Tienda Windows para acceder cómodamente a las aplicaciones de la empresa

2.3.3.5 *Propuesta de solución*

[20] La deduplicación de datos es una técnica especializada de compresión de datos para eliminar copias duplicadas de datos repetidos; es decir, compresión inteligente de datos.

La VPN que se implementa dentro de Deyfor, persigue la meta primordial de permitir el envío y recepción de información clave para el desarrollo de actividades de manera segura y confiable. No obstante, cuando la VPN esté implementada en su totalidad, ésta permite al recurso humano de la organización realizar teletrabajo y, además, navegar por la red sin ningún tipo de restricción regional (ofrece la posibilidad de realizar descargas P2P).

Actualmente, Deyfor cuenta con la infraestructura de red necesaria para implementar VPN; un router con la capacidad de soportar el tráfico de datos mediante VPN, cableado estructurado dentro de las instalaciones, internet de alta velocidad proporcionada por el ISP Claro Perú, un servidor de altas prestaciones operando con SO Windows Server 2012 R2.

Se estima que en promedio los usuarios que usen la VPN entre los 30 a 45 usuarios, ya que el número de colaboradores que tienen acceso al manejo de datos de la empresa en la actualidad son de 45; y se evidencia un crecimiento, con respecto al año anterior. Por ende, el tráfico que pase por la misma depende principalmente del tipo de información que cada usuario comparta o haga circular a través de la red. El ISP no tiene control sobre el tráfico de datos que circula por la VPN, por tanto, los usuarios tienen libertad de transferir información ilimitada.

Por otro lado, también es necesario aclarar que el número de conexiones VPN que soporta el router es superior a las 100 conexiones simultáneas, por lo tanto, se estima que nuestra red VPN podría aguantar un número de conexiones simultáneas mayor a 100.

Tabla 10: Tabla Muestra el N° de Colaboradores Deyfor en diferentes años

N° de Colaboradores del Saff Deyfor E.I.R.L.	
Año 2015	25
Año 2016	39
Año 2017	38

Los usuarios se autentican en la VPN usando contraseñas que cumplen con las medidas de encriptación y seguridad requeridas. Estas contraseñas contienen combinaciones de números, letras, mayúsculas, minúsculas y caracteres especiales con la finalidad de garantizar un alto nivel de seguridad y, por ende, evitar que sean fácilmente descifrables por atacantes.

2.3.3.6 *Seguridades*

Según Sommerville [48], la Seguridad, se refiere a la capacidad de un sistema para resistir ataques; es una propiedad muy compleja que no se puede medir fácilmente. Los ataques pueden ser ideados de forma que no fueron predichos por los diseñadores del sistema y así vencer las protecciones incorporadas. Los sistemas cuentan con propiedades emergentes no funcionales las cuales se relacionan con el comportamiento del sistema en su entorno operacional: Fiabilidad, rendimiento seguridad y protección. Estas propiedades con críticas para sistemas basados en computadora, pues las fallas para lograr un mínimo definido en dichas propiedades suelen hacer inútil al sistema, pudiendo no necesitar de alguna funcionalidad dada, que también sería aceptable; a esto se le suma el hecho de que un nivel de seguridad demasiado alto puede traer consigo un sistema lento, con altas probabilidades de rechazo.

Las propiedades como la seguridad y la protección no son mensurables. Aquí, usted no está interesado simplemente por los atributos que se relacionan con el comportamiento del sistema, sino también con el comportamiento no deseado o inaceptable. Un sistema seguro es aquel que impide el acceso no autorizado a sus datos. A pesar de ello, resulta claramente imposible predecir todos los posibles modos de acceso y prohibirlos de forma explícita. Por consiguiente, sólo sería posible valorar dichas propiedades “no se debe”. Esto es, sólo se sabe que un sistema no es seguro cuando alguien trata de penetrarlo [48].

Acorde con la descripción anterior, para el caso de Deyfor E.I.R.L.; La administración de seguridad no solo incluye la autenticación de usuarios desde otras ubicaciones y el control de sus derechos de acceso, sino también la administración de las claves criptográficas asociadas con los dispositivos VPN, con lo cual se garantiza seguridad para el manejo de información.

La información de la empresa se encuentra agrupada y debidamente diferenciada por área, de tal modo que el personal pueda acceder única y exclusivamente a la información que le compete al área a la cual pertenece. Los permisos que se le otorgan a cada uno de los usuarios dependen del rango jerárquico que posea dentro de la estructura orgánica de la empresa, es decir, a mayor rango mayor nivel de control sobe la información (lectura, escritura).

El protocolo PPTP (protocolo usado en la elaboración de la VPN en la presente tesis) puede usar PPP y sus opciones de cifrado negociables (incluidos DES y Triple DES) para cifrar datos, Microsoft ha incorporado un método de cifrado llamado Microsoft Point-to-Point Encryption (MPPE) para su uso con túneles PPTP. MPPE utiliza el algoritmo RC4 con claves de 40 bits o de 128 bits, dependiendo de las restricciones de exportación.

El router usado en la implementación de la VPN posee la característica de producto de cifrado basados en hardware y, por ende, es menos vulnerable al ataque físico, lo que reduce las posibilidades de que las claves del dispositivo se vean comprometidas y, por lo tanto, la necesidad de intercambiar nuevas claves entre las puertas de enlace.

Se cuenta con un firewall debidamente implementado para la protección de la información que se maneja dentro de la red VPN, o también llamado corta fuego, el cual bloquea cualquier intento de acceso no autorizado a dispositivos internos privados de nuestra red de datos (LAN) desde las conexiones externas de internet, además también un modo de filtrar la información que se comunica a través de la conexión de red.

A continuación, se presenta una gráfica sobre la seguridad de Red.

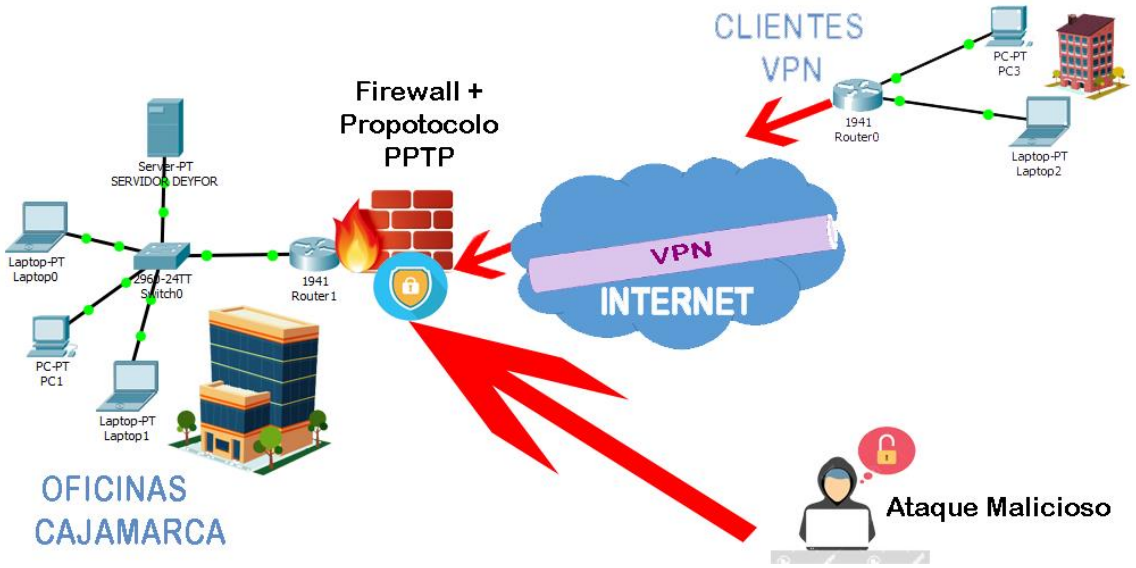


Fig. 31: Gráfica de seguridad de Red de la VPN de Deyfor E.I.R.L.

Por otro lado también es bien sabido que la fuga de información también parte de los colaboradores de la organización, para lo cual se ha elaborado una política de Confidencialidad, de la cual damos muestra un extracto en anexo9.

Además también se ha elaborado una Política de Seguridad de información, para establecer los puntos clave a proteger de los activos de información con los que cuenta la organización, parte de esta política podemos encontrarla en anexo10.

Para garantizar la transmisión de información respecto al fallo de la red VPN, y otros puntos se ha elaborado un Plan de contingencia, del cual se detalla en el punto siguiente.

Para el mejoramiento de la seguridad en cuanto a fallos de la red VPN se recomienda, hacer uso de otra infraestructura, como un router más robusto para la implementación de la misma, por ejemplo alguno de routers mencionados en el apartado **2.3.3.2.10,** consideración 2, Estudio de la infraestructura de Red.

En la ciudad de Cajamarca, hasta la elaboración del presente informe, aún no se han registrado incidencias de robo de datos corporativos a gran escala (tampoco existen informes documentados donde se indique que se ha perdido datos por intromisión de agentes no autorizados en los sistemas) por parte de atacantes que buscan vulnerabilidades de los sistemas para apropiarse de los mismos de manera ilegal y realizar tareas que perjudican y entorpecen el desarrollo de las actividades diarias en la organización. Aun así no se puede descartar, cualquier ataque o vulnerabilidad a la información que se comparte a través de la red VPN de la organización, por ello se ha

definido otros puntos importantes para la seguridad de esta, los cuales se pueden aplicar más adelante:

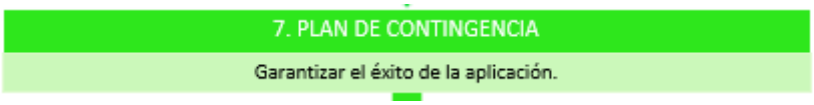
- La seguridad de una VPN debe ir más allá que simplemente controlar al acceso seguro a los recursos de la red. También debe proveer mecanismos para administrar la implementación de pólizas de seguridad que garanticen el desarrollo exitoso de una VPN.
- La seguridad de una VPN también debe establecer una conexión cifrada a una oficina LAN remota, y comprobar los niveles de seguridad que debe cumplir un equipo remoto que desea conectarse a la red corporativa debe ser lo más amplia posible.
- Es necesario establecer también un sistema de chequeo de status de seguridad de los equipos remotos conectados mediante VPN a la red corporativa, con suficiente amplitud como para abarcar productos y sistemas de seguridad no corporativos, sino elegidos por el trabajador remoto.
- Se deben clasificar las amenazas de seguridad de las redes, de acuerdo a las siguientes posibles amenazas:
    - **Amenazas no estructuradas**: Amenazas que pueden ser originadas por personas inexpertas, que utilizan herramientas de piratería en internet; conocidos como **script kiddies**.
    - **Amenazas estructuradas:** Amenazas que son causadas por persona con conocimientos en redes, conocen mucho de programación y crean programas capaces de penetrar sistemas; conocidos como **hackers y crackers**.
    - **Amenazas externas:** Amenazas causadas por personas ajenas a la red de la organización, que pueden entrar por medio del internet.
    - **Amenazas internas:** Amenazas cuadas por personas con acceso autorizado a la información, puede tratarse de algún colaborador de la organización.
- Se deben clasificar los ataques de seguridad de las redes, de acuerdo a las siguientes posibles ataques:
    - **Sniffers**: Este ataque tiene lugar cuando el usuario no autorizado utiliza un programa llamado **snnifer** o husmeador con el cual puede leer todos los paquetes que circulan por la red con lo que se puede tener acceso a información privada.
    - **Integridad de Datos**: Este ataque tiene lugar cuando alguien modifica o corrompe los datos que circulan por una red. Un atacante

puede modificar los datos de un paquete sin que el remitente ni el receptor lo adviertan.

- **Ataques de contraseña**: Este problema tiene que ver con el control de acceso basado en contraseñas.
- **Ataque de denegación de servicio(DOS)**: Este ataque tiene lugar cuanto un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar acceso a usuarios.
- **Ataque hombre en medio:** Ataque producido por alguien que se interpone entre dos usuarios que se están comunicando, este captura y controla los paquetes de los usuarios sin que estos puedan ser advertidos.
- **Spoofing:** Este ataque se basa en el uso de las IP. La mayoría de las redes y sistemas operativos utilizan la dirección IP para identificar un equipo como válido en un red; los atacantes pueden utilizar programas especiales para construir paquetes IP que parezcan provenir de direcciones válidas dentro de una organización, para modificar, desviar o eliminar información.

- Se debe con tecnologías que se basen en técnicas criptográficas para dar seguridad a los datos, y utilizar algoritmos de encriptación simétrica o también llamado cifradores de bloque como:
  - **DES- Estándar de Cifrado de Datos (Data Encryption Standar):** Clave simétrica de 56 bits para encriptar datos en bloques de 64 bits.
  - **3DES- Estándar de Cifrado de Datos Triple:** Repite el algoritmo DES tres veces, esto significa que un texto cifrado tres veces usando tres claves distintas.
  - **RSA- Riverst Shamir Adleman:** Algoritmo de clave pública, su clave varía de 512 a 2048 bits, lo que lo hace altamente seguro. Utiliza un número conocido como módulo público para conseguir las claves pública y privada.
  - **Diffie- Hellman (D-H).** Este método de encriptación de la clave pública el cual permite a dos partes que se comunicas usando IPSec establecer una clave simétrica que sólo ellos conocen; aunque se estén comunicando sobre un canal inseguro.
- Se debe contar también con funciones de dispersión(hash) unidireccionales, que son utilizadas para la autenticación de datos y la creación de firmas digitales.

2.3.3.7 *Plan de contingencia*



El equipo de desarrollo e implementación seleccionado para la ejecución del presente proyecto cuenta con la capacitación y experiencia necesarias para que éste se ejecute de manera correcta y eficiente, minimizando al máximo los riesgos potenciales e inherentes que se presenten durante el tiempo que tarde su culminación.

Cajamarca ha alcanzado un nivel de desarrollo considerable gracias al auge de la minería, por ende, se convierte en un centro atractivo para las inversiones de capitales tanto nacionales como extranjeros. Es en este contexto en el que cabe mencionar que en el ámbito de soporte para VPN existen dos grandes ISP's (Claro y Movistar) con la capacidad y experiencia necesarias para ejecutar la tarea antes mencionada. Por tanto, existe el soporte suficiente y necesario para cualquier VPN que se instale en las empresas pertenecientes a la ciudad de Cajamarca.

Con la finalidad de facilitar futuras mejoras o superar cualquier tipo de incidencia de manera rápida y eficaz, todo el proceso de implementación de la VPN se plasma en documentos físicos y digitales. Los documentos resultantes son un manual de acceso al servidor para usuarios, un plan de contingencia.

En una eventual salida del equipo de desarrollo, la organización cuenta con la documentación necesaria que sirve de punto de partida o base para que el funcionamiento de la VPN sea completamente entendido por el nuevo equipo que se forme.

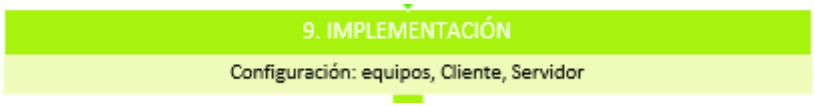
Si al finalizar el presente proyecto, cuando la VPN se encuentre en funcionamiento, y, se detecten fallos de seguridad y/o cualquier otro tipo de incidencias, existe la posibilidad de abordarlos de manera inmediata por el equipo a cargo del proyecto o, en su defecto, si el fallo lo amerita, se puede contactar al ISP encargado de brindar el soporte (vea anexo 8).

2.3.3.8 *Costos*

Los costos, en los cuales se ha incurrido en esta tesis, sólo se puede detallar el costo de la contratación de la IP pública al ISP, que tiene un costo de S/ 20.00 mensuales, adicionales al plan de internet y telefonía con los que cuenta la empresa; ya que se ha aprovechado al 100% el uso de la infraestructura con la que cuenta Deyfor.

En estricto cumplimiento con uno de los lineamientos contemplados en las políticas de la empresa Deyfor EIRL, otros costos inherentes a la implementación de la Red Privada Virtual no pueden ser detallados en la presente tesis.

2.3.3.9 *Implementación*



En este punto se describen todas las actividades de configuración de servidor, router y equipos desktops o portátiles que acceden a la VPN:

- Creación de las unidades organizativas y usuarios dentro del servidor de la organización (El servidor opera con Windows Server 2012 R2):

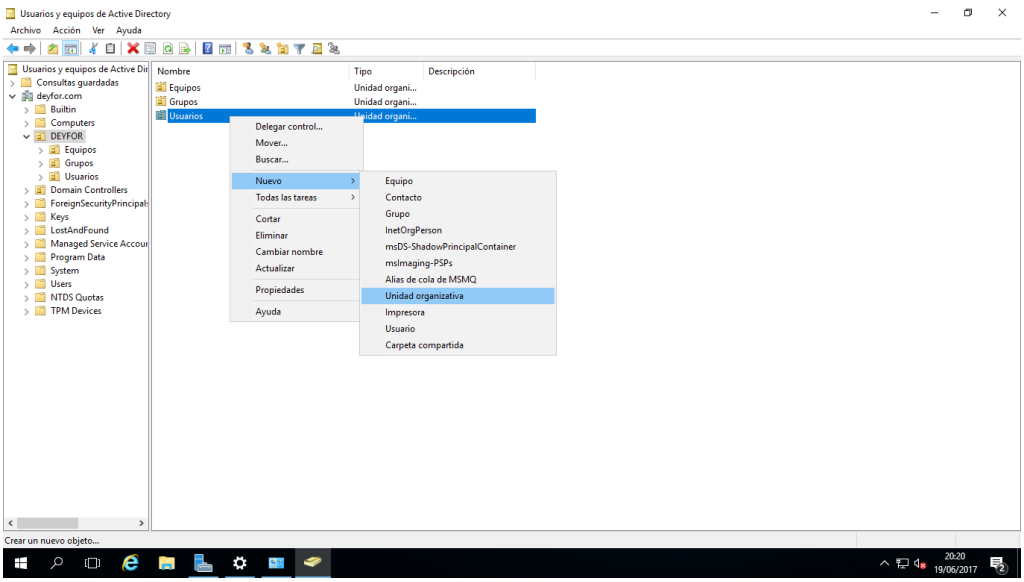


Fig. 32: Creación de una nueva unidad organizativa

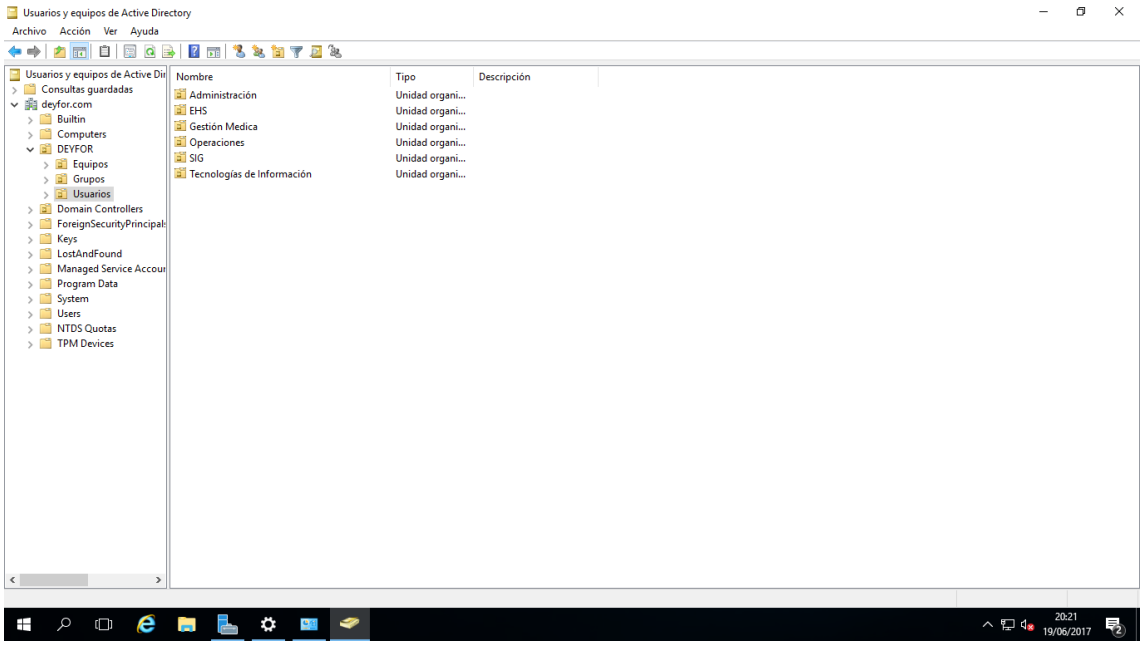


Fig. 33: Vista general de las unidades organizativas creadas dentro del Active Directory

