UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DISEÑO PARA LA IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL (VPN) EN LA EMPRESA AGROMAR INDUSTRIAL S.A - SULLANA; 2016.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

BACH. ITALO CRIOLLO LANDACAY

ASESOR:

DR. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN

PIURA – PERÚ

2017

JURADO EVALUADOR DE TESIS Y ASESOR

ING. RICARDO EDWIN MORE REAÑO
PRESIDENTE

ING. JENNIFER DENISSE SULLÓN CHINGA
SECRETARIA

MGTR. MARLENY SERNAQUÉ BARRANTES
MIEMBRO

DR. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN
ASESOR

DEDICATORIA

A mi familia por su gran apoyo y sacrificio permanente que me ha dado fuerzas para ser constante en la lucha de este objetivo.

AGRADECIMIENTO

A Dios, a mis padres y toda mi familia que me han apoyado directa e indirectamente con sus buenas vibras y apoyo constante.

A mis amigos del taller de investigación que han sido buenos compañeros, consejeros y sobre todo apoyo constante durante este largo recorrido.

Un agradecimiento muy especial a mi asesor Dr. Ing. Víctor Ángel Ancajima Miñán.

RESUMEN

El presente trabajo de investigación fue desarrollado bajo la línea de investigación en TIC, para la mejora continua de las organizaciones del Perú de la Escuela profesional de Ingeniería de Sistemas. El objetivos fue realizar el diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016. Para mejorar el acceso a la información y conexión entre las dos sucursales y la empresa Agromar Industrial S.A. La investigación tuvo un diseño de tipo no experimental siendo el tipo de la investigación descriptivo y de corte transversal, se delimito una muestra de 30 trabajadores que hacen uso de las tecnologías de información y comunicación en las oficinas y que están relacionados con el tema de la investigación, obteniendo los siguientes resultados: El 70% de los trabajadores encuestados expresaron que NO tiene el acceso a la información de las sucursales de la empresa, el 73,33 de los trabajadores encuestados dijeron que NO perciben ningún tipo de seguridad de la red interna y finalmente el 100% de los trabajadores encuestados indicaron que si es necesario realizar el diseño de una red privada virtual en la empresa, motivo por el cual queda demostrado la necesidad de realizar el diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016, con lo que se concluye que la hipótesis general queda aceptada.

Palabras claves: Diseño, Red Privada Virtual, Tecnología, Implementación, Seguridad

ABSTRACT

The present research work was developed under the line of research in ICT, for the continuous improvement of the organizations of Peru of the Professional School of Systems Engineering. The objectives were to design the implementation of a virtual private network (VPN) in the company Agromar Industrial S.A - Sullana; 2016. To improve access to information and connection between the two branches and the company Agromar Industrial S.A. The research had a design of non-experimental type being the type of descriptive and cross-sectional research, delimited a sample of 30 workers that make use of the information and communication technologies in the offices and that are related to the subject of the Research, obtaining the following results: 70% of the workers surveyed expressed that they do not have access to the information of the branches of the company, 73.33 of the workers surveyed said that they do not perceive any type of security of the internal network And finally 100% of the workers surveyed indicated that if it is necessary to design a virtual private network in the company, which is why it is demonstrated the need to design for the implementation of a virtual private network (VPN) in The company Agromar Industrial SA - Sullana; 2016, which concludes that the general hypothesis is accepted.

Keywords: Design, Virtual Private Network, Technology, Implementation, Safety

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

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.

Vamos a hablar dentro de estas tecnologías de redes en una muy específica, la red Privada Virtual, también conocida como VPN (Virtual Prívate Network), para la Universidad Tecnológica de Pereira (1), una Red Privada Virtual, "es una solución específica de red que conecta a usuarios remotos a su red privada por medio de una infraestructura pública, de manera segura proporcionando iguales beneficios y recursos que una red de área local típica. Constituye una asociación lógica de líneas y terminales que pertenecen a un usuario particular e incluye proporciones de red que no son dedicados a dicho usuario".

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones, según encuesta de TechTarget (2). La gestión y el monitoreo de redes es la principal iniciativa que las compañías esperan implementar este año como parte de sus estrategias de TI.

Pero qué pasa 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.

Actualmente la empresa AGROMAR INDUSTRIAL S.A cuenta con unos 15 equipos conectados a una red de datos, con una línea de internet de 4Mbps de transmisión y su topología de red es del tipo árbol así mismo se utiliza software de ofimática y sistema de almacén y administración hechos a medida. Hasta este punto podríamos decir que la actual red de datos es suficiente, pero que pasa si queremos compartir información con las demás sucursales de la empresa.

La red de datos de la empresa Agromar Industrial S.A no cuenta con las suficientes conexiones a nivel de sus dos sucursales, ya que resultan muy costosas, sobre todo cuando se trata de grandes distancias, lo que agrava la situación. Mantener este escenario disminuye la eficiencia, productividad y operatividad de la empresa, debido a que los recursos informáticos que brinda la red actual se encuentran aislados.

De acuerdo a esto la empresa AGROMAR INDUSTRIAL S.A tiene como necesidad realizar un diseño de una red privada virtual donde se pueda compartir información entre sus dos sucursales tomando las medidas adecuadas de seguridad de la información, brindando una solución a través de las tecnologías y herramientas adecuadas.

Ante este problema se planteó la siguiente pregunta:

¿De qué manera se realizará el diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016?

Por esta razón se tomó como objetivo general realizar el diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016 para lograr la comunicación entre las dos sedes y la empresa principal.

Lo que derivó a plantear los objetivos específicos:

1. Identificar los requerimientos de conexión y seguridad para garantizar que se satisfagan las necesidades de la empresa.

2. Evaluar las diferentes tecnologías que se pueden utilizar para implementar una red privada virtual.

3. Realizar la propuesta de implementación de las tecnologías VPN que más se adecuen a la red de datos actual de la empresa.

Las características de la presente investigación fueron de un enfoque cuantitativo. Asimismo el tipo es descriptiva y explicativa.

La justificación de esta investigación se basa en que las redes privadas virtuales se han convertido en una de las tecnologías más implementadas por las empresas y las razones por las cuales son implementadas son la reducción de costes en las comunicaciones entre oficinas, la mejora de acceso remoto de tele trabajadores y oficinas remotas así como clientes y proveedores.

A modo de justificación académica fue necesario recurrir a los conocimientos adquiridos durante todos los años de formación sólida en la Universidad Católica los Ángeles de Chimbote, lo cual nos permitirá hacer una evaluación de la situación actual requerido por la empresa y realizar el análisis y diseño para la posterior implementación de red privada virtual.

Como justificación operativa se estimó la actual red de computadoras para determinar si existen los recursos necesarios para una posterior implementación y que se cumplan con todas la normas actuales de la empresa teniendo en cuenta que el personal y recurso humano esté capacitado para operar la red privada virtual.

Así que como justificación económica a través de la implementación de una red privada virtual se pueden conectar sucursales de la empresa y usuarios móviles en una red corporativa ancha a través de Internet, reduciendo los costos de largas distancias, reduciendo tiempo en los procesos de generación y compartición de información. Al igual, proporciona conocimientos a cerca de una nueva forma de establecer conexiones remotas económicas y seguras.

Como justificación tecnológica las nuevas tecnologías están cambiando todos los ámbitos de nuestras vidas y están afectando la forma en que se hacen las cosas, como por ejemplo la forma de trabajar, este constante crecimiento hace que las empresas estén adoptando tendencias de TI relacionadas a los negocios, por ello se propone el diseño de una red privada virtual basándose en la necesidad de compartir información privada y el creciente volumen de información generado por la empresa lo cual le permitirá optimizar recursos y tiempo en el desempeño de sus trabajadores.

A modo de justificación institucional una empresa que incorpora las nuevas tecnologías es más competitiva, cuenta con mayores recursos de producción y competitividad y esto se ve reflejado en brindar un mejor servicio a sus trabajadores en todas las áreas, esto mejora la imagen institucional y acentúa la marca de la empresa como tal.

Como alcance de la investigación este proyecto se encuentra en el campo de la informática y las telecomunicaciones y pretende generar el diseño para la implementación de una red virtual VPN en la empresa Agromar Industrial S.A cuyo alcance de este proyecto lograra en beneficios a los trabajadores y administradores de la empresa y queda como referente para nuevas investigaciones.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Para **Romero y Romero** (3), 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.

En el 2015 **Tituaña** (4)**,** en su investigación titulada "Desarrollo de un Modelo de implementación de Redes Privadas Virtuales Multipunto Dinámicas (DMVPN) para Pequeñas y Medianas Empresas (PYMES)" nos explica que todo cambia a tener administración y control sobre los dispositivos electrónicos y mantener contacto con cualquier parte del mundo sin tener que movilizarse. En unos inicios el escritorio remoto fue la gran solución que prometía quedarse, sin embargo fueron apareciendo más soluciones que hacían lo mismo e integraban mayor número de características, este es el caso de las VPNs utilizadas en la actualidad, con esta propuesta innovadora es posible conectarse sin tener que desplazarse al lugar de trabajo, a otra ciudad o sector, este es el método utilizado por excelencia. Como solución al problema plantea el uso de los proveedores de Internet (ISP) o carriers que ya constan con una red desplegada y disponen de las tecnologías de acceso al medio dependiendo de dónde se requiera, ahora bien, los ISP o carriers dan una solución más rápida al usar su red lo que se conoce como enlaces de dicados, y por aquello obtienen su comisión que resulta igual de elevado.

Aguilar y Ramírez (5)**,** en el año 2014 en su tesis titulada "Diseño e implementación de una red privada virtual hospitalaria (VPN) mediante acceso remoto a un sistema centralizado de información en Bogotá" argumenta que se escogió la solución VPN debido a su bajo costo, ya que solo requiere de una conexión al proveedor de servicio, evitando implementación de infraestructura costosa. Por otra parte permite aumentar las sucursales ya que brinda una excelente escalabilidad. Mediante el túnel vpn podemos garantizar la seguridad en el tráfico de datos. Para esta labor en cuanto al proceso de implementación se tienen como principales parámetros la simplicidad en la consulta y la capacidad de enlace, para lograr registrar en su totalidad los aspectos que a nuestro concepto son más importantes y que más fallas presentan, siendo esto la base para la interconexión de la información generada por las diferentes

unidades y áreas que conforman cualquier posible sistema de información sanitario.

Sánchez (6)**,** en el año 2010 realizaron un "Diseño de una solución de IP Trunking sobre red VPN entre múltiples sedes de un Contact Centre" donde plantea el diseño para la solución de red con el objetivo de simplificar la estructura de la red original del cliente, unificando las tecnologías y aprovechando las sinergias proporcionadas por la tendencia hacia el mundo IP para canalizar todos los servicios por una única red. Como resultado se ha creado una red en la que todas las sedes están interconectadas mediante una VPN altamente escalable, que permite incorporar nuevas sedes de forma rápida y sencilla. Respecto a la telefonía se ha establecido una solución basada en ToIP (Telephony over IP), que además permite reutilizar parte del equipamiento de que dispone el cliente, simplificando toda la estructura de primarios y líneas de telefonía clásica con una reducción del coste.

2.1.2. Antecedentes a nivel nacional

Alva (7)**,** en su tesis titulada "Desarrollo e Implementación de una Herramienta Gráfica para la Configuración Remota de una VPN con Routers Cisco" realizada en el año 2013, propone una solución viable de una Red Privada Virtual o VPN (Virtual Private Network) que permita a las empresas crear su propia red privada con un 60% de seguridad permitiendo conectar a los locales; sin embargo, realizar esto requiere de un conocimiento avanzando en la configuración de equipos (routers), ya que podría resultar un problema para un usuario en general si deseará realizarlo por su cuenta. Por tal motivo, que se suele, usualmente, contratar a una empresa tercera (comúnmente el proveedor que nos brinda el servicio de internet) para que realice esta configuración, incurriendo en un gasto. Es por ello, que el siguiente proyecto busca desarrollar e implementar un herramienta gráfica que permita crear una

VPN (Red Privad Virtual), usando la tecnología IOS de Cisco DMVPN, entre dos o más locales de forma rápida y sencilla; esto siempre y cuando cada local posea una salida a internet a través de un router Cisco de la seria 800 o superior. Se cumplió con el objetivo principal, que era el desarrollar una herramienta gráfica para la construcción de una VPN de forma remota. Y qué además dicha interfaz sea amigable.

En ese mismo año **Ramírez** et al**.** (8)**,** en su investigación "Diseño de una Red de Banda Ancha para la Región de Puno" presentan una propuesta de una red de alta capacidad, que permita explotar el uso de las Tecnologías de la Información y Comunicación (TIC) a través de servicios de calidad, logrando con ello mejores condiciones de vida y mayor acceso a oportunidades para los pobladores. También, se desarrolla el análisis económico que demuestra que la implementación de la red es rentable y sostenible en el tiempo. Con la implementación no solo se beneficiarán los pobladores de Puno, sino también las entidades de educación (2,556 instituciones beneficiadas), entidades de salud (429 entidades, entre hospitales, centros de salud y puestos de salud), 70 comisarías, 27 Bancos de la Nación, 22 juzgados de paz, 3 museos,17 RENIEC, 13 municipalidades provinciales y 106 municipalidades distritales.

Molina (9)**,** en su proyecto de investigación titulado "Propuesta de Segmentación con Redes Virtuales y Priorización del Ancho de Banda con QoS para la Mejora del Rendimiento y Seguridad de la Red LAN en la empresa Editora el Comercio Planta Norte."; realizada en el año 2012 nos detalla la empresa Editora El Comercio – Planta Norte posee una red plana en su diseño lo cual dificulta la administración del tráfico de la Red, debido a la ausencia de estándares de calidad en gestión de tráfico LAN, políticas de seguridad en un 80% no alineadas a las necesidades de la empresa y desaprovechamiento de la performance de los equipos de comunicación instalados debido a ello, nace la propuesta de la

Segmentación de la Red de Datos con Redes Virtuales y la priorización del Ancho de Banda con QoS para mejorar así el Rendimiento y Seguridad de la Red LAN en la Empresa Editora El Comercio – Planta Norte, llegando a la conclusión que la proyección de crecimiento de la Planta Norte es de 16% anual, donde actualmente se cuenta con 50 terminales. Se implementó y configuró la red para soportar este promedio de crecimiento sin afectar el rendimiento de la Lan, gracias a los lineamientos de la metodología adoptada. Con lo que es posible conectar otros switch Cisco de 48 puertos hacia el swicth Core y responder a la tasa de crecimiento, con una velocidad de 100/1000 Gbps en cada troncal. Con ello concluimos que el objetivo de la Escalabilidad fue posible.

Por su parte **Rodríguez** y **Sánchez** (10)**,** en el año 2011 realizaron un "Diseño de una red de Banda Ancha para la Región de la Libertad" brindando una propuesta de red de alta capacidad, que permita explotar el uso de las Tecnologías de la Información y Comunicación (TICs); a través, de servicios de calidad, logrando con ello mejores condiciones de vida y mayor acceso a oportunidades para los pobladores de la región La Libertad. Así como, el análisis económico para especificar la rentabilidad económica y sostenibilidad en el tiempo de la propuesta. En el análisis económico mostrado en el capítulo 4, se concluye que la red propuesta es rentable y sostenible en el tiempo, ya que se tiene un TIR de 25% y un VAN positivo de S/. 54, 664,261.35. Asimismo, la inversión se recupera en un periodo de 3 años y 3 meses. La ejecución e implantación de este tipo de red, contribuye al beneficio social de acceso a mejores oportunidades de desarrollo (que incluye mejor y mayor acceso a la información, así como progresos en la educación, comercio y salud) ayudando al aumento del bienestar de la población de la Región La Libertad.

2.1.3. Antecedentes a nivel regional

Ancajima (11)**,** en su tesis titulada "PROPUESTA DE REINGENIERÍA DE LA RED DE DATOS EN LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL (UGEL) PAITA, 2014." realiza una propuesta de reingeniería de la red de datos perteneciente a la unidad de gestión educativa local (UGEL) PAITA para optimizar el sistema de comunicaciones de la institución. La investigación tuvo un diseño de tipo no experimental siendo el tipo de la investigación descriptivo y de corte transversal, con una población muestral de 30 trabajadores. Llegando a la conclusión luego de haber revisado diferentes normas necesarias para el diseño de infraestructura de red, se puede concluir que no siempre se cumplirán en su totalidad ya que las características de las instalaciones de un edificio y las exigencias del cliente serán las que definan el diseño real. Lo que se debe procurar es buscar solución que más se acerque a las recomendaciones de las diferentes normas. El diseño propuesto cumplió las exigencias del cliente al respetar la distribución de las zonas hechas y no exigir la demolición de las estructuras. Sin embargo, esto no implicó que no se siguieran las normas ya que se dieron soluciones que balanceen ambas necesidades.

Muñoz (12)**,** en su investigación "DISEÑO DE UNA RED DE TELECOMUNICACIONES DE BANDA ANCHA PARA LA REGIÓN TUMBES" la cual consiste en el diseño de una red de telecomunicaciones de banda ancha para la Región Tumbes y tiene como objetivo la conectividad regional, integrando todos los distritos de la región con redes de alta capacidad de transmisión que permita atender las necesidades de comunicaciones de banda ancha, además de la conectividad integral a la red de banda ancha nacional. Donde concluye que una red de telecomunicaciones de banda ancha para la región Tumbes contribuye al mejoramiento de la calidad de vida de la población de la región. Se genera un impacto positivo en el desarrollo

socioeconómico pues aumenta la competitividad por medio del acceso a información. Recomienda realizar un trabajo de campo de mayor profundidad en la región, es decir, realizar visitas que permitan comprobar la información obtenida en esta tesis además de verificar la infraestructura eléctrica existente en la región.

En el año 2012 **Ancí** (13)**,** en su investigación propone un "ESTUDIO DE PREFACTIBILIDAD Y DISEÑO DE LA RED DE TELECOMUNICACIONES PARA EL POBLADO DE SOL SOL EN PIURA" La razón principal para que las telecomunicaciones hayan pasado de ser una comodidad para pocos, a ser una necesidad básica para todos, es que gracias a ella lugares apartados pueden comunicarse entre sí, además de ser el mejor medio de circulación de una gran cantidad de información de origen variado a nivel mundial. Provocando que de manera inmediata las comunidades aisladas se integren a la economía global, permitiendo que sus pequeñas empresas accedan a la información de empresas grandes, cuyas experiencias sirvan de referencia para ser aplicadas en su propio desarrollo. Propone dos soluciones, la primera de ellas involucra una inversión mayor con un TIR de 12.65% y plantea brindar servicios completos a todo el pueblo de Sol Sol; la segunda solución requiere menor inversión con un TIR de 50.34% y asegura la comunicación de la casa del teniente gobernador, la posta médica, el colegio inicial, el colegio primario y el colegio secundario, recomendando adquirir los equipos de un proveedor confiable para poder acceder al servicio de soporte y garantía. Informar a la población sobre los beneficios que tendrían con los nuevos servicios de telecomunicaciones.

