



---

UNIVERSIDAD CATÓLICA LOS ÁNGELES  
CHIMBOTE

FACULTAD DE INGENIERÍA  
ESCUELA PROFESIONAL DE INGENIERÍA DE  
SISTEMAS

PROPUESTA DE IMPLEMENTACIÓN DE UNA RED  
PRIVADA VIRTUAL SEGURA CORPORATIVA CON  
LINUX EN UNA PLATAFORMA VIRTUALIZADA MIXTA  
PARA LA EMPRESA INFONET SOLUCIONES E.I.R.L -  
SULLANA; 2020.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL  
DE INGENIERO DE SISTEMAS

AUTOR:

JUÁREZ ORTIZ ALBERT IGNACIO

ORCID: 0000-0002-0544-233X

ASESOR:

MORE REAÑO RICARDO EDWIN

ORCID: 0000-0002-6223-4246

PIURA – PERÚ

2020

**EQUIPO DE TRABAJO**

**AUTOR**

**JUÁREZ ORTIZ ALBERT IGNACIO**

ORCID: 0000-0002-0544-233X

Universidad Católica Los Ángeles de Chimbote, Estudiante de Pregrado  
Piura, Perú

**ASESOR**

**MORE REAÑO RICARDO EDWIN**

ORCID: 0000-0002-6223-4246

Universidad Católica Los Ángeles de Chimbote, Facultad de Ingeniería,  
Escuela Profesional de Ingeniería de Sistemas, Piura, Perú

**JURADO**

**SULLÓN CHINGA JENNIFER DENISSE**

ORCID: 0000-0003-4363-0590

**SERNAQUÉ BARRANTES MARLENY**

ORCID: 0000-0002-5483-4997

**GARCÍA CÓRDOVA EDY JAVIER**

ORCID: 0000-0001-5644-4776

**HOJA DE FIRMA DEL JURADO Y ASESOR**

MGTR. JENNIFER DENISSE SULLÓN CHINGA

PRESIDENTE

MGTR. MARLENY SERNAQUÉ BARRANTES

MIEMBRO

MGTR. EDY JAVIER GARCÍA CÓRDOVA

MIEMBRO

MGTR. RICARDO EDWIN MORE REAÑO

ASESOR

## **DEDICATORIA**

Dedico toda mi investigación a mi ángel, mi Madre Aura Estela Ortiz que desde el cielo me guio y protegió para dedicarme a mis estudios y ahora plasmados en esta investigación. A mi padre Segundo Juárez Rivas que desde el cielo me guía y fortalece; a mis tíos: Carmen y Andrés que son mis protectores y consejeros para lograr lo que me propuse hace 05 años. Finalmente dedicarles esto a aquellas personas que siempre confiaron en mí y estuvieron a mi lado apoyándome en todo momento.

*Albert Ignacio Juárez Ortiz*

## **AGRADECIMIENTO**

Un agradecimiento enorme a mí asesor de este proyecto de investigación el Ing. Ricardo More Reaño parte del equipo y miembro de jurado de la universidad católica los ángeles de Chimbote, a todas las comunidades de software libre, a los proyectos de Linux en el mundo, las distribuciones lideradas por investigadores de software libre en el mundo, en Piura, en el Perú; a las comunidades de seguridad de VPN. donde me ha valido muchísimo para sacar gran parte de información necesaria y así comparar cosas, proyectos en paralelo, gracias a estas organizaciones para poder realizar toda mi investigación, si el software libre no hubiera llegado tan lejos como lo tenemos hoy en día nada de esto hubiera sido logrado.

*Albert Ignacio Juárez Ortiz*

## RESUMEN

La presente investigación es desarrollada bajo la línea de investigación Redes TIC, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; tuvo como objetivo Proponer la implementación de una Red Privada Virtual Segura Corporativa con Linux En Una Plataforma Virtualizada Mixta en la Empresa Infonet Soluciones E.I.R.L – Sullana 2020. El tipo de la investigación fue cuantitativa, nivel descriptivo, diseño no experimental y de corte transversal.; con una muestra de 5 personas; obteniendo como resultado en la dimensión: Nivel de Acceso a la Información se obtuvo que el 80% de los trabajadores expresaron que NO tienen ninguna facilidad en el acceso de la información. En la siguiente dimensión: Nivel de Seguridad de Red se obtuvo que el 60% de los encuestados expresaron que SI hay un nivel de seguridad en la red de la empresa. En la dimensión: Nivel de Diseño de Red Privada Virtual, se alcanzó que el 80% de los encuestados expresaron que SI es necesario el nivel de Diseño de Red Privada Virtual; observando los resultados, que llegan a tener una similitud con la hipótesis planteada de la investigación.

**Palabras claves:** Plataforma, Red, Virtualizada.

## **ABSTRACT**

The following research was developed in accordance with TIC Networks from the Professional School of Systems Engineering of Los Angeles of Chimbote Catholic University. The objective of the research was to design a private secure virtual network using Linux in a mixed, virtualized platform for the company Infonet Solutions E.I.R.L. in Sullana in 2020. Research was quantified using a descriptive type design using non-experimental, cross-sectional research, and working with a sample size of 5 people. The result from the study Level of Access Information was that 80% of employees expressed that they were unable to access information easily. Next, in sample Level of Network Security, results showed that 60% of employees expressed that the company's network operates with an optimal level of security. Finally, in the last study, Level of Virtual Private Network Design, results showed that 80% of employees expressed that the level of Virtual Private Network is necessary. According to these responses, it is my conclusion that the results coincide with the proposed hypothesis.

**Keywords:** Network, Platform, Virtual.

## ÍNDICE DE CONTENIDOS

EQUIPO DE TRABAJO .....	ii
HOJA DE FIRMA DEL JURADO Y ASESOR .....	iii
DEDICATORIA .....	iv
AGRADECIMIENTO .....	v
RESUMEN .....	vi
ABSTRACT.....	vii
ÍNDICE DE CONTENIDOS .....	viii
ÍNDICE DE GRÁFICOS.....	xi
ÍNDICE DE TABLAS .....	xiii
I. INTRODUCCIÓN.....	1
II. REVISIÓN DE LA LITERATURA.....	3
2.1 Antecedentes .....	3
2.1.1 Antecedentes a nivel internacional .....	3
2.1.2 Antecedentes a nivel nacional.....	5
2.1.3 Antecedentes a nivel regional .....	7
2.2 Bases Teóricas.....	9
2.2.1 Consultoría.....	9
2.2.2 Información de la empresa “Infonet Soluciones E.I.R.L” .....	9
2.2.3 Plataforma virtual.....	13
2.2.4 Seguridad informática.....	13
2.2.5 Red .....	14
2.2.6 Redes privadas virtuales.....	16
2.2.7 Transmisión de datos .....	21
2.2.8 Redes en ordenadores.....	21

2.2.9	Clasificación de redes .....	22
2.2.10	Componentes de redes en ordenadores .....	24
2.2.11	Tipos de VPN.....	29
III.	HIPÓTESIS .....	33
IV.	METODOLOGÍA.....	34
4.1	Diseño de la investigación .....	34
4.2	Población y muestra.....	35
4.3	Definición y operacionalización de variables e indicadores.....	36
4.4	Técnicas e instrumentos de recolección de datos.....	38
4.5	Plan de análisis.....	38
4.6	Matriz de consistencia.....	39
4.7	Principios éticos .....	41
V.	RESULTADOS .....	42
5.1	Resultados .....	42
5.1.1	Dimensión 01: Nivel de acceso a la información .....	42
5.1.2	Dimensión 02: Nivel de seguridad de red.....	49
5.1.3	Dimensión 03: Nivel de diseño de red privada virtual.....	56
5.2	Análisis de resultados.....	65
5.3	Propuesta de mejora.....	67
VI.	CONCLUSIONES.....	110
	RECOMENDACIONES.....	112
	REFERENCIAS BIBLIOGRÁFICAS .....	113
	ANEXOS .....	119
	ANEXO I: CRONOGRAMA DE ACTIVIDADES .....	120
	ANEXO II: PRESUPUESTO .....	121
	ANEXO III: CUESTIONARIO.....	122

ANEXO IV: PROTOCOLO DE CONSENTIMIENTO INFORMADO .....	125
ANEXO V: FICHA DE VALIDACIÓN PARA JUECES EXPERTOS .....	126
ANEXO VI: SOLICITUD DE IMPLEMENTACIÓN DEL PROYECTO DE TESIS.....	129

## ÍNDICE DE GRÁFICOS

Gráfico N° 1: Organigrama de la Empresa.....	11
Gráfico N° 2: Resultado de la Dimensión 01 Nivel de Acceso a la Información.....	48
Gráfico N° 3: Resultado de la Dimensión 02 Nivel de Seguridad de Red .....	55
Gráfico N° 4: Resultado de la Dimensión 03 Nivel de Diseño de Red Privada Virtual .....	62
Gráfico N° 5: Resumen general de dimensiones .....	64
Gráfico N° 6: Escenario VPN.....	68
Gráfico N° 7: Captura copia de script de configuración.....	71
Gráfico N° 8: Exportar variables .....	74
Gráfico N° 9: Creación de certificado y clave privada.....	75
Gráfico N° 10: Generar certificados y clave del servidor.....	77
Gráfico N° 11: Generar certificados y las claves de usuarios.....	78
Gráfico N° 12: Generación de clave de seguridad.....	79
Gráfico N° 13: Configuración dnsmasq.....	82
Gráfico N° 14: Enrutamiento de peticiones .....	89
Gráfico N° 15: Accediendo al router .....	90
Gráfico N° 16: Configurando router .....	90
Gráfico N° 17: Selección de componentes de instalación .....	92
Gráfico N° 18: Copiar claves de usuario .....	94
Gráfico N° 19: Ejecutar el programa OpenVPN .....	95
Gráfico N° 20: Ingresar Usuario.....	96
Gráfico N° 21: Máquina Virtual .....	97
Gráfico N° 22: Fondo de Máquina Virtual .....	97
Gráfico N° 23: Comienzo de Instalación.....	98
Gráfico N° 24: Unidad de Instalación.....	98
Gráfico N° 25: Elección del S.O.....	99
Gráfico N° 26: Ubicación del Primer Servidor.....	99
Gráfico N° 27: Tamaño del Disco .....	100
Gráfico N° 28: Verificación de Información .....	100
Gráfico N° 29: Inicio del Primer Servidor.....	101

Gráfico N° 30: Tamaño de la Ram .....	101
Gráfico N° 31: Configuración Terminada del Primer Servidor.....	102
Gráfico N° 32: Instalación de Segundo Servidor.....	102
Gráfico N° 33: Ubicación del Segundo Servidor.....	103
Gráfico N° 34: Inicio del Segundo Servidor.....	103

## ÍNDICE DE TABLAS

Tabla N° 1: Hardware .....	12
Tabla N° 2: Software .....	12
Tabla N° 3: Definición Operacional .....	36
Tabla N° 4: Matriz de Consistencia.....	39
Tabla N° 5: Disponibilidad de Información .....	42
Tabla N° 6: Eficacia en el servicio .....	43
Tabla N° 7: Medio físico .....	44
Tabla N° 8: Velocidad de transmisión de datos.....	45
Tabla N° 9: Compartir archivos.....	46
Tabla N° 10: Dimensión Nivel de Acceso a la Información .....	47
Tabla N° 11: Medidas de Seguridad .....	49
Tabla N° 12: Autenticación de usuarios .....	50
Tabla N° 13: Privilegios de los usuarios.....	51
Tabla N° 14: Políticas de Seguridad.....	52
Tabla N° 15: Detección de Software Malicioso .....	53
Tabla N° 16: Dimensión Nivel de Seguridad de Red .....	54
Tabla N° 17: Diseño de Red Privada.....	56
Tabla N° 18: Simplificación del Trabajo.....	57
Tabla N° 19: Beneficios a los Trabajadores .....	58
Tabla N° 20: Acceso a la Información.....	59
Tabla N° 21: Privacidad de Información .....	60
Tabla N° 22: Dimensión Nivel de Diseño de Red Privada Virtual .....	61
Tabla N° 23: Resumen de Dimensiones .....	63

## I. INTRODUCCIÓN

Según Marques (1) en su libro titulado Redes Privadas Virtuales SSL, algunos de los aspectos importantes que tenemos que tener en cuenta a la hora de elegir una solución VPN apropiada para nuestras necesidades es el impacto que esta va a tener en los usuarios finales de la red y los recursos y esfuerzo que nos va a costar implementarla y mantenerla. Los clientes remotos que quieran conectarse no necesitan instalar manualmente ningún tipo de software, esto se debe a que los VPN SSL funcionan a través del navegador web, que por norma general, todos los equipos de los usuarios lo tienen ya instalado y dichos usuarios ya saben usarlo.

La presente investigación es desarrollada bajo la línea de investigación Redes TIC. La investigación se realizó en la Empresa Infonet Soluciones E.I.R.L - Sullana; cuyas operaciones se ven afectadas por la forma como se manejan actualmente; De qué manera la propuesta de implementación de una red privada virtual segura corporativa con Linux en una Plataforma Virtualizada Mixta en la empresa Infonet Soluciones E.I.R.L. Sullana, optimiza la transmisión de la información?

La investigación tuvo como objetivo La Propuesta de Implementación de una Red Privada Virtual Segura Corporativa con Linux En Una Plataforma Virtualizada Mixta en la Empresa Infonet Soluciones E.I.R.L – Sullana, para optimizar la transmisión de la información.

El trabajo se justifica económicamente por lo que sustenta que todo el argumento de implementación se expondrá en una plataforma virtual, introduciendo S.O figoneros como; Windows 7/8/10 y sistemas operativos huéspedes como; GNU Linux Centos 7.4. Se expondrá a un ahorramiento de los gatos en cuanto a los recursos utilizados de manera manual y didáctica, por lo cual se expondrá en una precisión regular de datos en tiempo real.

La justificación tecnológica, se ven en sectores factibles por los crackers (infractor informático), por lo cual se consideró la implementación de Redes Privadas Virtuales en las organizaciones, la cual aumenta de manera óptima las redes empresariales, el traslado de información entre sí, van cifrados. La justificación de la investigación se llega fundamentar en que las organizaciones de hoy, estas instituciones deben hacerse cargo de la utilización eficaz de toda la información en las redes de computadoras, eludiendo la medición que estos puedan ser manipulados, por los infractores informáticos.

## II. REVISIÓN DE LA LITERATURA

### 2.1 Antecedentes

#### 2.1.1 Antecedentes a nivel internacional

En el 2020 Niño (2), en su investigación titulada “Diseño de un Modelo de Virtualización de un Sistema de Servidores en Alta Disponibilidad”, nos explica que el modelo de la Computación en la Nube para la prestación de servicios y tecnología cambia la forma tradicional con la que se entregan habitualmente y, aunque este concepto no es nuevo, su interés en Colombia ha crecido en los últimos 15 años, atrayendo cada vez más la atención de las comunidades académicas y de las tecnologías de información y comunicación (TIC). Las empresas empiezan a migrar sus procesos hacia la red, y gran ejemplo de esto es la posibilidad de que trabajar desde cualquier lugar (Teleworker) teniendo acceso a un computador con internet, y así poder acceder a la plataforma de la empresa, contando con acceso a bases de datos, herramientas de oficina, aplicativos, correo, etc. Las organizaciones ya sean públicas, privadas o pymes, las tecnologías empleadas o adquiridas suelen ser anticuadas u obsoletas, y no están aprovechando la tecnología del Cloud Computing y/o virtualización, ya que no se analiza a profundidad la selección de dicha tecnología.

Ramírez y Penagos (3), en el año 2018 en su tesis titulada “Diseño de una Red Privada Virtual (VPN) con Seguridad L2PT para la Empresa Laboratorios ExpoFarma S.A” argumenta que las empresas hoy en día buscan mayor conectividad a sus recursos desde fuera de la red, pero esto implica riesgos de seguridad para la información es por esto que

se desarrollaron tecnologías como lo son VPN (red virtual privada) que permite a los empleados conectarse desde redes externas con credenciales que brindan los permisos de tráfico de información por medio de un túnel sin riesgo de pérdida de información y o filtraciones de externos, reduciendo costos de infraestructura debido a que las personas pueden trabajar desde sus casas.

Para Romero y Romero (4), en su tesis “Fronteras de Seguridad en Redes Privadas Virtuales (VPN)” realizada el año 2016, hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de email, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa. A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad. Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services (RAS), este tipo de usuarios se tenían una insatisfacción del 79% con respecto al acceso de la información. Fue entonces cuando surgieron las VPN que permitieron conectar distintas sedes a través de internet, recortando costos y quitándole relevancia a la distancia entre los puntos geográficos de las sedes o usuario; todo esto a través de una conexión virtual cifrada.

### 2.1.2 Antecedentes a nivel nacional

Martel (5), en su tesis titulada “Diseño de una Red de Comunicación VPN sobre Internet para un Distribuidor Autorizado de Claro basado en el RFC 2764” realizada en el año 2019, propone cambios en la forma en que los individuos y distintos segmentos de la sociedad trabajan, se comunican e interactúan. Es así que las tecnologías de la información y comunicación (TIC), como Internet a través de las redes de datos, cobran un papel muy importante convirtiéndose en un medio global de comunicación de uso cotidiano en nuestras vidas, llegando a ser su uso una necesidad básica comparada al uso de la electricidad. Las redes privadas virtuales (VPN) cumplen con estas características mediante la conexión de redes locales (LAN) y usuarios que se encuentran en distintas ubicaciones geográficas mediante un túnel que se construye sobre Internet o cualquier red pública, permitiéndoles trabajar desde distintas ubicaciones usando infraestructura provista por una red pública como lo es Internet. Entre sus principales características y tal como su nombre lo indica las redes privadas virtuales son: “privadas” porque establecen comunicación única y exclusivamente entre el emisor y el receptor previamente definidos, y “virtuales” pues la comunicación directa entre el emisor y receptor no es por medio de una conexión física punto a punto o de extremo a extremo como se podría realizar con un cable o cualquier otro medio físico, sino más bien la comunicación es realizada a través de Internet donde se sabe que las comunicaciones recorren diversos caminos para llegar a su destino.

En el 2018 Espinoza (6), en su investigación “Propuesta de una Red Virtual para Mejorar el Servicio de Comunicación en las Tiendas MASS para la Empresa de Supermercados Peruanos S.A” presentan una propuesta de implementación de una Red Privada Virtual, cuyo objetivo principal es mejorar la comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A. Esto conlleva a múltiples

objetivos específicos, tales como mejorar el tiempo de latencia del Servicio de Comunicación, disminuir los incidentes por lentitud o intermitencia de la Red, proporcionar a la Red de datos escalabilidad, disminuir costos por el Servicio de Comunicación. La mejora del Servicio de Comunicación en las tiendas Mass se podrá constatar en el enlace virtual para enlazar dos o más sucursales geográficamente distanciadas.

Para Atencio y Mamani (7), en su proyecto de investigación titulado “Diseño e Implementación de un prototipo de Red Privada Virtual en Capa 3 Utilizando Cisco IOS para la Universidad Nacional del Altiplano”; realizada en el año 2017, nos detalla hoy en día con el avance exponencial de la tecnología de sistemas de información en las instituciones, las redes se vuelven más vulnerables ya que no cuentan con protocolos de seguridad o la seguridad implementada es básica. Además de ello, otro problema que se puede apreciar es la falta de interés por solucionar este tema, ya sea por desconocimiento o por falta de personal calificado para realizar estas labores. Actualmente son muy pocas las empresas que identifican este problema como grave y deciden implementar protocolos de seguridad en su red. La presente investigación tuvo como objetivo principal el realizar un diseño y posterior implementación de un prototipo de Red Privada Virtual que permita asegurar y encriptar la información compartida entre las oficinas pertenecientes a la Universidad Nacional del Altiplano. De la misma forma se definieron como objetivos específicos, diseñar el prototipo de la Red Privada Virtual para operar y controlar el tráfico en LAN y WAN e implementar la Red Privada Virtual en el Laboratorio de Cisco de la Universidad Nacional del Altiplano.

### 2.1.3 Antecedentes a nivel regional

Zavala (8), en su tesis titulada “Reingeniería de la Infraestructura de la Red de Datos Administrada Con Windows Server en Consorcio Supervisor Educa – Piura, 2020” realiza una propuesta de reingeniería teniendo en cuenta que las red de datos e Internet que proporcionan una comunicación continua entre personas, además de una gran variedad de servicios e información que pueden ser manejados a través de un único dispositivo. las empresas que tienen una gran capacidad de beneficiarse de la tecnología son organizaciones que, antes de añadir un componente tecnológico, describen detalladamente cuál será la repercusión para su empresa; en este caso una institución privada. Así pues, el objetivo debe ser que toda decisión relativa a la tecnología ayude a mejorar la productividad de la empresa, la organización o de uno mismo. En efecto, la manera en que se gestiona la materialización, operación y continuidad de los servicios tecnológicos requeridos por la organización ya no son una ventaja competitiva, sino un factor que, al no estar alineado a las necesidades de la empresa, constituirá una desventaja competitiva relevante. Es una forma de plantear una solución a los problemas, para mejorar el actual sistema de conectividad de dicha empresa, permitir a los trabajadores tener acceso de manera permanente en toda su área trabajo, evitando así cualquier interrupción en el largo proceso que conllevan los trabajos para los cuales han sido contratados, principales activos de una institución.

Castillo (9), en su investigación “Propuesta de Reingeniería de una Red de Datos para la Municipalidad Distrital de Salitral”, en el año 2018, la cual consiste en las fundamentales e importantes en las empresas, ya que gracias a su funcionamiento les permiten logran sus objetivos y poder estar al nivel de la competencia. Además, permiten crear protocolos de seguridad en cual garantice la integridad de la información y brindándole la confianza de realizarse libremente sin

preocuparse de amenazas o ataques que puedan realizar los trabajadores o terceros. Los problemas como la pérdida de conectividad, comunicación y la antigüedad de la red de datos, en el cual nace la necesidad de proponer una reingeniería de la red de datos para la municipalidad de Salitral, para mejorar la comunicación y obtener una mayor seguridad en su administración y transferencia de datos, es por ello que se debe adoptar nuevas estrategias de seguridad apoyadas con las nuevas tecnologías al fin de conseguir un mejor funcionamiento y los procesos que sean transferidos confiablemente.