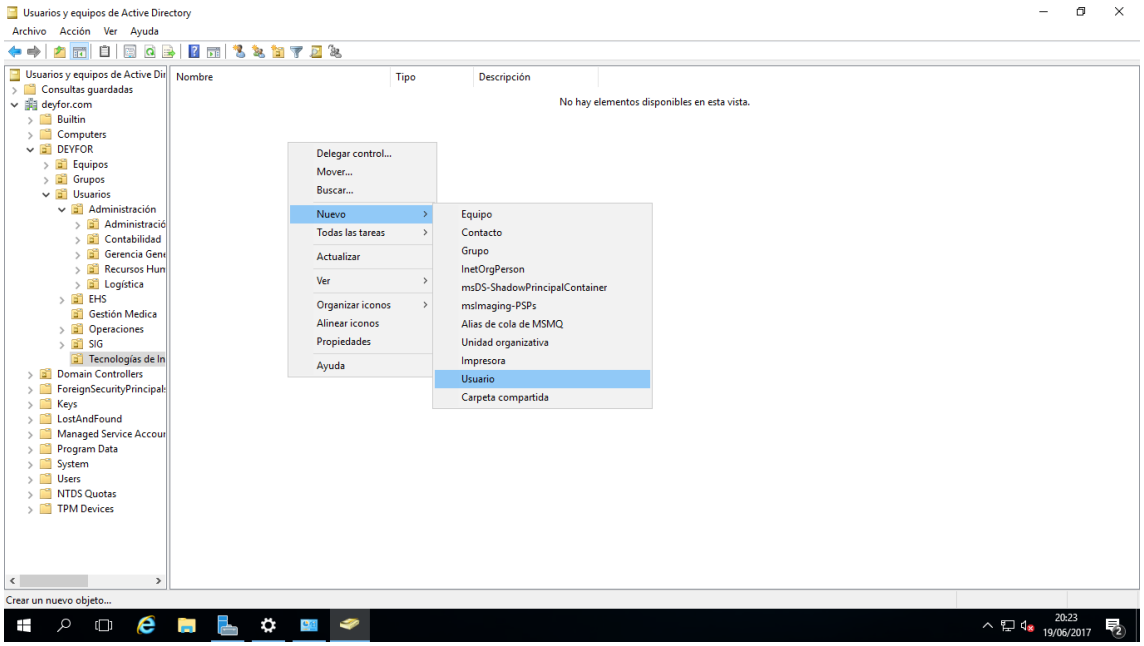


Fig. 34: Creación de un nuevo usuario de unidad organizativa

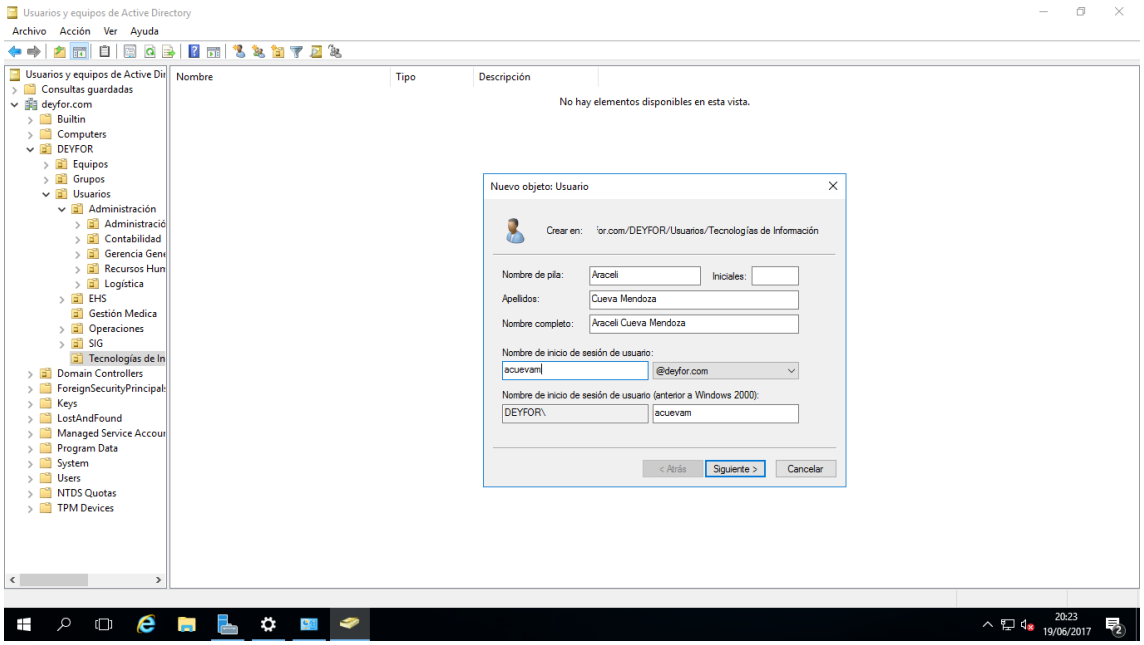


Fig. 35: Establecer datos generales del nuevo usuario

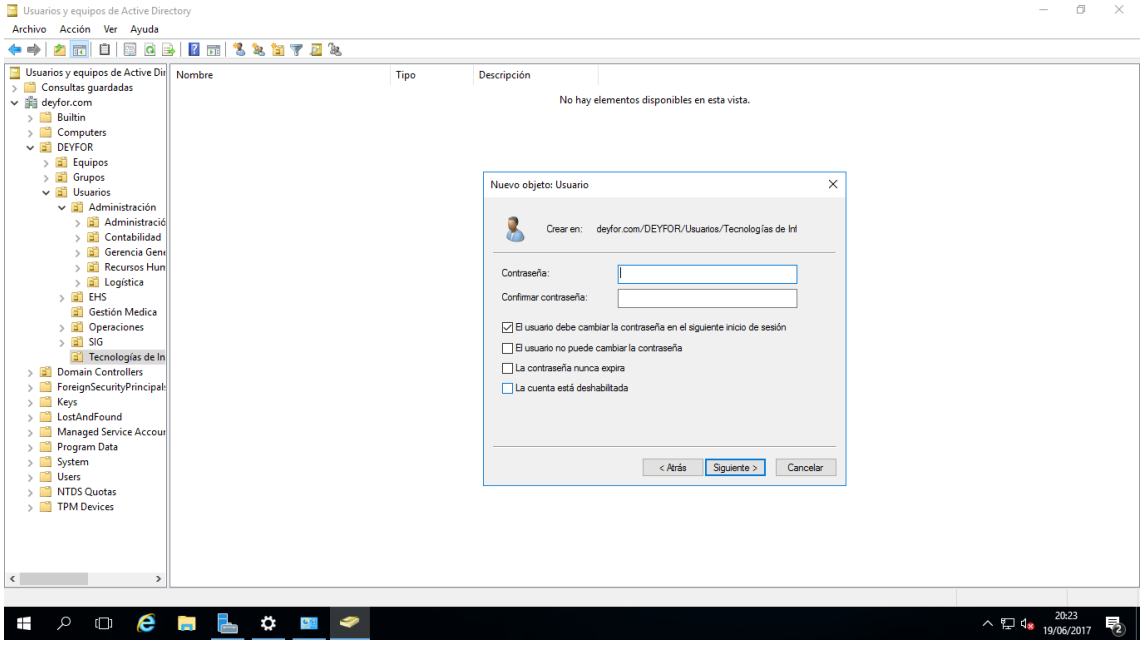


Fig. 36: Definir una contraseña para el usuario

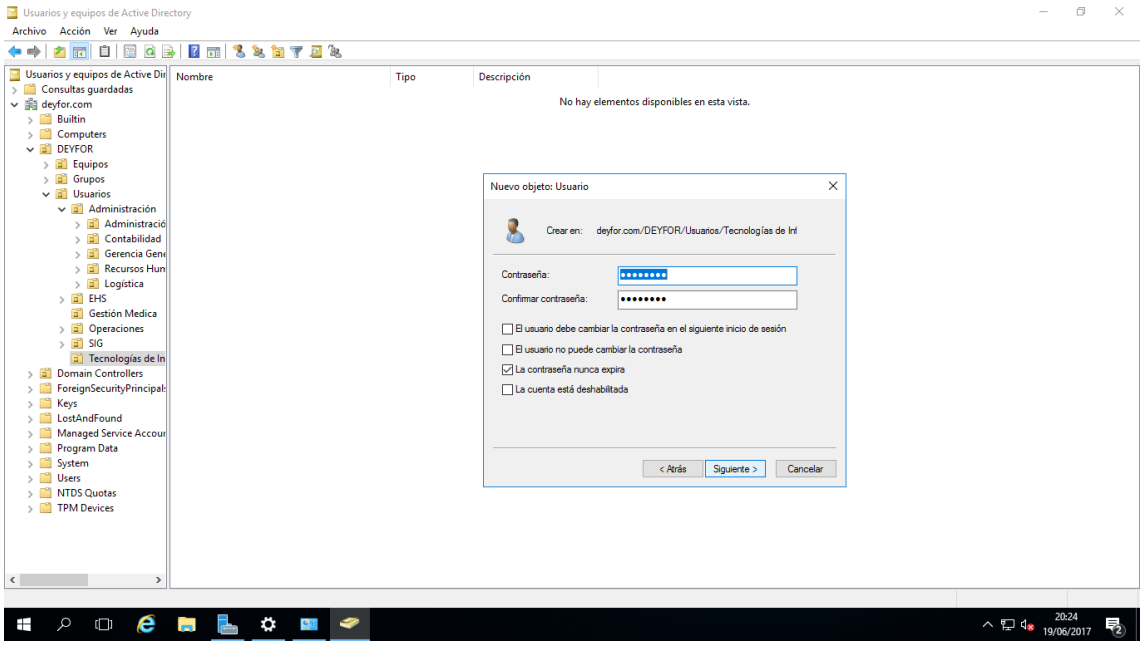


Fig. 37: Definir el periodo de expiración de la contraseña de usuario

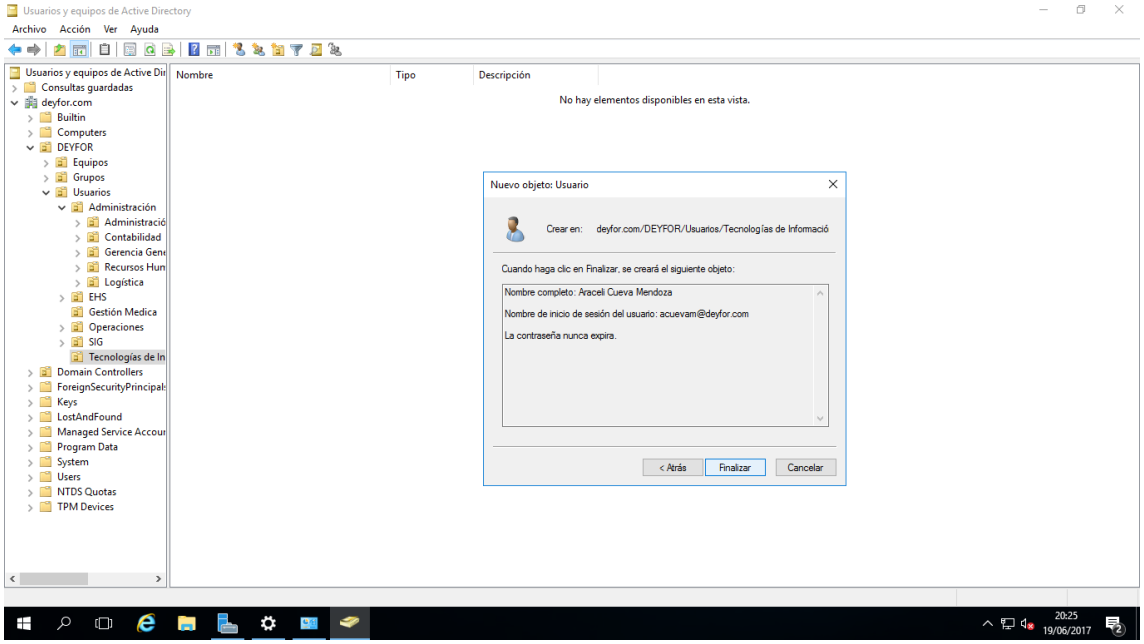


Fig. 38: Crear usuario de unidad organizativa

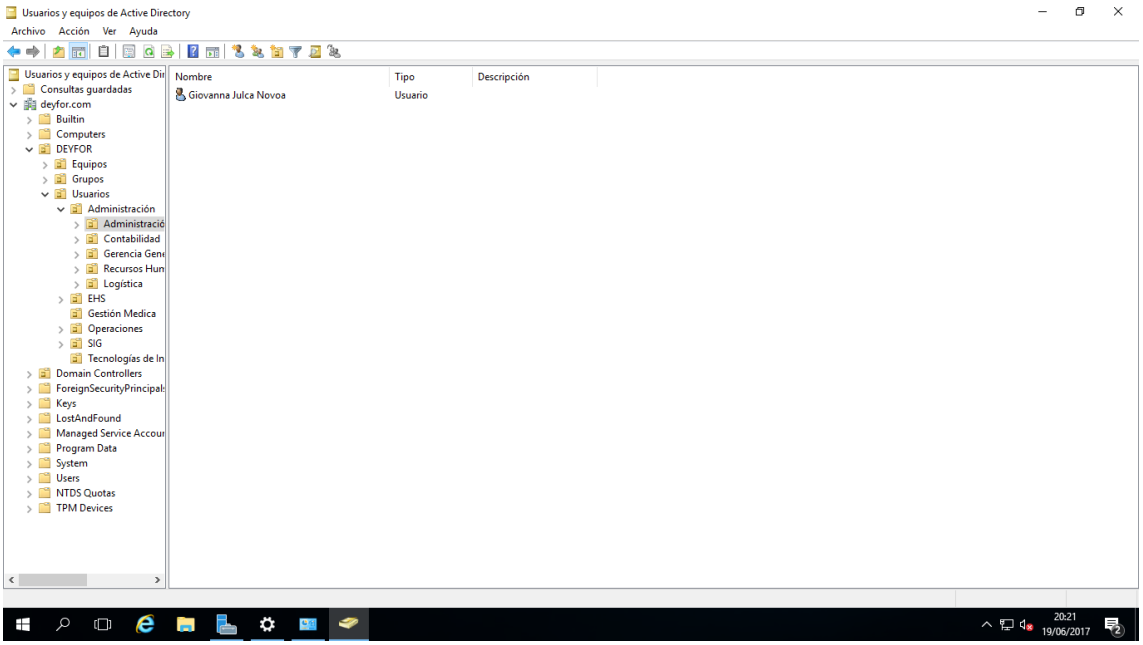


Fig. 39: El nuevo usuario se ha creado y agregado a la unidad organizativa

En las siguientes screenshots se muestra de forma detallada la forma como se agregan y configuran los usuarios de VPN dentro del router MicroTik que hace uso de su utilidad WinBox[21].

Haciendo uso de la plataforma de WinBox para administrar el router, accedemos a él, de la siguiente manera:

[21] Pequeña utilidad que permite la administración de Mikrotik RouterOs usando una interfaz gráfica de usuario fácil y simple. Es un binario Win32 nativo, pero lo que se puede ejecutar en Linux y Mac OSX usando Wine. Winbox se puede descargar directamente desde el Router

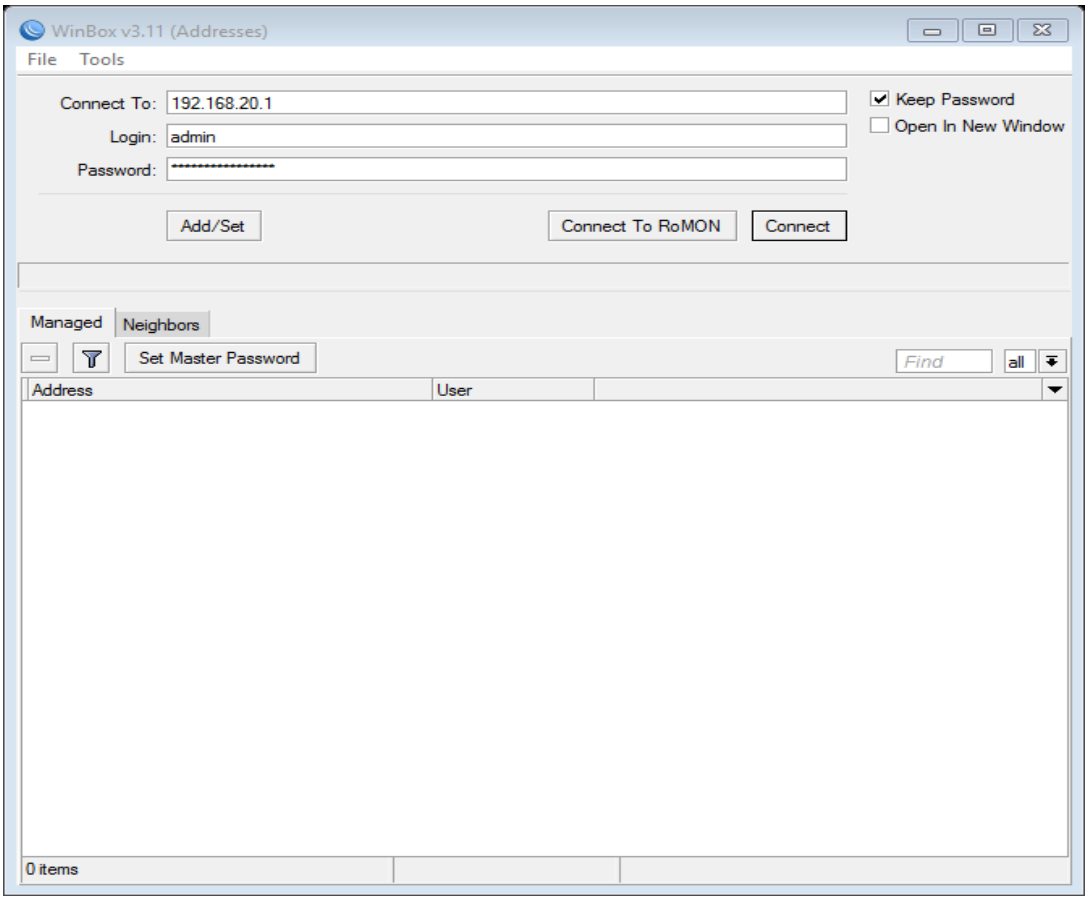


Fig. 40: Logueo para ingresar a la interfaz de administración del router Microtick

