UNIVERSIDAD ANDINA DEL CUSCO
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERA DE SISTEMAS

TESIS

Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI
CASO: Servidor de Correos

Presentado por:

Bach. Jenny Mar Segundo

Para optar al título profesional de

Ingeniero de Sistemas

Asesor:

Ing. Luis Alberto Sota Orellana

Cusco – Perú

2016

DEDICATORIA

El presente trabajo de investigación está dedicado a mis abuelos y a mis padres por brindarme todo su apoyo a lo largo de mi formación personal y ahora profesional y como no también va dedicada a mi hermana menor quien es a quien debo dar el ejemplo en todo momento.

AGRADECIMIENTOS

Agradezco a cada uno de los ingenieros de la escuela profesional de ingeniería de sistemas quienes me brindaron todos sus conocimientos a lo largo de mi aprendizaje en la carrera, especialmente a mi asesor de tesis ing. Luis Alberto Sota por su apoyo, exigencia y confianza en mi persona para que el presente trabajo de investigación se realice y como no a mis mejores amigos de la universidad por todos sus ánimos a mi persona.

RESUMEN

El presente trabajo de investigación se basa en emplear la tecnología de red “Virtual Private Network” (VPN), con la finalidad de mejorar la confidencialidad del intercambio de información entre las sedes Lima - Cusco del Instituto Nacional de Estadística e Informática (INEI), ya que en la actualidad los encargados de las oficinas técnicas de informática señalaron que un porcentaje del personal administrativo en común de las sedes Lima – Cusco del INEI presenta inconvenientes con sus cuentas de correo (cuentas hackeadas), debido a los bajos niveles de seguridad.

Asimismo, actualmente el personal administrativo quienes vienen laborando en ambas sedes se comunican a través de servicios de correos gratuitos (Hotmail), es decir utilizan correos no institucionales con sus cuentas personales.

En vista de los problemas mencionados, se ha visto por conveniente proponer la implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información tomando como caso un servidor de correos entre las sedes Lima y Cusco del INEI, el cual permitirá que dicha institución no solo maneje un solo dominio de correo “inei.com” para el envío y recepción de mensajes de texto relacionados únicamente a temas laborales entre el personal administrativo de ambas sedes, sino que a su vez ayudará a mejorar la confidencialidad en el intercambio de dicha información.

Para llevar a cabo las pruebas de seguridad para verificar que tan eficiente es la VPN para el resguardo de la confidencialidad de la información, se realizaron los ataques man in the middle con una conexión a la intranet vía VPN y otra prueba sin conexión a la misma.

ABSTRACT

This research is based on using network technology "Virtual Private Network" (VPN), with the aim of improving the confidentiality of information exchange between the Lima headquarters - Cusco National Institute of Statistics and Informatics (INEI) because now the computer area managers noted that a percentage of administrative staff in common of the Lima headquarters - Cusco INEI presents problems with their email accounts (hacked accounts), due to low levels of security.

Also, currently the administrative staff who are working in both sites communicate through free email services (Hotmail), use emails non-institutional with your personal accounts.

In view of the above problems, it has been deemed appropriate to propose the implementation of an intranet via VPN to improve confidentiality of information exchange taking as case, a mail server between Lima and Cusco INEI headquarters, which will allow the institution not only handle a single mail domain "inei.com" for sending and receiving text messages related only to labor issues between the administrative staff of both offices, but which in turn will help improve confidence in the exchange of such information.

To carry out safety tests to verify how efficient the VPN to guard the confidentiality of information , the man in the middle attacks were performed with a connection to the intranet via VPN and another test without connecting to it .

INTRODUCCIÓN

El presente trabajo de investigación tiene como finalidad dar a conocer la tecnología Virtual Prívate Network (Redes Privadas Virtuales), tecnología que ya es muy común dentro de las telecomunicaciones, existiendo empresas a nivel mundial que se dedican exclusivamente a la prestación de servicios de esta tecnología, ésta tecnología permitirá conectar redes distantes geográficamente de manera segura y a bajos costos, utilizando redes públicas como medio de enlace o transmisión.

Esta tecnología será elevada como propuesta para su implementación en el Instituto Nacional de Estadística e Informática (INEI), el cual es el encargado de manejar información confidencial sobre temas relacionados a proyectos que se dan a nivel nacional, tomando como muestra las áreas administrativas en común de las sedes Lima-Cusco de INEI (Jefatura, Oficina técnica de administración, Secretaría general, Oficina técnica de informática, Escuela nacional de estadística e informática, Dirección técnica de indicadores económicos, Dirección nacional de censos y encuestas y la Oficina técnica de estadísticas departamentales).

Se vio por conveniente optar por esta tecnología tomando como caso un servidor de correos, debido a que en la actualidad el personal administrativo de las áreas en común entre las sedes Lima – Cusco del INEI utilizan como medio de comunicación servicios gratuitos de correos electrónicos (Hotmail) con sus cuentas personales y un porcentaje de dichos trabajadores presentan inconvenientes con sus cuentas de correo, debido a los bajos niveles de seguridad, es así que el enfoque principal del presente trabajo de investigación es llevar a cabo la propuesta de implementación de una intranet vía VPN tomando como caso un servidor de correos, para interconectar las áreas administrativas de las sedes Lima – Cusco del INEI, con la finalidad de mejorar la confidencialidad en la transmisión de información entre ambas sedes. Cabe señalar que únicamente se consideraron las sedes Lima – Cusco como punto de estudio debido a la facilidad de extracción de la información.

El presente informe está comprendido por VII capítulos, donde:

Capítulo I: Explica la descripción de la situación actual en las que se encuentran las sedes Lima - Cusco del INEI en cuanto al intercambio de información, formulación del problema, objetivos, hipótesis, justificación, las variables identificadas, metodología y finalmente el cuadro de matriz de consistencia.

Capítulo II: Contiene los antecedentes de la investigación del presente trabajo de investigación realizado y el marco teórico el cual está comprendido por conceptos de los términos utilizados.

Capítulo III: Describe el tipo y el diseño de la investigación realizada, población, muestra del INEI con el que se trabajó y finalmente los instrumentos utilizados para la recolección de la información necesaria.

Capítulo IV: Los requerimientos, análisis y diseño de la intranet propuesta.

Capítulo V: Comprende todo el proceso de configuración realizado de la intranet vía VPN y el servidor de correos.

Capítulo VI: Pruebas con y sin conexión a la intranet vía VPN con ataques man in the middle.

Capítulo VII: Costos.

- Costos de investigación del proyecto.
- Costos de implementación del proyecto.

INFORME LEVANTAMIENTO DE OBSERVACIONES DE TESIS

A	:	Dr. Ing. Luis A. Mendoza Quispe Decano de la Facultad de Ingeniería y Arquitectura. Universidad Andina del Cusco
DE	:	Mgt. Ariadna Palomino Cahuaya Ing. Ivan Molero Delgado Ing. Ramiro Mora Jimenez Ing. Lizet Vargas Vera Docentes del Departamento Académico de Ingeniería de Sistemas.
ASUNTO	:	Levantamiento de observaciones de tesis.
REFERENCIA	:	Resolución N° 824-2016-DFIA-UAC de fecha 07 de Julio del 2016.
FECHA	:	Cusco, 09 de Setiembre del 2016.

Nos dirigimos a su despacho a fin de informar, que en cumplimiento de la Resolución N° 824-2016-DFIA-UAC de fecha 07 de Julio del 2016.

Se realizó el acto de exposición y sustentación de la tesis titulada: "PROPUESTA DE IMPLEMENTACIÓN DE UNA INTRANET VÍA VPN PARA MEJORAR LA CONFIDENCIALIDAD DEL INTERCAMBIO DE INFORMACIÓN ENTRE LAS SEDES LIMA-CUSCO DEL INEI CASO: SERVIDOR DE CORREOS", presentada por la bachiller JENNY MAR SEGUNDO, el día viernes 22 de Julio del 2016, señalando las observaciones que la graduanda debe subsanar.

Habiéndose levantado las mismas y estando el trabajo de tesis **CONFORME**, se recomienda su presentación final y se proceda al trámite correspondiente.

Atentamente,

Mgt. Ariadna Palomino Cahuaya
Dictaminante

Ing. Iván Molero Delgado
Dictaminante

Ing. Ramiro Mora Jimenez
Replicante

Ing. Lizet Vargas Vera
Replicante

INDICE GENERAL

Br. JENNY MAR SEGUNDO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

CAPÍTULO I

ASPECTOS GENERALES

1.1 DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

El Instituto Nacional de Estadística e Informática – INEI, es un organismo técnico especializado, con personería jurídica de derecho público interno, con autonomía técnica y de gestión, dependiente del Presidente del Consejo de Ministros. A su vez es considerada como un organismo central, rector del Sistema Estadístico Nacional y responsable de normar, planear, dirigir, coordinar y de supervisar las actividades estadísticas oficiales del país.

Esta institución tiene como misión producir y difundir información estadística oficial que el país necesitan con calidad, oportunidad y cobertura requerida con el propósito de contribuir al diseño, monitoreo y evaluación de políticas públicas y al proceso de toma de decisiones de los agentes socioeconómicos, el sector público y la comunidad en general

En cuanto a su visión, ser un organismo líder a nivel nacional e internacional, que utiliza los más altos estándares metodológicos y tecnológicos para la producción y difusión de estadísticas oficiales que contribuyan eficazmente en el diseño de políticas públicas para el desarrollo del país.

La sede Lima del INEI, quien es la encargada de enviar información confidencial a la sede Cusco y demás sedes ubicadas en cada departamento del Perú, con la finalidad de llevar a cabo el acuerdo de temas tales como: Acuerdos de proyectos a nivel nacional a realizar, envío del monto económico por cobrar, agenda a tratar en reunión, entre otros, en los últimos meses un porcentaje de los trabajadores de las áreas administrativas en común entre dicha Sede y la Sede Cusco del INEI quienes

utilizan sus cuentas personales de correos no institucionales (Hotmail) para el envío y recepción de información confidencial netas de la institución, accediendo a un servicio público como es el internet, presentan inconvenientes con sus cuentas de correo (cuentas hackeadas) debido a los bajos niveles de seguridad. Éste problema se pudo identificar gracias a las encuestas realizadas al personal administrativo de ambas sedes los cuales pueden ser corroborados en el capítulo III – 3.5 Recolección y Análisis de Datos según el cuestionario elaborado y adjuntado en el **ANEXO 4.**

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede mejorar la confidencialidad del intercambio de información entre las sedes Lima y Cusco del INEI?

1.2.1 PROBLEMAS ESPECÍFICOS

- ¿Cómo simular el intercambio seguro de la información?
- ¿Cómo probar la funcionalidad de la intranet propuesta?
- ¿Cómo se podría asegurar la integridad de la información enviada del origen al destino?
- ¿Cómo se podría verificar la disponibilidad de la información?
- ¿Cómo determinar el costo de investigación del proyecto?
- ¿Cómo determinar el costo de implementación del proyecto?

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Elaborar la propuesta de implementación de una intranet vía VPN, para mejorar la confidencialidad del intercambio de información entre las sedes Lima y Cusco del INEI.

1.3.2 OBJETIVOS ESPECÍFICOS

- Simular el intercambio de información por medio del servidor de correos entre cuentas de clientes VPN.
- Configurar un servidor de correos para la prueba de funcionalidad de la intranet.
- Asegurar la integridad de la información enviada al receptor.
- Verificar la disponibilidad de la información por medio del servidor de correos.
- Determinar los costos de investigación del proyecto.
- Determinar los costos de implementación del proyecto.

1.4 HIPÓTESIS

Con la propuesta de implementación de una intranet vía VPN se mejorará la confidencialidad del intercambio de información por medio de un servidor de correos entre las sedes Lima y Cusco del INEI.

1.5 JUSTIFICACIÓN

El presente trabajo de investigación tiene como finalidad la elaboración de la propuesta de implementación de una intranet vía VPN tomando como caso un servidor de correos, los cuales se encargarán de interconectar las áreas administrativas en común sedes Lima - Cusco del INEI en una red corporativa (privada) y de mejorar la confidencialidad del intercambio de información entre dichas áreas de ambas sedes.

1.6 VARIABLES

1.6.1 VARIABLE DEPENDIENTE

Confidencialidad del Intercambio de Información.

1.6.2 VARIABLE INDEPENDIENTE

Implementación de una Intranet vía VPN.

1.7 METODOLOGÍA

El presente trabajo de investigación es del tipo descriptiva, debido a que se describirá paso a paso todas las configuraciones realizadas (intranet vía VPN y servidor de correos).

1.8 MATRIZ DE CONSISTENCIA

FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
¿Cómo se puede mejorar la confidencialidad del intercambio de información entre las sedes Lima y Cusco del INEI?	OBJETIVO GENERAL Elaborar la propuesta de implementación de una intranet vía VPN, para mejorar la confidencialidad del intercambio de información entre las sedes Lima y Cusco del INEI.	Con la propuesta de implementación de una intranet vía VPN se mejorará la confidencialidad del intercambio de información por medio de un servidor de correos entre las sedes Lima y Cusco del INEI.	VARIABLE DEPENDIENTE Confidencialidad del Intercambio de Información	TIPOS DE INVESTIGACIÓN 1. INVESTIGACIÓN DESCRIPTIVA Se recolectará toda la información necesaria para poder llevar a cabo la propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI. 2. POBLACIÓN Y MUESTRA • POBLACION Todas las áreas administrativas de las sedes Lima – Cusco del INEI. • MUESTRA Áreas administrativas en común entre las sedes Lima – Cusco del INEI. 3. MÉTODOS, TÉCNICAS E INSTRUMENTOS Observación y cuestionario.
PROBLEMAS ESPECÍFICOS	OBJETIVOS ESPECÍFICOS		VARIABLE INDEPENDIENTE	
• ¿Cómo simular el intercambio seguro de la información? • ¿Cómo probar la funcionalidad de la intranet propuesta? • ¿Cómo se podría asegurar la integridad de la información enviada del origen al destino? • ¿Cómo se podría verificar la disponibilidad de la información? • ¿Cómo determinar el costo de investigación del proyecto? • ¿Cómo determinar el costo de implementación del proyecto?	• Simular el intercambio de información por medio del servidor de correos entre cuentas de clientes VPN. • Configurar un servidor de correos para la prueba de funcionalidad de la intranet. • Asegurar la integridad de la información enviada al receptor. • Verificar la disponibilidad de la información por medio del servidor de correos. • Determinar los cotos de investigación del proyecto. • Determinar los costos de implementación del proyecto.		Implementación de una Intranet vía VPN	

Tabla 1. Matriz de Consistencia

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

"Protocolos de seguridad para redes VPN"

LIMARI RAMIREZ, Víctor Humberto (2010)

Tesis de Grado

Universidad Austral de Chile

- VPN, es una robusta combinación entre seguridad e interoperabilidad, que cada vez más se ofrece como solución a las organizaciones en crecimiento y expansión. Ya que estas otorgan altos niveles de seguridad dentro de un medio de transmisión público, y permiten reemplazar enlaces dedicados que requieren grandes inversiones para su establecimiento. Por lo tanto dado sus ventajas en función a cada nivel de seguridad que requiera una organización es recomendable establecer este tipo de tecnología.
- Hay diversos esquemas de implementación de VPN, los cuales varían según tamaño de la red corporativa y seguridad que requiera para sus servidores. Estos pueden estar basados en software o hardware, siendo estos últimos los más efectivos al momento de efectuar procesos de autentificación y encriptación, debido a que no adhieren sobrepeso a los servidores dedicados a los enrutamientos dentro de la propia red local, agilizando el trabajo dentro de esta. Además que manejar parámetros bastante potentes de seguridad que sería poco probable implementar como software.
- Por otro lado el hecho de existir un ente regulador, que todo el tiempo este procesando claves y encriptaciones a los mensajes, provoca lentitud en los flujos bidireccionales. Pero con el avance de la tecnología nuevos y robustos procesadores dedicados a los hardwares con bancos de memoria muy potentes agilizaran estos procesos, dando más dinamismo a las conexiones de este tipo.
- Por último, es conveniente a nivel empresarial invertir en una buena combinación VPN entre hardware y software para optar por la tranquilidad del sistema, y no sufrir ataques o acceso indeseados que pueden ocasionar efectos lamentables a todo el conjunto de recursos.