2.2. Bases teóricas

2.2.1. Agroindustria y Agroexportaciones

Agroindustrias:

La agroindustria es la actividad económica que comprende la producción, industrialización y comercialización de productos agrarios pecuarios, forestales y biológicos (14).

En los últimos años la agroindustria peruana se viene desarrollando con tecnología y buena gestión empresarial, aprovechando nuestra gran diversidad climática y natural que permite la producción agroindustrial durante todo el año, constituyendo no solo una fuente de empleo descentralizado sino de divisas, debido a la creciente exportación agroindustrial hacia todos los mercados regionales del mundo.

La Agroindustria se divide en dos categorías: alimentaria y no alimentaria.
La primera se realiza la transformación de los productos de la agricultura, ganadería, riqueza forestal y pesca, en productos de elaboración para el consumo alimenticio, que incluye los procesos de selección de calidad, embalaje-empaque y almacenamiento.

La rama no-alimentaria es la encargada de la parte de transformación de estos productos que sirven como materias primas, utilizando sus recursos naturales para realizar diferentes productos industriales

Clasificación:

Según **Mayorga** (15), las agroindustrias se clasifican de la siguiente manera.

A. Sin transformación

a. **Centro de Acopio.**

Para pequeños productores: Selección, empaque y mercadeo.

- Leche cortada
- Pescado (pesca costera)
- Frutas y verduras Materia prima para la industria

b. **Almacenamiento**

- Silo de granos
- Almacenes de materia prima o producto elaborado
- Cámara Frigorífica

c. **Selección, clasificación y Empaque**

- Fruta cítrica. Clasificación por volumen, 7 tamaños.
- Fruta de carozo. Clasificación por peso y tamaño.
- Banano. Empaque de manos, por peso. Maduración programada.
- Hortalizas. Clasificación por volumen, 3-4 tamaños.
- Flores. Clasificación por variedad, color y largo de tallo
- Empaque minorista. Impresión de peso y precio.

B. Con Transformación

a. Primer grado de transformación

- Conservación y empaque del producto
    - Deshidratado de frutas, verduras, especias, pescado.
    - Secado de tabaco.
    - Secado y tostado de pipas de girasol.
    - Enlatado de frutas y verduras
    - Encurtido de hortalizas
    - Congelado de verduras
    - Beneficio de café
    - Beneficio de cacao
    - Lavadora de lana
    - jaleas y mermeladas
    - Pasteurizado de leche
    - Pasteurizado de miel
    - Descascarado y pelado de fruto seco
- Elaboración
    - Jugos de frutas, concentrados
    - Ingenios de azúcar. Panela
    - Concentrados de tomate
    - Subproductos de la papa
    - Mataderos de vacuno, ovino y porcino
    - Mataderos de pollos y pavo
    - Limpieza y fileteado de pescado

- Harina de carne
- Harina de pescado
- Bodega de vino
- Fábrica de cerveza
- Molino de cereales
- Fábrica de alimento balanceado
- Aserradero y secado de madera
- Tratamiento de fibras vegetales
- Fabricación de papel
- Aceite de oliva
- Aceites vegetales

b. Segundo grado de Transformación

- Subproductos de la leche
- Subproductos de la carne
- Salado, curtido y tratamiento del cuero
- Harina de carne
- Pasta y aceite de pescado
- Tostado de café
- Productos de panadería
- Sopas y comidas preparadas
- Derivados del azúcar
- Fábrica de sogas y esterillas
- Productos de pasta

c. **Tercer grado de elaboración**

- Tejedurías
- Subproductos del cacao
- café instantáneo
- Puertas y ventanas. Muebles

d. Servicio

- Incubadoras de huevos
- Tratamiento de desperdicios
- Talleres de mantenimiento

Agro exportación en el Perú:

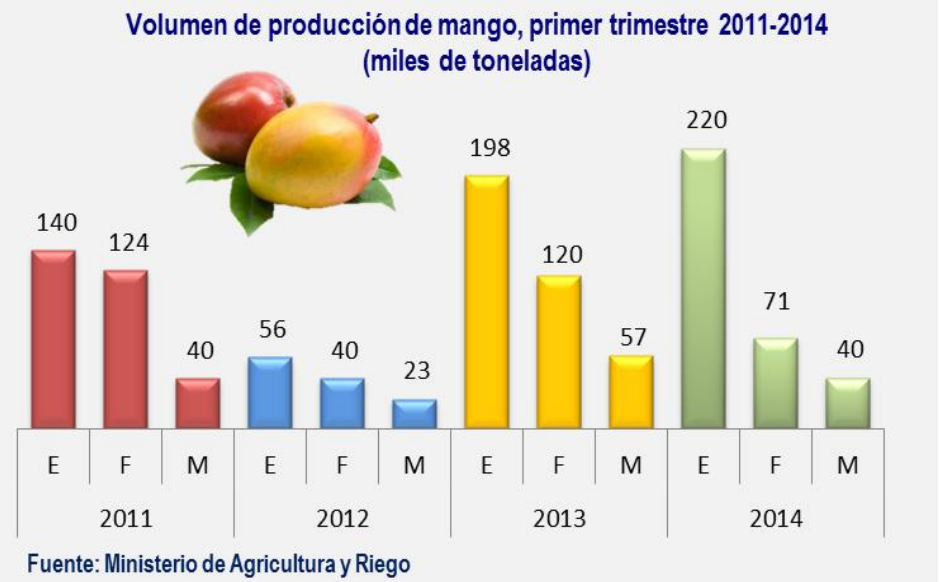
Vinelli (16)**,** es su edición para CNN en español dice:

> El Perú no es el Perú de hace 10 años. Las agroexportaciones han crecido un 17% anual, lo que ha permitido duplicar su valor cada cinco años. Estamos posicionados entre los 10 principales proveedores de alimentos en el mundo, con productos como quinua, espárrago, café, mango, maca, aceituna, uva y, recientemente, arándanos, todos los cuales tienen un enorme valor para la seguridad alimentaria mundial.
>
> El buen desempeño ha convertido a las agroexportaciones en el segundo sector económico generador de divisas. De hecho, se estima que llegarán a los 7.000 millones de dólares a finales del 2016 gracias a la apertura de nuevos mercados.

Producción nacional de mango:

La producción de mango en el primer trimestre de 2014 fue menor en 11,9% comparado con igual periodo del 2013. Piura, Lambayeque y Áncash fueron los principales departamentos productores de mango (17).

Gráfico Nro. 1: Volumen de producción de mango 2011-2014



Fuente: INEI (17)

Superficies cultivadas según Regiones y volúmenes de exportación:

En un documento publicado por la Asociación Peruana de Productores y Exportadores de Mango (18), nos muestra datos estadísticos de cual son las superficies cultivadas según regiones y las exportaciones totales de mango entre el año 2010 y 2014.

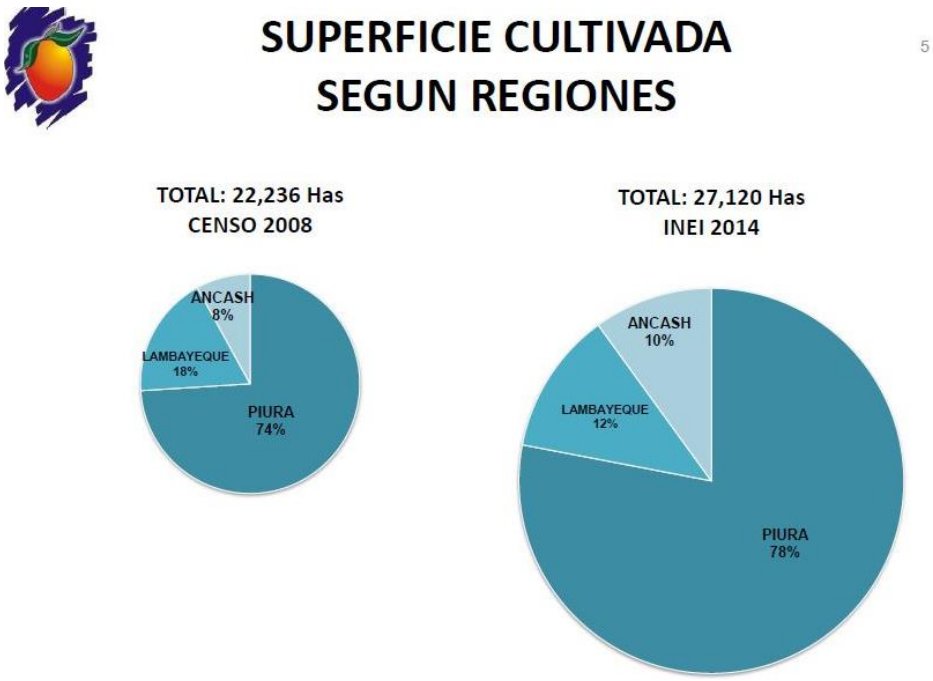
Además nos dice que el Perú exporta entre la semana 44 y la semana 9 aproximadamente 5,000 contenedores (35% a EE.UU, 60% a Europa y 5% a otros países). Todos los años APEM realiza una prospección de volumen para la exportación de mango fresco.

Gráfico Nro. 2: Prospección de exportación de mango fresco

REGION	ZONA	AREA (HAS) INEI	AREA EVALUADA (HAS)	NIVEL DE MUESTREO (%)
Piura	San Lorenzo y Cieneguillo	18,564	1,671	9%
	Alto Piura	2,600	182	7%
Lambayeque	Olmos y Motupe	3,356	784	23%
Ancash	Casma	2,600	303	12%
TOTAL		27,120	2,940	11%

Fuente: APEM (18)

Gráfico Nro. 3: Superficie cultivada según regiones



Fuente: APEM (18)

2.2.2. Agroindustrias

Definición:

"La Agroindustria es un sistema dinámico que implica la combinación de dos procesos productivos, el agrícola y el industrial, para transformar de manera rentable los productos provenientes del campo" (19).

"Es un conjunto de procesos de transformación aplicados a materias primas de origen agropecuario y forestal, que abarca desde su beneficio o primera agregación de valor, hasta la instancia que generan productos finales con mayor grado de elaboración constituye uno de los subsectores de gran relevancia para el país, pues se encuentra estrechamente vinculada con los demás sectores de la actividad económica" (19).

Agromar Industrial

A. Información General

Agromar Industrial S.A. con RUC: 20110378956 y con nombre comercial Agromar Industrial S.A., ubicado en: AV. Paseo de la Republica Nro. 3195 INT. 902 Urb. CORPAC Lima - Lima - San Isidro. Dedicado a elaboración de almidones y derivados, con CIIU: 15329 como actividad principal y Elaboración de frutas, Legumbres y hortalizas, con CIIU: 15130 como actividad secundaria. Agromar Industrial S.A. tiene 6 locales, entre sucursales, oficinas y demás.

Tabla Nro. 1: Sucursales y / Oficinas

N°	Dirección	Tipo
1	CAR. CARRET SULLANA TAMBOGRANDE NRO. 43.5 CAS. TBO GRANDE PIURA PIURA TAMBO GRANDE	S.PRODUCTIVA
2	CAL. TUMBES NRO. 1211 Z.I. TAMBOGRANDE PIURA PIURA TAMBO GRANDE	S.PRODUCTIVA
3	CAL. D NRO. SN Z.I. INDUSTRIAL (PARQUE INDUSTRIAL SULLANA) PIURA SULLANA SULLANA	S.PRODUCTIVA
4	CAR. PANAMERICANA NORTE NRO. 66 URB. VILLA RICA LAMBAYEQUE LAMBAYEQUE MOTUPE	DEPOSITO
5	CAL. LOS FRESNOS MZA. D LOTE. 1A1B URB. HUERTOS DE VILLENA (ESQUINA CALLE LOS LAURELES) LIMA LIMA PACHACAMAC	S.PRODUCTIVA
6	AV. RAMÓN CASTILLA NRO. 1750 PIURA MORROPON CHULUCANAS	DEPOSITO

Fuente: Elaboración propia

B. Historia

Agromar Industrial S.A. es una empresa agroindustrial dedicada desde hace 22 años a la producción y comercialización de pulpa de frutas, principalmente mango en sus diferentes variedades y maracuyá. En 1987, inicia sus operaciones productivas en la región (20).

Cuenta con un área de 9339.80 m2. Desde Enero del 2003 está incursionando en el área de frutas y hortalizas congeladas, iniciándose con mango IQF y pretendiendo ampliar sus horizontes al congelamiento de otras frutas como banano, melón, papaya, palta; hortalizas como pimiento, espárragos, cebollas, alcachofas; legumbres como fréjoles; raíces como yuca, etc. En la actualidad la planta se encuentra certificada con HACCP, KOSHER, así como para proceso y certificación ORGÁNICO.

Debido a la estratégica ubicación geográfica de nuestra planta, todo el año contamos con materias primas. De Octubre a Marzo cuenta con abundantes cantidades de mango en sus diferentes variedades tanto para nuestra línea de pulpas como para la línea de IQF, de Febrero a Septiembre disponemos de maracuyá y piña. Asimismo, el clima de la región se presta para el desarrollo de cultivos de hortalizas y leguminosas durante todo el año, los mismos que de acuerdo a los requerimientos del mercado internacional pueden convertirse en potenciales cultivares industriales.

C. Objetivos organizacionales

Misión

Proveer sostenidamente a nuestros clientes de productos de alta calidad, con protección del medio ambiente donde procesamos y de los lugares donde nuestra materia prima es obtenida.

La calidad es un compromiso de nuestra empresa basado en sistemas de seguridad alimentaria, acciones de control, trabajo técnico de campo y supervisión en el transporte, mejora continua de nuestros procesos en base a la investigación y con soporte en nuestro personal, a quienes capacitamos y brindamos las condiciones de

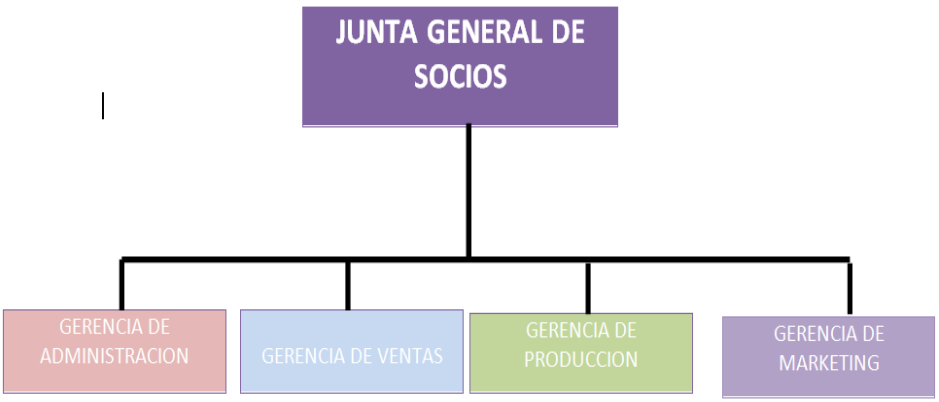
salud y seguridad. Nuestro compromiso se extiende hacia la sociedad y el medio ambiente.

Visión

Maximizar las utilidades de la empresa, sin olvidar nuestras responsabilidades con nuestra gente y nuestro entorno, que sea agradable el ambiente de trabajo a fin de potenciar las competencias de nuestros colaboradores, que permita ofrecer a nuestros clientes, lo mejor de nosotros, que satisfagan sus necesidades y expectativas, manteniendo para ello un alto estándar de calidad que los incorpore como socios estratégicos de nuestro crecimiento, creando una lealtad mutua y duradera. De igual manera todas nuestras acciones están orientadas al cuidado de nuestro planeta, aportaremos nuestra responsabilidad en ello para vivir en un mundo mejor.

D. Organigrama

Gráfico Nro. 4: Organigrama



Fuente: Agromar Industrial

E. Funciones

Directorio

Establecer y controlar la política general de la Sociedad, teniendo como objetivo primordial brindar los servicios en las mejores condiciones de calidad y continuidad, así como buscar viabilidad económica, con las facultades y atribuciones que señala para el efecto el Estatuto de la Empresa.

Gerencia General

Planificar, dirigir, coordinar y controlar las actividades de la empresa AGROMAR INDUSTRIAL S. A. para el cumplimiento de sus fines, objetivos y metas, de acuerdo a las normas vigentes y a los acuerdos y disposiciones del Directorio.

Gerencia Administrativa

Administrar y controlar de manera eficiente los recursos humanos, materiales, económicos y financieros de la empresa.

Gerencia de Producción

Planificar, organizar, controlar y evaluar eficientemente los procesos de la producción y comercialización de pulpa de frutas, principalmente mango en sus diferentes variedades y maracuyá.

Gerencia Comercial y ventas

Planificar, organizar, dirigir, desarrollar y evaluar la atención al cliente, promoción del servicio, actualización del catastro comercial, la cobranza correspondiente.

F. Infraestructura Tecnológica Existente

1. **Hardware**

Computadoras: la empresa Agromar Industrial S.A cuenta con un total de 25 computadoras distribuidas entre sus diferentes sedes de trabajo y que están distribuidas de la siguiente manera.

Tabla Nro. 2: Distribución del equipamiento de computadoras

SEDE	AREA	Nª EQUIPOS PC/LAPTOP
Agromar Industrial	Administración	7
	Almacén	4
	Producción	2
	Laboratorio	2
Aceites Esenciales del Perú S.A.C.	Administración	3
	Almacén	2
Cítricos Peruanos S.A	Administración	4
	Acopio	1
	TOTAL	25

Fuente: elaboración propia

Tabla Nro. 3: Equipamiento de impresoras

Característica	Tipo	Nº Impresora
Impresora industrial	zdesigner zm400 200	1
	Tsc ttp2410 m pro	1
	TSC TTP 247	1
Impresora matricial	EPSON LX - 350	1
Impresora Laser	HP LASERJET PROFESIONAL 1102W	1
Impresora Multifuncionales	Epson L355 Impresora	8
	Epson L575 EcoTank	2
	xerox workcenter 3325	1

Fuente: elaboración propia

Otros equipos.

