Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática
Escuela Profesional de Ingeniería Informática

Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Tesis

Para optar el Título Profesional de Ingeniero Informático

autor

Jose Luis Ataypoma Llanto

Asesor

Ing. Carlos Manuel Cruz Castañeda

Huacho – Perú

2023

COMO LA IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL (VPN) MEJORA LA COMUNICACIÓN DE LAS OFICINAS EXTERNAS DE LA UNIVERSIDAD JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

INFORME DE ORIGINALIDAD

15%	14%	0%	9%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unjfsc.edu.pe Fuente de Internet	3%
2	www.ecured.cu Fuente de Internet	2%
3	Submitted to Universidad Nacional Jose Faustino Sanchez Carrion Trabajo del estudiante	2%
4	tareaseinvestigaciones440211006.wordpress.com Fuente de Internet	1%
5	Submitted to Universidad Peruana de Las Americas Trabajo del estudiante	1%
6	blogsgallegosmundoinformatico.blogspot.com Fuente de Internet	1%
7	repositorio.unprg.edu.pe:8080 Fuente de Internet	1%
8	2481331242.blogspot.com	

DEDICATORIA

A Dios por cada una de las personas que puso en mi camino. A mi Padres Felipa Llanto y Eladio Ataypoma Arotoma, por apoyarme en transcurso de mi carrera. A mis hermanos Rocío Ataypoma, Moisés Ataypoma, Isaac Ataypoma y mi sobrina Alessia Pomalazo que me han dado la fuerza y acompañado durante esta etapa de mi vida. A ustedes les dedico el trabajo de grado.

AGRADECIMIENTO

En esta parte importante de mi vida, expreso mi agradecimiento a:

Mis padres y maestros por su constate apoyo a lo largo de toda mi etapa de desarrollo profesional.

También hacer una grata mención al Ing. Carlos Márquez, Ing. Carlos Cruz, por la orientación y apoyo prestado tanto con la parte Metodológica y como el Marco conceptual, conocimientos claves para la base y culminación de esta Tesis. Sus aportes sus conocimientos permitieron mejorar la culminación de la Tesis.

RESÚMEN

El presente estudio denominado tiene como **Objetivo:** Determinar la implementación de una red privada virtual (VPN) y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión. **Metodología**: Se empleó el método científico de tipo de investigación fue básica, conocida como pura o fundamental, el nivel de investigación fue correlacional, es decir, el analista reflexiona de forma contemplada, utilizando la técnica deductiva, para reaccionar a los problemas planteados y tiene como principal ayuda, la percepción. **Material y Método: Población:** El universo de población constó de 35 administrativos de las oficinas externas de la Universidad José Faustino Sánchez Carrión. **Conclusión:** Como la implementación de una red privada virtual (VPN) mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Spearman que arroja un valor de 0,907 lo que presenta una muy buena asociación.

Palabras claves: Red privada virtual y comunicación.

ABSTRACT

The objective of this study is to: Determine the implementation of a virtual private network (VPN) and the improvement of the communication of the external offices of the José Faustino Sánchez Carrión University. Methodology: The scientific method of the type of research was basic, known as pure or fundamental, the level of research was correlational, that is, the analyst reflects in a contemplated way, using the deductive technique, to react to the problems raised and has as the main aid, perception. Material and Method: Population: The population universe consisted of 35 administrative staff from the external offices of the José Faustino Sánchez Carrión University. Conclusion: How the implementation of a virtual private network (VPN) significantly improves the communication of the external offices of the José Faustino Sánchez Carrión University, due to the Spearman correlation that yields a value of 0.907, which presents a very good association.

Keywords: Virtual private network and communication.

ÍNDICE

ÍNDICE DE TABLA

ÍNDICE DE FIGURA

INTRODUCCIÓN

En el tiempo que vivimos se caracteriza por la creación y la implementación de toda clase de tecnologías de la información. En la actualidad, las organizaciones han incrementado las implementaciones de una VPN, dicha implementación se encarga de conectar usuario remoto a la LAN de las Organizaciones, Instituciones. La conexión vía OpenVPN, que ofrece una conectividad de punto a punto con una validación, jerárquica de usuario y host conectados remotamente. La conexión a través de una infraestructura pública, permite la reducción de costos en su implementación y se puede establecer una conexión segura de cualquier ubicación geográfica.

En la actualidad la Universidad cuenta con oficinas descentralizadas, la cual requiere una comunicación LAN directa con el Campus Universitario, desde este punto la conexión VPN facilitara acceso a los recursos compartidos.

La investigación se estructuró de la siguiente manera: el Capítulo I toma en cuenta el problema al describir la realidad problemática, y la formulación del problema con sus respectivos objetivos de investigación toma en cuenta la justificación de la investigación, los límites del estudio, la viabilidad del estudio y las estrategias metodológicas. En el segundo capítulo del marco teórico, que contiene los antecedentes del estudio, que toma en cuenta la investigación en conexión con el estudio y luego de las publicaciones, realizamos en los fundamentos teóricos la discusión de teorías sobre la variable independiente y dependiente, definiciones de términos sistema de hipótesis básicas y operacionalización. de variables. En el Capítulo III, el marco metodológico, que contiene el diseño de la investigación, la población y la muestra, las técnicas de adquisición de datos y las técnicas de procesamiento

de información, el Capítulo IV contiene los resultados estadísticos con el programa estadístico SPSS 24.0 y sus respectivas pruebas de hipótesis, en el Capítulo V se tiene en cuenta la discusión de los resultados, en el Capítulo VI contiene las conclusiones, recomendaciones y finalmente las referencias bibliográficas y sus respectivos anexos.

CAPÍTULO I

PLANTAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

La Universidad Nacional José Faustino Sánchez Carrión (UNJFSC), es una Universidad pública ubicada en la ciudad de huacho al norte de la ciudad de Lima en Perú. Fue creada en el año 1968, constituyéndose como la primera Universidad de la provincia de Huaura del Departamento de Lima. En el presente, la Universidad ofrece un servicio de calidad en la enseñanza académicas a través de 13 facultades y 46 escuelas profesionales.

La Universidad Nacional José Faustino Sánchez Carrión (UNJFSC) cuenta con distintas áreas administrativas y académicas, 4 altas direcciones, 39 oficinas, y 46 unidades ubicados dentro del campus Universitario, contando además con oficinas fuera de la ciudad Universitaria, como son la oficina de órgano de control institucional (auditoria), el centro de idiomas, centro Pre Universitario y el museo arqueológico.

Las oficinas externas de la Universidad José Faustino Sánchez Carrión (UNJFSC) no cuentan con las aplicaciones a nivel de escritorio que tienen conectividad a nivel LAN; tal como es el Sistema Integrado de Gestión Administrativa (SIGA) donde se realiza los requerimientos de bienes y servicios, requerimiento del plan anual, se realiza el avance del cuadro de necesidades trimestral, el plan de adquisiciones, plan operativo institucional.

El Sistema Integrado de Tramites Documentario (SISTRAD) es un sistema desarrollado por la identidad para optimizar los procesos administrativos; los procesos administrativos son:

- Recepción de expediente inicio del proceso administrativo para la verificación de folios, procedencia.
- Tramitar expediente dar por concluido la recepción del expediente para el área o unidad correspondiente.
- Restaurar expediente un error del documento al momento de tramitar.

Otros recursos disponibles a nivel de red de área local (LAN).

La autenticación de las licencias del antivirus (f-Secure) y actualización de los mismos requieren también una conexión LAN hacia el servidor que maneja la consola de políticas de administración (Policy Manager Consolé), a través de la conexión local se podrán conectar los clientes al Police Manager y las políticas de administración del antivirus se podrán aplicar en los clientes ubicados fuera del campus tal y como estuvieran en la red de área local (LAN) del campus.

1.2. Formulación del problema

1.2.1. Problema general

¿De qué manera la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión?

1.2.2. Problemas específicos

1. ¿De qué manera la funcionalidad mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión?
2. ¿De qué manera la seguridad mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión?
3. ¿De qué manera la confidencialidad mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión?

1.3. Objetivos de la Investigación

1.3.1. Objetivo general

Determinar la implementación de una red privada virtual (VPN) y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

1.3.2. Objetivos específicos

1. Determinar la funcionalidad y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.
2. Determinar la seguridad y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.
3. Determinar la confidencialidad y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

1.4. Justificación de la investigación

1.4.1. Justificación teórica

A través del internet se puede tener gran comunicación con todo el mundo y para la Universidad José Faustino Sánchez Carrión es muy importante, la Universidad José Faustino Sánchez Carrión es muy importante que se comunique con las diferentes oficinas externas de la Universidad ubicadas en Huacho, por tal motivo se vio en la necesidad de implementar una conexión de Red Privada Virtual (VPN), para esto usaremos la herramienta de conectividad OpenVPN basado el software libre SSL para tener mejor comunicación y una mayor seguridad de transmisión de datos.

Se utilizará como software de distribución CentOS GNU/LINUX por ser un software robusto y de masivo uso en soluciones de este tipo a nivel mundial, como software de solución específica para la implementación de la Red Privada Virtual se utilizará; el software libre OpenVPN que es una herramienta basada en SSL que nos ofrece un nivel elevado de seguridad.

1.4.2. Justificación práctica

Con la Red Privada Virtual, se va permitir tener la conexión de las diferentes oficinas externas de la Universidad José Faustino Sánchez Carrión, para transmitir los datos de los diferentes servicios y accesos que se encuentran en la Red LAN del campus Universitario.

En la red de datos de la Universidad existen recursos que se comparten a través de la conectividad de la conectividad LAN (red privada), recursos como:

Servidores de archivos, Sistema Integrado de Gestión Administrativa (SIGA), Sistema Integrado de Administración Financiera (SIAF), Software de Inventario Mobiliario Institucional (SIMI), Sistema Integrado de Administración Documentaria (SISTRAD), acceso a la consola de administración de antivirus.

1.5. Delimitaciones del estudio

Esta investigación abarcara principalmente la implementación de la Red Privada Virtual (VPN) para comunicar las oficinas externas de la Universidad José Faustino Sánchez Carrión - Huacho, mediante herramientas de Software Libre.

1.5.1. Delimitación del tiempo

El tiempo sé que llevará a cabo la investigación será de 11 meses entre los meses de Noviembre 2019 a Setiembre 2020.

1.5.2. Delimitación del espacio

El entorno al cual se desarrollará la investigación comprende de las oficinas externas de la universidad José Faustino Sánchez Carrión, ubicada en la ciudad de Huacho, provincia de Huaura, departamento de Lima Provincia.

1.6. Viabilidad del estudio

Dado que en la actualidad trabajo en la oficina de servicios informáticos en el área de la unidad de soporte, desarrollo de software y mantenimiento de computadoras – UNJFSC; debo mencionar que la información que me brindará estará en mi alcance para realizar esta investigación.

Es viable porque se cuenta con los recursos, herramientas tecnológicas necesarias para iniciar el desarrollo de la investigación, existe la facilidad por parte del personal que trabaja en la Universidad tanto externo como interno para la recolección de datos.

CAPÍTULO II

MARCO TEÓRICO

Para entender el contexto en que se desarrollara la investigación, es importante conocer, entender lo que es una Red Privada Virtual, y todo lo que esta implica, dichos conceptos van de la mano con la investigación a desarrollarse, así mismo se brinda una descripción de la investigación, de otras fuentes y autores que se ha hecho respecto al tema.

2.1. Antecedentes de la investigación

En la investigación realice para los antecedentes para mi tesis, tanto nacionales como internacionales con respecto a cómo la implementación de una red privada virtual, para comunicar dos o más oficinas externas de una empresa.

2.1.1. Investigaciones internacionales

Perdomo (2018) Titulo: " Diseño de una red privada virtual segura para facilitar la comunicación, trabajo y flujo de información en la empresa QOS LTDA" de la Universidad Cooperativa de Colombia, para obtener el título de Ingeniero de Telecomunicaciones; el cual concluye diciendo: En la actualidad las VPN ofrecen un gran servicio para las empresas que quieran tener una comunicación segura con sus proveedores, clientes u otros, sin necesidad de implantar una red de comunicación costosa que permita lo mismo. Los indiscutibles beneficios en infraestructura y costos a nivel empresarial que ofrece la creación de Redes Privadas Virtuales como soporte de las comunicaciones corporativas en la empresa QOS LTDA. Son el principal logro que otorga este proyecto de modalidad de grado en la interconexión de las áreas que conforman

esta empresa. Esta implementación de VPN ofrece garantía de seguridad en los datos y fácil implementación, debido a que estas reemplazaran las conexiones dedicadas punto a punto por cables físicos al utilizar la Internet como su estructura y camino esencial. Se concluye que las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que representan una excelente tecnología de acceso remoto. Se cumplió con el objetivo principal, el cual era diseñar una red privada virtual segura para facilitar la comunicación, trabajo y flujo de información de la empresa QOS LTDA ubicada en la ciudad de Bogotá, basados en la norma internacional seguridad ISO 27001.

Quishpe (2021) Título: "Estudio para la Implementación de una red privada virtual (VPN) utilizando herramientas de software libre" de la Pontificia Universidad Católica del Ecuador, para obtener la Maestría en Tecnologías de la Información Mención Redes de Comunicación; el cual concluye diciendo: Una vez establecidos los requerimientos y recursos de los que dispone la empresa, se utilizará el servicio de internet PYME de 75 Mbps con una dirección IP pública como medio para la conexión VPN, se realizará la compra de un computador clon mejorado para ser utilizado como servidor VPN, de igual manera la infraestructura de red local es aceptable para el funcionamiento adecuado de red privada virtual. Luego de revisados los conceptos teóricos y analizadas las diferentes tecnologías existentes para realizar el diseño de la VPN, se ha llegado a la conclusión que se debe utilizar el sistema operativo Linux CentOS, con la versión 8, como software de red privada virtual OpenVPN, para servicio de firewall se utilizará firewalld y

como servidor proxy a Squid proxy. Una vez realizada la instalación y configuración de Linux CentOS, Firewalld, Squid Proxy y OpenVPN, se concluye que se cumple con la implementación de la red privada virtual y se establece el manual técnico de configuración de nuevos usuarios como anexo 1, con lo cual el administrador del servicio podrá agregar o eliminar cuentas de manera sencilla. Una vez evaluado la red privada virtual, realizando la verificación de conectividad, pruebas de conexión, pruebas de pérdidas de paquetes, pruebas de acceso a la red local, pruebas de acceso remoto y prueba de encriptación se verifica que se cuenta con una red privada virtual con un adecuado funcionamiento y con la seguridad necesaria. Realizada la implementación de la red privada virtual ha sido posible que los empleados de la COMISION FULBRIGHT DEL ECUADOR que requerían acceso de manera remota lo puedan realizar de manera sencilla, siendo para esto necesario únicamente el contar con el servicio de internet, los empleados podrán conectarse a la red local y por ende a los sistemas y servicios con los que se cuentan en la empresa desde cualquier sitio, para lo cual se estructuró una guía de usuario como anexo 2. La implementación de la red privada virtual se ha realizado con un costo mínimo comparado con otras soluciones en las cuales se requieren adquirir equipos y licencias de uso, dado que en este caso ha sido necesario únicamente el adquirir un equipo clon mejorado y no ha sido necesario adquirir licencias de ningún tipo al utilizar herramientas y sistemas de software libre

Baleta (2020) título: “Diseño de una red virtual privada de acceso remoto para establecer conexiones de teletrabajo de forma segura en las organizaciones” de la Universidad Cooperativa de Colombia, para obtener el título de Ingeniero de Sistemas; el cual concluye diciendo: Podemos apreciar que al establecer una red de acceso remoto vpn bajo el protocolo IPSec que nos ofrece garantías de seguridad en los datos debido al alto nivel de cifrado que ofrece, se fortalece en gran medida algunas de las vulnerabilidades que se presentan en las conexiones remotas sin ningún tipo de seguridad y que es un factor fundamental para hacerle frente a los ciberataques de terceros que buscan infiltrarse en la red y obtener información en la misma ofreciendo de esta manera una transferencia confiable de datos a estas entidades que aplican el teletrabajo en el desarrollo de sus actividades y así cumplir con el trabajo que se venía ejecutando normalmente.

Quezada (2016) Titulo: “Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja” de la Universidad Nacional de Loja, para optar el Título de Ingeniero en Sistemas; el cual concluye diciendo: Mediante el respectivo análisis de los principales elementos que componen las redes privadas virtuales y casos de éxitos orientados al diseño privadas virtuales se determinó que las redes privadas virtuales son la mejor alternativa para permitir que los estudiantes accedan a las bases de datos científicas de la Universidad Nacional de Loja, debido a su alto grado de confidencialidad, seguridad, integridad y autenticidad. Con el uso del software OpenVPN se logró diseñar una red privada virtual basada en una tecnología y protocolos de seguridad SLL-TLS que permitió a los usuarios remotos acceder de una forma segura a las bases de datos científicas de la Universidad Nacional de Loja. La instalación y

configuración del Servidor de Acceso OpenVPN permitió establecer un enlace de comunicación directo entre los servidores de la red interna de la Universidad Nacional de Loja y los usuarios remotos, sin preocuparse de la infraestructura física de la red ni de los equipos que la conforman. Con la implementación de la red privada virtual en la Universidad Nacional de Loja se creó un servicio de acceso a biblioteca virtual que permitió acceder a los recursos internos (base de datos científicas, libros electrónicos, revistas digitales) desde una red externa a la institución.

2.1.2. Investigaciones nacionales

.

Sánchez (2018) Titulo: "Implementación de una VPN en una red corporativa para mejorar la gestión de la información de los servicios en la empresa Técnica Plástica SRL" de la Universidad César Vallejo, para obtener el título de Ingeniero de Sistemas; el cual concluye diciendo: – Que, en efecto, la implementación de una VPN en una red corporativa mejora la gestión de la información en la empresa Técnica Plástica SRL.– Con esto se demuestra que la implementación de una VPN en una red corporativa mejora la gestión de la información en la empresa Técnica Plástica SRL. por medio de las dimensiones control de la información y accesibilidad con los niveles adecuados de significancia

Espinoza (2018) Título: "Propuesta de una Red Privada Virtual para mejorar el Servicio de Comunicación Tiendas MASS para la empresa supermercados Peruanos S.A." de la Universidad Autónoma del Perú, para obtener el título de

Ingeniero de Sistemas; el cual concluye diciendo: La implementación del rediseño de red planteado, permitirá estar a la vanguardia tecnológica, optimizando recursos y costos. Vendría a solucionar, en gran medida, muchos de los problemas de las empresas en la actualidad presentan en lo que al manejo de la información respecta, permitiéndole a quienes allí laboran poder acceder a ésta de manera más rápida, eficiente y confiable. La implementación de una red LAN con categoría 6, permitirá estar a la vanguardia tecnológica, optimizando recursos y costos. Elegimos esta marca porque tiene una muy buena integración con todos los sistemas de instalación. Además, nos brinda mejor soporte. La solución de cableado estructurado es capaz de soportar tanto la red de datos, como los servicios de telefonía IP, al igual que cámaras de vigilancia presentes en el edificio y los servicios de videoconferencia, y asegura disponibilidad, escalabilidad y seguridad para la red". Una red inalámbrica permitirá reducir tiempo y problemas en la correcta actualización de la información y el cambio automático de uno a otro, para que sea más fácil el acceso inalámbrico al desplazarse entre distintos puntos de acceso. Se realizó la factibilidad económica: costo de materiales, costo de accesorios, costo de herramientas, costo de implantación, costo de mantenimiento y Costo de Hardware.