"Metodología para la implementación de redes privadas virtuales con internet como red de enlace"

ORTEGA BUSTAMANTE, COSME MACARTHUR (2014)

Tesis de Grado

Universidad Técnica del Norte

- Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.
- Las VPN permiten una comunicación entre las oficinas centrales y las oficinas remotas, muy distantes geográficamente a través de internet de una forma segura.
- La VPN permiten brindar servicios a los clientes de la empresa en cualquier lugar del mundo, con lo que los clientes obtendrán la información que el necesita al instante, lo que generara una mayor productividad de la empresa.
- La implementación de una VPN, necesita de personal calificado para el análisis de requerimientos de la empresa y ver si es conveniente la implementación, para la misma. Este personal debe recibir la colaboración de cada uno de los departamentos de la empresa para que la implementación de la VPN sea óptima.
- Esta tecnología dispone de varias arquitecturas y topologías fácilmente adaptables a los diferentes tipos de empresas que puedan existir, ya que es una tecnología muy flexible y fácilmente acoplable al diseño de red de su empresa.
- La velocidad de comunicación a través de una VPN, se ve afectada considerablemente por la encriptación y encapsulación que los datos transferidos necesitan, para navegar seguros por la red pública.

2.2 ASPECTOS TEÓRICOS PERTINENTES

2.2.1 VIRTUAL PRIVATE NETWORK, RED PRIVADA VIRTUAL (VPN)

Una red privada virtual - VPN (Virtual Private Network), es una tecnología de red que permite a sus usuarios extender su red local sobre una red pública, con el fin de evitar un costoso sistema de arrendamiento o compra de líneas, que será utilizada por una sola organización.[1]

El objetivo de una VPN es ofrecer a la organización las mismas capacidades de seguridad, pero a un menor costo, esta tecnología también:

- Nos da la posibilidad de interconectar dos o más sucursales de la empresa utilizando como medio el Internet.
- Permite a los trabajadores de una determinada empresa, la conexión desde sus casas al centro de cómputo.
- Hace posible que los usuarios puedan tener acceso a su equipo del hogar desde algún lugar remoto.

2.2.2 COMPONENTES DE LAS VPN[2]

Una conexión de red privada virtual (VPN) consta de los siguientes componentes:

- **SERVIDOR VPN**

  Equipo que acepta las conexiones VPN de clientes VPN.
- **CLIENTE VPN**

  Equipo que inicia una conexión VPN a un servidor VPN. Un cliente VPN puede ser tanto un equipo individual como un enrutador.
- **TÚNEL**

  Viene a ser la parte de la conexión en la que se encapsulan los datos.

[1] Dennis, F. (2012). *Virtual Private Networks: Making the right connection, 1ra Edicion.* Morgan Kaufmann Publishers.

[2] (Microsoft, Microsoft, 2015)

- **CONEXIÓN VPN**

  Es la parte de la conexión en la que se cifran los datos. En las conexiones VPN seguras, los datos se cifran y encapsulan en la misma parte de la conexión.

- **PROTOCOLOS DE TÚNEL**

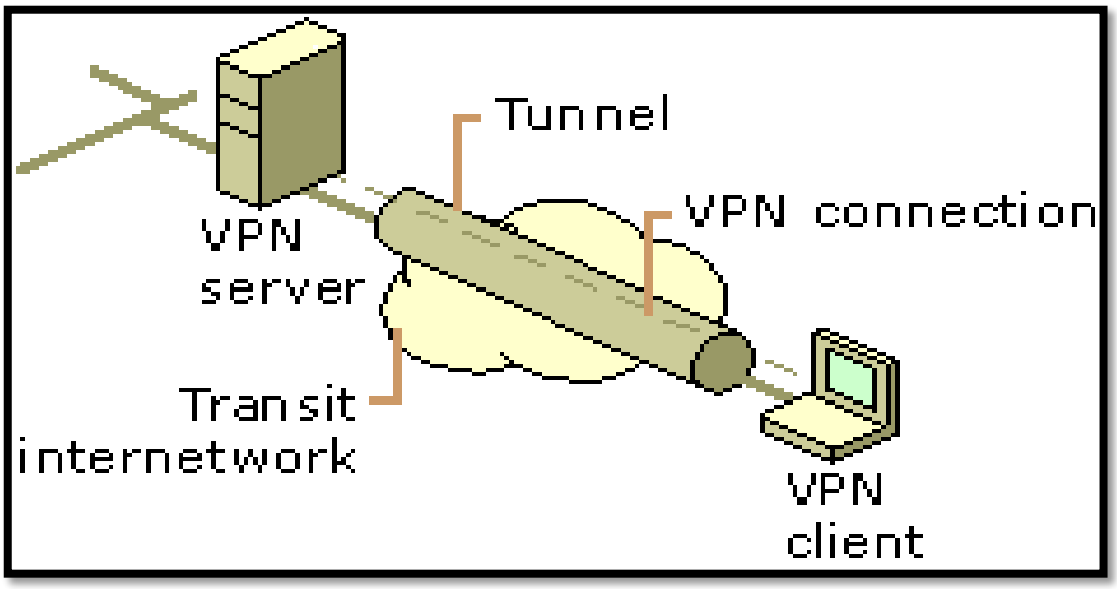
  Son utilizados para administrar túneles y encapsular datos privados. Los datos que se envían por el túnel también deben estar cifrados para construir una conexión VPN.

- **DATOS EN TÚNEL**

  Son los datos que normalmente se envían a través de un vínculo punto a punto privado.

- **REDES PRIVADAS DE TRÁNSITO**

  Es la red compartida o privada que atraviesan los datos encapsulados. En este caso el conjunto de redes públicas o privadas de tránsito puede ser Internet o una Intranet Privada Basada en IP.



Img 1. Componentes de una red Privada, Fuente: (Microsoft, 2015)

Br. JENNY MAR SEGUNDO

2.2.3 REQUISITOS QUE GARANTIZAN QUE UNA VPN SEA SEGURA[3]

Los requisitos que garantizaran que una VPN sea segura son:

- **DISPONIBILIDAD**

Este requisito se aplica tanto al tiempo de actualización como al tiempo de acceso.

- **CONTROL**

El control debe ser implementado por el supervisor o administrador de la Red Privada Virtual, sea este interno o externo dependiendo de cómo se realice la implementación de VPN.

- **COMPATIBILIDAD**

Debido que al utilizar las tecnologías VPN e internet, se basan en protocolos IP, la arquitectura interna del protocolo de red de una determinada compañía debe ser compatible con el IP originario de internet.

- **SEGURIDAD**

Hablar de seguridad y de red privada virtual, hasta cierto punto se podría decir que son sinónimos. La seguridad en una VPN abarca todo, desde el proceso de cifrado que se implementa hasta los servicios de autenticación de usuarios.

- **CONFIABILIDAD**

La confiabilidad es uno de los requisitos importantes que debe poseer una Red Privada Virtual, en algunos casos este requisito se ve afectado en las VPN´s que se sujetan de la confiabilidad que se tiene por parte del ISP, ya que si el servicio del ISP se interrumpe, la conexión no se establecerá, por ende no se podrá hacer nada hasta que el ISP nuevamente brinde su servicio a los clientes.

[3] (CopolInformática, 2015)

- **AUTENTICACIÓN DE DATOS Y USUARIOS**

DATOS

Reafirma que el mensaje ha sido enviado completamente y que no ha sido alterado de ninguna forma.

USUARIOS

Es el proceso que permite que el usuario acceda a la red.

La autenticación de datos y de usuarios es el proceso en el que se controla que sólo los usuarios admitidos tengan acceso, este requisito es sumamente importante dentro de cualquier configuración de Red privada Virtual, ya que afirma que los datos han sido entregados a su destinatario sin ningún tipo de alteraciones.

- **SOBRECARGA DE TRÁFICO**

La sobrecarga de tráfico es un problema de cualquier tipo de tecnología de redes, y por ende también es un problema inevitable, especialmente si tenemos una red privada virtual a través de un ISP.

2.2.4 PROTOCOLOS DE TÚNEL DE LAS VPN

- **POINT TO POINT TUNNELING PROTOCOL, PROTOCOLO PUNTO A PUNTO DE TÚNELES (PPTP)**

PPTP permite que el tráfico multiprotocolo se cifre y se encapsule en un encabezado IP para que de éste modo se envíe a través de una red IP pública, como Internet. PPTP puede utilizarse para el acceso remoto y las conexiones VPN entre sitios. Cuando se usa Internet como la red pública de una VPN, el servidor PPTP es un servidor VPN habilitado para PPTP con una interfaz en Internet y una segunda interfaz en la intranet.[4] El protocolo de túnel de punto a punto (PPTP) utiliza una conexión de TCP (puerto 1723) para el mantenimiento del túnel.

[4] (Microsoft, Microsoft, 2015)(10 de Octubre del 2015). Obtenido de Microsoft: (04 de febrero de 2015). Obtenido de Microsoft: https://msdn.microsoft.com/es-es/library/cc786563%28v=ws.10%29.aspx

PPTP encapsula las tramas PPP en datagramas IP para su transmisión a través de la red. PPTP usa una conexión TCP para la administración del túnel.

En cuanto a la seguridad de la VPN, este protocolo únicamente ofrece una encriptación básica.[5]

En la velocidad de VPN, este protocolo es rápido debido a la encriptación más baja.[6]

- **LAYER 2 TUNNELING PROTOCOL (L2TP)**

  Es una extensión de la PPTP, utilizado por los proveedores de servicios de Internet para proporcionar servicios VPN en internet, permite cifrar el tráfico multiprotocolo y enviarlo a través de cualquier medio compatible con la entrega de datagramas punto a punto, como IP. Este protocolo ofrece do

  Este protocolo facilita el enrutamiento de paquetes PPP a través de una red de tal manera que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

  En cuanto a la seguridad de la VPN, L2TP ofrece una máxima encriptación (comprueba la integridad de los datos y encapsula los datos dos veces).[7]

  En la velocidad de VPN, este protocolo necesita más proceso de la CPU para encapsular los datos dos veces.[8]

2.2.5 TIPOS DE VPN

- **HYBRID VPN**

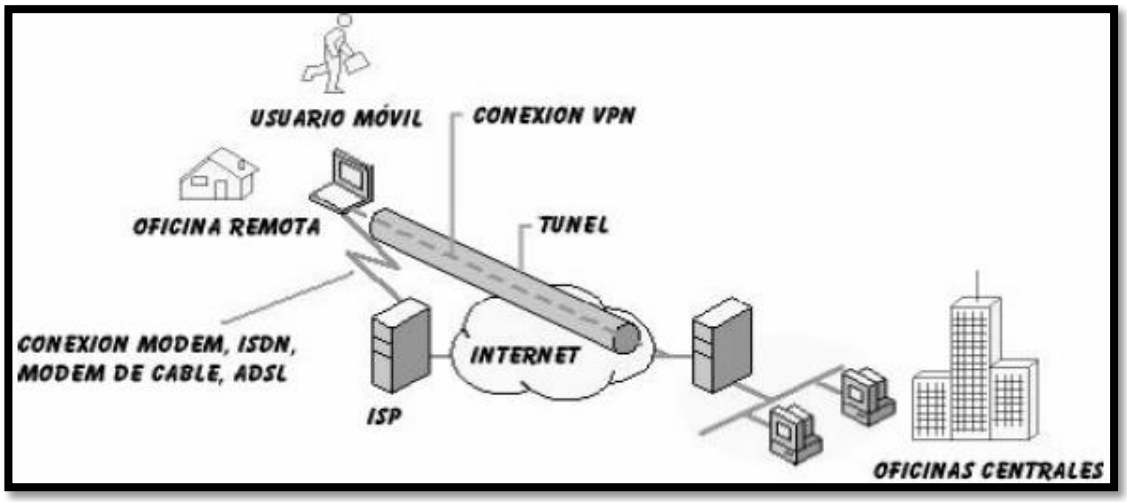
  Servidores VPN híbridos son capaces de aceptar conexiones de varios tipos de clientes de VPN, así mismo los VPN híbridos ofrecen una mayor flexibilidad tanto en cliente y en el servidor.

- **ACCESO REMOTO**

  Es considerado uno de los modelos más usados en la actualidad, donde usuarios, proveedores pueden tener acceso a las redes privadas de las oficinas, comercios, casas, hoteles, entre otros utilizando la infraestructura

[5] (VyprVPN, 2015)
[6] (VyprVPN, 2015)
[7] (VyprVPN, 2015)
[8] (VyprVPN, 2015)

de Internet para acceder a su red. Desde el momento en que son identificados y autenticados poseen acceso parecido al que tienen dentro de la red de la empresa.