En el año 2017 Criollo (10), en su investigación propone un “Diseño para la Implementación de una Red Privada Virtual (VPN) en la empresa Agromar Industrial S.A.” Estamos ante una sociedad tan digitalizada que la vorágine de la tecnología está que abarca todos los ámbitos de nuestras vidas, no hay espacio donde no tenga cavidad la tecnología y uno de los tantos ámbitos que abarcan las tecnologías de información y comunicación (TIC) son las redes donde actualmente están de moda y que al combinarlas obtenemos mayor beneficio a menor costo y mayor eficiencia. Tanto como un objeto en común, como las organizaciones estatales y privadas están muy vinculadas a esta tecnología y las han incluido en sus procesos diarios porque de tal manera agilizan su información y amplían su cobertura entre las diferentes áreas. cuando una organización implementa una red de datos sin toman en cuenta un escalamiento a futuro o un crecimiento organizacional, peor aun cuando se maneja mucha información de carácter privado donde se tenga que compartir entre demás sucursales, pues surge un gran problema que muchas empresas tienen que afrontar.

## 2.2 Bases Teóricas

### 2.2.1 Consultoría

#### **Definición**

Esta base parte de un servicio de asesoramiento buscados por las organizaciones pequeñas y multinacionales, ya que estos cuentan con personas capacitadas y calificadas para prestar asistencia de todo tipo, de manera independiente, a la organización para poner en déficit los problemas en general de la organización (marketing, jurídica, etc) llegando así a reforzar las debilidades de la organización (11).

### 2.2.2 Información de la empresa “Infonet Soluciones E.I.R.L”

#### **Reseña histórica**

Infonet Soluciones EIRL es una empresa que da consultoría de seguridad informática, implementación y configuraciones de servidores, asesorías, charlas. Contamos con más de 10 años de experiencia. Somos especializados, contamos con muchos años de experiencia, nuestros clientes nos respaldan.

#### **Ubicación**

Av. José de Lama Sullana 149 – Sullana – Piura.

## **Misión, visión, organigrama**

### **Misión**

Nuestra misión es concientizar y securizar a las empresas a mejorar sus servidores, aplicaciones web, Sistemas, con asesorías y Análisis Pen test, Hacking Ético, mejorando su infraestructura, evitar filtraciones de datos, documentos y alteración de dicho. Dándole una mejor solución en Seguridad para las empresas.

### **Visión**

Alcanzar y prevenir múltiples ataques que perjudiquen a las empresas. La prevención es el arma para un Hackeo y que cada día sea un reto más en proteger la seguridad de la empresa. Que nuestros clientes queden satisfechos, por contactar a Infonet Soluciones.

## Organigrama

Gráfico N° 1: Organigrama de la Empresa



Fuente: Elaboración Propia

## Infraestructura Tecnológica

Esta parte debemos de tener en cuenta, ya que depende el manejo de una infraestructura informática o tecnológica, puede ser una organización. En informática comprendemos la infraestructura como una agrupación de estructuras de ingeniería, del cual tienen una larga vida útil y que componen la base que realizan el servicio de un beneficio (12).

## Hardware

El hardware comprende todo arquetipo de elemento físico tecnológico que llega a tener la organización para la conjugación de la red privada virtual, etc (13).

Tabla N° 1: Hardware

Equipo	Especificaciones
Laptop	Hp core i5, procesador de 64 bits, disco duro (Cap. 1TB).
Mouse	Inalámbrico Micronics.
Cableado	Cable UTP cat 5E.
Conectores	Rj45.

Fuente: elaboración propia

### **Software**

Es la equipación o apoyo lógico de un sistema, llega a constituirlo un grupo de elementos lógicos, no tangibles y no físicos, indispensables para llevar a cabo una ocupación específica. Definimos software como el grupo de programas de informáticos, procedimientos, documentación e información asociadas (14).

Tabla N° 2: Software

Equipo	Especificaciones
Sistema Operativo	Windows 10.
Antivirus	Security Nod 32.
Ofimática	Adobe reader, office.

Fuente: elaboración propia

### 2.2.3 Plataforma virtual

Se trabaja en la Plataforma Virtual. Dicha plataforma es un Learning Management System (LMS) basado en Moodle. Moodle es uno de los LMS más utilizados a nivel internacional. Actualmente se emplea como campus virtual en 239 países con más de 87.000 sitios registrados. España es el segundo país del mundo en la utilización de esta plataforma con más de 7.500 sitios registrados. Los criterios utilizados por la Universidad de Burgos SDUD HOHJLU 0RRGOH FRPR &DPSXV 9LUWXDO IXHURQ VX ÀH [LELOLGDG GLGiFWLFD \ WHF -nológica y su facilidad de utilización. Con relación a la primera característica se ha considerado la base pedagógica subyacente centrada en el aprendizaje constructivista. Desde este enfoque se entiende el aprendizaje como un proceso interactivo que se desarrolla cuando se comparte información. \$VLPLVPR HO VLVWHPD PRGXODU GH 0RRGOH SHUPLWH OD FRQJXUDFLyQ SURJUHVLyD de Virtual en función de las necesidades detectadas (15).

### 2.2.4 Seguridad informática

La seguridad informática lleva asociada un conjunto de términos, en muchos casos nuevos términos en inglés, que hacen difícil la tarea de estar al día en materia de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información (16).

## **Confidencialidad**

Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y sólo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una interceptación de éste y que pueda ser leído por una persona no autorizada. Los conceptos confidencialidad, integridad o disponibilidad son muy comunes en el ámbito de la seguridad y aparecen como fundamentales en toda arquitectura de seguridad de la información, ya sea en el ámbito de la protección de datos, normativa vigente relacionada con la protección de datos de carácter personal, como de códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de prestigiosas certificaciones internacionales (16).

### **2.2.5 Red**

Una red de ordenadores se puede definir de varias formas. Un enfoque es considerar que la red es simplemente la «red física». Se puede decir que la red física se compone de todos los nodos de conmutación internos, sus enlaces de interconexión y los enlaces que conducen a los dispositivos conectados externamente (17).

#### **Esquema de red**

Las recomendaciones de la UIT-T J.112 (DOCSIS 1.1) y J.122 (DOCSIS 2.0) se desarrollan en el contexto de los sistemas HFC para su uso global. La Recomendación, “Sistema de transmisión para servicios interactivos

de televisión por cable”, amplía el alcance de la UIT-T J.83, “Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable”, para tener en cuenta la transmisión de datos bidireccionales por cables coaxiales y cables híbridos de fibra óptica / coaxiales en servicios interactivos (18).

## **Tipos**

### **Red de transporte**

La red de transporte es la red, que desde un punto central, lleva las señales a las cabeceras remotas, que forman parte del tramo de red troncal, más próximo a los usuarios finales. La finalidad de esta red es la misma que la de cualquier red de transporte y, por esta razón, el transporte se suele hacer con medios digitales, tales como la fibra óptica, los radioenlaces de microondas e, incluso, los cables coaxiales sobre los que se montan tecnologías de transmisión tradicionales (18).

### **Red de transporte**

La red troncal es la mayor beneficiada de la introducción de la fibra en las redes de cable, para conformar las redes HFC. La fibra óptica, junto con láseres de suficiente linealidad como para garantizar la correcta transmisión de los canales AM-VSB, ha permitido aumentar las distancias cubiertas hasta los 100 km sin repetición, haciendo que el tamaño de las redes de distribución se reduzca, disminuyendo así los problemas de calidad en estas redes. Asimismo, se ha hecho posible, y siempre más sencilla, la transmisión bidireccional en este tipo de redes, cuyas contribuciones de ruido de los diferentes usuarios en sentido ascendente en una red coaxial pura, harían imposible la comunicación salvo en redes de muy pequeño tamaño (18).

### 2.2.6 Redes privadas virtuales

En todo el bum de la tecnología, hubo una partición entre una red pública y privada (19). La pública es una cadena de distintos lugares sin ningún enlace que se interactúa los datos libremente entre sí. La multitud que ingresa a esta red puede o no tener una conexión o tener algo similar y una sola persona dentro de esa red, puede que solo interactúe con una diminuta división de los usuarios. La privada se dispone de distintos ordenadores que competen a una organización y que interconectan datos específicos entre sí; ellos se encuentran con la certeza que son exclusivos en emplear los recursos de esta red y lo que se distribuye en ella.

#### **Red de computadoras**

Es un grupo equipos (computadoras y dispositivos), interconectados mediante cables, señales, ondas o cualquier otro procedimiento del traslado de información, para dividir información, recursos y servicios (acceso a una base de datos, internet, chat, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo (20).

#### **Modelo OSI**

Es un modelo conceptual que no define ni específicas interfaces y protocolos, únicamente establece criterios generales sobre cómo concebir las redes de comunicaciones de datos.

El proceso de transmisión de datos, intervienen componentes software y hardware. Debido a ello, los procedimientos se dividen en capas o niveles.

En el modelo OSI se consideran siete niveles, en cada uno de ellos se procesan unidades de información denominadas PDU (Unidad de datos de protocolo). En los ordenadores emisores las PDU se transmiten del nivel superior al inferior, y en cada uno de ellos se añade información de control (cabeceras, AH, PH, SH, TH, NH, DH, o terminales DT). En los Ordenadores receptores la información se procesa desde el nivel inferior, comprobando y eliminando en cada nivel las cabeceras o terminales de cada PDU correspondiente a dicho nivel (21).

### **CAPA 1. Capa Física**

Es donde se especifican los parámetros mecánicos (grosor de los cables, tipo de conectores), eléctricos (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, infrarojos, Wifi, fibra óptica), si el emisor envía un 0 al receptor debe de llegar un 0 (21).

Existen diferentes formas de ampliar una red aislada o interconectar redes individuales, con dispositivos de interconexión de redes y son:

- Repetidor (Repeater) : Capa física del modelo OSI
- Concentrador (Hub) : Capa física del modelo OSI
- Puente (Bridge): Capa física y de enlace de datos capa 2 del modelo OSI.
- Conmutador (switch): Actúan como filtros en la Capa de enlace de datos (Capa 2) del Modelo OSI.
- Router: Capa 3 del Modelo OSI (Físico, enlace de datos y red).
- Pasarela (Gateway): Niveles de transporte, sesión, presentación y aplicación del modelo OSI.

## **CAPA 2. Capa de enlace de datos**

Esta capa llega a suministrar el tráfico de datos verídico a través de un enlace físico. Al hacerlo, la capa de enlace de datos emplea el direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio (22)

### **CAPA 3. Capa de la Red**

La capa de red es una capa laberíntica que promedia conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Si queremos recordar la Capa 3 debemos pensar definitivamente en la selección de ruta, direccionamiento y enrutamiento (22).

### **CAPA 4. Capa de Transporte**

Esta se divide la información original del host emisor y los acopla a una corriente de información dentro del sistema del host receptor. El fin de la capa de transporte y la de sesión puede figurar como el término entre los protocolos de aplicación y los flujos de datos. Por lo tanto todas las capas de aplicación, presentación y sesión están referidas con temas de aplicaciones, las 4 capas interiores se sujetan a la movilidad de información. La capa de transporte intenta surtir una utilidad de transporte de información que aparta las capas superiores de los fragmentos de implementación del traslado. Al tener la utilidad de intercomunicación, se establece, mantiene y culminan apropiadamente los circuitos virtuales. Al proporcionar una utilidad verídica, se emplean dispositivos de detección y recuperación de errores de transporte (22).

### **CAPA 5. Capa de sesión**

La capa de sesión llega a establecer, suministrar y finalizar las sesiones entre 2 hosts que se están en interacción; la sesión facilita sus servicios

a la capa de presentación. Así mismo coincide el diálogo entre las capas de presentación de los 2 hosts y suministra el intercambio de información. Además de controlar la sesión, la capa consagra disposiciones para una óptima transferencia de información, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación (22).

### **CAPA 6. Capa de Presentación**

En esta capa se llega a resaltar la codificación y conversión de información de la capa de aplicación para asegurar que la información del dispositivo de origen puedan ser interpretados por la aplicación óptima en el dispositivo de destino; dentro de ello la compresión de los datos da forma a que puedan ser descomprimidos por el dispositivo de destino, llevando de esa manera a una encriptación de la información para transmisión y descifre para cuando sean recibidos en el destino (23).

### **CAPA 7. Capa de Aplicación**

Esta llega a proporcionar el diseño y la utilidad que dan soporte a las aplicaciones; esta se confía en dar acceso general a la red. Esta etapa llega a suministrar las herramientas que el usuario visualiza. Presenta servicios de red vinculados con estas aplicaciones de usuario, como la administración de la misiva y la transferencia de archivos (23).

### 2.2.7 Transmisión de datos

#### Transmisión paralela

Los datos binarios, formados por unos y ceros, se agrupan formando palabras. En la transmisión paralela se envían simultáneamente los  $n$  bits que forman una palabra. Para ello se emplea un solo cable por cada bit de la palabra. El valor típico de bits para la transmisión en paralelo es de 8 bits. Este tipo de transmisión aporta en principio más velocidad, ya que se pueden transmitir varios bits simultáneamente. La principal desventaja es el coste, por tanto, se utiliza solo para distancias cortas (24).

#### Transmisión en serie

Los datos binarios se envían bit a bit, uno detrás de otro, por un solo canal de comunicaciones. La ventaja de este tipo de comunicación es su bajo coste respecto a la transmisión paralela. Normalmente, los equipos de emisión y recepción trabajan con la información en paralelo, por lo que se necesitarán conversores paralelo-serie y serie-paralelo (24).

### 2.2.8 Redes en ordenadores

Cuando se usa el término «red de ordenadores», la interpretación común es que se está hablando de una red en la cual los ETDs son ordenadores. Pero en casi cualquier red actual los nodos, si no son ordenadores, están controlados en gran parte por ordenadores. Para los propósitos de este libro, consideraremos a estos conmutadores basados en ordenador como un asunto de discusión tan importante como los ETDs conectados a la red. Además, la mayor parte de los servicios ofrecidos «en» la red, esto es, prestados por la administración que explota la red física, están

basados también en ordenadores. Estos servicios basados en ordenador pueden realizarse en los nodos mediante software, o también prestarse en ordenadores conectados a ella, que son como ETDs en todos los aspectos, excepto en que es el administrador de la red física, y no un abonado, quien los posee y controla (17).

#### 2.2.9 Clasificación de redes

##### **Alcance:**

- Red de área amplia (WAN), red de área personal (PAN), red de área local (LAN), red de área metropolitana (MAN), Red de área simple (SPL), Red de área de almacenamiento (SAN), red de área de campus (CAN).

##### **Método de la Conexión:**

- Medios guiados: Cable coaxial, cable de par trenzado, Fibra óptica y otros tipos de cables.
- Medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas.

##### **Relación Funcional**

- Cliente-servidor / Igual-a-Igual (P2p)

## **Topología de red**

- Red en estrella, red en bus, red en anillo (o doble anillo), red en malla (o totalmente conexas), red en árbol, red mixta.

## **Direccionalidad de los Datos (Tipos de transmisión)**

- Simplex (unidireccionales): un Equipo Terminal de Datos transmite y otro recibe. (p. ej. Streaming).
- Half-Duplex (bidireccionales): sólo un equipo transmite a la vez. También se llama Semi-Duplex (p. ej. Una comunicación por equipos de radio, si los equipos no son full dúplex, uno no podría transmitir (hablar) si la otra persona está también transmitiendo (hablando) porque su equipo estaría recibiendo (escuchando) en ese momento).

## **Protocolo de Redes**

El Protocolo de red o también protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de Datos u órdenes durante la Comunicación entre las entidades que forman parte de una red.

## **Estándares**

Crear un estándar es crear compatibilidad, intercambiabilidad entre componentes, así como establecer criterios técnicos y sociales que permitan la integración de cada una de las partes dentro de un sistema tecnológico. Implica cuantificar, codificar, acumular y transmitir esa información. El proceso de estandarización es fundamentalmente un proceso de transferencia de información material y organizacional al

interior de dispositivos técnicos, convenciones o reglas y sistemas de información. Un estándar establece la referencia, la cualidad mínima sobre todo las normas que permiten que un componente sea compatible o actúe adecuadamente como interface dentro de una red (25).

#### 2.2.10 Componentes de redes en ordenadores

##### **El Ordenador**

Un ordenador, también denominado como computadora, es una máquina electrónica que llega a recibir datos con la misión procesarlos y transformarlos en información útil. Se encuentra compuesto por una serie de circuitos integrados y otros tantos elementos relacionados que son los que permiten la ejecución de una variedad de secuencias o rutinas de instrucciones que indicará el usuario del mismo (25).

##### **Tarjetas de Red**

A las tarjetas de red también se les llama adaptadores de red o NIC (Network Interface Card, tarjeta de interfaz de red). Hay diversos tipos de tarjetas de red, en función del tipo de cable o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, fibra de vidrio, etc.), pero hoy día el más utilizado es del tipo Ethernet con un conector RJ-45. Asimismo, está cada vez más extendido el uso de redes Wi-Fi. Actualmente, la mayoría de las placas base ya tienen integrada una tarjeta de red con conector RJ-45 (26).

## **Tipos de Sitios de Trabajo**

Hay muchos tipos de sitios de trabajo que se pueden incorporar en una red particular, algo de la cual tiene exhibiciones high-end, sistemas con varios CPU, las grandes cantidades de RAM, las grandes cantidades de espacio de almacenamiento en Disco duro, u otros componentes requeridos para las tareas de proceso de datos especiales, los gráficos, u otros usos intensivos del recurso (25).

## **Tipos de Servidores**

Los servidores operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por tanto, el servidor realiza otras tareas para beneficio de los clientes. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando. En el contexto de redes Internet Protocol (IP), un servidor es un programa que opera como oyente de un socket.

## **Tipos de Redes**

### **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. El alcance de una PAN es

de algunos metros. Se pueden conectar con cables a los USB y FireWire de la computadora (27).

### **Red de área local (LAN)**

Una red que se limita a un área tal como un cuarto, un solo edificio o una nave. Una LAN grande se divide generalmente en segmentos lógicos más pequeños llamados grupos de trabajo (27).

### **Red de área metropolitana (MAN)**

Una red que conecta las redes de dos o más locales pero no se extiende más allá de los límites de la una ciudad (27).

### **Red de área mundial (MAN)**

Es una red que cubre un área geográfica amplia y en gran parte de su estructura utiliza instalaciones de transmisión telefónicas (27).

### **Redes de área local de alta velocidad**

El rápido avance de las tecnologías ha producido grandes cambios en aplicaciones, diseño y, como no, en las redes. En el apartado de Ethernet se estudiaron las redes que tenía definidas en un principio el estándar 802.3. Actualmente dicho estándar comprende velocidades de transmisión de 10 Mbps, 100 Mbps, 1 Gbps y 10 Gbps (28).

### **Las redes de alta velocidad más importantes son:**

- Fast Ethernet y Gigabit Ethernet: es la extensión de la técnica de acceso múltiple con detección de portadora y detección de colisiones, o CSMA/CD, de 10 Mbps (28).
- Canal de fibra: este estándar proporciona una solución de bajo coste y fácilmente escalable para alcanzar tasas de datos elevadas en áreas locales (28).
- Redes LAN inalámbricas de alta velocidad (28).

### **Redes de área extensa**

Las redes de área extensa, son de comunicaciones que acaparan grandes zonas geográficas. Teniendo el patrón descrito de Internet, las WAN llega a servir para intercomunicar las distintas LAN, de manera que los dispositivos de una LAN pueden tener una interconexión con los de una red diferente a pesar de no compartir el mismo medio. Cuando 2 dispositivos en una LAN se requieren la comunicación, al repartir un mismo modo de comunicación pueden enviarse de manera directa los mensajes en una dimensión de señalización. En el instante en que el emisor y receptor no reparte esto, como están en distintas LAN, hará falta un mediador que haga llegar la señal a la red donde se encuentra el receptor, de manera que lo pueda percibir y tener una recepción óptima (29).

## **Seguridad IP**

El estándar IPsec (IP Security – Seguridad IP) aprueba agregar servicios de autenticación, encriptación de información e cambio de claves a toda la conexión IP. Por lo tanto, resulta muy atractivo cuando se necesita seguridad en la información que viaja por una WAN o por Internet y para poder asegurar los 4 requerimientos. El de IPsec es muy beneficioso para las redes privadas virtuales (VPN) a través de Internet, el comercio electrónico en Internet, las Extranets (30).

## **Encriptación de datos**

La encriptación de datos (data encryption), también conocida con el término cifrado, consiste en la alteración de un mensaje o contenido mediante alguna codificación que lo torne inentendible e irreconocible. En un entorno de comunicaciones, si el emisor y el receptor son los únicos que entienden ese código, ningún otro podrá descifrar el mensaje oculto. La forma más sencilla de comprender la encriptación de datos es su comparación con los diferentes idiomas. Si dos personas comienzan a conversar en japonés en una reunión en la cual ningún otro sabe ese idioma, mantendrán una comunicación secreta que nadie les podrá interceptar (30).

## **Redes Privadas Virtuales VPN**

Las empresas tienen redes LAN y WLAN para sus oficinas, pero también suelen necesitar que los empleados puedan entrar a esa misma red desde cualquier otro lugar de Internet (su casa, la sede de otra empresa, etc.), por cualquier motivo (buscar información en la intranet, recuperar un fichero del disco compartido, actualizar un pedido, etc.).

Algo como establecer una VLAN entre el ordenador del empleado y la LAN de la empresa, utilizando Internet como transporte. Estamos hablando de montar una VPN (Virtual Private Network, red privada virtual). El objetivo final de la VPN es que el empleado (más bien, su ordenador) no note si está en la empresa o fuera de ella. En ambos casos recibe una configuración IP privada (direcciones 10.X.X.X, por ejemplo), por lo que no necesita cambiar nada en la configuración de sus aplicaciones (correo, intranet, etc.). El responsable de conseguir esta transparencia es el software de la VPN. En el ordenador del empleado hay que instalar un software cliente VPN. Este software instala un driver de red, de manera que para el sistema operativo es una tarjeta más (31).

#### 2.2.11 Tipos de VPN

##### **VPN de acceso remoto**

Consiste en usuarios que se conectan a una empresa desde sitios remotos utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso similar a estar dentro de la red local (32).

##### **VPN punto a punto**

Este esquema es el empleado para conectar oficinas remotas con una sede central. El servidor VPN está conectado permanentemente a Internet, acepta conexiones entrantes desde los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet y a través de ésta al túnel VPN de la oficina central. Se utiliza para eliminar las conexiones punto a puntos tradicionales (32).

## **VPN interna**

Este esquema es el menos difundido, pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi) (32).

## **Tunneling**

La tunelización es una técnica que permite a los usuarios de acceso remoto conectarse a una variedad de recursos de red (Puertas de enlace domésticas corporativas o un Proveedor de servicios de Internet) a través de una red pública de datos. En general, los túneles establecidos a través de la red pública son punto a punto (aunque es posible un túnel multipunto) y vinculan a un usuario remoto a algún recurso en el extremo más alejado del túnel. Los principales protocolos de túnel (es decir, el Protocolo de túnel de capa 2 (L2TP), el Protocolo de túnel de punto a punto (PPTP) y el Reenvío de capa 2 (L2F)) encapsulan el tráfico de capa 2 del usuario remoto y lo envían a través de la red pública hasta el extremo del túnel donde se desencapsula y se envía a su destino. El beneficio más importante de Tunneling es que permite la creación de redes privadas virtuales (VPN, por sus siglas en inglés) a través de redes públicas de datos para proporcionar ahorros a los usuarios finales, que no tienen que crear redes dedicadas, y a los proveedores de servicios, que pueden aprovechar sus inversiones en redes en muchos Clientes de VPN (33).