García (2021) título: "Implementación de una VPN tipo cliente para una entidad financiera" de la Universidad Tecnológica del Perú, para obtener el título de Ingeniero de Telecomunicaciones; el cual concluye diciendo: • Se logró brindar continuidad a las funciones de manera remota de los colaboradores de la entidad financiera implementando la fase 1 del servicio de VPN en una semana, logrando

integrar las cuentas de red. • Se logró elevar la seguridad en las conexiones VPN como parte de la fase 2 implementando controles de seguridad como Host Information Profiles de Palo Alto (HIP) para asegurar e identificar cuáles son los equipos de propiedad de la entidad financiera, así como la habilitación del MFA de Azure para todos los colaboradores asegurando el inicio de sesión. • Se entrega las métricas de manera semanal para seguimiento evolutivo y de control de uso de cuentas VPN asignadas. Estas métricas son solicitadas por la gerencia de Operaciones de TI para ser presentado al comité directivo para fines convenientes. • De sobrepasar las 1024 conexiones VPN concurrentes el fabricante Palo Alto recomienda cambiar el modo de funcionamiento de los equipos Firewall de Activo - pasivo pasar a Activo - Activo y utilizar un máximo de 90% de la capacidad soportada por los equipos que sería 1843 conexiones en simultáneo.

Mamani (2019) Título: "Diseño e Implementación de Red Privada Virtual IPSEC para la comunicación de caja rural de ahorro y crédito los Andes SA, Puno - 2019", de la Universidad Nacional del Altiplano, para obtener el título de Ingeniero de Sistemas; el cual concluye diciendo: Del análisis de la situación actual se obtuvo que el tiempo, el costo de instalación y mantenimiento del servicio de Red Privada Virtual contratado por la entidad son bastante elevados, porque las actividades que se realizaron durante la instalación demandaron un promedio de 2 meses por cada sucursal, con un costo único de instalación, y un costo promedio mensual de mantenimiento del servicio que supera los mil soles. Durante el inicio del proyecto, se diseñó una topología física y lógica de una Red Privada Virtual IPSec con IP Dinámica que requieren un tiempo reducido en las

actividades a realizar para su implementación, y el costo de mantenimiento del servicio también se reduce considerablemente, sin embargo, el costo de instalación es superior a lo cobrado por el proveedor contratado, porque se requiere de la adquisición de equipos como routers, módems y chips de Internet móvil para ejecutar el proyecto. Se implementó la Red Privada Virtual con IP Dinámica con Routers Cisco y verificó la conectividad de las sucursales de la Caja Rural de Ahorro y crédito los Andes SA, para la implementación se cumplió con las actividades del diseño y el resultado obtenido en las pruebas de conectividad fue de un 75 % de las sucursales como aceptables respecto a la conectividad, y el 25% de las sucursales obtuvieron una calificación no aceptable, porque la cobertura de internet móvil del operador utilizado en esta sucursal fue defectuosa, para mejorar la conectividad en esta sucursal se puede optar por utilizar otro proveedor de internet móvil. Durante la evaluación de la disminución de tiempo y costo de instalación de servicio luego de la implementación del proyecto, se obtuvo que existe una disminución promedio de cuarenta días, que representa el 68% del tiempo que demora el proveedor para la instalación del servicio por cada sucursal, también los resultados obtenidos respecto al costo de instalación y mantenimiento del servicio se reducen en un 88.8% que equivale a más de cien mil soles ahorrados, para un periodo de 36 meses de contrato.

2.2. Bases Teóricas

2.2.1. Red de computadoras

2.2.1.1. Introducción

Conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos),

recursos (CD-ROM, impresoras,USB), servicios (acceso a internet, E-mail, chat, juegos). Gorgona (2016) señaló que:

> Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica - master/Slave). Normalmente se trata de transmitir datos, audio y video por ondas electromagnéticas a través de diversos medios de transmisión (aire, vacío, cable de cobre, cable de fibra óptica). (p.6)

Anónimo (2010) indicó que: “Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el modelo OSI por la ISO, el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un enlace definido”.

Figura 1. Red de Ordenadores o Red Informática

2.2.1.2. Modelo OSI

El modelo OSI (Open Systems Interconexión de Sistemas Abiertos) es una estructura referencial que fue desarrollada en los 80s por la Organización Internacional de Estándares (ISO) con la intención de establecer un marco que sirviera de guía en el desarrollo de protocolos de comunicación. Estos protocolos siguen sus propios estándares internamente, pero se manejan dentro de este marco referencial, por tanto, se podría decir que el modelo OSI es un estándar de estándares. MPachano (2014) señaló que:

> "La información se transmite de forma vertical a través de las 7 capas desde la aplicación fuente hasta la estructura física (cables que transmiten información en forma de bits) desde donde se transmite de nuevo hacia arriba en la estructura para llegar a la aplicación destino".

Figura 2. Diseño de Red Modelo Osi

- **Capa 1. Capa física**

Es donde se especifican los parámetros mecánicos (grosor de los cables, tipo de conectores), electicos (temporizador de las señales, niveles de tensión) de las conexiones físicas.

Las unidades de información que considera son bits, y trata de la transmisión de cadenas de bits en el canal de comunicación (pares trenzados de cobre, cable coaxial, radio, infrarrojos, wifi, fibra óptica), si el emisor envía un 0, al receptor debe de llegar. Giraldo (2017) mencionó que:

> "Existen diferentes formas de ampliar una red aislada o interconectar redes individuales, con dispositivos de interconexión de redes y son: (1) Repetidor (Repeater): Capa física del modelo OSI. (2)Concentrador (Hub): Capa física del modelo OSI. (3)Puente (Bridge): Capa física y de enlace de datos capa 2 del modelo OSI. (4)Conmutador (Switch): Actúan como filtros en la capa de enlace de datos (capa 2) del modelo OSI. (5)Router: Capa 3 del modelo OSI (Físico, enlace de datos y red). (6)Pasarela (Gateway): Niveles de transporte, sesión, presentación y aplicación del modelo OSI". (p.3)

- **Capa 2. Capa de enlace de datos**

Giraldo (2017) mencionó que:

> “Descompone los mensajes que recibe del nivel superior en tramas o bloques de información, en las que añade una cabecera (DH) e información redundante para control de errores. La cabecera suele contener información de direcciones de origen y destino, ruta que va seguir la trama, etc. También se encarga de transmitir sin error las tramas entre cada enlace que conecte directamente dos puntos físicos (nodos) adyacentes de la red y desconectar el enlace de datos sin perdidas de información” (p.4)

- **Capa 3. Capa de la red**

Se encarga de fragmentar los segmentos que se transmiten entre dos equipos de datos en unidades denominados paquetes. En el ordenador receptor se efectúa el proceso inverso: los paquetes se ensamblan en segmentos.

Realiza el encaminamiento de los paquetes. Se encargará de realizar algoritmos eficientes para la elección de la ruta más adecuada en cada momento, para reexpedir los paquetes en cada uno de los nodos de la red que debe atravesar.

“Prevenir la producción de bloqueos, así como la congestión en los nudos de la red de transporte que pudiesen producirse en horas punta por la llegada de paquetes en forma masiva” (Giraldo, 2017, p. 5)

- **Capa 4. Capa de transporte**

Se encarga de transportar la información, desde la fuente al destino, a través de la red. Giraldo (2017) mencionó que:

> "Los accesos a la capa de transporte se efectúan a través de puertos (sockets). El objetivo es realizar un servicio de transporte eficiente entre procesos o usuarios finales. Para dicho fin, toma los mensajes del nivel de sesión, los distribuye en pequeñas unidades (Segmentos) y los pasa a la red. Los protocolos de la capa de transporte se aseguran que todos los segmentos lleguen de forma correcta a su destino, para la cual realizan detección y corrección de errores, además de controlar el flujo y la secuenciación. Otras funcionalidades es optimizar el transporte, realizando multiplexaciones de varios mensajes en un segmento para abaratar costes". (p. 6)

- **Capa 5. Capa de sesión**

Cuando se realiza una transferencia entre dos ordenadores se establece una sesión de comunicación entre ambos. La capa de sesión es responsable de:

- Actuar de interfaz entre el usuario y la red, gestionando el establecimiento de la conexión entre procesos remotos.
- Establecer un dialogo entre dos equipos remotos para controlar la forma en que se intercambian los datos.
- Identificar los usuarios de procesos remotos.
- Cuando se corta la conexión de forma anormal, en la capa de

transporte o en inferiores, la capa de sesión puede encargarse de restablecer la sesión de forma transparente al usuario.

"Su función es aumentar la fiabilidad de la comunicación obtenible por las capas inferiores, proporcionando el control de la comunicación entre aplicaciones al establecer, gestionar y cerrar sesiones o conexiones entre las aplicaciones que se comunican" (Giraldo, 2017, p.7)

- **Capa 6. Capa de presentación**

Trata de homogeneizar los formatos de presentación de los datos entre equipos de la red. Para homogeneizar la representación de datos (texto, sonido, imágenes, instrucciones), la capa de presentación interpreta las estructuras de las informaciones intercambiadas por los procesos de la aplicación y las transforma convenientemente.

Puede realizar transformaciones para conseguir mayor eficacia en la red (compresión de texto y cifrado de seguridad). Los programas del nivel 6 suelen incluirse en el propio Sistema Operativo. La representación de los caracteres como los datos de textos y numéricos dependen del ordenador, se representan por códigos de representación EBCDIC, UNICODE.

- **Capa 7. Capa de aplicación**

Dos ordenadores se intercomunican a través de procesos,

correspondiente a unas determinadas aplicaciones. El intercambio de información entre dos procesos se efectúa por medio de algún protocolo de la capa aplicación. Algunos protocolos de la capa de aplicación son TELNET, FTP, SMTP, POP3, DNS, RTP, HTTP.

- TELNET: Es una aplicación que permite desde nuestro sitio y con el teclado y la pantalla de nuestro ordenador, conectarnos a otro ordenador remoto a través de la red.
- FTP: Es una herramienta que te permite, a través de la red, copiar ficheros de un ordenador a otro.
- SMTP: Es un servicio de correo a través de servidores, usando un protocolo estándar para enviar y para recibir el correo.
- POP3: Protocolo POP (Protocolo de oficina de correos), permite recoger el correo electrónico en un servidor remoto.
- DNS: El servicio permite, una vez configurado, que tu web y tu correo electrónico sean localizados desde cualquier lugar del mundo mediante tu nombre de dominio.
- RTP: (Real-Time Transfer Protocol) se utiliza para encapsular VoIP paquetes de datos dentro de paquetes UDP.
- HTTP: Protocolo de Transmisión Hipertexto. Protocolo de comunicaciones utilizado por los programas cliente y servidores WWW para comunicarse entre sí.

2.2.1.3. Modelo TCP/IP

TCP/IP es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. La sigla TCP/IP significa

Protocolo de Control de Transmisión/Protocolo de Internet y se pronuncia “T-C-P-I-P”. Proviene de los nombres de dos protocolos importantes incluidos en el conjunto TCP/IP, es decir, del protocolo TCP y del protocolo IP. César (2018) indicó que:

> “En algunos aspectos, TCP/IP representa todas las reglas de comunicación para internet y se basa en la noción de direcciones IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder en rutar paquetes de datos. Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos, dividir mensajes en paquetes, usar un sistema de direcciones, en rutar datos por la red y detectar errores en las transmisiones de datos”.

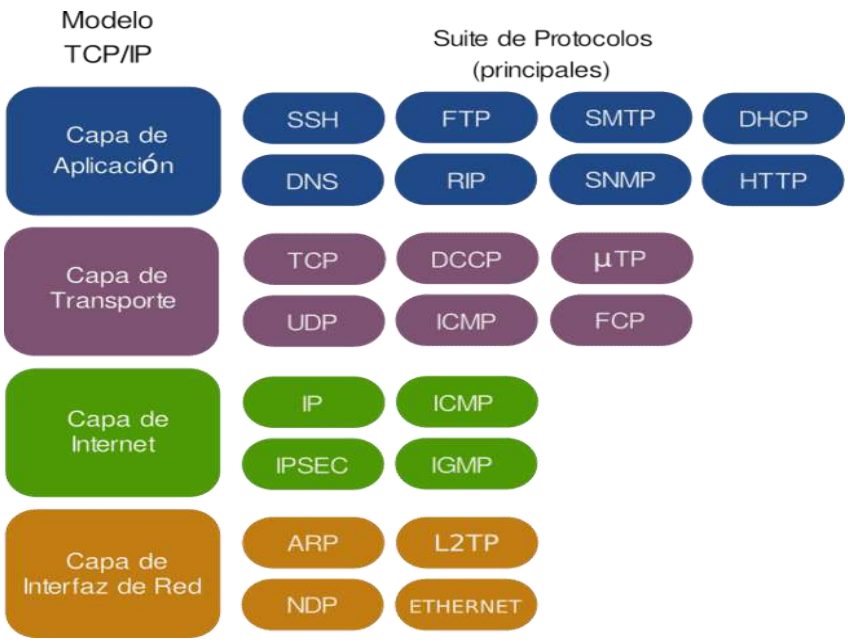


Figura 3. *Diseño* de *Red Modelo TCP/IP*

Capa de aplicación

La capa de aplicación proporciona a las aplicaciones la capacidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos. Existen muchos protocolos de capa de aplicación y continuamente se están desarrollando nuevos.

En esta arquitectura de protocolos, los de capa de aplicación más ampliamente conocidos son los utilizados para el intercambio de información de los usuarios.

- **Hypertext Transfer Protocol (HTTP):** Se utiliza para transferir archivos que componen las páginas Web de la World Wide Web.
- **File Transfer Protocol (FTP):** Se utiliza para la transferencia interactiva de archivos.
- **Simple Mail Transfer Protocol (SMTP):** Se utiliza para la transferencia de mensajes de correo electrónico y archivos adjuntos.
- **TELNET:** Es un protocolo de emulación de terminal, se utiliza para iniciar la sesión de forma remota en máquinas de la red.

Además, dentro de la arquitectura de protocolos TCP/IP, estos otros protocolos de capa de aplicación ayudan a facilitar en el uso y la gestión de redes TCP/IP.

- **Domain Name System (DNS):** Se utiliza para resolver un nombre de host a una dirección ip.

- **Routing Information Protocol (RIP):** Es un protocolo de enrutamiento que los enrutadores utilizan para intercambiar información de enrutamiento en una red IP.
- **Simple Network Management Protocol (SNMP):** "Se utiliza entre una consola de gestión de red y dispositivos de red (routers, bridges, hubs inteligentes) para recoger e intercambiar información de gestión de la red" (Valencia, 2016).

Capa de transporte

La capa de transporte de esta arquitectura de protocolos es responsable de proporcionar a la capa de aplicación, servicios de sesión y de comunicación de datagrama. Los protocolos básicos de la capa de transporte son:

- **Transmission Control Protocol (TCP):** Proporciona un servicio de comunicaciones fiable orientado a la conexión uno a uno. TCP es responsable del establecimiento de una conexión. TCP, la secuencia y el acuse de recibo de los paquetes enviados, y la recuperación de paquetes perdidos durante la transmisión.
- **User Datagram Protocol (UDP):** "Proporciona una conexión, uno a uno a muchos poco fiable. Por eso UDP se utiliza cuando la cantidad de datos a transferir es pequeña y no se desea la sobrecarga que supone establecer una conexión TCP o cuando las aplicaciones o protocolos de capa superior proporcionan una entrega fiable" (Valencia, 2016).

Capa de internet

La capa de internet de esta arquitectura de protocolos es responsable de las funciones de direccionamiento, empaquetado y enrutamiento. Los protocolos básicos de la capa de internet son:

- **Internet Protocol (IP):** Es un protocolo enrutable responsable del direccionamiento IP, enrutamiento y fragmentación y reensamblado de paquete.
- **Address Resolution Protocol (ARP):** Es responsable de la resolución de la dirección de la capa de internet a la dirección de la capa de interfaz de la red, tales como una dirección de hardware.
- **Internet Control Message Protocol (ICMP):** Es responsable de proporcionar funciones de diagnóstico y notificación de errores debidos a la entrega sin éxitos de paquetes IP.
- **Internet Group Management Protocol (IGMP):** Es responsable de la gestión de grupos de multidifusión IP.

Capa de Interfaz de Red

Valencia (2016) señaló que:

> "La capa interfaz de red de esta arquitectura de protocolos (también llamada capa de acceso de red) es responsable de la colocación de paquetes TCP/IP en la red y de la recepción de paquetes TCP/IP de fuera la red. TCP/IP fue diseñado para ser independiente del método de acceso a la red, el formato y el medio. De esta manera, TCP/IP se puede utilizar para conectar diferentes tipos de red. Estas incluyen tecnologías LAN como las tecnologías Ethenet y Token

Ring y WAN tales como X.25 y Frame Relay. Su independencia de cualquier tecnología de red especificada a TCP/ip la capacidad de adaptarse a las nuevas tecnologías tales como modo de transferencia asíncrono o Asynchronous Transfer Mode (ATM)".

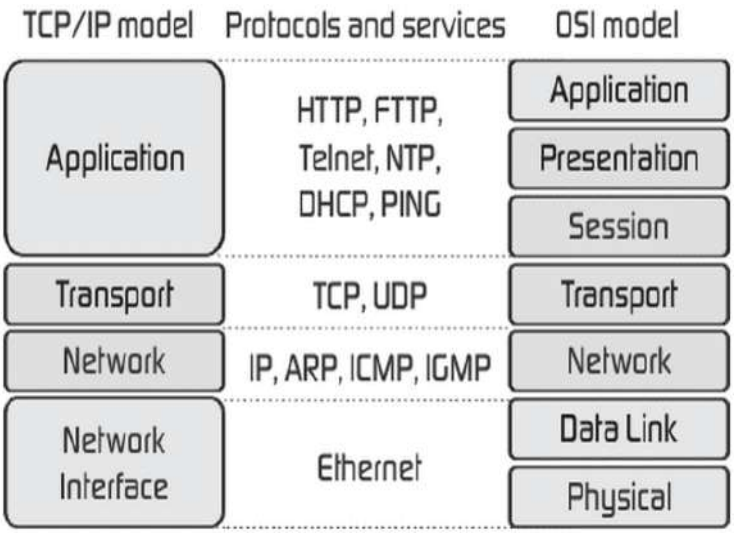


Figura 4. Comparación de Modelo Osi con Modelo TCP/IP

2.2.1.4. Clasificación de redes

Las redes se clasifican por su alcance, por el tipo de conexión, por la relación funcional, por topología, por grado de autentificación y por grado de difusión.

El termino red obedece a un desarrollo conjunto de equipos y conexión de programas que permiten la unión de los mismos entre sí, con el fin de facilitar el trabajo coordinado y más eficiente; ya que contribuye

al mejor funcionamiento de los equipos como también la potenciación de la labor que se debe realizar.

La tipología de las redes presenta gran importancia para los ingenieros e informáticos, con el fin de estudiar las mismas y poder potenciarlas al máximo, con el objetivo de aprovechar sus beneficios en cada una de las actividades en las que son necesarios.