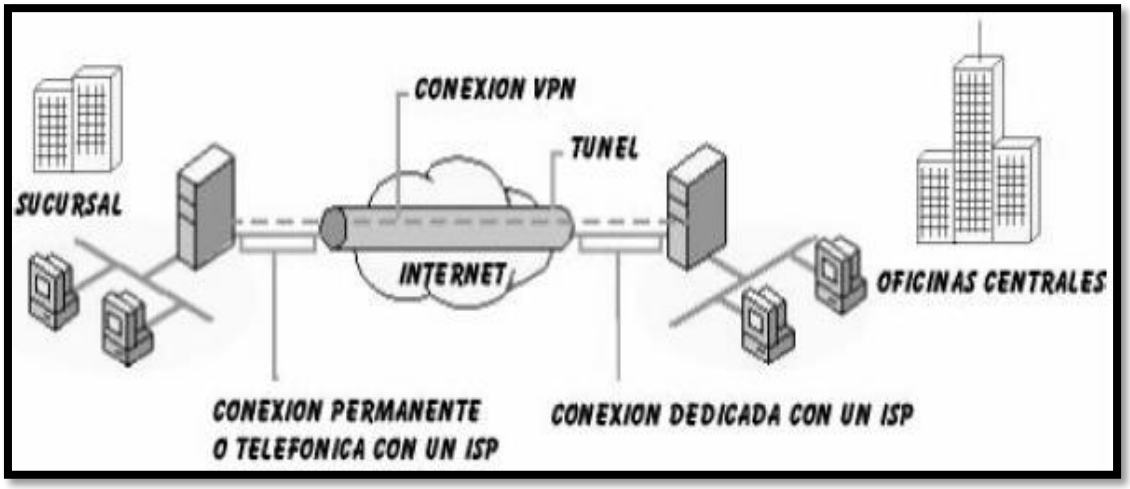
Img 2. Arquitectura de Acceso Remoto, Fuente (Microsoft, 2015)

- **PUNTO A PUNTO**

INTRANET

Una red privada virtual interna, es una implementación que no tiene un uso frecuente en el entorno de las redes. Este tipo de implementación se crea en una LAN, siempre que se considere necesario transferir información con mucha privacidad entre departamentos de una empresa.[9]

A su vez una intranet también es considerada como una red corporativa ya que permite compartir recursos entre sus miembros en forma segura.

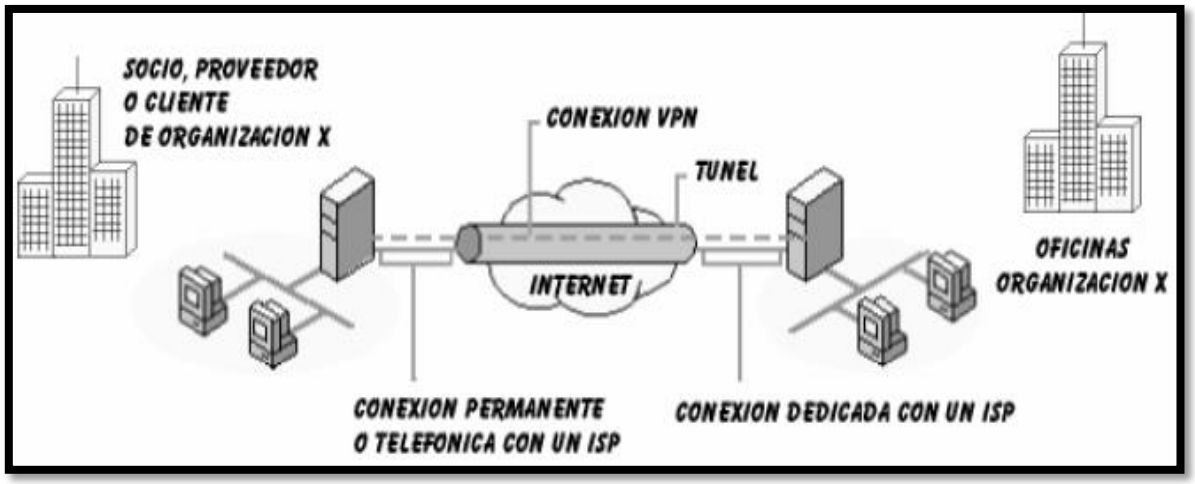


Img 3. Arquitectura Punto a Punto – Intranet Fuente (Microsoft, 2015)

[9] Stallings, W. (2012). *Data and Computer Networks, 8va Edicion.* Pearson Prentice Hall.

EXTRANET

Este tipo de implementación está dada por la creación de una conexión entre las oficinas centrales corporativas y las oficinas remotas que se encuentran en el exterior (proveedores). A comparación con una Intranet típica el acceso viene desde el exterior a la red y no desde el interior.



Img 4. Arquitectura Punto a Punto – Extranet Fuente (Microsoft, 2015)

2.2.6 DIFERENCIAS ENTRE INTERNET, EXTRANET E INTRANET

Entre las diferencias se tiene lo siguiente:

- **INTERNET**

  Está dirigido a cualquier usuario en general que tenga una conexión con la finalidad que pueda extraer información de cualquier tipo de página web.

- **EXTRANET**

  La extranet se dirige a usuarios tanto de la empresa como externos, pero en este caso la información que se encuentra en la extranet es totalmente restringida ya que tienen acceso a esta red aquellos usuarios que tengan permiso.

- **INTRANET**

  En este caso sólo podrán conectarse a ella las personas quienes tengan sus cuentas en un determinado servidor VPN, es decir que se encuentren conectadas a la red privada de la empresa. Esta red permite el intercambio de información entre los trabajadores de la empresa.

	TIPO DE ACCESO	USUARIOS	INFORMACIÓN
INTERNET	Público	General	General
EXTRANET	Semi - Público.	Grupo de empresas relacionadas.	Compartida dentro de un círculo de empresas.
INTRANET	Privado.	Miembros de una empresa.	Propia de la institución.

Tabla 2 Diferencias entre Internet, Extranet e Intranet

2.2.7 ARQUITECTURA DE LAS VPN[10]

- **VPN BASADA EN HARDWARE**

Las VPN basadas en Hardware poseen en el extremo del Servidor de la organización un “router” o “enrutador” dedicado, el cual tiene la misión de encriptar los datos, además de abrir y cerrar los túneles VPN cuando funciona como receptor. Estos proporcionan facilidades al usuario que administra la implementación VPN, ya que son seguros, rápidos, de fácil instalación y fáciles de usar.

Ofrecen un gran rendimiento ya que este es configurado para las operaciones que requiera el servicio VPN.

- **VPN BASADA EN FIREWALL**

Estos sistemas aprovechan las ventajas del “Firewall”. La desventaja de un sistema basado en Firewall afecta en mayor o menor medida al rendimiento del sistema general, lo que puede ser un problema para la organización dependiendo de las necesidades que se requieran. Algunos fabricantes de

[10] (Alfonso, 2015)

Firewalls ofrecen en sus productos procesadores dedicados a encriptación para minimizar el efecto del servicio VPN en el sistema.[11]

- **VPN BASADA EN SOFTWARE**

Estos sistemas son ideales en el caso en que los dos extremos que deseen comunicarse en forma remota y privada no pertenezcan a la misma organización. Esta solución permite mayor flexibilidad en cuanto a la decisión de que trafico enviar por el túnel seguro VPN, pudiendo decidir por protocolo y dirección donde en un sistema basado en hardware solo se puede decidir por dirección.

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

- **VPN PROPORCIONADA POR UN PROVEEDOR DE SERVICIOS DE RED (ISP)**

Este tipo de servicio es proporcionado por los Proveedores de Servicio de Internet (ISP), el cual se encarga de mantener el túnel entre una organización y el ISP. Correspondería al ISP mantener la VPN funcionando adecuadamente, y para esto el ISP se haría cargo de la instalación y configuración de la VPN.

El problema en este tipo de arquitectura es de quién se haría cargo de cada responsabilidad, lógicamente si el ISP instala su propio equipo, entonces la responsabilidad sería del ISP.[12]

- **VPN DE SISTEMA OPERATIVO**

Ofrecen servicios de VPN los sistemas operativos tales como: Windows server de Microsoft, Linux en sus diversas distribuciones (Debian, Red Hat) que requieren ser configurados adecuadamente para su funcionamiento. La ventaja principal de esta solución es que resulta ser económica, debido a que en un

[11] Ramirez Limari, V. H. (2010). Protocolos De Seguridad Para Redes Vpn.

[12] (Dennis, 2012)

mismo sistema operativo se puede contar con varios servicios tales como: administración de usuarios active directory, DHCP, VPN.

2.2.8 ACTIVE DIRECTORY (AD)

Es un servicio de directorio de red que se encarga de almacenar información y controlar, administrar el acceso a los recursos de la red. A su vez un servicio de directorio es el conjunto de aplicaciones, quienes se encargan de gestionar los objetos de red, tales como los recursos de red y los usuarios quienes permiten a los administradores de red tener un control más centralizado sobre la misma.

AD se basa en una estructura jerárquica de objetos, el cual se divide en tres categorías usuarios, servicios y recursos.

La finalidad del AD, es proporcionar, organizar información, así como la de establecer políticas de seguridad.

2.2.9 SERVIDOR DE CORREOS

Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

2.2.10 PROTOCOLOS PARA UN SERVIDOR DE CORREOS

- **SIMPLE MAIL TRANSFER PROTOCOL (SMTP)**

  Protocolo para la transferencia simple de correo electrónico, es el protocolo encargado de enviar y recibir mensajes.

- **POST OFFICE PROTOCOL (POP)**

  Protocolo de Oficina de Correo, se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

- **INTERNET MESSAGE ACCESS PROTOCOL (IMAP)**

  Protocolo de acceso a mensajes de internet, es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. Mediante

IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.[13]

2.2.11 SERVICIOS DE ACCESO Y DIRECTIVAS DE REDES (NPAS)

Encargados de proporcionar tecnologías las cuales permiten implementar las VPN´s, las mismas ayudan a definir y aplicar directivas de autenticación para acceso a redes, autorización y mantenimiento del cliente por medio de Servidor de Directivas de redes (NPS).

2.2.12 DIFERENCIAS ENTRE DOMINIO, ÁRBOL Y BOSQUE

- **DOMINIO**

  Zona definida de objetos de dominio, conformada por: usuarios, unidades organizativas, controladores de dominio.

- **ÁRBOL**

  Cuando un dominio raíz contiene “sub dominios”, a este conjunto de subdominios se le conoce como árbol, cabe indicar que cada subdominio a su vez contiene su propio control de dominio, el cual es el responsable de autenticar y almacenar la información de la cuenta de usuario.

- **BOSQUE**

  Es el conjunto de árboles de domino.

2.2.13 SISTEMA DE NOMBRES DE DOMINIO, DOMAIN NAME SYSTEM (DNS)

Sistema encargado de asignar nombres a equipos y servicios de red, los cuales se organiza en una jerarquía de dominios.

La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.[14]

---

[13] *Stallings, W. (2012). Data and Computer Networks, 8va Edicion. Pearson Prentice Hall.*

[14] *Microsoft, (2015). Obtenido de Microsoft: https://msdn.microsoft.com/es-es/library/cc787920(v=ws.10).aspx*

2.2.14 ZONAS DE BÚSQUEDA DNS[15]

Las zonas son las encargadas de traducir nombres DNS en direcciones IP, además de almacenar la información de uno o varios dominios, existen dos tipos de zonas de búsqueda: las zonas de búsqueda directa y las zonas de búsqueda inversa.

- **ZONA DE BÚSQUEDA DIRECTA**

  Encargada de traducir un nombre de dominio en una dirección IP, este tipo de zona es la más común en ser utilizada.

- **ZONA DE BÚSQUEDA INVERSA**

  Este tipo de zona se encarga de traducir direcciones IP en nombres DNS.

  Por ejemplo el registro con el formato ".in-addr.arpa", es el nombre de la búsqueda de zona inversa.

La diferencia entre ambas zonas es que, si se crea una zona de búsqueda directa, esta debe ser respaldada creando una zona de búsqueda inversa, asimismo cabe señalar, que sólo se crea la zona de búsqueda inversa, debido a que las zonas de búsqueda directa las crea el Active Directory automáticamente.

2.2.15 ISO 27001, SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)[16]

Para garantizar que la seguridad de la información sea gestionada correctamente, se debe identificar inicialmente los aspectos relevantes adoptados para garantizar su C-I-D:

- **CONFIDENCIALIDAD**

  Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

- **INTEGRIDAD**

  Salvaguardar la exactitud e integridad de la información y activos asociados.

- **DISPONIBILIDAD**

  Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

[15] (Mircrosoft, 2015)
[16] (-CNB, 2009)

En base a estos tres aspectos, es como se debe de adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.[17]

2.2.16 ATAQUES MAN IN THE MIDDLE

Un ataque **"**man in the midle**"**(hombre en el medio), es un tipo de amenaza en donde el atacante tiene la habilidad de desviar o controlar las comunicaciones entre dos partes (víctima- servidor) ó (víctima - router).[18]

Además de ello, éste tipo de ataque consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por el atacante y poder así des-encriptar los datos, contraseñas, etc.[19] Los componentes para llevar a cabo éste tipo de ataque son los siguientes:

- ✓ Víctima.
- ✓ Atacante.
- ✓ Router o servidor.

Para realizar éste tipo de ataque es necesario conocer los siguientes aspectos:

- **MODO PROMISCUO**

  Capturar todo el tráfico que circula por una red.[20]

- **TÉCNICA ARPSPOOF**

  ARP Spoofing o envenenamiento de tablas ARP, es una técnica de hacking usada para infiltrarse en una red, con el objetivo de que un atacante pueda husmear los paquetes de datos que pasan por la LAN (red de área local), modificar el tráfico, o incluso detenerlo.[21]

  Mediante este tipo de ataques, se puede obtener información sensible de una víctima que esté en la misma red que el atacante, como nombres de usuario, contraseñas, cookies, mensajes de correo y mensajería instantánea, conversaciones VoIP, etc.[22]

[17] ISO 27001:2008
[18] (Microsoft, Microsoft, 2015)
[19] (Ccurso de hackers, 2016)
[20] (Linux GNU Blog, 2016)
[21] (Linux GNU Blog, 2016)
[22] (Linux GNU Blog, 2016)

- **HERRAMIENTA SSLSTRIP**

  Sslstrip es una aplicación para sistemas operativos Linux capaz de "descifrar todo el tráfico HTTPS" que viaja a través de la red y sniffea el tráfico (usuarios y claves) que viaja a través de la red en "HTTPS (cifrado)".[23]

2.2.17 ESPECIFICACIONES ROUTER CISCO RV325

Cisco RV325 es una opción perfecta para compañías que necesitan una combinación de rendimiento, seguridad y fiabilidad para la gestión de redes de alto rendimiento.[24] Este router ofrece rendimiento, flexibilidad y seguridad en un sólo dispositivo.