## **GNU-Linux**

Para entender todo el movimiento del software libre, debemos situarnos a finales de la década de los sesenta, principios de los setenta. En aquellos tiempos las grandes compañías de ordenadores no daban el valor que hoy día se da al software. En su gran mayoría eran fabricantes de ordenadores que obtenían sus principales ingresos vendiendo sus grandes máquinas, a las que incorporaban algún tipo de sistema operativo y aplicaciones. Las universidades tenían permiso para coger y estudiar el código fuente del sistema operativo para fines docentes. Los mismos usuarios podían pedir el código fuente de drivers y programas para adaptarlos a sus necesidades. Se consideraba que el software no tenía valor por sí mismo si no estaba acompañado por el hardware que lo soportaba. En este entorno, los laboratorios Bell (AT&T) diseñaron un sistema operativo llamado UNIX, caracterizado por la buena gestión de los recursos del sistema, su estabilidad y su compatibilidad con el hardware de diferentes fabricantes (para homogeneizar todos sus sistemas). Este último hecho fue importantísimo (hasta entonces todos los fabricantes tenían sus propios operativos incompatibles con los otros), ya que devino el factor que le proporcionó mucha popularidad (34).

## **Centos**

CentOS (Community ENTerprise Operating System) es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente publicado por Red Hat, siendo la principal diferencia con este la remoción de todas las referencias a las marcas y logos propiedad de Red Hat.

Es un sistema operativo de código abierto, basado en la distribución 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 y utilizar. Desde la versión 5, cada lanzamiento recibe soporte durante diez años, por lo que la actual versión 7 recibirá actualizaciones de seguridad hasta el 30 de junio de 2024 (35).

### III. HIPÓTESIS

La propuesta de implementación de una Red Privada Virtual Segura Corporativa con linux en una Plataforma Virtualizada Mixta en la empresa Infonet Soluciones E.I.R.L - Sullana; optimizará la transmisión de la información.

## IV. METODOLOGÍA

### 4.1 Diseño de la investigación

#### **Tipo de investigación**

Esta investigación es una investigación cuantitativa, por lo tanto, Fernández, P. y Díaz, P. (36), define que trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede.

#### **Nivel de la investigación**

De acuerdo a la naturaleza del estudio de la investigación, reúne por su nivel, las características de un estudio descriptivo. Según Tamayo y Tamayo M. (37), en su libro *Proceso de Investigación Científica*, la investigación descriptiva “comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre grupo de personas, grupo o cosas, se conduce o funciona en presente”.

Según Sabino (38), “La investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta. Para la investigación descriptiva, su preocupación primordial radica en descubrir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permitan poner de manifiesto su estructura o comportamiento. De esta forma se pueden obtener las notas que caracterizan a la realidad estudiada”.

## **Diseño de la investigación**

El diseño de esta investigación fue de tipo no experimental el mismo que define Shadish W. (39), afirma que: “Los Diseños no experimentales, son aquellos en los que se identifica un conjunto de entidades que representan el objeto del estudio y se procede a la observación de los datos. En cuanto a la dimensión temporal, la investigación además de ser no experimental también es de corte transversal como lo define Seehorn (40), implica la recogida de datos una vez durante una cantidad de tiempo limitada. La investigación transversal suele ser descriptiva más que experimental.

### **4.2 Población y muestra.**

La Población conjunto de elementos que tengan una o más propiedades en común definidas por el investigador y que puede ser desde toda la realidad, hasta un grupo muy reducido de fenómenos (41).

La población se conforma por 5 trabajadores, quienes llegarán a estar involucrados a participar en la plataforma virtualizada, en la en la empresa “Infonet Soluciones E.I.R.L.”.

La muestra se llega a constituir por toda la población, debido a que se desea obtener resultados más precisos, ya que están relacionados directamente con el trabajo de investigación.

### 4.3 Definición y operacionalización de variables e indicadores

Tabla N° 3: Definición Operacional

<b>Variable</b>	<b>Descripción Conceptual</b>	<b>Dimensiones</b>	<b>Indicadores</b>	<b>Definición Operacional</b>
Propuesta de Implementación de una red privada virtual segura corporativa con Linux en una plataforma Virtualizada mixta	<p><b>Diseño de una red privada virtual</b></p> <p>El Diseño es una actividad creativa cuyo propósito es establecer las cualidades multifacéticas de</p>	Nivel de satisfacción con respecto a la implementación del sistema actual.	<ul style="list-style-type: none"> <li>• Administración de la información</li> <li>• Actualmente se puede compartir recursos.</li> </ul>	El diseño de una red privada virtual segura corporativa con Linux en una plataforma Virtualizada mixta, llega hacer el proceso la cual se desarrolla o

	<p>objetos, procesos, servicios y sus sistemas, en todo su ciclo de vida (42).</p> <p>Una red privada virtual (VPN) es una tecnología que crea una conexión cifrada en una red menos segura (43).</p>	<p>Nivel del servicio en red</p> <p>Nivel de Seguridad de la información.</p>	<ul style="list-style-type: none"> <li>• Personal especializado en red de datos.</li> <li>• Disminución de tiempo empleado en el manejo de los procesos.</li> <li>• Autenticación de usuarios.</li> </ul>	<p>pone en ejecución de una plataforma virtualizada mixta para la ayuda en la toma de decisiones, en la cual permitirá un menor manejo en la empresa “Infonet Soluciones E.I.R.L”, la eficacia se medirá, con mayor exactitud.</p>
--	---	---	---	--

Fuente: Elaboración Propia.

#### 4.4 Técnicas e instrumentos de recolección de datos

En el presente trabajo de investigación se utilizará la técnica de la encuesta y como instrumento para la elaboración de ésta, será el cuestionario.

La técnica que se utilizó en esta investigación será la encuesta que según Mayntz citado por Díaz de Rada, describen que es la búsqueda sistemática de información en la que el investigador pregunta a los investigados sobre los datos que desea obtener, y posteriormente reúne estos datos individuales para obtener durante la evaluación datos agregados (44), y el instrumento que se utilizó es el cuestionario que según Casas es un documento que recoge en forma organizada los indicadores de las variables implicadas en el objetivo de la encuesta (45).

#### 4.5 Plan de análisis

A partir de los datos que se obtuvieron, se creó una base de datos temporal en el software Microsoft Excel 2013, y se procedió a la tabulación de los mismos. Se realizó el análisis de datos con cada una de las preguntas establecidas dentro del cuestionario dado permitiendo así resumir los datos en un gráfico que muestra el impacto porcentual de las mismas.

Este procedimiento se utilizó para agrupar los datos por medio de computadoras, a tabular, ponderar e interpretar los datos usando una hoja de cálculo en Excel, se presentó la información recopilada por medio de encuestas que fueron transcritas a su posterior análisis, en este caso el indicador estadístico fueron presentados como información en forma de cuadros y gráficos.

#### 4.6 Matriz de consistencia

TITULO: PROPUESTA DE IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL SEGURA CORPORATIVA CON LINUX EN UNA PLATAFORMA VIRTUALIZADA MIXTA PARA LA EMPRESA INFONET SOLUCIONES E.I.R.L - SULLANA; 2020.

Tabla N° 4: Matriz de Consistencia

<b>PROBLEMA</b>	<b>OBJETIVOS</b>	<b>HIPÓTESIS</b>	<b>METODOLOGÍA</b>
¿De qué manera la propuesta de implementación de una red privada virtual segura corporativa con Linux en una Plataforma Virtualizada Mixta en la empresa Infonet Soluciones E.I.R.L. Sullana, optimiza la transmisión de la información?	<p><b>OBJETIVO GENERAL</b></p> <p>Proponer la implementación de una Red Privada Virtual Segura Corporativa con Linux En Una Plataforma Virtualizada Mixta en la Empresa Infonet Soluciones E.I.R.L – Sullana, para optimizar la transmisión de la información.</p>	<p>La propuesta de implementación de una Red Privada Virtual Segura Corporativa con linux en una Plataforma Virtualizada Mixta en la empresa Infonet Soluciones E.I.R.L - Sullana; optimizará la transmisión de la información.</p>	<p>Tipo: Cuantitativa</p> <p>Nivel: Descriptiva</p> <p>Diseño: No experimental, de corte transversal.</p>

	<p><b>OBJETIVOS ESPECÍFICOS</b></p> <ul style="list-style-type: none"> <li>- Determinar el nivel de satisfacción de la red privada actual.</li> <li>- Utilizar redes gratuitas como Internet, para conectar las redes privadas.</li> <li>- Cifrar todas las conexiones, para que los datos vayan de host a host de forma segura.</li> <li>- Determinar el nivel de satisfacción de la propuesta de implementación de la Red Privada Virtual Segura Corporativa con Linux En Una Plataforma Virtualizada Mixta en la Empresa Infonet Soluciones E.I.R.L – Sullana.</li> </ul>		
--	--	--	--

Fuente: Elaboración Propia.

#### 4.7 Principios éticos

Para el desarrollo de esta investigación denominada “El diseño para la implementación de una red privada virtual segura corporativa con linux en una plataforma virtualizada mixta en la empresa Infonet Soluciones E.I.R.L - Sullana; 2020”, se ha considerado muy estrictamente el cumplimiento de los principios éticos que permitan asegurar la originalidad de toda la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas.

Por otro lado, considerando que una gran parte de la información utilizada son de carácter público, y pueden ser conocidos y empleados por diversos analistas, sin mayores restricciones, se ha incluido su contenido sin modificaciones, salvo aquellas necesarias por la aplicación de la metodología para el análisis requerido en este trabajo de investigación.

La presente investigación se está realizando acatando el código de ética versión 002, el cual tiene por finalidad establecer los principios y valores éticos, de la misma forma del reglamento de sanción por infracción al ejercicio de la investigación Científica y se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico.

## V. RESULTADOS

### 5.1 Resultados

#### 5.1.1 Dimensión 01: Nivel de acceso a la información

Tabla N° 5: Disponibilidad de Información

Distribución de frecuencias y respuestas relacionadas con la disponibilidad de la información; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	2	40
No	3	60
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Cuenta con disponibilidad de la información entre las áreas?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 5 se puede observar que el 60% de los trabajadores encuestados expresaron que NO cuentan con la disponibilidad de información entre las áreas; mientras que el 40% indicaron que SI.

Tabla N° 6: Eficacia en el servicio

Distribución de frecuencias y respuestas relacionadas con la eficacia en el servicio; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	1	20
No	4	80
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Existe eficacia con el servicio de acceso a la información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 6 se puede observar que el 80% de los trabajadores encuestados expresaron que NO hay eficacia con el servicio de acceso a la información; mientras que el 20% indicaron que SI.

Tabla N° 7: Medio físico

Distribución de frecuencias y respuestas relacionadas con el medio físico para compartir información; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	1	20
No	4	80
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Emplea algún medio físico (memoria, disco duro) para compartir información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 7 se puede observar que el 80% de los trabajadores encuestados expresaron que NO se emplea ningún medio físico para compartir información; mientras que el 20% indicaron que SI.

Tabla N° 8: Velocidad de transmisión de datos

Distribución de frecuencias y respuestas relacionadas con la velocidad de transmisión de datos; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	1	20
No	4	80
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿La velocidad de transmisión de datos actual es óptima?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 8 se puede observar que el 80% de los trabajadores encuestados expresaron que NO hay dificultades con la velocidad de transmisión de datos; mientras que el 20% indicaron que SI.

Tabla N° 9: Compartir archivos

Distribución de frecuencias y respuestas relacionadas con la compartición de archivos mediante la red; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	2	40
No	3	60
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Actualmente puede compartir sus archivos mediante la red o con otro compañero de trabajo?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 9 se puede observar que el 60% de los trabajadores encuestados expresaron que NO se puede compartir archivos mediante la red con otro compañero de trabajo; mientras que el 40% indicaron que SI.

## A. Resumen de la Dimensión 01

Tabla N° 10: Dimensión Nivel de Acceso a la Información

Distribución de frecuencias relacionadas con la dimensión 01: Nivel de Acceso a la Información, la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2017.

Alternativas	n	%
Si	1	20
No	4	80
Total	5	100

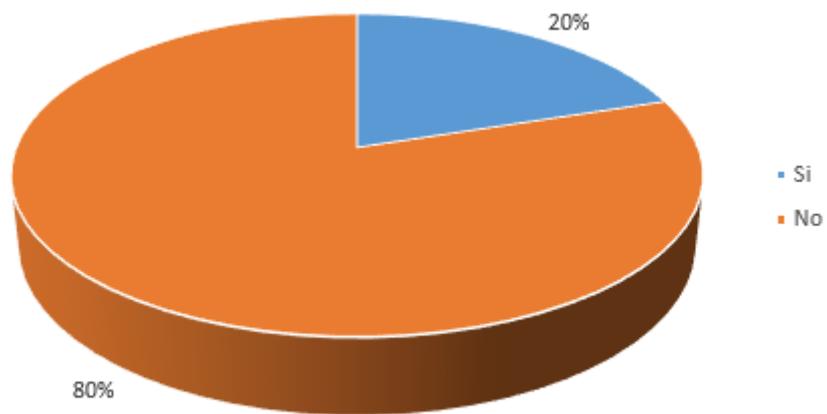
Fuente: Aplicación del instrumento para medir la Dimensión 01: Nivel de Acceso a la Información, basado en 5 preguntas aplicadas a los trabajadores de la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 10 se puede observar que el 80% de los trabajadores que se encuestaron expresaron que NO tienen ninguna facilidad en el acceso de la información, la cual no se puede compartir archivos mediante la red con otro compañero de trabajo; mientras que el 20% indicaron que SI.

Gráfico N° 2: Resultado de la Dimensión 01 Nivel de Acceso a la Información

Distribución porcentual de frecuencia y respuestas relacionadas con la dimensión 01: Nivel de Acceso a la Información; para la Propuesta de Implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.



Fuente: Tabla N° 10

### 5.1.2 Dimensión 02: Nivel de seguridad de red

Tabla N° 11: Medidas de Seguridad

Distribución de frecuencias y respuestas relacionadas con las medidas de seguridad; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	5	100
No	0	0
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Según usted cree que existen medidas de seguridad para proteger la información que comparte?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 11 se puede observar que el 100% de los trabajadores encuestados expresaron que SI existen medidas de seguridad para proteger la información que comparten.

Tabla N° 12: Autenticación de usuarios

Distribución de frecuencias y respuestas relacionadas con la autenticación de usuarios; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	4	80
No	1	20
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Existe autenticación de usuarios en el intercambio de la información, que se realizan mediante los sistemas?, en la empresa Infonet Soluciones E.I.R.L-Sullana; 2020.

Aplicado por: Juárez, A.; 2018.

En la Tabla N° 12 se puede observar que el 80% de los trabajadores encuestados expresaron que SI existe autenticación de usuarios en el intercambio de la información, mientras que el 20% indico que NO.

Tabla N° 13: Privilegios de los usuarios

Distribución de frecuencias y respuestas relacionadas con los privilegios de los usuarios; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	0	0
No	5	100
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Hay privilegios de los usuarios, respecto al uso de los sistemas de información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 13 se puede observar que el 100% de los trabajadores encuestados expresaron que NO hay privilegios de los usuarios, respecto al uso de los sistemas de información.

Tabla N° 14: Políticas de Seguridad

Distribución de frecuencias y respuestas relacionadas con las políticas de seguridad; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	4	80
No	1	20
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Cree que hay políticas de seguridad en el uso de la Red e Internet?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 14 se puede observar que el 80% de los trabajadores encuestados expresaron que SI cree que hay políticas de seguridad en el uso de la red, mientras que el 20% indico que NO.

Tabla N° 15: Detección de Software Malicioso

Distribución de frecuencias y respuestas relacionadas con la detección de software malicioso; la propuesta de implementación Diseño de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	2	40
No	3	60
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Cree usted que hay prevención, detección y corrección de Software malicioso?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 15 se puede observar que el 60% de los trabajadores encuestados expresaron que SI prevención, detección y corrección de software malicioso, mientras que el 40% indico que NO.

## B. Resumen de la Dimensión 02

Tabla N° 16: Dimensión Nivel de Seguridad de Red

Distribución de frecuencias relacionadas con la dimensión 02: Nivel de Seguridad de Red, la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	3	60
No	2	40
Total	5	100

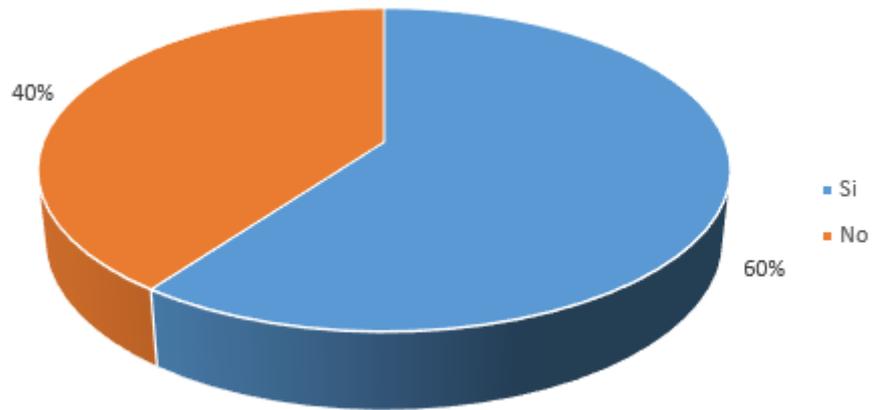
Fuente: Aplicación del instrumento para medir la Dimensión 02: Nivel de Seguridad de Red, basado en 5 preguntas aplicadas a los trabajadores de la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 16 se puede observar que el 60% de los trabajadores encuestados expresaron que SI hay un nivel de seguridad en la red de la empresa, mientras que el 40% indico que NO.

Gráfico N° 3: Resultado de la Dimensión 02 Nivel de Seguridad de Red

Distribución porcentual de frecuencia y respuestas relacionadas con la dimensión 02: Nivel de Seguridad de Red; para la Propuesta de Implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.



Fuente: Tabla N° 16

### 5.1.3 Dimensión 03: Nivel de diseño de red privada virtual

Tabla N° 17: Diseño de Red Privada

Distribución de frecuencias y respuestas relacionadas con el diseño de la red privada; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	4	80
No	1	20
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Cree necesario realizar un diseño de una red privada virtual segura corporativa con Linux en una plataforma Virtualizada mixta para la empresa Infonet Soluciones E.I.R.L - Sullana; 2020?

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 17 se puede observar que el 80% de los trabajadores encuestados expresaron que SI es necesario realizar el diseño de una red privada virtual; mientras que el 20% indicaron que NO.

Tabla N° 18: Simplificación del Trabajo

Distribución de frecuencias y respuestas relacionadas con la simplificación del trabajo diario; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	3	60
No	2	40
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿A su criterio piensa o cree que una red privada virtual le simplificaría el trabajo diario?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 18 se puede observar que el 60% de los trabajadores encuestados expresaron que SI cree que una red privada virtual les simplificaría el trabajo diario; mientras que el 40% indicaron que NO.

Tabla N° 19: Beneficios a los Trabajadores

Distribución de frecuencias y respuestas relacionadas con los beneficios de los trabajadores; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	3	60
No	2	40
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Cree usted que una eventual implementación de una red privada virtual beneficiaría a los trabajadores de la empresa?, Infonet Soluciones E.I.R.L - Sullana; 2020?

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 19 se puede observar que el 60% de los trabajadores encuestados expresaron que SI se beneficiarían con una eventual implementación de un red privada virtual; mientras que el 40% indicaron que NO.

Tabla N° 20: Acceso a la Información

Distribución de frecuencias y respuestas relacionadas con el acceso a la información; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	5	100
No	0	0
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Piensa que la implementación de una red privada virtual permitiría un mejor acceso a la información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 20 se puede observar que el 100% de los trabajadores encuestados expresaron que SI permitirían un mejor acceso a la información con la implementación de una red privada virtual.

Tabla N° 21: Privacidad de Información

Distribución de frecuencias y respuestas relacionadas con el acceso a la información; la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	5	100
No	0	0
Total	5	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Piensa que la implementación de una red privada virtual permitiría un mejor acceso a la información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 21 se puede observar que el 100% de los trabajadores encuestados expresaron que SI permitirían un mejor acceso a la información con la implementación de una red privada virtual.

### C. Resumen de la Dimensión 03

Tabla N° 22: Dimensión Nivel de Diseño de Red Privada Virtual

Distribución de frecuencias relacionadas con la dimensión 03: Nivel de Diseño de Red Privada Virtual, la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Alternativas	n	%
Si	4	80
No	1	20
Total	5	100

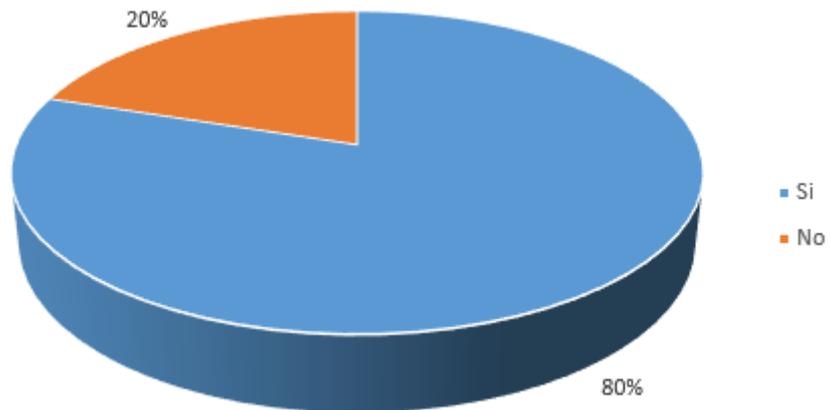
Fuente: Aplicación del instrumento para medir la Dimensión 03: Nivel de Diseño de Red Privada Virtual, basado en 5 preguntas aplicadas a los trabajadores de la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Juárez, A.; 2020.

En la Tabla N° 22 se puede observar que el 80% de los trabajadores encuestados expresaron que SI es necesario el nivel de Diseño de Red Privada Virtual para la empresa; mientras que el 20% indicaron que NO.

Gráfico N° 4: Resultado de la Dimensión 03 Nivel de Diseño de Red Privada Virtual

Distribución porcentual de frecuencia y respuestas relacionadas con la dimensión 03: Nivel de Diseño de Red Privada Virtual; para la propuesta de Implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.