2.2.1.4.1. Por alcance

- **Red de área personal (PAN)**

  Mansilla (2018) indicó que: "Es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (Teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. El alcance de un PAN es de algunos metros" (p.4). Se puede conectar con cables alos USB y FireWire de la computadora.

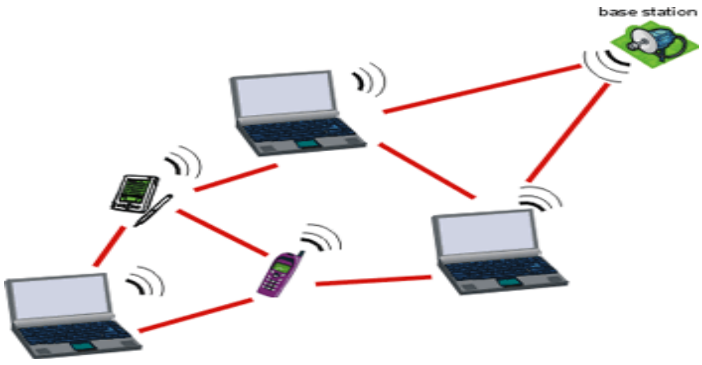


Figura 5. Una red de área personal.

- **Red de área local (LAN)**

  Una Red de Área Local, red local o LAN (del inglés local área network) es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión.

Las redes de área local a veces se llaman una sola red de localización.

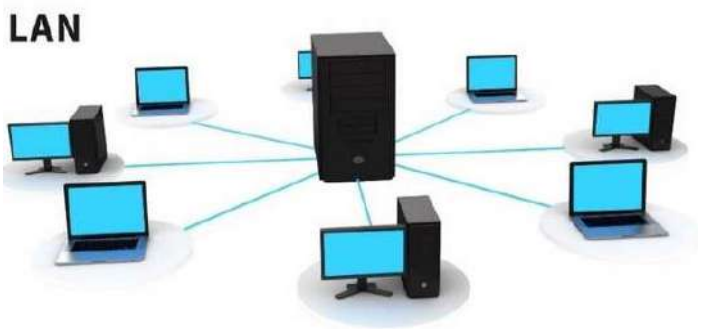


Figura 6. Una red de área local

- **Red de área local inalámbrica (WLAN)**

Quintana (s.f.) señaló que:

> "Una Red de Área Local Inalámbrica, más conocida como WLAN, es básicamente un sistema de transferencia y comunicaciones de datos el cual no requiere que las computadoras que la componen tengan que estar cableadas entre sí, ya que todo el tráfico de datos entre las mismas se realiza a través de ondas de radio. A pesar de que son menos seguras que su contrapartida cableada. Ofrecen una amplia variedad de ventajas, y es por ello que su implementación crece día a día en todos los ámbitos" (p.3).

Figura 7. Una red de *área* local inalámbrica

- **Red de área amplia (WAN)**

Red de Área Extensa, también llamada Red de Área Amplia o WAN (Sigla inglesa Wide Área Network), son redes de comunicaciones que conectan equipos destinados a ejecutar programas de usuario (en el nivel de aplicación) en áreas geográficas de cientos o incluso miles de kilómetros cuadrados (regiones, países, continentes).

Cada uno de los equipos terminales suele denominarse nodo o host, y se llama subred de comunicación (o, simplemente, subred) al conjunto de líneas de transmisión y en caminadores (o router) que permiten que los hosts se comuniquen entre sí. Distintas subredes pueden cambiarse entre sí dando lugar a más de área extensa más grandes, como en el caso de internet.

Lo más habitual es que los hosts se conecten a las redes de área extensa a través de la red local o LAN, pero también puede haber terminales que se conecten directamente a un router, sin necesidad de estar integrados en ningún otro tipo de red. Cuando un host envía una secuencia de paquetes de datos, cada router los almacena y espera a que la línea de transmisión que considera optima este libre para reenviarlos hasta el siguiente router, y así hasta llegar al destino

Figura 8. Una red de área amplia

2.2.1.4.2. Por método de la conexión

Medios Guiados y no Guiados dentro de los medios de transmisión hay medios guiados y medios no guiados; la diferencia radica en que los medios guiados el canal por el que se transmite las señales son medios físicos, es decir, por medio de un cable; y en los medios no guiados no son medios físicos.

Medios guiados

- **Par trenzado**

  Normalmente se le conoce como un par de conductores de cobre aislados entrelazados formando un espiral. Es un enlace de comunicaciones. En estos el paso del trenzado es variable y pueden ir varios en una envoltura. El hecho de ser trenzado es para evitar la diafonía (la diafonía es un sonido indeseado en cual es producido por un receptor telefónico). Es el medio más común de transmisión de datos que existe en la actualidad, pudiéndose encontrar en todas las casas o construcciones de casi cualquier lugar. Se utiliza para la

formación de una red telefónica, la cual se da entre un abonado o usuario y una central local. En ocasiones dentro de un edificio se construyen centrales privadas conocidas como PBX. Las redes locales manejan una velocidad de transmisión de información comprendida entre los 10 Mgps y los 100 Mbps. En este medio de transmisión encontramos a favor el hecho de ser prácticamente el más económico que se puede ubicar en el mercado actual, por otro lado, es el más fácil de trabajar por lo que cualquier persona con un mínimo de conocimientos puede adaptarlo a sus necesidades.

Por otro lado, tiene en contra que tiene una baja velocidad de transferencia en medio rango de alcance y un corto rango de alcance en LAN para mantener la velocidad alta de transferencia (100 mts). Dentro de sus características de transmisión nos encontramos con que con un transmisor analógico necesitamos transmisores cada 5 o 6 Kms; con un transmisor digitales tenemos que las señales que viajan pueden ser tanto analógicas como digitales, necesitan repetidores de señal cada 2 o 3 Kms lo que les da muy poca velocidad de transmisión, menos de 2 Mbps; en una red LAN las velocidades varían entre 10 y 100Mbps en una distancia de 100 mts, de lo cual podemos además decir que la capacidad de transmisión está limitada a 100 Mbps, además es muy susceptible a interferencias y ruidos. Para esto se han buscado soluciones como la creación de cables UTP (los más comunes, es el cable telefónico normal pero dado a interferencias

electromagnéticas) y los cables STP (cuyos pares vienen dentro mallas metálicas que producen menos interferencias, aunque es más caro y difícil de manejar ya que es más grueso y pesado). Dentro de los cables UTP encontramos las categorías cat 3 (con calidad telefónica, más económico, con diseño apropiado y distancias limitadas hasta 16 MHz con datos; y la longitud del trenzado es de 7'5 a 10 cm), cat 4 (hasta 20 MHz) y cat 5 (llega hasta 100 MHz, es más caro, aunque esta siento altamente usado en las nuevas construcciones, y su longitud de trenzado va de 0'6 a 0'85 cm) se dice entonces que el par trenzado cubre una distancia aproximada de menos de 100 mts y transporte aproximadamente menos de 1 Mbps.

- **Cable coaxial**

El cable coaxial es un medio de transmisión relativamente reciente y muy conocido ya que es el más usado en los sistemas de televisión por cable físicamente es un cable cilíndrico constituido por un conducto cilíndrico externo que rodea a un cable conductor, usualmente de cobre. Es un medio más versátil ya que tiene más ancho de banda (500MHz) y es más inmune al ruido. Es un poco más caro que el par trenzado, aunque bastante accesible al usuario común. Encuentra múltiples aplicaciones dentro de la televisión (TV por cable, cientos de canales), telefonía a larga distancia (puede llevar 10 000 llamadas de voz simultáneamente), redes de área local (tienda a desaparecer ya que un problema en un punto

compromete a toda la red). Tiene como características de transmisión que cuando es analógica, necesita amplificadores cada pocos kilómetros y los amplificadores más cerca de mayores frecuencias de trabajos y hasta 500 MHz; cuando la transmisión es digital necesita repetidores cada 1 Km y los repetidores más cerca de mayores velocidades transmisión. La transmisión del cable coaxial entonces cubre varios cientos de metros y transporta decenas de Mbps.

- **Fibra óptica**

  Es el medio de transmisión más novedoso de los guiados y su uso se está masificando en todo el mundo reemplazando el par trenzado y el cable coaxial en casi todos los campos. En estos días lo podemos encontrar en la televisión por cable y la telefonía. En este medio los datos se transmiten mediante una has confinado de naturaleza óptica, de ahí su nombre, es mucho más caro y difícil de manejar, pero sus ventajas sobre los otros medios lo convierten muchas veces en una muy buena elección al momento de observar rendimiento y calidad de transmisión. Físicamente un cable de fibra óptica está constituido por un núcleo formado por una o varias fibras o hebras muy finas de cristal o plástico; un revestimiento de cristal o plástico con propiedades ópticas diferentes a las del núcleo, cada fibra viene rodeada de su propio revestimiento y una cubierta plástica para protegerla de humedades y el entorno. La fibra óptica encuentra aplicación en los enlaces entre nodos, backbones, atm, redes LAN’s, Gigabit Ethernet, largas distancia,

etc. Dentro de las características de transmisión encontramos que se basan en el principio de “reflexión total” (índice de refracción del entorno mayor que el del medio de transmisión), su guía de ondas va desde 10^14 Hz a 10^15 Hz, esto incluye todo el espectro visible y el parte del infrarrojo.

Se suele usar como transmisores el LED (Light emitting diode) que es relativamente barato, su rango de funcionamiento con la temperatura es más amplio y su vida media es más alta y el ILD (injection laser diode) que es más eficiente y más caro, además tiene una mayor velocidad de transferencia. La tecnología de fibra óptica usa multiplexacion por división que es lo mismo que la división por frecuencia, utiliza multiples canales cada uno en diferentes longitudes de onda (policromatico) y una fibra (en la actualidad) hasta 80 haces 10 Gbps cada uno. Usa dos modos de transmisión, el monomodo (este cubre largas distancias, más caro, más velocidad debido a no tener distorsión multimodal) y el multimodo (cubre cortas distancias, es más barata, pero tiene menos velocidad (100 Mbps) además se ve afectado por distorsión multimodal). De la fibra óptica podemos decir que su distancia está definida por varios Kmts y su capacidad de transmisión viene dada por varios Gbps.

Medios no guiados

Los medios no guiados o sin cable han tenido gran acogida al ser un buen medio de cubrir grandes distancias y hacia cualquier dirección, su mayor logro se dio desde la conquista espacial a través de los satélites y su tecnología no para de cambiar. De manera general podemos definir las siguienes características de este tipo de medios: la transmisión y recepción se realiza por medio de antenas, ls cuales deben estar alineadas cuando la transmisión es direccional, o si es omnidireccional la señal se propaga en todas las direcciones.

- **Microondas terrestres**

  Los sistemas de microondas terrestres han abierto una puerta a los problemas de transmisión de datos, sin importar cuales sean, aunque sus aplicaciones no estén restringidas a este campo solamente. Las microondas están definidas como un tipo de onda electromagnética situada en el intervalo del milímetro al metro y cuya propagación puede efectuarse por el interior de tubos metálicos. Es en si una onda de corta longitud. Tiene como características que su ancho de banda varía entre 300 a 3.000 MHz, aunque con algunos canales de banda superior. Entre 3’5 GHz y 26 GHz. Es usado como enlace entre una empresa y un centro que funcione como centro de conmutación del operador, o como un enlace entre redes LAN.

  Para la comunicación de microondas terrestres se deben usar

antenas parabólicas, las cuales deben estar alineadas o tener visión directa entre ellas, además entre mayor sea la altura mayor el alcance, sus problemas se dan perdidas de datos por atenuación e interferencias, y es muy sensible a las malas condiciones atmosféricas.

- **Satélites**

  Conocidas como microondas por satélite, está basado en la comunicación llevada a cabo a través de estos dispositivos, los cuales después de ser lanzados de la tierra y ubicarse en la órbita terrestre siguiendo las leyes descubiertas por Kepler, realizan la transmisión de todo tipo de datos, imágenes, etc, según el fin con que se han creado. Las microondas por satélite manejan un ancho de banda entre los 3 y los 30 GHz, y son usados para sistemas de televisión, transmisión telefónica a larga distancia y punto a punto y redes privadas punto a punto. Las microondas por satélite, o mejor, el satélite en si no procesan información, sino que actúa como un repetidor-amplificador y puede cubrir un amplio espacio de espectro terrestre.

- **Ondas de radio**

  Son las más usadas, pero tienen apenas un rango de ancho de banda entre 3 KHz y los 300 GHz. Son poco precisas y solo y usados por determinadas redes de datos o los infrarrojos.

2.2.1.4.3. Por relación funcional

- **Servidor**

Es una aplicación que ofrece un servicio a usuario de internet, el servidor es un programa que recibe una solicitud, realizada el servicio requerido y devuelve los resultados en forma de una respuesta. Generalmente un servidor puede tratar múltiples peticiones (múltiples clientes) al mismo tiempo.

Las funciones que lleva a cabo el proceso servidor en los siguientes puntos

- Aceptar los requerimientos de bases de datos que hacen los clientes.
- Procesar requerimientos de bases de datos.
- Formatear datos para transmitirlos a los clientes.
- Procesar la lógica de la aplicación y realizar validaciones a nivel de base de datos.

Cliente-Servidor

Es la tecnología que proporciona al usuario final el acceso transparente a las aplicaciones, datos, servicios de cómputo o cualquier otro recurso del grupo de trabajo y/o, a través de la organización de trabajo inteligentes o “cliente, resultan en un trabajo realizado por otros computadores llamados servidores”.

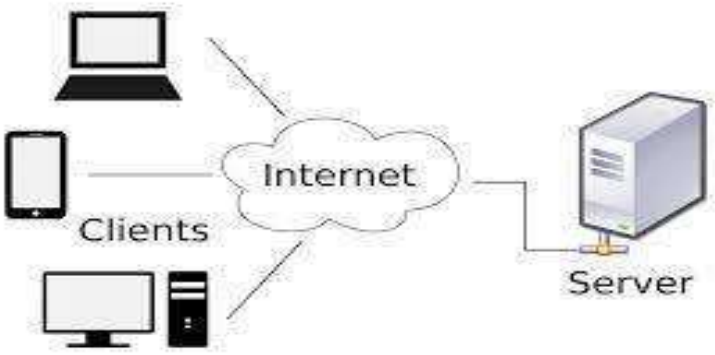


Figura 9. Modelo de un servidor cliente-servidor

2.2.1.5. Peer to peer (P2P)

Peer to Peer. En una red P2P, los "pares" son sistemas informáticos que están conectados entre sí a través de Internet. Los archivos se pueden compartir directamente entre sistemas en la red sin la necesidad de un servidor central. En otras palabras, cada computadora en una red P2P se convierte en un servidor de archivos y en un cliente.

Los únicos requisitos para que una computadora se una a una red peer-to-peer son una conexión a Internet y un software P2P. Los programas de software P2P comunes incluyen Kazaa, Limewire, BearShare, Morpheus y Acquisition. Estos programas se conectan a una red P2P, como "Gnutella", que permite que la computadora acceda a miles de otros sistemas en la red.

Una vez conectado a la red, el software P2P le permite buscar archivos en las computadoras de otras personas. Mientras tanto, otros usuarios de la red pueden buscar archivos en su computadora, pero normalmente solo

dentro de una sola carpeta que haya designado para compartir. Si bien las redes P2P hacen que compartir archivos sea fácil y conveniente, también ha llevado a una gran cantidad de piratería de software y descargas ilegales de música. Por lo tanto, es mejor estar seguro y descargar solo software y música de sitios web legítimos.

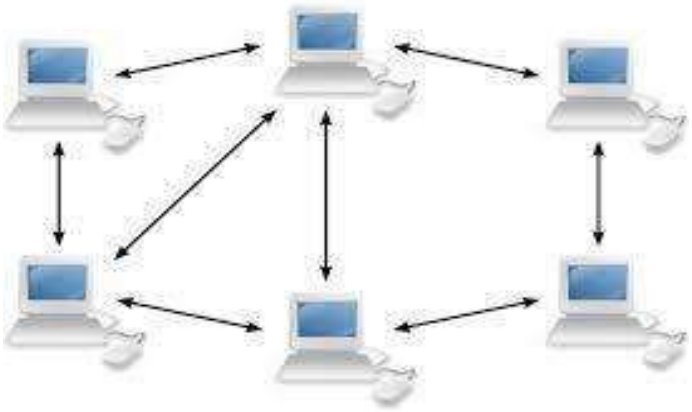


Figura 10. Modelo peer to peer

2.2.1.6. Topología de red

La topología de red no es otra cosa que la forma en que se conectan las computadoras para intercambiar datos ente sí. Es como una familia de comunicación, que define como se va a diseñar la red tanto de manera física, como de manera lógica.

- **Topología bus**

  Esta red se caracteriza por tener un canal de comunicación el cual conecta a todos los distintos dispositivos; es decir, todos los dispositivos comparten el mismo canal para comunicarse entre sí. Esta topología puede enviar información directamente o indirectamente (Bidireccional) y su velocidad va entre los 10/100 Mbps.

- **Topología estrella**

  Dado su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

  Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) sigue esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.

- **Topología anillo**

  En este tipo de red la comunicación se da por el paso de un token o testigo, que se conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evita eventuales perdidas de información debidas a colisiones. En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos). Esto se puede aprecias en la de muestra dando, si uno de los anillos presenta algún problema, el anillo activo tomara hacer la función de los dos.

- **Topología malla**

  La topología en malla es una topología en la que cada nodo o computadora está conectado a las demás computadoras. De esta forma es más fácil llevar los mensajes de una computadora a otra computadora por diferentes caminos.

  Si la red malla está correctamente conectada de forma completa, no puede existir de ninguna manera algún tipo de interrupción en la comunicación, además cada servidor tiene sus propias conexiones con todos los demás servidores que se encuentran en la red.

- **Topología en árbol**

  Las conexiones entre los nodos (terminales o computadoras) están dispuestas en forma de árbol, con una punta y una base. Es similar a la topología de estrella y se basa directamente en la topología de bus. Si un nodo falla, no se representan problemas entre los nodos subsiguientes. Cuenta con un cable principal llamado Backbone, que lleva la comunicación a todos los nodos de la red, compartiendo un mismo canal de comunicación.

- **Red mixta**

  En la topología mixta es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red, de aquí el nombre “hibridas” o “mixtas”.

Ejemplo de topologías mixtas: en árbol, estrella-estrella, bus-estrella, etc.

2.2.1.7. Tipos de transmisión

- **Simplex (Unidireccionales):** Un equipo de terminal de datos transmite y otro recibe. (ej. Streaming).
- **Half-Duplex (bidireccionales):** Solo un equipo transmite a la vez. También se llama Semi-Duplex (ej. Una comunicación por equipos de radio, si los equipos no son full-dúplex uno podría transmitir (hablar) si la otra persona está también transmitiendo (hablando) porque su equipo estaría recibiendo (escuchando) en se momento).
- **Full-Duplex (bidireccionales):** Ambos pueden transmitir y recibir a la vez de una misma información (ej. videoconferencia).

2.2.1.8. Estándares de redes

- **IEEE 802.3**, estándar para Ethernet.
- **IEEE 802.5**, estándar para Token Ring.
- **IEEE 802.11**, estándar para Wifi.
- **IEEE 802.15**, estándar para Bluetooh.