Fig. 41: Interfaz de administración del router Microtick

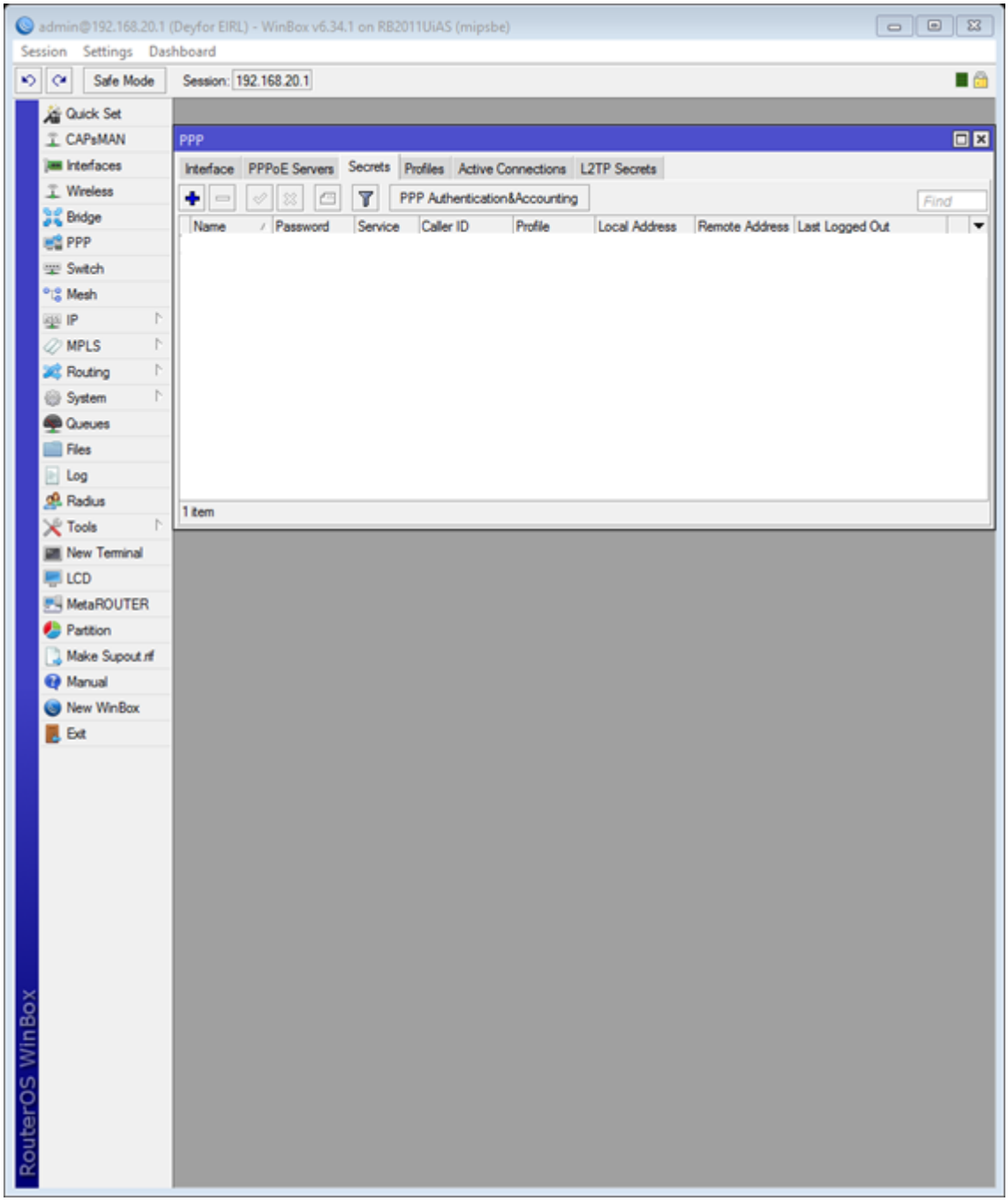


Fig. 42: Interfaz para la creación de usuarios de la red VPN.

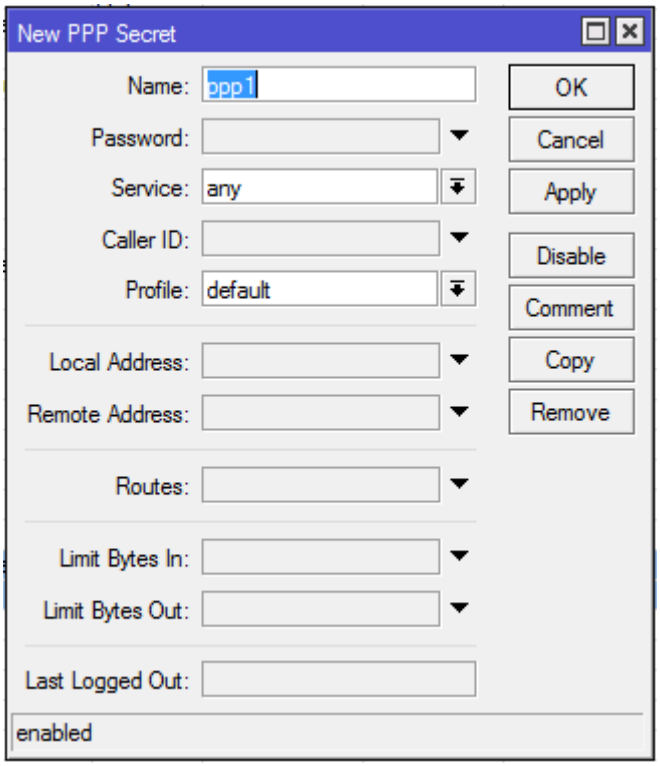


Fig. 43: Creación de un nuevo usuario de la red VPN.

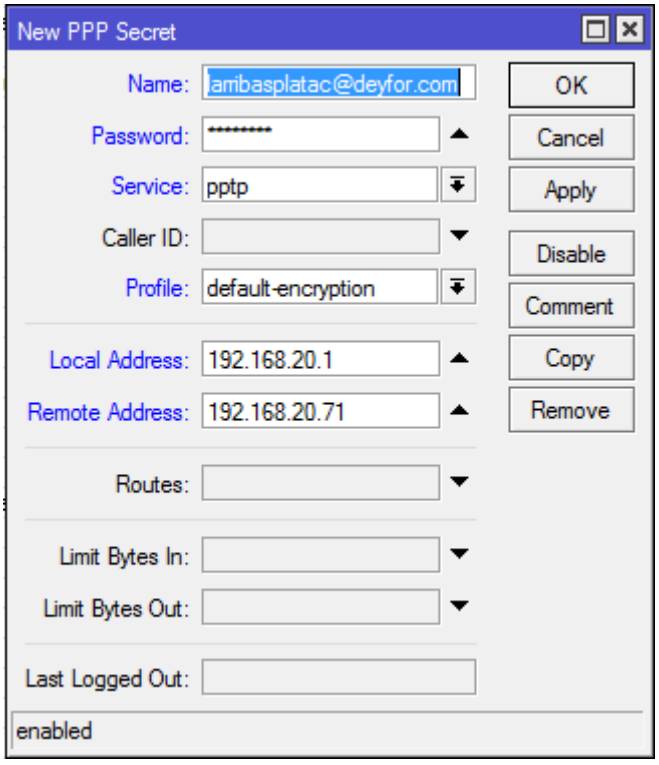


Fig. 44: Creación de un nuevo usuario de la red VPN.

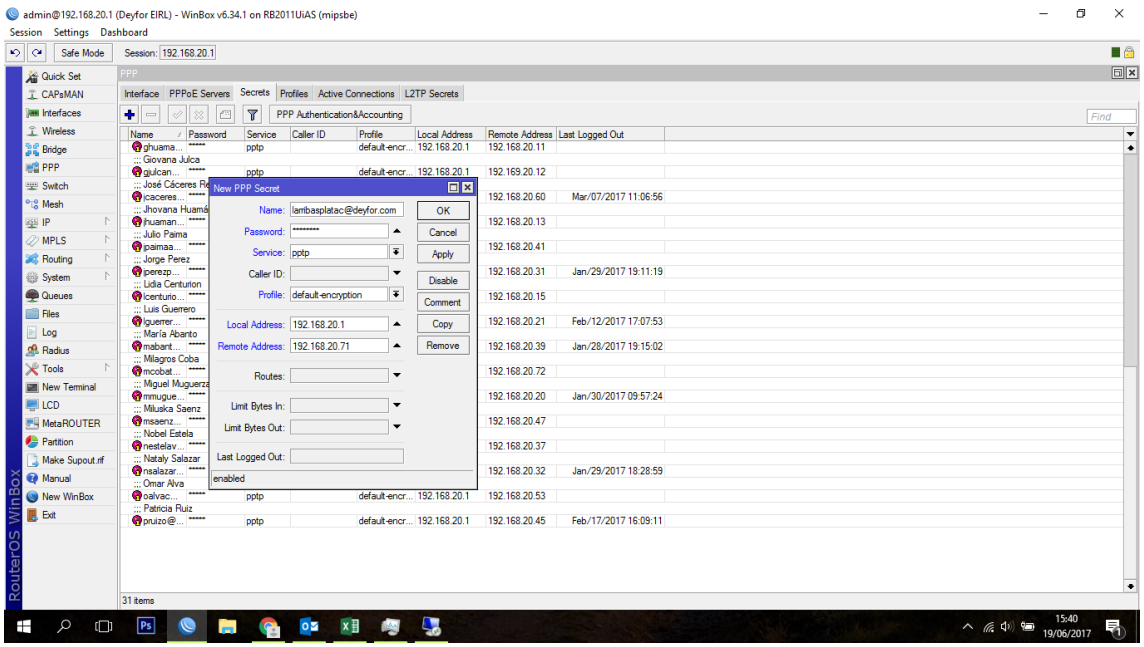


Fig. 45: Lista de usuarios de la red VPN.

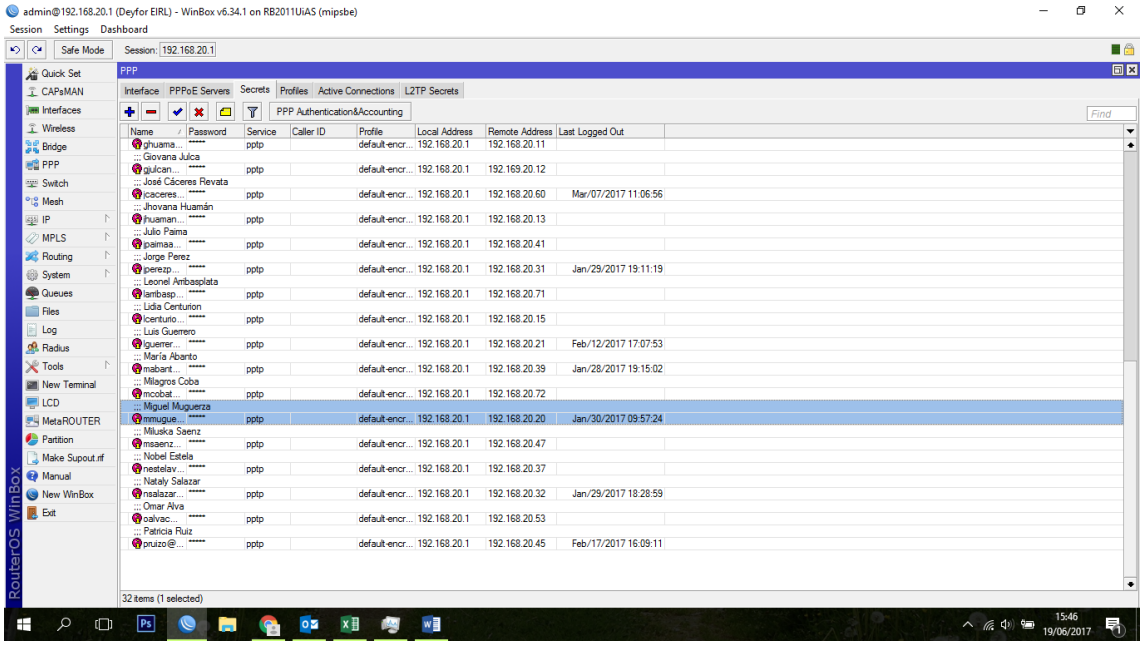
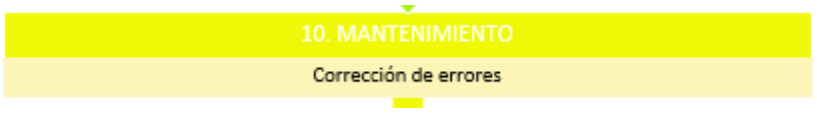


Fig. 46: Lista de usuarios de la red VPN.

2.3.3.10 *Mantenimiento*



Se programan tareas de mantenimiento periódicas. Lo tiempos de ejecución del mantenimiento pueden variar dependiendo de los puntos álgidos de tráfico de datos y son especificados por el equipo de trabajo. Si se registra una incidencia o error, se asume de inmediato por el equipo de desarrollo e implementación con la finalidad de encontrar la más rápida y óptima solución.

Tabla 11:Cronograma de Mantenimiento de la red VPN de la empresa Deyfor E.I.R.L.

CRONOGRAMA DE MANTENIMIENTO DE LA RED VPN DEYFOR E.I.R.L.																
ITEM	ACTIVIDAD	FRECUENCIAS	RESPONSABLE	SEGUIMIENTO	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT
	MANTENIMIENTO LOCATIVO (incluye equipos de oficina y equipos de emergencias)															
1	Revisión del servicio del servidor de archivos	TRIMESTRAL	Área de Tecnologías de Información	Programado												
				Ejecutado												
2	Revisión del buen funcionamiento del router e IP Pública	TRIMESTRAL	Área de Tecnologías de Información	Programado												
				Ejecutado												
3	Verificación del tráfico de red biridecional	TRIMESTRAL	Área de Tecnologías de Información	Programado												
				Ejecutado												
4	Monitorizar todos los equipos de la red	TRIMESTRAL	Área de Tecnologías de Información	Programado												
				Ejecutado												
5	Monitorizar Conexiones	TRIMESTRAL	Área de Tecnologías de Información	Programado												
				Ejecutado												

2.3.3.11 *Medición*

Evaluación del trabajo realizado:

Este punto es necesario para poder realizar una evaluación del trabajo realizado en la institución, por tanto, la evaluación se realizará en todo momento, se evaluará a partir de la puesta en marcha del proyecto y se podrá medir como se está avanzando en la ejecución, en lo posterior se evaluará la utilización de los servicios y por defecto se estará evaluando la conformidad, la aceptación por parte de los usuarios hacia la nueva implementación.

2.4 TRATAMIENTO, ANÁLISIS DE DATOS Y PRESENTACIÓN DE RESULTADOS

2.4.1 Pre y post prueba

2.4.1.1 *Resultados ficha de encuesta*

La ficha de encuesta (vea anexo 2) aplicada está constituida por 12 preguntas bien definidas acerca de la experiencia que han tenido los usuarios finales de la Red Privada Virtual después de que ésta ha sido desplegada dentro de la organización y se ha oficializado su funcionamiento. Los resultados de la encuesta aplicada a 33 trabajadores de la organización, se muestran en el siguiente gráfico.

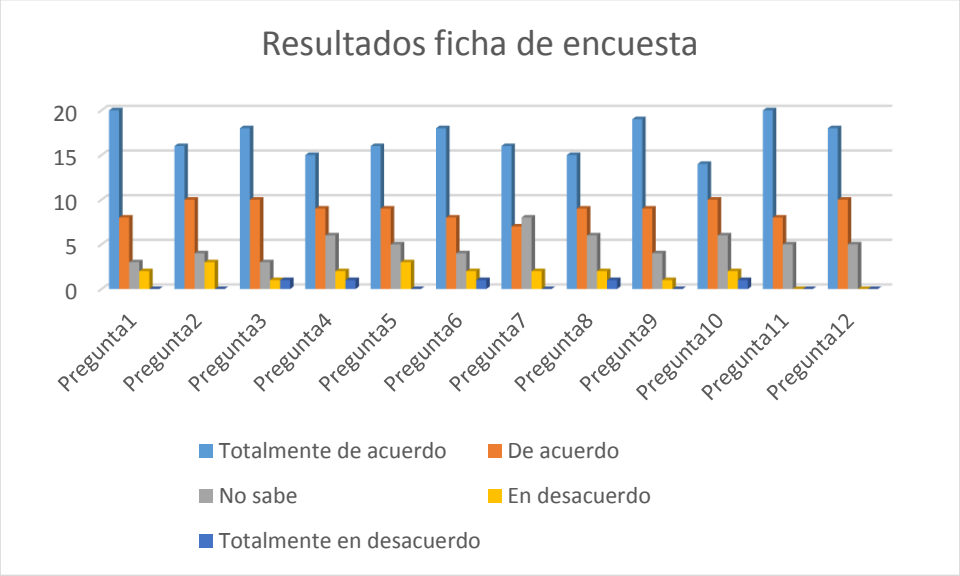


Gráfico 1: Resultados obtenidos al aplicar la ficha de encuesta

Del gráfico podemos concluir que las preguntas con respuestas positivas (totalmente de acuerdo) son predominantes, con lo que queda demostrado que la Red Privada Virtual tiene un elevado nivel de aceptación por parte de los usuarios finales.

2.4.1.2 *Resultados ficha de observación*

Mediante el uso de fichas de observación se toman muestras del tiempo en minutos que tarda la ejecución de actividades por área dentro de Deyfor, tanto antes como después de implementar VPN. En cada una de las tablas que se muestran a continuación, se presenta de manera clara y precisa el tiempo que toma la ejecución de actividades (relacionadas con acceso y manejo de información) por área dentro de la organización sobre la cual enfocamos nuestra investigación. Los datos mostrados recogen los tiempos de ejecución de actividades tanto antes como después de la implementación

de la Red Privada Virtual; esto con la finalidad de facilitar el contraste respectivo entre estos datos.