Fuente: Tabla N° 22

#### D. Resumen de las Dimensiones

Tabla N° 23: Resumen de Dimensiones

Distribución de frecuencia y respuesta relacionada al resumen de las 3 dimensiones la cual son el Nivel de Acceso a la Información, Nivel de Seguridad de Red y Nivel de Diseño de Red Privada Virtual; para la propuesta de Implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Dimensiones	SI		NO		TOTAL	
	n	%	n	%	n	%
Nivel de Acceso a la Información	1	20	4	80	5	100
Nivel de Seguridad de Red	3	60	2	40	5	100
Nivel de Diseño de Red Privada Virtual	4	80	1	20	5	100

Fuente: El instrumento aplicado para el conocimiento de los trabajadores encuestados sobre las tres dimensiones definidas en la investigación; de la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

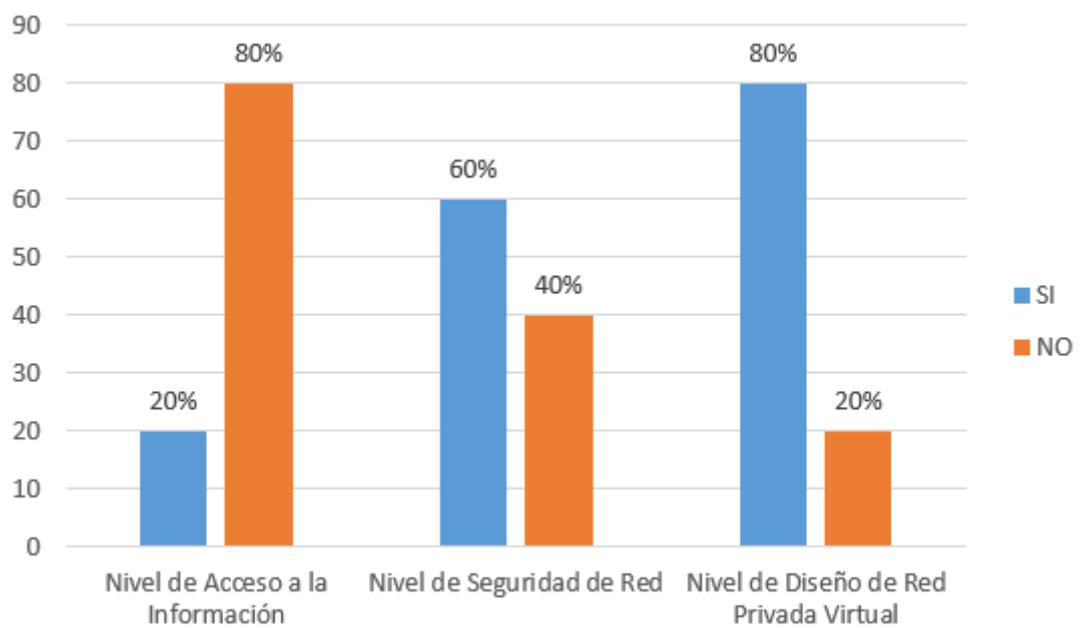
Aplicado por: Juárez, A.; 2020.

En la Tabla N° 23, en la primera dimensión se observa que el 80% de los encuestados NO tienen ninguna facilidad en el acceso de la información; mientras que el 20% indico que NO. En la segunda dimensión el 60% de los trabajadores

encuestados expresaron que SI hay un nivel de seguridad en la red de la empresa, mientras que el 40% indico que NO. En la tercera dimensión el 80% de los trabajadores encuestados expresaron que SI es necesario el nivel de Diseño de Red Privada Virtual para la empresa; mientras que el 20% indicaron que NO.

Gráfico N° 5: Resumen general de dimensiones

Distribución porcentual de frecuencia y respuestas relacionadas con los resultados del resumen general de las tres dimensiones escogidas en la investigación; para la Propuesta de Implementación una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.



Fuente: Tabla N° 23.

## 5.2 Análisis de resultados

El objetivo de la presente investigación fue: Realizar la Propuesta de Implementación de una red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; que solucione los problemas de comunicación y acceso a la información de la empresa; en este sentido para poder cumplir con este objetivo es preciso realizar una apreciación del escenario actual con el fin de que este diseño identifique claramente las necesidades y pueda cubrir las exigencias de la entidad a través de una propuesta de implementación. Por lo cual realizaremos un análisis de los resultados obtenidos de esta investigación de la siguiente manera:

1. En lo que respecta a la dimensión: Acceso a la información, en la Tabla Nro. 10, nos muestra los resultados donde podemos apreciar que el 80% de los trabajadores encuestados respondieron que NO tienen un buen acceso de la información de las demás sucursales de la empresa, este resultado es similar al resultado que ha obtenido Ancajima (8), en su investigación donde obtuvo como resultado en una dimensión similar a la nuestra, un resultado de 70% insatisfacción con respecto al acceso de la información. Esta similitud en los resultados se justifica porque en las empresas investigadas cada una tiene una red local aisladas de las demás, es decir cada una existía una configuración local que no necesariamente era compatible con las otras configuraciones de la empresa.
2. Con relación a la dimensión: Seguridad de la red, en la tabla Nro. 16 nos detalla los resultados donde se puede observar que el 60% de los trabajadores expuso que SI cuentan con una buena seguridad de la red, este resultado no coincide con el obtenido por Ancajima (8), donde en una investigación similar obtuvo como deducción que el 73,33% de los trabajadores manifestaron que había seguridad de red en la empresa en la que laboraban.

3. Asimismo de acuerdo a los resultados obtenidos en la dimensión: Diseño de la red privada virtual, la Tabla Nro. 22 nos muestra los resultados donde se puede observar que el 80% de los trabajadores encuestados expresaron que SI están de acuerdo con el diseño para la implementación de una red privada virtual. Este resultado coincide con los resultados obtenidos por Muñoz (9), donde en su investigación indica que el 100% de los trabajadores SI están de acuerdo en el diseño e implementación de una red privada virtual, generando la urgente necesidad de un diseño y propuesta de implementación de red privada virtual la cual se ve reflejada en las respuesta de los trabajadores encuestados en busca de cumplir con los objetivos organizacionales propuesto por la empresa.

### 5.3 Propuesta de mejora

Después de haber desarrollado uno a uno los resultados de nuestra investigación y haber realizado la observación correspondiente, se planea la siguiente propuesta económica.

Se ha decidido instalar como servidor principal de la red privada virtual OpenVPN bajo la plataforma de software libre Centos Server en su versión 7, teniendo en cuenta que la empresa Infonet Soluciones E.I.R.L tiene como plataforma principal de sistema operativo Windows la aplicación cliente de OpenVPN se ejecutara sobre Windows ya que es la plataforma principal, así no se hará ninguna actualización ni cambio de tecnología que pueda afectar en la usabilidad y aprendizaje de los usuarios.

#### 1. Escenario

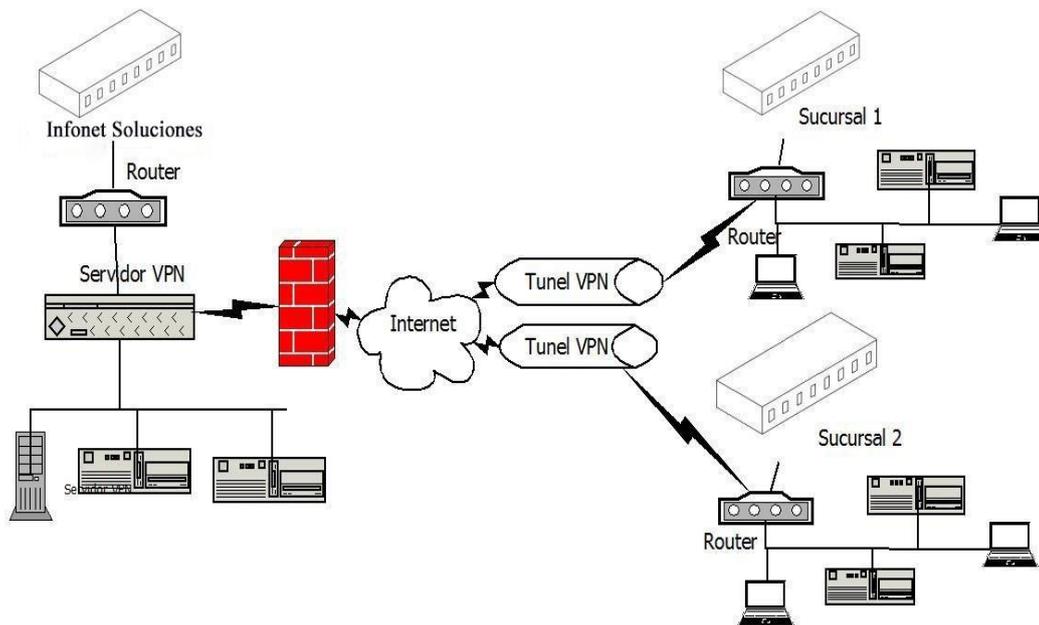
Lo que sea desea es tener la posibilidad de acceder a una red local (protegida detrás de un firewall/gateway) desde Internet (o desde cualquier otra red insegura). El fin es que un usuario de la empresa ubicado físicamente fuera de la red local y posiblemente a kilómetros de distancia parezca conectado de forma local. El servidor de VPN es el que posibilita la "extensión" y es quien nos realiza una conexión segura entre el usuario y la red local a través de SSL. Al utilizar certificados se obtiene autenticación mutua y confidencialidad.

Cumpliendo con los objetivos y necesidades de la empresa se ha optado por utilizar la tecnología OpenVPN que es un Software que hace de cliente y servidor según como lo configuremos, es la mejor opción que ofrece una mezcla semejante de seguridad a nivel empresarial, seguridad, facilidad de uso y riqueza de características. Es una solución multiplataforma que

simplifica mucho la configuración de VPN haciéndola más accesible para los usuarios en este tipo de tecnología.

El siguiente diagrama muestra el escenario planteado.

Gráfico N° 6: Escenario VPN



Fuente: Elaboración Propia

## 2. Tipo de configuración VPN

Hay varias formas de configurar el servidor OpenVPN. Los distintos tipos de configuración existentes son Host to Host, Road to Warrior (Host to LAN) y Net to net. La mejor conexión que se adapta a las necesidades de la empresa y en la cual nosotros nos focalizaremos es el Road to Warrior o Host to LAN, por ser el más adecuado de todos y el que seguramente se adaptará a prácticamente las necesidades y requerimientos de la empresa.

La configuración Road to Warrior (Host to LAN mediante túnel) permitirá que múltiples dispositivos u ordenadores se puedan conectar simultáneamente a nuestra red VPN y compartir recursos e informaciones con la red a que se conectan. Por lo tanto en este caso tenemos varios usuarios que se pueden conectar de forma independiente al servidor VPN.

### 3. IP fija de la red local

Es muy importante asegurar que nuestro servidor disponga de una IP interna fija en la red local. Es importante porque cuando recibamos una petición de los clientes VPN, el router tendrá que saber a qué IP interna tiene que redireccionar la petición del cliente VPN.

### 4. Redireccionamiento dinámico

Cuando ya se haya puesto en marcha el servidor VPN, lo más probable es que algún usuario de la empresa tenga que conectarse desde el exterior hacia la red local mediante el servidor VPN. Para conectarnos a nuestra red local es necesario saber nuestra IP Pública pero nuestro servidor VPN en este caso la IP que tiene es dinámica. Por este motivo es que es necesario que la empresa adquiriera un servicio de IP estática.

### 5. Instalación del servidor

La instalación del servidor la vamos a realizar en un sistema operativo Ubuntu. Una de las características por la cual se eligió la tecnología OpenVPN es porque puede funcionar en cualquier distribución que derive de Debian como pueden ser Ubuntu, Crunchbang, Linux Mint, Kubuntu y por

supuesto Windows lo que lo hace multiplataforma siendo unos de los principales objetivos que se adapte mejor a la necesidades de la empresa.

Para instalar el servidor OpenVPN lo que tenemos que hacer es abrir una terminal. Dentro de la terminal teclean el siguiente comando: `sudo apt-get install openvpn openssl`

Este comando descargara todos lo repositorios necesarios para luego instalar el servidor vpn.

## 6. Autoridad de certificación

OpenVPN es un protocolo de VPN basado SSL/TLS mediante certificado y clave RSA creadas mediante openssl. Por lo tanto el nivel de seguridad proporcionado por OpenVPN es muy elevado.

Al ser un protocolo que funciona bajo certificados y claves necesitaremos crear una autoridad de certificación para luego generar los certificados.

Nota: La principal función de una autoridad de certificación es la de emitir y revocar certificados digitales para terceros. Crear el certificado raíz CA para firmar y revocar los certificados de los clientes para poder emitir y revocar la claves necesitamos crear nuestra propia autoridad certificadora y disponer de nuestro certificado raíz `ca.ctr` y de nuestra clave `ca.key` para poder crear y firmar las claves de los clientes y del servidor.

Para realizar este paso, y el resto de pasos, ejecutaremos los scripts que OpenVPN trae incorporados de serie. Para ello tenemos que crear una carpeta con nombre easy-rsa dentro de la ubicación /etc/openvpn.

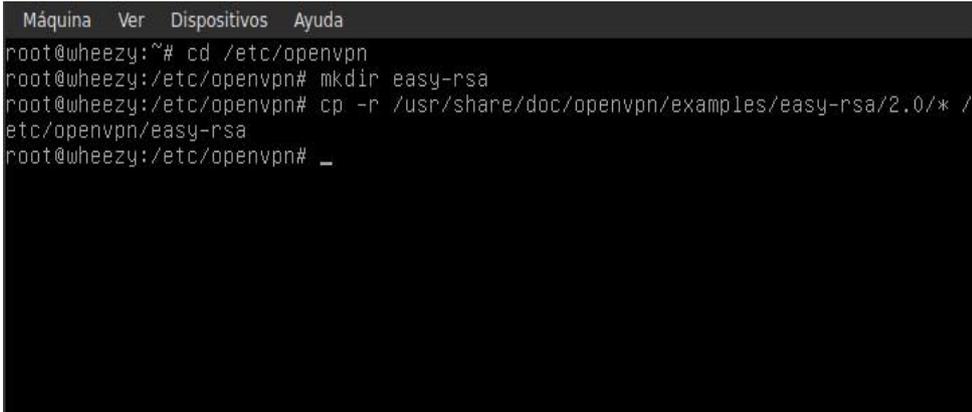
Para ello abrimos una terminal y tecleamos el siguiente comando:

```
cd /etc/openvpn
mkdir easy-rsa
```

Después hay que copiar los scripts de configuración de OpenVPN, que se hallan en la ubicación /usr/share/doc/openvpn/examples/easyrsa/2.0/, dentro de la carpeta easy-rsa que acabamos de crear. Para ello en la terminal tecleamos el siguiente comando:

```
cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* easy-rsa
```

#### Gráfico N° 7: Captura copia de script de configuración



```
Máquina Ver Dispositivos Ayuda
root@wheezy:~# cd /etc/openvpn
root@wheezy:/etc/openvpn# mkdir easy-rsa
root@wheezy:/etc/openvpn# cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /
etc/openvpn/easy-rsa
root@wheezy:/etc/openvpn# _
```

Fuente elaboración: propia

Para ejecutar los scripts que acabamos de copiar o de obtener, tenemos que ir a la ubicación donde los guardamos. Para ello ingresamos el siguiente comando en la terminal:

```
cd /etc/openvpn/easy-rsa
```

Antes de ejecutar los scripts editaremos el fichero vars para modificar una serie de parámetros. Para modificar el fichero vars se tiene que introducir el siguiente comando en la terminal:

```
nano vars
```

Una vez abierto el editor de texto tenemos que localizar y modificar la siguiente línea:

```
export_KEY_SIZE=1024
```

Una vez encontrada la sustituyen por la siguiente línea:

```
export_KEY_SIZE=2048
```

Nota: Con esta modificación estamos incrementando el tamaño de las claves privadas (.key) que vamos a generar y también del parámetro de Diffie Hellman. Con esta modificación incrementamos el tamaño de las claves de 1024 bits a 2048 bits. También sería posible usar 4096 bits. Este parámetro no tiene porqué penalizar en exceso el rendimiento del servidor. Únicamente penalizará el proceso autenticación Handshake de SSL/TLS.

Datos de la entidad emisora de los certificados

Seguidamente tenemos que introducir los datos de la entidad emisora de los certificados que en este caso los emitirá a nombre de la empresa Agromar Industrial S.A. Para ello tenemos que localizar las siguientes líneas y reemplazar el contenido por defecto por nuestros datos reales.

```
export KEY_COUNTRY=PE  
  
export KEY_PROVINCE=SU  
  
export KEY_CITY=Sullana  
  
export KEY_ORG=Infonet Soluciones  
  
KEY_EMAIL=contacto@gmail.com  
  
export KEY_EMAIL=contacto@gmail.com  
  
export KEY_CN= infonet  
  
export KEY_NAME=vpninfonet  
  
export KEY_OI=IT
```

Una vez modificado el archivo vars guardamos los cambios y lo cerramos. Ahora tendremos que exportar sus variables. Para exportar sus variables tenemos que teclear el siguiente comando en la terminal:

```
source ./vars
```

Seguidamente ejecutaremos el script clean-all. El script clean-all borrará la totalidad de claves que podrían existir en la ubicación /etc/openvpn/easy-



Finalmente vamos a crear el certificado y la clave privada de nuestra propia autoridad certificadora. Para ello tenemos que teclear el siguiente comando en la terminal:

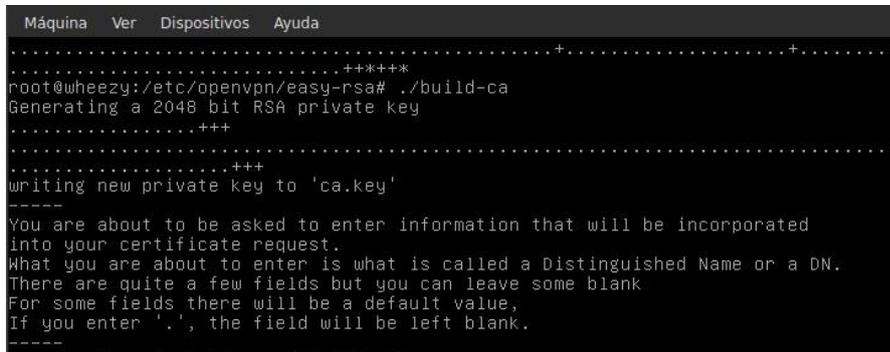
```
./build-ca
```

Al terminar el proceso dentro de la ubicación `/etc/openvpn/easyrsa/keys` se ha creado `ca.crt` y `ca.key`:

`ca.crt`: Es el certificado raíz público de la autoridad de certificación (CA).

`Ca.key`: Este fichero contiene la clave privada de la autoridad de certificación (CA). Este archivo debe mantenerse protegido y no debe estar al alcance de terceros.

Gráfico N° 9: Creación de certificado y clave privada



```
Máquina Ver Dispositivos Ayuda
.....+.....+.....
.....+*+*+*
root@wheezy:/etc/openvpn/easy-rsa# ./build-ca
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Fuente: elaboración propia

## 7. Generar certificados y la clave del servidor OpenVPN

Vamos a introducir el siguiente comando en la terminal:

```
./build-key-server SEVERVPN
```

Una vez introducido este comando se nos hará una serie de preguntas. Simplemente tienen que contestar el valor por defecto ya que anteriormente hemos modificado el archivo vars.

Al terminar el proceso dentro de la ubicación `/etc/openvpn/easyrsa/keys` se habrán creado los siguientes archivos:

`whezzyVPN.key`: Este fichero contiene la clave privada del servidor.

Este archivo no debe estar al alcance de nadie.

`whezzyVPN.crt`: Este fichero corresponde al certificado público del servidor.

`whezzyVPN.csr`: Este archivo es la petición de certificado que se envía a la autoridad de certificación. Mediante la información que contiene el archivo `.csr`, la autoridad de certificación podrá realizar el certificado del servidor una vez hayan realizado las comprobaciones de seguridad pertinentes.

Gráfico N° 10: Generar certificados y clave del servidor



```
Máquina Ver Dispositivos Ayuda
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:solsona
An optional company name []:geekland.hol.es
Using configuration from /etc/openssl/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
```

Fuente: elaboración propia.

## 8. Generar certificado y las claves de los usuarios

El siguiente paso es crear los certificados y las claves de los clientes que se podrán conectar al servidor VPN. Para ello tenemos que teclear el siguiente comando en la terminal:

```
./build-key usuariovpn
```

Una vez introducido este comando se nos hará una serie de preguntas. Simplemente tienen que contestar el valor por defecto ya que anteriormente hemos editado el fichero vars.

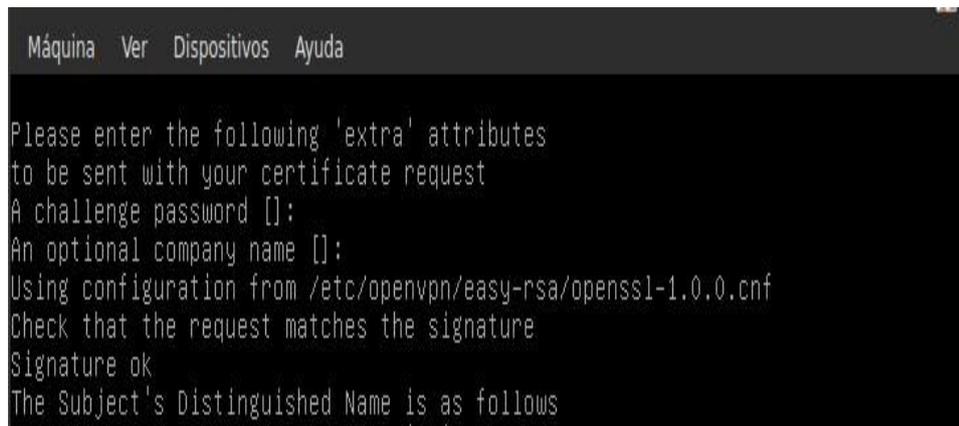
Al terminar el proceso dentro de la ubicación `/etc/openssl/easyrsa/keys` se habrán creado los siguientes archivos

usuariovpn.key: Este fichero contiene la clave privada del cliente. Este archivo no debe estar al alcance de nadie. usuariovpn.crt: Este fichero corresponde al certificado público del servidor.

usuariovpn.csr: Este archivo es la petición de certificado que es envía a la autoridad de certificación. Mediante la información contenida en el archivo .csr, la autoridad de certificación podrá realizar el certificado del cliente una vez hayan realizado las comprobaciones de seguridad pertinentes.

Nota: El procedimiento de generación de clientes se deberá repetir tantas veces como clientes queráis que tenga el servidor OpenVPN.

Gráfico N° 11: Generar certificados y las claves de usuarios