2.2.1.9. Tipos de redes

- **Red pública**

Una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz

de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

- **Red privada**

  Una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

- **Red de área personal (PAN)**

  Es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de un PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación ente los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar una red de alto nivel y el internet (un up link). Las redes personales del área se pueden conectar con cables con los buses de la computadora tales como USB y Firewire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.

- **Red de área local (LAN)**

  Una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o avión. Las redes de

área local a veces se llaman una sola red de la localización. Nota: Para los propósitos administrativos, LANs grande se divide generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroups es un grupo de las computadoras que comparten un sistema común de recursos dentro de un LAN.

- **Red de área local virtual (VLAN)**

  Una virtual LAN o comúnmente conocida como VLAN, es un grupo de computadoras, con un conjunto común de recursos a compartir y de requerimiento, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos pueden alcanzar a los otros por medio de Broadcast en la capa de enlace de datos, a pesar de su diversa localización física. Con esto, se pueden lógicamente agrupar computadoras para que la localización de la red ya no sea tan asociada y restringida a la localización física de cada computadora, como sucede con una LAN, otorgando además seguridad, flexibilidad y ahorro de recursos. Para lograrlo, se ha establecido la especificación IEEE 802.1Q como un estándar diseñado para dar dirección al problema de como separar redes físicamente muy largas en partes pequeñas, así como proveer un alto nivel de seguridad entre segmentos de redes internas teniendo la libertad de administrarlas sin importar su ubicación física.

- **Red de área del campus (CAN)**

  Se deriva a una red que conecta dos o más LANs los cuales deben

estar conectados en un área geográfica específica tal como un Campus de Universidad, un Complejo Industrial o un Base Militar.

- **Red de área metropolitana (MAN)**

  Es una red que conecta las redes de un área dos o más locales juntos, pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Los enrutadores (Routers) múltiples, los interruptores (Switch) y los cubos están conectados para crear a una MAN.

- **Red de área de almacenamiento (SAN)**

  Es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, esa basada en tecnología de fibra o ISCSl. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos de almacenamiento que conforman.

- **Red de privada virtual (VPN)**

  Una red se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicas a ejecutar programas de usuario (aplicaciones). En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes trasmiten información vita, por tanto, dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en

costos. Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una ventaja para las organizaciones sobre todo las que cuentas con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atracar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls y las VPN.

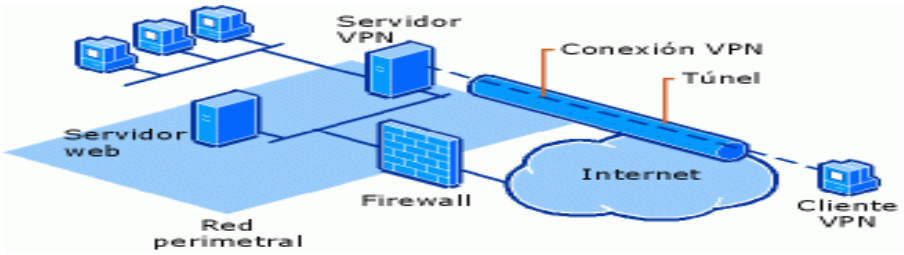


Figura 11. Modelo de una red privada virtual

2.2.1.10. ¿Por qué una VPM?

Cuando deseo enlazar mis oficinas centrales con algunas sucursales u oficina remorata tengo 3 opciones.

- **Modem:** Las desventajas es el costo de la llamada, ya que el costo de esta llamada seria por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuada.
- **Línea Provada:** Tendria que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200 kilómetros de distancia el costo seria

por la renta mensual por kilómetro sin importar el uso.

- **VPN:** Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

Una Red Privada Virtual (Virtual Prívate Network) es una red privada que se extiende, mediante un proceso de encapsulación y en algún caso de encriptación, desde los paquetes de datos a diferentes puntos remotos, mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por un túnel definido en la red pública.

2.2.1.11. Tipos de redes VPN

- **VPN basadas en el cliente**

Estas redes hacen uso de una aplicación (cliente) que es la encargada de controlar complemente la conexión y establecerla. Para poder navegar por esta red, generalmente, los usuarios necesitan de un usuario y una contraseña que les identifique que el servidor. Una vez se inicia sesión se establece la conexión segura de manera que toda la comunicación entre el cliente y el servidor se establece la conexión de manera que toda la comunicación entre el cliente y el servidor se realiza segura.

Este es el método más rápido y sencillo para conectar prácticamente cualquier equipo o dispositivo a una red segura navegar a través de ella.

Los protocolos más utilizados para este tipo de conexiones son L2TP (Layer 2 Tunneling Protocol). PPTP y SSTP, Además, si queremos una seguridad superior, podemos utilizar protocolos como OpenVPN, aunque son algo más complicados de utilizar (ya que funcionan mediante certificados).

- **VPN basadas en la red**

Este tipo de conexiones se utiliza para conectar dos o más redes entre sí a través de una red no segura como internet. Estas conexiones suelen ser utilizados generalmente por empresas y organismos que buscan conectar de forma segura dos o más sedes alrededor de todo el mundo sin tener que conectarlas físicamente, algo totalmente imposible.

Aunque existen varios protocolos para este tipo de conexiones, el más utilizado debido a su simplicidad es IPSec. Para establecer la conexión se deben definir los dispositivos encargados de encapsular y desencapsular el tráfico que viaja de extremo a extremo. También se definen los usuarios y contraseñas y los certificados que se van a utilizar y además, el tipo de tráfico que viajara por dicha red.

Las redes IPSec son mucho más dinámicas que las redes VPN basadas en cliente, por lo que desde ellas vamos a poder configurar el tipo de tráfico e incluso aplicar una serie de reglas o filtros, aumentando tanto el rendimiento de las redes como la seguridad.

- **VPN de acceso remoto**

  Muchas empresas han reemplazado con esta tecnología VPN su infraestructura “dial-up”, donde el cliente utilizaba un modem para llamar a través de la Red Telefónica Conmutada a un nodo del proveedor de servicios de internet y este con un servidor PPP establecía un enlace modem-a-modem, qye permite entonces que se enrute a internet.

  Esta implementación se trata de comunicaciones donde los usuarios se conectan con la empresa desde sitios remotos (oficinas comerciales, casas, hoteles, etc) utilizando internet como medio de acceso. Una vez autenticados tiene un nivel de acceso muy similar al que tiene en la red local de la empresa.

- **VPN interna**

  Una aplicación realmente desconocida pero muy útil y potente consiste en establecer redes privadas virtuales dentro de una misma red local. El objetivo último es aislar partes de la red y sus servicios entre sí, aumentando la seguridad. Una aplicación muy típica de este modelo se utiliza para aumentar la seguridad en redes de acceso inalámbrico, separándolas asi de la red física para evitar posibles guas de información o accesos no autorizados.

2.2.1.12. Seguridad VPN

Una red VPN bien implementada garantizara conexiones seguras en todas sus comunicaciones. Hay varios aspectos que habrá que tener en cuenta cuando se trata de la seguridad de una VPN.

Autenticación

Para que la red VPN sea segura, es necesario autenticación de usuarios. Esta autenticación puede venir de contraseñas, códigos biométricos, u otros métodos criptográficos. La autenticación puede implicar la acción del usuario, o puede ir incorporada en el cliente VPN de manera que el usuario no tenga que hacer nada.

Mecanismo de Seguridad

Las VPNs seguras usan protocolos de tunnelling criptográficos para ofrecer.

- Confidencialidad: Bloqueo de la intercepción de paquetes.
- Autenticación: Bloqueo de la suplantación de identidad.
- Integridad: Bloqueo de la alteración de los mensajes.

Ventajas

- El costo de los enlaces es más barato, lo que permite realizar y rentabilizar innumerables proyectos orientados a optimizar la gestión comercial y de operaciones de empresas e instituciones.
- Debido a la utilización de internet como red de soporte, ofrecen un gran ahorro en la infraestructura de red.

- Relativa independencia de ISPs, ya que internet provee la interconectividad.
- Las transmisiones de datos son autentificadas, garantizando la seguridad del acceso e integridad de la información.
- Ofrecen la posibilidad de una gran diversidad de usuarios remotos.
- Simplicidad en el manejo de topologías.
- Escalabilidad vía incremento de ancho de banda.

Desventajas

- El tiempo de respuesta no está garantizado y, por lo tanto, no son recomendables para aplicaciones críticas.
- Si, eventualmente, el ISP de algunos de los puntos pierde la conexión, la conectividad del enlace deja de existir entre esos puntos.
- Los anchos de banda reales son inferiores a los teóricamente contratados, que no existe calidad de servicio.
- No todos los equipos actualmente instalados poseen facilidades para realizar VPNs. Además, se rigen por distintas normas y estándares y no son compatibles entre ellos.

2.2.2. Software libre

2.2.1.13. Introducción

El término Software Libre se refiere al conjunto de software (programa informático) que, por elección manifiesta de su autor, puede ser copiado, estudiado, modificado, utilizado libremente con cualquier

fin y redistribuido con o sin cambios o mejoras. Su definición está asociada al nacimiento del movimiento de software libre, encabezado por Richard Stallman y la consecuente fundación en 1985 de la Free Software Foundation, que coloca la libertad del usuario informático como propósito ético fundamental. Proviene del término en ingles free software, que presenta ambigüedad entre los significados libre y gratis asociados a la palabra free. Por esto que suele ser considerado como software gratuito y no en su acepción amas precisa como software que puede ser modificado sin restricciones de licencia.

2.2.1.14. GNU/LINUX

GNU/LINUX (más conocido como Linux) es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado: la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente.

El sistema lo forma el núcleo del sistema (kernel) más un gran número de programas y librerías que hacen posible su utilización. Linux se distribuye bajo la Licencia Publica General GNU (GLP), por lo tanto, el código fuente tiene que estas siempre accesible.

Existen cientos de distribuciones Linux en el mundo; la mayoría se puede obtener a través de internet, aunque también se pueden comprar algunas de ellas. Las distribuciones más conocidas son: SuSE, RedHat, Fedora, CentOS, Debian y Mandrake.

2.2.1.15. CentOS

CentOS (Comunidad enterprise OTRABAJO System), publicado en mayo de 2004, es una distribución de sistema operativo libre 100% basado en el núcleo de Linux. Se deriva completamente de la distribución de Red Hat Enterprise Linux (RHEL). CentOS existe para proporcionar una plataforma informática de clase empresarial gratuita y se esfuerza por mantener una compatibilidad binaria del 100% con su fuente original, Red Hat.

Figura 12. Software libre centOS

2.2.1.16. OpenVPN

OpenVPN es una aplicación de software de código abierto que implementa las técnicas de Red Virtual Privada (VPN) para crear una conexión de punto a punto a página a página en configuraciones en rutas o en puentes y en lugares de remoto acceso. Utiliza un protocolo de seguridad personalizado que utiliza SSL/TLS para intercambios de claves. Es capaz de atravesar traductores de direcciones de red (NATs;

por sus siglas en ingles) y firewalls. Fue escrito por James Yonan y está publicado bajo una GNU Licencia Publica General, comúnmente conocida como la GLP. Esto significa que es capaz de enlazar 2 nodos (nodo A conectado a una red privada y a internet, nodo B en cualquier otra parte del mundo con conexión a internet) de forma que parezca que están en la misma LAN.

OpenVPN le permite a los compañeros verificar la autencidad de su identidad utilizando contraseñas previamente compartidas y certificados de usuario y contraseña. Al utilizar una configuración de servidores para múltiples clientes, le permite al servidor liberar certificados de autentificación para cada uno, utilizando una firma y la autoridad del certificado. Utiliza la biblioteca de encriptación de OpenSSL extensivamente, así como el protocolo SSLv3/TLSv1 y contiene muchas características adicionales de control y seguridad.

Ventaja

- Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no IP como IPX o broadcast (NETBIOS).
- Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aun cuando no es un equipo de la red local. Por otra parte, solo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.

- Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.
- Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como clienre (iniciando conexiones).
- Solo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.
- Las interfaces virtuales (tun0, tun1, etc) permiten la implementación de reglas de firewall muy específicas.
- Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.

Desventaja

- No tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.
- Falta de masa crítica.
- Todavía existe poca gente que conoce cómo usar OpenVPN.
- Al dia de hoy solo se puede conectar a otras computadoras. Pero esto está cambiando, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.

2.3. Definición de términos básicos

a) Implementación

La realización de una aplicación, instalación o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política. En ciencias de la computación, una implementación es la realización de una especificación técnica o algoritmos como un programa, componente software, u otro sistema de cómputo. Muchas implementaciones son dadas según a una especificación o un estándar.

b) Red

Una red informática está formada por un conjunto de ordenadores intercomunicados entre sí que se utilizan distintas tecnologías de Hardware/Software. Las tecnologías que utilizan (tipos de cables, de tarjetas, dispositivos, etc y los programas (protocolos) varían según la dimensión y función de la propia red, de hecho, una puede estar formada por solo dos ordenadores, aunque también por un nuevo casi infinito; muy a menudo, algunas redes se conectan entre si creando, por ejemplo, un conjunto de múltiples redes interconectadas, es decir, lo que conocemos por internet.

c) Redes públicas

Una red pública es básicamente el tipo de red que nos proporciona un servicio de conexión o telecomunicaciones a nuestro equipo a cambio de pago de una cuota de servicio. Cuando nosotros nos conectamos internet, a través de un Router, nos estamos conectando claramente a una red pública. En este tipo de redes, disponemos de acceso a servidores ubicados de distintos lugares del mundo para que estos nos presten un servicio que puede ser gratuito o de pago.

d) Red privada

Es una tecnología de red de computadora que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como internet. Permite que la computadora en la red envié y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

e) Cable coaxial

El cable coaxial, por su parte, es un tipo de cable que utiliza para transmitir señales de electricidad de alta frecuencia. Estos cables cuentan con un par de conectores concéntricos: el conductor vivo o central (dedicado a transportar los datos) y el conductor exterior, blindaje o malla (que actúan como retorno de la corriente y referencia de tierra). Entre ambos se sitúa el dieléctrico, una capa aisladora.

f) Cable de fibra óptica

La fibra óptica es un medio de transmisión, empleado habitualmente en redes de datos y telecomunicaciones, consistente en un hilo muy fino de material transparente, vidrio o materiales plásticos por el que se envían pulsos de luz que representan los datos a transmitir. Las fibras se utilizan ampliamente en telecomunicaciones, ya que permite enviar gran cantidad de datos en una gran

distancia, con velocidades similares a las de la radio y superiores a las de un cable convencional.

g) Red privada virtual

Una VPN o (siglas en ingles de Virtual Prívate Network o red privada virtual) consiste en una red privada de ordenadores que usa internet para conectar entre si sus nodos.

Una VPN nos permite cubrir la necesidad de compartir recursos entre varios equipos de un usuario de tal norma que este pueda disponer de la misma información en todos ellos. A nivel empresarial permite conectar a través de internet las diferentes sucursales de una empresa.

h) Protocolo de túnel

Se conoce como túnel o tunneling a la técnica que consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel de información dentro de una red de computadoras. El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la dirección de tráfico, etc. La técnica de tunelizar se suele utilizar para transportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría. Otro uso de tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.

i) GNU/Linux

GNU/Linux es un sistema operativo de software libre, es decir, respeta la libertad de los usuarios. El desarrollo GNU ha permitido que se pueda utilizar un ordenador sin software que atropelle nuestra libertad (más precisamente, distribuciones GNU/Linux) que son completamente software libre.

j) CentOS

CentOS es una distribución de Linux basada en Red Hat Enterprise Linux. Cada versión de CentOS es mantenida durante 7 años (por medio de actualizaciones de seguridad). Las versiones nuevas son liberadas cada 2 años y actualizadas regularmente (cada 6 meses) para el soporte de hardware nuevo.

Es un sistema de código abierto, basado en distribuciones Red Hat Enterprise Linux, operándose de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto estable y fácil de instalar utilizar.

k) OpenVPN

OpenVPN es una herramienta de conectividad basada en software libre: SSL (Secure Socket Layer), VPN Virtual Prívate Network (red virtual privada). OpenVPN conectividad punto-a-punto con validación jerárquica de usuario a host conectados remotamente. Resulta una muy buena opción en tecnologías WI-FO (redes inalámbricas IEEE 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Este publicado bajo la licencia GPL, de software libre.

2.4. Hipótesis de investigación

2.4.1. Hipótesis general

La implementación de una red privada virtual (VPN) mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

2.4.2. Hipótesis específicas

1. La funcionalidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.
2. La seguridad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.
3. La confidencialidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

2.5. Operacionalización de las variables

Tabla 1. ***Operacionalización de la variables***

VARIABLES	DIMENSIONES	INDICADORES	ESCALA
(X) Implementación de una red privada virtual (VPN)	X.1. Funcionalidad X.2. Seguridad X.3. Confidencialidad	X.1.1. VPN de acceso remoto X.1.2. VPN de router X.2.1. Riesgos informáticos X.2.2. Ataque por virus X.2.3. Intentos de instrucción X.3.1. Autentificación X.3.2. Integridad	Siempre. Casi Siempre A veces Casi nunca Nunca Likert.
(Y) Mejora de la comunicación de las oficinas externas	Y.1. Calidad Y.2. Satisfacción	Y.1.1. Calidad de servicios Y.1.2. Calidad de comunicación Y.1.3. Calidad de conectividad Y.2.1. Recursos Y.2.2. Conexión Y.2.3. Velocidad	Siempre. Casi Siempre A veces Casi nunca Nunca Likert.

Fuente: Propia.

CAPÍTULO III

METODOLOGÍA

3.1. Diseño metodológico

3.1.1. Tipo

El tipo de investigación fue aplicado. Valderrama (2002) indicó que: "También denominada activa o dinámica y se encuentra íntimamente ligada a la anterior ya que depende de sus descubrimientos y aportes teóricos"

3.1.2. Nivel

El nivel de investigación es correlacional. Hernández, Fernández y Baptista (2014) indicaron que: "Asocian variables mediante un patrón predecible para un grupo o población"

3.1.3. Enfoque

El enfoque de la investigación es cuantitativo. Hernández, Fernández y Baptista (2014) indicaron que: "Utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin establecer pautas de comportamiento" (p.4).

3.2. Población y muestra

3.2.1. Población

La población está constituida por las oficinas externas de la Universidad José Faustino Sánchez Carrión: 15 administrativos, en el Centro Pre Universitario; 10 administrativos, en el Órgano de Control Institucional; 2 administrativos, en el

Museo Arqueológico Nacional de la UNJFSC; 4 administrativos, en el Centro de Idiomas, la facultad de Medicina también cuenta con 4 personal administrativo dentro del Hospital Regional.

3.2.2. Muestra

La muestra de estudio se consideró a la totalidad de la población por ser pequeña fueron todas las unidades de observación, es decir los 35 administrativos de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Dado que la población es pequeña, se ve como un ejemplo no probabilístico, a la luz del hecho de que el especialista, al darse cuenta bien de la población y con capacidad de toma de decisiones, elige que las unidades de percepción incorporen el ejemplo. Lo que se utilizó de la estrategia, o método de prueba llamado examen de sentimientos con propósito, con la regla de acomodación del científico para ser delegado, el ejemplo se aplicó a todos los componentes de percepción con atributos similares, según Córdoba (2009) en su libro llamado Las estadísticas aplicadas a la investigación y la ecuación objetiva que presentamos, su aplicación no es importante para obtener el ejemplo, que considera.