2.4.1.2.1 Gerencia

Tabla 12: Tiempos empleados en la ejecución de actividades en el área de Gerencia

ÁREA: GERENCIA								
Actividades Involucradas								
Ciclo por colaborador	Buscar Archivos (min)		Expedir actas y certificaciones de sesiones de directorio (min)		Brindar charlas informativas de gestión (min)		Atender reclamos presenciales hacia colaboradores (min)	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
E1	0.321	0.072	1.625	0.914	25.25	10.215	20.541	12.657
E2	0.214	0.052	1.642	0.872	23.321	11.213	28.642	13.214
E3	0.174	0.048	1.628	0.867	21.624	9.548	26.315	11.368
E4	0.302	0.057	1.534	0.902	24.57	9.576	24.615	12.596
E5	0.241	0.064	1.426	0.871	22.97	0.012	19.945	13.684
Promedio	0.2504	0.0586	1.571	0.8852	23.547	8.1128	24.0116	12.7038

2.4.1.2.2 Recursos Humanos

Tabla 13: Tiempos empleados en la ejecución de actividades en el área de Recursos Humanos

ÁREA: RECURSOS HUMANOS								
Actividades Involucradas								
Ciclo por colaborador	Acceso a hojas de vida de colaboradores (min)		Brindar charlas motivacionales (min)		Acceso y control de planilla (min)		Alojar información del personal en el servidor (min)	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
E1	0.467	0.021	22.124	13.721	0.521	0.124	2.714	0.954
E2	0.387	0.016	23.541	13.542	0.542	0.201	2.317	0.876
E3	0.459	0.028	21.541	14.564	0.534	0.123	1.876	0.912
E4	0.512	0.028	22.346	12.324	0.514	0.121	2.314	0.954
E5	0.426	0.031	20.541	12.567	0.517	0.132	2.116	0.182
Promedio	0.4502	0.0248	22.0186	13.3436	0.5256	0.1402	2.2674	0.7756

2.4.1.2.3 Administración

Tabla 14: Tiempos empleados en la ejecución de actividades en el área de Administración

ÁREA: ADMINISTRACIÓN								
Actividades Involucradas								
Ciclo por colaborador	Distribución de informes a todo el personal de la empresa (min)		Acceso a bancos de datos financieros de la empresa (min)		Dirección del personal en la ejecución de actividades específicas (min)		Actualizar información respecto a planes y objetivos estratégicos en carpeta de servidor (min)	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
E1	0.932	0.054	1.115	0.521	15.214	6.471	1.324	0.458
E2	0.954	0.048	1.123	0.612	13.216	6.542	1.214	0.521
E3	0.875	0.053	1.201	0.421	14.321	5.847	1.174	0.471
E4	0.962	0.051	1.121	0.542	13.542	6.512	1.231	0.523
E5	0.878	0.048	1.115	0.478	13.141	5.981	1.132	0.419
Promedio	0.9202	0.0508	1.135	0.5148	13.8868	6.2706	1.215	0.4784

2.4.1.2.4 Contabilidad

Tabla 15: Tiempos empleados en la ejecución de actividades en el área de Contabilidad

ÁREA: CONTABILIDAD								
Actividades Involucradas								
Ciclo por colaborador	Distribución de informes a todo el personal de la empresa (min)		Acceso al sistema contable institucional (min)		Depurar los registros contables y presupuestales alojados en el servidor (min)		Actualizar estados financieros (min)	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
E1	1.542	0.601	0.321	0.026	1.101	0.084	0.932	0.054
E2	1.587	0.604	0.435	0.015	1.123	0.082	0.954	0.048
E3	1.498	0.598	0.314	0.025	1.111	0.087	0.875	0.053
E4	1.503	0.532	0.283	0.036	1.087	0.092	0.962	0.051
E5	1.507	0.543	0.275	0.025	1.098	0.051	0.878	0.048
Promedio	1.5274	0.5756	0.3256	0.0254	1.104	0.0792	0.9202	0.0508

2.4.1.2.5 Logística

Tabla 16: Tiempos empleados en la ejecución de actividades en el área de Logística

ÁREA: LOGÍSTICA								
Actividades Involucradas								
Ciclo por colaborador	Acceso al sistema ERP institucional (min)		Generar una orden de compra (min)		Actualizar stock de productos (min)		Revisar y hacer seguimiento de cronogramas y metas (min)	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**

E1	0.392	0.192	3.224	0.911	2.033	0.998	10.542	5.214
E2	0.523	0.108	3.229	0.813	2.041	0.989	10.847	5.642
E3	0.582	0.128	3.228	0.912	2.034	0.978	10.641	4.121
E4	0.491	0.109	3.225	0.911	2.036	0.997	9.847	4.321
E5	0.501	0.118	3.226	0.912	2.033	0.998	10.527	3.987
Promedio	0.4978	0.131	3.2264	0.8918	2.0354	0.992	10.4808	4.657

2.4.1.2.6 TI

Tabla 17: Tiempos empleados en la ejecución de actividades en el área de TI

ÁREA: TECNOLOGÍAS DE INFORMACIÓN								
Ciclo por colaborador	Actividades Involucradas							
	Acceso remoto al servidor (min)		Subir archivos al servidor (min)		Enviar informes masivos (min)		Brindar video conferencias (min)	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
E1	0.904	0.086	1.421	0.055	0.028	0.019	30.412	15.647
E2	0.937	0.088	1.519	0.044	0.033	0.016	29.124	15.841
E3	0.832	0.097	1.622	0.066	0.031	0.017	35.642	14.652
E4	0.934	0.084	1.518	0.055	0.029	0.018	37.124	14.357
E5	0.836	0.065	1.419	0.054	0.031	0.015	32.654	12.654
Promedio	0.8886	0.084	1.4998	0.0548	0.0304	0.017	32.9912	14.6302

2.4.1.2.7 Operaciones.

Tabla 18: Tiempos empleados en la ejecución de actividades en el área de Operaciones

ÁREA: OPERACIONES								
Ciclo por colaborador	**Administrar Comprobantes de Venta**							
	Actividades Involucradas							
	Acceso a expedientes técnicos de proyectos (min)		Actualización de expedientes técnicos (min)		Envío de reportes completos de operaciones (min)		Emitir un requerimiento de materiales (min)	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
E1	5.213	1.845	4.867	1.623	2.123	0.204	3.033	0.012
E2	5.231	1.787	4.856	1.642	2.451	0.254	3.04	0.011
E3	5.645	1.954	4.957	1.602	2.317	0.301	3.036	0.01
E4	5.421	1.978	4.871	1.504	2.214	0.221	3.038	0.012
E5	4.987	1.968	5.107	1.342	2.142	0.203	3.036	0.012
Promedio	5.2994	1.9064	4.9316	1.5426	2.2494	0.2366	3.0366	0.0114

2.4.2 Representación gráfica de resultados de ficha de observación

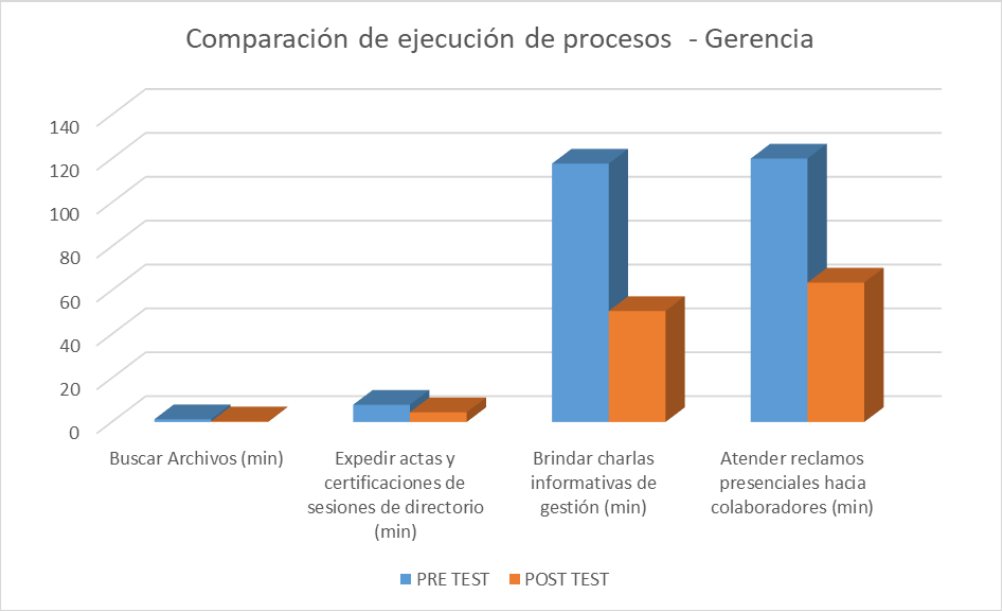


Gráfico 2: Comparación de ejecución de procesos (pre test y pos test) en el área de gerencia

Según el gráfico anterior, se puede observar claramente la reducción de tiempos que ha sufrido la ejecución de procesos por parte del área de Gerencia después de implementar la Red Privada Virtual dentro de la empresa Deyfor. El porcentaje de mejora total para los procesos en estudio dentro del área de Gerencia es del 55.6%.

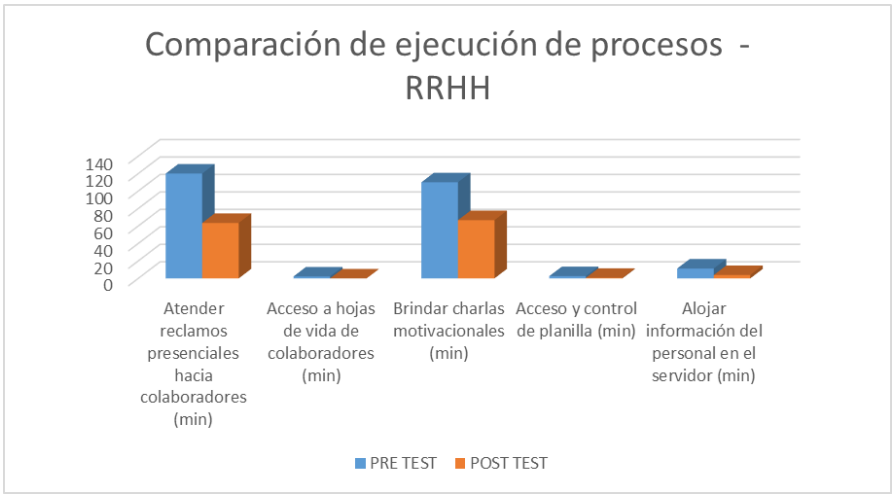


Gráfico 3: Comparación de ejecución de procesos (pre test y pos test) en el área de RRHH

La ejecución de procesos y/o actividades en el área de Recursos Humanos, ha mejorado sustancialmente luego de la implementación de la Red Privada Virtual. En el gráfico anterior se observan claramente las comparaciones entre los tiempos antes y después de implementar VPN, cuyas diferencias son innegables con un balance positivo y muy

por encima del estimado. El porcentaje de mejora total para los procesos en estudio dentro del área de Recursos Humanos es del 53.8%.

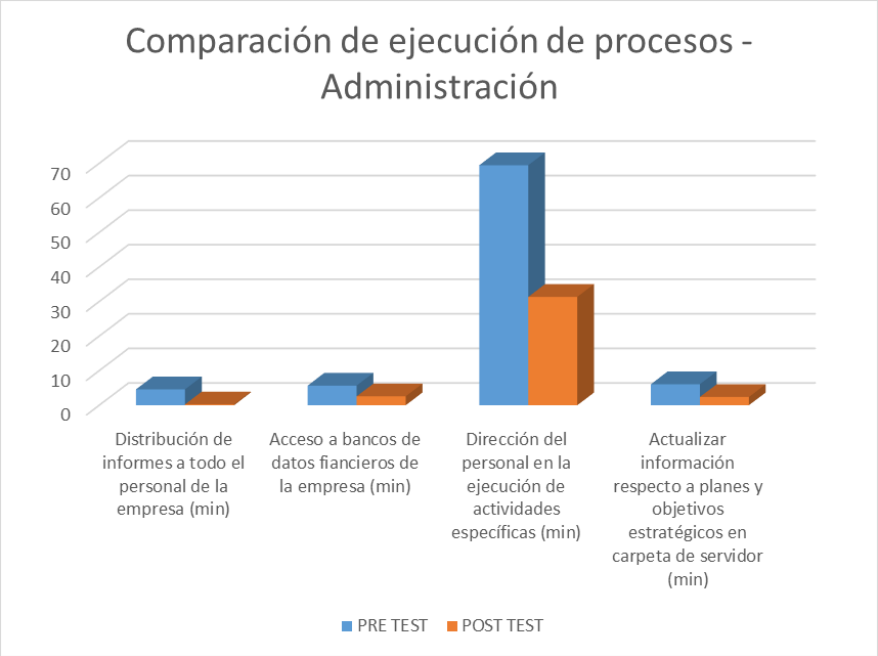


Gráfico 4: Comparación de ejecución de procesos (pre test y pos test) en el área de Administración

En el área de administración la mejora más significativa después de implementar la VPN, según el gráfico anterior, se evidencia en cuanto al proceso de actualizar información en el servidor y también dirigir al personal en la ejecución de sus actividades. El porcentaje de mejora total para los procesos en estudio dentro del área de Administración es del 57.36%.

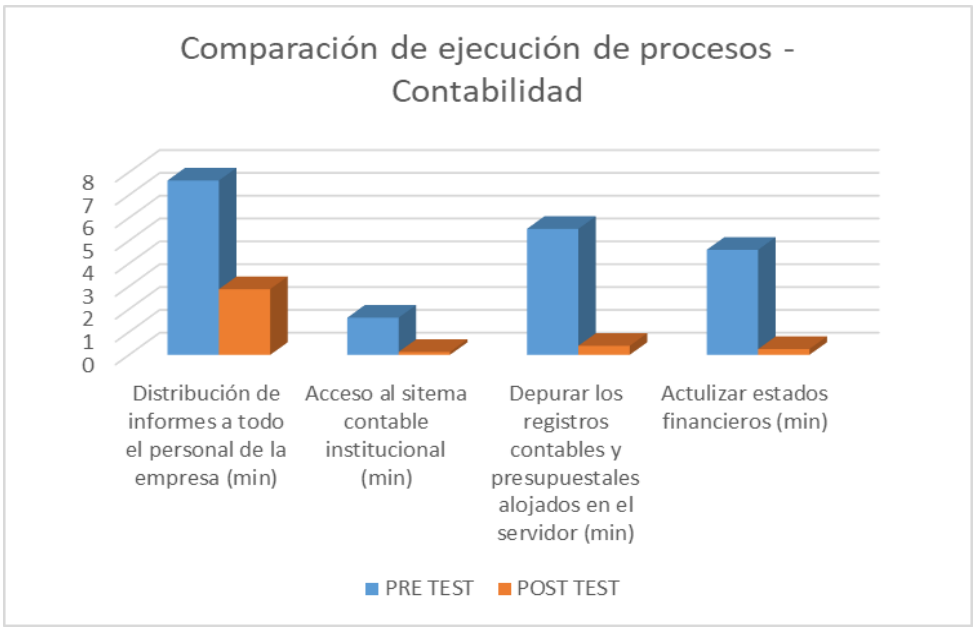


Gráfico 5: Comparación de ejecución de procesos (pre test y pos test) en el área de Contabilidad

Según el gráfico anterior, para el área de contabilidad, la mejora más significativa que trajo consigo la implementación de VPN, se evidencia en cuanto a depurar los registros contables y presupuestales, además de una mejora sustancial en la distribución de informes de forma rápida y segura a todo el personal de la empresa. El porcentaje de mejora total para los procesos en estudio dentro del área de Contabilidad es del 81.15%.

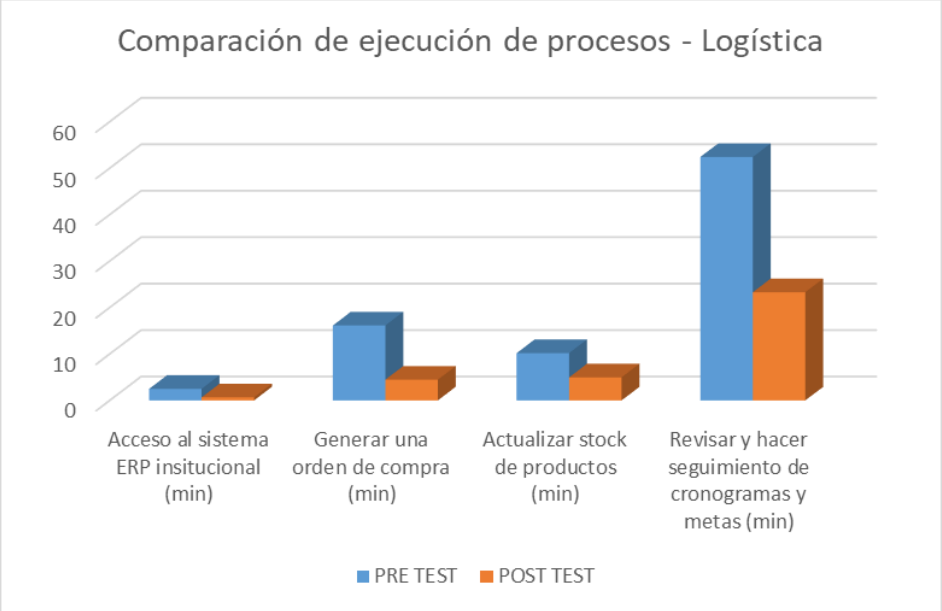


Gráfico 6: Comparación de ejecución de procesos (pre test y pos test) en el área de Logística

Para el área de logística, con la implementación de la VPN se ha logrado reducir de manera muy significativa todos los procesos que involucran acceder y usar el sistema ERP alojado en el servidor institucional adoptado para gestionar procesos logísticos. El porcentaje de mejora total para los procesos en estudio dentro del área de gerencia es del 58.92%.

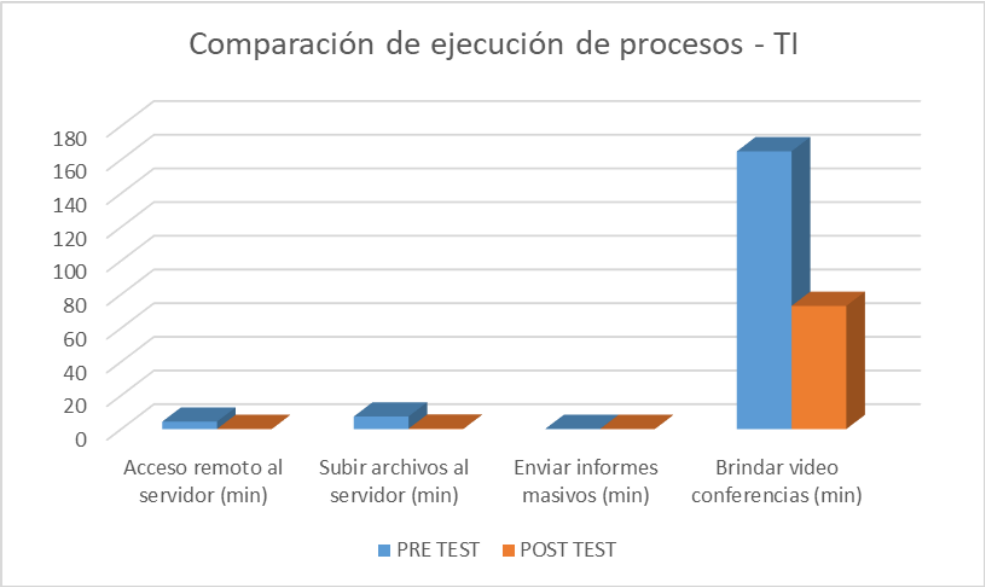


Gráfico 7: Comparación de ejecución de procesos (pre test y pos test) en el área de TI

Para procesos relacionados con el área de Tecnologías de la Información, implementar VPN ha significado una mejora sustancial en cuanto a optimización de tiempos durante su ejecución. Según el gráfico anterior, se puede observar que para los procesos evaluados las mejoras superan el 50% de optimización o reducción para su ejecución. El porcentaje de mejora total para los procesos en estudio dentro del área de TI es del 58.25%.

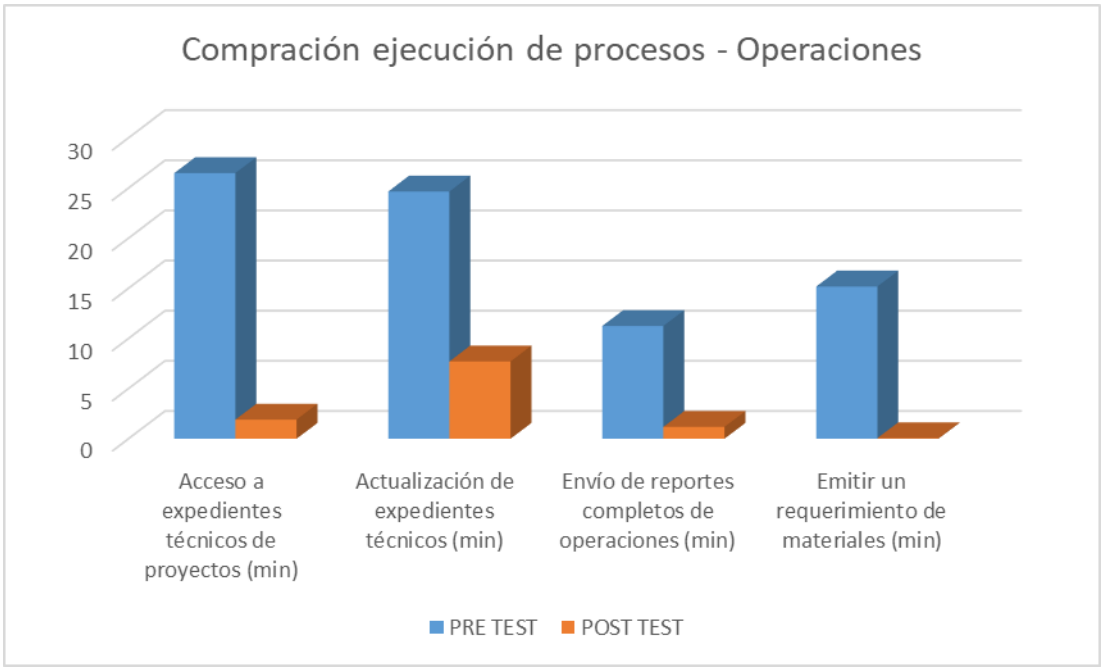


Gráfico 8: Comparación de ejecución de procesos (pre test y pos test) en el área de Operaciones

De acuerdo al gráfico anterior, los procesos ejecutados por el área de Operaciones han sufrido mejoras exponencialmente altas, llegando en algunos casos a superar el 80% de optimización. El porcentaje de mejora total para los procesos en estudio dentro del área de Operaciones es del 76.17%.