```
Máquina Ver Dispositivos Ayuda
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
```

Fuente: elaboración propia

## 9. Fortalecer la seguridad del servidor OpenVPN con tls-auth

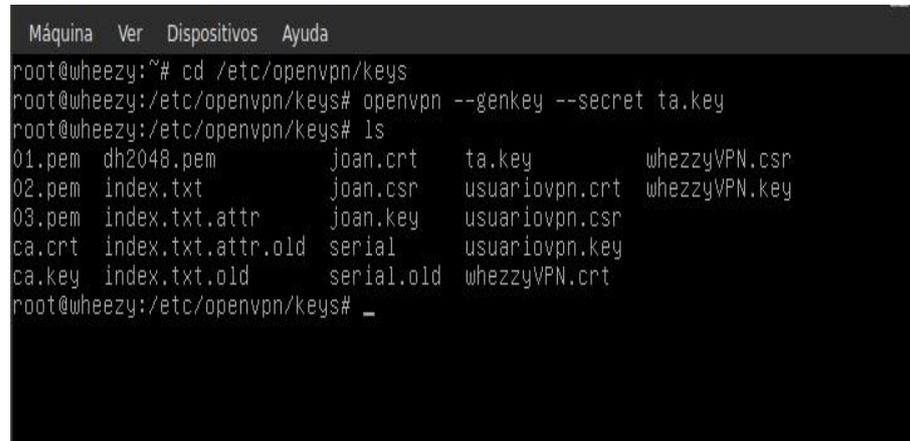
Ahora generamos otra clave. Esta clave nos servirá para agregar soporte para usar la autenticación TLS y de este modo fortificar la seguridad del servidor VPN. Para generar la clave para poder fortificar el servidor se tiene que introducir el siguiente comando en la terminal: `cd /etc/openvpn/easy-rsa/keys`

Una vez hemos accedido a la ubicación `/etc/openvpn/easy-rsa/keys` tecleamos el siguiente comando:

```
openvpn --genkey --secret ta.key
```

Justo al ejecutar el comando, Como se puede ver en la captura de pantalla, se generará una clave con el nombre ta.key en la misma ubicación dónde hemos aplicado el comando.

Gráfico N° 12: Generación de clave de seguridad



```
Máquina Ver Dispositivos Ayuda
root@wheezy:~# cd /etc/openvpn/keys
root@wheezy:/etc/openvpn/keys# openvpn --genkey --secret ta.key
root@wheezy:/etc/openvpn/keys# ls
01.pem  dh2048.pem      joan.crt  ta.key      wheezyVPN.csr
02.pem  index.txt       joan.csr  usuariovpn.crt  wheezyVPN.key
03.pem  index.txt.attr  joan.key  usuariovpn.csr
ca.crt  index.txt.attr.old  serial  usuariovpn.key
ca.key  index.txt.old    serial.old  wheezyVPN.crt
root@wheezy:/etc/openvpn/keys# _
```

Fuente: elaboración propia

La clave creada servirá para introducir una firma digital HMAC en todas las transacciones del protocolo handshake de SSL/TLS entre el cliente y el servidor. De esta forma podremos verificar la integridad de los paquetes intercambiados entre el cliente y el servidor VPN, y en el caso que un cliente intente conectarse al servidor VPN sin poseer la clave para firmar los paquetes la conexión se rechazará automáticamente. Además con el uso de autenticación TLS también conseguiremos prevenir los siguientes ataques:

1. Ataques de denegación de servicio DoS.
2. Ataques de denegación de servicio por inundación UDP al puerto del VPN.
3. Escaneo de puertos en nuestro servidor para intentar averiguar vulnerabilidades.

Anteriormente ya he detallado el uso de cada una de la claves. Seguidamente vamos a detallar la ubicación de cada una de las claves, ubicación de las claves generadas.

Tabla 24: Ubicación de las claves generadas

<i>Archivo</i>	<i>Descripción</i>	<i>Ubicación</i>	<i>Secreto</i>
<i>dh2048.pem</i>	Parámetros Diffie Hellman	Servidor ( <a href="#">/etc/openvpn</a> )	Sí
<i>ca.crt</i>	Certificado raíz de la entidad certificadora	Servidor ( <a href="#">/etc/openvpn</a> ) y cliente	No
<i>ca.key</i>	Clave de la entidad certificadora	Servidor ( <a href="#">/etc/openvpn</a> )	Sí
<i>whezzyVPN.key</i>	Clave del servidor VPN	Servidor ( <a href="#">/etc/openvpn</a> )	Sí
<i>whezzyVPN.crt</i>	Certificado del servidor VPN	Servidor ( <a href="#">/etc/openvpn</a> ) y cliente	No
<i>whezzyVPN.csr</i>	Archivo de petición de certificado	Servidor ( <a href="#">/etc/openvpn</a> )	No
<i>usuariovpn.key</i>	Clave privada del cliente VPN	Cliente	Sí
<i>usuariovpn.crt</i>	Certificado del cliente VPN	Cliente	No

usuariovpn.csr	Archivo de petición de certificado	Servidor (/etc/openvpn)	No
ta.key	Clave para la Autenticación TLS	Servidor (/etc/openvpn) y cliente	Sí

Fuente: Elaboración propia

Nota: Se tiene que trasladar cada una de las llaves mencionadas en las ubicaciones que se detallan en la tabla Nro. 45. Se recomienda transmitir y trasladar las claves y certificados del servidor al cliente por un canal seguro.

#### 10. Certificar que las peticiones DNS se realizan por el VPN

Para que nadie capture las peticiones DNS lo que realizaremos es canalizar la totalidad de nuestras peticiones a través del túnel del servidor OpenVPN. Así las peticiones DNS se enviarán al servidor VPN de forma cifrada y será el servidor OpenVPN el encargado de resolverlas. Para poder realizar lo que acabo de describir lo primero que tienen que realizar es instalar dnsmasq. Para poder instalar dnsmasq teclean el siguiente comando en la terminal:

```
apt-get install dnsmasq
```

Una vez instalado dnsmasq lo tenemos que configurar para que escuche las peticiones DNS dirigidas al servidor VPN. Para ello accedemos al archivo de configuración introduciendo el siguiente comando en la terminal:

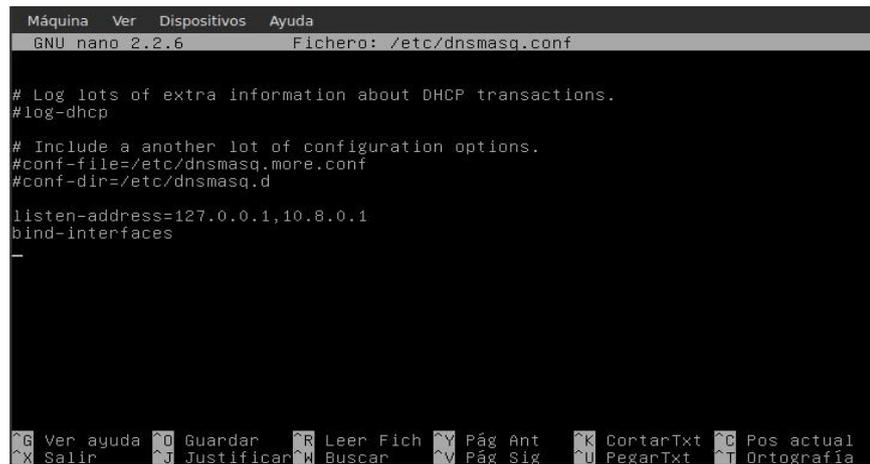
```
nano /etc/dnsmasq.conf
```

Una vez abierto el editor de texto introducen las siguientes líneas:

```
listen-address=127.0.0.1,192.168.0.1
```

```
bind-interfaces
```

Gráfico N° 13: Configuración dnsmasq



```
Máquina Ver Dispositivos Ayuda
GNU nano 2.2.6 Fichero: /etc/dnsmasq.conf

# Log lots of extra information about DHCP transactions.
#log-dhcp

# Include a another lot of configuration options.
#conf-file=/etc/dnsmasq.more.conf
#conf-dir=/etc/dnsmasq.d

listen-address=127.0.0.1,10.8.0.1
bind-interfaces
-

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^G Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

Fuente: elaboración propia

Ahora tan solo tienen que guardar los cambios y salir del archivo de configuración. La configuración ha terminado y solamente hace falta reiniciar los servicios OpenVPN y dnsmasq. Para ello teclean los siguientes comandos en la terminal:

```
/etc/init.d/openvpn restart
```

```
/etc/init.d/dnsmasq restart
```

## 11. Configurar el servidor OpenVPN

Existen ficheros de configuración standard que deben funcionar out of the box y que vamos a aprovechar para realizar nuestra configuración. Los ficheros que podemos usar para ver la totalidad de opciones que tenemos disponibles se hallan comprimidos en la siguiente ubicación:

```
/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
```

Para consultarlos teclear el siguiente comando para acceder a la ubicación de este archivo:

```
cd /usr/share/doc/openvpn/examples/sample-config-files
```

Posteriormente copiamos el archivo comprimido que dispone de los archivos de muestra de configuración en la ubicación `/etc/openvpn`.

Para ello tecleamos el siguiente comando:

```
Cp -a /usr/share/doc/openvpn/examples/sample-config-  
files/server.conf.gz /etc/openvpn/
```

Seguidamente accedemos a la ubicación donde hemos copiado el archivo comprimido que contiene los archivos de configuración:

```
cd /etc/openvpn
```

Para descomprimir el archivo que contiene los archivos de configuración tecleamos:

```
gunzip server.conf.gz
```

Una vez descomprimido el archivo ya podemos buscar la configuración tanto de los usuarios como del servidor. Para ver y modificar la configuración estándar para adaptarla a las necesidades del proyecto se tienen que teclear el siguiente comando en la terminal:

```
nano server.conf
```

Se abrirá el editor de texto en el que podrán ver de forma detallada las opciones de configuración de del servidor. Ahora tendréis que comprobar que la totalidad de parámetros que se muestran en la tabla de este apartado estén dentro del fichero de configuración de ejemplo que es el que vamos a usar. En el caso de que los parámetros estén comentados habrá que descomentarlos, en el caso que no existen se deberán añadir y/o modificar.

## 12. Configurar el usuario OpenVPN

Una vez configurado el servidor ahora pasaremos a configurar el usuario. Para ello dentro de la ubicación `/etc/openvpn` tecleamos el siguiente comando:

```
nano client.conf
```

Se abrirá el fichero de configuración en el que podrá ver un ejemplo de configuración para un cliente estándar. Vamos asegurar que el fichero de

configuración estándar tenga los parámetros que se muestran en la tabla Nro. 47. En caso de no tenerlos habrá que añadirlos manualmente, en el caso de que los parámetros estén comentados habrá que descomentarlos y en el caso que no existan se deberán añadir y/o modificar.

### 13. Autenticación del cliente mediante login y password

A pesar de toda la seguridad que hemos implementado hasta el momento podría darse el caso que alguien robará un ordenador de la empresa. Si alguien robará algún ordenador, teléfono o tablet podría encontrarse con la totalidad de nuestras claves criptográficas y de esta forma podría acceder fácilmente a nuestra red.

Para solucionar este problema vamos a introducir un usuario y un password para los usuarios de nuestro servidor vpn. Para ello tan solo tenemos que añadir uno o los usuarios que queramos.

Para añadir un usuario, como por ejemplo el usuariovpn2, tienen que teclear el siguiente comando en la terminal:

```
useradd usuariovpn2 -M -s /bin/false
```

Una vez creado el usuario tenemos que definir un password del usuariovpn2. Para ello tecleamos el siguiente comando en la terminal:

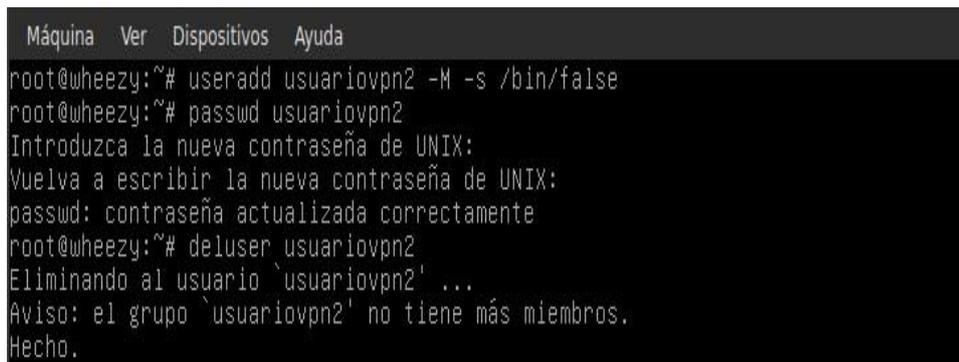
```
passwd usuariovpn2
```

Una vez introducido el comando nos pedirá que introduzcamos la clave de usuario y después nos pedirá confirmación.

En el caso que a posterior se precise eliminar el usuariovpn2 tan solo tienen que introducir el siguiente comando en la terminal:

```
deluser usuariovpn2
```

Tabla 25: Autenticación de usuarios



```
Máquina Ver Dispositivos Ayuda
root@wheezy:~# useradd usuariovpn2 -M -s /bin/false
root@wheezy:~# passwd usuariovpn2
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@wheezy:~# deluser usuariovpn2
Eliminando al usuario `usuariovpn2' ...
Aviso: el grupo `usuariovpn2' no tiene más miembros.
Hecho.
```

Fuente: Elaboración propia

**Nota:** Para que la autenticación mediante usuario y password funcione tienen que tener configurado el servidor y el cliente tal y como se detalla en los apartados Configurar el servidor y configurar el Usuario.

#### 14. Configurar iptables para el enrutamiento de peticiones

Cuando el servidor OpenVPN reciba las peticiones de los clientes se deberán enrutar adecuadamente, y además tendremos que tener configurar el firewall de nuestro equipo para que permita el tráfico a través del túnel que se ha creado ente el cliente y el servidor.

Para ello lo primero que tenemos que hacer es habilitar el IP forwarding. Para habilitar el IP Forwarding de forma permanente tecleamos el siguiente comando en la terminal:

```
nano /etc/sysctl.conf
```

Se abrirá el editor de textos y seguidamente tendremos que localizar la siguiente línea:

```
#net.ipv4.ip_forward=1
```

Una vez localizada tan solo hay que descomentarla de forma que quede de la siguiente forma:

```
net.ipv4.ip_forward=1
```

Guardamos los cambios y cerramos el archivo. Una vez habilitado el Ipforwarding tenemos que permitir el tráfico por nuestro túnel VPN, y además tenemos que hacer que los clientes VPN puedan acceder a redes externas públicas y otras subredes dentro de la red VPN. Para poder conseguir esto en la terminal escriben el siguiente comando:

```
nano /etc/rc.local
```

Una vez se abra el editor de textos tienen que escribir las siguientes reglas en nuestro firewall

```
iptables -A FORWARD -i eth0 -o tun0 -m state --state  
ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A FORWARD -s 192.168.0.1/24 -o eth0 -j ACCEPT
```

```
iptables -t nat -A POSTROUTING -s 192.168.0.1/24 -o eth0 -j  
MASQUERADE
```

Nota: En función de las características de nuestra red y configuración de nuestro firewall es posible que tenga que implementar reglas adicionales a las que se muestran.

Con la primera de las reglas estamos permitiendo el tráfico por el dispositivo virtual en que se crea el túnel.

Con la segunda de las reglas estamos permitiendo que los paquetes provenientes de 192.168.0.1/24 pueden enviarse o salir por la interfaz de salida eth0.

Con la tercera de las reglas estamos diciendo al servidor OpenVPN que cuando reciba una petición de cualquiera de los clientes, proceda el mismo a resolverla y enviarla en representación del cliente. Una vez finalizado el proceso guardan el archivo y cierran el editor de textos.

Gráfico N° 14: Enrutamiento de peticiones

```
Máquina Ver Dispositivos Ayuda
GNU nano 2.2.6 Fichero: /etc/rc.local

# By default this script does nothing.
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQUERADE
iptables -A INPUT -p udp -i eth0 --dport 1194 -j ACCEPT
iptables -A FORWARD -i eth0 -o tun0 -m state --state ESTABLISHED,RELATED -j ACC$
iptables -A FORWARD -s 10.8.0.0/24 -o eth0 -j ACCEPT
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

/etc/init.d/dnsmasq restart

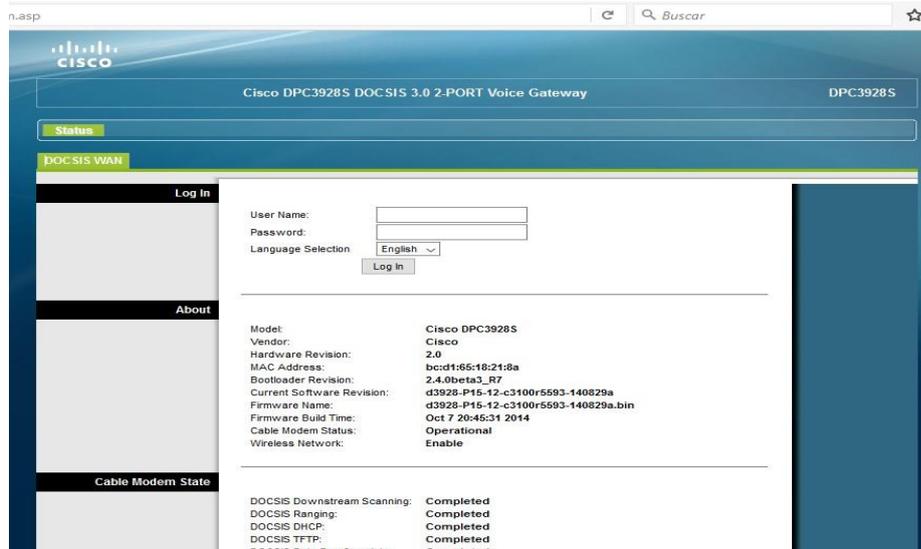
exit 0
_
```

Fuente: Elaboración propia

#### 15. Configurar el router y abrir el puerto del servidor OpenVPN

Ya para finalizar solo nos falta configurar nuestro router, para que redirija las peticiones de los clientes al servidor Opevpn, y abrir el puerto del servidor OpenVPN. Para realizar esto tenemos que abrir nuestro navegador y teclear nuestra puerta de entrada. Una vez realizado esto, tal y como se puede ver en la captura de pantalla, se abrirá una ventana en que nos pedirá nuestro nombre de usuario y contraseña:

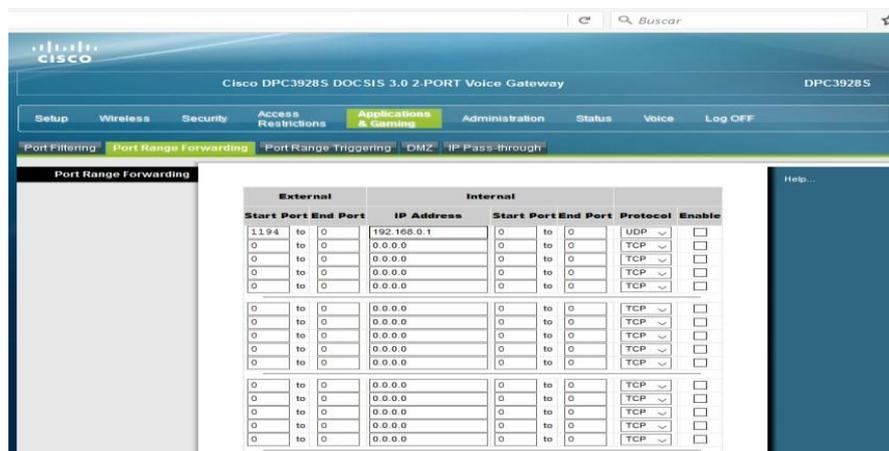
Gráfico N° 15: Accediendo al router



Fuente: Elaboración propia

Una vez introducida la información accederemos a la configuración de nuestro router. Seguidamente, tal y como se puede ver en la captura de pantalla, tenemos que acceder a los menús Applications & Gaming / Port Filtering

Gráfico N° 16: Configurando router



Fuente: elaboración propia

Como se puede ver en la captura de pantalla, en el campo custom server hay que escribir un nombre cualquiera. Seguidamente en el campo Server IP Address tenemos que escribir la IP del servidor OpenVPN. En este caso tal y como se puede ver en la captura de pantalla es la 192.168.0.1. Finalmente tal y como se puede ver en el Grafico Nro. 17 seleccionamos el protocolo UDP y escribimos el puerto de nuestro servidor OpenVPN (1194) en los puertos internos y externos.

Presionamos el botón Apply/Save y de esta forma todas las peticiones exteriores que lleguen a nuestro router por el puerto 1194 serán redirigidas a nuestro servidor OpenVPN.

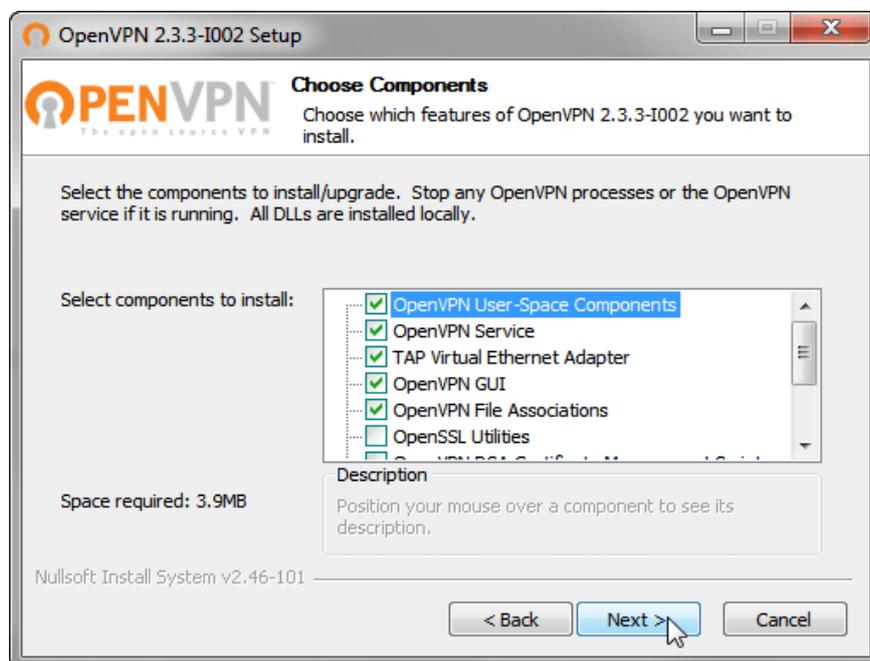
#### 16. Conectarse al servidor OpenVPN

En este punto debemos recopilar las claves necesarias para la conexión al servidor OpenVPN en Windows, OpenVPN funciona mediante certificados y claves RSA construidas con Openssl. Anteriormente ya creamos la totalidad de claves para que los usuarios puedan conectarse al servidor OpenVPN. Ahora que ya hemos hecho todo lo anterior.