➢ **VENTAJAS DE CISCO RV325**

- **ALTO RENDIMIENTO**

  Fácilmente maneja archivos grandes y usuarios concurrentes para guardar a empleados productivos

- **ACCESO SIMPLE, MUY SEGURO**

  Une ubicaciones múltiples y trabajadores remotos que usan VPN.

- **FÁCIL DE USAR**

  Reducen el tiempo de la configuración.

[23] (Seguridad Informática, 2016)
[24] (Cisco, Cisco, 2016)

CAPÍTULO III

METODOLOGÍA

3.1 TIPO DE INVESTIGACIÓN

Este proyecto es considerado una investigación del tipo descriptiva. Investigación Descriptiva según el autor Roberto Hernández Sampieri en el libro Metodología de la Investigación quinta edición[25], indica lo siguiente:

La investigación descriptiva, consiste en buscar especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice[26]. Es decir se recolectará toda la información necesaria para poder llevar a cabo la propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI.

3.2 DISEÑO DE LA INVESTIGACIÓN

El diseño de la presente investigación es de tipo transversal, el cual se refiere a que los individuos son observados únicamente una vez y que las encuestas, cuestionarios y los censos son estudios transversales.[27] Este tipo de diseño fue elegido debido a que con anterioridad mi persona realizó sus prácticas pre profesionales en el Instituto Nacional de Estadística e Informática sede Cusco, en donde se pudo observar de cerca de que manera se lleva a cabo el proceso de intercambio de información entre las sedes Lima y Cusco del INEI, a su vez este tipo de diseño también fue elegido debido a que para la obtención de la información se aplicaron cuestionarios al personal de las áreas administrativas en común de las sedes Lima – Cusco del INEI.

Para realizar el presente trabajo de investigación, se consideró lo siguiente:

- Determinar las áreas de estudio.
- Establecer las técnicas de estudio: observación y cuestionarios, los cuales se tomaron en cuenta para recopilar toda la información necesaria

[25] Roberto Hernández Sampieri, Metodología de la Investigación, 5ta Edición, México
[26] Roberto Hernández Sampieri, Metodología de la Investigación, 5ta Edición, México
[27] Altman Douglas G. “Practical Statistics for Medical Research”, 1st edition, London

- Instalar los sistemas operativos para el desarrollo del trabajo de investigación, en este caso Windows server 2008 r2 como servidor y Windows 7 para clientes.
- Configuración de la intranet y el servidor de correos.
- Configuración de cuentas de usuarios (clientes VPN).
- Pruebas de envío y recepción de mensajes entre las cuentas configuradas.
- Realizar pruebas con el ataque man in the middle para probar la efectividad de la VPN.
- Analizar los resultados de la fase de pruebas para obtener las conclusiones.
- Finalmente elaborar las recomendaciones para futuros trabajos de investigación.

3.3 POBLACIÓN Y MUESTRA

3.3.1 POBLACIÓN

Como población se consideró a todas las áreas administrativas de las sedes Lima - Cusco del INEI, la cantidad de éstas fueron especificadas en el siguiente cuadro.

SEDE INEI	AREAS EN TOTAL INEI		AREAS EN TOTAL
	AREAS ADMINISTRATIVAS EN COMUN	AREAS ADMINISTRATIVAS	
LIMA	8	17	17
CUSCO	8		8
AREAS TOTAL LIMA - CUSCO	**25 ÁREAS ADMINISTRATIVAS**		

Tabla 3 Población del INEI sedes Lima – Cusco – Fuente (Elaboración Propia)

En el cuadro anterior se puede apreciar que en la sede Lima del INEI se tiene un total de 17 áreas administrativas **(véase en el ANEXO 1)**, mientras que en la sede Cusco se tiene un total de 08 áreas administrativas **(véase en el ANEXO 2)**. En el siguiente cuadro se puede apreciar la cantidad total del personal, los cuales laboran en las áreas administrativas de las sedes Lima – Cusco del INEI.

SEDE	CANTIDAD DE PERSONAL		TOTAL CANTIDAD DE PERSONAL
	AREAS ADMINISTRATIVAS	AREAS ADMINISTRATIVAS EN COMUN	
LIMA	150	70	220
CUSCO	13		13
TOTAL TRABAJADORES LIMA - CUSCO	233 Trabajadores en Áreas Administrativas		

Tabla 4 Total Personal en las Áreas Administrativas de las Sedes Lima - Cusco del INEI– Fuente (Elaboración Propia)

Según los datos expuestos en el cuadro anterior, se puede observar que en la sede Lima se tiene un total de 220 trabajadores en las áreas administrativas en general, mientras que en la sede Cusco sólo se tiene un total de 13 trabajadores, obteniendo un total de 233 trabajadores en las áreas administrativas.

3.3.2 MUESTRA

El tipo de muestra que se utilizó en el presente trabajo de investigación fue del tipo "probabilístico", debido a que todos los trabajadores de las áreas administrativas en común entre las sedes Lima – Cusco del INEI **(véase en el ANEXO 3)**, tienen la misma probabilidad de ser elegidos para representar a la población en general. La técnica del muestreo probabilístico utilizada fue el "muestreo aleatorio estratificado", ya que el personal administrativo a los cuales se les aplicó el cuestionario adjuntado en el **ANEXO 4**, fueron realizados en los horarios de jornada laboral en ambas sedes.

Asimismo cabe indicar que el muestreo probabilístico es "la selección de elementos que se basa parcialmente en el criterio del investigador"[28] y que la técnica de muestreo aleatorio estratificado, hace referencia al estudio de un subgrupo dentro de la población, que está conformada por sujetos fácilmente accesibles y presentes en un lugar determinado.

El siguiente cuadro hace referencia a la cantidad total de trabajadores y áreas administrativas en común entre las sedes Lima – Cusco del INEI, los cuales fueron tomados como punto de estudio (muestra) del presente trabajo de investigación.

[28] Kinnear y Taylor, Metodología, 1998. Pág. 145

SEDE INEI	AREAS ADMINISTRATIVAS EN COMÚN	TOTAL DE TRABAJADORES DE AREAS ADMINISTRATIVAS EN COMUN
LIMA	8	70
CUSCO		13
TOTAL LIMA - CUSCO	**8 AREAS ADMINISTRATIVAS EN COMÚN**	**83 Trabajadores**

Tabla 5 Muestra de estudio INEI Sedes Lima - Cusco– Fuente (Elaboración Propia)

- **CRITERIOS DE INCLUSIÓN DE LA MUESTRA**

Para el desarrollo del presente trabajo de investigación se consideró como único punto de estudio las "áreas administrativas en común de las sedes Lima - Cusco del INEI", debido a que se tuvo más accesibilidad específicamente a las áreas administrativas de la sede Cusco del INEI **(véase ANEXO 2)**.

Como se obtuvo un total de 83 trabajadores como muestra, se vio por conveniente determinar un único tamaño del muestreo utilizando la siguiente fórmula del tipo de población finita, en donde se trabajó con el 95% de confiabilidad y el 5% de margen de error.

$$\mathrm{n} = \frac{z^2 p * (1-q) * N}{Ne^2 + Z^2 * p * (1-q)}$$

Donde:

n : Tamaño de la muestra.

e : Error de estimación.

Z : Nivel de confianza.

N : Universo.

p : Probabilidad a favor.

q : Probabilidad en contra.

DATOS:

n : ?

e : 5% = 0.05

Z : 1.96 (tabla de distribución normal para el 95% de confiabilidad y 5% error)

N : 83 trabajadores

p : 0.50

q : 0.50

SOLUCIÓN:

Reemplazando los valores de la información que se tiene, se obtuvo lo siguiente:

$$n = \frac{(1.96)^2(0.5)(1-0.50)(83)}{(83)(0.05)^2 + (1.96)^2(0.50)(1-0.50)}$$

$$n = 68.25$$

$$n = 68 \text{ Trabajadores}$$

Con el resultado obtenido de 68 trabajadores, esa fue la cantidad la cual representó al total de los 83 trabajadores que en un inicio se tenía.

3.4 INSTRUMENTOS

3.4.1 INSTRUMENTOS PARA LA RECOLECCIÓN DE INFORMACIÓN

Para la recolección de datos se tomó en cuenta el uso de las siguientes técnicas:

- **LA OBSERVACIÓN**

  Esta técnica permitió identificar con más facilidad el problema ya que mi persona anteriormente realizó sus prácticas pre profesionales en dicha institución en la sede Cusco, cabe mencionar que se utilizó el tipo de observación “no estructurada” debido a que al momento de realizar las prácticas pre profesionales aún no se tenía identificado el problema”.

  Gracias a la utilización de esta técnica se pudo identificar el problema, así mismo se planteó una solución para la mejora de la confidencialidad en el intercambio de información.

- **CUESTIONARIO**

  Esta técnica permitió plantear un listado de preguntas, con la finalidad de verificar de qué manera actualmente se lleva a cabo el intercambio de información entre las sedes Lima – Cusco del INEI, este cuestionario puede ser observado en el **ANEXO 4,** el cual está compuesto por un total de ocho (08) preguntas, en donde las cinco (05) primeras preguntas fueron dirigidas a todo el personal de las áreas administrativas en común de las sedes Lima y Cusco del INEI, y las tres (03) preguntas restantes fueron dirigidas solo al personal del área de informática.

3.5 RECOLECCIÓN Y ANÁLISIS DE DATOS

Para dar fiabilidad de la herramienta utilizada (cuestionario), para la recolección de la información, se utilizó la prueba alfa de Cronbach **(véase ANEXO 7)**, dando un total del 0.88 de fiabilidad, teniendo en cuenta que el rango de fiabilidad en la prueba alfa de cronbach es >0.6 y <=1.

Con las respuestas obtenidas del cuestionario aplicado al personal administrativo en común de las sedes Lima- Cusco del INEI, se obtuvieron los siguientes resultados:

Las siguientes preguntas se realizaron a los trabajadores de las áreas administrativas de las sedes Lima – Cusco del INEI.

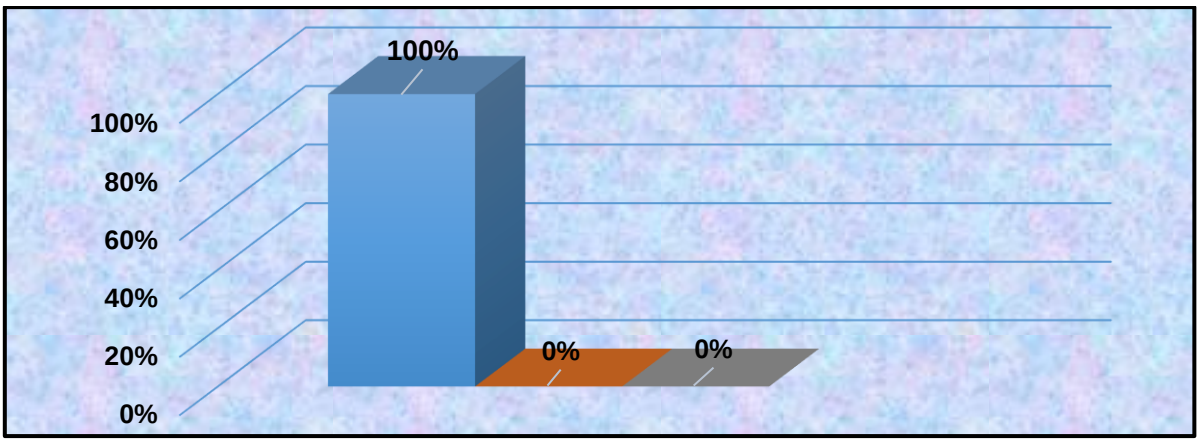
1) **¿Actualmente en la institución se utilizan correos no institucionales para el envío y recepción de información confidencial?**

   Si ( ) -> Hotmail ( ) Gmail ( ) otros ( )

   No ( ) ¿Por qué?

ALTERNATIVAS		RESULTADOS
SÍ	Hotmail	100%
	Gmail	0%
	Otros	0%
NO		0%

Tabla 6 Porcentaje de uso de servidores de correo – Fuente (Elaboración Propia)



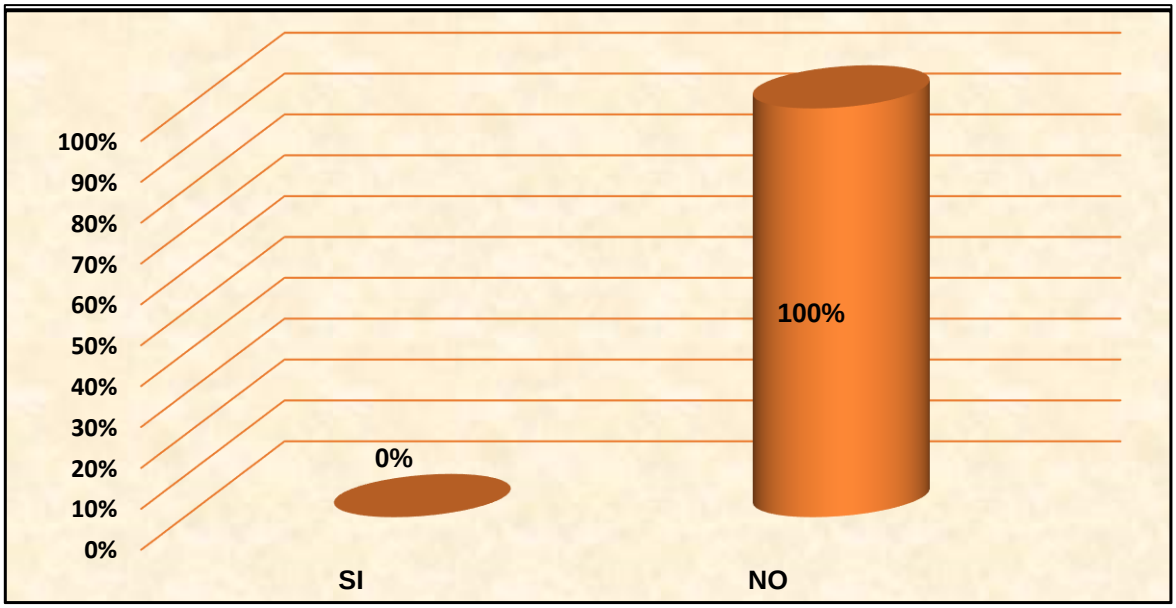
Img 5. Porcentaje de uso de Hotmail para el envío y recepción de información confidencial– Fuente (Elaboración Propia)

Aplicada la encuesta, la respuesta por parte del 100% de los trabajadores fue que ciertamente en la institución se utilizan correos no institucionales como es el Hotmail, utilizado como medio para el envío y recepción de información confidencial.

2) ¿Usted posee una cuenta de correo institucional?