3.3. Técnicas de recolección de datos

Las Técnicas e instrumentos utilizados en el presente trabajo de investigación se muestran a continuación:

Técnicas:

- Análisis documental

- Observación
- Encuesta

Instrumentos:

- Fichas bibliográficas, hemerográficas y de investigación
- Guía de observación
- Cuestionario de preguntas.

3.4. Técnicas para el procesamiento de la información

Análisis Documental

Mediante el análisis documental y sus respectivos instrumentos se revisarán fuentes bibliográficas, publicaciones especializadas y portales de Internet; directamente relacionados con el tema de investigación.

A través de la entrevista y su instrumento – cuestionario, elaborado por el tesista especialmente para esta investigación, se recopilará información sobre cada una de las dimensiones de la variable, las preguntas están referidas a los aspectos concretos que aportaran para recopilar datos y ubicar las deficiencias en la Vd.

Mediante la observación y su respectivo instrumento vamos a comprender procesos, interrelaciones entre personas y sus situaciones o circunstancias y eventos que suceden a través del tiempo, así como los patrones que se desarrollan y los contextos sociales y culturales en los cuales ocurren las experiencias humanas; así como identificar problemas.

a) Ficha Técnica de Instrumentos

La encuesta está constituida por preguntas de la Vi y la Vd., La medición se hará a través de la Escala de Likert, que mide de 1 a 5.

b) Administración de los instrumentos y obtención de los datos

Para la recolección de datos la información se contará con un cuestionario, confiable y validado. La confiabilidad que se logrará aplicando 02 veces el cuestionario a la muestra previamente seleccionada.

Para lograr la validez del instrumento, se recurrirá a profesionales capacitados especialistas relacionados al estudio. En la administración de cuestionarios se contará con el valioso apoyo en la recopilación de datos recogidos de las muestras.

Análisis Estadístico

Se llevará a cabo utilizando el paquete estadístico SPSS 25.0 el cual procesará, para lograr la interpretación, análisis y discusión los gráficos y figuras estadísticos, para lograr los resultados y contar con las conclusiones, implicando los objetivos y las hipótesis que será el producto final de la investigación.

Formulación del modelo

a. Hipótesis Nula.

Existen evidencias que las medias de los tratamientos estadísticamente no difieren significativamente.

b. Hipótesis alterna.

Estadísticamente las medias de los tratamientos difieren significativamente.

c. Recolección de datos y cálculos de los estadísticos correspondientes.

La recolección de datos se efectuará una vez aplicado los tratamientos correspondientes a cada muestra y para el procesamiento se utilizarán programas estadísticos.

d. Decisión estadística.

La decisión estadística se tomará como consecuencia de la comparación del estadístico de prueba calculado y el obtenido mediante tablas estadísticas correspondientes a la distribución del estadístico de prueba; esto quiere decir si el valor del estadístico de prueba calculado se encuentra en la región de rechazo se rechaza la hipótesis nula, en caso contrario se acepta; es decir:

Si: **$F0 > F\alpha, a-1, N-a$ se rechaza**

CAPÍTULO IV
RESULTADOS

4.1. Instalación del equipamiento lógico a utilizar

Fedora 9 en adelante incluye paquete openvpn en sus depósitos Yum, por lo que solo es necesario instalarlo desde la terminal a través de la orden yum. La siguiente forma solo es necesario para CentOS 7.

4.1.1. Instalación de los repositorios

Instalamos los repositorios para poder instalar los paquetes necesarios de OpenVPN. Como el usuario root, desde una terminal, tenemos que habilitar el paquete epel, yum install epel – release, utilizando cualquier editor de texto.

Figura 13. Instalando paquetes openVPN.

4.1.2. Instalación de openVPN

Instalamos y habilitamos todo el paquete del repositorio epel, instalar el equipamiento lógico (software) necesario con el mandato yum. Se requiere el paquete OpenVPN, **yum install OpenVPN –y.**

Figura 14. Instalación de openPVN.

Instalando el paquete de OpenVPN, creando los certificados **easy-rsa** que vamos a necesitar para los clientes.

Figura 15. Instalación de los certificados.

Luego de instalar los 3 paquetes, se copiará el archivo **/server.conf,** de configuración de OpenVPN que por defecto se encuentran en la siguiente ruta**: cp /usr/share/doc/openvpn-2.3.6/ simple-config-files/server.conf**, movemos a la siguiente ruta **/usr/etc/openvpn/**

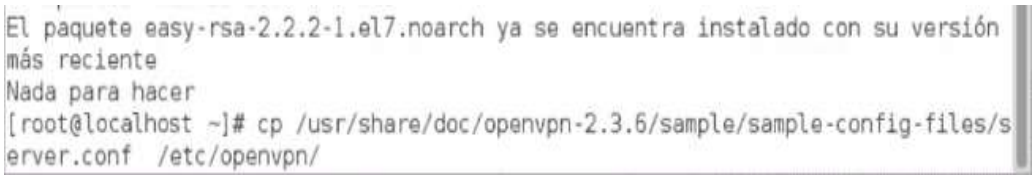


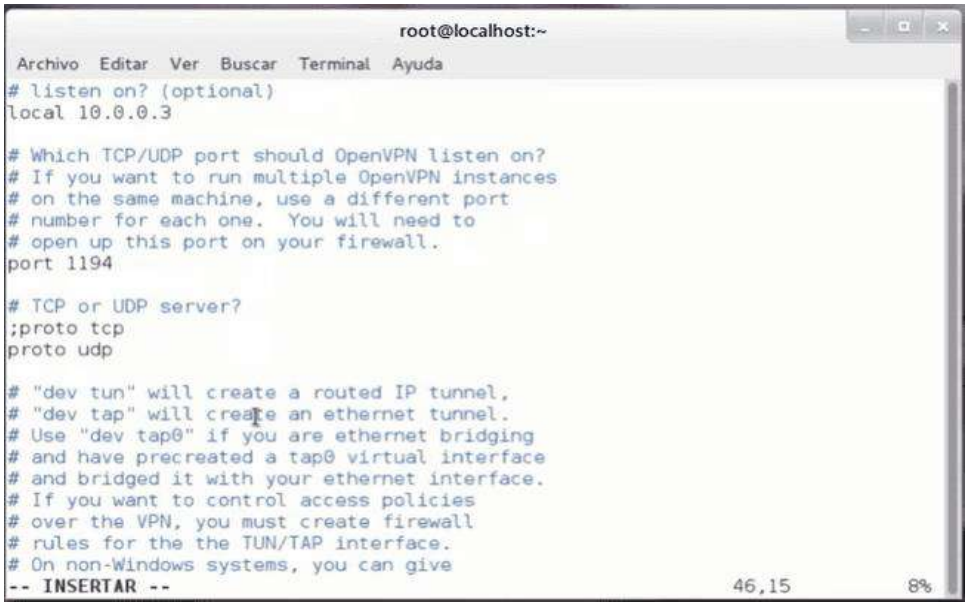
Figura 16. Cambiando el directorio de archivos server.

4.1.3. Configuración de openVPN

Para la **VPN** se recomienda utilizar una red privada, a fin de poder permitir a los clientes conectarse sin conflictos de red. Un ejemplo de red poco usada seria

10.8.0.0/ 255.255.255.0, por lo cual permitirá conectarse a la **VPN** a 254 clientes.

Abrir el archivo de configuración con cualquier editor con el siguiente comando:



vim /etc/openvpn/server.conf.

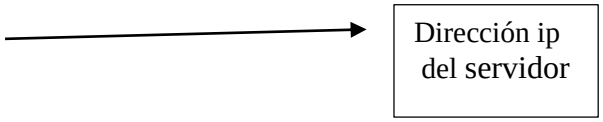


Figura 17. Contenido del server.

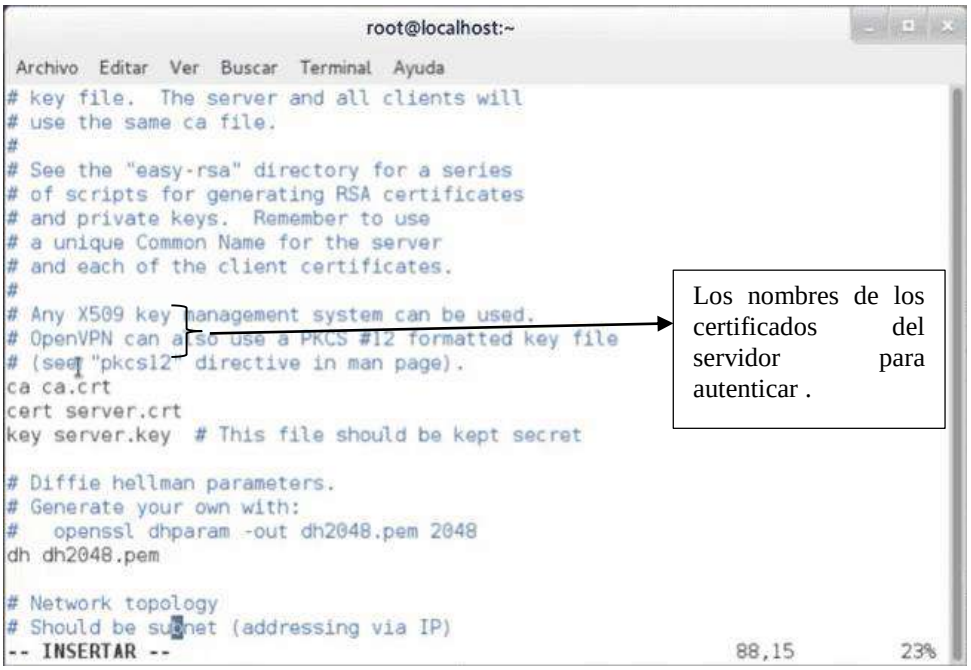


Figura 18. Identificando los certificados.

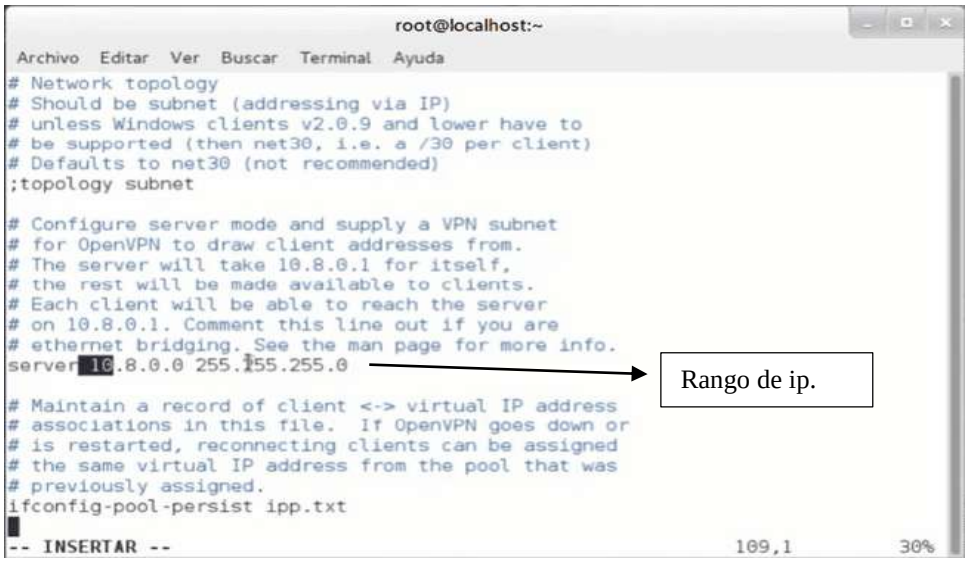


Figura 19. Rango de ip para los clientes.

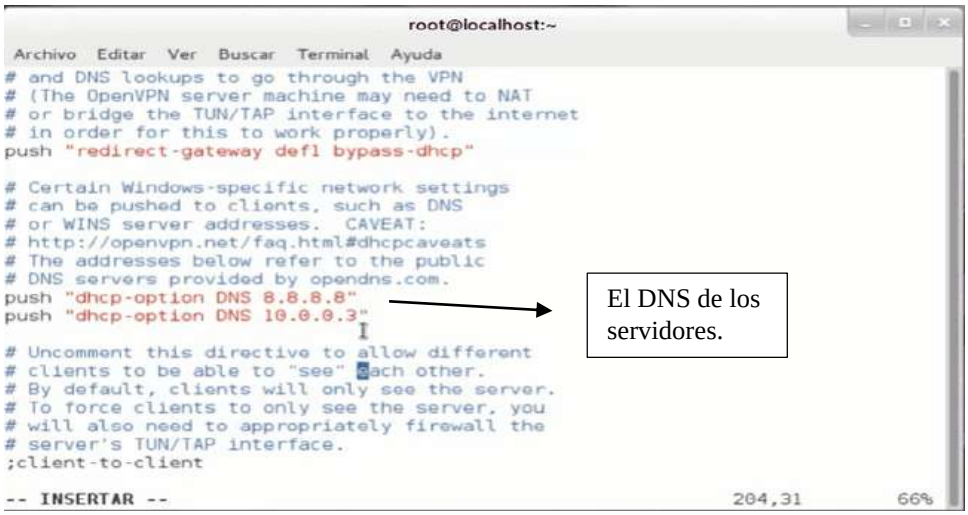


Figura 20. El DNS del servidor.

Descripción de los parámetros:

- **Proto:** tipo de protocolo que se empleara en la conexión atraves de VPN
- **Port:** Especifica el puerto que será utilizado para que los clientes VPN puedan conectarse.
- **Dev:** tipo de interfaz de conexión virtual que se utilizara el servidor openVPN.
- **Ca:** Especifica la ubicación exacta del archivo de Autoridad Certificadora [.ca].
- **Key:** Especifica la ubicación de la llave [.key] creada para el servidor.
- **Cert:** Especifica la ubicación del archivo [.crt] creada para el servidor.
- **Server:** Se asigna el rango de IP virtual que se utilizara en la red del túnel VPN.
- **Dh:** Ruta exacta del archivo [.pem] el cual contiene el formato de Diffie Hellman (requerido para –**tls-server** solamente).

Se crea el archivo keys dentro de la carpeta openvpn, con el siguiente comando:

mkdir –p /etc/openvpn/easy – rsa/keys

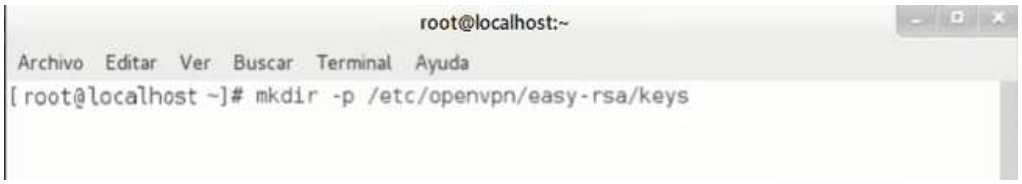


Figura 21. Creando keys.

4.1.4. Generar los script de los certificados

Se copiarán dentro del directorio **/etc/openvpn/easy-rsa/** los archivos **openssl.cnf, pkitool, whichopensslcnf y vars** necesarios para generar los certificados que se localizan en **/usr/share/easy-rsa/2.0/.**

cp –rf /usr/share/easy-rsa/2.0/* /etc/openvpn/easy-rsa/

Figura 22. Copiando los directorios.

Utilizar el editor de texto para abrir el archivo **/etc/openvpn/vars** y modificar, con el siguiente comando.

Figura 23. Abriendo el directorio vars.

Dentro del archivo **/etc/openvpn/vars** modificamos todos los valores que empiezan con KEY.

Figura 24. Modificando el directorio vars.

Desbloqueamos para poder habilitar el dominio **export KEY_CN**=" CENTOS"

Cada vez que se vayan a generar nuevos certificados, debe ejecutarse el mandato anterior a fin de que carguen las variables de entorno definidas.

Se copiarán archivos **etc/openvpn/easy-rsa/openssl.cnf** al directorio **/etc/openvpn/easy-rsa/openssl -1.0.0.cnf**, con el siguiente comando.

cp /etc/openvpn/easy-rsa/openssl -1.0.0.cnf /etc/openvpn/easy-rsa/openssl.cnf

Figura 25. Copiando el directorio openssl.

4.1.5. Generando certificado para las llaves

Creamos las llaves, los certificados para que tenga autentificación de los clientes al servidor, con el siguiente comando: **cd /etc/openvpn/easy-rsa/**

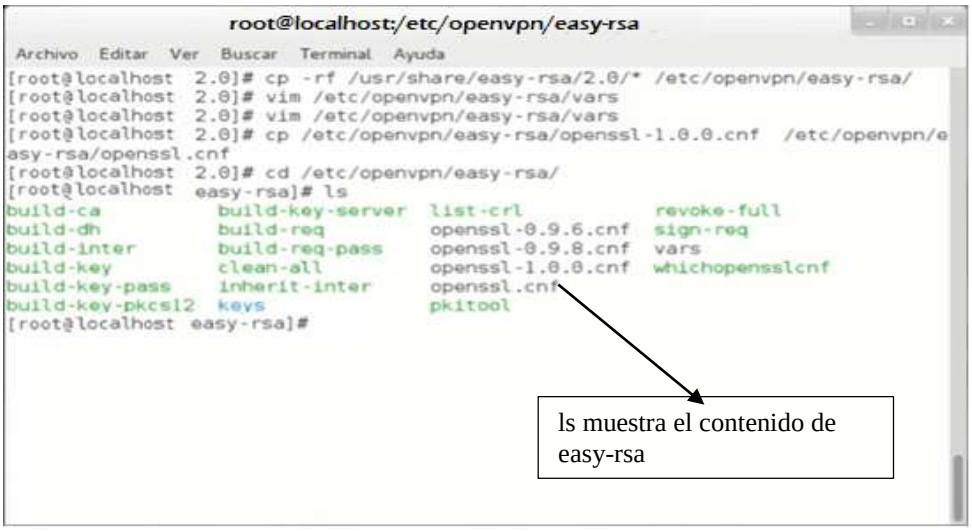


Figura 26. Visualizando el contenido de esay-rsa.

Se ejecuta el archivo **./clean – all** a fin de limpiar cualquier firma digital correspondiente a las llaves.

```
[root@localhost easy-rsa]# ./clean-all
```

Figura 27. Limpiando archivo easy-rsa

Crear el primer certificado del servidor, con el siguiente comando.

```
[root@localhost 2.0]# cd /etc/openvpn/easy-rsa/ ./build-ca
```

Resultado de la creación del primer certificado.