Tabla Nro. 4: Equipos varios

EQUIPO	MODELO	CANTIDAD
Lector de códigos	Datalogic Matrix 300	1
	Zebra scanner LS1203	15
Estabilizadores	Mega Tech 220V	10
Sistema de circuito cerrado TV	Cámara Tipo Tubo Dahua	4
	Cámara Tipo Domo Dahua	4
	DVR 8 CH CVI metal dahua	2
PROYECTOR	LG PF1500	2
Reloj Biométrico	LX14 ZKTECO	1

Fuente: elaboración propia

Red de Datos: Agromar Industrial S.A cuenta con una red de datos de tipo árbol con los equipos siguientes.

Tabla Nro. 5: Equipamiento de la Red de datos

EQUIPO	MODELO	CANTIDAD
Modem	Cisco Model DPC3928	1
Switch	Switch 24 puertos 10/100/1000Mbps No Gestionable	1
Switch	Cisco Sg110-24 24 puetos	1
Cableado	Cableado UTP categoría 5	30
Conectores	Conector RJ45	60
Cajas	Caja RJ45	15
Uniones	Uniones RJ45	5

Fuente: elaboración propia

2. Software

Sistemas operativos, software de ofimática, antivirus.

Tabla Nro. 6: Software con el que cuenta Agromar Industrial S.A.

SOFTWARE	TIPO	OBSERVACION	CANTIDAD
Sistemas operativos	Windows 7	Sin licencia	20
Sistemas operativos	Windows 8	Sin licencia	4
Sistemas operativos	Windows server 2008 64X	Sin licencia	1

Ofimática	Office 2007	Sin licencia	20
Ofimática	Office 2010	Sin licencia	5
Antivirus	Avast	Libre	25
Base de datos	SQL server 2008	Sin licencia	1

Fuente: elaboración propia

Software a Medida

Tabla Nro. 7: Aplicativos y sistemas a medida.

SOFTWARE	CANTIDAD
Control de asistencia (desarrollado en la empresa)	1
Control de comedor (desarrollado en la empresa)	1
SAP control almacén	1
NISIRA ERP producción	1
BarTender (diseño de etiquetas)	1

Fuente: elaboración propia

2.2.3. Las Tecnologías de información y comunicaciones (TIC)

- Definición

Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes (21).

Las tecnologías de información y comunicaciones (TIC) es un término que contempla toda forma de tecnología usada para crear, almacenar, intercambiar y procesar información en sus varias formas, tales como datos, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquéllas aún no concebidas. En particular, las TIC están íntimamente relacionadas con computadoras, software y telecomunicaciones. Su objetivo principal es la mejora y el soporte a los procesos de operación y negocios para incrementar la competitividad y productividad de las personas y organizaciones en el tratamiento de cualquier tipo de información (22).

- Historia

Las telecomunicaciones surgen de manera aproximativa a raíz de la invención del telégrafo (1833) y el posterior despliegue de redes telegráficas por la geografía nacional, que en España se desarrolla entre los años 1850 y 1900. Actualmente, estamos acostumbrados a coexistir con todo tipo de servicios que nos facilitan la comunicación entre personas, pero la experiencia con estos sistemas es relativamente reciente. A lo largo de la historia las señales han ido evolucionando

en cuanto a su variedad y complejidad, para ajustarse a las necesidades de comunicación del hombre. Esta evolución de las comunicaciones entre personas se ha beneficiado en gran medida de los avances tecnológicos experimentados en todas las épocas, que han ido suprimiendo las barreras que tradicionalmente han limitado la interactividad entre las personas: riqueza de contenido, distancia de las comunicaciones, cantidad de información transmitida. El uso de nuevos tipos de señales y el desarrollo de nuevos medios de transmisión, adaptados a las crecientes necesidades de comunicación, han sido fenómenos paralelos al desarrollo de la historia. Otros hitos y hechos importantes que han marcado la evolución de las telecomunicaciones y, por tanto, el devenir de las tecnologías de la información y comunicaciones (23).

- 1876 (10 de marzo): Grahan Bell inventa el teléfono, en Boston, mientras Thomas Watson construye el primer aparato.
- 1927 (11 de Enero): Se realiza la primera transmisión de radiotelefonía de larga distancia, entre USA y el Reino Unido, a cargo de AT&T y la British Postal Office.
- 1948 (1 de Julio): Tres ingenieros de Bell Laboratories inventaron el transistor, lo cual, sin ninguna, supuso un avance fundamental para toda la industria de telefonía y comunicaciones.
- 1951 (17 de Agosto): Comienza a operar el primer sistema transcontinental de microondas, entre Nueva York y San Francisco.
- 1956 (a lo largo del año): Comienza a instalarse el primer cable telefónico trasatlántico.
- 1963 (10 de Noviembre): Se instala la primera central pública telefónica, en USA, con componentes electrónicos e incluso parcialmente digital.
- 1965 (11 de Abril): En Succasunna, USA, se llega a instalar la

primera oficina informatizada, lo cual, sin duda, constituyó el nacimiento del desarrollo informático.

- 1984 (1 de Enero): Por resolución judicial, la compañía AT&T se divide en siete proveedores (the Baby Bells), lo que significó el comienzo de la liberación del segmento de operadores de telecomunicaciones, a nivel mundial, el cual progresivamente se ha ido materializando hasta nuestros días.

- Desde 1995 hasta el momento actual los equipos han ido incorporando tecnología digital, lo cual ha posibilitado todo el cambio y nuevas tendencias a las que asistimos. Se abandona la transmisión analógica y nace la Modulación por Impulsos Codificados o, lo que es lo mismo, la frecuencia inestable se convierte en código binario, estableciendo los datos como único elemento de comunicación

- ERP

a) ¿Qué es un ERP?

ERP son las siglas de "Enterprise Resource Planning"o "Planificación de Recursos Empresariales". Por tanto en primer lugar podemos decir que ERP son unas siglas, pero ¿qué hay detrás de esas siglas? ¿Qué es realmente un ERP? En pocas palabras un ERP es (24), un sistema informático de gestión de información para una empresa.

Un ERP es un sistema de gestión y de datos único, donde converge toda la información de una empresa y ésta es utilizada para tomar decisiones. Decir esto es referirnos a algo muy amplio y sin límites claramente definidos: pues eso es un ERP, algo que puede ser tan variable en tamaño y

funcionalidad como variables pueden ser el tamaño y fines de las millones de empresas que funcionan en los distintos países.

Otra definición sencilla de lo que es un ERP es esta: “Un ERP es un sistema informático que facilita la gestión de una empresa en todos sus ámbitos (recursos humanos, compras, ventas, etc.)”.

El origen de los ERP se puede atribuir a las necesidades de planificación y gestión de recursos bélicos que genera un gran acontecimiento militar: la Segunda Guerra Mundial. Los ejércitos requieren de una gran logística: planificación y control de dónde está destinado el personal, los materiales, stocks, etc. Con este primer enfoque inicialmente “militar” los sistemas de información fueron evolucionando para dar soporte a todo tipo de empresas en sus necesidades de gestión cotidianas.

- NISIRA ERP

Nisira ERP (25), es un sistema de gestión integral que administra todas las áreas funcionales de una organización.

b) ¿Qué es SAP?

Para **Yecas Hector** (26)**,** nombre de SAP proviene de: Sistemas, Aplicaciones y Productos en Procesamiento de datos. EL nombre SAP es al mismo tiempo el nombre de una empresa y el de un sistema informático. Este sistema comprende muchos módulos completamente integrados, que abarca prácticamente todos los aspectos de la administración empresarial. Cada módulo realiza una función diferente, pero está diseñado para trabajar con otros módulos.

La integración total de los módulos ofrece real compatibilidad a lo largo de las funciones de una empresa. Esta es la característica más importante del sistema SAP y significa que la información se comparte entre todos los módulos que la necesiten y que pueden tener acceso a ella. La información se comparte, tanto entre módulos, como entre todas las áreas.

SAP establece e integra el sistema productivo de las empresas. Se constituye con herramientas ideales para cubrir todas las necesidades de la gestión empresarial -sean grandes o pequeñas- en torno a: administración de negocios, sistemas contables, manejo de finanzas, contabilidad, administración de operaciones y planes de mercadotecnia, logística, etc. SAP proporciona productos y servicios de software para solucionar problemas en las empresas que surgen del entorno competitivo mundial, los desarrollos de estrategias de satisfacción al cliente, las necesidades de innovación tecnológica, procesos de calidad y mejoras continuas, así como, el cumplimiento de normatividad legal impuesta por las instituciones gubernamentales.

2.2.4. Redes Privadas Virtuales

a) Introducción

Siempre habido una clara división entre una red pública y una privada (27). Una red pública es una serie de diferentes puntos sin relación que intercambian información más o menos libremente entre ellos. La gente que accede a este tipo de red puede o no estar relacionada o tener algo en común y una sola persona dentro de esa red puede que solo se comunique con una pequeña fracción de los usuarios de la misma. Una red privada se compone de varias computadoras pertenecientes a una sola organización y que intercambian información específica entre ellas dentro de esta red ellos están seguros que son los únicos que utilizan los recursos de esta red y lo que se comparte en ella .

b) Que es una red de computadoras

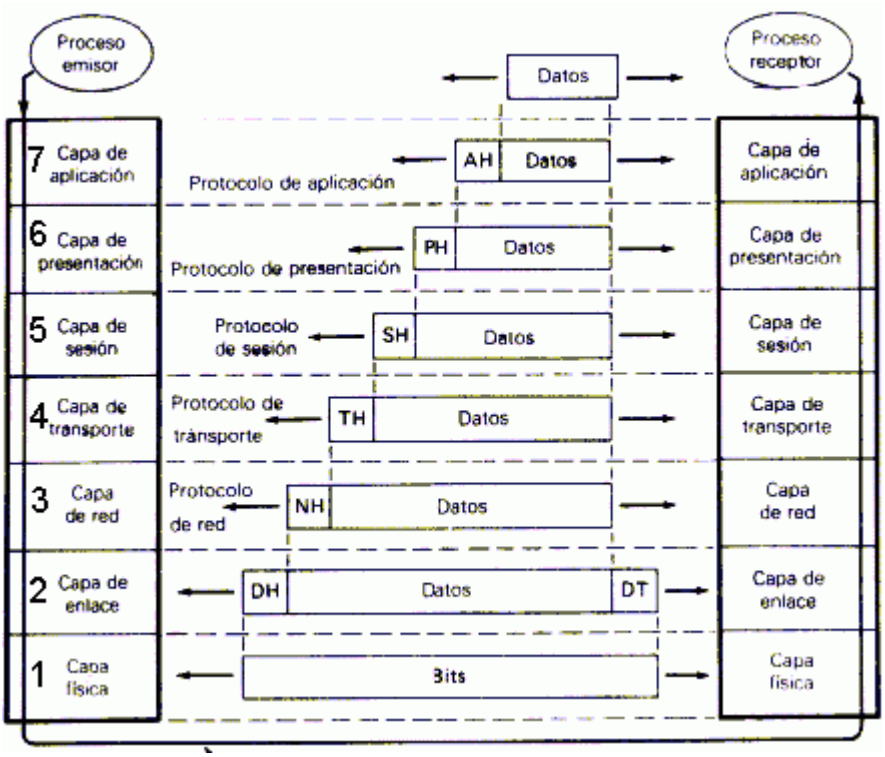
Una red de computadoras (28), también llamada red de ordenadores o red informática es un conjunto equipos (computadoras y dispositivos), conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, para compartir información (archivos), recursos (discos, impresoras, programas, etc.) y servicios (acceso a una base de datos, internet, correo electrónico, chat, juegos, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo.

c) Modelo OSI

El modelo OSI es un modelo conceptual que no define ni específica 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.

Gráfico Nro. 5: Modelo OSI



Fuente: Telepieza (29)

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.

Las funciones de cada nivel son (29):

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.

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

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

CAPA 3. Capa de la Red

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

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

- Prevenir la producción de bloqueos así como la congestión en los nudos de la red de transporte que pudiesen producirse en horas punta por la llegada de paquetes en forma masiva.

CAPA 4. Capa de Transporte

Se encarga del transporte de la información, desde la fuente al destino, a través de la red.

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

CAPA 5. Capa de sesión

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

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

puede encargarse de restablecer la sesión de forma transparente al usuario.

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

CAPA 6. Capa de Presentación

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

Puede realizar transformaciones para conseguir mayor eficacia en la red (compresión de texto y cifrado de seguridad). Los programas del nivel 6 suelen incluirse en el propio Sistema Operativo.

La representación de los caracteres como los datos de texto y de representación EBCDIC, ASCII y UNICODE.

CAPA 7. Capa de Aplicación

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

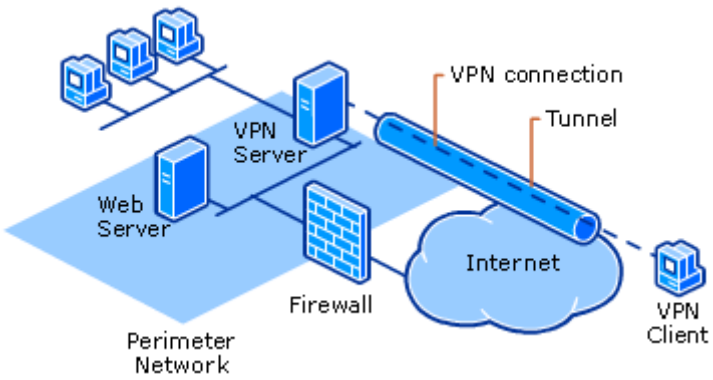
- **TELNET:** Es una aplicación que permite desde nuestro sitio y con el teclado y la pantalla de nuestro Ordenador, conectarnos a otro ordenador remoto a través de la red.
- **FTP:** Es una herramienta que te permite, a través de la red, copiar ficheros de un ordenador a otro.
- **SMTP:** Es un servicio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

d) Red Privada Virtual (VPN)

La Red Privada Virtual (VPN), según Galarza (30), cuyo nombre deriva del inglés Virtual Prívate Network, es una tecnología de red que permite la extensión de una red local sobre una red pública o no controlada, como por ejemplo Internet, mediante un proceso de encapsulación y encriptación, en la cual los paquetes de datos viajan a distintos puntos remotos por medio de un "túnel" definido en una infraestructura pública de transporte. Como ejemplos se encuentran conectar dos o más sucursales a la red corporativa de una empresa dentro de un área geográfica amplia utilizando como vínculo Internet, que también puede servir para permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto como un hotel.

En el caso de acceso remoto la VPN permite al usuario acceder a su red corporativa asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público.

Gráfico Nro. 6: Servidor VPN con firewall



Fuente: Microsoft

e) Requerimientos de una VPN

Requerimientos básicos de la VPN (31):

- Autenticación de usuario

  La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados. Además, las solución deberá proporcionar registros de auditoría y contables para mostrar quién accedió a qué información y cuándo.

- Administración de dirección

  La solución deberá asignar una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan así.

- Encriptación de datos

  Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

- Administración de llaves

  La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

- Soporte de protocolo múltiple

  La solución deberá poder manejar protocolos comunes utilizados en las redes públicas. Estos incluyen Protocolo de Internet (IP), Central de paquete de Internet (IPX).

f) Arquitecturas VPN

Existen dos tipos comunes de VPN (32), los cuales son:

Acceso remoto: también conocida como red virtual de acceso telefónico privada (VPDN). Es una conexión de usuario a LAN utilizada por una empresa que tiene empleados que necesitan conectarse a la red privada desde varias ubicaciones remotas. Normalmente, una empresa que desee configurar una gran VPN de acceso remoto proporciona a sus usuarios algún tipo de cuenta de acceso telefónico a Internet mediante un proveedor de servicios de Internet (ISP). Así, los trabajadores que están de viaje pueden marcar un número 1-800 para entrar en Internet y usar su software cliente de VPN para acceder a la red de la empresa. Este tipo de VPN es muy útil, por ejemplo, para una gran empresa con cientos de comerciales que necesite una VPN de acceso remoto. Las VPN de acceso remoto permiten establecer conexiones seguras y cifradas entre la red privada de una empresa y usuarios remotos a través de un proveedor de servicios.

Sitio a sitio: una empresa pueden conectar varios sitios fijos a través de una red pública como Internet, utilizando un equipo exclusivo y un cifrado a gran escala. Cada sitio necesita únicamente disponer de una conexión local a la misma red pública, lo que permite que la empresa ahorre dinero en largas líneas alquiladas privadas. Las VPN de sitio a sitio pueden dividirse entre intranet y extranet. Una VPN de sitio a sitio creada entre oficinas de la misma empresa es una VPN intranet, mientras que una VPN creada para conectar la empresa con su empresa asociada o un cliente es una VPN extranet.

g) Tecnología VPN

Tecnologías de VPN Una VPN bien diseñada utiliza varios métodos para mantener la conexión y los datos seguros.

Confidencialidad de los datos: probablemente se trata del servicio más importante suministrado por cualquier implementación de VPN. Dado que los datos privados viajan por una red pública, conservar su confidencialidad es de importancia vital y para ello se cifran. Cifrar es el proceso de tomar todos los datos que un equipo envía a otro equipo y codificarlos de tal modo que sólo el equipo que los recibe pueda descodificarlos.

La mayoría de las VPN utilizan los protocolos siguientes para suministrar cifrado (32).

IPSec: protocolo de seguridad del protocolo de Internet (IPSec) proporciona características de seguridad mejoradas como algoritmos de cifrado más fuertes y una autenticación más amplia. IPSec tiene dos modos de cifrado: de túnel y de transporte. El modo de túnel cifra la cabecera y la carga de cada paquete, mientras que el modo de transporte sólo cifra la carga. Sólo los sistemas compatibles con IPSec pueden aprovechar este protocolo. Asimismo, todos los dispositivos deben utilizar una clave o certificado común y tener configuradas políticas de seguridad similares.
Para los usuarios de VPN de acceso remoto, algún tipo de paquete de software de otros fabricantes permite la conexión y cifrado en el equipo de los usuarios. IPSec admite el cifrado de 56 bits (DES único) o de 168 bits (DES triple).

PPTP/MPPE: PPTP fue creado por el foro PPTP, un consorcio en el que figuran US Robotics, Microsoft, 3COM, Ascend y ECI

Telematics. PPTP es compatible con las VPN de varios protocolos, con cifrado de 40 y 128 bits que utilizan un protocolo llamado MPPE (Cifrado punto a punto de Microsoft). Por sí mismo, PPTP no proporciona cifrado de datos.