2.4.3 Herramientas de procesamiento de datos

2.4.3.1 *Encuesta*

Se utilizó una encuesta, para realizar una recolección sistemática de datos en base a los usuarios finales de la VPN, con la finalidad de conocer distintos puntos de vista respecto a los beneficios, facilidades, problemas, entre otras consideraciones después de usar la VPN (Vea anexo 2).

2.4.3.2 *Ficha de observación*

Se elaboraron fichas de observación con la finalidad de registrar los tiempos que tarda la ejecución de determinado proceso y sus actividades inherentes. Estos registros se realizan para poder contrastar los tiempos de ejecución de procesos tanto antes, así como después de la implementación de la VPN.

2.4.4 Establecimiento de técnicas e instrumentos de procesamiento de datos

Para establecer las técnicas y/o instrumentos de procesamiento de datos se hace uso del software de oficina Microsoft Excel en su versión 2016 (Vea anexo 3) el mismo que gracias a su facilidad de manejo, su versatilidad y sus incontables funciones, permite a los investigadores lograr buenos resultados de manera rápida y precisa.

Se elaboran matrices de procesamiento de datos recogidos mediante la aplicación de la ficha de encuesta, así como para los datos que se recogen mediante el uso de las fichas de observación. Los datos recabados mediante la utilización de las fichas de encuestas constituyen el pre (antes de implementar VPN) y post test (después de implementar VPN).

2.4.4.1 *Ficha de observación*

Con la finalidad de evaluar el tiempo que tarda la ejecución de procesos dentro de la empresa Deyfor antes y después de implementar la VPN, se toman cinco muestras aleatorias de tiempos [48], ya que según el libro citado, es una prueba estándar para el número de personas a las cuales se van a evaluar en la organización que es de 34

personas, con dependencia del número de personas con las que se cuenta para el estudio. A continuación, se presenta la matriz de procesamiento de datos usada para medir la ejecución total de un proceso.

Tabla 19: Matriz de procesamiento de datos (pre y post prueba) de tiempos por proceso

Ciclo por colaborador	Área NNN							
	Tiempos por proceso							
	P(min)		**P(min)**		**P(min)**		**P(min)**	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
C1								
C2								
C3								
C4								
C5								
Promedio								

Tener en cuenta que:

- **NNN:** Área donde se tomarán los datos.
- **P:** Especificación del proceso que se está evaluando.
- **P**: Ciclo de ejecución de las actividades involucradas en un proceso.
- **TAVPN:** Tiempo antes de VPN (tiempo que tarda ejecutar una actividad antes de implementar VPN).
- **TDVPN:** Tiempo después de VPN (tiempo que tarda ejecutar una actividad después de implementar VPN).
- **min:** Tiempo en minutos

Para cada una de los procesos, se toman un mínimo de 5 muestras (ejecuciones - ciclos) de tiempos usados en la ejecución de las actividades involucradas dentro del mismo antes y después de que la VPN se implementa y despliega completamente dentro de la empresa Deyfor.

Tabla 20: Matriz de procesamiento de datos (pre y post prueba) de tiempos por actividad

Ciclo por colaborador	Proceso N							
	Actividades Involucradas							
	A(min)		**A(min)**		**A(min)**		**A(min)**	
	TAVPN	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**	**TAVPN**	**TDVPN**
C1								
C2								
C3								
C4								
C5								
Promedio								

Tener en cuenta que:

- **N:** Nombre del proceso evaluado.

- **C:** Ciclo de ejecución de las actividades involucradas en un proceso.
- **A**: Especificación de la actividad realizada.
- **TAVPN:** Tiempo antes de VPN (tiempo que tarda ejecutar una actividad antes de implementar VPN).
- **TDVPN:** Tiempo después de VPN (tiempo que tarda ejecutar una actividad después de implementar VPN).
- **min:** Tiempo en minutos

2.4.4.2 *Ficha de encuesta*

Tabla 21: Matriz de procesamiento de datos recogidos mediante la ficha de encuesta

CRITERIOS	Pregunta								
	P1	P2	P3	P4	P5	P6	P7	P8	P9
C1									
C2									
C3									
,,,									
Cn									
Conteo General									

2.4.5 Validación de instrumentos de recolección de datos

Con la finalidad de determinar la validez y fiabilidad de los instrumentos de recolección de datos se siguen los siguientes lineamientos (Vea anexo 3):

La confiabilidad de una medición o de un instrumento, según el propósito de la primera y ciertas características del segundo, puede tomar varias formas o expresiones al ser medida o estimada: coeficientes de precisión, estabilidad, equivalencia, homogeneidad o consistencia interna, pero el denominador común es que todos son básicamente expresados como diversos coeficientes de correlación. En el caso específico del coeficiente de confiabilidad vinculado a la homogeneidad o consistencia interna, se dispone del coeficiente (alpha), propuesto por Lee J. Cronbach (1916-2001) en el año 1951. Se ha demostrado que este coeficiente representa una generalización de las populares fórmulas KR-20 y KR-21 de consistencia interna, desarrolladas en 1937 por Kuder y Richardson, las cuales eran solo aplicables a formatos binarios de calificación o de respuesta (dicotómicas). Por lo tanto, con la creación del alfa de Cronbach, los investigadores fueron capaces de evaluar la confiabilidad o consistencia interna de un instrumento constituido por una escala Likert, o cualquier escala de opciones múltiples [49].

Para determinar el coeficiente Cronbach el investigador calcula la correlación de cada reactivo o ítem con cada uno de los otros, resultando una gran cantidad de coeficientes de correlación. El valor de α es el promedio de todos los coeficientes de correlación. Visto desde otra perspectiva, el coeficiente Cronbach puede considerarse como la media de todas las correlaciones de división por mitades posibles, otro método de cálculo de consistencia interna, las buenas junto las malas [49]. El coeficiente alfa de Cronbach puede ser calculado de dos formas distintas:

a. Mediante la varianza de los ítems y la varianza del puntaje total.

$$r_{tt} = \frac{k}{(k-1)[\frac{1-\sum S_i^2}{S_t^2}]}$$

Donde:

- ✓ $\mathbf{r_{tt}}$: coeficiente de confiabilidad de la prueba o cuestionario.
- ✓ **k**: número de ítems del instrumento.
- ✓ S_t^2: Varianza total del instrumento.
- ✓ S_i^2: Sumatoria de las varianzas de los ítems.

Cuanto menor sea la variabilidad de respuesta, es decir, que haya homogeneidad en las respuestas dentro de cada ítem, mayor será el Alfa de Cronbach.

b. Mediante la matriz de correlación de los ítems.

$$\alpha = \frac{np}{1 + p\,(n-1)}$$

Donde:

- ✓ **n**: Número de ítems
- ✓ **p**: Promedio de las correlaciones lineales entre cada uno de los ítems.

Cuanto mayor sea la correlación lineal entre ítems, mayor será el alfa de Cronbach.

2.4.6 Selección de la prueba estadística

Partiendo de la premisa de que la población (número N < 30) en estudio en el presente proyecto de investigación conforma la muestra, es decir, es una muestra poblacional; y que existen mediciones antes y después de implementar la Red Privada Virtual, se hace uso de la prueba estadística T-Student para muestras dependientes. De esta manera, los requisitos que deben satisfacerse son los mismos, excepto la independencia de las

muestras; es decir, en esta prueba estadística se exige dependencia entre ambas, en las que hay dos momentos uno antes y otro después. Con esto se da a entender que, en el primer periodo, las observaciones obtenidas haciendo uso de fichas de observación para recabar datos de los tiempos de ejecución de procesos y sus actividades dentro de Deyfor E.I.R.L, servirán de control o testigo, para conocer los cambios que se susciten después de aplicar una variable experimental.

Con la prueba t se comparan las medias y las desviaciones estándar de grupo de datos y se determina si entre esos parámetros las diferencias son estadísticamente significativas o si sólo son diferencias aleatorias. Utilizaremos la siguiente fórmula para muestras relacionadas:

$$t = \frac{\bar{d}}{\frac{\sigma d}{\sqrt{N}}}$$

Donde:

- ✓ **t:** Valor estadístico del procedimiento.
- ✓ **$\bar{d}$':** Valor promedio o media aritmética de las diferencias entre los momentos después y antes.
- ✓ **σd:** Desviación estándar de las diferencias entre los momentos después y antes.
- ✓ **N:** Tamaño de la muestra

La media aritmética de las diferencias se obtiene de la siguiente manera:

$$\bar{d} = \frac{\sum d}{N}$$

La desviación estándar de las diferencias se obtiene como sigue:

$$\sigma d = \sqrt{\frac{\sum (d - \bar{d})^2}{N - 1}}$$

2.5 PRUEBA DE HIPÓTESIS

Finalizada la implementación de la Red Privada Virtual dentro de la empresa y, posteriormente realizada la comparación de datos obtenidos a través de los instrumentos de recolección de datos, se procede a validar si el rumbo que tomó la investigación en su inicio es el correcto. En este apartado nos centramos en el contraste de hipótesis a través del uso de técnicas e instrumentos estadísticos. El resultado final es la aceptación o rechazo del enunciado hipotético de que la implementación de una Red Privada Virtual mejora la gestión de información dentro de la empresa Deyfor E.I.R.L. En última instancia, se evalúa la concordancia de la investigación recurrente con las investigaciones que fueron tomadas como antecedentes de la misma.

En el siguiente cuadro se muestra un consolidado de los tiempos empleados en la ejecución de procesos por área tanto antes (pre test) de implementar la solución planteada, así como después (pos test) de la implementación. Este cuadro ayuda a verificar las diferencias entre las ejecuciones de pre y pos test, facilitando a nuestro papel de investigadores para realizar los cálculos de medidas estadísticas.

Tabla 22: Cuadro resumen de registro de tiempos en ejecución de procesos

N°	Á.	PROCESO	PRE TEST	POST TEST	D	D - D'	$(D - D')^2$
1	GERENCIA	Buscar Archivos (min)	1.252	0.293	-0.959	15.686	246.04723
2		Expedir actas y certificaciones de sesiones de directorio (min)	7.855	4.426	-3.429	13.216	174.65982
3		Brindar charlas informativas de gestión (min)	117.735	50.564	-67.171	-50.526	2552.88750
4		Atender reclamos presenciales hacia colaboradores (min)	120.058	63.519	-56.539	-39.894	1591.53978
5	RRHH	Acceso a hojas de vida de colaboradores (min)	2.251	0.0248	-2.2262	14.419	207.89870
6		Brindar charlas motivacionales (min)	110.093	66.718	-43.375	-26.730	714.49863
7		Acceso y control de planilla (min)	2.628	0.701	-1.927	14.718	216.61637
8		Alojar información del personal en el servidor (min)	11.337	3.878	-7.459	9.186	84.38063
9	ADMINISTRACIÓN	Distribución de informes a todo el personal de la empresa (min)	4.601	0.254	-4.347	12.298	151.23817
10		Acceso a bancos de datos financieros de la empresa (min)	5.675	2.574	-3.101	13.544	183.43703
11		Dirección del personal en la ejecución de actividades específicas (min)	69.434	31.353	-38.081	-21.436	459.50669
12		Actualizar información respecto a planes y objetivos estratégicos en carpeta de servidor (min)	6.075	2.392	-3.683	12.962	168.01067

13	CONTABILIDAD	Distribución de informes a todo el personal de la empresa (min)	7.637	2.878	-4.759	11.886	141.27445
14		Acceso al sistema contable institucional (min)	1.628	0.127	-1.501	15.144	229.33749
15		Depurar los registros contables y presupuestales alojados en el servidor (min)	5.52	0.396	-5.124	11.521	132.73097
16		Actualizar estados financieros (min)	4.601	0.254	-4.347	12.298	151.23817
17	LOGÍSTICA	Acceso al sistema ERP institucional (min)	2.489	0.655	-1.834	14.811	219.36255
18		Generar una orden de compra (min)	16.132	4.459	-11.673	4.972	24.71972
19		Actualizar stock de productos (min)	10.177	4.96	-5.217	11.428	130.59674
20		Revisar y hacer seguimiento de cronogramas y metas (min)	52.404	23.285	-29.119	-12.474	155.60335
21	TI	Acceso remoto al servidor (min)	4.443	0.084	-4.359	12.286	150.94316
22		Subir archivos al servidor (min)	7.499	0.274	-7.225	9.420	88.73438
23		Enviar informes masivos (min)	0.152	0.085	-0.067	16.578	274.82653
24		Brindar video conferencias (min)	164.96	73.151	-91.809	-75.164	5649.64300
25	OPERACIONES	Acceso a expedientes técnicos de proyectos (min)	26.497	1.9064	-24.5906	-7.946	63.13426
26		Actualización de expedientes técnicos (min)	24.658	7.713	-16.945	-0.300	0.09006
27		Envío de reportes completos de operaciones (min)	11.247	1.183	-10.064	6.581	43.30815
28		Emitir un requerimiento de materiales (min)	15.183	0.057	-15.126	1.519	2.30704
		TOTAL	**814.221**	**348.164**	**-466.057**	**0.000**	**14208.5713**

2.5.1 Hipótesis nula (H_0)

La implementación de una red privada virtual no mejorará la gestión de información de la empresa Deyfor E.I.R.L.

$$\boldsymbol{Ho}: \mu D \geq \mu A;\ \mu D - \mu A \geq 0$$

2.5.2 Hipótesis alternativa (H_a)

La implementación de una red privada virtual mejorará la gestión de información de la empresa Deyfor E.I.R.L.

$$\boldsymbol{Ha}: \mu D < \mu A;\ \mu D - \mu A < 0$$

2.5.3 Nivel de significancia

Para el presente trabajo de investigación se toma un nivel de significancia del 5%.

$$\alpha = 0.05$$

2.5.4 Valor estadístico del procedimiento

$$\mathbf{D'} = -466.057/28 = -16.645$$

$$\boldsymbol{\sigma D} = \sqrt{\frac{14208.5713}{27}} = 22.94$$

$$\mathbf{t} = -16.645 / (22.94/\sqrt{28}) = -3.84$$

En función a la tabla T-Student, el valor de la probabilidad **p** del valor estadístico del procedimiento es:

$$\mathbf{p}\ (\mathbf{t} < -3.84) = 0.000337889$$

2.5.5 Establecer región crítica

- ✓ Grados de libertad: 27
- ✓ N = 28

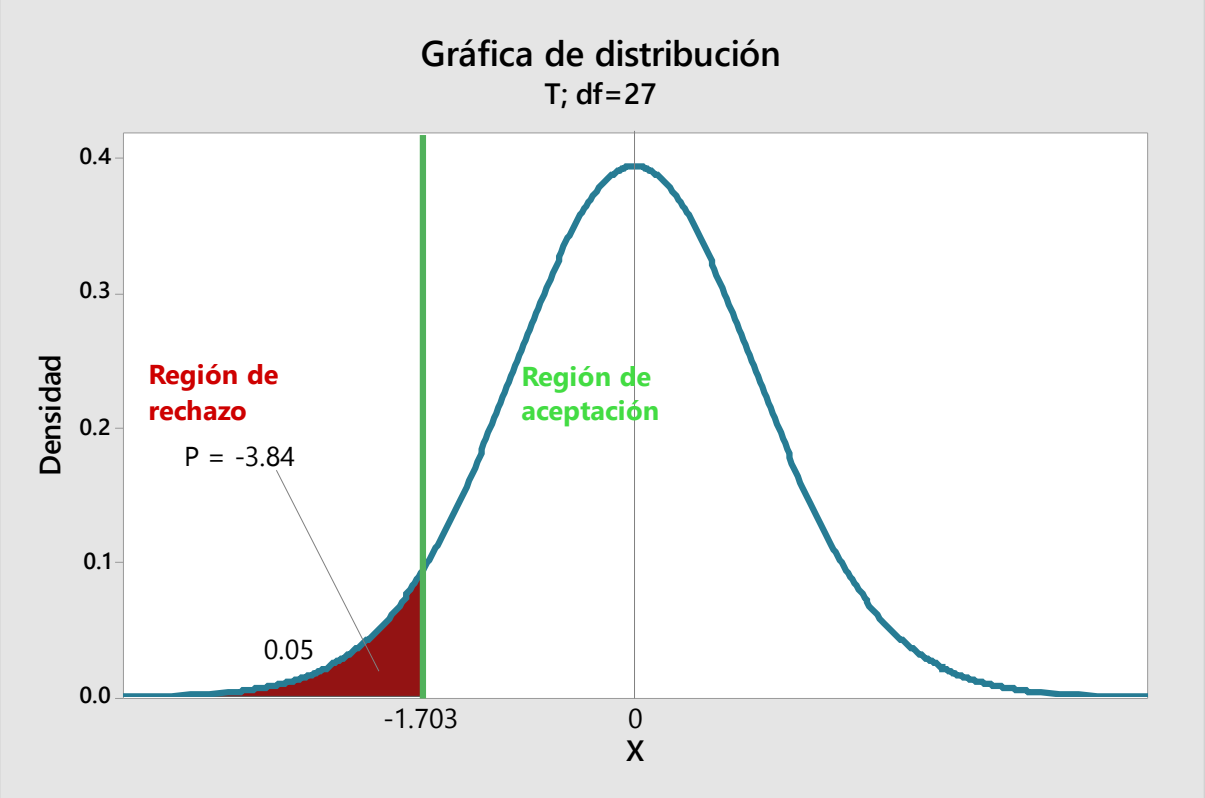


Gráfico 9: Distribución T Student - establecimiento de la región crítica

2.5.6 Toma de la decisión

Según los resultados obtenidos en los apartados anteriores, se puede notar claramente que el valor de la probabilidad **p** = 0.000337889 es menor que el valor del nivel de significancia **α** = 0.05 y el valor estadístico del procedimiento **t** = -3.84 es menor que el valor crítico -1.703, por tanto, en virtud de estos resultados, se obtiene evidencia suficiente para rechazar $\mathbf{H_0}$ y aceptar $\mathbf{H_a}$**.** Por consiguiente, se puede afirmar que la implementación de una red privada virtual mejorará la gestión de información de la empresa DEYFOR E.I.R.L, con un nivel de significancia del 5% y un nivel de confianza del 95%.

CAPÍTULO IV. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

2.5.7 Discusión de resultados

En este apartado se verifica que los resultados obtenidos post implementación de la solución (VPN) dentro de la empresa cumplan o satisfagan los objetivos planteados al iniciar nuestra investigación. Es en este punto dónde se establece hasta qué punto se llega a concordar con las investigaciones que fueron tomadas como antecedentes válidos para la nuestra. Estos resultados se muestran a continuación:

Después de realizar el análisis y procesamiento de resultados de los datos obtenidos a través de la aplicación de la ficha de encuesta, se determina con claridad el impacto positivo de la implementación de una Red Privada Virtual dentro de la empresa Deyfor, mejorando significativamente los tiempos empleados en los procesos involucrados dentro de la gestión de información. En las líneas subsiguientes se realiza el análisis del nivel de concordancia entre los resultados obtenidos en la presente investigación y las conclusiones a las que llegaron los autores de las investigaciones que fueron tomadas como antecedentes al iniciar la presente investigación:

Tal como lo manifiestan Hostos y Zambrano [4], la implementación de una red Privada Virtual, permite ofrecer seguridad en las comunicaciones por medio de protocolos de encriptamiento y llaves compartidas, servicio de antivirus, anti-spam, anti-hacker, etc. Se llega a una concordancia total con estos autores, puesto que la VPN implementada, garantiza un gran nivel de seguridad al momento de transmitir información crítica perteneciente a la organización donde se realiza el presente trabajo de investigación.