ALTERNATIVAS	RESULTADOS
SÍ	0%
NO	100%

Tabla 7 Porcentaje de Trabajadores que Poseen una Cuenta de Correos Institucional– Fuente (Elaboración Propia)



Img 6. Porcentaje de Trabajadores que Poseen o no una Cuenta de Correo Institucional – Fuente (Elaboración Propia)

Con las respuestas obtenidas se puede observar que el total del 100% de los trabajadores no posee una cuenta de correo institucional para el envío y recepción de correos los cuales la mayoría de ellos contienen temas confidenciales pertinentes a la institución.

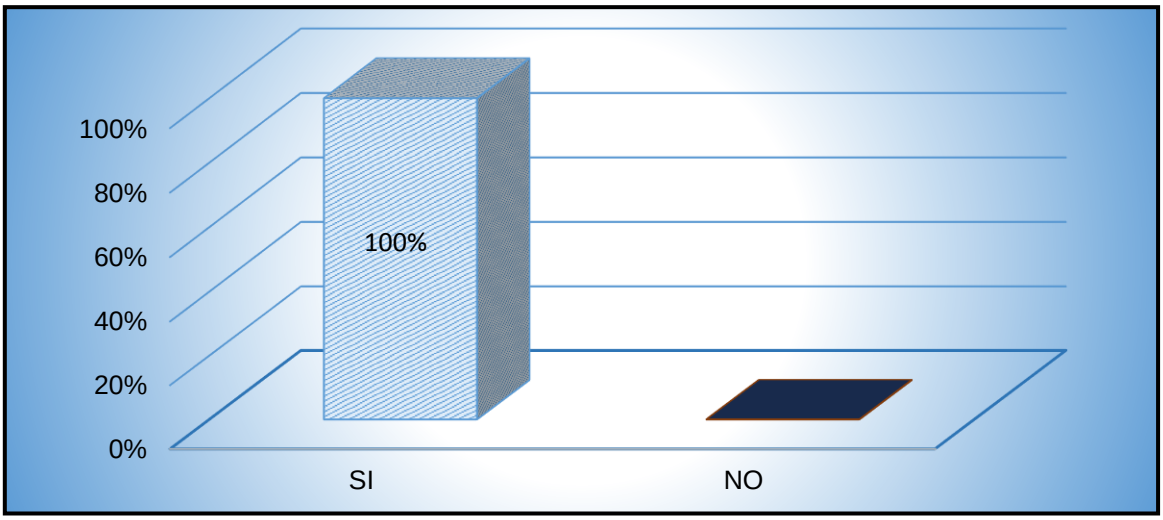
3) ¿Utiliza su cuenta de correo no institucional para el envío de información laboral y confidencial?

Si ( )

No ( ) ¿Por qué?

ALTERNATIVAS	RESULTADOS
SÍ	100%
NO	0%

Tabla 8 Porcentaje de trabajadores que utilizan cuentas de correo no institucional– Fuente (Elaboración Propia)



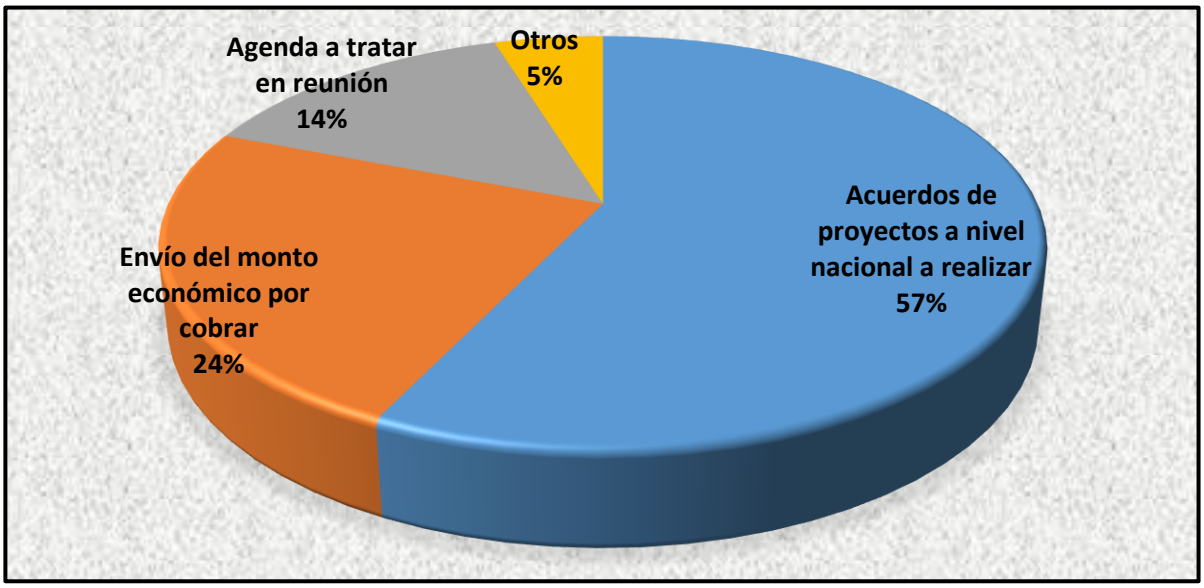
Img 7. Porcentaje de trabajadores que utilizan sus cuentas de correo no institucional– Fuente (Elaboración Propia)

Según el 100% de trabajadores encuestados, afirman utilizar sus cuentas de correos no institucionales como Hotmail, para el envío de información personal y confidencial de una sede a otra (Lima - Cusco).

4) ¿Qué tipo de información es la que se envía por estas cuentas?

ALTERNATIVAS		RESULTADOS
a)	Acuerdos de proyectos a nivel nacional a realizar	**57%**
b)	Envío del monto económico por cobrar	**24%**
c)	Agenda a tratar en reunión	**14%**
d)	Otros	**5%**

Tabla 9 Tipo de Información Enviado por Cuentas de Correos no Institucionales– Fuente (Elaboración Propia)



Img 8. Porcentaje de tipo de información enviada por cuentas de correos instruccionales– Fuente (Elaboración Propia)

El tipo de información confidencial que se envía con más frecuencia por las cuentas de correo no institucional, son:

- Con un 57% los acuerdos de proyectos que se han de desarrollar a nivel nacional, en este punto se indican la cantidad específica de materiales que se envían de una sede a otra.
- Con un 24% el envío de monto económico por cobrar, este hace referencia a la suma económica que envía la sede Lima a la sede Cusco para el desarrollo de uno de los proyectos que éste ordenó.
- Con un 14% la agenda a tratar en reunión.
- Con un 5 % otros.

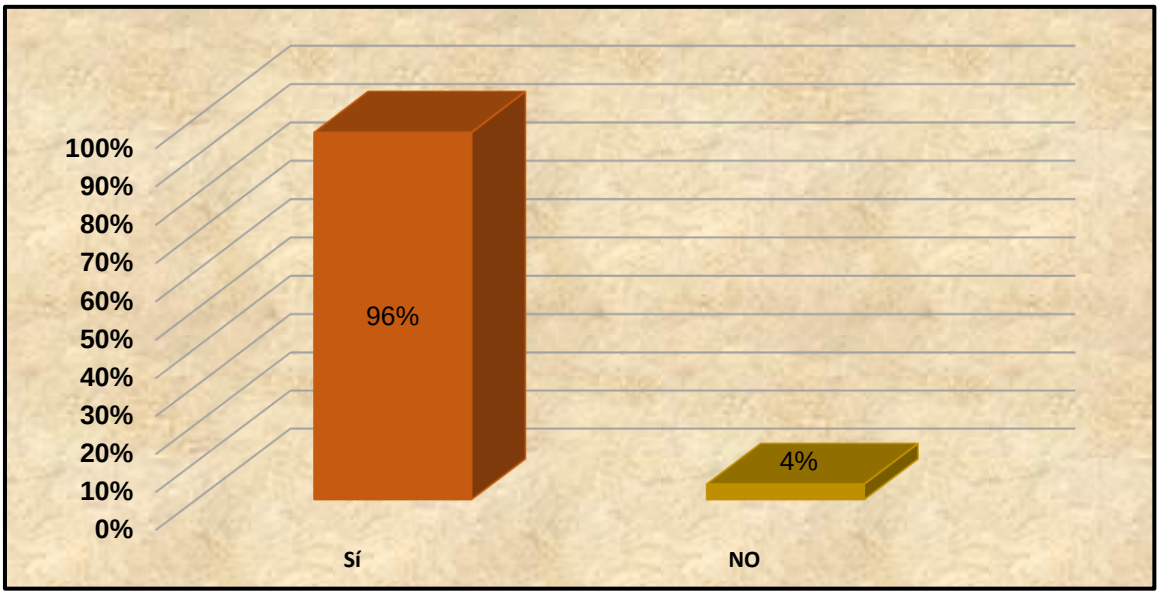
5) ¿Le gustaría que se implemente un correo institucional para el envío y recepción de información netamente institucional?

Si ( )

No ( ) ¿Por qué?

ALTERNATIVAS	RESULTADOS
Sí	96%
NO	4%

Tabla 10 Porcentaje de trabajadores a favor que se implemente un correo institucional– Fuente (Elaboración Propia)



Img 9. Porcentaje de trabajadores a favor que se implemente un correo institucional– Fuente (Elaboración Propia)

El 96% del personal encuestado indicó que si le gustaría que se lleve a cabo la implementación de un correo institucional para el envío y recepción de información netamente institucional, así mismo cabe señalar que el 4% del personal indicó todo lo contrario, debido a que se teme que el manejo de procedimientos para el envío y recepción de información al cual están acostumbrados, sea diferente a como hoy en día la viene realizando.

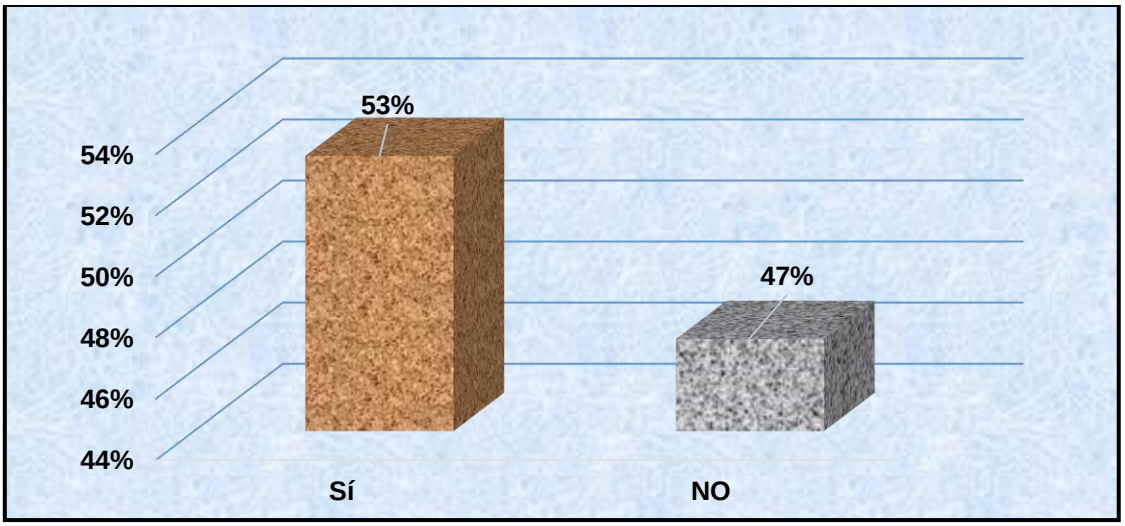
Las siguientes preguntas se realizaron sólo al personal del área de informática de las sedes Lima – Cusco del INEI.

6) ¿Existen antecedentes de vulnerabilidades de información anteriormente realizadas a alguna cuenta?

Si ( ) ¿Como cuáles?
No ( )

ALTERNATIVAS	RESULTADOS
Sí	53%
NO	47%

Tabla 11 Porcentaje de Antecedentes de Vulnerabilidades de Información – Fuente (Elaboración Propia)



Img 10. Porcentaje de Antecedentes de Vulnerabilidad de Información – Fuente (Elaboración Propia)

El personal del área de informática señaló que el 53% del personal administrativo en común de las sedes Lima – Cusco del INEI en la actualidad presenta inconvenientes con sus cuentas de correo, debido a que estas fueron hackeadas y el 47% indicaron que no presentan ningún tipo de problemas con sus cuentas de correo no institucionales.

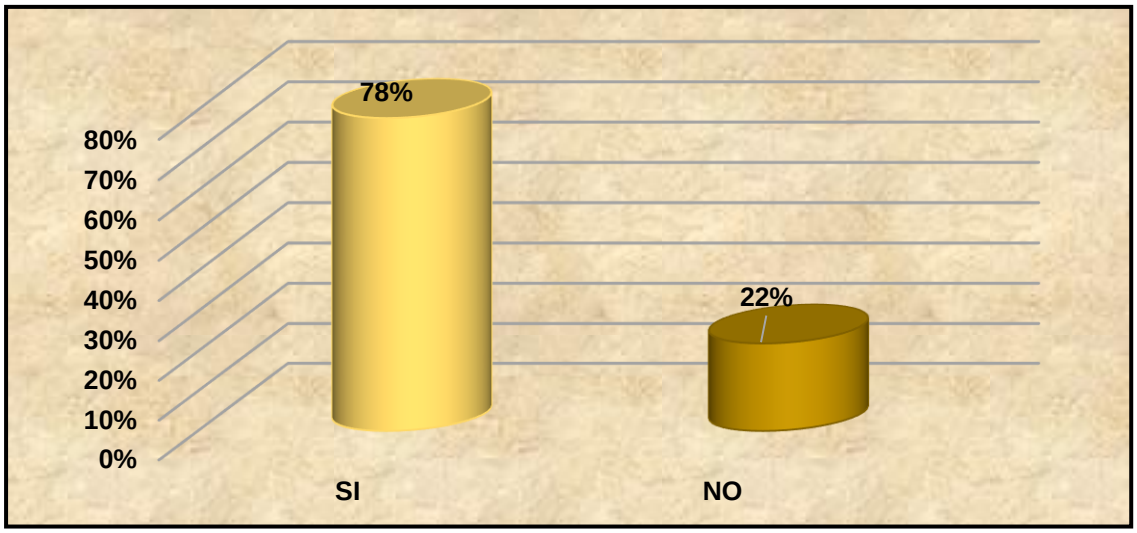
7) ¿Se cuenta con medidas de seguridad en caso de posibles ataques?

Si ( ) ¿Como cuáles?

No ( ) ¿Por qué?