Una vez que se haya hecho lo anterior procedemos a instalar el cliente de OpenVPN para Windows en cada una de las respectivas computadoras de la empresa, descargamos el cliente Openvpn para Windows que nos permitirá conectarnos a nuestro servidor OpenVPN, elegimos la versión según la arquitectura de la pc, luego de haberlo descargado clicamos el botón derecho del mouse y elegimos la opción “Ejecutar como administrador”. Una vez realizado esto empezará la instalación del cliente. Las etapas de la instalación serán las siguientes:

- Primero saldrá un mensaje de si deseamos que el programa que vamos a instalar realice cambios en el equipo. Nosotros debemos responder que Sí.
- Seguidamente aparecerá una ventana que bienvenida. Tan solo tenemos que presionar el botón Next.
- Luego, tal y como se puede ver en la captura de pantalla, aparecerá una ventana para seleccionar los componentes que instalaremos:

Gráfico N° 17: Selección de componentes de instalación



Fuente: elaboración propia

Dejaremos las opciones por defecto sin modificar nada y presionaremos el botón Next.

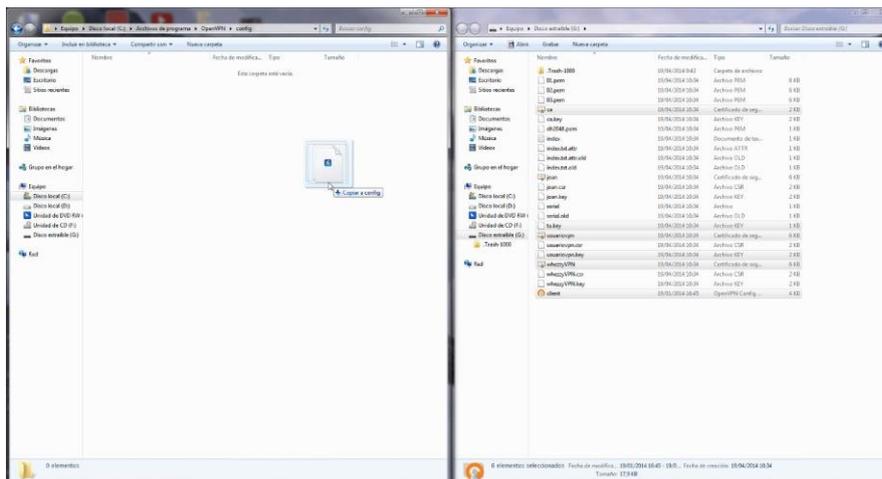
- En el cuarto paso aparecerá una ventana para seleccionar la ruta de instalación del programa. Dejamos la ruta por defecto, y presionamos el botón Next y empezará la instalación que será cuestión de segundos.

**Nota:** Es posible que durante la instalación os aparezca una ventana para que aceptes la instalación de un nuevo adaptador virtual de Red con nombre (TAP-Windows Provider). En el caso que aparezca la ventana tan solo tiene que presionar el botón Instalar.

- Una vez finalizada la instalación tan solo tenemos que presionar en el botón Next y en la siguiente ventana que aparezca presionamos el botón Finish.

Una vez realizados estos pasos hemos finalizado la instalación del cliente. También observarán que en el escritorio de windows habrá aparecido un icono de acceso directo al cliente OpenVPN. Tenemos que localizar el fichero client.conf. Una vez localizado el fichero client.conf deberemos cambiar su extensión a client.ovpn Una vez realizado esto ya podemos copiar las claves y el fichero de configuración del cliente del pendrive a la ubicación C:/Archivos de programa/OpenVPN/config

Gráfico N° 18: Copiar claves de usuario



Fuente: Elaboración propia

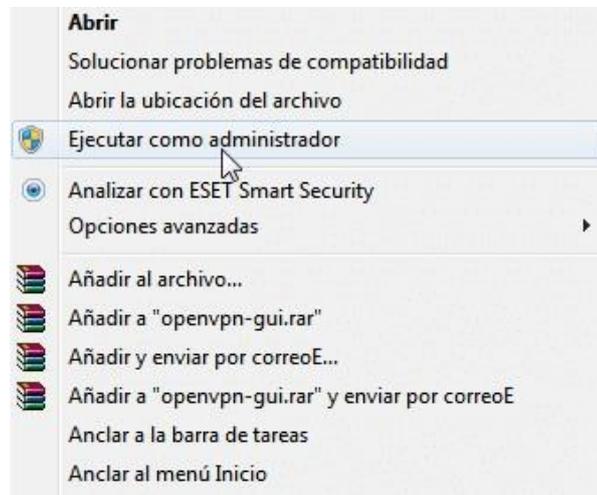
Tenemos que seleccionar los siguientes archivos del pendrive.

- ca.crt “Certificado raíz de la entidad certificadora”
- whezzyVPN.crt “Certificado del servidor VPN”
- usuariovpn.key “Clave privada del cliente VPN”
- usuariovpn.crt “Certificado del cliente VPN”
- ta.key “Clave de Autenticación TLS”
- client.ovpn “Fichero de configuración del cliente”

Posteriormente, también podemos ver en la captura de pantalla, tenemos que arrastrar los 6 archivos seleccionados dentro de la ventana con ubicación C:/Archivos de programa/OpenVPN/config. Una vez realizados estos pasos ya tenemos copiadas las claves y ficheros de configuración necesarios en nuestro cliente OpenVPN.

Para finalizar hay que conectarnos al servidor OpenVPN en Windows nos vamos a nuestro escritorio en el que encontraremos un icono de acceso directo al cliente OpenVPN.

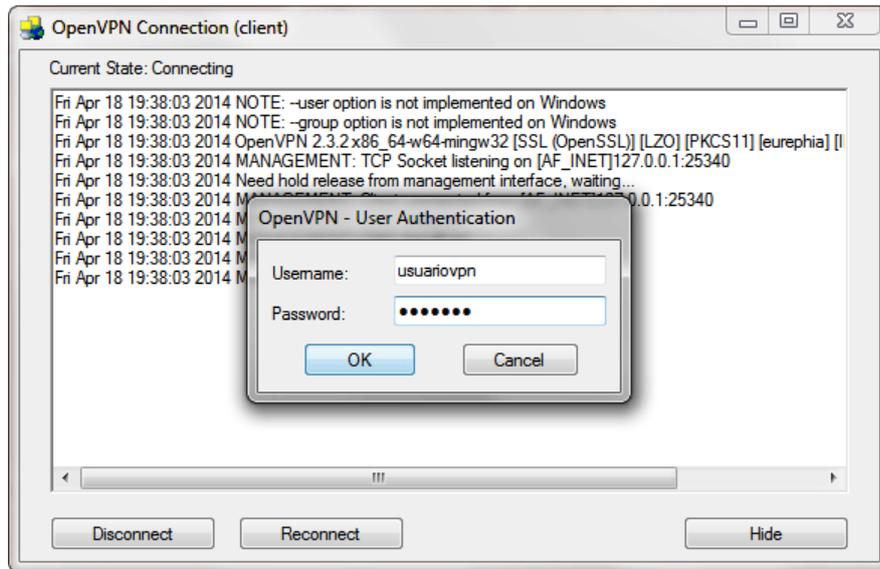
Gráfico N° 19: Ejecutar el programa OpenVPN



Fuente: Elaboración propia

Como vemos el en Grafico Nro. 25 presionamos con el botón derecho del mouse encima del icono del programa OpenVPN. Aparecerá una lista desplegable de opciones en la que deberemos seleccionar la opción “Ejecutar como administrador”

Gráfico N° 20: Ingresar Usuario

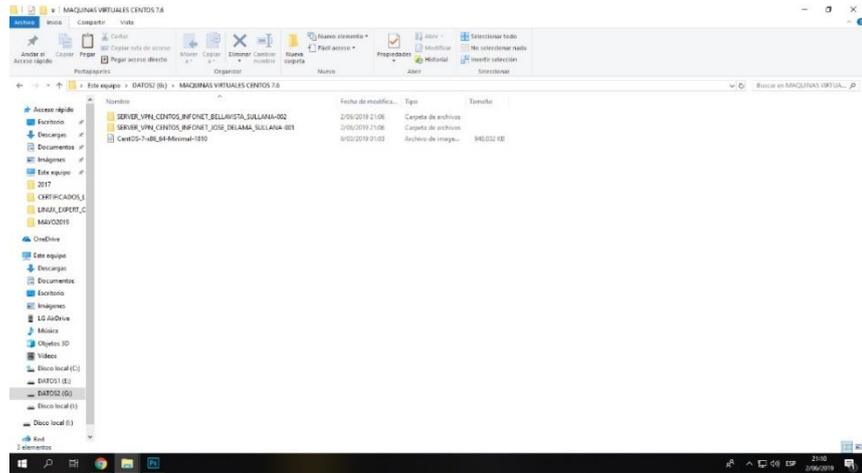


Fuente: Elaboración propia

Introducen el usuario y contraseña que creamos en la configuración del servidor y presionan el botón OK. Una vez presionado el botón OK esperan unos segundos y en la parte inferior de la pantalla les tiene que aparecer un mensaje diciendo el cliente está conectado ahora, en estos momentos ya estamos conectados al servidor OpenVPN en Windows, hasta este punto ya habremos finalizado con la instalación del servidor y la conexión de un usuario al servidor VPN tener en cuenta que este procedimientos se hace para cada uno de los usuarios que quieran conectarse a la red privada virtual de la empresa Agromar Industrial previamente con sus credenciales configuradas.