Llegamos a un punto elevado de concordancia con Rodríguez y Gonzáles [5], quienes plantean una solución VPN para compartir información y proteger los datos; creando intercambio de ideas, para que puedan ser fácilmente capturas y transformadas a través de internet; manteniendo la información a salvo de intrusiones. Otro de los puntos importantes a tomar en cuenta es que coincidimos en que las VPN's funcionan óptimamente en cualquier sistema operativo, como por ejemplo Windows que es sobre el cuál se ha realizado la implementación descrita en este documento.

Es importante mencionar que tras la búsqueda de nuevas formas de comunicación entre colaboradores, proveedores y clientes; Deyfor encuentra una solución satisfactoria el haber optado por la implementación de una VPN, ya que permite hacer extensión de la red privada corporativa mediante el uso de técnicas criptográficas a más bajo costo ya que utiliza un medio público como estructura física. Estas consideraciones son mencionadas también por Paillier y Arzuaga [6].

Con la implementación de la VPN, los empleados pueden acceder a la red desde cualquier parte donde se encuentren, facilitando la movilidad de los mismos, aumentando exponencialmente sus niveles de productividad. En este punto coincidimos con Trujillo [7] quien hace las mismas aseveraciones respecto de la implementación de VPN.

En el presente trabajo de investigación se documentan aspectos y conceptos relacionados con VPN que sirven como base para justificar el desarrollo de la misma. Con la implementación de VPN en la empresa Deyfor se garantiza el acceso remoto seguro a los recursos digitales y sistemáticos con los que ésta cuenta. Este acceso se realiza de manera íntegra, confidencial y segura; puntos que también menciona Peña [9], así como Alva [10], en sus trabajos de investigación respectivos. A similares conclusiones llegan Díaz y Vieyra [11] en su trabajo de investigación donde afirman que una VPN permite la comunicación segura y en tiempo real entre las sucursales y el centro de operaciones de una organización.

Debido a que no se ha usado software libre para la implementación de la VPN descrita en el presente documento, no podemos negar ni afirmar las consideraciones hechas por Amenero [12], cuyo trabajo se centra en la implementación de VPN haciendo uso de software libre.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

3.1 CONCLUSIONES

- Al término del presente trabajo de investigación, se obtiene como producto final una Red Privada Virtual debidamente implementada con las medidas de seguridad pertinentes. Esta solución tiene la capacidad de facilitar enormemente el trabajo de los usuarios finales que necesiten acceder a los recursos tecnológicos y digitales con los que cuenta la empresa Deyfor sin la necesidad de estar presentes de manera física en sus instalaciones.
- El alcance obtenido con la Red Privada Virtual, ha sido definido de acuerdo a las necesidades de Deyfor E.I.R.L. como el manejo de información, se cuenta con la definición de usuarios, con restricción a la información de acuerdo a sus unidades organizativas, y se ha definido una estructura de manejo del contenido de la información (EDT).
- Se realizó el estudio y análisis de los requisitos de la red Privada Virtual, sobre los cuales se estableció el requisito base que es garantizar la seguridad de la información, a través del establecimiento de usuarios debidamente autentificados, y el acceso a la información de la organización desde cualquier punto donde los colaboradores de Deyfor E.I.R.L. se encuentren. No se puede contar con un sistema totalmente seguro, es por ello que solo se ha utilizado para el caso los recursos de la organización como el protocolo PPTP y firewall de Windows.
- Para la elección de la plataforma que se ha utilizado para la Red Privada Virtual de Deyfor E.I.R.L. se evaluó los equipos con los que ya contaba la organización; para este caso se utilizó un servidor HP ProLiant DL380 Gen9 (S.O. Windows Server 2012 R2), 1 router Cisco modelo DPC-3825 y router Microtik Routerboard RB 3011 Ui AS–RM por parte de lado servidor y por parte del lado cliente equipos con sistema operativo Windows.
- Para el diseño de la red Privada Virtual de Deyfor E.I.R.L., se tomó en cuenta el diseño con el que ya contaba la organización; además de incorporar el diseño del protocolo PPTP, que consta del establecimiento de un tunel, punto a punto para el transporte de la información.
- En cuanto a la Política de seguridad de la Red Privada Virtual se propuso dicho documento donde se establece un modelo de seguridad de la información. Por otro lado en cuanto al cifrado de datos se ha utilizado el protocolo PPTP

(Protocolo de Túnel Punto a Punto); además de contar con firewall, permitiendo la confidencialidad e integridad de dicha información mediante protocolos de encriptación que eviten la manipulación de terceros.

- La red Privada Virtual materia de investigación en este documento ha sido implementada haciendo uso de la infraestructura pública de red con la que cuenta la empresa, por lo que no hubo necesidad de hacer conexiones base (desde cero); se ha implementado haciendo uso de software propietario con lo que se garantiza un mejor funcionamiento y mejores posibilidades de soporte eficaz en caso de presentarse algún tipo de inconveniente. Se tiene estimado un número de conexiones superior a 100, garantizado por el número de conexiones permitidas por el router utilizado para la implementación de la red VPN.
- Para la red Privada Virtual de Deyfor E.I.R.L. se ha establecido un Active Directory de Windows como mecanismo para el manejo de información de manera clara y puntual, diferenciando la información de las diferentes áreas de la organización.
- La Red Privad Virtual mejoró la manera en que se venía gestionando el acceso a la información en la empresa Deyfor, optimizando tiempos en 50% aproximadamente, mejorando la calidad de los servicios de red, y brindando una mayor comodidad a los colaboradores con los que cuenta la empresa. En términos porcentuales la mejora total por área es: Gerencia 55.6%, Recursos Humanos 53.8%, Administración 57.36%, Contabilidad 81.15%, Logística 98.15%, TI 58.24%, Operaciones 76.17%.

3.2 RECOMENDACIONES

- Se recomienda realizar el mantenimiento periódico de todos los equipos que componen la infraestructura de red de la organización a fin de garantizar su correcto funcionamiento y, por ende, evitar fallos que conlleven a gastos imprevistos de reparación.
- Se recomienda informar con la anticipación debida a los usuarios acerca de los beneficios que trae consigo la implementación de cualquier solución tecnológica, puesto que, mejora su desempeño y eficiencia al momento de desarrollar sus actividades diarias.
- Se recomienda a la organización destinar los recursos necesarios, para mejorar la seguridad de la red Privada Virtual, en cuanto al mejoramiento de encriptación de la información y la creación de llaves digitales. Además de evaluar los tipos de ataques que esta pudiera recibir, con mayor estrictez.

- Se recomienda adquirir software como Snort (sistema de prevención de intrusión de código abierto capaz de análisis de tráfico en tiempo real y registro de paquetes) especializado en detección de intrusiones hacia las redes de comunicaciones a fin de garantizar la reducción al mínimo de posibles intrusiones.
- Se recomienda que la empresa destine un mayor monto presupuestario para la adquisición de soluciones tecnológicas destinadas a facilitar el desarrollo de las operaciones organizacionales y, por consiguiente, mejorar la rentabilidad en ingresos mensuales.

REFERENCIAS

[1] J. J. N. e. al, Dirección y Gestión de los Sistemas de Información en la Empresa, Madrid: ESIC, 2006.

[2] J. C. Morales, Sistemas de información en la empresa, Barcelona, España: UOC, 2013.

[3] C. d. P. e. al, Informática y Comunicaciones en la Empresa, Madrid: ESIC, 2004.

[4] M. A. E. H. G. y. L. C. Zambrano, «Bliblioteca Ucab,» 16 Febrero 2009. [En línea]. Available: http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAR6248.pdf. [Último acceso: 21 Abril 2017].

[5] A. P. M. G. y. N. M. M. Rodríguez, «Biblioeca Unitecnología,» 2004. [En línea]. Available: http://biblioteca.unitecnologica.edu.co/notas/tesis/0026335.pdf. [Último acceso: 20 Abril 2017].

[6] L. P. V. y. K. R. A. Araujo, «Biblioteca Unitecnológica,» 2004. [En línea]. Available: http://biblioteca.unitecnologica.edu.co/notas/tesis/0026233.pdf. [Último acceso: 21 Abril 2017].

[7] E. R. T. Machado, Marzo 2006. [En línea]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/214/1/CD-0210.pdf. [Último acceso: 23 Mayo 2017].

[8] V. H. L. Ramírez, «REPOSITORIO UACH,» 2004. [En línea]. Available: limari: http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/sources/bmfcil732p.pdf. [Último acceso: 10 Junio 2017].

[9] D. V. P. Q., «MEDILLO,» Octubre 2016. [En línea]. Available: http://mendillo.info/seguridad/tesis/Pe%C3%B1a.pdf. [Último acceso: 11 Junio 2017].

[10] E. A. Maldonado, «Repositorio PUCP,» 07 11 2013. [En línea]. Available: http://tesis.pucp.edu.pe/repositorio/handle/123456789/4918. [Último acceso: 25 Mayo 2017].

[11] M. A. D. L. y. G. L. A. V. Dioses, «Repositorio UNPRG,» 2015. [En línea]. Available: http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/462/BC-TES-4224.pdf?sequence=1&isAllowed=y. [Último acceso: 27 Mayo 2017].

[12] V. M. Vásquez, «REPOSITORIO UNPRG,» Junio 2012. [En línea]. Available: http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/905/BC-TES-4224.pdf?sequence=1&isAllowed=y. [Último acceso: 10 Junio 2017].

[13] G. P. Duarte, Gestión de Información: Dimensiones e Implemetación para el éxito Organizacional, Rosario, Argentina: Nuevo Pharadigma, 2004.

[14] G. P. Duarte, Gestión de Información en las Organizaciones, Santigo de Chile: Cecapi, 1998.

[15] I. Carrión, «El reto de los Sistemas de Informacion,» [En línea]. Available: https://es.slideshare.net/isabeldsam/captulo-1-el-reto-de-los-sistemas-de-informacion. [Último acceso: 3 10 2017].

[16] W. Stallings, Comunicaciones y Redes de Computadores, Madrid: Prentice Hall, 2004.

[17] NetPrivateer, «Network Infraestructure,» [En línea]. Available: http://www.netprivateer.com/lanwan.html. [Último acceso: 10 10 2017].

[18] TutorialesPoint, «Ethical Hacking - Sniffing,» [En línea]. Available: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm. [Último acceso: 05 12 2017].

[19] OROSK, «OROSK.COM,» [En línea]. Available: http://www.orosk.com/star-topology/. [Último acceso: 15 11 2017].

[20] Allround Computer Solutions, «Topologies,» [En línea]. Available: https://allroundcomputersolutions.weebly.com/topologies.html. [Último acceso: 17 11 2017].

[21] Networks Manía, «Mesh Topology,» [En línea]. Available: https://networksmania.wordpress.com/topics/network-topology/mesh-topology/. [Último acceso: 16 11 2017].

[22] TutorialesPoint, «DCN - Computer Network Toplogies,» [En línea]. Available: https://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm. [Último acceso: 14 10 2017].

[23] K. C. L. y. J. P. Laudon, Sistemas de Información Gerencial, México: Pearson, 2012.

[24] S. C. y. V. C. Jon Postel, Redes de Comunicaciones, España: Güimi, 2009.

[25] P. W. y. M. E. Charlie Scott, Virtual Private Networks, O'Reilly, 1999.

[26] D. Fowler, Virtual Private Networks Making The Right Connection, California: Morgan Kauffman Publisher, Inc, 1999.

[27] Microsoft, «Technet Microsoft,» [En línea]. Available: https://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx. [Último acceso: 13 12 2017].

[28] K. Masica. [En línea]. Available: http://sunsite.uakom.sk/sunworldonline/swol-06-1998/swol-06-ipsec.html. [Último acceso: 14 12 2017].

[29] Cisco, [En línea]. Available: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-19/what-is-a-vpn.html. [Último acceso: 2 12 2017].

[30] Cisco, «Qué es una VPN - Parte II - The Internet Protocol Journal,» [En línea]. Available: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-19/what-is-a-vpn.html. [Último acceso: 13 12 2017].

[31] J. J. K. Eric F Crist, Mstering Open VPN, Packt Publishing, 2015.

[32] VPNTunnel, «VPNTunnel Anonimous Internet,» [En línea]. Available: https://vpntunnel.com/es/faqs/. [Último acceso: 7 12 2017].

[33] W. Z. Xicheng Lu, Networking and Mobile Computing: 3rd International Conference, ICCNMC 2005, Springer: 2005.

[34] K. GUITTEAUD, «IKEv2 Site-to-Site VPN,» [En línea]. Available: https://www.supinfo.com/articles/single/244-ikev2-site-to-site-vpn. [Último acceso: 10 12 2017].

[35] A. I. Graham Bartlett, IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, Cisco Press, 2016.

[36] M. A. Abellán, La evaluación del impacto ambiental de proyectos y actividades agroforestales, La Mancha: Graficas Cuenca S.A, 2006.

[37] S. Ballew, Managing IP Networks with Cisco Routers, USA: O'Reilly & Associates, 1997.

[38] FORBES, «Forbes Global 2000: Top Regarded Companies,» 2017. [En línea]. Available: https://www.forbes.com/companies/cisco-systems/. [Último acceso: 05 Noviembre 2017].

[39] T. Dean, Network + Guide to Network, Boston, USA: Course Technology, Cengage Learning, 2013.

[40] C. Patridge, Gigabit Networking, USA: Addison-Wesley Publishing Company, 1994.

[41] J. A. Gómez, Servicios en Red, España: Editex, 2010.

[42] Cisco, Redes Cisco, México: Gradi S.A., 2010.

[43] «AEM.COM,» [En línea]. Available: https://algoentremanos.com/los-mejores-routers-para-usar-con-tu-red-vpn/. [Último acceso: 07 Setiembre 2018].

[44] Autoridad Nacional de Protección de Datos Personales - MINJUS, Directiva de Seguridad, Lima: Diskcopy sac, 2013.

[45] «Hewlett Packard Enterprise,» [En línea]. Available: https://www.hpe.com/lamerica/es/product-catalog/servers/proliant-servers/pip.hpe-proliant-dl380-gen9-server.7271241.html. [Último acceso: 17 12 17].

[46] J. d. l. Cruz, Windows Server 2012 R2 - Acelerando la Continuidad del Negocio, VEEAM.

[47] Microsoft Corporation, «Windows 10 Pro,» [En línea]. Available: https://www.microsoft.com/es-es/store/d/Windows-10-Pro/DF77X4D43RKT/48DN. [Último acceso: 17 12 17].

[48] F. A. Durán, INGENIERÍA DE MÉTODOS : Técnicas para el Manejo Eficiente de Recursos Organizacionales Fabriles, de Servicios y Hospitalarias, Guayaquil, 2007.

[49] C. M. Soto, Comparación estadística de la confiabilidad alfa de Cronbach, Red Revista de Psicología, 2005.

[50] D. Kosiur, Building and Managing Virtual Private Networks, Wiley Computer Publishing, 1998.

[51] G. G. D. D. Shilpa PareekAshutosh, «Research Gate,» [En línea]. Available: https://www.researchgate.net/figure/316782131_fig6_Fig5-Phishing-Attack-7-Hijack-Attack-In-hijack-attack-a-hacker-takes-over-a-session. [Último acceso: 27 11 2017].

[52] Imperva, «MAN IN THE MIDDLE (MITM) ATTACK,» [En línea]. Available: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html. [Último acceso: 10 12 2017].

[53] Guy Fawkes, «Comparación de protocolos de VPN: PPTP vs L2TP vs OpenVPN vs SSPT vs IKEv2,» [En línea]. Available: https://es.vpnmentor.com/blog/comparacion-de-protocolos-de-vpn-pptp-vs-l2tp-vs-openvpn-vs-sspt-vs-ikev2/. [Último acceso: 13 12 2017].

[54] F. A. A. L. Izaskun Pellejero, Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica, Barcelona: Marcombo, 2006.

FIRMA DEL ASESOR Y TESISTA

----------	----------
Araceli Y. Cueva Mendoza	Ing. Manuel Enrique Malpica Rodríguez
TESISTA	**ASESOR**

ANEXOS

ANEXO 01: FICHA DE ENCUESTA ANTES DE LA IMPLEMENTACIÓN DE LA VPN

OBJETIVO

A través de las siguientes preguntas contenidas en esta ficha de encuesta se busca recolectar datos cualitativos en cuanto a opiniones diversas (de acuerdo a la pregunta planteada) frente a la forma en que se viene gestionando la información dentro de la empresa Deyfor E.I.R.L. Una respuesta consciente ayudará al investigador a realizar un mejor trabajo.

Encuestador - Investigador:	**Araceli Yoselín Cueva Mendoza**
Institución foco	**Deyfor E.R.L.**
Condición del encuestado	Alta Gerencia ☐ Otro ☐

INSTRUCCIONES

Lea con mucho cuidado cada una de las preguntas planteadas a continuación y marque con una x dentro del recuadro de la opción que crea conveniente:

1. La información institucional está disponible desde cualquier punto donde Ud. se encuentre.
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
2. Considera que existe la necesidad de una solución eficaz que ayude a gestionar de manera correcta la información.
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
3. Se siente seguro al momento de transmitir información haciendo uso de dispositivos físicos y/o correos electrónicos.
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo

4. ¿Considera usted que la alta gerencia de la organización concentra los esfuerzos suficientes en cuanto a garantizar la autenticidad, calidad e integridad de la información crítica para la organización?
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
5. Ud. es consciente y ha sido debidamente informado acerca de los peligros que acarrea para la organización el hecho de que la información se transmita haciendo uso de dispositivos electrónicos físicos.
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
6. ¿Considera usted que una mejor gestión de la información institucional ayudaría a aumentar considerablemente la rentabilidad de la organización?
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
7. Debido a que actualmente la información se difunde a través de medios físicos, existe un riesgo alto de pérdida o fuga de la misma.
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
8. El acceso a la información organizacional de manera rápida y oportuna, presenta altos niveles de dificultad por la forma en que se realiza.
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
9. ¿Recomendaría de manera inequívoca que se implemente una solución inmediata que ayude a gestionar el acceso y transmisión de información organizacional?
   - ☐ (1) Altamente de acuerdo
   - ☐ (2) De acuerdo
   - ☐ (3) Indiferente
   - ☐ (4) En desacuerdo
   - ☐ (5) Altamente en desacuerdo
10. ¿Si se implementan soluciones para administrar de manera correcta la información institucional, ud. estaría dispuesto a adaptarlas rápidamente?
    - ☐ (1) Altamente de acuerdo
    - ☐ (2) De acuerdo
    - ☐ (3) Indiferente
    - ☐ (4) En desacuerdo
    - ☐ (5) Altamente en desacuerdo

ANEXO 02: FICHA DE ENCUESTA DESPUÉS DE LA IMPLEMENTACIÓN DE LA VPN

OBJETIVO

A través de las siguientes preguntas contenidas en esta ficha de encuesta se busca recolectar datos cualitativos en cuanto a opiniones diversas (de acuerdo a la pregunta planteada) frente a la implementación de la red VPN dentro de la empresa Deyfor E.I.R.L. Una respuesta consciente ayudará al investigador a realizar un mejor trabajo.