ALTERNATIVAS	RESULTADOS
Sí	78%
NO	22%

Tabla 12 Porcentaje de trabajadores que afirman la existencia de medidas de seguridad ante posibles ataques – Fuente (Elaboración Propia)



Img 11. Porcentaje trabajadores que afirman contar con medidas de seguridad – Fuente (Elaboración Propia)

Según el porcentaje de las respuestas obtenidas por parte de los trabajadores del área de informática de las sedes Lima – Cusco del INEI, señalan lo siguiente: el 78% indica que la institución se basa en algunas de las políticas de seguridad del ISO 27001 pero que éstas NO están siendo aplicadas, a su vez mi persona puede ratificar con lo señalado debido a que con anterioridad me encontraba en calidad de practicante en el área de informática del INEI sede Cusco, finalmente el 22% señala todo lo contrario ya que éstos se encuentran en calidad de nuevo personal.

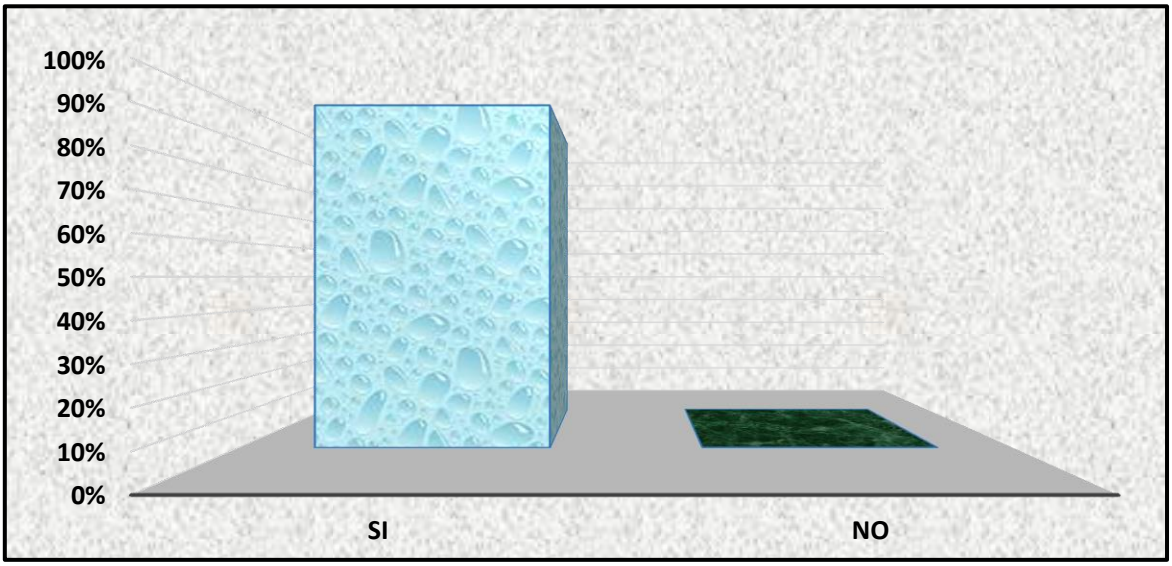
8) ¿Estaría de acuerdo con la implementación de una intranet vía VPN para la interconexión de las sedes Lima – Cusco del INEI?

Si ( ) ¿Por qué?

No ( ) ¿Por qué?

ALTERNATIVAS	RESULTADOS
Sí	100%
NO	0%

Tabla 13 Porcentaje de trabajadores a favor de la implementación de una intranet Vía VPN – Fuente (Elaboración Propia)



Img 12. Porcentaje de Trabajadores que Desean que se Realice la Implementación de una Intranet Vía VPN – Fuente (Elaboración Propia)

El 100% del personal informático encuestado indicó que si estaría de acuerdo con la implementación de una intranet vía VPN para la mejora de la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI, obteniendo así ninguna negativa ante dicha propuesta.

CAPÍTULO IV

REQUERIMIENTOS, ANÁLISIS Y DISEÑO DE LA INTRANET PROPUESTA

4.1 IDENTIFICACIÓN DE REQUERIMIENTOS

Anteriormente mi persona realizó sus prácticas pre profesionales en la sede Cusco del INEI, durante mi estancia en dicha institución pude observar de qué manera se lleva a cabo la transmisión de información entre las sedes Lima- Cusco del INEI, así como también algunos incidentes que se produjeron en la sede Cusco los cuales fueron anteriormente mencionados en la descripción de la situación actual perteneciente al Capítulo I.

Una vez culminado con el periodo de prácticas pre profesionales, decido realizar para la entidad una mejora en la seguridad de la información en base al ISO 27001, tomando al CID (confidencialidad, integridad y disponibilidad) para dar solución a los problemas observados en la entidad.

- **CONFIDENCIALIDAD**

  Asegura que la información de la entidad sea accesible únicamente al personal administrativo autorizado de las sedes Lima – Cusco del INEI.

- **INTEGRIDAD**

  Asegura que la información llegue completa y exacta tal y como se envió del emisor al receptor, ya sea entre el personal administrativo perteneciente a la sede Lima - Cusco, o entre el personal de una sola sede en particular.

- **DISPONIBILIDAD**

  El personal administrativo de ambas sedes podrá tener acceso a la información propia de la entidad que éste haya enviado o recibido del emisor, cuando sea necesario.

4.2 ANÁLISIS DE LA SOLUCIÓN

Para llevar a cabo la fase de análisis de la solución, se realizó la comparación entre una conexión con VPN y otra con una red normal la cual actualmente viene utilizando las sedes Lima – Cusco del INEI, dicha comparación se realizó con el objeto de ver cuál de éstas sería la mejor opción que se ajuste a las necesidades actuales de la entidad, teniendo como objetivo garantizar la confidencialidad, integridad y la disponibilidad de la información que ejecutan ambas sedes.

4.2.1 RED ACTUAL VERSUS RED CON VPN

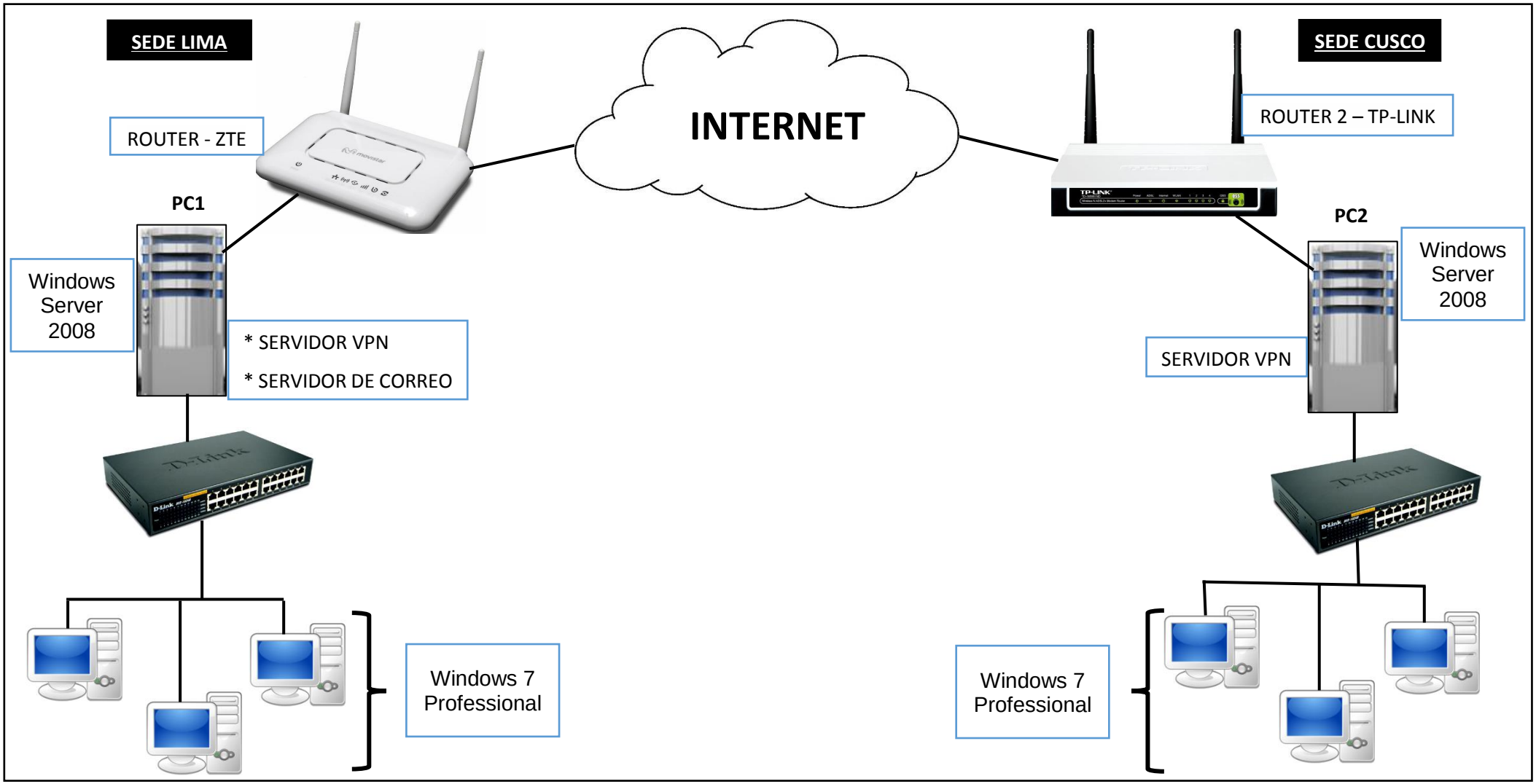
	RED ACTUAL	RED CON VPN
VENTAJAS		• Encripta la información. • Permite a los usuarios tener una conexión remota. • Mejora la seguridad de la información. • Mejora la productividad. • Confidencialidad de la información. • Permite la integridad, confidencialidad de los datos. • limitado a los costes de hardware, mantenimiento y actualización • Integridad de la información. • Autenticación y autorización.
DESVENTAJAS	• La información que se establece de una sede a otra viaja sin ser encriptada. • Posible robo de información durante él envió de información entre una sede a otra.	• Velocidad de internet es menor al de una conexión tradicional.
COSTO	• Pago al proveedor por el servicio de internet.	• Los costos para llevar a cabo tanto la implementación como el mantenimiento de esta tecnología, tiene que ver más con la capacitación que se deba brindar al personal encargado de las oficinas de informática de ambas sedes decir la entidad más que realizar un gasto, estaría realizando una inversión cuya retribución sería asegurar la integridad, confidencialidad y seguridad de la información. • Pago al proveedor por el servicio de internet.
BENEFICIO		• Bajos costos. • Facilidad de uso. • Optima la comunicación y el flujo de información entre empleados. • Control de acceso basado en las políticas de la organización. • Hace posible la comunicación con un número extenso de usuarios a bajo costo.

		• Incrementa el nivel de seguridad para el resguardo de la confidencialidad de la información emitidas de una sede a otra. • Utiliza protocolos de seguridad y encriptación de datos para mantener la confidencialidad y autenticidad de los mismos.

Tabla 14. Red actual versus Red con VPN – Fuente (Elaboración Propia)

Una vez habiéndose realizado la comparativa entre la red actual que viene utilizando el INEI y la red con VPN, se vio por conveniente proponer la implementación de una intranet vía VPN (red con VPN), con la finalidad de mejorar la confidencialidad, la integridad y la disponibilidad de la información, asimismo asegurando el resguardo de ésta.

4.2.2 DISEÑO DE LA SOLUCIÓN



Img 13. Diseño de la solución – Fuente (Elaboración Propia)

- **DESCRIPCIÓN DEL DISEÑO DE LA SOLUCIÓN**
  - El tipo de VPN utilizado en el presente trabajo de investigación, fue del tipo “punto a punto” con la finalidad de interconectar las sedes Lima – Cuso del INEI, ambas sedes ubicadas en distintos lugares geográficos.
  - La arquitectura utilizada, fue VPN de sistema operativo, debido a que el sistema operativo que se utilizó para la configuración de la intranet fue Windows server 2008 r2 utilizando los servicios de: domino de Active Directory, servicios de acceso y directivas de redes, servicios de acceso remoto y creación de usuarios para el personal de las áreas administrativas en común entre las sedes Lima – Cusco del INEI, asimismo se utilizó Windows 7 Professional para la configuración de los clientes VPN, utilizando los servicios de conectividad para conectarse a la intranet.
  - El protocolo de túnel empleado fue el PPTP, utilizando la conexión TCP con el puerto 1723 (puerto VPN). El protocolo PPTP muy aparte de ofrecer una encriptación básica de la información que se establezca entre las sedes Lima – Cusco del INEI, ofrece una velocidad más rápida de la VPN.
  - La plataforma en la que se realizaron las configuraciones de la VPN fue en Windows Server 2008 r2, esto implica a que si la intranet se configura en versiones posteriores a ésta, la intranet funcionara perfectamente al igual como funcionó en esta versión.
  - Para la creación de la intranet, simular su funcionamiento y acorde a mis factibilidades técnicas, se utilizaron dos routers convencionales (ZTE y TP - LINK), con los cuales la intranet funcionó perfectamente, esto quiere decir que si la intranet se configura en otros routers de gama alta como por ejemplo CISCO y otras marcas, la intranet ha de funcionar con mayor razón. Cada router estuvo ubicado en diferente zona geográfica. Las características de cada router, se detallan en el siguiente cuadro:

	ROUTER 1	ROUTER 2
Marca	ZTE	TP-LINK
Modelo	ZXHN H108N	TD-W8901G
Velocidad de Transmisión	4MB	4MB

Tabla 15. Routers ZTE y TP-LINK – Fuente (Elaboración Propia)

NOTA: El ISP utilizado en ambos casos fue el ISP de telefónica.