L2TP/IPSec: por lo general, llamado L2TP sobre IPSec. Aporta la seguridad del protocolo IPSec sobre la tunelización del protocolo de tunelización de la capa 2 (L2TP). L2TP es el producto de una asociación entre los miembros del foro PPTP, Cisco y el Grupo de trabajo de ingeniería en Internet (IETF). Se utiliza principalmente en las VPN de acceso remoto con sistemas operativos Windows 2000, dado que Windows 2000 proporciona un cliente L2TP e IPSec nativo. Los proveedores de servicio de Internet también pueden suministrar conexiones L2TP a usuarios de acceso telefónico y, a continuación, cifrar el tráfico con IPSec entre su punto de acceso y el servidor de red de la oficina remota.

h) Que es OpenVpn

OpenVPN es una de las soluciones de software para VPN más populares y utilizadas. Su popularidad se basa en sus sólidas características, facilidad de uso y amplio soporte. OpenVPN es un software de código abierto, lo que significa que todo el mundo lo puede usar gratuitamente y modificarlo si es necesario. OpenVPN puede ser utilizada para varias necesidades de conectividad, pero es especialmente popular para disfrutar de un acceso anónimo y privado a Internet.

OpenVPN funciona bajo modo cliente y servidor. Esto significa que existe un servidor OpenVPN que está conectado a Internet. El cliente de OpenVPN se conecta al servidor, y así obtiene acceso completo a Internet. Una vez conectado al servidor, el cliente utiliza el servidor

para terminar todo su tráfico de Internet. Esto significa que el cliente es visto como el servidor, o lo que es lo mismo, el cliente adopta la ubicación física y los contactos administrativos del servidor. Por lo tanto, toda la privacidad del cliente OpenVPN está protegida (33).

i) CERTIFICADOS SSL Y PROTOCOLO TSL

Los certificados SSL (capa de sockets seguros) son una pieza esencial de la seguridad de los sitios web. Al visitar un sitio web con SSL, el certificado SSL del sitio web permite cifrar los datos que se envían, como la información sobre tarjetas de créditos, nombres y direcciones de modo que ningún hacker pueda acceder a ellos. Para comprobar si un sitio web usa SSL correctamente, escriba la dirección del sitio web en nuestro Comprobador de instalación SSL (34).

El protocolo TLS (seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL. Si bien aún denominamos a nuestros certificados de seguridad SSL porque es un término más común, al comprar certificados SSL en Symantec, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA (34).

2.3. Sistema de hipótesis

2.3.1. Hipótesis principal

El diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016 permitirá solucionar los problemas de comunicación y acceso de información entre sedes de la empresa y la oficina principal.

2.3.2. Hipótesis específicas

1. La identificación de los requerimientos de conexión y seguridad permitirán garantizar las necesidades de la empresa.

2. La evaluación de las diferentes tecnologías que se pueden utilizar permitirá reforzar el diseño para la implementación de una red privada virtual.

3. La propuesta de implementación de las tecnologías de red privada virtual aprovechara de manera adecuada los recursos tecnológicos disponibles de la empresa.

III. METODOLOGÍA

3.1. Diseño de la investigación

La presente investigación fue de diseño no experimental y de corte transversal, podríamos definirla como la investigación que se realiza sin manipular deliberadamente variables (35).

Según **Ortiz** (36)**,** nos dice: en la investigación no experimental se observa fenómenos tal y como se presentan en su contexto natural, se obtienen datos y después estos se analizan.

Por la características del su ejecución fue de corte transversal y de nivel descriptiva porque se apunta a un momento y tiempo definido. Por otro lado, un estudio transversal toma una instantánea de una población en un momento determinado, lo que permite extraer conclusiones acerca de los fenómenos a través de una amplia población (37).

3.2. Población y Muestra

Población es el conjunto de elementos que tienes características comunes (38). La población es la que constituye el objeto de la investigación, y por la cual se convierte en el centro de la misma y de ella se extrae la información requerida para el estudio requerido.

La muestra es un subconjunto fielmente representativo de la población (39). Asimismo la muestra, es fundamental para el análisis de datos de todo proyecto de investigación, deben sintetizarse en muchos casos, el conjunto de sujetos con características semejantes que están sometidos al estudio.

En el caso para esta investigación, la población objeto de estudio estuvo constituida por el personal del área administrativa que estaban vinculados con

las TIC y que usaban una PC, de toda la población se tomó 30 trabajadores como muestra de los que forman la población que estaban distribuidos de la siguiente forma:

Tabla Nro. 8: División Trabajadores Agromar Industrial S.A.

Sedes	**Área**	**Cantidad**
Agromar Industrial	Administrativa y almacén	15
Aceites Esenciales del Perú S.A.C.	Administrativa	8
Cítricos Peruanos S.A	Administrativa	7
	Total	30

Fuente: Elaboración propia

3.3. Técnicas e instrumentos.

3.3.1. Técnica

Se utilizó la técnica de la encuesta, aplicada a cada uno de los empleados que constituyen la muestra. Con esta técnica de recolección de datos da lugar a establecer contacto con las unidades de observación por medio de los cuestionarios previamente establecidos.

3.3.2. Instrumentos

Los instrumentos fueron aplicados en las áreas que conforman la muestra. Se utilizó un listado de preguntas referentes a la definición de la arquitectura de las redes e información para determinar el estado actual.

3.4. Procedimiento de recolección de datos.

Se seleccionó a las personas adecuadas, para poder aplicar los cuestionarios, ya que así se obtuvo la información apropiada, por medio de visitas a las diversas sedes de la empresa Agromar Industrial S.A.

Asimismo se entregó los cuestionarios a las personas seleccionadas, para poder resolver cualquier duda en relación a las interrogantes planteadas en los mismos.

Se creó un archivo en formato MS Excel 2013 para la tabulación de las respuestas de cada cuestionario en base a cada dimensión de estudio, así se obtuvo rápidamente los resultados y se pudo dar su conclusión a cada una de ellas.

3.5. Definición operacional de las variables en estudio

Tabla Nro. 9: Matriz de operacionalización de Variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Escala de medición	Definición Operacional
Diseño de Red Privada Virtual.	El Diseño es una actividad creativa cuyo propósito es establecer las cualidades multifacéticas de objetos, procesos, servicios y sus sistemas, en todo su ciclo de vida (40) . Una red privada virtual (VPN) es una tecnología que crea una conexión cifrada en una red menos segura (41).	Acceso a la información	• Se puede compartir archivos en red. • Las impresoras están en red. • Actualmente se puede compartir recursos.	Ordinal	• SI • NO
		Servicio de red	• La red actual es estable • Personal especializado en red de datos		
		Seguridad de la información	• Políticas de seguridad • Autentificación de usuarios • Privilegios de usuarios		

3.6. 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..

IV. RESULTADOS

4.1. Resultados

A. Dimensión 01. ACCESO A LA INFORMACIÓN

Tabla Nro. 10: Disponibilidad de la información

Distribución de frecuencias y respuestas relacionadas con la disponibilidad de la información entre las áreas de la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	9	30,00
No	21	70,00
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuenta con disponibilidad de la información entre las áreas?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 10 se aprecia que el 70% de los trabajadores encuestados opinaron que NO tienen disponibilidad de la información entre las áreas de la empresa, mientras que el 30% dijeron que SI tenían disponibilidad de la información.

Tabla Nro. 11: Eficiencia de servicio

Distribución de frecuencias y respuestas relacionadas con la eficiencia del servicio de acceso a la información de la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	6	20,00
No	24	80,00
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe eficiencia con el servicio de acceso a la información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro.11 se aprecia que el 80% de los trabajadores encuestados dijeron que NO existe eficiencia con el servicio de acceso a la información, mientras que el 20% dijeron que SI tienes un buen servicio de acceso a la información.

Tabla Nro. 12: Conexión entre sucursales

Distribución de frecuencias y respuestas relacionadas con la conexión de sucursales en una sola red de trabajo en la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	1	3,33
No	29	96,67
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree usted que las sucursales de la empresa se encuentran conectadas en una sola red de trabajo?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 12 se aprecia que el 96,67% de los trabajadores encuestados expresaron que NO existe una conexión de locales en una sola red de trabajo, mientras que el 3,33% dijeron que SI están conectadas.

Tabla Nro. 13: Velocidad transmisión de datos

Distribución de frecuencias y respuestas relacionadas con la velocidad de transmisión de datos; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	14	46,67
No	16	53,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Tiene problemas con la velocidad transmisión de datos?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 13 se aprecia que el 53.33% de los trabajadores encuestados dijeron que NO existe problemas con la velocidad de transmisión de datos, mientras que el 46,67% respondieron que SI tienen problemas con la velocidad de transmisión de datos.

Tabla Nro. 14: Acceso a la información

Distribución de frecuencias y respuestas relacionadas con el acceso a la información de las demás empresas; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	15	50,00
No	15	50,00
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree usted que es necesario acceder a la información de las demás sucursales?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 14 se aprecia que el 50% de los trabajadores encuestados expresaron que NO es necesario acceder a la información de las otras empresas, mientras que el 50% respondieron que si hay una necesidad de acceso a información de las sucursales de la empresa.

Tabla Nro. 15: Transmisión de información entre sucursales.

Distribución de frecuencias y respuestas relacionadas con la trasmisión de la información mediante la red de datos para las diferentes áreas y sucursales de la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	10	33,33
No	20	66,67
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿La información se transmite mediante la red de datos para diferentes áreas y sucursales de la empresa?, Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 15 se observa que el 66,67% de los trabajadores encuestados manifestaron que NO se trasmite la información mediante la red de datos hacia las áreas y sucursales de la empresa y el 33,33% respondieron que SI hay una trasmisión de la información.

Tabla Nro. 16: Capacidad de Compartir archivos

Distribución de frecuencias y respuestas relacionadas con la capacidad de compartir archivos mediante la red o con otro compañero de trabajo; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	11	36,67
No	19	63,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Actualmente puede compartir sus archivos mediante la red o con otro compañero de trabajo?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 16 se aprecia que el 63,33% de los trabajadores encuestados dijeron que NO tienen la capacidad de compartir archivos mediante la red o con otro compañero de trabajo y el 36,67% respondieron que SI pueden compartir archivos mediante la red.

Tabla Nro. 17: Medios físicos

Distribución de frecuencias y respuestas relacionadas a la utilización de medios físicos (memoria, disco duro) para compartir información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	17	56,67
No	13	43,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Utiliza algún medio físico (memoria, disco duro) para compartir información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 17 se aprecia que el 56,67% de los trabajadores encuestados dijeron que SI utilizan medios físicos (memorias, disco duro) para compartir información y que el 43,33% respondieron que NO utilizan ningún medio físico para compartir información.

Tabla Nro. 18: Conformidad con el servicio

Distribución de frecuencias y respuestas relacionadas a la conformidad con el servicio de red y acceso a la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	09	30,00
No	21	70,00
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Está conforme con el servicio de red y acceso de la información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 18 se aprecia que el 70,00% de los trabajadores encuestados manifestaron que NO están conformes con el servicio de red y acceso a la información y el 30,00% respondieron que SI están conformes con el servicio actual de la red y el acceso a la información que utilizan.

Tabla Nro. 19: Integridad de la información

Distribución de frecuencias y respuestas relacionadas a la integridad de la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	14	46,67
No	16	53,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree usted que hay integridad de la información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 19 se aprecia que el 53,33% de los trabajadores encuestados respondieron que NO creen que haya una integridad de la información y que 46,67% respondieron que SI existe integridad de los datos.

Tabla Nro. 20: Dimensión acceso a la información

Distribución de frecuencias y respuestas relacionadas con la dimensión 01: Acceso a la información: respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	09	30.00
No	21	70.00
Total	30	100.00

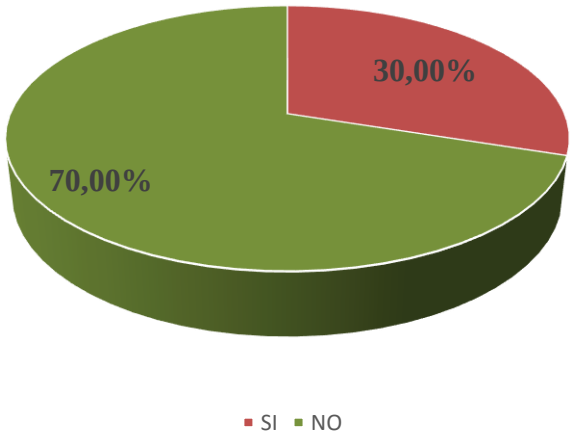
Fuente: Aplicación del instrumento para medir el nivel el acceso a la información, basado en 30 preguntas aplicadas a los trabajadores de la empresa Agromar Industrial S.A; 2016.

Aplicado por: Criollo; I.; 2016.

En la tabla Nro. 20 se puede interpretar que el 70.00% de los trabajadores encuestados NO tiene el suficiente acceso a la información de la empresa mientras que el 30.00% de ellos dijeron SI tenían el acceso a la información.

Gráfico Nro. 7: Resultados de la dimensión acceso a la información

Distribución porcentual de las frecuencias y respuestas relacionadas con la dimensión 01: Acceso a la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.



Fuente: Tabla Nro. 20.

B. Dimensión 02: SEGURIDAD DE RED

Tabla Nro. 21: Medidas de seguridad

Distribución de frecuencias y respuestas relacionadas a las medidas de seguridad para proteger la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	10	33,33
No	20	66,67
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Según usted cree que existen medidas de seguridad para proteger la información que comparte?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 21 se aprecia que el 66,67% de los trabajadores encuestados manifestaron que NO creen que hayan medidas de seguridad para proteger la información y el 33,33% respondieron que SI existen medidas de seguridad para salvaguardar la información.

Tabla Nro. 22: Autentificación de usuarios

Distribución de frecuencias y respuestas relacionadas a la autentificación de usuarios en el intercambio de la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	14	46,67
No	16	53,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe autenticación de usuarios en el intercambio de la información, que se realizan mediante los sistemas?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 22 se aprecia que el 53,33% de los trabajadores encuestados expresaron que NO hay autentificación de usuarios y el 46,67% respondieron que SI se autentifican al usar los sistemas.

Tabla Nro. 23: Privilegios de usuario

Distribución de frecuencias y respuestas relacionadas a los privilegios de usuario de acuerdo al uso de los sistemas de información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	12	40,00
No	18	60,00
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Hay privilegios de los usuarios, respecto al uso de los sistemas de información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 23 se aprecia que el 60,00% de los trabajadores encuestados dijeron que NO hay privilegios de usuarios de acuerdo al uso de los sistemas de información y el 40,00% respondieron que SI disponen de privilegios de usuarios.

Tabla Nro. 24: Seguridad direccionada a los procesos de negocio

Distribución de frecuencias y respuestas relacionadas a la seguridad direccionada a los procesos de negocio de la empresa; del diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	11	36,67
No	19	63,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿La seguridad de los sistemas de información, están direccionadas a los procesos de negocios?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 24 se aprecia que el 63,33% de los trabajadores encuestados expresaron que NO creen que la seguridad este direccionada a los procesos de negocio de la empresa y el 36,67% respondieron que SI piensan que la seguridad está encaminada a los procesos de negocio de la empresa.

Tabla Nro. 25: Políticas de seguridad

Distribución de frecuencias y respuestas relacionadas a las políticas de seguridad en el uso de la red e internet establecidas por la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	06	20,00
No	24	80,00
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree que hay políticas de seguridad en el uso de la Red e Internet?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 25 se aprecia que el 80,00% de los trabajadores encuestados manifestaron que NO creen que haya políticas de seguridad con respecto al uso de la red e internet y el 20,00% respondieron que SI creen que existan políticas de seguridad para el uso de la red e internet.

Tabla Nro. 26: Seguridad al compartir información.

Distribución de frecuencias y respuestas relacionadas a la seguridad al compartir información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	07	23,33
No	23	76,67
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Usted se siente seguro al compartir información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 26 se aprecia que el 76,67% de los trabajadores encuestados dijeron que NO se sienten seguros al compartir información y el 23,33% manifestaron que SI sentían seguridad al compartir información.

Tabla Nro. 27: Prevención, detección y corrección de software malicioso.

Distribución de frecuencias y respuestas relacionadas a la prevención, detección y corrección de software malicioso; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	20	66,67
No	10	33,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree usted que hay prevención, detección y corrección de Software malicioso?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 27 se aprecia que el 66,67% de los trabajadores encuestados dijeron que SI hay prevención, y corrección de software malicioso y el 33,33% opinaron que NO hay detección y corrección de software malicioso.

Tabla Nro. 28: Instalación de antivirus

Distribución de frecuencias y respuestas relacionadas a la instalación de antivirus en los ordenadores; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	13	43,33
No	17	56,67
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Los ordenadores de su empresa, tienen instalado antivirus?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 28 se observa que el 56,67% de los trabajadores encuestados expresaron que NO tenían antivirus instalados en los ordenadores y el 43,33% expresaron que SI contaban con un antivirus.

Tabla Nro. 29: Copias de seguridad

Distribución de frecuencias y respuestas relacionadas a la realización de copias de seguridad de la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	08	26,67
No	22	73,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Se realiza copia de seguridad de los datos de la empresa?, Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 29 se aprecia que el 733,3% de los trabajadores encuestados consideran que NO se realizan copias de seguridad de la información de la empresa y el 26,67% expresaron que SI se realiza tal medida de seguridad.

Tabla Nro. 30: Firewall de internet

Distribución de frecuencias y respuestas relacionadas a la existencia de firewall de internet; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	05	16,67
No	25	83,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuenta con un firewall de internet?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 30 se aprecia que el 83,33% de los trabajadores encuestados consideran que NO existe ningún firewall de internet y el 16,67% dijeron si cuentan con un firewall de internet.

Tabla Nro. 31: Dimensión seguridad de la red

Distribución de frecuencias y respuestas relacionadas con la dimensión 01: seguridad de la red; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	08	26,67
No	22	73,33
Total	30	100,00

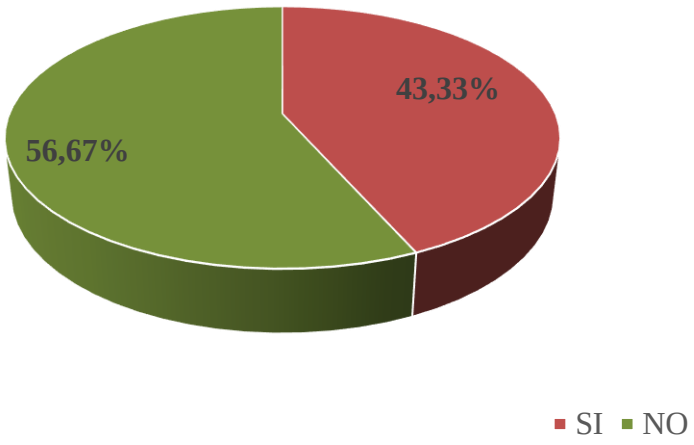
Fuente: Aplicación del instrumento para medir la seguridad de red, basado en 30 preguntas aplicadas a los trabajadores de la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 31 se puede lograr interpretar que el 73,33% de los trabajadores encuestados manifestaron que NO hay seguridad en la red de datos, mientras el 26,67 testifico que SI hay seguridad en la red de datos.