Encuestador - Investigador:	**Araceli Yoselín Cueva Mendoza**
Institución foco	**Deyfor E.R.L.**
Condición del encuestado	Alta Gerencia ☐ Otro ☐

INSTRUCCIONES

Lea con mucho cuidado cada una de las preguntas planteadas a continuación y marque con una x dentro del recuadro de la opción que crea conveniente:

1. La VPN implementada dentro de la empresa Deyfor constituye una solución fiable y segura para la transmisión de información crítica institucional.
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
2. Las contraseñas de usuario asignadas para el acceso a VPN, cumplen con los requisitos mínimos de seguridad exigidos.
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
3. Las contraseñas de usuario asignadas para el acceso a la VPN son fáciles de recordar.
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
4. ¿Considera usted que la relación costo – beneficio después de implementar la Red Privad Virtual tiene un balance positivo?
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo

5. La velocidad de transferencia de información a través de la VPN es considerablemente alta, es decir, mayor a la velocidad de transferencia usada anteriormente.
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
6. ¿Considera usted que el sistema implementado contribuye al aumento de la rentabilidad de la empresa?
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
7. El acceso a la información institucional mediante VPN está disponible desde cualquier equipo que soporte ejecución de un navegador web.
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
8. Los desarrolladores de la red VPN abordan oportunamente las incidencias presentadas
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
9. El equipo de desarrollo realizó las jornadas de capacitación necesarias para entrenarlo a usted en el correcto uso de la VPN.
   - ☐ (6) Altamente de acuerdo
   - ☐ (7) De acuerdo
   - ☐ (8) Indiferente
   - ☐ (9) En desacuerdo
   - ☐ (10)Altamente en desacuerdo
10. ¿La Red Privada Virtual que se ha implementado es tan eficiente que no dudaría en recomendar su implementación a otras empresas cuyas operaciones sean similares a las de Deyfor?
    - ☐ (6) Altamente de acuerdo
    - ☐ (7) De acuerdo
    - ☐ (8) Indiferente
    - ☐ (9) En desacuerdo
    - ☐ (10)Altamente en desacuerdo
11. ¿Usted se siente seguro al momento de transferir información confidencial a través de la Red Privada Virtual?
    - ☐ (1) Altamente de acuerdo
    - ☐ (2) De acuerdo
    - ☐ (3) Indiferente
    - ☐ (4) En desacuerdo
    - ☐ (5) Altamente en desacuerdo

12. ¿La Red Privada Virtual implementada contribuye al logro de objetivos estratégicos de la empresa Deyfor E.I.R.L.?
    - ☐ (1) Altamente de acuerdo
    - ☐ (2) De acuerdo
    - ☐ (3) Indiferente
    - ☐ (4) En desacuerdo
    - ☐ (5) Altamente en desacuerdo

GRACIAS POR SU COLABORACIÓN

ANEXO 03: MATRIZ DE PROCESAMIENTO DE DATOS DE ENCUESTA

Tabla 23: Matriz de procesamiento de resultados de encuestas

N°	PREGUNTA	ID	ESCALA				
			1	**2**	**3**	**4**	**5**
1	La VPN implementada dentro de la empresa Deyfor constituye una solución fiable y segura para la transmisión de información crítica institucional.	Pregunta1					
2	Las contraseñas de usuario asignadas para el acceso a VPN, cumplen con los requisitos mínimos de seguridad exigidos.	Pregunta2					
3	Las contraseñas de usuario asignadas para el acceso a la VPN son fáciles de recordar.	Pregunta3					
4	Considera usted que la relación costo – beneficio después de implementar la Red Privad Virtual tiene un balance positivo	Pregunta4					
5	La velocidad de transferencia de información a través de la VPN es considerablemente alta, es decir, mayor a la velocidad de transferencia usada anteriormente.	Pregunta5					
6	Considera usted que el sistema implementado contribuye al aumento de la rentabilidad de la empresa	Pregunta6					
7	El acceso a la información institucional mediante VPN está disponible desde cualquier equipo que soporte ejecución de un navegador web.	Pregunta7					
8	Los desarrolladores de la red VPN abordan oportunamente las incidencias presentadas	Pregunta8					
9	El equipo de desarrollo realizó las jornadas de capacitación necesarias para entrenarlo a usted en el correcto uso de la VPN.	Pregunta9					
10	La Red Privada Virtual que se ha implementado es tan eficiente que no dudaría en recomendar su implementación a otras empresas cuyas operaciones sean similares a las de Deyfor	Pregunta10					
11	Usted se siente seguro al momento de transferir información confidencial a través de la Red Privada Virtual	Pregunta11					
12	La Red Privada Virtual implementada contribuye al logro de objetivos estratégicos de la empresa Deyfor E.I.R.L.	Pregunta12					

ANEXO 04: VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Gracias al uso del software estadístico informático IMB SPSS en su versión 25, es posible realizar las pruebas de fiabilidad alfa (**alpha de Cronbach**) de los instrumentos de recolección de datos. El alfa de Cronbach determina la fiabilidad de un instrumento bajo los siguientes criterios:

- ✓ Coeficiente alfa >.9 es excelente
- ✓ Coeficiente alfa >.8 es bueno
- ✓ Coeficiente alfa >.7 es aceptable
- ✓ Coeficiente alfa >.6 es cuestionable

Ficha de encuesta N°1: Se realizan 10 encuestas de prueba aleatorias con la finalidad de determinar qué tan fiable es este instrumento de recolección de datos, los resultados obtenidos fueron los siguientes:

Tabla 24: Estadísticas por elemento - análisis de fiabilidad ficha encuesta N°1

Estadísticas de elemento

	Media	Desviación	N
Pregunta1	2,70	1,494	10
Pregunta2	2,90	1,524	10
Pregunta3	2,90	,994	10
Pregunta4	3,00	1,491	10
Pregunta5	2,80	1,229	10
Pregunta6	2,50	1,269	10
Pregunta7	2,70	1,418	10
Pregunta8	2,40	1,350	10
Pregunta9	2,10	1,101	10
Pregunta10	2,50	1,354	10

Tabla 25: Resumen procesamiento de casos - análisis de fiabilidad ficha encuesta N°1

Resumen de procesamiento de casos

		N	%
Casos	Válido	10	100,0
	Excluido[a]	0	,0
	Total	10	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Tabla 26: Nivel de fiabilidad alfa - análisis de fiabilidad ficha encuesta N°1

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,876	,877	10

Ficha de encuesta N°2: Se realizan 10 encuestas de prueba aleatorias con la finalidad de determinar qué tan fiable es este instrumento de recolección de datos, los resultados obtenidos fueron los siguientes:

Tabla 27: Estadísticas por elemento - análisis de fiabilidad ficha encuesta N°2

Estadísticas de elemento

	Media	Desv. Desviación	N
Pregunta1	2,70	1,337	10
Pregunta2	2,70	1,418	10
Pregunta3	2,70	1,059	10
Pregunta4	2,90	1,595	10
Pregunta5	2,40	1,350	10
Pregunta6	2,20	1,398	10
Pregunta7	2,60	1,430	10
Pregunta8	2,40	1,350	10
Pregunta9	1,90	1,101	10
Pregunta10	2,40	1,350	10
Pregunta11	2,00	1,414	10
Pregunta12	2,40	1,350	10

Tabla 28: Resumen procesamiento de casos - análisis de fiabilidad ficha encuesta N°2

Resumen de procesamiento de casos

		N	%
Casos	Válido	10	100,0
	Excluido[a]	0	,0
	Total	10	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Tabla 29: Nivel de fiabilidad alfa - análisis de fiabilidad ficha encuesta N°2

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,906	,904	12

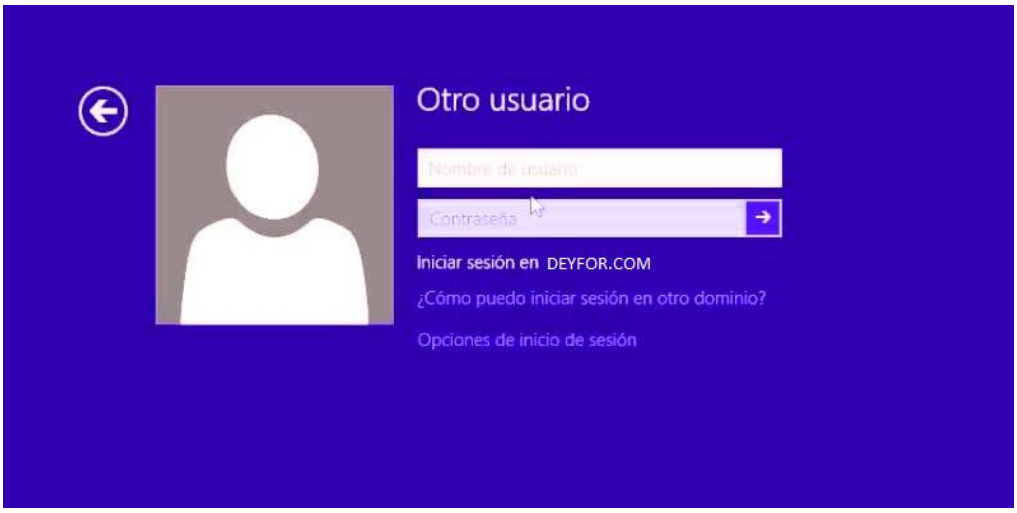
ANEXO 05: MANUAL DE ACCESO AL SERVIDOR Y A LA VPN DEYFOR

A. ACCESO AL SERVIDOR

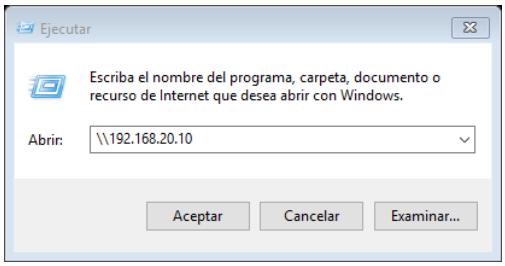
NOTA: Para iniciar sesión con usuarios de domino (SERVIDOR), se debe tener en cuenta que cada máquina de la empresa debe estar unida a dominio; estas configuraciones han sido dadas por el área de TI.

Usted podrá acceder a la información del servidor siempre y cuando se encuentre conectado dentro de las redes de la empresa DEYFOR, si usted quisiese acceder desde fuera, tendría que estar conectado a la red VPN; este procedimiento lo explicaremos más adelante.

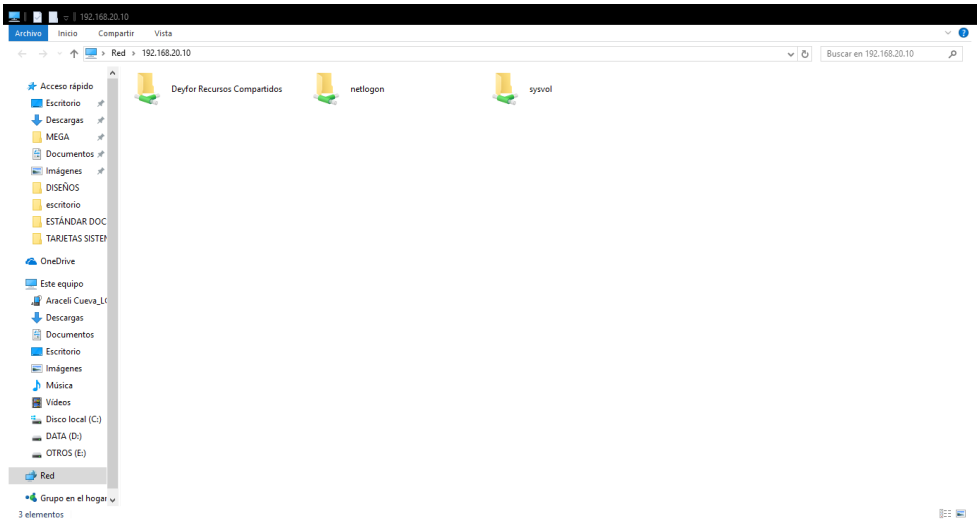
1. **Iniciar sesión con usuarios de dominio:**
   Al iniciar el sistema operativo tú tendrás, la opción de iniciar con tu usuario frecuente y otro usuario, seleccionamos Otro Usuario e ingresamos nuestras credenciales:



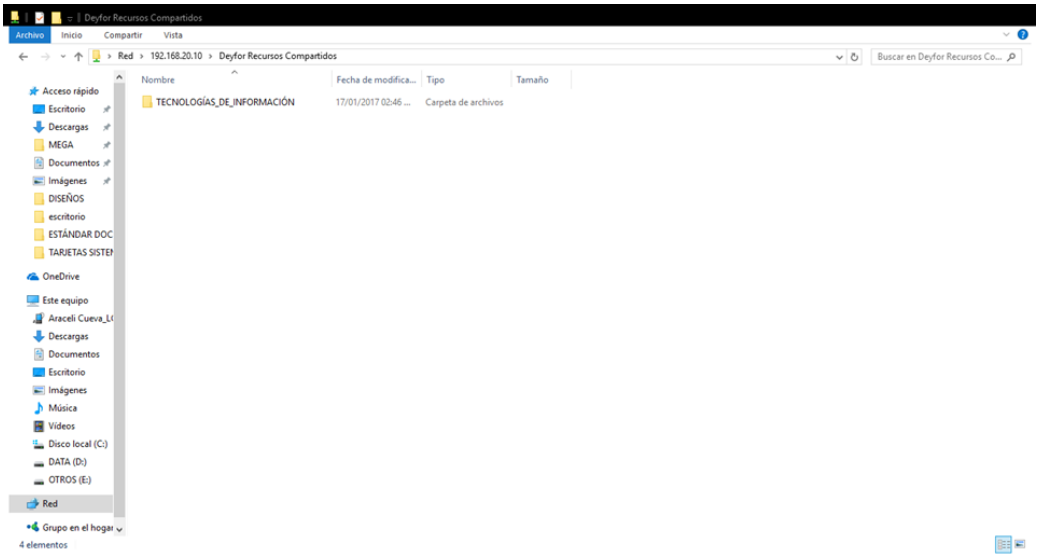
2. **Si usted inicia por primera vez esto puede tardar unos minutos.**
3. **Luego de esto usted deberá abrir la ventana de ejecutar.**
   Esta ventana puede ser abierta presionando la tecla Windows (⊞) + la letra R.
   Y escribir la siguiente dirección IP: \\192.168.20**192.168.20.10** .10 y clic en aceptar.



Esperamos unos minutos para que cargue, luego nos abrirá una ventana, en la cual encontraremos una carpeta con el Nombre: **Deyfor Recursos Compartidos**



Una vez dentro de la carpeta esta cargará de acuerdo a los archivos que se tenga permisos acceder.

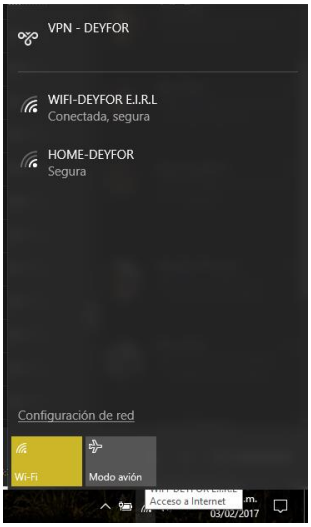


4. **Aquí usted podrá disponer de acuerdo a su área de la información que se requiera.**

B. ACCESO AL SERVIDOR A TRAVÉS DE LA VPN

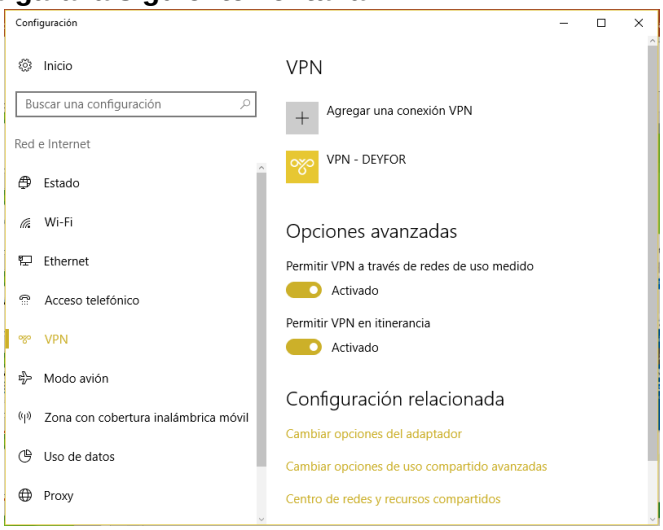
NOTA: Para poder conectarse a la red VPN – DEYFOR, es necesario que en nuestra máquina se hayan hecho anteriormente las configuraciones para dicha red VPN (estas configuraciones deben estar echas por lo ideal dentro del usuario de dominio). En caso no se hayan hecho estas configuraciones, más adelante mostramos el apartado para que usted realice estas configuraciones.

1. **Si el equipo que usted está usando, ya se realizaron las configuraciones correspondientes, en la barra d de tareas dónde localizamos el icono del adaptador de red bien sea por wifi o por cable; damos doble clic a este y nos aparecerá la siguiente pantalla, según la red en que estemos conectados:**

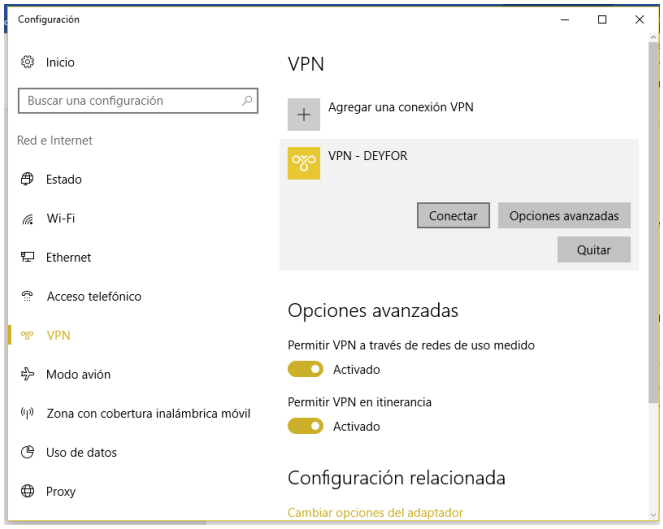


2. **Damos doble clic en donde aparece VPN – DEYFOR:**

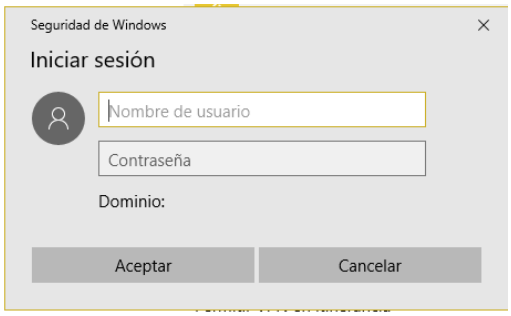
3. **Luego nos cargará la siguiente ventana:**



4. **Damos doble clic en VPN – DEYFOR:**



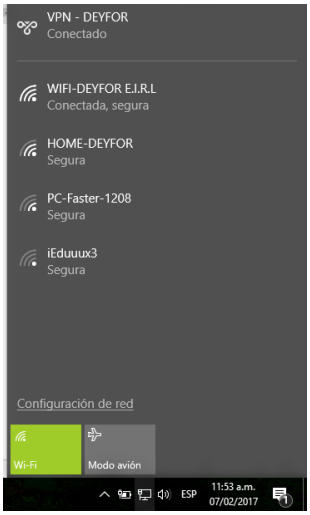
5. **Damos clic en conectar, y en la siguiente ventana ingresaremos nuestras credenciales, anteriormente entregadas por la oficina de TI por correo electrónico:**



6. **Una vez ingresadas las credenciales, y si estas son correctas observaremos la siguiente ventana lo cual indica que ya estamos conectados.**

7. **Luego de esto observaremos que nuestro adaptador de red, aparece como si estuviésemos recibiendo red por cable, esto es completamente normal, debido a que nos hemos conectado a la red VPN – DEYFOR. Luego dando clic en el adaptador de red:**

Observaremos el siguiente escenario:

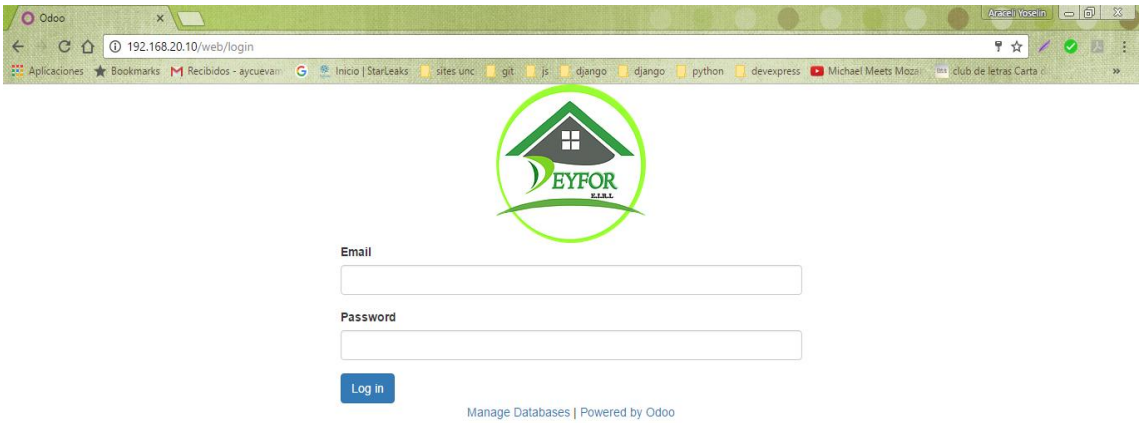


8. **En esta pantalla se observa que ya estamos conectados tanto a una red cualquiera sea el caso de usted, y tanto a la VPN – DEYFOR. Ahora ya que estamos conectados a la VPN, podemos acceder al servidor de archivos**

DEYFOR, con los pasos desarrollados y explicados anteriormente para el acceso al SERVIDOR en el punto A.