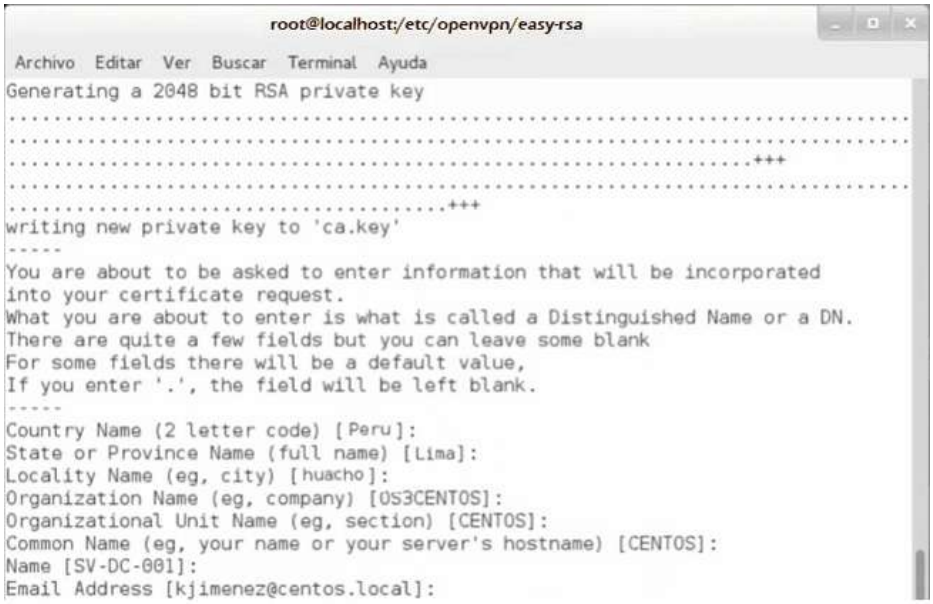


Figura 28. Resultado de la configuración del certificado

Generar la firma digital, con el siguiente comando. Resultado de la firma

```
[root@localhost 2.0]# cd /etc/openvpn/easy-rsa/ ./build-key-server server
```

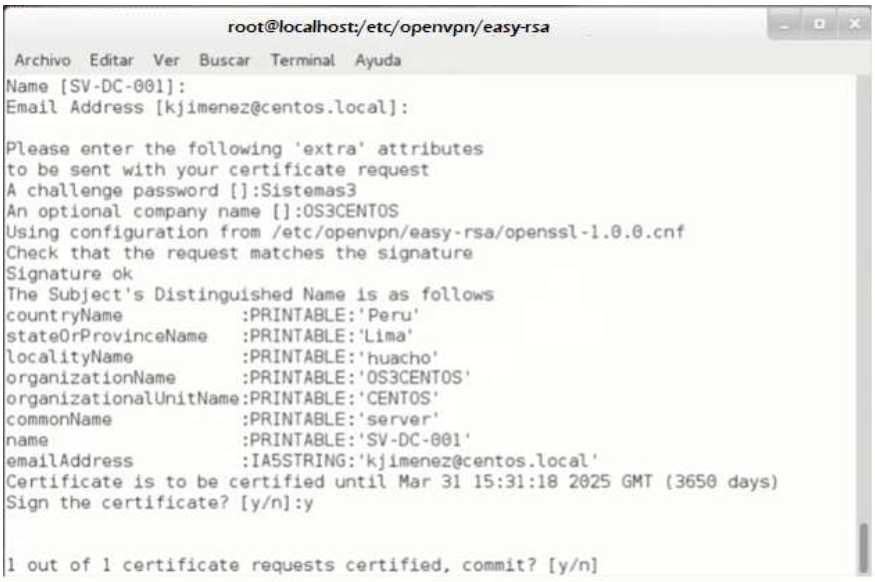


Figura 29. Resultado de la configuración de la firma digital

Ingresamos a la siguiente ruta de las llaves,

```
[root@localhost easy-rsa]# cd /etc/openvpn/easy-rsa/keys/
```

Moveremos dentro del directorio **/etc/openvpn/** los archivos **cp dh2048.pem ca.crt server.crt server.crt server.key,** para que puedan ser leídos por openvpn.

```
[root@localhost keys]# cp dh2048.pem ca.crt server.crt server.key /etc/openvpn
/
```

4.1.6. Configuración del ruteo

Instalación de de iptables es la parte que se encarga de filtrar la red, con el siguiente comando:

```
[root@localhost keys]# yum install iptables-services -y
```

Ejecutamos el siguiente comando para habilitar los servicios de iptables

```
[root@localhost keys]# systemctl enable iptables.service
ln -s '/usr/lib/systemd/system/iptables.service' '/etc/systemd/system/basic.targ
et.wants/iptables.service'
```

Ejecutamos el siguiente comando

```
[root@localhost keys]# systemctl mask firewalld
ln -s '/dev/null' '/etc/systemd/system/firewalld.service'
```

Ejecutamos el siguiente comando para detener los servicios del firewall

```
[root@localhost keys]# systemctl stop firewalld
```

Ejecutar el siguiente comando para iniciar los servicios de iptables

```
[root@localhost keys]# systemctl start iptables
```

Limpiamos la tabla de iptables con el siguiente comando

```
[root@localhost keys]# iptables --flush
```

Agregamos una ruta del nateo en la tabla de iptables, con el siguiente comando

```
[root@localhost keys]# iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o ens33 -j
 MASQUERADE
```

Guardar la configuración de iptables

```
[root@localhost keys]# iptables-save > /etc/sysconfig/iptables
```

Para que las configuraciones tengan efecto, es necesario reiniciar todos los servicios con el siguiente comando

```
[root@localhost keys]# systemctl restart network.service
```

4.1.7. Iniciamos los servicios openVPN

Ejecutamos el siguiente comando para Habilitar los servicios openVPN.

```
[root@localhost  keys]# systemctl -f enable openvpn@server.service
ln -s '/usr/lib/systemd/system/openvpn@.service' '/etc/systemd/system/multi-user
.target.wants/openvpn@server.service'
```

Iniciamos los servicios de openVPN, con el siguiente comando

```
[root@localhost  keys]# systemctl start  openvpn@server.service
[root@localhost  keys]# cd /etc/openvpn/easy-rsa/
[root@localhost  easy-rsa]# ./build-key cliente
```

4.1.8. Autentificar a los clientes

Finalmente se crean los certificados para los clientes, ingresando los siguientes comandos.

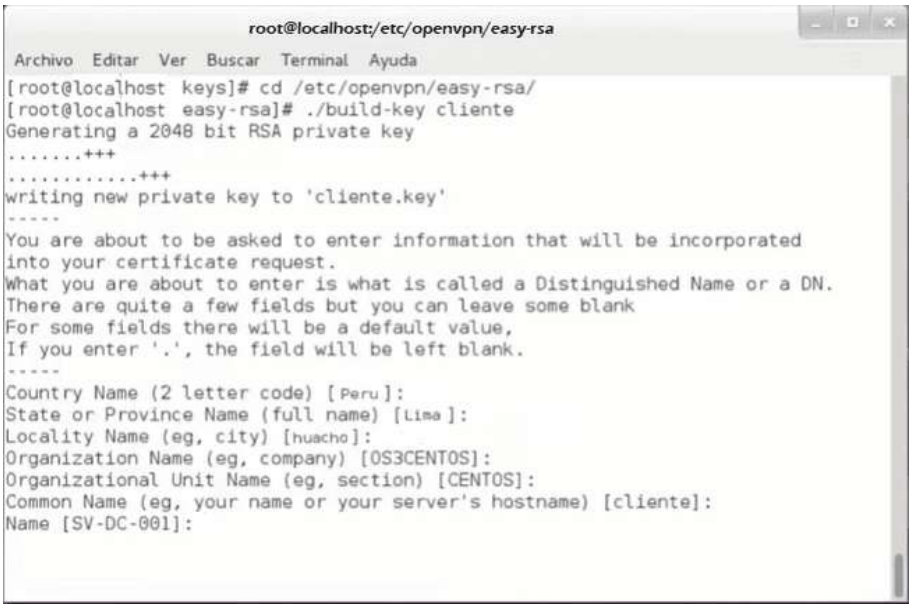


Figura 30. Configuración del certificado para el cliente.

4.1.9. Configuración de clientes windows

Después de instalar nuestro servidor openVPN en la distribución Linux, vamos a instalar el cliente openVPN en Windows.

La siguiente ventana pertenece a la ubicación donde se localiza los certificados e instalador de openVPN.

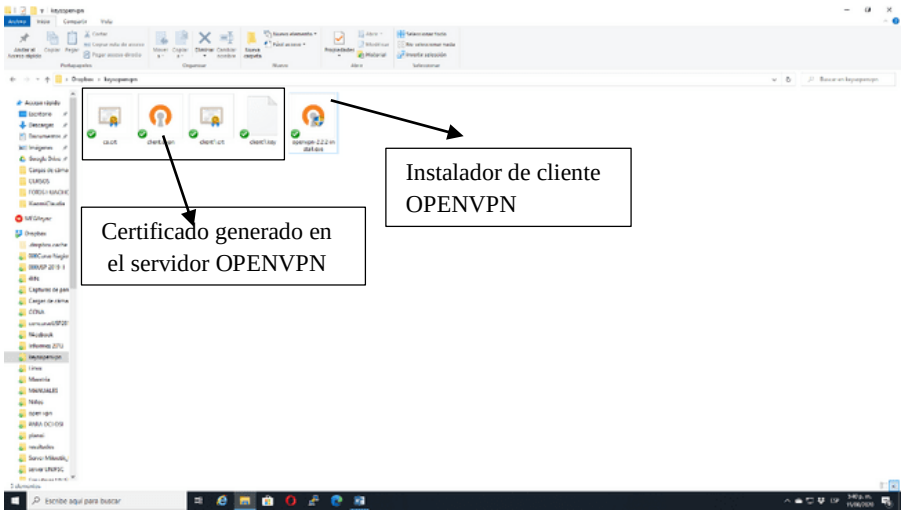


Figura 31. Archivo de configuración en Windows 10

Instalar **openVPN GUI,** se requiere instalar la versión de desarrollo 2.2.2 de **openVPN GUI.** El cliente es estable siempre que se verifique que funcione adecuadamente la configuración utilizada antes de poner en marcha en un entorno productivo.

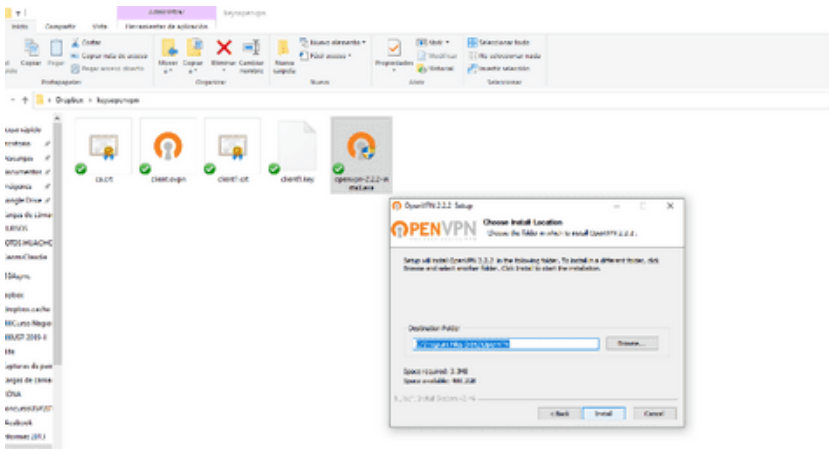


Figura 32. Ejecutando OpenVPN

Se copia los certificados en el disco duro de la PC del cliente que van a ser utilizado para la conexión.

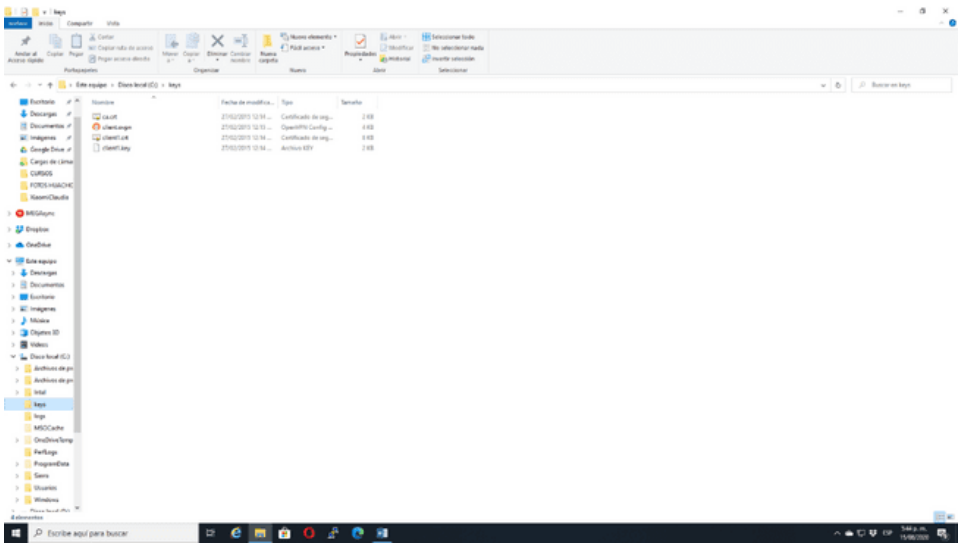


Figura 33. Ubicación de los certificados

En el archivo cliente.ovpn se referencia la dirección del servidor OpenVPN y la ruta de los certificados.

```
# If you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 200.48.125.180 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind
```

Puerto de comunicación al servidor OpenVPN.

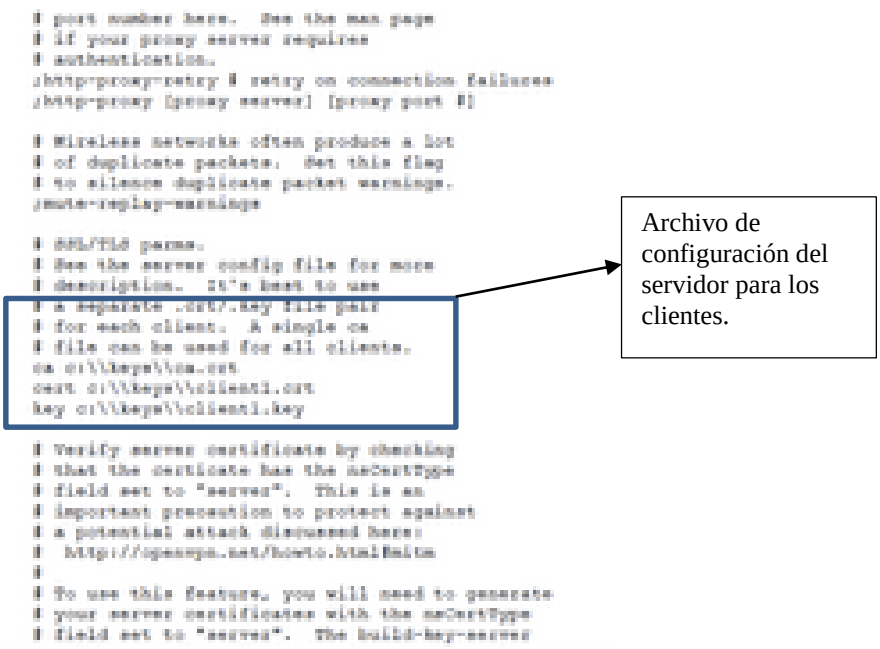


Figura 34. Líneas del archivo de configuración.

4.1.10. Ejecutando openVPN GUI

Este archivo se puede utilizar con la interfaz gráfica de **NetworkManager.** Solo hay que hacer click sobre el icono en el escritorio.

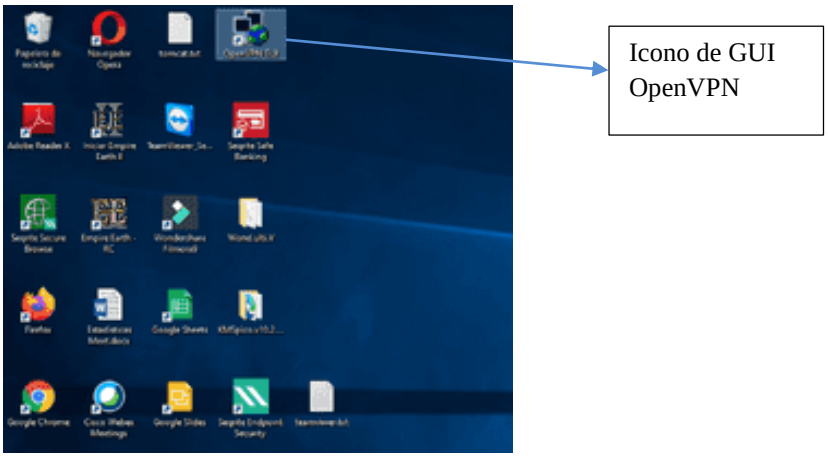


Figura 35. Ubicación del ejecutable openVPN en windows10.

Aparecerá la interfaz de la conexión del cliente **openVPN** en Windows hacia el servidor **centOS.**

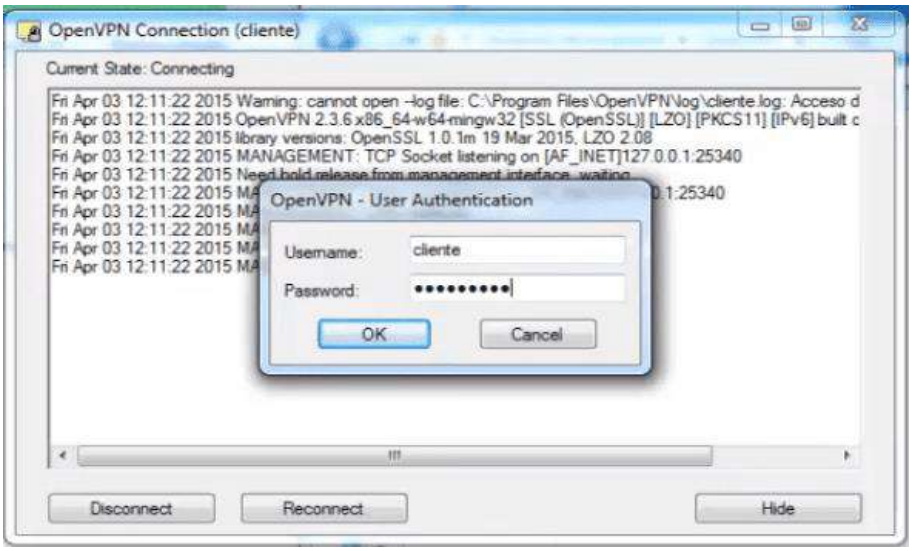


Figura 36. Conectándose el cliente VPN.

Aparecerá un dialogo donde se muestra el mensaje del cliente está conectado al vpn.

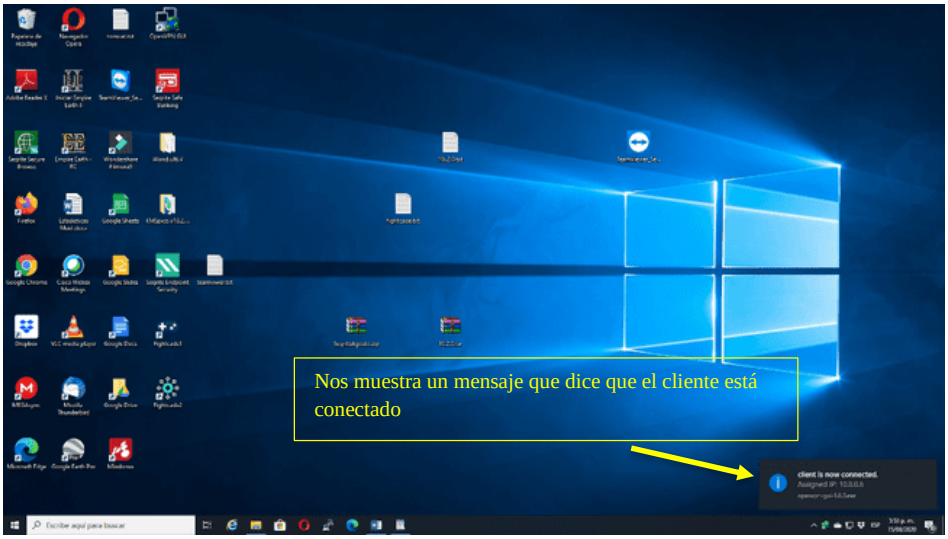


Figura 37. Confirmando la conexión del VPN.