4.2.3 DESCRIPCIÓN TÉCNICA

- **HARDWARE**

Para llevar a cabo las configuraciones de la intranet vía VPN en Windows server 2008 r2, se utilizó lo siguiente:

CANTIDAD	BIEN	DESCRIPCIÓN
2	PC de Escritorio 1	Servidor VPN
		Servidor de Correos
	PC de Escritorio 2	Servidor VPN
2	Laptop 1	Clientes VPN
	Laptop 2	

Tabla 16. Descripción técnica – Hardware – Fuente (Elaboración Propia)

- **PC DE ESCRITORIO 1**

La PC de escritorio 1, la cual contiene al servidor VPN y al servidor de correos, comprende las siguientes características:

SERVIDOR VPN – SERVIDOR DE CORREOS	CARACTERÍSTICAS
Placa madre	H97 Gigabyte
FSB de Placa	1333 MHz
Procesador	CORE i5

Arquitectura	x64
RAM	8GB
Tipo de Ranura de RAM	DDR3
Sistema Operativo	Windows Server 2008 r2 - 64bits
Disco	1TB
Tarjeta de video	no integrado

Tabla 17. Descripción Técnica - Máquina de escritorio 1 – Fuente (Elaboración Propia)

- **PC DE ESCRITORIO 2**

La PC de escritorio 2, simula al servidor VPN y comprende las siguientes características:

SERVIDOR VPN	CARACTERÍSTICAS
Placa madre	H81 Gigabyte
FSB de Placa	1333 MHz
Procesador	CORE i5
Arquitectura	x64
RAM	8GB
Tipo de Ranura de RAM	DDR3
Sistema Operativo	Windows Server 2008 r2 - 64bits
Disco	500GB
Tarjeta de video	Integrado

Tabla 18. Descripción Técnica - Máquina de escritorio 2 – Fuente (Elaboración Propia)

- **LAPTOP 1**

CLIENTE VPN	CARACTERÍSTICAS
Marca	HP
Modelo	G4-2050la
Procesador	Core i5
Arquitectura	x64
RAM	8GB
Tipo de Ranura de RAM	DDR3
Sistema Operativo	Windows 7 Professional - 64 bits
Disco	500GB

Tabla 19. Descripción Técnica – Laptop 1 – Fuente (Elaboración Propia)

- **LAPTOP 2**

CLIENTE VPN	CARACTERÍSTICAS
Marca	Toshiba
Modelo	Satelite L50T-A-11T
Procesador	Core i7
Arquitectura	x64
RAM	6GB
Tipo de Ranura de RAM	DDR3
Sistema Operativo	Windows 7 Professional - 64 bits
Disco	750 GB

Tabla 20. Descripción Técnica – Laptop 2 – Fuente (Elaboración Propia)

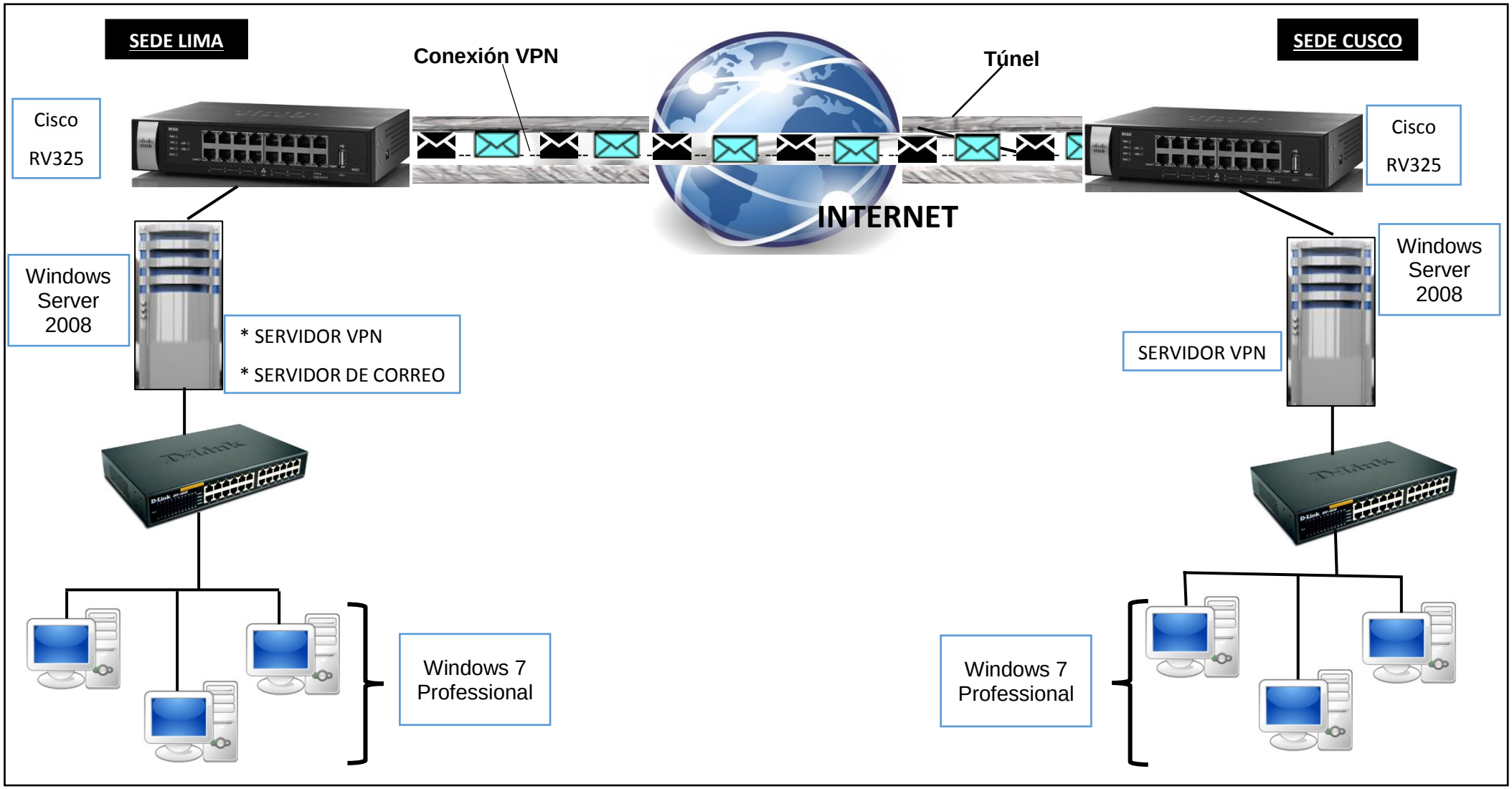
- **SOFTWARE**

  En el siguiente cuadro se puede observar los instaladores que fueron utilizados para llevar a cabo las configuraciones tanto de la VPN como el servidor de correos.

BIEN	SERVICIO	SOTFWARE UTILIZADO
Máquina de Escritorio 1	Servidor VPN	Windows Server 2008 R2
	Servidor de Correos	Windows Server 2008 r2
		Exchange Server 2010
Máquina de Escritorio 2	Servidor VPN	Windows Server 2008 r2
Laptop 1 y 2	Configuración de clientes VPN	Windows 7 Professional

Tabla 21. Descripción Técnica – Software – Fuente (Elaboración Propia)

4.2.4 DISEÑO DE LA INTRANET EN PRODUCCIÓN



Img 14. Diseño de la intranet en producción – Fuente (Elaboración Propia)

- **DESCRIPCIÓN DEL DISEÑO DE LA INTRANET EN PRODUCCIÓN**

Si deseara implementar la intranet VPN para la mejora de la confidencialidad en el intercambio de información entre las sedes Lima Cusco del INEI, se necesitaría los siguientes aspectos:

- Pc´s con Windows 7 Professional para los clientes VPN, los cuales actualmente son utilizados por los trabajadores administrativos de ambas sedes.
- Un servidor VPN y Correo para la sede Lima en la plataforma Windows server 2008.
- Un servidor VPN para la sede Cusco en la plataforma Windows server 2008.
- Dos routers Cisco una para cada sede (Lima – Cusco del INEI), para el uso exclusivo de la intranet vía VPN con las siguientes especificaciones:

	ROUTER – SEDE LIMA	ROUTER – SEDE CUSCO
Marca	Cisco	Cisco
Modelo	Cisco RV325	Cisco RV325
Velocidad de Transmisión	8MB	4MB

Tabla 22. Especificaciones routers cisco para sedes Lima – Cusco – Fuente (Elaboración Propia)

CAPÍTULO V

DESARROLLO DE LA INVESTIGACIÓN

5.1 CONSTRUCCIÓN DE LA INTRANET VÍA VPN

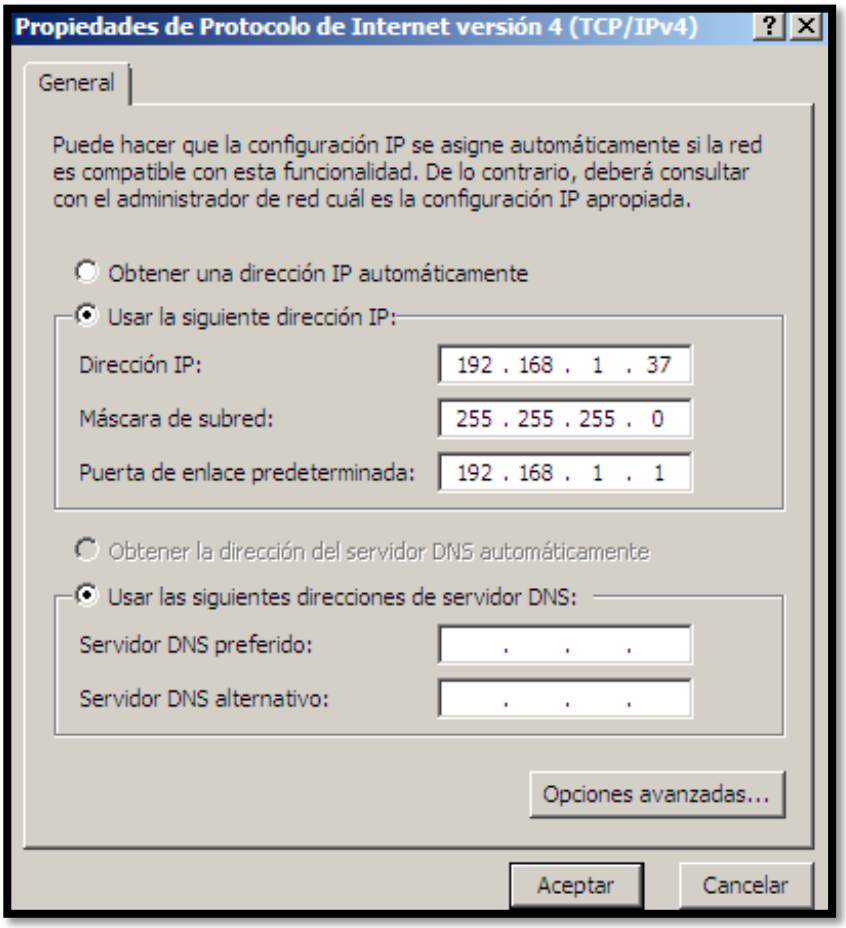
5.1.1 CONFIGURACIÓN DEL SERVIDOR VPN

Para iniciar con el proceso configuración VPN, se realizaron las instalaciones previas tanto para el Servidor VPN como para los clientes VPN (Personal administrativo).

Para el servidor VPN, se utilizó el sistema operativo Windows server 2008 Enterprise, la instalación de dicho sistema operativo se muestra en el **ANEXO 5**.

5.1.2 DIRECCIÓN IP DEL SERVIDOR

Para asignar una dirección IP al servidor se siguieron los siguientes pasos: propiedades de red, administrar conexiones de red, conexión de área local (presionar anticlick), propiedades, protocolo de internet versión 4 (TCP/IPv4), pulsar aceptar y verificar la conexión a internet.



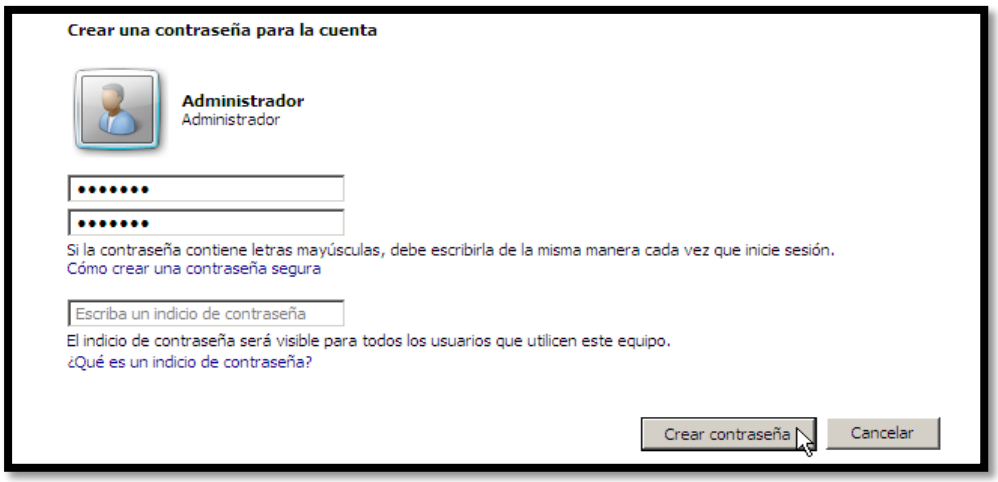
Img 15. Dirección IP del Servidor VPN – Fuente (Elaboración

5.1.3 ASIGNACIÓN DE CONTRASEÑA

Para no tener ningún inconveniente durante el proceso de configuración del Servidor VPN, fue necesario asignarle una contraseña, para ello se deben seguir los siguientes pasos: panel de control, cuentas de usuario, crear una contraseña para la cuenta.

Es importante que la contraseña incluya números, letras mayúsculas y minúsculas con el propósito de brindar seguridad al servidor.

Una vez asignado y confirmado la contraseña se seleccionó la opción “Crear Contraseña”.



Img 16. Asignación de Contraseña al Servidor VPN – Fuente (Elaboración Propia)

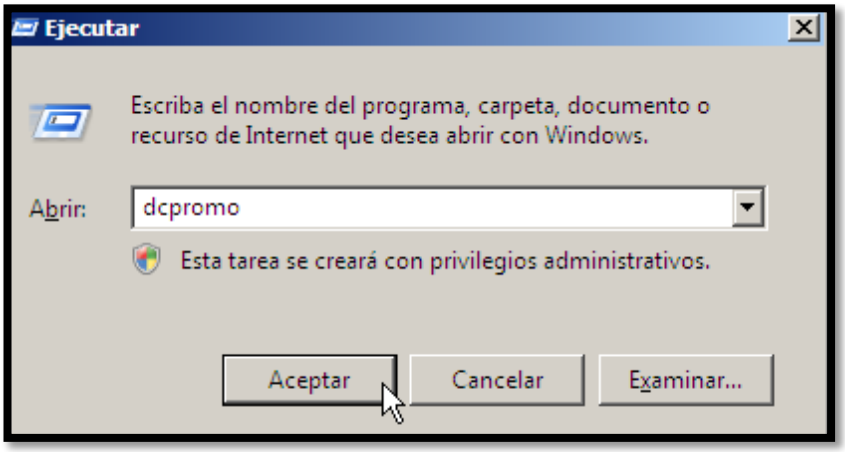
Para guardar los cambios efectuados se reinició el equipo. Una vez iniciado la sesión del administrador colocar la contraseña que se asignó al servidor.