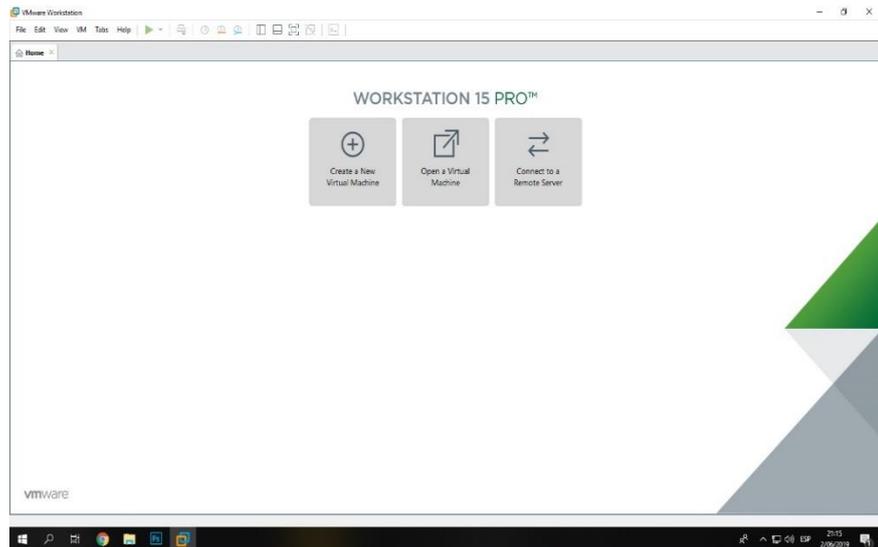
## Creación de máquina virtual

Gráfico N° 21: Máquina Virtual



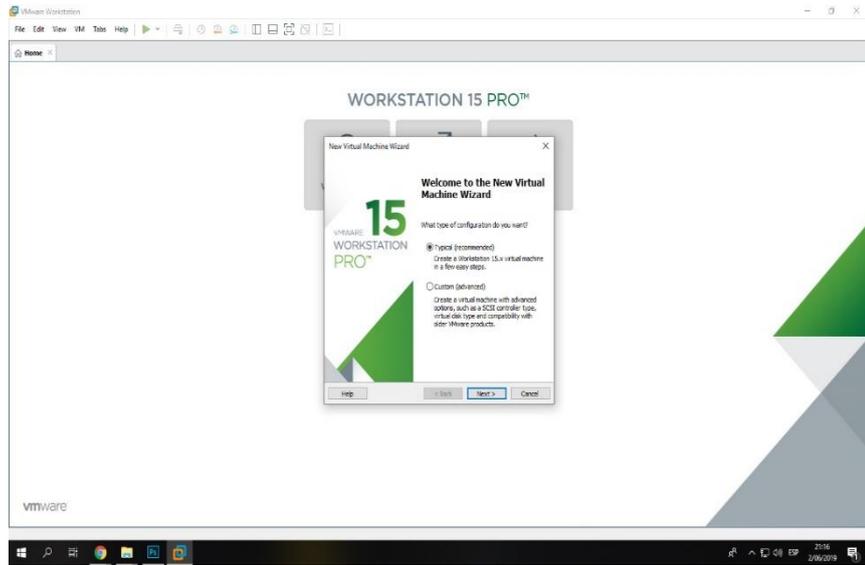
Fuente: Elaboración propia

Gráfico N° 24: Fondo de Máquina Virtual



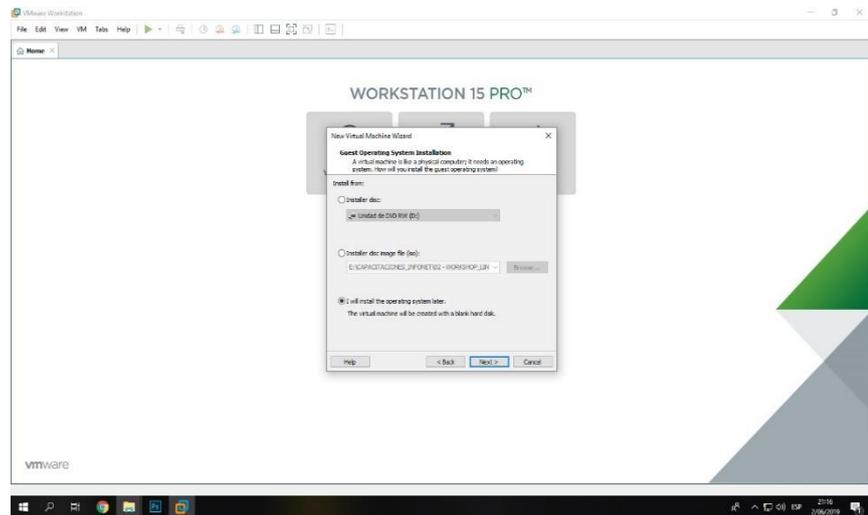
Fuente: Elaboración propia

Gráfico N° 27: Comienzo de Instalación



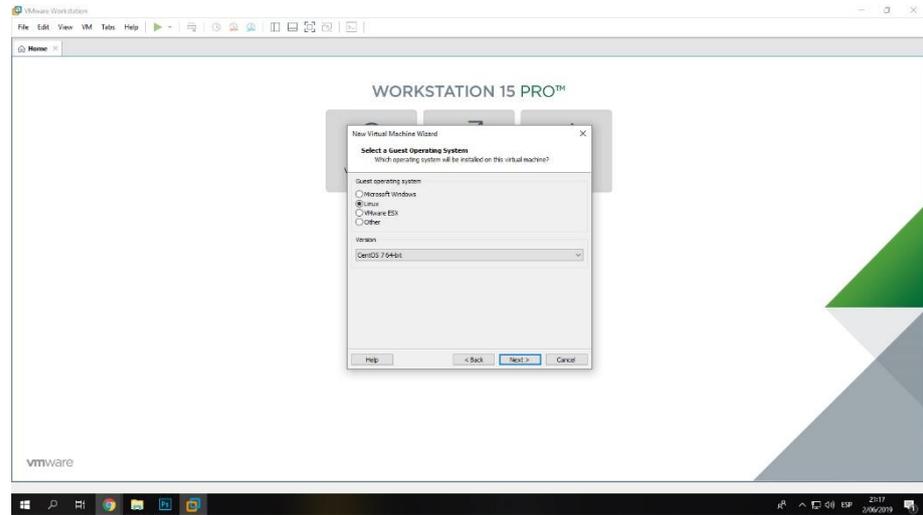
Fuente: Elaboración propia

Gráfico N° 30: Unidad de Instalación



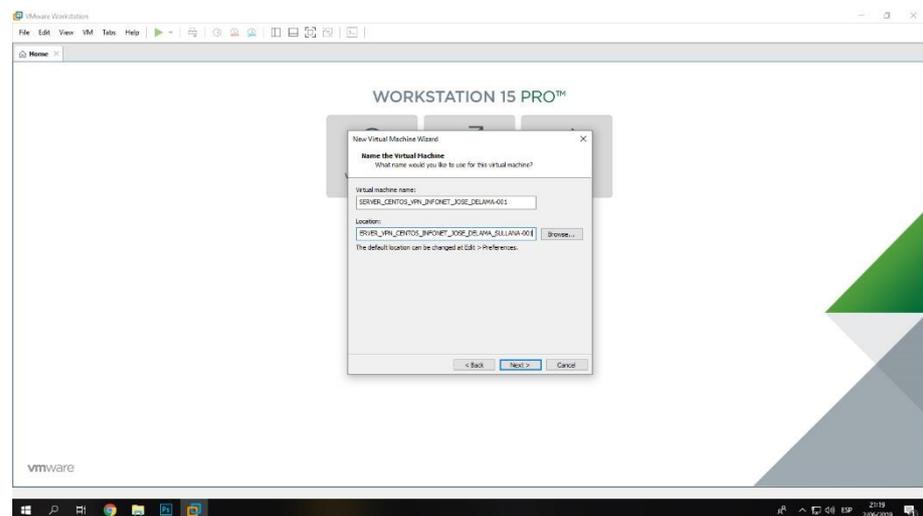
Fuente: Elaboración propia

Gráfico N° 33: Elección del S.O



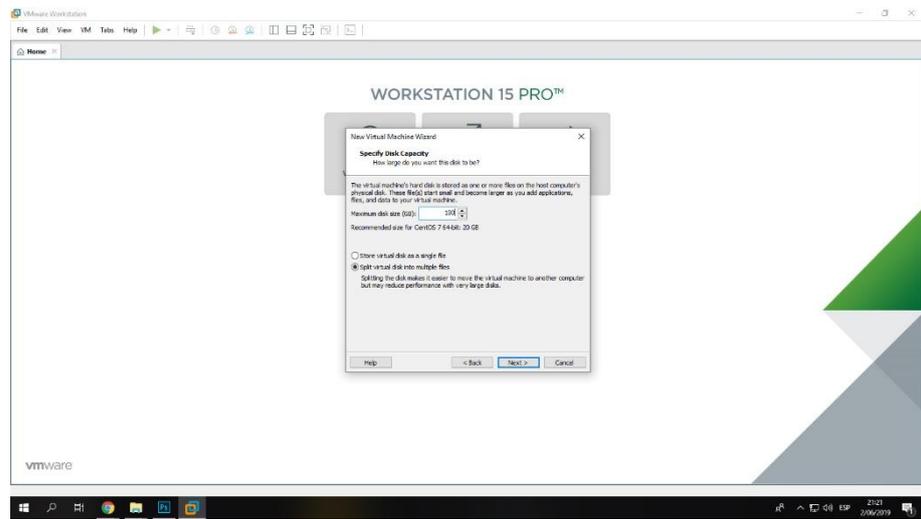
Fuente: Elaboración propia

Gráfico N° 36: Ubicación del Primer Servidor



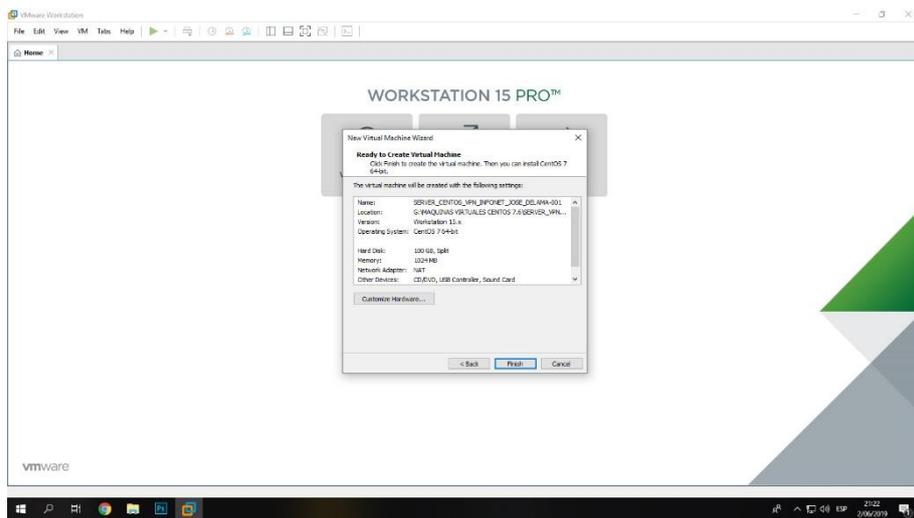
Fuente: Elaboración propia

Gráfico N° 39: Tamaño del Disco



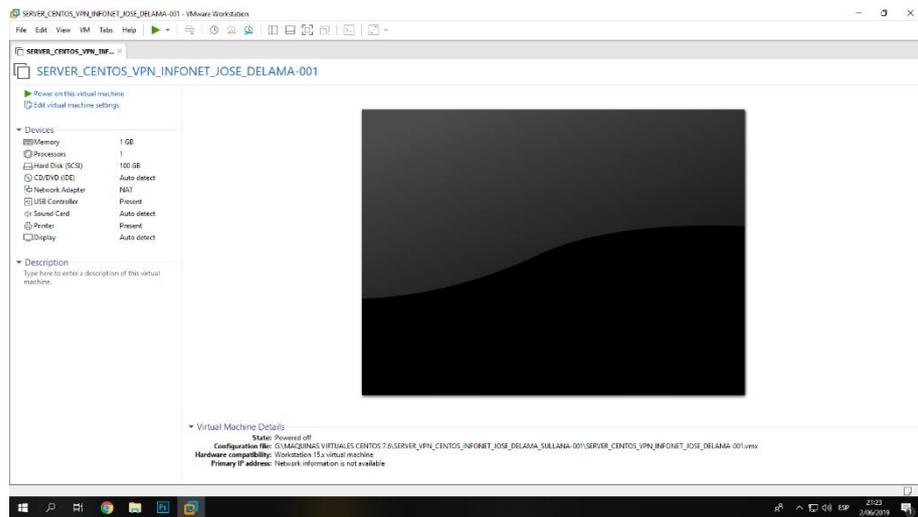
Fuente: Elaboración propia

Gráfico N° 42: Verificación de Información



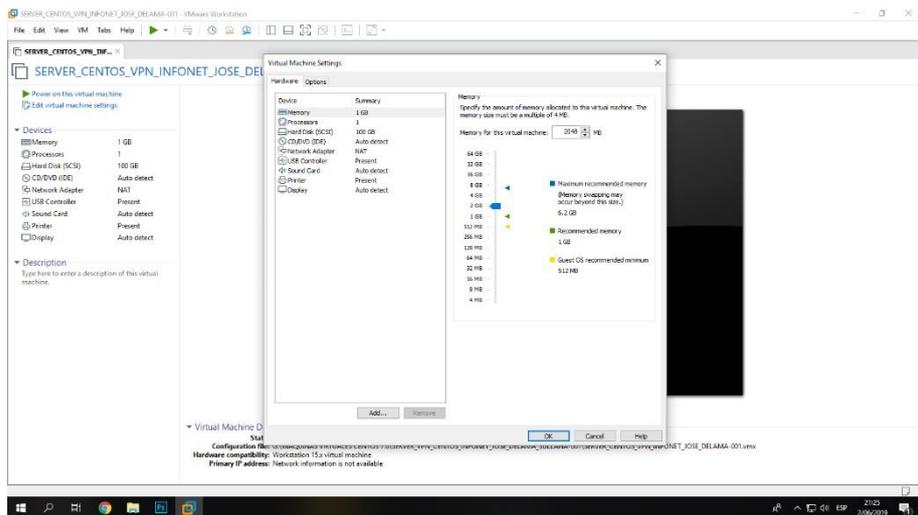
Fuente: Elaboración propia

Gráfico N° 45: Inicio del Primer Servidor



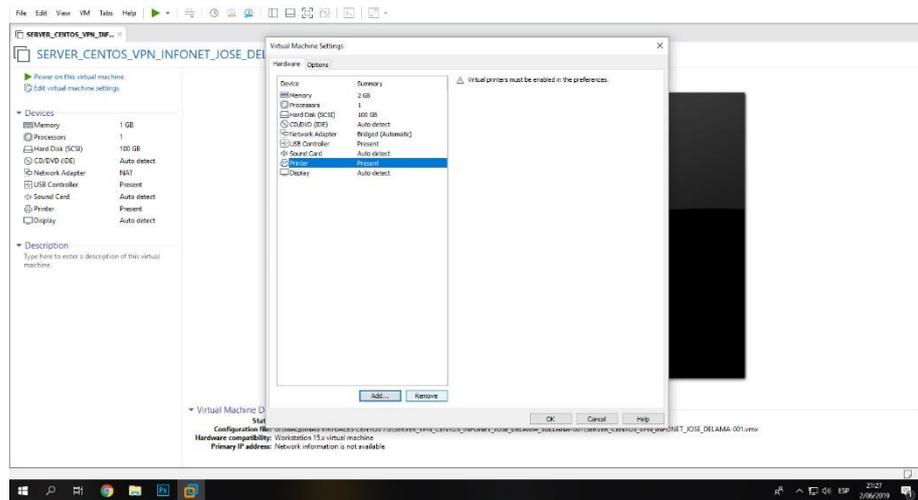
Fuente: Elaboración propia

Gráfico N° 48: Tamaño de la Ram



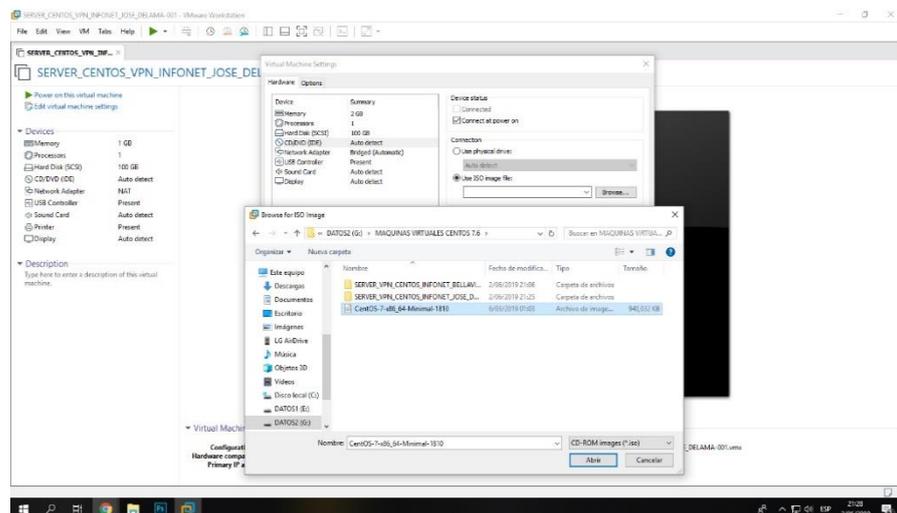
Fuente: Elaboración propia

Gráfico N° 51: Configuración Terminada del Primer Servidor



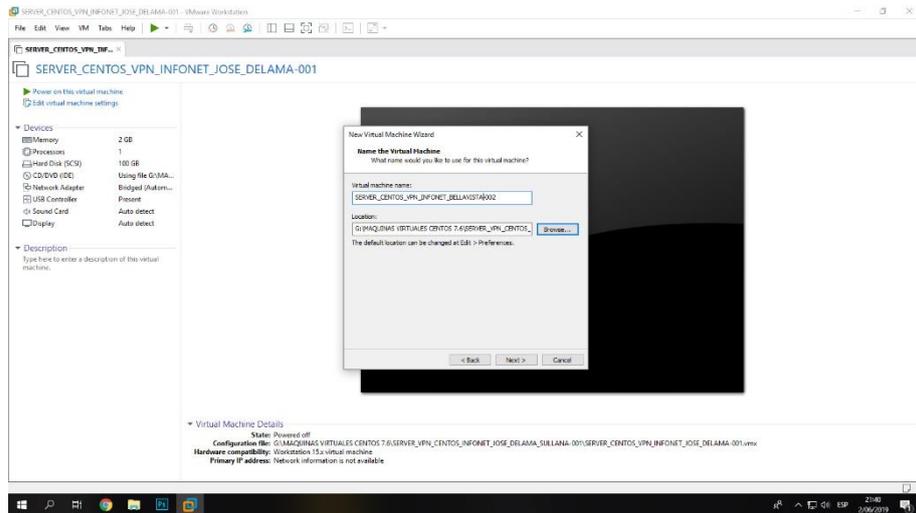
Fuente: Elaboración propia

Gráfico N° 54: Instalación de Segundo Servidor



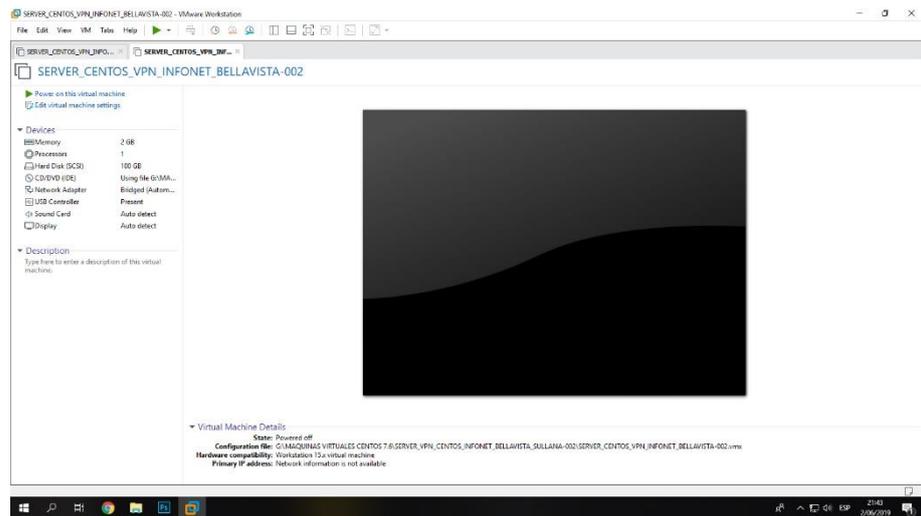
Fuente: Elaboración propia

Gráfico N° 57: Ubicación del Segundo Servidor



Fuente: Elaboración propia

Gráfico N° 60: Inicio del Segundo Servidor



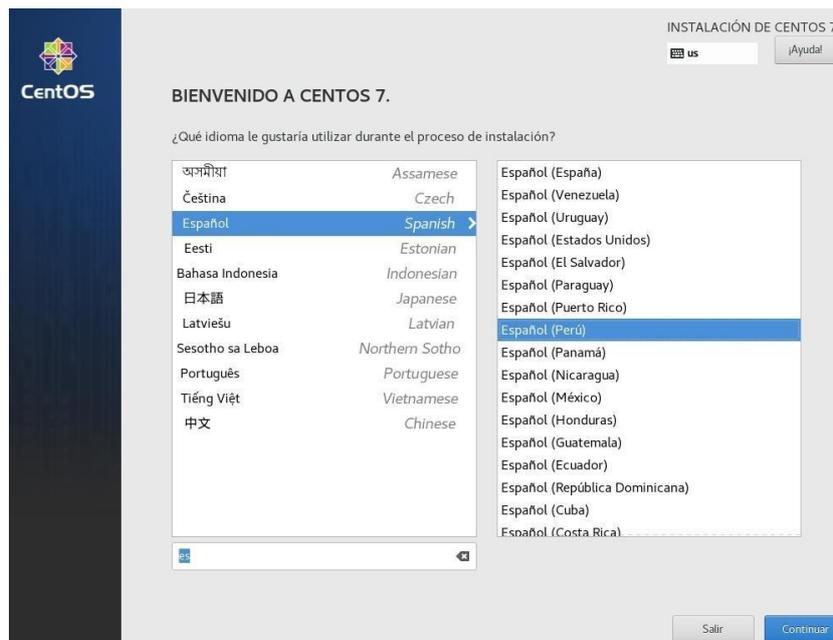
Fuente: Elaboración propia

Gráfico N° 35: Instalación de Centos



Fuente: Elaboración propia

Gráfico N° 36: Configuración de Idioma



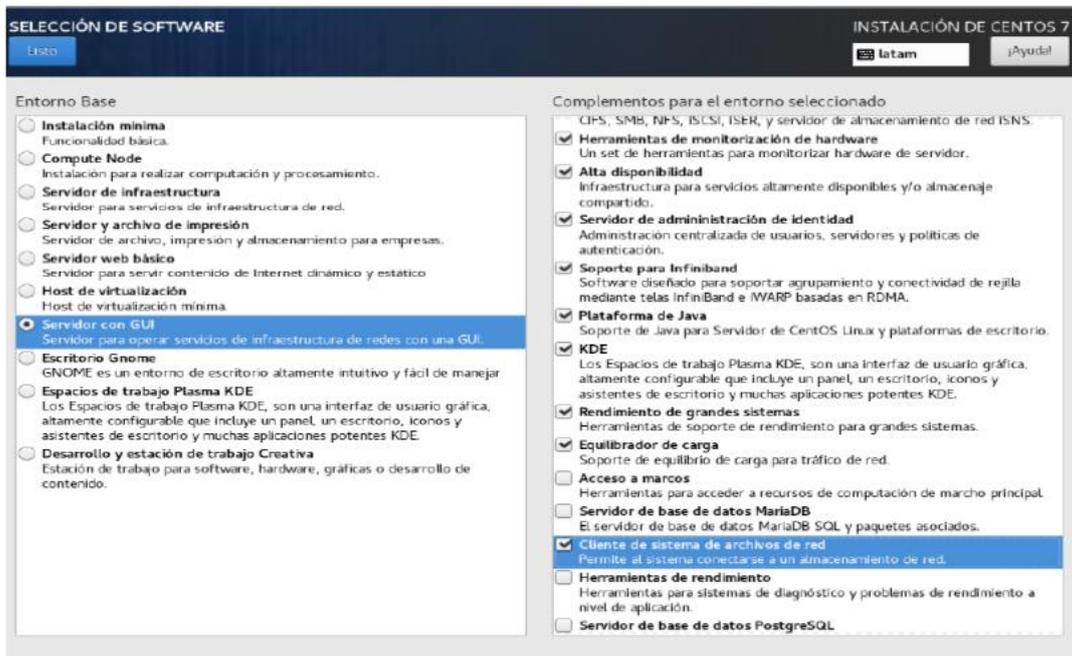
Fuente: Elaboración propia

Gráfico N° 37: Elección de configuración



Fuente: Elaboración propia

Gráfico N° 38: Selección de software



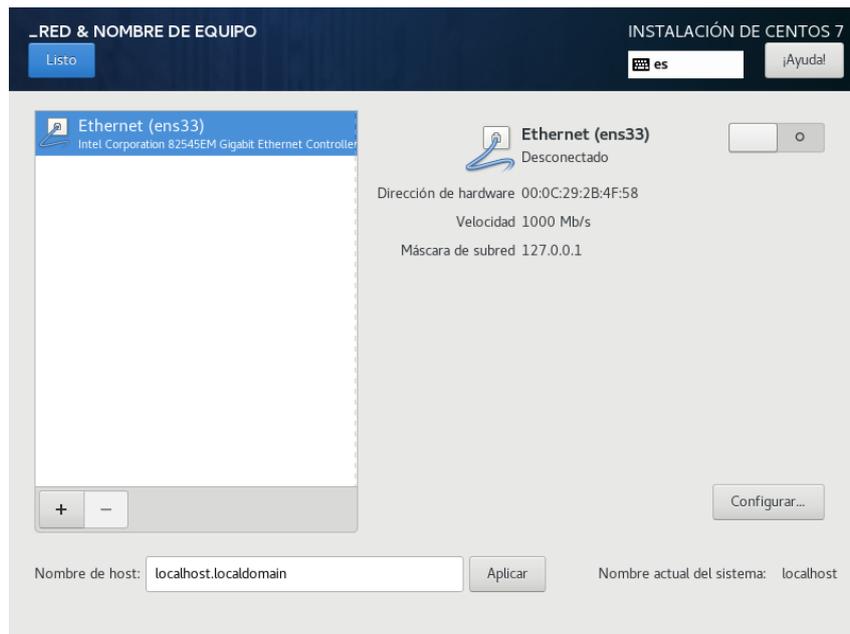
Fuente: Elaboración propia

Gráfico N° 39: Destino de instalación



Fuente: Elaboración propia

Gráfico N° 40: Configuración de red



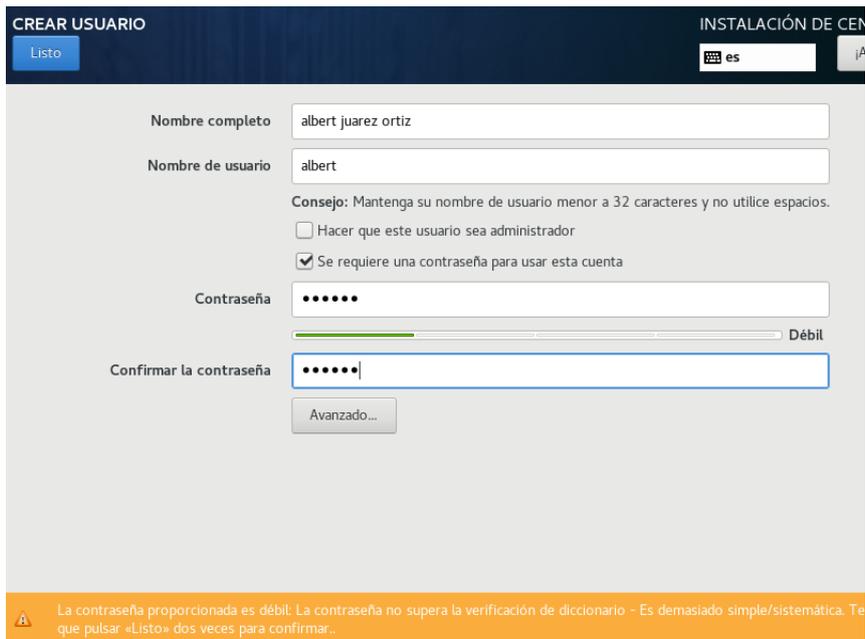
Fuente: Elaboración propia

Gráfico N° 41: Inicio de instalación



Fuente: Elaboración propia

Gráfico N° 42: Configuración de usuario



Fuente: Elaboración propia

Gráfico N° 43: Reinicio de instalación



Fuente: Elaboración propia

Gráfico N° 44: Aceptación de licencia



Fuente: Elaboración propia

Gráfico N° 45: Login de acceso

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64

josedelama login: root
Password:
[root@josedelama ~]# ls /sys/class/net/
ens33  lo
[root@josedelama ~]# _
```

Fuente: Elaboración propia

## VI. CONCLUSIONES

De acuerdo a los resultados obtenidos en el estudio para la propuesta de implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020, queda confirmada la necesidad prioritaria de solucionar los problemas de comunicación y acceso a la información que tiene actualmente la empresa Infonet Soluciones E.I.R.L, ya sea para el beneficio de la empresa como para los clientes, lo cual este resultado es similar al indicado a la hipótesis general por lo que se concluye que la hipótesis general queda aceptada.

1. En la Tabla Nro. 10 se puede determinar que el 80% de los trabajadores indicó que el acceso de la información es insuficiente, lo cual este resultado es similar al indicado en la hipótesis específica lo que me permite identificar los requerimientos que satisfagan las necesidades de la empresa al igual que a los clientes, por lo que se concluye que la hipótesis específica queda aceptada.
2. En la Tabla Nro. 16 se puede observar que el 60% de los trabajadores respondió que la seguridad es la más óptima y que no existen políticas de seguridad lo cual requiere un estudio de las tecnologías para determinar la más adecuada y difundirlas dentro de lo que cabe, lo cual este resultado es similar al indicado en la hipótesis específica en el trabajo de investigación; por lo que se concluye que la hipótesis específica queda aceptada.
3. En la Tabla Nro. 22 se puede interpretar que el 80% de los trabajadores expreso que están de acuerdo con la propuesta de implementación de una red privada virtual porque creen que beneficiara a la empresa y en su trabajo diario, llegando a evitar demoras en el traslado de información al

igual que sus procesos serán muchos más óptimos y seguros, este resultado es similar al indicado en la hipótesis específica, por lo que se concluye que la hipótesis específica queda aceptada.

## **RECOMENDACIONES**

1. Es conveniente que la empresa implemente políticas orientadas a la protección e integridad de la información con la que trabaja.
2. El diseño de la red privada virtual es prioridad pero esta se debe realizar cumpliendo con los lineamientos que permitan que la red privada virtual sea creíble con las nuevas tecnologías y se adapte a las ya alcanzada por la empresa sin tener necesidad alguna de volver a modelar una nueva red.
3. Dar anticipación a la viabilidad de la propuesta económica dentro del presupuesto de la entidad para su subsiguiente implementación.

## REFERENCIAS BIBLIOGRÁFICAS

1. MARQUÈS G. REDES VIRTUALES SSL (WEB VPN) LULU.COM , EDITOR.; 2016.
2. VASQUEZ DFN. DISEÑO DE UN MODELO DE VIRTUALIZACIÓN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE SERVIDORES EN ALTA DISPONIBILIDAD. TESIS LICENCIATURA. BOGOTÁ: UNIVERSIDAD COOPERATIVA DE COLOMBIA, DEPARTAMENTO DE INGENIERIA; 2020.
3. JOTA FONSECA YM, RAMIREZ CASTAÑEDA DS, PENAGOS AREVALO AR. DISEÑO DE UNA RED PRIVADA VIRTUAL (VPN) CON SEGURIDAD L2PT PARA LA EMPRESA LABORATORIOS EXPOFARMA S.A. TESIS. BOGOTÁ: UNIVERSIDAD COOPERATIVA DE COLOMBIA, DEPARTAMENTO DE SISTEMAS; 2018.
4. ROMERO LÓPEZ JP, ROMERO LÓPEZ CE. FRONTERAS DE SEGURIDAD EN REDES PRIVADAS VIRTUALES (VPN). TESIS DE GRADO. PEREIRA: UNIVERSIDAD TECNOLÓGICA DE PEREIRA, DEPARTAMENTO DE INGENIERIA DE SISTEMAS; 2016.
5. MARTEL VELASQUEZ VR. DISEÑO DE UNA RED DE COMUNICACIÓN VPN SOBRE INTERNET PARA UN DISTRIBUIDOR AUTORIZADO DE CLARO BASADO EN EL RFC 2764. TESIS. LIMA: UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS, DEPARTAMENTO DE INGENIERÍA; 2019.
6. ESPINOZA CHIPANE CR. PROPUESTA DE UNA RED PRIVADA VIRTUAL PARA MEJORAR EL SERVICIO DE COMUNICACIÓN EN LAS TIENDAS MASS PARA LA EMPRESA SUPERMERCADOS PERUANOS S.A. TESIS BACHILLER. LIMA: UNIVERSIDAD AUTÓNOMA DEL PERÚ, DEPARTAMENTO INGENIERÍA; 2018.

7. ATENCIO MENDOZA AI, MAMANI FIGUEROA EJ. DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE RED PRIVADA VIRTUAL EN CAPA 3 UTILIZANDO CISCO IOS PARA LA UNIVERSIDAD NACIONAL DEL ALTIPLANO. TESIS. PUNO: UNIVERSIDAD NACIONAL DEL ALTIPLANO, DEPARTAMENTO DE INGENIERÍA; 2017.
8. ZAVALA BOULANGGER FE. REINGENIERÍA DE LA INFRAESTRUCTURA DE LA RED DE DATOS ADMINISTRADA CON WINDOWS SERVER EN CONSORCIO SUPERVISOR EDUCA. TESIS. PIURA: UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE, DEPARTAMENTO DE INGENIERÍA; 2020.
9. CASTILLO HUANCAS JS. PROPUESTA DE REINGENIERÍA DE UNA RED DE DATOS PARA LA MUNICIPALIDAD DISTRITAL DE SALITRAL. TESIS. MORROPÓN : UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE, FACULTAD DE INGENIERÍA; 2018.
10. CRIOLLO LANDACAY I. DISEÑO PARA LA IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL (VPN) EN LA EMPRESA AGROMAR INDUSTRIAL S.A. TESIS. SULLANA: UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE, FACULTAD DE INGENIERÍA; 2017.
11. ALVARADO F. CONSEJERIA EMPRESARIAL. [ONLINE]. [CITED 2018 NOVIEMBRE 07. AVAILABLE FROM: [HTTP://WWW.CONSEJERIAEMPRESARIAL.COM/PUBLICACIONES/PRINCIPIOS%20BASICOS%20DE%20CONSULTORIA.PDF](http://www.consejeriaempresarial.com/publicaciones/principios%20basicos%20de%20consultoria.pdf).
12. MOODLE. [ONLINE].; 2018 [CITED 2018 ABRIL 27. AVAILABLE FROM: [HTTP://MOODLE2.UNID.EDU.MX/DTS\\_CURSOS\\_MDL/LIC/TIC/IT/S01/IT01\\_LECTURA.PDF](http://moodle2.unid.edu.mx/dts_cursos_mdL/LIC/TIC/IT/S01/IT01_LECTURA.PDF).
13. VERA ÁA. INSTALACIÓN Y PARAMETRIZACIÓN DEL SOFTWARE (UF1893). PRIMERA ED. MADRID: IC EDITORIAL; 2014.
14. PÉREZ JCM, PÉREZ AFR. ADMINISTRACIÓN DE SOFTWARE DE UN SISTEMA INFORMÁTICO. PRIMERA ED. MADRID: RA-MA EDITORIAL; 2014.

15. MANZANARES MCS, GARCÍA EM. METODOLOGÍAS ACTIVAS EN DOCENCIA UNIVERSITARIA: DISEÑO DE UNA ASIGNATURA DE CIENCIAS DE LA SALUD EN LA PLATAFORMA VIRTUAL MADRID: EDITORIAL UNIVERSIDAD DE BURGOS; 2016.
16. SANTOS JC. SEGURIDAD INFORMÁTICA. PRIMERA ED. MADRID: RA-MA EDITORIAL; 2014.
17. COLMENAREJO JB, LANCEROS AG, MAS AM, PAZOS JAS, GALLO EV. REDES DE TELECOMUNICACIONES Y ORDENADORES. PRIMERA ED. MADRID: DIAZ DE SANTOS S.A.; 2014.
18. ESCALONA AS. TECNOLOGÍAS DE ACCESO PARA LAS ICTS. EL INSTALADOR, LOS SERVICIOS Y LAS REDES DE TELECOMUNICACIONES BARCELONA: EDICIONES EXPERIENCIA; 2015.
19. PALMA E. ACADEMIA EDU. [ONLINE]. [CITED 2018 NOVIEMBRE 07. AVAILABLE FROM: [HTTPS://WWW.ACADEMIA.EDU/11646101/INTRODUCCION\\_A\\_VPN\\_REDES\\_PRIVADAS\\_VIRTUALES](https://www.academia.edu/11646101/introduccion_a_vpn_redes_privadas_virtuales).
20. LITORAL UND. UNIVERSIDAD NACIONAL DEL LITORAL. [ONLINE]. [CITED 2018 NOVIEMBRE 07. AVAILABLE FROM: [HTTP://WWW.FCA.UNL.EDU.AR/INFORMATICABASICA/REDES.PDF](http://www.fca.unl.edu.ar/informaticabasica/redes.pdf).
21. TELEPIEZA. TELEPIEZA. [ONLINE].; 2016 [CITED 2018 NOVIEMBRE 07. AVAILABLE FROM: [HTTPS://WWW.TELEPIEZA.COM/WORDPRESS/2008/04/28/LOS-7-NIVELES-O-CAPAS-DEL-MODELO-OSI/#COMMENTS](https://www.telepieza.com/wordpress/2008/04/28/los-7-niveles-o-capas-del-modelo-osi/#comments).
22. UNICEN. [ONLINE].; 2015 [CITED 2018 NOVIEMBRE 13. AVAILABLE FROM: [HTTP://WWW.EXA.UNICEN.EDU.AR/CATEDRAS/COMDAT1/MATERIAL/ELMODELOOSI.PDF](http://www.exa.unicen.edu.ar/catedras/comdat1/material/elmodeloosi.pdf).
23. BLYX. [ONLINE].; 2015 [CITED 2018 NOVIEMBRE 13. AVAILABLE FROM: [HTTPS://BLYX.COM/PUBLIC/DOCS/PILA\\_OSI.PDF](https://blyx.com/public/docs/pila_osi.pdf).

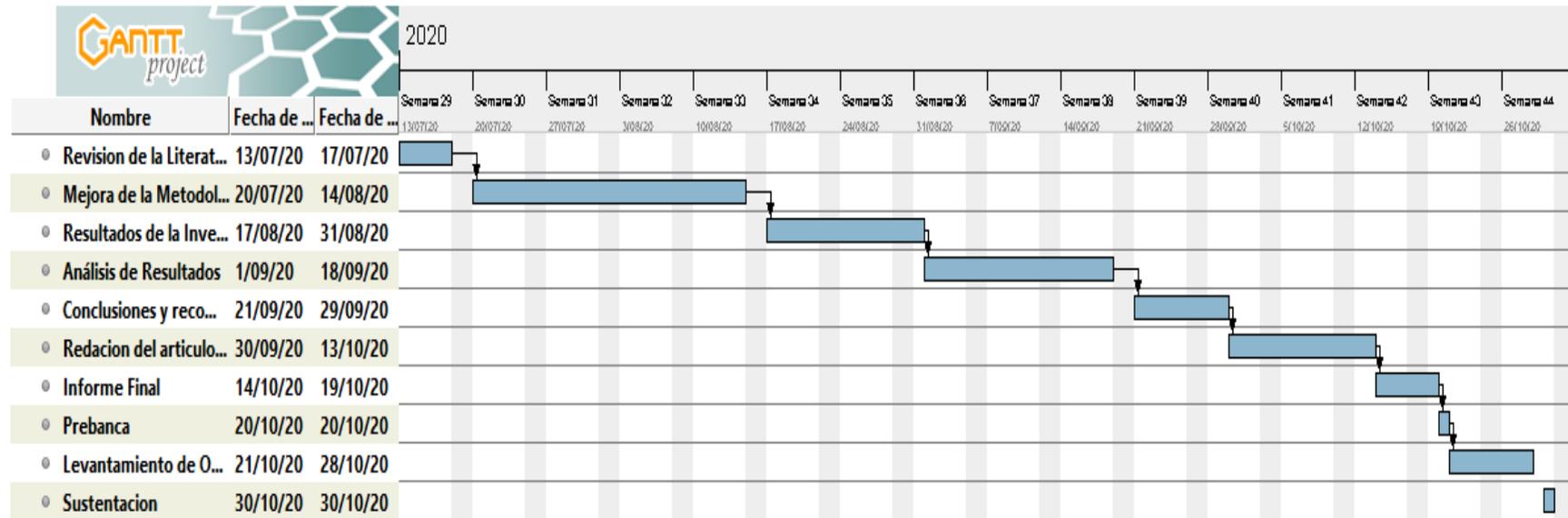
24. GONZÁLEZ MS. DISEÑO DE REDES TELEMÁTICAS MADRID: RA-MA EDITORIAL; 2014.
25. RIVERO AL. REDES Y COMPETENCIA TECNOLÓGICA EN LA CONSTRUCCIÓN DE ESTÁNDARES AZCAPOTZALCO; 2015.
26. ALICIA RAMOS MARTÍN MJRMSVV. MONTAJE Y MANTENIMIENTO DE EQUIPOS. PRIMERA ED. MADRID: MCGRAW-HILL; 2014.
27. REDES DE COMPUTADORAS. [ONLINE]. [CITED 2018 JULIO 19. AVAILABLE FROM: [HTTP://WWW.FCA.UNL.EDU.AR/INFORMATICABASICA/REDES.PDF](http://www.fca.unl.edu.ar/informaticabasica/reDES.pdf).
28. OLIVA NCGMADOG. REDES DE COMUNICACIONES INDUSTRIALES MADRID: UNED - UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA; 2014.
29. MORENO JA. REDES DE COMUNICACIONES BARCELONA: UOC; 2013.
30. HILLAR GC. REDES: DISEÑO, ACTUALIZACIÓN Y REPARACIÓN BUENO AIRES: HISPANO AMERICANA HASA; 2015.
31. BUENDÍA JFR. SEGURIDAD INFORMÁTICA MADRID: MCGRAW-HIL; 2014.
32. DELGADO DÁ, CÁCERES CJ, JORQUERA GS, ESQUIVEL CZ. ELO-322: REDES DE COMPUTADORES I. [ONLINE].; 2014 [CITED 2018 JULIO 19. AVAILABLE FROM: [HTTP://PROFESORES.ELO.UTFSM.CL/~AGV/ELO322/1S14/PROJECTS/REPORTS/G20/REDES%20PRIVADAS%20VIRTUALES%20%28VPN%29.PDF](http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/g20/reDES%20PRIVADAS%20VIRTUALES%20%28VPN%29.pdf).
33. CISCO. CISCO. [ONLINE]. [CITED 2018 NOVIEMBRE 07. AVAILABLE FROM: [HTTPS://WWW.CISCO.COM/C/EN/US/PRODUCTS/IOS-NX-OS-SOFTWARE/TUNNELING/INDEX.HTML](https://www.cisco.com/c/en/us/products/ios-nx-os-software/tunneling/index.html).
34. VIÑAS RB, LLINÀS FA. SOFTLIBRE. [ONLINE]. [CITED 2018 NOVIEMBRE 07. AVAILABLE FROM: [HTTP://SOFTLIBRE.UNIZAR.ES/MANUALES/LINUX/868.PDF](http://softlibre.unizar.es/manuales/linux/868.pdf).

35. ZAVALETA P. SCRIBD. [ONLINE]. [CITED 2018 NOVIEMBRE 07. AVAILABLE FROM: <HTTPS://ES.SCRIBD.COM/DOCUMENT/274948908/CENTOS-PDF>.
36. FERNÁNDEZ PYDP. INVESTIGACIÓN CUANTITATIVA. PRIMERA ED.; 2015.
37. T T. METODOLOGIA DE LA INVESTIGACION. PRIMERA ED.; 2014.
38. SABINO. LA INVESTIGACIÓN DE TIPO DESCRIPTIVA TRABAJA SOBRE REALIDADES DE HECHOS, Y SU CARACTERÍSTICA FUNDAMENTAL ES LA DE PRESENTAR UNA INTERPRETACIÓN CORRECTA. PRIMERA ED.; 2015.