Se genera la conexión del tipo TAP que permite al **VPN** conectarse al servidor, este controlador es usado para proporcionar una correcta operación del **VPN.**

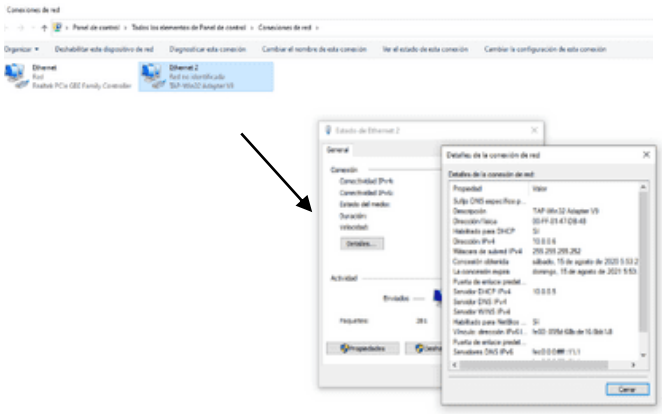


Figura 38. Conexión tipo TAP-win32

4.2. Análisis de resultados

Tabla 2. ***Funcionalidad***

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	7	20,0	20,0	20,0
	Medio	18	51,4	51,4	71,4
	Alto	10	28,6	28,6	100,0
	Total	35	100,0	100,0	

Para efectos de una mejor visualización y presentación de datos se muestra la siguiente figura:

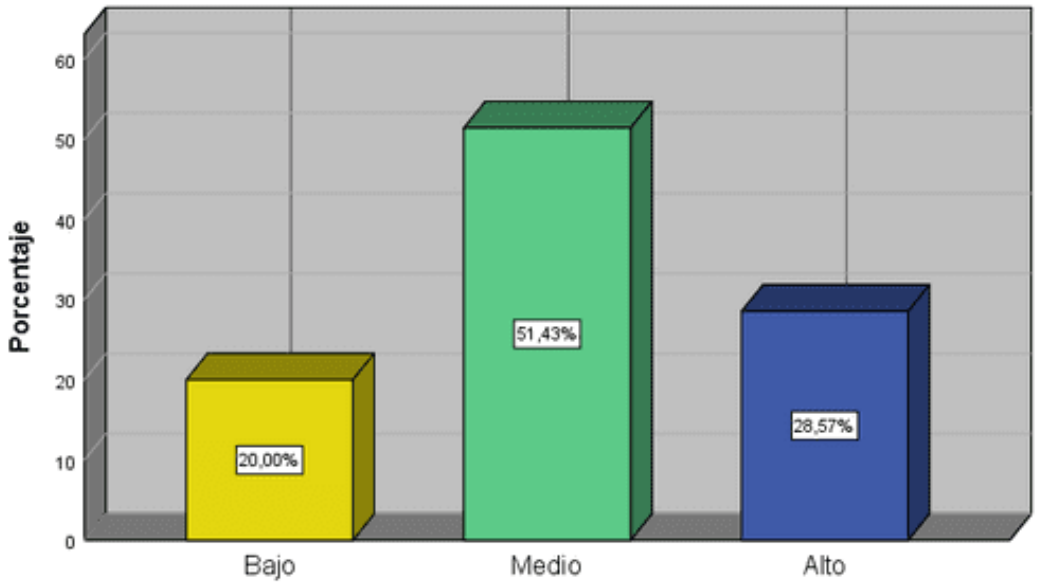


Figura 39. **Funcionalidad**

De la figura 39, un 51,43% de los administrativos de las oficinas externas de la Universidad José Faustino Sánchez Carrión creen que existe un nivel medio en la dimensión funcionalidad, un 28,57% un nivel alto y un 20,00% un nivel bajo.

Tabla 3. ***Seguridad***

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	6	17,1	17,1	17,1
	Medio	16	45,7	45,7	62,9
	Alto	13	37,1	37,1	100,0
	Total	35	100,0	100,0	

Para efectos de una mejor visualización y presentación de datos se muestra la siguiente figura:

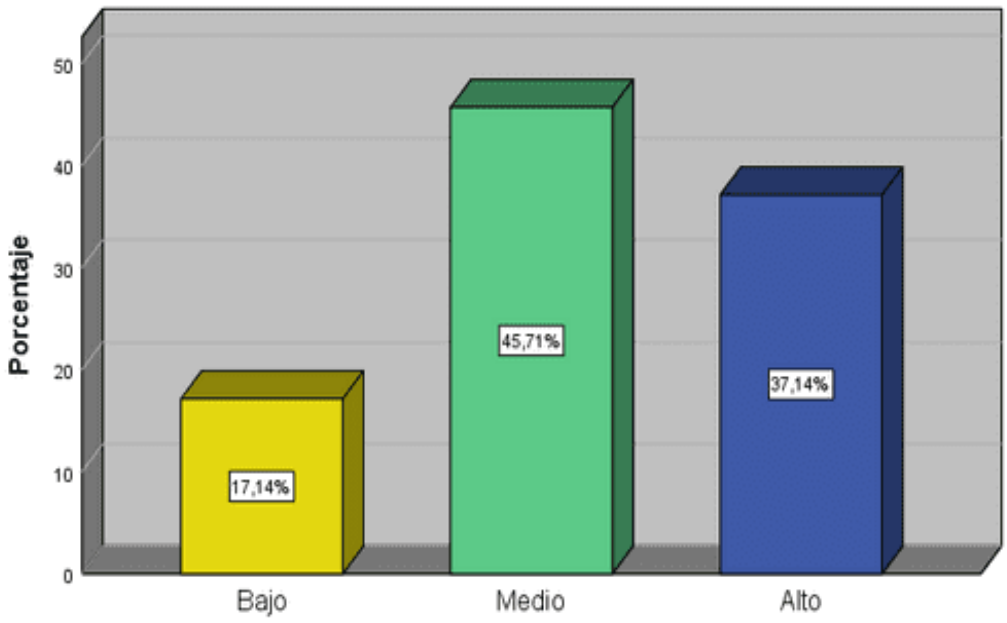


Figura 40. **Seguridad**

De la figura 40, un 45,71% de los administrativos de las oficinas externas de la Universidad José Faustino Sánchez Carrión creen que existe un nivel medio en la dimensión seguridad, un 37,14% un nivel alto y un 17,14% un nivel bajo.

Tabla 4. ***Confidencialidad***

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	8	22,9	22,9	22,9
	Medio	19	54,3	54,3	77,1
	Alto	8	22,9	22,9	100,0
	Total	35	100,0	100,0	

Para efectos de una mejor visualización y presentación de datos se muestra la siguiente figura:

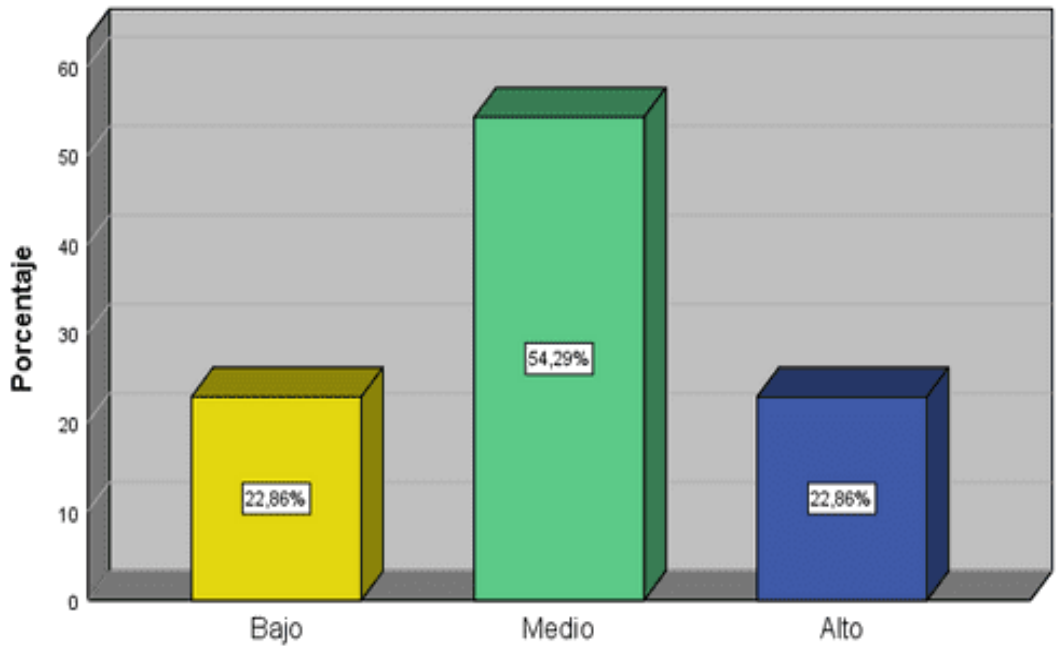


Figura 41. **Confidencialidad**

De la figura 41, un 54,29% de los administrativos de las oficinas externas de la Universidad José Faustino Sánchez Carrión creen que existe un nivel medio en la dimensión confidencialidad, un 22,86% un nivel alto y un 22,86% un nivel bajo.

Tabla 5. ***Calidad***

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	3	8,6	8,6	8,6
	Medio	19	54,3	54,3	62,9
	Alto	13	37,1	37,1	100,0
	Total	35	100,0	100,0	

Para efectos de una mejor visualización y presentación de datos se muestra la siguiente figura:

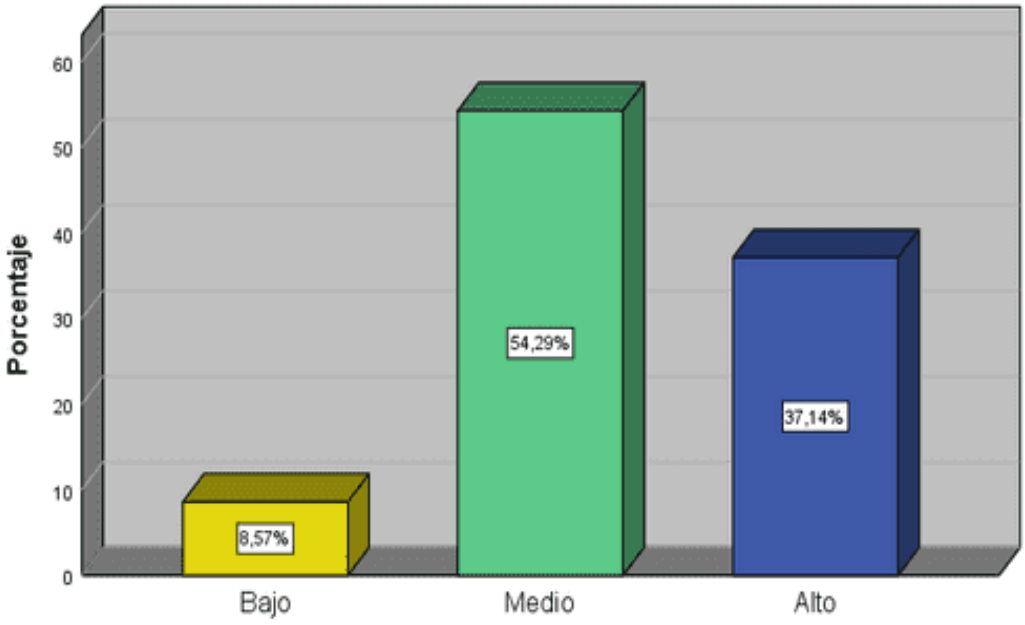


Figura 42. **Calidad**

De la figura 42, un 54,29% de los administrativos de las oficinas externas de la Universidad José Faustino Sánchez Carrión creen que existe un nivel medio en la dimensión calidad, un 37,14% un nivel alto y un 8,57% un nivel bajo.

Tabla 6. ***Satisfacción***

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	11	31,4	31,4	31,4
	Medio	20	57,1	57,1	88,6
	Alto	4	11,4	11,4	100,0
	Total	35	100,0	100,0	

Para efectos de una mejor visualización y presentación de datos se muestra la siguiente figura:

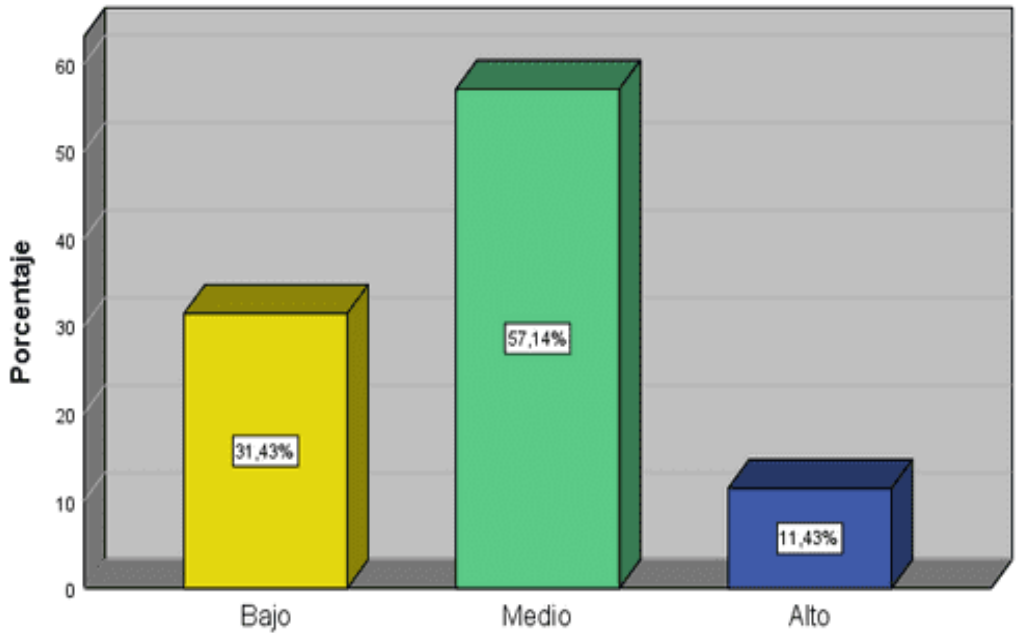


Figura 43. Satisfacción

De la figura 43, un 57,14% de los administrativos de las oficinas externas de la Universidad José Faustino Sánchez Carrión creen que existe un nivel medio en la dimensión satisfacción, un 31,43% un nivel bajo y un 11,43% un nivel bajo.

4.3. Contrastación de hipótesis

Hipótesis General

Hipótesis Alternativa: La implementación de una red privada virtual (VPN) mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Hipótesis nula: La implementación de una red privada virtual (VPN) no mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Tabla 7. ***La implementación de una red privada virtual y la comunicación de las oficinas externas***

			Implementación de una red privada virtual	Comunicaciones de las oficinas externas
Rho de Spearman	Implementación de una red privada virtual	Coeficiente de correlación	1,000	,907**
		Sig. (bilateral)	.	,000
		N	35	35
	Comunicaciones de las oficinas externas	Coeficiente de correlación	,907**	1,000
		Sig. (bilateral)	,000	.
		N	35	35

Como se observa en la tabla 7 se obtuvo una p=0.000 (p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que la implementación de una red privada virtual (VPN) mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

También se puede observar que el Rho de Spearman es r= 0.907, con lo que se llega a la conclusión que el coeficiente de correlación es de magnitud **muy buena**.

Hipótesis Específica 1

Hipótesis Alternativa**:** La funcionalidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Hipótesis nula**:** La funcionalidad no mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Tabla 8. ***La funcionalidad y la comunicación de las oficinas externas***

			Funcionalidad	Comunicaciones de las oficinas externas
Rho de Spearman	Funcionalidad	Coeficiente de correlación	1,000	,882**
		Sig. (bilateral)	.	,000
		N	35	35
	Comunicaciones de las oficinas externas	Coeficiente de correlación	,882**	1,000
		Sig. (bilateral)	,000	.
		N	35	35

Como se observa en la tabla 8 se obtuvo una p=0.000 (p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que la funcionalidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión

También se puede observar que el Rho de Spearman es r= 0.882, con lo que se llega a la conclusión que el coeficiente de correlación es de magnitud **buena.**

Hipótesis Específica 2

Hipótesis Alternativa**:** La seguridad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Hipótesis nula: La seguridad no mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Tabla 9. ***La seguridad y la comunicación de las oficinas externas***

			Seguridad	Comunicaciones de las oficinas externas
Rho de Spearman	Seguridad	Coeficiente de correlación	1,000	,791**
		Sig. (bilateral)	.	,000
		N	35	35
	Comunicaciones de las oficinas externas	Coeficiente de correlación	,791**	1,000
		Sig. (bilateral)	,000	.
		N	35	35

Como se observa en la tabla 9 se obtuvo una p=0.000 (p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que la seguridad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

También se puede observar que el Rho de Spearman es r= 0.791, con lo que se llega a la conclusión que el coeficiente de correlación es de magnitud **buena**.

Hipótesis Específica 3

Hipótesis Alternativa: La confidencialidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Hipótesis nula: La confidencialidad no mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

Tabla 10. ***La confidencialidad y la comunicación de las oficinas***

			Confidencialidad	Comunicaciones de las oficinas externas
Rho de Spearman	Confidencialidad	Coeficiente de correlación	1,000	,903**
		Sig. (bilateral)	.	,000
		N	35	35
	Comunicaciones de las oficinas externas	Coeficiente de correlación	,903**	1,000
		Sig. (bilateral)	,000	.
		N	35	35

Como se observa en la tabla 10 se obtuvo una p=0.000 (p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que existe la confidencialidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

También se puede observar que el Rho de Spearman es r= 0.903, con lo que se llega a la conclusión que el coeficiente de correlación es de magnitud **buena**.

CAPÍTULO V

DISCUSIÓN

5.1. Discusión de resultados

Los resultados estadísticos muestran que la implementación de una red privada virtual (VPN) mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Sperman que arroja un valor de 0,907 lo que presenta una muy buena asociación. Entre las variables estudiadas, a continuación, analizamos estadísticamente las variables por dimensiones, cuya primera dimensión se puede observar, la funcionalidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Spearman que arroja un valor de 0,882 lo que presenta una buena asociación. En la segunda dimensión, también se puede observar que la seguridad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Spearman que arroja un valor de 0,791 lo que presenta una buena asociación.