Grafico Nro. 8: Resultados de la dimensión seguridad de la red

Distribución porcentual de las frecuencias y respuestas relacionadas con la dimensión 02: Seguridad de la red respecto al del diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.



Fuente: Tabla Nro. 31.

C. Dimensión 03: DISEÑO DE RED PRIVADA VIRTUAL

Tabla Nro. 32: Diseño de red privada virtual

Distribución de frecuencias y respuestas relacionadas al servicio de comunicación y seguridad de información de la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	29	96,67
No	01	3,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree necesario realizar un diseño de una red privada virtual para mejorar el servicio de comunicación y seguridad de información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 33 se aprecia que el 96,67% de los trabajadores encuestados manifestaron que SI creen necesario el diseño de la red privada virtual y el 3,33% dijeron NO era necesario.

Tabla Nro. 33: Propuesta de una red privada virtual

Distribución de frecuencias y respuestas relacionadas a la propuesta de una red privada virtual; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	26	86,67
No	04	13,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿A su opinión considera que la propuesta de una red privada virtual sea necesaria para una posterior implementación?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 34 se aprecia que el 86,67% de los trabajadores encuestados consideran que SI es necesario la propuesta de una red privada virtual para una posterior implementación y el 13,33% dijeron que NO era necesario.

Tabla Nro. 34: Simplificación del trabajo

Distribución de frecuencias y respuestas relacionadas a la simplificación del trabajo con la red privada virtual; del diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	25	83,33
No	05	16,67
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿A su criterio piensa o cree que una red privada virtual le simplificaría el trabajo diario?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 35 se aprecia que el 83,33% de los trabajadores encuestados respondieron que la red privada virtual SI simplificara el trabajo diario en la empresa y el 16,67% dijeron NO lo haría.

Tabla Nro. 35: Beneficios de la red privada virtual

Distribución de frecuencias y respuestas relacionadas a si beneficiara o no la red privada virtual a los trabajadores de la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	30	100,00
No	-	-
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree usted que una eventual implementación de una red privada virtual beneficiaria a los trabajadores de la empresa?, Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 36 se aprecia que el 100,00% de los trabajadores encuestados expresaron que una eventual implementación de una red privada virtual SI beneficiaria a todos los trabajadores de la empresa.

Tabla Nro. 36: Mejor acceso de la información

Distribución de frecuencias y respuestas relacionadas al mejoramiento del acceso a la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	27	90,00
No	03	10,00
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Piensa que la implementación de una red privada virtual permitiría un mejor acceso a la información?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 37 se aprecia que el 90,00% de los trabajadores encuestados contestaron que la implementación de la red privada virtual SI mejoraría el acceso de la información y el 10.00% dijeron que NO mejoraría el acceso a la información.

Tabla Nro. 37: Garantizar integridad de los datos

Distribución de frecuencias y respuestas relacionadas a garantizar la integridad de los datos e información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	23	76,67
No	07	23,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿A su opinión cree que la implementación de una red privada virtual garantizaría la integridad de los datos?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 38 se aprecia que el 76,67% de los trabajadores encuestados contestaron que la implementación de la red privada virtual SI garantizara la integridad de los datos y el 23,33% expresaron que NO.

Tabla Nro. 38: Comunicación entre diferentes sucursales de trabajo

Distribución de frecuencias y respuestas relacionadas a la implementación de una red privada virtual de acuerdo si comunicaría a las diferentes sucursales de trabajo; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	**n**	**%**
Si	29	96,67
No	01	3,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Considera que una red privada virtual comunicaría a las diferentes sucursales de trabajo?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 39 se aprecia que el 96,67% de los trabajadores encuestados indicaron que la implementación de la red privada virtual SI comunicaría a las diferentes sucursales de trabajo y el 3,33% expresaron que NO.

Tabla Nro. 39: Compartir archivos de forma segura

Distribución de frecuencias y respuestas relacionadas a compartir archivos de forma segura; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	20	66,67
No	10	33,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cree usted que una eventual implementación de una red privada virtual le permitiría compartir archivos de forma segura?, en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 40 se aprecia que el 66,67% de los trabajadores encuestados indicaron que una eventual implementación de la red privada virtual SI permitiría compartir archivos de forma más segura y el 33,33% contestó que la implementación NO permitiría compartir archivos de forma segura.

Tabla Nro. 40: Privacidad de la información

Distribución de frecuencias y respuestas relacionadas a la privacidad de la información; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	19	63,33
No	11	36,67
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿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?, Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 41 se aprecia que el 63,3% de los trabajadores encuestados expresaron que la implementación de la red privada virtual SI ayudaría a mejorar la privacidad de la información y el 36,67% contestó que la implementación NO ayudaría en la seguridad de la información.

Tabla Nro. 41: Imagen institucional de la empresa

Distribución de frecuencias y respuestas relacionadas a la imagen institucional de la empresa; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	26	86,67
No	4	13,33
Total	30	100,00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Considera que la implementación de una red privada virtual ayudara a mejorar la imagen institucional de la empresa?, Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 42 se aprecia que el 86,67% de los trabajadores encuestados expresaron que la implementación de la red privada virtual SI ayudara a mejorar la imagen institucional de la empresa y el 13,33% respondió que NO.

Tabla Nro. 42: Dimensión diseño de la red privada virtual

Distribución de frecuencias y respuestas relacionadas con la dimensión 03: diseño de la red privada virtual respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Alternativa	n	%
Si	30	100,00
No	-	-
Total	30	100,00

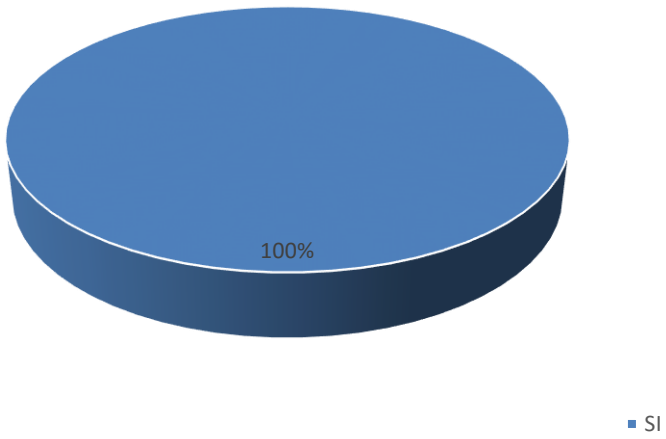
Fuente: Aplicación del instrumento para medir el diseño de la red privada virtual, basado en 30 preguntas aplicadas a los trabajadores de la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 43 se aprecia que el 100,00% de los trabajadores encuestados SI están de acuerdo con el diseño para la implementación de la red privada virtual.

Gráfico Nro. 9: Resultados de la dimensión diseño de la red privada virtual

Distribución porcentual de las frecuencias y respuestas relacionadas con la dimensión 03: Diseño de la red privada virtual; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.



Fuente: Tabla Nro. 43.

Tabla Nro. 43: Resumen general de las dimensiones

Distribución de frecuencias y respuestas relacionadas con las tres dimensiones definidas para determinar los requerimientos y seguridad, respecto al diseño de la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Dimensiones	SI		NO		TOTAL	
	n	%	n	%	n	%
Acceso a la información	9	30,00	21	70,00	30	100,00
Seguridad de red	8	26,67	22	73,33	30	100,00
Diseño de la red privada virtual	30	100,00	-	-	30	100,00

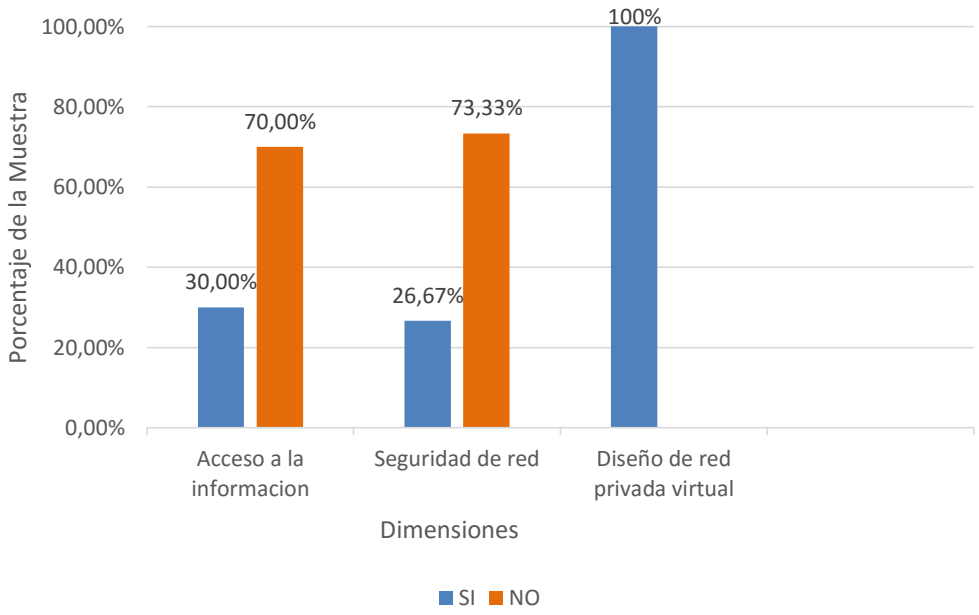
Fuente: Aplicación del instrumento para el conocimiento de los trabajadores encuestados acerca de las tres dimensiones definidas para la investigación; respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.

Aplicado por: Criollo, I.; 2016.

En la Tabla Nro. 44 se aprecia que el 100,00% de los trabajadores encuestados SI están de acuerdo con el diseño para la implementación de la red privada virtual.

Gráfico Nro. 10: Resumen general de las dimensiones

Distribución porcentual de las frecuencias y respuestas relacionadas con las tres dimensiones definidas para determinar los requerimientos y seguridad, respecto al diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016.



Fuente: Elaboración propia

4.2. Análisis de resultados

El objetivo general de la presente investigación fue: Realizar el diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; que solucione los problemas de comunicación y acceso a la información entre las sucursales de la empresa; en este sentido para poder cumplir con este objetivo es preciso realizar una apreciación del escenario actual a fin de que este diseño identifique claramente las necesidades y pueda cubrir las exigencias de la entidad a través de una propuesta de mejora seria y técnica.

Para realizar esta sección de análisis de resultados se diseñó un cuestionario agrupado en 03 dimensiones y luego de los resultados obtenidos e interpretados en la sección anterior, se realiza el siguiente análisis:

1. En lo que respecta a la dimensión: Acceso a la información, en la Tabla Nro. 20, nos muestra los resultados donde podemos apreciar que el 70% 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 Romero y Romero (3), en su investigación donde obtuvo como resultado en una dimensión similar a la nuestra, un resultado de 79% 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 las otras sucursales de la empresa.

2. Con relación a la dimensión: Seguridad de la red, en la tabla Nro. 31 nos detalla los resultados donde se puede observar que el 73,33% de los trabajadores expreso que NO cuentas con una buena seguridad de la red, este resultado no coincide con el obtenido por Alva (7), donde en una investigación similar obtuvo como deducción que el 60% de los trabajadores manifestaron que había seguridad de red en la empresa en la que laboraban sin embargo este resultado coincide con los logrados por Molina (9), donde se indica que el 80% de los trabajadores expresaron que no existe seguridad en la red que utilizan. Esta similitud de los resultados se justifica porque en la primera empresa objeto de estudio evidencia que la empresa solicita trabajadores con conocimientos avanzados en manejo de tic mientras que en la última evidencia la ausencia de estándares de calidad en gestión de tráfico de red, y políticas de seguridad no alineadas a las necesidades de la empresa.

3. Asimismo de acuerdo a los resultados obtenidos en la dimensión: Diseño de la red privada virtual, la Tabla Nro. 43 nos muestra los resultados donde se puede observar que el 100.00% 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 Aguilar y Ramírez (5), donde en su investigación indica que los trabajadores están de acuerdo en el diseño e implementación de una red privada virtual, así mismo coincide con la investigación de Molina (9), donde sus resultados indican que en su totalidad están de acuerdo con la propuesta de segmentación con redes privadas. Esta similitud en los resultados se justifica porque todas empresas en estudio partes de una necesidad en común, la cual es conectar las diferentes sucursales y áreas que operan totalmente aisladas la una de las otra, 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.

4.3. Propuesta de mejora

Luego de haber desarrollado cada uno de 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 Ubuntu Server en su versión 16.0, teniendo en cuenta que la empresa Agromar Industrial S.A tiene como plataforma principal de sistema operativo Windows la aplicación cliente de 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

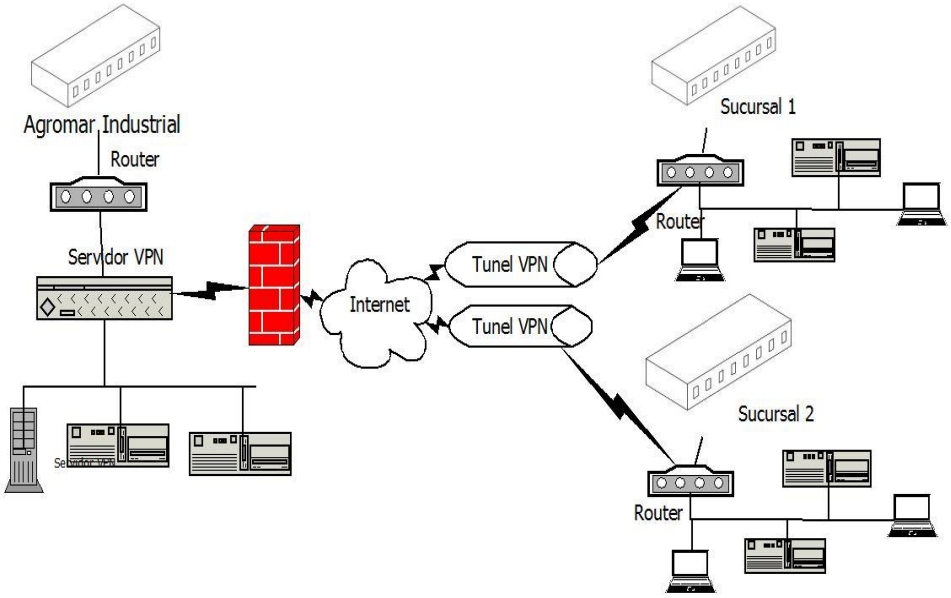
   Lo que sea desea es tener la posibilidad de acceder a una red local (protegida detrás de un firewall/gateway) desde Internet (o desde cualquier otra red insegura). El fin es que un usuario de la empresa ubicado físicamente fuera de la red local y posiblemente a kilómetros de distancia parezca conectado 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 Nro. 11: 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 adaptar 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 porqué 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 conectase 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 adquiera 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 luegon 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, ejecutoriaremos 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:

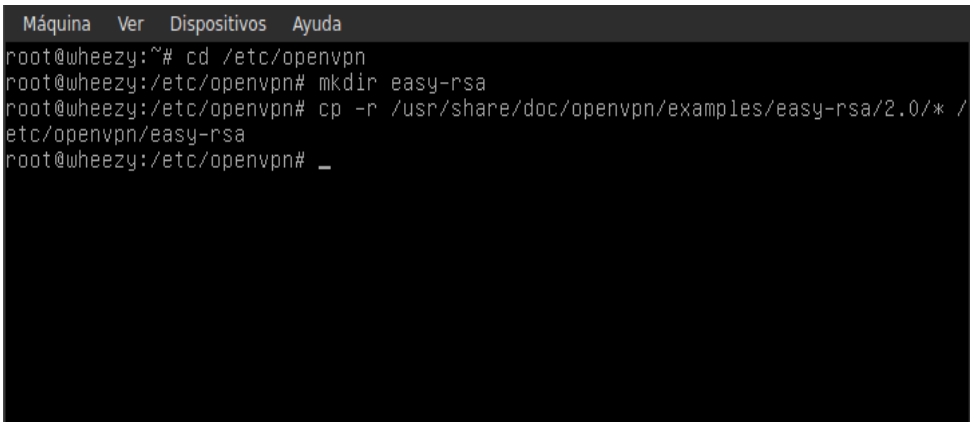
```
cd /etc/openvpn

mkdir easy-rsa
```

Después hay que copiar los scripts de configuración de OpenVPN, que se hallan en la ubicación /usr/share/doc/openvpn/examples/easy-rsa/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 Nro. 12: Captura copia de script de configuración



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 incrementarios del 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 autentificación 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=Agromar Industrial

export KEY_EMAIL=contacto@gmail.com

export KEY_EMAIL=contacto@gmail.com

export KEY_CN= agromar

export KEY_NAME=vpnagromar

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-rsa/keys. Para ejecutar el script tenemos que teclear el siguiente comando en la terminal:

```
./clean-all
```

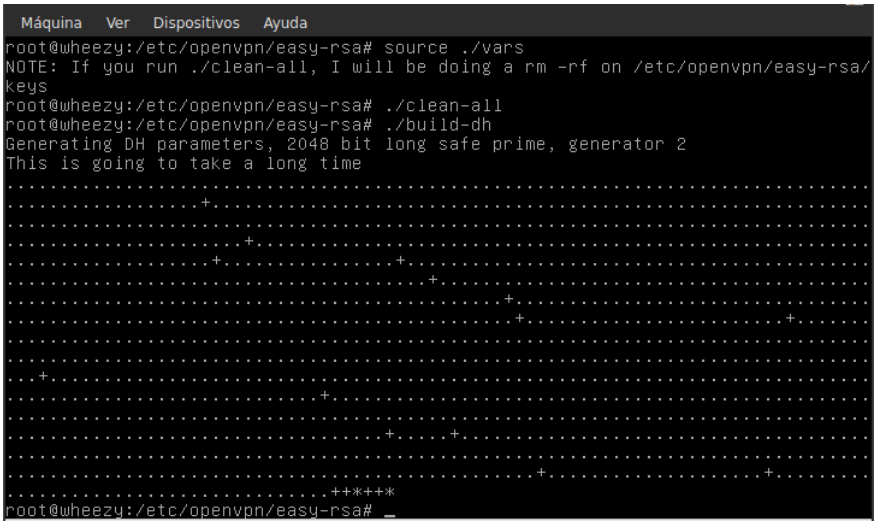
El siguiente paso es generar los parámetros de Diffie Hellman. Los parámetros de Diffie Hellman se utilizarán para poder intercambiar las claves ente cliente y servidor de forma segura. Para poder realizar este paso tenemos que teclear el siguiente comando en la terminal:

```
./build-dh
```

Al terminar el proceso dentro de la ubicación /etc/openvpn/easy-rsa/keys se habrá creado el archivo dh2048.pem que contiene los parámetros Diffie Hellman.