39. SHADISH W CTCD. TIPO DE ESTUDIO Y DISEÑO. PRIMERA ED.; 2014.
40. SEEHORN A. MÉTODOS DE INVESTIGACIÓN DE CORTE TRANSVERSAL. PRIMERA ED.; 2014.
41. P. J. TESIS DE INVESTIGACIÓN. [ONLINE].; 2015 [CITED 2018 NOVIEMBRE 09. AVAILABLE FROM: <HTTP://TESISDEINVESTIG.BLOGSPOT.COM/2013/06/POBLACIONMUESTRAEJEMPLO.HTML>.
42. J C. UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. [ONLINE].; 2014 [CITED 2018 NOVIEMBRE 09. AVAILABLE FROM: <WWW.INGENIERIA.UNAM.MX/INDUSTRIALES/DESCARGAS/DOCUMENTOS/CATEDRA/APUNTESDSP.DOC>.
43. M R. TECHTARGET. [ONLINE].; 2016 [CITED 2018 NOVIEMBRE 09. AVAILABLE FROM: <HTTP://SEARCHENTERPRISEWAN.TECHTARGET.COM/DEFINITION/VIRTUAL-PRIVATE-NETWORK>.
44. D D. DISEÑO Y ELABORACIÓN DE CUESTIONARIOS PARA LA INVESTIGACIÓN COMERCIAL. PRIMERA ED. ESPAÑA; 2014.
45. CASAS J RLDC. LA ENCUESTA COMO TÉCNICA DE INVESTIGACIÓN. [ONLINE].; 2015 [CITED 2018 NOVIEMBRE 09. AVAILABLE FROM: <HTTP://EXTERNAL.DOYMA.ES/PDF/27/27V31N08A13047738PDF001.PDF>.



# **ANEXOS**

## ANEXO I: CRONOGRAMA DE ACTIVIDADES



Fuente: Elaboración Propia.

## ANEXO II: PRESUPUESTO

<b>Presupuesto desembolsable (Estudiante)</b>			
Categoría	Base	Costo Unitario	Total (S/.)
<b>Suministros</b>			
• Impresiones	0.3	200	60.00
• Fotocopias	0.1	60	6.00
• Empastado	30	2	60.00
• Agenda	15	1	15.00
• Lapiceros	3	4	12.00
• USB	20	1	20.00
<b>Servicios</b>			
• Uso de Turnitin	100	1	100.00
• Uso de Internet	50	4	200.00
<b>Gastos de Viaje</b>			
• Pasajes Interprovinciales	40	4	160.00
• Pasajes Locales	5	8	40.00
<b>Total, de Presupuesto Desembolsable</b>			673.00
<b>Presupuesto no desembolsable (Universidad)</b>			
Categoría	Base	Costo Unitario	Total (S/.)
<b>Servicios</b>			
Uso de Internet Laboratorio de Aprendizaje Digital - LAD	30	4	120.00
Búsqueda de información en base de datos	35	2	70.00
Soporte informático (Modulo de Investigación del ERP University - MOIC)	40	4	160.00
Publicación de artículo en repositorio institucional	50	1	50.00
<b>Recurso Humano</b>			
Asesoría Personalizada (5 horas por semana)	63	16	1,008.00
<b>Total, de Presupuesto No Desembolsable</b>			1408.00
<b>Total (S/.)</b>			2081.00

Fuente: Elaboración Propia.

### ANEXO III: CUESTIONARIO

El presente cuestionario forma parte del trabajo de investigación, para la Propuesta de Implementación Diseño De Una Red Privada Virtual Segura Corporativa Con Linux En Una Plataforma Virtualizada Mixta Para La Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

Por lo que solicitamos su participación, respondiendo a cada pregunta de manera objetiva y veraz, la información a proporcionar es de carácter confidencial y reservado y los resultados serán utilizados sólo para la presente investigación.

**Instrucciones:**

A continuación, se le presenta 15 preguntas en 3 diferentes dimensiones en la que deberán contestar, marcando con un aspa “X” en el recuadro correspondiente (Si o No) según considere la alternativa correcta.

Ítem	Preguntas	Alternativa	
		Si	No
<b>Dimensión 01: Nivel de Acceso A La Información</b>			
1	¿Cuenta con disponibilidad de la información entre las áreas?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
2	¿Existe eficacia con el servicio de acceso a la información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
3	¿Emplea algún medio físico (memoria, disco duro) para compartir información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
4	¿La velocidad de transmisión de datos actual es óptima?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		

5	¿Actualmente puede compartir sus archivos mediante la red o con otro compañero de trabajo?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
---	--	--	--

<b>Dimensión 02: Nivel de Seguridad De Red</b>			
--	--	--	--

6	¿Según usted cree que existen medidas de seguridad para proteger la información que comparte?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
7	¿Existe autenticación de usuarios en el intercambio de la información, que se realizan mediante los sistemas?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
8	¿Hay privilegios de los usuarios, respecto al uso de los sistemas de información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
9	¿Cree que hay políticas de seguridad en el uso de la Red e Internet?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
10	¿Cree usted que hay prevención, detección y corrección de Software malicioso?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		

<b>Dimensión 03: Nivel de Diseño De Red Privada Virtual</b>			
11	¿Cree necesario realizar un diseño de una red privada virtual segura corporativa con Linux en una plataforma Virtualizada mixta para la empresa Infonet Soluciones E.I.R.L - Sullana; 2020?		
12	¿A su criterio piensa o cree que una red privada virtual le simplificaría el trabajo diario?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
13	¿Cree usted que una eventual implementación de una red privada virtual beneficiaría a los trabajadores de la empresa?, Infonet Soluciones E.I.R.L - Sullana; 2020?		
14	¿Piensa que la implementación de una red privada virtual permitiría un mejor acceso a la información?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.		
15	¿Usted cree que la implementación de una red privada virtual ayudaría a mejorar la privacidad de la información y proteger los activos de la empresa?, Infonet Soluciones E.I.R.L- Sullana; 2020.		

Fuente: elaboración propia

## ANEXO IV: PROTOCOLO DE CONSENTIMIENTO INFORMADO



### PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS (Ingeniería y Tecnología)

La finalidad de este protocolo en Ingeniería y tecnología es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, el investigador y usted se quedarán con una copia.

La presente investigación se Propuesta De Implementación De Una Red Privada Virtual Segura Corporativa Con Linux En Una Plataforma Virtualizada Mixta Para La Empresa Infonet Soluciones E.I.R.L - SULLANA; 2020 y es dirigido por Albert Ignacio Juárez Ortiz, investigador de la Universidad Católica Los Ángeles de Chimbote.

El propósito de la investigación es Proponer la implementación de una Red Privada Virtual Segura Corporativa con Linux En Una Plataforma Virtualizada Mixta en la Empresa Infonet Soluciones E.I.R.L – Sullana, para optimizar la transmisión de la información.

Para ello, se le invita a participar en una encuesta que le tomará 15 minutos de su tiempo. Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través de correo electrónico. Si desea, también podrá escribir al correo [albert.jortiz96@gmail.com](mailto:albert.jortiz96@gmail.com) para recibir mayor información. Asimismo, para consultas sobre aspectos éticos, puede comunicarse con el Comité de Ética de la Investigación de la universidad Católica los Ángeles de Chimbote.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Carmen Amelia Ortiz Maza

Fecha: 07 de octubre del 2020

Correo electrónico: [infonetperu1@gmail.com](mailto:infonetperu1@gmail.com)

Firma del participante:



  
Carmen A. Ortiz Maza  
Titular - Gerente General  
Infonet Soluciones EIRL

Firma del investigador (o encargado de recoger información):

  
Albert Ignacio Juárez Ortiz  
DNI N° 71059542  
C.U. N° 0809131023

COMITÉ INSTITUCIONAL DE ÉTICA EN INVESTIGACIÓN – ULADECH CATÓLICA

## ANEXO V: FICHA DE VALIDACIÓN PARA JUECES EXPERTOS

### FICHA DE VALIDACIÓN DEL INSTRUMENTO

#### I. DATOS GENERALES

1.1 Nombres y apellidos del validador : Hugo Luis Chunga Gutiérrez  
 1.2 Cargo e institución donde labora : Docente Universitario / Uladech.  
 1.3 Nombre del instrumento evaluado :  cuestionario  
 1.4 Autor del instrumento : Alberto Ignacio Juarez Ortiz

#### II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Criterios	Aspectos de validación del instrumento Indicadores	1 2 3			Observaciones Sugerencias
		D	R	B	
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<i>deben ser y, preciso</i>
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<b>CONTEO TOTAL</b>			<b>2</b>	<b>27</b>	
(Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		<b>C</b>	<b>B</b>	<b>A</b>	<b>Total</b>

Coefficiente de validez :  $\frac{A + B + C}{30} = 0,96$

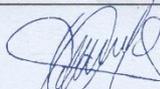
#### III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

*Validez muy buena*

Piura, agosto del 2020

Intervalos	Resultado
0,00 - 0,49	• Validez nula
0,50 - 0,59	• Validez muy baja
0,60 - 0,69	• Validez baja
0,70 - 0,79	• Validez aceptable
0,80 - 0,89	• Validez buena
0,90 - 1,00	• Validez muy buena



HUGO LUIS CHUNGA GUTIERREZ  
LIC. EN ESTADÍSTICA  
COESPE 503

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : Carol Guisella Anton Alvarado  
 1.2 Cargo e institución donde labora : Prof. Comunicación / I.E. NSTEBA SEA PILAE  
 1.3 Nombre del instrumento evaluado : Questionario  
 1.4 Autor del instrumento : Abel Ignacio Juárez Ortiz

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones Sugerencias
Criterios	Indicadores	D	R	B	
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<b>CONTEO TOTAL</b>			4	24	
(Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		C	B	A	Total

Coefficiente de validez :  $\frac{A + B + C}{30} = 0,93$

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez muy buena

Piura, agosto del 2020

Intervalos	Resultado
0,00 - 0,49	• Validez nula
0,50 - 0,59	• Validez muy baja
0,60 - 0,69	• Validez baja
0,70 - 0,79	• Validez aceptable
0,80 - 0,89	• Validez buena
0,90 - 1,00	• Validez muy buena

Carol G. Anton Alvarado  
 Carol G. ANTON ALVARADO

**FICHA DE VALIDACIÓN DEL INSTRUMENTO**

**I. DATOS GENERALES**

1.1 Nombres y apellidos del validador : Danny Daniel Anton Asanza  
 1.2 Cargo e institución donde labora : Docente, Universidad Cesar Vallejo  
 1.3 Nombre del instrumento evaluado : Cuestionario  
 1.4 Autor del instrumento : Alberto Ignacio Juny Ortiz

**II. ASPECTOS DE VALIDACIÓN**

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Criterios	Aspectos de validación del instrumento Indicadores	1 2 3			Observaciones Sugerencias
		D	R	B	
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<b>CONTEO TOTAL</b> (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		<b>C</b>	<b>B</b>	<b>A</b>	<b>Total</b>
				30	

Coefficiente de validez :  $\frac{A + B + C}{30} = 1,00$

**III. CALIFICACIÓN GLOBAL**

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez muy buena

Piura, agosto del 2020

Intervalos	Resultado
0,00 – 0,49	• Validez nula
0,50 – 0,59	• Validez muy baja
0,60 – 0,69	• Validez baja
0,70 – 0,79	• Validez aceptable
0,80 – 0,89	• Validez buena
0,90 – 1,00	• Validez muy buena

Ing. Danny Daniel Anton Asanza  
 MBA, ADM. DE NEGOCIOS Y RELACIONES  
 INTERNACIONALES  
 CIP 12074

## ANEXO VI: SOLICITUD DE IMPLEMENTACIÓN DEL PROYECTO DE TESIS



“AÑO DE LA UNIVERSALIZACIÓN DE LA SALUD”

Piura, 13 de Julio del 2020

Sra. Carmen Amelia Ortiz Maza

**Gerente General de Infonet Soluciones E.I.R.L**

Presente. –

Asunto: **PROPONER LA IMPLEMENTACION DE MI PROYECTO DE TESIS EN INFONET SOLUCIONES E.I.R.L PARA OBTENER EL TITULO PROFESIONAL EN INGENIERIA DE SISTEMAS.**

De mi consideración. –

Yo, Albert Ignacio Juárez Ortiz, identificado con **D.N.I N° 71059542**, con **C.U N° 0809131023**, egresado de la Facultad de Ingeniería de Sistemas; ante Ud. Respetuosamente me presento y expongo:

Que actualmente cursando el Taller de Tesis para optar mi título profesional de Ingeniería de Sistemas en la Universidad Católica los Ángeles de Chimbote, solicito a Ud. Se me considere mi petición, proyecto de tesis que cuenta con información suficiente y necesaria para el desarrollo de acuerdo a la necesidad de la empresa.

Agradezco anticipadamente la atención que le brinde a mi solicitud, aprovechando la oportunidad para reiterarle mi más alta consideración y estima.

Atentamente

  
Albert Ignacio Juárez Ortiz  
DNI N° 71059542  
C.U. N° 0809131023

  
Carmen Amelia Ortiz Maza  
**GERENTE GENERAL**