En la tercera dimensión, podríamos mostrar que la confidencialidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Spearman que arroja un valor de 0,903 lo que presenta una buena asociación. Nos ayuda a experimentar la implementación de una red privada virtual y comunicación de las oficinas externas. En este punto estamos de acuerdo con lo dicho por Qhuispe, (2021) Una vez establecidos los requerimientos y recursos de los que dispone la empresa, se utilizará el servicio de internet PYME de 75 Mbps con una dirección IP pública como medio para la conexión

VPN, se realizará la compra de un computador clon mejorado para ser utilizado como servidor VPN, de igual manera la infraestructura de red local es aceptable para el funcionamiento adecuado de red privada virtual. Luego de revisados los conceptos teóricos y analizadas las diferentes tecnologías existentes para realizar el diseño de la VPN, se ha llegado a la conclusión que se debe utilizar el sistema operativo Linux CentOS, con la versión 8, como software de red privada virtual OpenVPN, para servicio de firewall se utilizará firewalld y como servidor proxy a Squid proxy. Una vez realizada la instalación y configuración de Linux CentOS, Firewalld, Squid Proxy y OpenVPN, se concluye que se cumple con la implementación de la red privada virtual y se establece el manual técnico de configuración de nuevos usuarios como anexo 1, con lo cual el administrador del servicio podrá agregar o eliminar cuentas de manera sencilla. Una vez evaluado la red privada virtual, realizando la verificación de conectividad, pruebas de conexión, pruebas de pérdidas de paquetes, pruebas de acceso a la red local, pruebas de acceso remoto y prueba de encriptación se verifica que se cuenta con una red privada virtual con un adecuado funcionamiento y con la seguridad necesaria. Realizada la implementación de la red privada virtual ha sido posible que los empleados de la COMISION FULBRIGHT DEL ECUADOR que requerían acceso de manera remota lo puedan realizar de manera sencilla, siendo para esto necesario únicamente el contar con el servicio de internet, los empleados podrán conectarse a la red local y por ende a los sistemas y servicios con los que se cuentan en la empresa desde cualquier sitio, para lo cual se estructuró una guía de usuario como anexo 2. La implementación de la red privada virtual se ha realizado con un costo mínimo comparado con otras soluciones en las cuales se requieren adquirir equipos y licencias de uso, dado que en este caso ha sido necesario únicamente el adquirir un equipo clon mejorado y no ha sido necesario adquirir licencias de ningún tipo al utilizar herramientas y sistemas de software libre

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

De las pruebas realizadas podemos concluir:

1. **Primera:** La implementación de una red privada virtual (VPN) mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Sperman que arroja un valor de 0,907 lo que presenta una **muy buena** asociación.

2. **Segunda:** La funcionalidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Spearman que arroja un valor de 0,882 lo que presenta una **buena** asociación.

3. **Tercera:** La seguridad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la correlación de Spearman que arroja un valor de 0,791 lo que presenta una **buena** asociación.

4. **Cuarta:** La confidencialidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión, debido a la

correlación de Spearman que arroja un valor de 0,903 lo que presenta una **buena** asociación.

6.2. Recomendaciones

1. Realizar estudios sobre las variables examinadas con una muestra mayor a nivel nacional con el fin de estandarizar y fijar criterios más específicos de implementación de una red privada virtual y comunicación de las oficinas externas en las comunidades de nuestro país.

2. Determinar otras variables relacionadas con el estudio de implementación de una red privada virtual y la comunicación con el fin de mejorar calidad de vida en la sociedad de nuestro país.

3. Utilizar las herramientas de medición aplicadas en este estudio para obtener información de precisa para analizar las características del trabajo de investigación.

REFERENCIAS BIBLIOGRAFICAS

7.1. Fuentes bibliográficas

Alonso, A. (2009). *Redes y Telecomunicaciones.* Madrid: Ra-ma.

Buelvas, D. (2010). Implementación de redes privadas virtuales en la mediana empresa. *Revista Visiòn Electrònica*, p.28.

7.2. Fuentes documentales

Baleta. (2020). *Diseño de una red virtual privada de acceso remoto para establecer conexiones de teletrabajo de forma segura en las organizaciones.* Colombia: Universidad Cooperativa.

Espinoza. (2018). *"Propuesta de una Red Privada Virtual para mejorar el Servicio de Comunicación Tiendas MASS para la empresa supermercados Peruanos S.A.* Perú: Universidad Autonoma.

Garcia. (2021). *Implementación de una VPN tipo cliente para una entidad financiera.* Perú: Universidad Tecnologica.

Mamani. (2019). *Diseño e Implementación de Red Privada Virtual IPSEC para la comunicación de caja rural de ahorro y crédito los Andes SA, Pun.* Puno: Universidad Nacional del Antiplano.

Perdomo. (2018). *Diseño de una Red Privada Virtual Segura Para Facilitar la comunicacion, Trabnajo y Flujo de Informacion en la empresa QOS LTDA.* Colombia: Universidad Cooperativa.

Qhuispe. (2021). *Estudio para la Implementación de una red privada virtual (VPN) utilizando herramientas de software libre.* Ecuador: Pontifica Universidad Catolica

Sánchez. (2018). *Implementación de una VPN en una red corporativa para mejorar la gestión de la información de los servicios en la empresa Técnica Plástica SRL.* Trujillo: Universidad Cesar Vallejo.

Torres, P. (2016). *Diseño de una Red Privada Virtual para la optimización de las comunicaciones en la Empresa Comunicaciones E Informática SAC.* Lima: Universo SA.

7.3. Fuentes Electrónicas

Bembibre, V. (2009). *https://www.definicionabc.com/tecnologia/vpn.php*.

Espinoza, J. (27 de noviembre de 2007). *http://www.usmp.edu.pe*. Obtenido de Boletines: http://www.usmp.edu.pe

Jean-Francois, P. (2017). *https://es.ccm.net/contents*.

Trujillo, E. (2006). *https://bibdigital.epn.edu.ec/bitstream*. Obtenido de https://bibdigital.epn.edu.ec/bitstream

Valencia, E. d. (17 de Agosto de 2016). *universidadviu*. Obtenido de universidadviu: https://www.universidadviu.com/explicando-la-arquitectura-protocolos-tcpip/

ANEXOS

Anexo 1: Matriz de consistencia

Anexo 2: Instrumento de recolecta de datos

Anexo 3: Tabla de datos (base de datos)

Anexo 1 Matriz de consistencia

TEMA: Implementación de una red privada virtual (vpn) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLE	DIMENSIONES	INDICADORES	MÉTODOLOGIA
Problema General ¿De qué manera la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión?	**Objetivo General** Determinar la implementación de una red privada virtual (VPN) y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.	**Hipótesis General** La implementación de una red privada virtual (VPN) mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.	**(X)** **Implementación de una red privada virtual (VPN)**	X.1. Funcionalidad X.2. Seguridad X.3. Confidencialidad	X.1.1. VPN de acceso remoto X.1.2. VPN de router X.2.1. Riesgos informáticos X.2.2. Ataque por virus X.2.3. Intentos de instrucción X.3.1. Autentificación X.3.2. Integridad	Población = 35 administrativos Muestra = 35 administrativos **Método:** Científico **Técnicas:** **Para acopio de datos:** La observación Encuesta Análisis documental y bibliográfica. **Instrumentos de recolección de datos:** Observación indirecta. Cuestionario Análisis de contenidos y fichas. **Para el procesamiento de datos.** Consistencia, codificación, tabulación de datos. **Técnicas para el análisis e interpretación de datos.** Paquete estadístico SPSS 25.0 Estadística descriptiva para cada variable. **Para presentación de datos** Cuadros, gráficos y figuras estadísticas. **Para el informe final:** Esquema propuesto por la Universidad Católica de Trujillo Benediscto XVI **Tipo de investigación:** Aplicada **Diseño de investigación:** Correlacional.
Problemas Específicos 1) ¿De qué manera la funcionalidad mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión? 2) ¿De qué manera la seguridad mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión? 3) ¿De qué manera la confidencialidad mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión?	**Objetivos Específicos** 1) Determinar la funcionalidad y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión. 2) Determinar la seguridad y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión. 3) Determinar la confidencialidad y la mejora de la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.	**Objetivos Específicos** 1) La funcionalidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión. 2) La seguridad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión. 3) La confidencialidad mejora significativamente la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.	**(Y)** **Mejora de la comunicación de las oficinas externas**	Y.1. Calidad Y.2. Satisfacción	Y.1.1. Calidad de servicios Y.1.2. Calidad de comunicación Y.1.3. Calidad de conectividad Y.2.1. Recursos Y.2.2. Conexión Y.2.3. Velocidad	

Anexo 2: Validación

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

VALIDACIÓN CON JUICIO DE EXPERTO:

TEMA: Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

OPINIÓN Ó JUICIO DE EXPERTO:

1.- La opinión que UD. Nos brinde es personal, sincera y anónima.

2.- marque con un aspa "X" dentro del cuadrado de valoración, solo una vez por cada criterio, el que UD, Considere su Opinión.

1: Muy Malo
2: Malo
3: Regular
4: Bueno
5: Muy Bueno

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.				✓	
Objetividad: Esta expresado en conductas observables.				✓	
Actualidad: Adecuado al avance de la ciencia y la tecnología.			✓		
Organización: Existe una organización lógica.				✓	
Suficiencia: Comprende los aspectos de cantidad y calidad.				✓	
Intencionalidad: Adecuado para conocer las opiniones de los encuestados.				✓	
Consistencia: Basados en aspectos teóricos científicos de organización.				✓	
Coherencia: Establece coherencia entre las variables y los indicadores			✓		
Metodología: La estrategia responde a los propósitos del estudio				✓	
Pertinencia: El instrumento es adecuado al tipo de investigación.				✓	

Datos y firma del juez Experto

EDDY IVAN GUASPE SOTO
INGENIERO INFORMATICO
Reg. CIP N° 91455

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

VALIDACIÓN CON JUICIO DE EXPERTO:

TEMA: Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

OPINIÓN Ó JUICIO DE EXPERTO:

1.- La opinión que UD. Nos brinde es personal, sincera y anónima.

2.- marque con un aspa "X" dentro del cuadrado de valoración, solo una vez por cada criterio, el que UD, Considere su Opinión.

1: Muy Malo
2: Malo
3: Regular
4: Bueno
5: Muy Bueno

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.					X
Objetividad: Esta expresado en conductas observables.				X	
Actualidad: Adecuado al avance de la ciencia y la tecnología.					X
Organización: Existe una organización lógica.				X	
Suficiencia: Comprende los aspectos de cantidad y calidad.				X	
Intencionalidad: Adecuado para conocer las opiniones de los encuestados.				X	
Consistencia: Basados en aspectos teóricos científicos de organización.			X		
Coherencia: Establece coherencia entre las variables y los indicadores				X	
Metodología: La estrategia responde a los propósitos del estudio				X	
Pertinencia: El instrumento es adecuado al tipo de investigación.				X	

Datos y firma del juez Experto
Hugo A. Osorio Olivos
CIP 090696

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

VALIDACIÓN CON JUICIO DE EXPERTO:

TEMA: Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

OPINIÓN Ó JUICIO DE EXPERTO:

1.- La opinión que UD. Nos brinde es personal, sincera y anónima.

2.- marque con un aspa "X" dentro del cuadrado de valoración, solo una vez por cada criterio, el que UD, Considere su Opinión.

1: Muy Malo
2: Malo
3: Regular
4: Bueno
5: Muy Bueno

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.					X
Objetividad: Esta expresado en conductas observables.					X
Actualidad: Adecuado al avance de la ciencia y la tecnologia.					X
Organización: Existe una organización lógica.					X
Suficiencia: Comprende los aspectos de cantidad y calidad.					X
Intencionalidad: Adecuado para conocer las opiniones de los encuestados.					X
Consistencia: Basados en aspectos teóricos científicos de organización.					X
Coherencia: Establece coherencia entre las variables y los indicadores					X
Metodologia: La estrategia responde a los propósitos del estudio					X
Pertinencia: El instrumento es adecuado al tipo de investigación.					X

Datos y firma del juez Experto

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

VALIDACIÓN CON JUICIO DE EXPERTO:

TEMA: Como la implementación de una red privada virtual (VPN) mejora la comunicación de las oficinas externas de la Universidad José Faustino Sánchez Carrión.

OPINIÓN Ó JUICIO DE EXPERTO:

1.- La opinión que UD. Nos brinde es personal, sincera y anónima.

2.- marque con un aspa "X" dentro del cuadrado de valoración, solo una vez por cada criterio, el que UD, Considere su Opinión.

1: Muy Malo
2: Malo
3: Regular
4: Bueno
5: Muy Bueno

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.				X	
Objetividad: Esta expresado en conductas observables.				X	
Actualidad: Adecuado al avance de la ciencia y la tecnología.				X	
Organización: Existe una organización lógica.			X		
Suficiencia: Comprende los aspectos de cantidad y calidad.			X		
Intencionalidad: Adecuado para conocer las opiniones de los encuestados.				X	
Consistencia: Basados en aspectos teóricos científicos de organización.				X	
Coherencia: Establece coherencia entre las variables y los indicadores			X		
Metodología: La estrategia responde a los propósitos del estudio				X	
Pertinencia: El instrumento es adecuado al tipo de investigación.				X	

Datos y firma del juez Experto

CIP 90228

Anexo 3: Tabla de datos

N	Implementación de una red privada virtual (X)														
	Funcionalidad				Seguridad					Confidencialidad				ST1	X
	1	2	S1	D1	3	4	5	S2	D2	6	7	S3	D3		
1	1	2	3	Bajo	2	2	1	5	Bajo	1	2	3	Bajo	11	Bajo
2	2	5	7	Medio	5	5	2	12	Alto	5	1	6	Medio	25	Medio
3	5	5	10	Alto	5	5	5	15	Alto	5	5	10	Alto	35	Alto
4	3	4	7	Medio	2	2	4	8	Medio	4	2	6	Medio	21	Medio
5	1	2	3	Bajo	2	3	1	6	Bajo	1	3	4	Bajo	13	Bajo
6	5	5	10	Alto	5	5	4	14	Alto	4	5	9	Alto	33	Alto
7	3	4	7	Medio	4	4	3	11	Medio	4	2	6	Medio	24	Medio
8	4	3	7	Medio	2	2	4	8	Medio	2	3	5	Medio	20	Medio
9	2	5	7	Medio	5	5	1	11	Medio	5	1	6	Medio	24	Medio
10	3	4	7	Medio	4	4	2	10	Medio	3	3	6	Medio	23	Medio
11	2	5	7	Medio	4	4	4	12	Alto	5	1	6	Medio	25	Medio
12	1	5	6	Medio	5	5	2	12	Alto	5	3	8	Alto	26	Alto
13	4	4	8	Alto	4	4	3	11	Medio	3	3	6	Medio	25	Medio
14	2	2	4	Bajo	2	2	4	8	Medio	2	1	3	Bajo	15	Bajo
15	5	1	6	Medio	3	3	5	11	Medio	3	3	6	Medio	23	Medio
16	4	4	8	Alto	4	4	4	12	Alto	3	3	6	Medio	26	Alto
17	5	5	10	Alto	4	4	5	13	Alto	5	4	9	Alto	32	Alto
18	3	5	8	Alto	3	3	3	9	Medio	1	3	4	Bajo	21	Medio
19	3	3	6	Medio	3	3	5	11	Medio	3	3	6	Medio	23	Medio
20	3	4	7	Medio	4	4	4	12	Alto	4	2	6	Medio	25	Medio
21	1	3	4	Bajo	2	2	1	5	Bajo	1	1	2	Bajo	11	Bajo
22	5	3	8	Alto	3	3	4	10	Medio	5	3	8	Alto	26	Alto
23	3	4	7	Medio	4	4	3	11	Medio	5	2	7	Medio	25	Medio
24	1	1	2	Bajo	2	2	1	5	Bajo	1	1	2	Bajo	9	Bajo
25	5	1	6	Medio	3	3	5	11	Medio	5	2	7	Medio	24	Medio
26	1	2	3	Bajo	2	2	1	5	Bajo	1	1	2	Bajo	10	Bajo
27	2	4	6	Medio	2	2	4	8	Medio	2	4	6	Medio	20	Medio
28	4	5	9	Alto	5	5	5	15	Alto	5	5	10	Alto	34	Alto
29	1	3	4	Bajo	1	4	1	6	Bajo	1	2	3	Bajo	13	Bajo
30	3	4	7	Medio	4	4	4	12	Alto	4	2	6	Medio	25	Medio
31	2	5	7	Medio	5	5	2	12	Alto	5	1	6	Medio	25	Medio
32	5	5	10	Alto	5	5	5	15	Alto	5	5	10	Alto	35	Alto
33	1	5	6	Medio	5	5	1	11	Medio	4	3	7	Medio	24	Medio
34	5	5	10	Alto	5	5	4	14	Alto	4	5	9	Alto	33	Alto
35	3	4	7	Medio	4	4	3	11	Medio	4	2	6	Medio	24	Medio

N	Comunicación (Y)											
	Calidad					Satisfacción					ST2	Y
	8	9	10	S1	D1	11	12	13	S2	D2		
1	2	2	1	5	Bajo	1	4	4	9	Medio	14	Bajo
2	5	5	2	12	Alto	3	2	3	8	Medio	20	Medio
3	5	5	5	15	Alto	4	3	4	11	Medio	26	Alto
4	2	2	4	8	Medio	3	2	4	9	Medio	17	Medio
5	1	1	1	3	Bajo	3	2	3	8	Medio	11	Bajo
6	5	5	4	14	Alto	5	5	5	15	Alto	29	Alto
7	4	4	3	11	Medio	2	2	3	7	Bajo	18	Medio
8	2	2	4	8	Medio	2	3	2	7	Bajo	15	Medio
9	5	5	1	11	Medio	5	3	2	10	Medio	21	Medio
10	4	4	2	10	Medio	2	1	2	5	Bajo	15	Medio
11	4	4	4	12	Alto	3	3	3	9	Medio	21	Medio
12	5	5	2	12	Alto	3	2	3	8	Medio	20	Medio
13	4	4	3	11	Medio	3	2	3	8	Medio	19	Medio
14	2	2	4	8	Medio	1	1	1	3	Bajo	11	Bajo
15	3	3	5	11	Medio	3	2	4	9	Medio	20	Medio
16	4	4	4	12	Alto	3	2	3	8	Medio	20	Medio
17	4	4	5	13	Alto	5	5	5	15	Alto	28	Alto
18	3	3	3	9	Medio	2	2	3	7	Bajo	16	Medio
19	3	3	5	11	Medio	2	3	2	7	Bajo	18	Medio
20	4	4	4	12	Alto	5	3	2	10	Medio	22	Medio
21	3	3	3	9	Medio	2	1	2	5	Bajo	14	Bajo
22	3	3	4	10	Medio	3	3	3	9	Medio	19	Medio
23	4	4	3	11	Medio	3	2	3	8	Medio	19	Medio
24	2	2	4	8	Medio	1	1	1	3	Bajo	11	Bajo
25	3	3	5	11	Medio	3	2	3	8	Medio	19	Medio
26	2	2	1	5	Bajo	1	1	1	3	Bajo	8	Bajo
27	2	2	4	8	Medio	2	3	3	8	Medio	16	Medio
28	5	5	5	15	Alto	5	5	5	15	Alto	30	Alto
29	4	1	4	9	Medio	1	1	2	4	Bajo	13	Bajo
30	4	4	4	12	Alto	1	4	4	9	Medio	21	Medio
31	5	5	2	12	Alto	3	2	3	8	Medio	20	Medio
32	5	5	5	15	Alto	4	3	4	11	Medio	26	Alto
33	5	5	1	11	Medio	3	2	3	8	Medio	19	Medio
34	5	5	4	14	Alto	5	5	5	15	Alto	29	Alto
35	4	4	3	11	Medio	2	2	3	7	Bajo	18	Medio