Este parámetro se usará para poder un intercambio de claves entre 2 participantes de forma segura.

Gráfico Nro. 13: Exportar variables



Fuente: Elaboración propia

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:

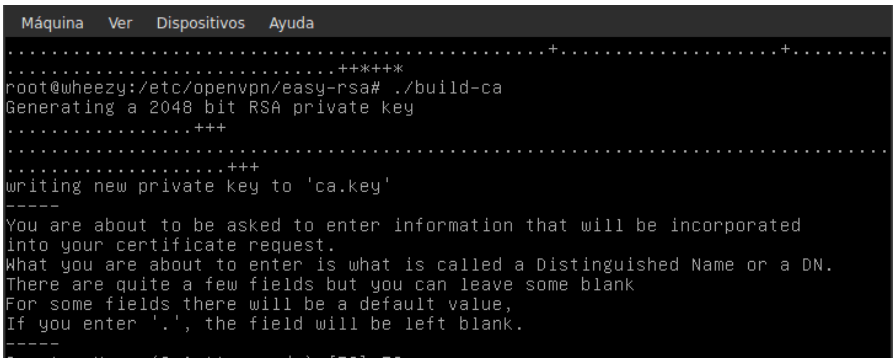
./build-ca

Al terminar el proceso dentro de la ubicación /etc/openvpn/easy-rsa/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 Nro. 14: Creación de certificado y clave privada.



Fuente: elaboración propia

7. Generar certificados y la clave del servidor OpenVPN

Vamos a introducimos 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/easy-rsa/keys se habrán creado los siguientes archivos:

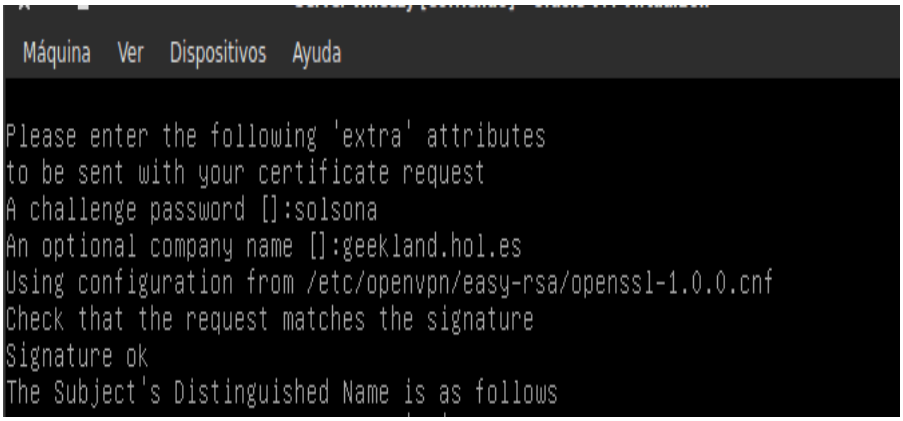
whezzyVPN.key: Este fichero contiene la clave privada del servidor. Este archivo no debe estar al alcance de nadie.

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 Nro. 15: Generar certificados y clave del servidor



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

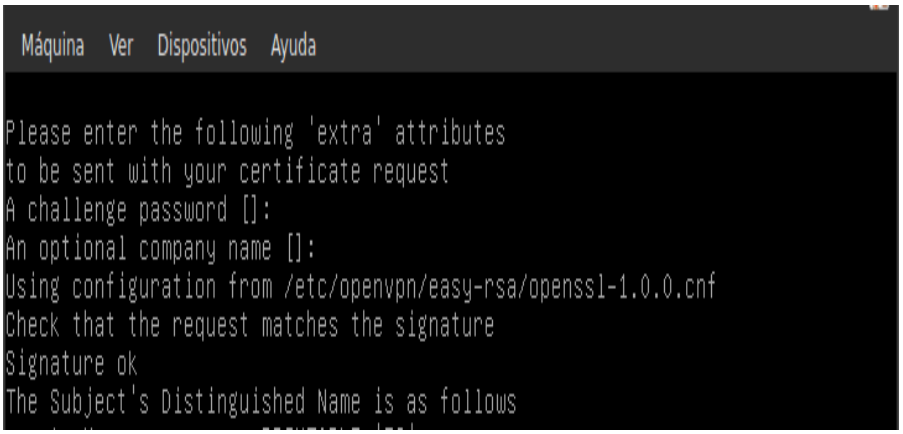
Una vez introducido este comando se nos hará una serie de preguntas. Simplemente tienen que contestar el valor por defecto ya que anteriormente hemos editado el fichero vars.

Al terminar el proceso dentro de la ubicación /etc/openvpn/easy-rsa/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 Nro. 16: Generar certificados y las claves de usuarios



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 autentificación 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:

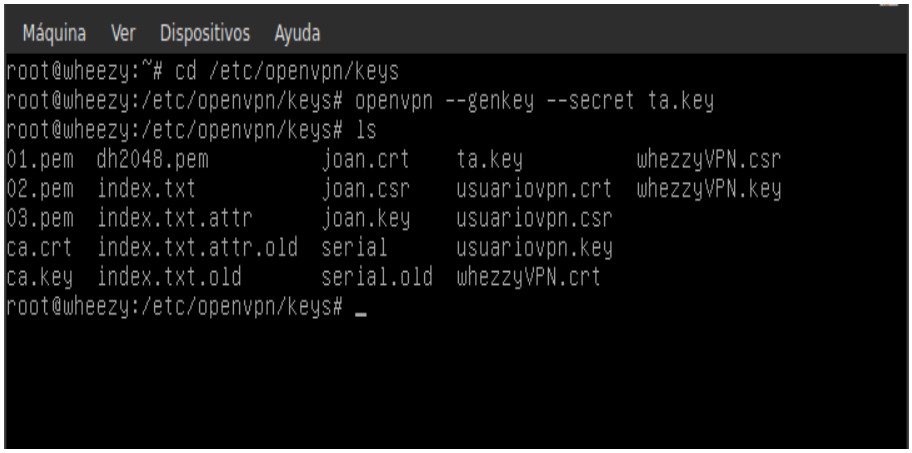
cd /etc/openvpn/easy-rsa/keys

Una vez hemos accedido a la ubicación /etc/opnevpn/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 Nro. 17: Generación de clave de seguridad



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 autentificación 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 Nro. 44: Ubicación de las claves generadas

Archivo	***Descripción***	***Ubicación***	***Secreto***
dh2048.pem	Parámetros Diffie Hellman	Servidor (/etc/openvpn)	Sí
ca.crt	Certificado raíz de la entidad certificadora	Servidor (/etc/openvpn) y cliente	No
ca.key	Clave de la entidad certificadora	Servidor (/etc/openvpn)	Sí
whezzyVPN.key	Clave del servidor VPN	Servidor (/etc/openvpn)	Sí
whezzyVPN.crt	Certificado del servidor VPN	Servidor (/etc/openvpn) y cliente	No
whezzyVPN.csr	Archivo de petición de certificado	Servidor (/etc/openvpn)	No

usuariovpn.key	Clave privada del cliente VPN	Cliente	Sí
usuariovpn.crt	Certificado del cliente VPN	Cliente	No
usuariovpn.csr	Archivo de petición de certificado	Servidor (/etc/openvpn)	No
ta.key	Clave para la Autentificación 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:

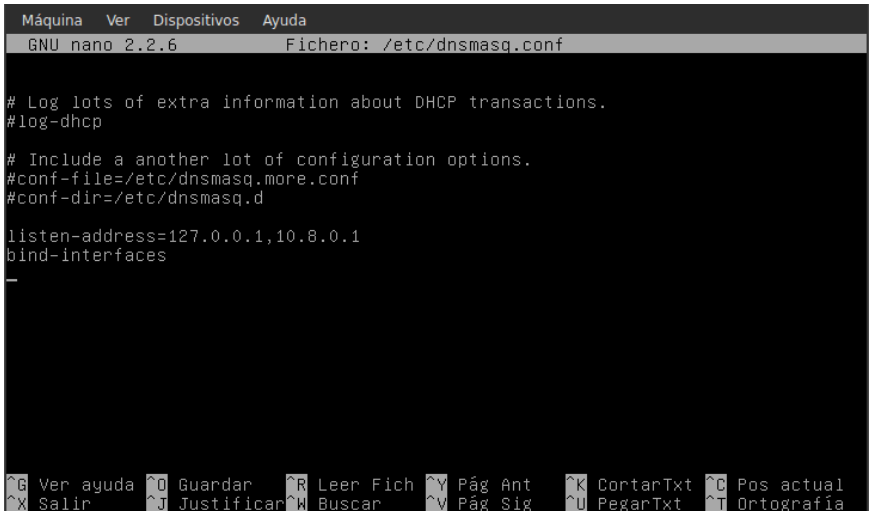
nano /etc/dnsmasq.conf

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

listen-address=127.0.0.1,192.168.0.1

bind-interfaces

Gráfico Nro. 18: Configuración dnsmasq



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 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.

Tabla Nro. 45: Parámetros de configuración del servidor

Parámetro	**Descripción**
dev tun	Dispositivo virtual en el cual se creara el túnel.
proto udp	Protocolo de la conexión VPN. También podríamos usar el tcp.
port 1194	Puerto de escucha del servicio. El puerto de escucha se puede modificar.
ca ca.crt	Certificado de la autoridad certificadora que creamos.
cert whezzyVPN.crt	Certificado del servidor que hemos creado.
key whezzyVPN.key	Clave privada del servidor que hemos creado.
dh dh2048.pem	Carga de los parámetro de Diffie Hellman.

Server 10.8.0.0 255.255.255.0	Indicamos que a los clientes del VPN se les asignará IP del tipo 10.8.0.0/24
ifconfig-pool-persist ipp.txt	Se crea un fichero ipp.txt en el que se registran las IP de los clientes que se conectan al servidor VPN.
push "route 192.168.1.0 255.255.255.0"	Con esta línea hacemos que los paquetes que tengan como destino la red 192.168.1.0 viajen por la interfaz del túnel (tun0). De esta forma el cliente VPN se podrá comunicar con cualquier máquina de la red 192.168.1.0.
keepalive 10 120	El servidor VPN enviará un ping cada 10 segundos y como máximo esperará 120 segundos para que el cliente de una contestación.
tls-aut ta.key 0	Activación de la autentificación TLS en el servidor.
comp-lzo	Activar compresión LZO para la transmisión de datos.
max-clients 10	Número máximo de clientes que se pueden conectar de forma simultánea. El valor se puede modificar según las necesidades.
user nobody	Para limitar los privilegios del demonio de VPN hacemos que funcione con el usuario nobody.
group nogroup	Para limitar los privilegios del demonio de VPN hacemos que funcione con el grupo nogroup.
push "redirect-gateway def1"	Para que la totalidad de tráfico vaya a través de nuestro VPN

push "dhcp-option DNS 10.8.0.1"	Estamos definiendo que las peticiones DNS de los clientes se hagan a través del servidor VPN ubicado en 192.168.0.1
cipher AES-256-CBC	Por defecto el algoritmo de cifrado de OpenVPN es Blowfish con un tamaño de clave de 128 bits. Quien crea que no es suficiente puede añadir esta línea para cambiar el algoritmo de cifrado a AES con un clave de cifrado de 256 bits. Para ver todos los algoritmos de cifrado disponibles teclear **openvpn –show-ciphers** en la terminal.
persist-key	En caso que el servidor OpenVPN se caiga las claves no tendrán que ser analizadas de nuevo.
persist-tun	El dispositivo tun0 no tendrá que ser reabierto ni cerrado en el caso que tengamos que reiniciar el servidor.
status openvpn-status-log	Log donde se guardará información respecto al túnel creado.
plugin /usr/lib/openvpn/openvpn-auth-pam.so /etc/pam.d/login	Activación del script encargado de realizar la autenticación del usuario y del cliente. (Ver el apartado "Autentificación del cliente mediante usuario y password")
verb 3	Grado de detalle del estado del túnel en los logs.

Fuente: Elaboración propia

Una vez tenemos listo el fichero de configuración tan solo tenemos que guardar los cambios y cerrarlo.

Nota: para que los clientes que están conectados al servidor VPN puedan comunicarse entre ellos tenemos que añadir la frase client-to-client en el fichero de configuración del servidor.

Nota: La configuración propuesta en este caso tendrá que adaptar a las características de nuestra red y a las necesidades del proyecto.

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.

Tabla Nro. 46: Parámetros de configuración de usuario

Parámetro	**Descripción**
dev tun	Dispositivo virtual en el cual se creara el túnel.
proto udp	Protocolo de transmisión de paquetes del servidor VPN. Se puede usar TCP.
remote geekland.sytes.net 1194	Dirección IP pública/Host DNS dinámico y puerto de escucha del servidor VPN. El puerto 1194 se puede cambiar. Si lo cambiamos deberemos adaptar el resto de configuraciones al nuevo puerto
resolv-retry infinite	El cliente intentará de forma indefinida resolver la dirección o nombre de host indicado por la directiva remote (agromarvpn).
nobind	A los clientes se les asignará puertos dinámicos (no privilegiados) cuando haya retorno de paquetes del servidor al cliente.
user nobody	Para limitar los privilegios de los clientes que se conectan al VPN les asignamos el usuario nobody. (no necesario para windows)
group nogroup	Para limitar los privilegios de los clientes que se conectan al VPN les asignamos el grupo nogroup. (no necesario para windows)
persist-key	En caso que el servidor OpenVPN sea reiniciado no se tendrán que volver a leer las claves.
persist-tun	El dispositivo tun0 no tendrá que ser reabierto ni cerrado en el caso que tengamos que reiniciar el cliente Vpn.
ca ca.crt	Certificado de la autoridad certificadora que creamos
cert usuariovpn.crt	Certificado del cliente

key usuariovpn.key	Clave privada del cliente
ns-cert-type server	Para prevenir ataques man in the middle. Con esta frase hacemos que los clientes solo puedan aceptar un certificado de servidor del tipo servidor "nsCertType=server". En este campo podríamos aplicar otras alternativas similares como por ejemplo "remote-cert-tls server".
tls-auth ta.key 1	Activación de la autentificación TLS en el cliente.
cipher AES-256-CBC	Por defecto el algoritmo de cifrado de OpenVPN es Blowfish con un tamaño de clave de 128 bits. Quien crea que no es suficiente puede añadir esta línea para cambiar el algoritmo de cifrado a AES con un clave de cifrado de 256 bits. Para ver todos los algoritmos de cifrado disponibles teclear **openvpn –show-ciphers** en la terminal.
auth-user-pass	Para indicar que el cliente tiene que introducir un nombre de usuario y un password.
auth-nocache	Para evitar que los password queden almacenados en la memoria cache de los clientes.
comp-lzo	Activar compresión LZO para la transmisión de datos.
verb 3	Grado de detalle del estado del túnel

Fuente: Elaboración propia

13. Autentificación 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:

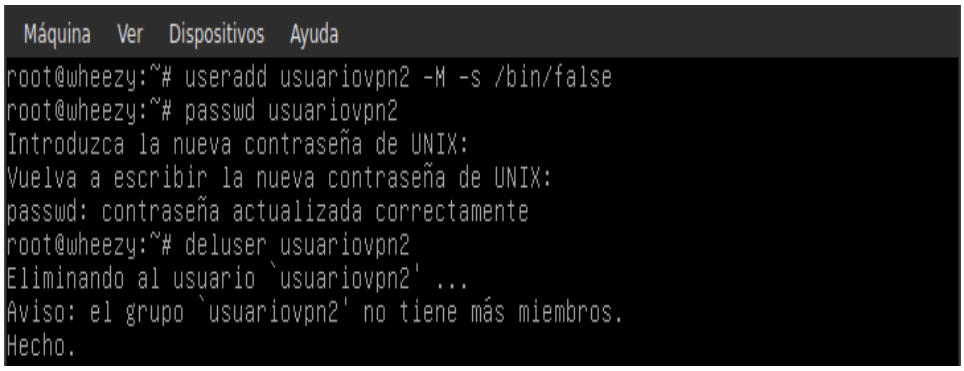
```
passwd usuariovpn2
```

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
```

Gráfico Nro. 19: Autentificación de usuarios



Fuente: Elaboración propia

Nota: Para que la autentificación 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 Forwading 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 linea:

#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
```

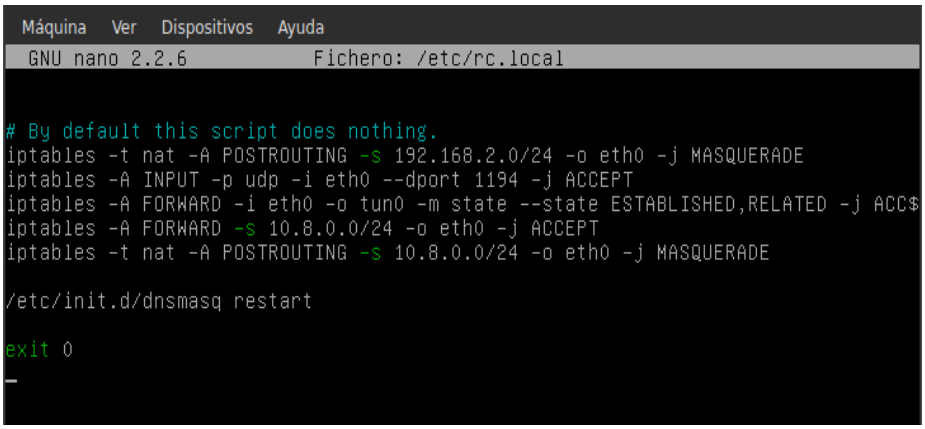
Nota: En función de las características de nuestra red y configuración de nuestro firewall es posible que tenga que implementar reglas adicionales a las que se muestran.