9. **También podremos acceder a la ERP (Sistema para la gestión logística que se viene implementando actualmente en la institución). Abriendo cualquier navegador e ingresando la siguiente dirección:** 192.168.20.10

Observaremos un escenario similar al siguiente:



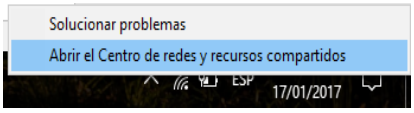
NOTA: Las credenciales para acceder al sistema, serán proporcionadas por el área de TI, en cuanto se culmine con la implementación de éste.

C. UNIR MÁQUINA A VPN - DEYFOR

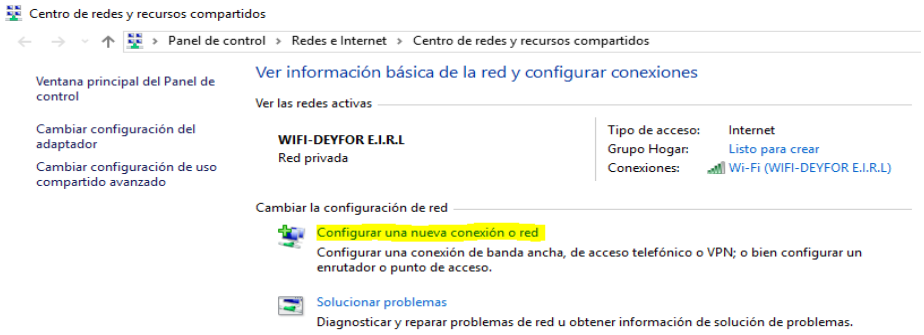
NOTA: Para unir cualquier máquina a la red VPN – DEYFOR, debe seguir los siguientes pasos, para que estos sigan correctamente se recomienda conectarse a internet a cualquier red que sea posible, que permita hacer la conexión.

Es importante aclarar también que estas configuraciones no afectan en nada si se realizan en máquinas personales; si usted realiza esta configuración podrá acceder de igual manera que las otras computadoras a la información solo ingresando las credenciales.

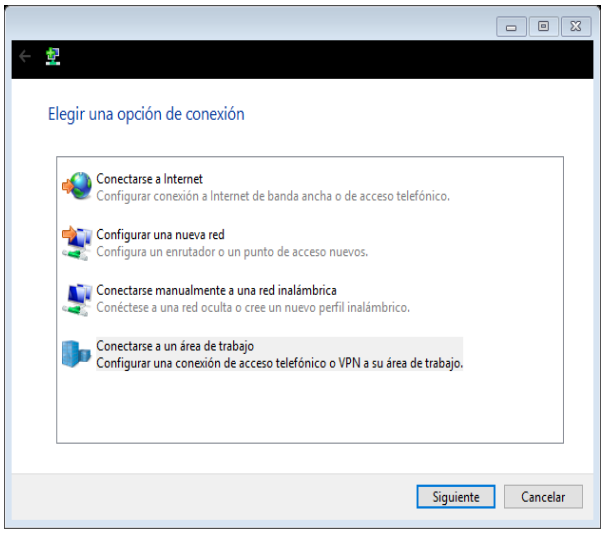
1. **Diríjase al icono del adaptador de red ya sea por cable o wifi, damos clic derecho y luego damos clic en *Abrir Centro de Redes y Recursos Compartidos*:**



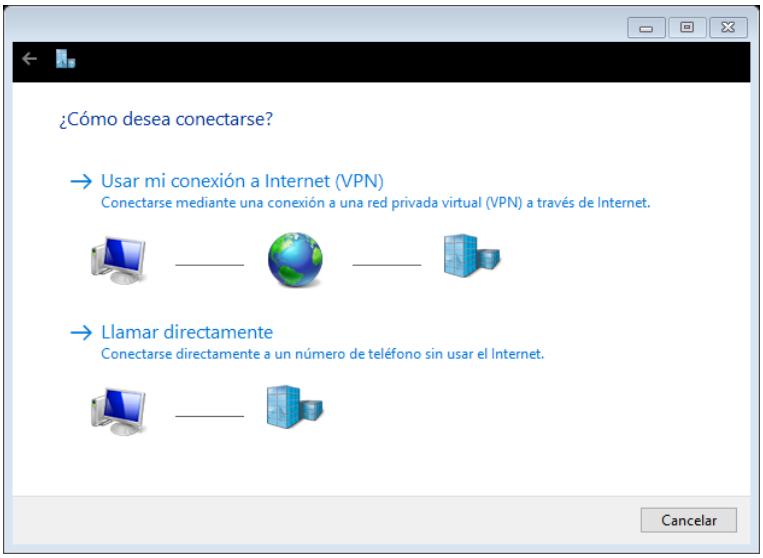
2. **Se abrirá la siguiente ventana, en la cual daremos clic en *Configurar una nueva conexión o red*:**



3. **Se abrirá una ventana como la siguiente, amos click en *Conectarse a un Área de Trabajo:***



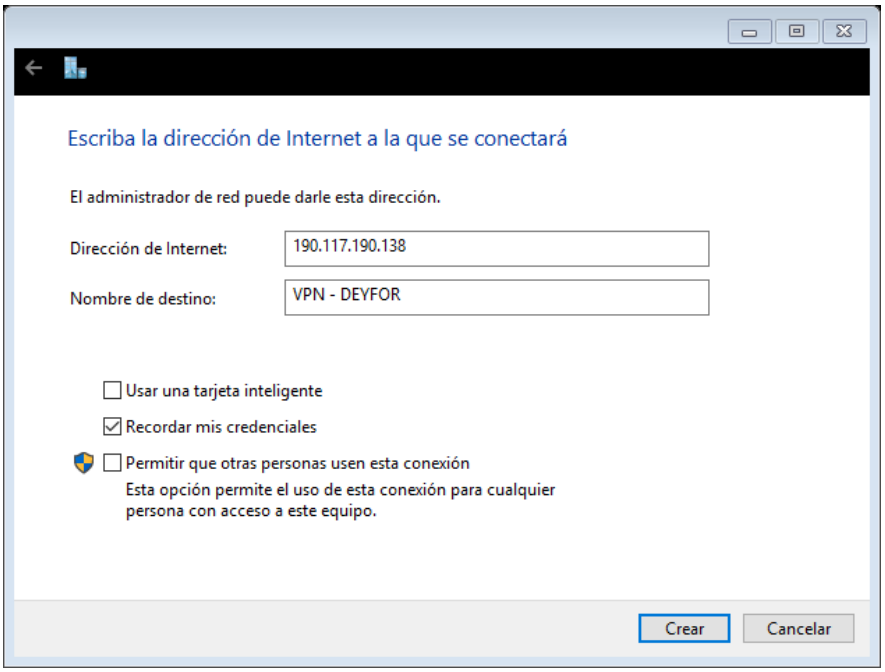
4. **En la siguiente ventana hacemos clic en *Usar mi conexión a Internet (VPN):***



5. **Se abrirá una ventana, en la cual llenaremos los datos, damos clic en crear:**

Dirección de Internet: 190.117.190.138

Nombre de Destino: VPN – DEYFOR


Escriba la dirección de Internet a la que se conectará
El administrador de red puede darle esta dirección.
Dirección de Internet:
190.117.190.138
Nombre de destino:
VPN - DEYFOR
Usar una tarjeta inteligente
Recordar mis credenciales
Permitir que otras personas usen esta conexión
Esta opción permite el uso de esta conexión para cualquier persona con acceso a este equipo.
Crear
Cancelar

6. **Con esto observaremos, que la red ha sido creada, observamos esto haciendo clic en el icono del adaptador de red del computador, y tendremos un escenario parecido al siguiente:**

7. **Ahora que tenemos la red VPN – DEYFOR configurada, procedemos a conectarnos siguiendo los pasos explicados anteriormente en el punto B, para conectarnos a la red VPN, y luego de esto seguir los pasos del punto A, para acceder a los archivos.**

ANEXO 06: SOLICITUD DE VALIDACIÓN DE INSTRUMENTOS DIRIGIDA A UN EXPERTO

Señor:

Enrique Fernández Mendoza

CREATIVIDAPPS E.I.R.L

Presente

Reciba un cordial saludo

Teniendo conocimiento de su reconocida formación y experiencia en temas relacionados al desarrollo de soluciones de software para diversas organizaciones, me complace dirigirme a usted en respuesta a su valiosa colaboración para la validación de los instrumentos que anexo, el mismo que servirá para recolectar información relativa a la investigación denominada: "**IMPACTO DE LA IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL EN LA GESTIÓN DE INFORMACIÓN DE LA EMPRESA DEYFOR E.I.R.L."**, investigación que estoy realizando para obtener mi Título Profesional de Ingeniero de Sistemas.

Asimismo, anexo los instrumentos para la validación de los instrumentos y el cuadro de variables e indicadores para una rápida comprensión y validación de estos.

Agradeciendo su valiosa colaboración en el desarrollo e impulso de la investigación, me suscribo.

Muy cordialmente.

Bach. Araceli Yoselín Cueva Mendoza

ANEXO 07: RESULTADOS DEL JUICIO DE EXPERTOS

Creatividapps

FICHA PARA VALIDACION DEL INSTRUMENTO

I. **REFERENCIA**

1.1. Experto: Enrique Fernández Mendoza
1.2. Especialidad: Ing. Sistemas
1.3. Cargo actual: Gerente
1.4. Grado académico: Universitario
1.5. Institución: Creatividapps
1.6. Tipo de instrumento: Encuesta
1.7. Lugar y fecha: 15-05-18

II. **TABLA DE VALORACION POR EVIDENCIAS**

N°	EVIDENCIAS	VALORACION					
		5	4	3	2	1	0
1	Pertinencia de indicadores	✓					
2	Formulado con lenguaje apropiado	✓					
3	Adecuado para los sujetos en estudio		✓				
4	Facilita la prueba de hipótesis		✓				
5	Suficiencia para medir la variable		✓				
6	Facilita la interpretación del instrumento			✓			
7	Acorde al avance de la ciencia y tecnología		✓				
8	Expresado en hechos perceptibles		✓				
9	Tiene secuencia lógica		✓				
10	Basado en aspectos teóricos		✓				
	Total	10	28	3			

Coeficiente de valoración porcentual: c = 78%

III. **OBSERVACIONES Y/O RECOMENDACIONES**

.....
.....
.....
.....
.....

CREATIVIDAPPS E.I.R.L.
Enrique G. Fernández Mendoza
GERENTE
Firma y sello del Experto

ANEXO 08: EXTRACTO DEL PLAN DE CONTINGENCIA

Resumen

El plan de contingencia es el proceso de garantizar que la información esencial se pueda mantener accesible para los colaboradores de la empresa Deyfor E.I.R.L. a lo largo de una variedad de incidentes y emergencias. El Plan de Contingencia se esfuerza por proteger la confidencialidad, integridad y disponibilidad de Información. El Plan de Contingencia sirve para identificar operaciones o funciones comerciales esenciales; las instalaciones, equipos, registros, personal y otros recursos necesarios para realizar esas funciones; y los planes para permitir una recuperación efectiva de un evento que afecte el funcionamiento normal.

Propietario del plan

Guillermo Huamán Mantilla – Gerente General Deyfor E.I.R.L.

Análisis del impacto del negocio

Uno de los recursos tecnológicos más importantes con el que cuenta la organización es el servidor institucional, puesto que, es en este servidor donde se almacena información de cualquier índole. Además, como recursos críticos para el correcto funcionamiento de la Red Privada Virtual, se encuentra el router, switches, cableado estructurado.

Amenazas y riesgos

Los riesgos potenciales se listan a continuación:

- Incendios, paralizan todas las operaciones institucionales incluyendo pérdidas monetarias cuantiosas y, en el peor de los casos, pérdidas humanas.
- Pérdida de conexión con el servidor de dominios del ISP, la información contenida dentro del servidor a la que se accede a través de la red, se encuentra inaccesible.
- Borrado accidental de la información contenida en los discos del servidor, si no se cuenta con copias de seguridad, la pérdida de información constituye un retroceso en cuanto a la búsqueda y/o consecución de los objetivos de negocio.

Plan de operaciones en modo de emergencia.

A continuación, se listan las distintas medidas a tomar por parte de la organización ante una situación de emergencia:

- Cumplir con el cronograma establecido de mantenimiento de la red VPN con el que cuenta la organización, a detalle y de manera efectiva.
- Identificar si los fallos de deben a problemas de conectividad de Red, o problemas con los equipos con los que se da el servicio, problemas con la Seguridad de Transferencia:
  - Problemas de Conectividad de Red: Se hará un testo de la red midiendo con una herramienta llamada SpeedTest, para determinar el ancho de banda y la velocidad con que cuenta la transmisión de información. En caso de depender de ello se contactará con el ISP, que permita solucionar problemas como pérdida de conexión con el servidor de dominios, lentitud de conexión, etc; con un tiempo estimado de 1 a 2 horas.
  - Problemas con equipos: Se realizará un testeo del funcionamiento de estos equipos. En caso deberse algún fallo de este tipo se deberá buscar una evaluación de personal dedicado; debido a esto no podemos determinar tiempo explícitamente. Para garantizar con la continuidad de la información contenida dentro del servidor tenga el respaldo necesario en discos duros externos y de ser posible también contar con almacenamiento en la nube.
  - Problemas con la seguridad de Transferencia de datos: Se deberá instalar software de vigilancia de redes, como por ejemplo Nagios con Centreón como interfaz gráfica; con la finalidad de vigilar el tráfico en la red permitiendo al administrador de la misma conocer los cuellos de botella que dificultan su óptimo desempeño.

ANEXO 09: EXTRACTO DE LA POLÍTICA DE CONFIDENCIALIDAD DE DEYFOR E.I.R.L.

La confidencialidad y debida protección de la información personal confiada a Deyfor E.I.R.L. En adelante EL EMPLEADOR es de máxima importancia. Deyfor E.I.R.L. Está comprometido a manejar sus datos personales de manera responsable y con apego a la normatividad aplicable.

Para Deyfor E.I.R.L. resulta necesaria la recopilación de ciertos datos personales para llevar a cabo las actividades intrínsecas a su giro comercial y mercantil. Deyfor E.I.R.L. tiene la obligación legal y social de cumplir con las medidas de confidencialidad y de seguridad suficientes para proteger aquellos datos personales que haya recabado para las finalidades que en la presente política de privacidad serán descritas.

Todo lo anterior se realiza con el objetivo de que usted tenga pleno control y decisión sobre sus datos personales. Por ello, le recomendamos que lea atentamente la siguiente información.

Deyfor E.I.R.L. para cumplir con las finalidades de la relación laboral podrá recolectar y tratar en algunos casos específicos, datos personales sensibles, como aquellos que pueden revelar aspectos relacionados con estado de salud presente y futura, datos biométricos, información relacionada con el estilo de vida, entre otros. Nos comprometemos a que los mismos serán tratados bajo estrictas medidas de seguridad, siempre garantizando su confidencialidad.

1. Finalidad del Tratamiento de Datos:

Los datos personales de los EMPLEADOS podrán ser utilizados para las siguientes finalidades primarias y necesarias relacionadas con el desempeño de su relación laboral:

- Identificación.
- Resguardo de información de prestaciones de empleados.
- Gestión de seguros personales.
- Gestión de nóminas y prestaciones.
- Administración de fondos, gestión de préstamos y cajas de ahorro
- Administración de personal.
- Emisión y gestión de beneficios.
- Administración de personal para el alta, baja (cartas de renuncia, información de entrevistas de salida, pólizas de finiquitos por cada

concepto de prestación, cambios (promociones, transferencias) de empleados.

- Evaluaciones del desempeño y reportes de competencias, capacitaciones, clima laboral (cumpleaños, empleados destacados, comunicación formal de quejas y sugerencias de los empleados–línea telefónica).
- Información y contacto con clientes.
- En general, cualquier actividad necesaria para el desempeño de la relación laboral.

2. Transferencias y Transmisiones de datos:

Sus datos pueden ser transmitidos a empresas subsidiarias y terceros con relaciones contractuales con la compañía. Para ello, en el contrato correspondiente Deyfor E.I.R.L. incluirá las obligaciones pertinentes para garantizar que dichas empresas subsidiarias y terceros otorgan el nivel de protección de datos personales requerido por la Ley.

Asimismo, Deyfor E.I.R.L. para cumplir la(s) finalidad(es) necesarias anteriormente descrita(s) u otras exigidas legalmente; o por las autoridades competentes sólo transferirá los datos necesarios en los casos legalmente previstos.

En todo momento, Deyfor E.I.R.L. salvaguardará la confidencialidad de los datos y el procesamiento de estos de tal manera que su privacidad esté protegida en términos de la Ley, garantizando el cumplimiento de la presente política por la empresa y por aquellos terceros con quienes mantenga una relación jurídica para la adecuada prestación de sus servicios.

ANEXO 10: EXTRACTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE DEYFOR E.I.R.L.

En Deyfor E.I.R.L., la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, Deyfor E.I.R.L. implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes. El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en Deyfor E.I.R.L.; este proceso será liderado de manera permanente por el Oficial de Seguridad de la Información. Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

1. Políticas Generales:

1. Deyfor E.I.R.L. ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:
2. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de Deyfor E.I.R.L.
3. Los activos de información de Deyfor E.I.R.L., serán identificados y clasificados para establecer los mecanismos de protección necesarios.
4. Deyfor E.I.R.L. definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

5. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
6. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de Deyfor E.I.R.L.
7. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución.
8. Es responsabilidad de todos los funcionarios y contratistas de Deyfor E.I.R.L. reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.