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 Nro. 20: Enrutamiento de peticiones



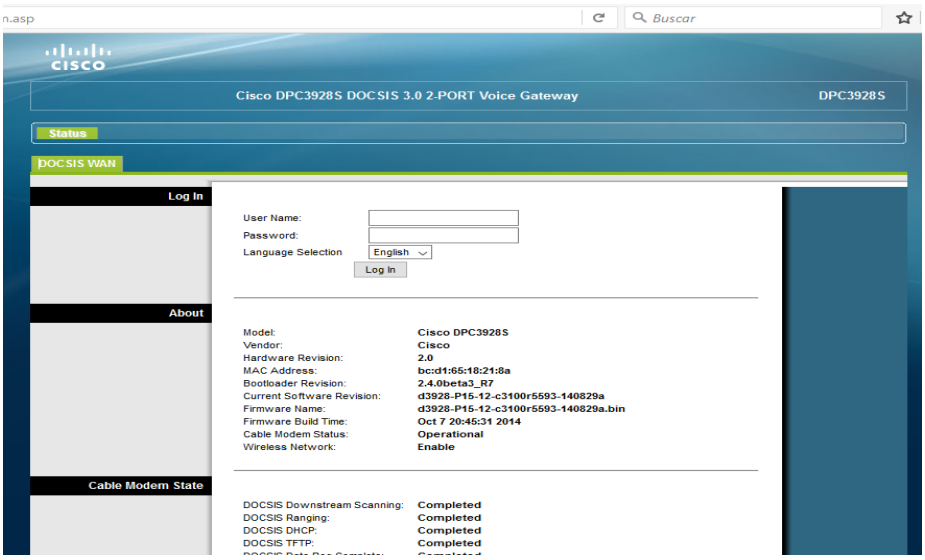
Fuente: Elaboración propia

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:

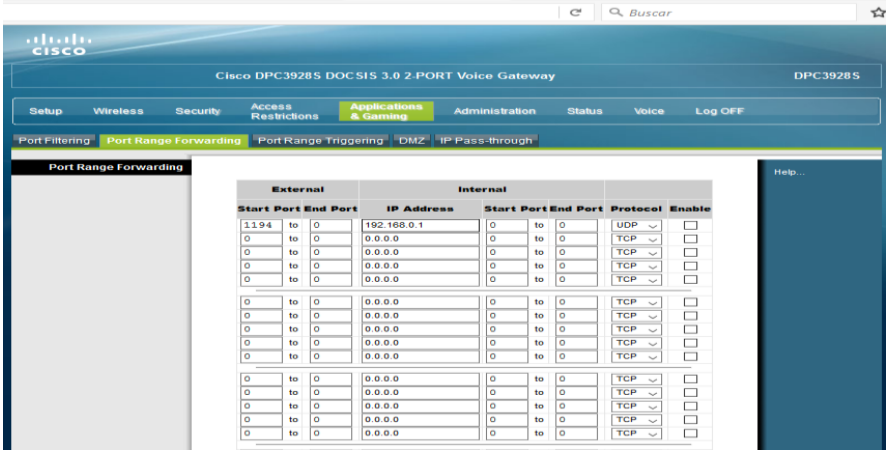
Gráfico Nro. 21: Accediendo al router



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 Filterning

Gráfico Nro. 22: 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, en la ubicación /etc/openvpn/keys tenmos que tener las siguientes claves:

Tabla Nro. 47: Claves generadas para el servidor

Archivo	**Descripción**	**Ubicación**	**Secreto**
ca.crt	Certificado raíz de la entidad certificadora	Servidor (/etc/openvpn) y cliente	No
whezzyVPN.crt	Certificado del servidor VPN	Servidor (/etc/openvpn) y cliente	No
usuariovpn.key	Clave privada del cliente VPN	Cliente	Sí
usuariovpn.crt	Certificado del cliente VPN	Cliente	No
ta.key	Clave para la Autentificación TLS	Servidor (/etc/openvpn) y cliente	Sí

Fuente: elaboración propia

Ahora tenemos que copiar las claves detalladas en la tabla Nro. 48 en el usuario que en este caso será un sistema operativo Windows. Lo haremos mediante una memoria USB. Una vez montada la memoria USB tan solo tenemos que copiar las claves del servidor a la memoria USB. Para ello en el caso que no tengan entorno gráfico puede utilizar el siguiente comando:

```
cp /etc/openvpn/keys/* /media/usb
```

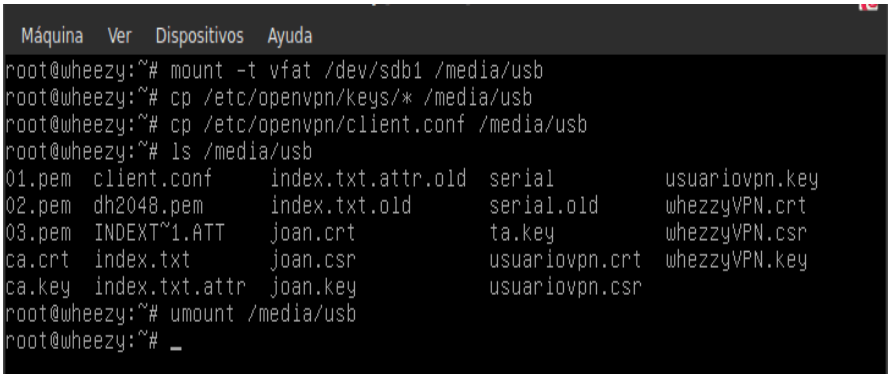
Nota: Este comando copia la totalidad de contenido de la /etc/openvpn/keys, que es donde están nuestras claves, en nuestra memoria USB que hemos montado en la carpeta /media/usb, cuando configuramos el servidor también creamos un fichero de configuración para el usuario. Este fichero lo guardamos en la ubicación /etc/openvpn con el nombre client.conf.

Este fichero también lo copiaremos a nuestra memoria USB. Para ellos introduciremos el siguiente comando en la terminal:

cp /etc/openvpn/client.conf /media/usb

Nota: Este comando copia el fichero client.conf ubicado en /etc/openvpn/keys a nuestra memoria USB que hemos montado en la carpeta /media/usb.

Gráfico Nro. 23: Copia de los archivos para la conexión



Fuente: Elaboración propia

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,

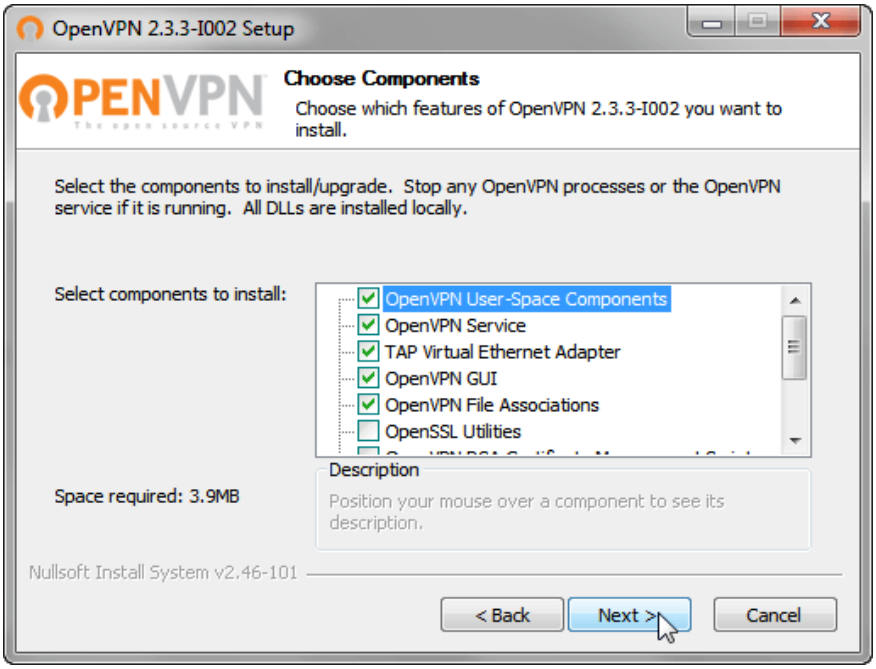
elegimos la versión según la arquitectura de la pc, luego de haberlo descargado clicamos el botón derecho del mouse y elegimos la opción “Ejecutar como administrador”. Una vez realizado esto empezará la instalación del cliente. Las etapas de la instalación serán las siguientes:

- 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 Nro. 24: Selección de componentes de instalación



Fuente: elaboración propia

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

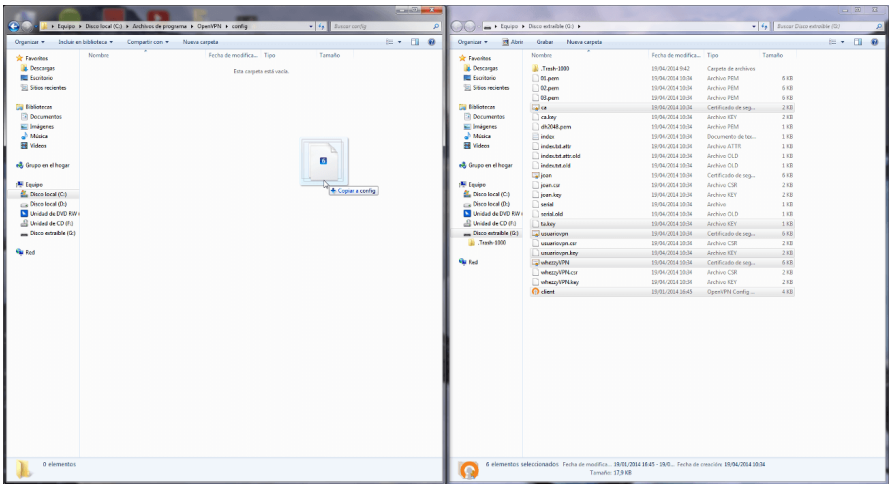
- En el cuarto paso aparecerá una ventana para seleccionar la ruta de instalación del programa. Dejamos la ruta por defecto, y presionamos el botón Next y empezará la instalación que será cuestión de segundos.

  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 Nro. 25: Copiar claves de usuario



Fuente: Elaboración propia

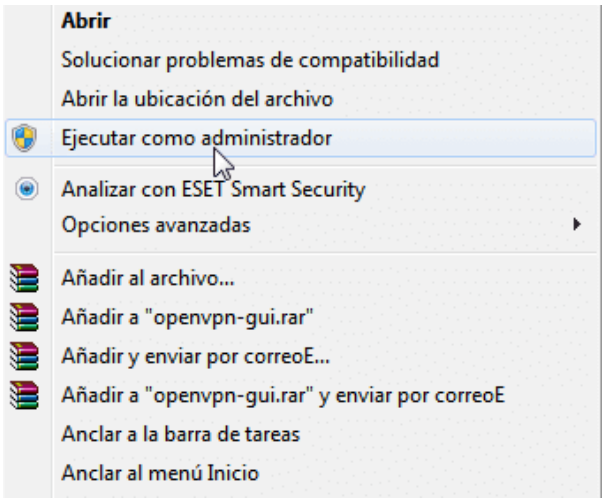
Tenemos que seleccionar los siguientes archivos del pendrive.

- 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 Autentificación 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.

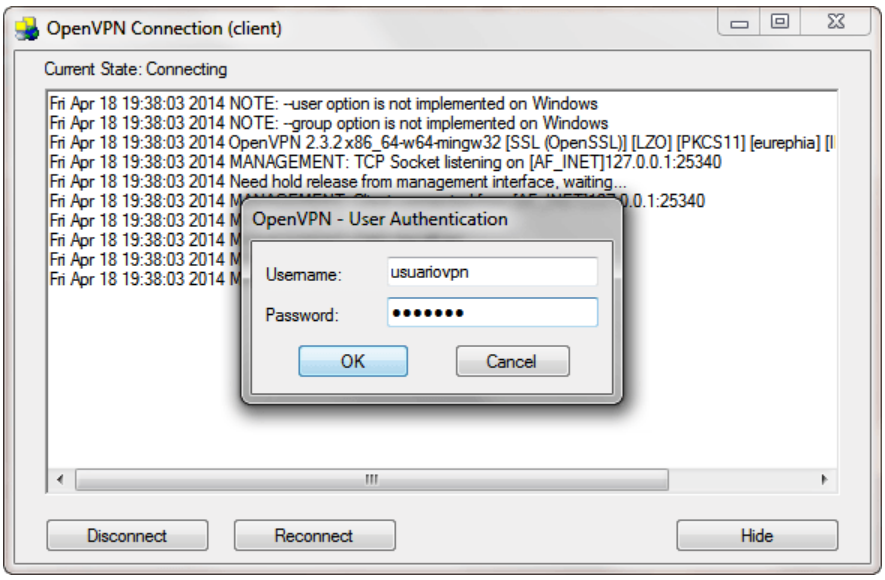
Para finalizar hay que conectarnos al servidor OpenVPN en Windows nos vamos a nuestro escritorio en el que encontraremos un icono de acceso directo al cliente OpenVPN.

Gráfico Nro. 26: 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”



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.

17. PROPUESTA ECONÓMICA

Tabla Nro. 48: Costo total del proyecto

Descripción	Unidad	Cantidad	Precio S/	Tota S/
CPU servidor	Unidad	1	2 000	2 000
Cisco Router (RV042GNA)	Unidad	1	450	450
Servicio de dirección pública fija	Unidad	1 año	20	240
Movilidad	Unidad	1	50	50
Capacitación	Unidad	1	500	500
Mano de Obra	Unida	1	1 800	1 800
			Total	5 040

Fuente: Elaboración propia

18. CRONOGRAMA DE EJECUCION DE PROYECTO

Tabla Nro. 49: Cronograma de Actividades

Actividades	Tiempo (semanas)									
	1	2	3	4	5	6	7	8	9	10
Aprobación del proyecto										
Adquisición de equipos										
Adquisición de servicios										
Instalación configuración del servidor VPN										
Prueba de red VPN										
Capacitación										
Implementación Entrega										

Fuente: Elaboración propia

V. CONCLUSIONES

De acuerdo a los resultados obtenidos en el estudio para el diseño de la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A - Sullana; 2016, queda confirmada la necesidad prioritaria de solucionar los problemas de comunicación y acceso a la información que tiene actualmente la empresa Agromar Industrial S.A, este resultado es similar al indicado a la hipótesis general por lo que se concluye que la hipótesis general queda aceptada.

En cuanto a las dimensiones se concluye lo siguiente:

1. En la tabla Nro. 20 se puede determinar que el 70.00% de los trabajadores indicó que el acceso de la información es insuficiente e inoportuno este resultado es similar al indicado en la hipótesis especifica lo que me permite identificar los requerimientos que satisfagan las necesidades de la empresa, por lo que se concluye que la hipótesis especifica queda aceptada.

2. En la tabla Nro. 31 se puede observar que el 73,33% de los trabajadores respondió que la seguridad no es la más óptima y que no existen políticas de seguridad lo cual requiere un estudio de las tecnologías para determinar la más adecuada, este resultado es similar al indicado en la hipótesis específica; por lo que se concluye que la hipótesis especifica queda aceptada.

3. En la tabla Nro. 43 se puede interpretar que el 100.00% de los trabajadores expreso que están de acuerdo con el diseño e implementación de una red privada virtual porque creen que beneficiara a la empresa y en su trabajo diario, este resultado es similar al indicado en la hipótesis específica, por lo que se concluye que la hipótesis especifica queda aceptada.

VI. RECOMENDACIONES

1. Es importante que la empresa implemente políticas orientadas a la seguridad 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 factible con las nuevas tecnologías y se adapte a las ya adquirida por la empresa sin la necesidad de volver a diseñar una nueva red.

3. Es necesario que el personal del área de informática de la empresa se encuentre debidamente capacitado para poder manipular; modificar y configurar la red privada virtual.

4. Dar prioridad a la viabilidad de la propuesta económica dentro del presupuesto de la institución para su posterior implementación.

5. Se sugiere que para la implementación de la red privada virtual se adquiera un mejor servicio de internet con mucha más capacidad de ancho de banda.

REFERENCIAS BIBLIOGRÁFICAS

1. PEREIRA UTD. UTP. [ONLINE].; 2015 [CITED 2016 SEPTIEMBRE 2. AVAILABLE FROM: HTTP://WWW.UTP.EDU.CO/~VICTABO/INTRODUCCION.HTM.
2. OSORES. TECHTARGET. [ONLINE].; 2016 [CITED 2016 SEPTIEMBRE 2. AVAILABLE FROM: HTTP://SEARCHDATACENTER.TECHTARGET.COM/ES/CRONICA/LA-GESTION-Y-EL-MONITOREO-DE-REDES-SIGUE-SIENDO-PRIORIDAD-EN-AL?PLATFORM=HOOTSUITE.
3. ROMERO JP, ROMERO CE. FRONTERAS DE SEGURIDAD EN REDES PRIVADAS VIRTUALES (VPN). TESIS. PEREIRA: UNIVERSIDAD TECNOLÓGICA DE PEREIRA, DEPARTAMENTO DE INGENIERIA DE SISTEMAS; 2016.
4. TITUAÑA ES. DESARROLLO DE UN MODELO DE IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES MULTIPUNTO DINÁMICAS (DMVPN) PARA PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES). TESIS LICENCIATURA. UNIVERSIDAD DE LAS AMERICAS, SISTEMAS; 2015.
5. AGUILAR EY, RAMIREZ LE. DISEÑO E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL HOSPITALARIA (VPN) MEDIANTE ACCESO REMOTO A UN SISTEMA CENTRALIZADO DE INFORMACION EN BOGOTA. TESIS. BOGOTÁ: UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS, DEPARTAMENTO DE SISTEMAS; 2014.
6. SÁNCHEZ J. DISEÑO DE UNA SOLUCIÓN DE IP TRUNKING SOBRE RED VPN ENTRE MÚLTIPLES SEDES DE UN CONTACT CENTRE. TESIS LICENCIATURA. MADRID: UNIVERSIDAD CARLOS III DE MADRID, DEPARTAMENTO DE INGENIERIA TELEMATICA; 2010.
7. ALVA E. DESARROLLO E IMPLEMENTACIÓN DE UNA HERRAMIENTA GRÁFICA PARA LA CONFIGURACIÓN REMOTA DE UNA VPN CON ROUTERS CISCO. TESIS BACHILLER. LIMA: PONTIFICIA

UNIVERSIDAD CATÓLICA DEL PERÚ, FACULTAD DE CIENCIAS E INGENIERÍA; 2013.

8. RAMÍREZ YK, GAMMARA VILLANUEVA CL. DISEÑO DE UNA RED DE BANDA ANCHA PARA LA REGIÓN. TESIS BACHILLER. LIMA: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, FACULTAD DE CIENCIAS E INGENIERÍA; 2013.
9. MOLINA E. PROPUESTA DE SEGMENTACIÓN CON REDES CON REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QOS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDAD DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO PLANTA NORTE. TESIS. CHICLAYO: UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO, FACULTAD DE INGENIERÍA; 2012.
10. RODRÍGUEZ DA, SÁNCHEZ ROLANDO L. DISEÑO DE UNA RED DE BANDA ANCHA PARA LA LIBERTAD. TESIS BACHILLER. LIMA: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, FACULTAD DE CIENCIAS E INGENIERÍA; 2011.
11. ANCAJIMA A. PROPUESTA DE REINGENIERÍA DE LA RED DE DATOS EN LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL (UGEL) PAITA, 2014. TESIS. PIURA: UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE, FACULTAD DE INGENIERIA; 2014.
12. MUÑOZ CC. DISEÑO DE UNA RED DE TELECOMUNICACIONES DE. TESIS. LIMA: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, FACULTAD DE CIENCIA E INGENIERÍA; 2013.
13. ANCÍ DM. ESTUDIO DE PREFACTIBILIDAD Y DISEÑO DE LA RED DE TELECOMUNICACIONES PARA EL POBLADO DE SOL SOL EN PIURA. TESIS. LIMA: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, FACULTAD DE CIENCIAS E INGENIERÍA; 2012.
14. PERÚ O. OH PERÚ. [ONLINE].; 2013 [CITED 2016 OCTUBRE 1. AVAILABLE FROM: HTTP://WWW.OHPERU.COM/EMPRESAS/AGROINDUSTRIA.HTM.

15. MAYORGA M. AGROINDUSTRIAS MAGALI. [ONLINE].; 2012 [CITED 2016 NOVIEMBRE 2. AVAILABLE FROM: HTTP://AGROINDUSTRIAS-MAGALI.BLOGSPOT.PE/2012/04/LA-AGROINDUSTRIA-Y-SU-CLASIFICACION.HTML.
16. VINELLI M. CNN EN ESPAÑOL. [ONLINE].; 2016 [CITED 2016 DICIEMBRE 7. AVAILABLE FROM: HTTP://CNNESPANOL.CNN.COM/2016/06/06/EL-PERU-Y-LAS-AGROEXPORTACIONES-EN-EL-ENTORNO-MUNDIAL/.
17. INEI. INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA. [ONLINE].; 2014 [CITED 2016 DICIEMBRE 2. AVAILABLE FROM: HTTPS://WWW.INEI.GOB.PE/PRENSA/NOTICIAS/DIVISAS-POR-EXPORTACION-DE-MANGO-AUMENTARON-EN-4024-7576/.
18. APEM. ASOCIACIÓN PERUANA DE PRODUCTORES Y EXPORTADORES DE MANGO. [ONLINE].; 2014 [CITED 2016 DICIEMBRE 2. AVAILABLE FROM: WWW.PERUVIANMANGO.ORG/13CONGRESO/12.PDF.
19. INET. INSTITUTO NACIONAL DE EDUCACIÓN TECNOLÓGICA. [ONLINE].; 2012 [CITED 2016 DICIEMBRE 2. AVAILABLE FROM: HTTP://WWW.ONI.ESCUELAS.EDU.AR/2002/SANTIAGO_DEL_ESTERO/MADRE-FERTIL/AGROIND.HTM.
20. AGROMAR INDUSTRIAL. AGROMAR INDUSTRIAL. [ONLINE].; 2010 [CITED 2016 OCTUBRE 1. AVAILABLE FROM: HTTP://WWW.AGROMARINDUSTRIAL.COM.PE/WEB_ES/INDEX.HTML#PAGE2.
21. APRENDE EN LINEA. [ONLINE].; 2015 [CITED 2016 OCTUBRE JUEVES. AVAILABLE FROM: HTTP://APRENDEENLINEA.UDEA.EDU.CO/LMS/INVESTIGACION/MOD/PAGE/VIEW.PHP?ID=3118.
22. TELLO LEAL E. UNIVERSITAT OBERTA DE CATALUNYA. [ONLINE].; 2007 [CITED 2016 OCTUBRE 4. AVAILABLE FROM: HTTP://WWW.UOC.EDU/RUSC/4/2/DT/ESP/TELLO.PDF.

23. BONILLA M. TECNOLOGIA DE LA INFORMACION Y COMUNICACION - YOPAL. [ONLINE].; 2009 [CITED 2016 OCTUBRE SABADO. AVAILABLE FROM: HTTPS://SITES.GOOGLE.COM/SITE/TICSYOPAL5/ASSIGNMENTS.
24. MM. APRENDE A PROGRAMAR. [ONLINE].; 2013 [CITED 2016 OCTUBRE 5. AVAILABLE FROM: HTTP://WWW.APRENDERAPROGRAMAR.COM/INDEX.PHP?OPTION=COM_CONTENT&VIEW=ARTICLE&ID=889:IQUE-ES-Y-PARA-QUE-SIRVE-UN-ERP-SOFTWARE-EMPRESARIAL-SAP-SAGE-ORACLE-MICROSOFT-DYNAMICS-INFOR-LN-ETC-&CATID=57:HERRAMIENTAS-INFORMATICAS&ITEMID=179.
25. NISIRA. NISIRA SOLUCIONES INFORMATICAS DE GESTION. [ONLINE].; 2016 [CITED 2016 OCTUBRE 5. AVAILABLE FROM: HTTP://WWW.NISIRA.COM.PE/ERP.XHTML.
26. YECAS H. BLOG DIARIO. [ONLINE].; 2007 [CITED 2016 OCTUBRE 5. AVAILABLE FROM: HTTP://HECTORYESCAS.BLOGDIARIO.COM/1176213300/.
27. PALMA E. ACADEMIA EDU. [ONLINE]. [CITED 2016 OCTUBRE 5. AVAILABLE FROM: HTTPS://WWW.ACADEMIA.EDU/11646101/INTRODUCCION_A_VPN_REDES_PRIVADAS_VIRTUALES.
28. UNIVERSIDAD NACIONAL DEL LITORAL. UNIVERSIDAD NACIONAL DEL LITORAL. [ONLINE].; 2009 [CITED 2016 OCTUBRE 4. AVAILABLE FROM: HTTP://WWW.FCA.UNL.EDU.AR/INFORMATICABASICA/REDES.PDF.
29. TELEPIEZA. TELEPIEZA. [ONLINE].; 2016 [CITED 2016 OCTUBRE 5. AVAILABLE FROM: HTTPS://WWW.TELEPIEZA.COM/WORDPRESS/2008/04/28/LOS-7-NIVELES-O-CAPAS-DEL-MODELO-OSI/#COMMENTS.
30. GALARZA LM, SANTOS P A. UNIVERSIDAD ECOTEC. [ONLINE].; 2011 [CITED 2016 OCTUBRE 5. AVAILABLE FROM:

HTTP://WWW.ECOTEC.EDU.EC/DOCUMENTACION%5CINVESTIGACIONES%5CESTUDIANTES%5CTRABAJOS_DE_CLASES/1580_TRECALDE_0033.PDF.

31. OVIEDO. BLOG REDES PRIVADAS VIRTUALES. [ONLINE].; 2012 [CITED 2016 OCTUBRE 5. AVAILABLE FROM: HTTP://REDESPRIVADASVIRTUALESVPN.BLOGSPOT.PE/2012/07/REQUERIMIENTOS-BASICOS-DE-LA-VPN.HTML.
32. CISCO. CISCO. [ONLINE].; 2014 [CITED 2016 OCTUBRE 6. AVAILABLE FROM: HTTP://WWW.CISCO.COM/CISCO/WEB/SUPPORT/LA/7/74/74718_HOW_VPN_WORKS.PDF.
33. VPNTUNNEL. [ONLINE].; 2016 [CITED 2015 DICIEMBRE 2. AVAILABLE FROM: HTTPS://VPNTUNNEL.COM/ES/FAQS/WHAT-IS-OPENVPN/.
34. SYMANTEC. SYMANTEC. [ONLINE].; 2015 [CITED 2016 DICIEMBRE 2. AVAILABLE FROM: HTTPS://WWW.SYMANTEC.COM/ES/ES/PAGE.JSP?ID=SSL-INFORMATION-CENTER#.
35. GÓMEZ MM. INTRODUCCION A LA METODOLOGÍA DE LA INVESTIGACIÓN CIENTÍFICA. PRIMERA ED. CÓRDOBA: EDITORIAL BRUJAS; 2006.
36. ORTIZ FG. DICCIONARIO DE METODOLOGÍA DE LA INVESTIGACIÓN CIENTÍFICA. PRIMERA ED. NORIEGA , EDITOR. MÉXICO: LIMUSA; 2014.
37. SHUTTLEWORTH M. EXPLORABLE. [ONLINE].; 2010 [CITED 2016 OCTUBRE MARTES. AVAILABLE FROM: HTTPS://EXPLORABLE.COM/ES/ESTUDIO-TRANSVERSAL.
38. JUEZ P, DÍEZ VEGAS J. PROBABILIDAD Y ESTADÍSTICA EN MEDICINA BRAVO J, EDITOR. MADRID: EDICIONES DÍAZ DE SANTOS; 1997.
39. WIGODSKI S J. METODOLOGÍA DE LA INVESTIGACIÓN. [ONLINE].; 2010 [CITED 2016 OCTUBRE MARTES. AVAILABLE FROM:

HTTP://METODOLOGIAENINVESTIGACION.BLOGSPOT.PE/2010/07/POBLACION-Y-MUESTRA.HTML.

40. CASTILLO J. UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. [ONLINE].; 2004 [CITED 2016 OCTUBRE 2. AVAILABLE FROM: WWW.INGENIERIA.UNAM.MX/INDUSTRIALES/DESCARGAS/DOCUMENTOS/CATEDRA/APUNTESDSP.DOC.
41. ROUSE M. TECHTARGET. [ONLINE].; 2016 [CITED 2016 OCTUBRE 2. AVAILABLE FROM: HTTP://SEARCHENTERPRISEWAN.TECHTARGET.COM/DEFINITION/VIRTUAL-PRIVATE-NETWORK.

ANEXOS

ANEXO Nº 1: CRONOGRAMA DE ACTIVIDADES

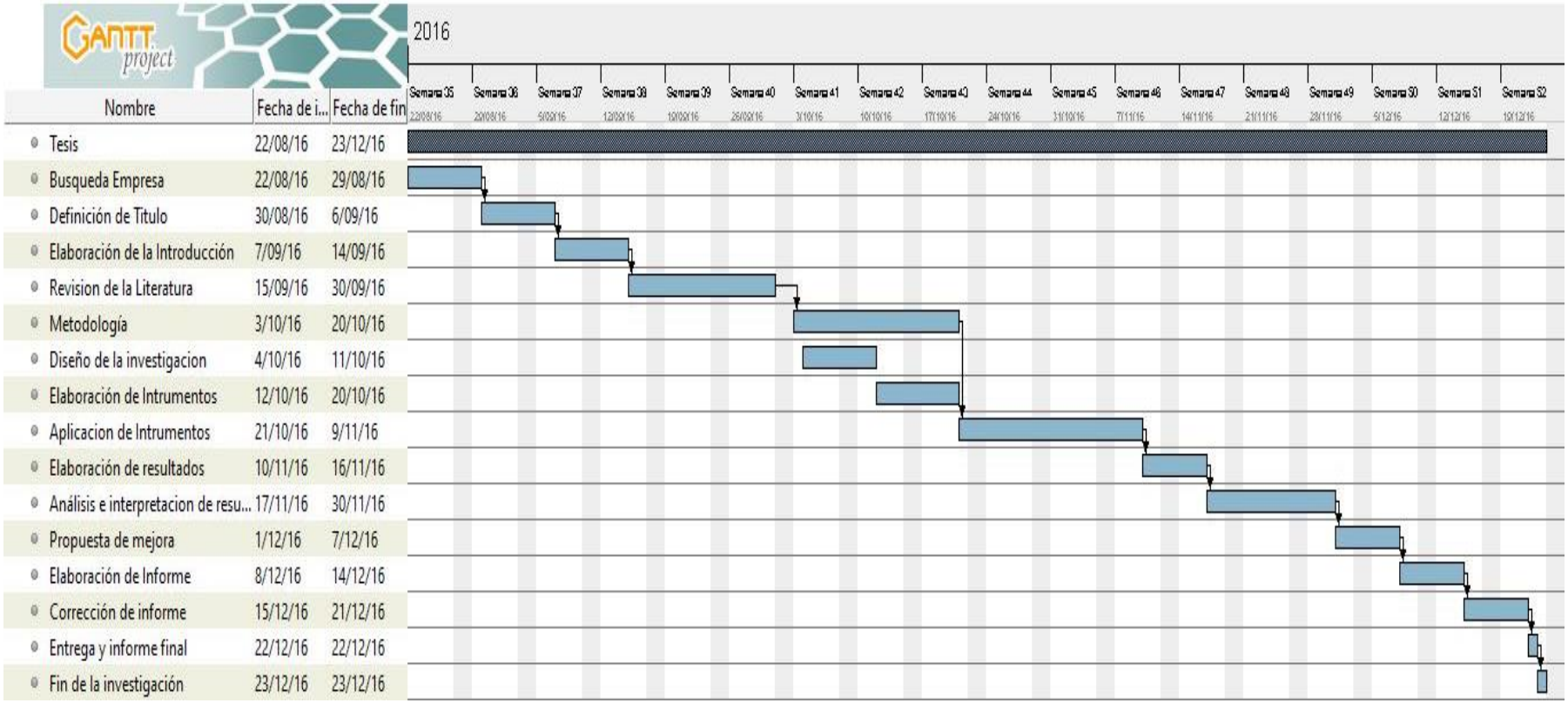


Imagen Elaborada con Software libre “Gantt Proyect”

ANEXO Nº 2: PRESUPUESTO Y FINANCIAMIENTO

DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO S/	TOTAL PARCIAL S/	TOTAL S/
1. RENUMERACIONES				
1.1. Asesor	01	1400.00	1400.00	
1.2. Estadístico	01	200.00	200.00	
			1 600.00	1 600,00
2. BIENES DE INVERSION				
2.1. Impresora	01	250.00	250.00	
			250.00	250,00
3. BIENES DE CONSUMO				
3.1. Papel bond A-4 80	01 m	25.00	25.00	
3.2. Tóner para impresora	01	45.00	45.00	
3.3. CD	02	2.00	2.00	
3.4. Lapiceros	02	1.00	1.00	
3.5. Lápices	02	2.00	2.00	
			75.00	75,00
4. SERVICIOS				
4.1. Fotocopias	50 hoja	25.00	25.00	
4.2. Anillados	3	15.00	15.00	
4.2. Servicios de Internet	80hrs	80.00	80.00	
4.3. Pasajes locales		235.00	235.00	
			355.00	355,00
TOTAL				**2 280,00**

Fuente: Elaboración Propia

ANEXO Nº 3: CUESTIONARIO

INSTRUMENTO DE RECOLECCION DE DATOS – AGROMAR INDUSTRIAL S.A

ENCUESTA **AREA:**

En este cuestionario te presentamos una serie de preguntas relacionadas con las tecnologías que usas a diario en tu centro de trabajo, divididas en tres dimensiones con el objeto de conocer las necesidades y por tanto adaptar el desarrollo de futuras tecnologías que ayuden y simplifiquen el trabajo diario.

INTRUCCIONES: En las páginas siguientes se presentan las preguntas del tipo cerradas para contestar esta parte de la encuesta deberás marcar dos alternativas SI □ y NO □ de las cuales deberá marcar solo una. Esta encuesta es anónima. Te garantizamos que el tratamiento de los datos que facilites será totalmente confidencial y anónimo.

A.- DIMENSIÓN ACCESO A LA INFORMACIÓN			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Cuenta con disponibilidad de la información entre las áreas de la empresa?		
2	¿Existe eficiencia con el servicio de acceso a la información de la empresa?		
3	¿Cree usted que las sucursales de la empresa se encuentran conectadas en una sola red de trabajo?		
4	¿Tiene problemas con la velocidad transmisión de datos?		

5	¿Cree usted que es necesario acceder a la información de las demás empresas?		
6	¿La información se transmite mediante la red de datos para diferentes áreas y sucursales de la empresa?		
7	¿Actualmente puede compartir sus archivos mediante la red o con otro compañero de trabajo?		
8	¿Utiliza algún medio físico (memoria, disco duro) para compartir información?		
9	¿Está conforme con el servicio de red y acceso de la información?		
10	¿Cree usted que hay integridad de la información?		
11	¿Hay suficiente capacidad para los servicios de red e Internet?		

B.- DIMENSIÓN SEGURIDAD DE RED			
1	¿Según usted cree que existen medidas de seguridad para proteger la información que comparte?		
2	¿Existe autenticación de usuarios en el intercambio de la información, que se realizan mediante los sistemas?		
3	¿Hay privilegios de los usuarios, respecto al uso de los sistemas de información?		
4	¿La seguridad de los sistemas de información, están direccionadas a los procesos de negocios?		
5	¿Cree que hay políticas de seguridad en el uso de la Red e Internet?		
6	¿Usted se siente seguro al compartir información?		
7	¿Cree usted que hay prevención, detección y corrección de Software malicioso?		
8	¿Los ordenadores de su empresa, tienen instalado antivirus?		

9	¿Se realiza copia de seguridad de los datos de la empresa?		
10	¿Cuenta con un firewall de internet?		

C.- DIMENSIÓN DISEÑO DE RED PRIVADA VIRTUAL			
1	¿Cree necesario realizar un diseño de una red privada virtual para mejorar el servicio de comunicación y seguridad de información de la empresa?		
2	¿A su opinión considera que la propuesta de una red privada virtual sea necesaria para una posterior implementación?		
3	¿A su criterio piensa o cree que una red privada virtual le simplificaría el trabajo diario?		
4	¿Cree usted que una eventual implementación de una red privada virtual beneficiaria a los trabajadores de la empresa?		
5	¿Piensa que la implementación de una red privada virtual permitiría un mejor acceso a la información?		
6	¿A su opinión cree que la implementación de una red privada virtual garantizaría la integridad de los datos?		
7	¿Considera que una red privada virtual comunicaría a las diferentes sucursales de trabajo?		
8	¿Cree usted que una eventual implementación de una red privada virtual le permitiría compartir archivos de forma segura?		
9	¿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?		
10	¿Considera que la implementación de una red privada virtual ayudara a mejorar la imagen institucional de la empresa?		