Img 17. Inicio de Sesión al Servidor VPN – Fuente (Elaboración Propia)

Br. JENNY MAR SEGUNDO

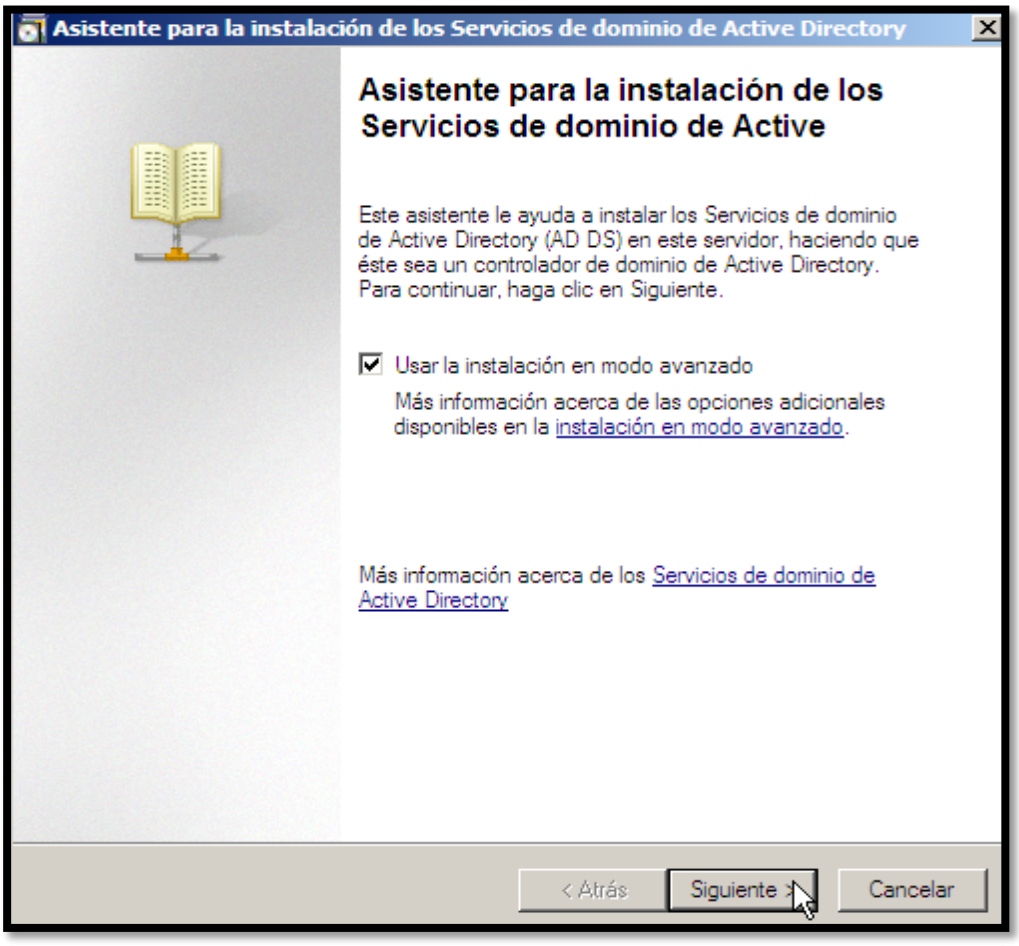
5.1.4 INSTALACIÓN DE SERVICIOS DE DOMINIO DE ACTIVE DIRECTORY

Para iniciar con la configuración de Active Directory se siguieron los siguientes pasos: presionar las teclas Windows + R, escribir el comando dcpromo.



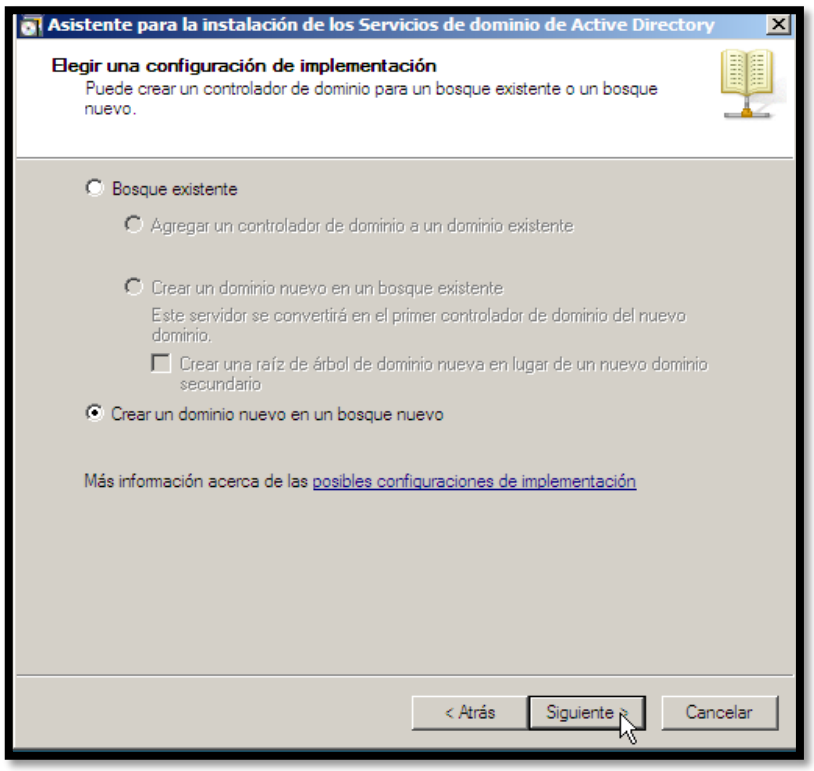
Img 18. Ventana de Ejecución dcpromo – Fuente (Elaboración Propia)

En la ventana del asistente para la instalación de los Servicios de dominio de Active, se seleccionó la opción “usar la instalación en modo avanzado”.



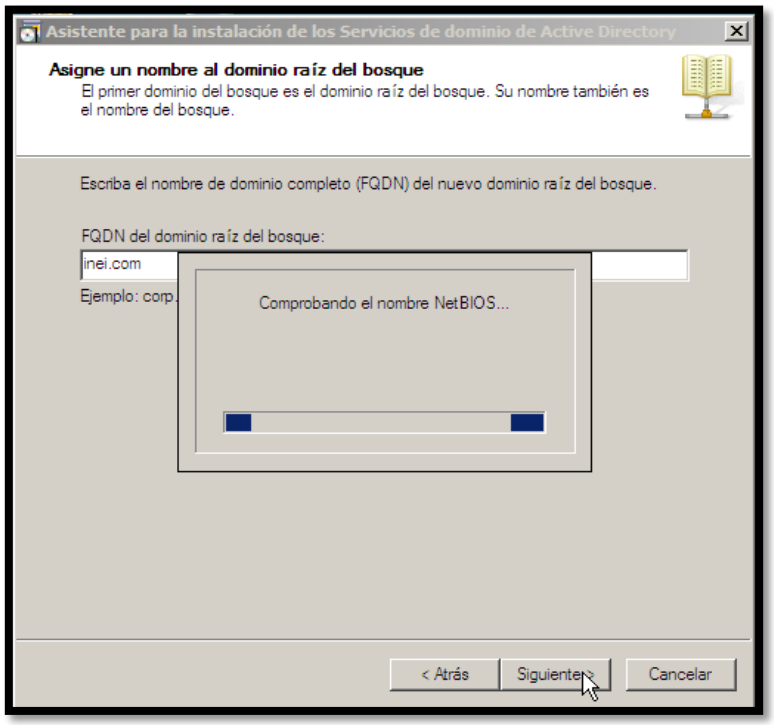
Img 19. Ventana del Asistente para la Instalación de los Servicios de dominio de Active – Fuente (Elaboración Propia)

Se seleccionó la opción “Crear un dominio nuevo en un bosque nuevo”, ya que se creará por primera vez un nuevo dominio.



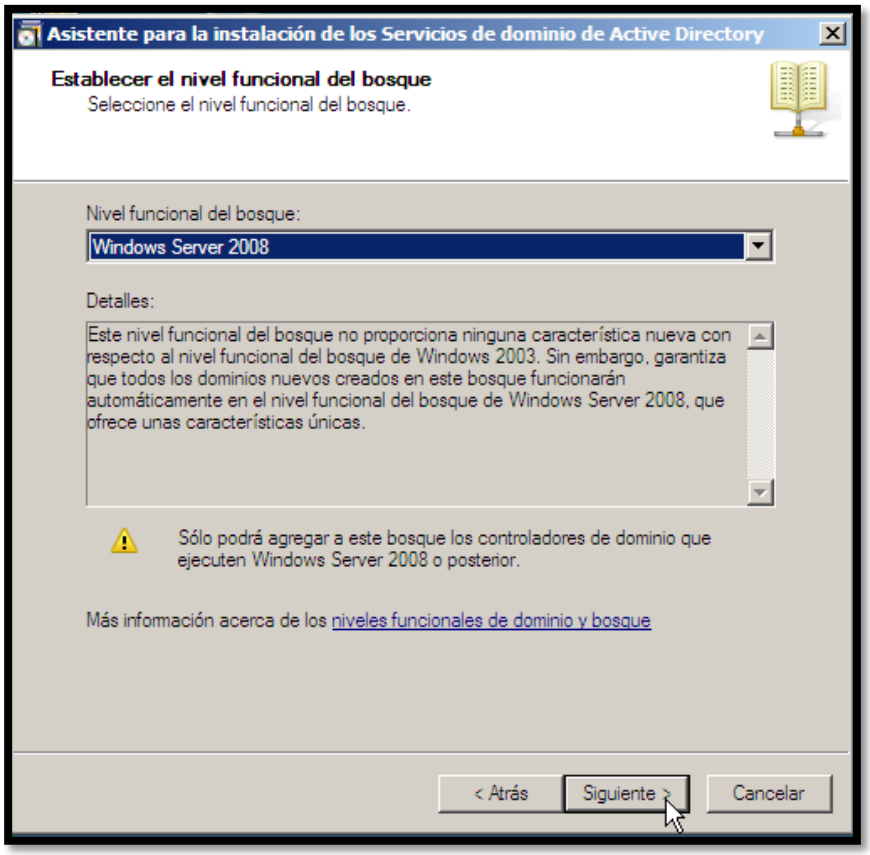
Img 20. Asistente para la Instalación de los Servicios de Dominio de Active Directory – Fuente (Elaboración Propia)

El nombre del dominio raíz del bosque que se utilizó para la configuración del servidor VPN fue el nombre de la institución, en este caso fue “inei.com”.



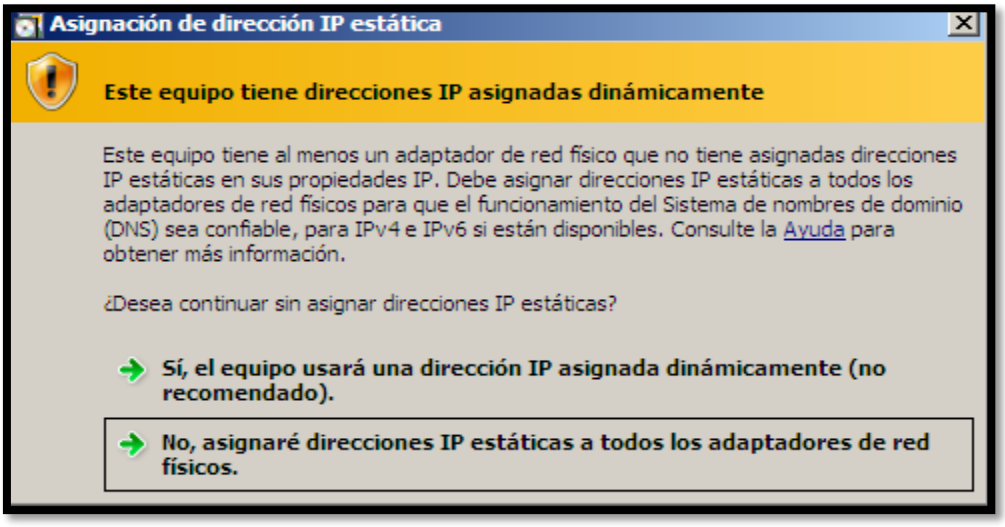
Img 21. Nombre del dominio raíz del bosque – Fuente (Elaboración Propia)

Los niveles de funcionalidad del bosque pueden ser Windows server 2000,2003 y 2008, en este caso se eligió la plataforma en que se está configurando el servidor "Windows server 2008".



Img 22. Nivel funcional del bosque – Fuente (Elaboración Propia)

En cuanto a la asignación de IP's s, en los equipos de cómputo de ambas sedes se utilizaron IP´s estáticas, debido a que si se presentara algún tipo de problema tales como la ausencia de internet, las IP´s facilitaran la ubicación del equipo que presenta inconvenientes con la red.

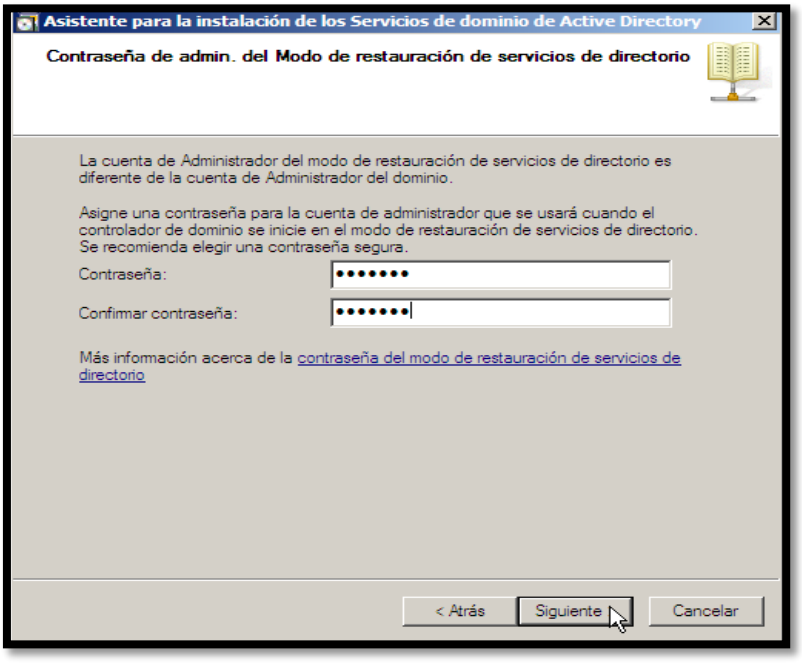


Img 23. Asignación de dirección IP estática – Fuente (Elaboración Propia)

Se dejó por defecto la ruta en donde las carpetas se crearán por defecto.

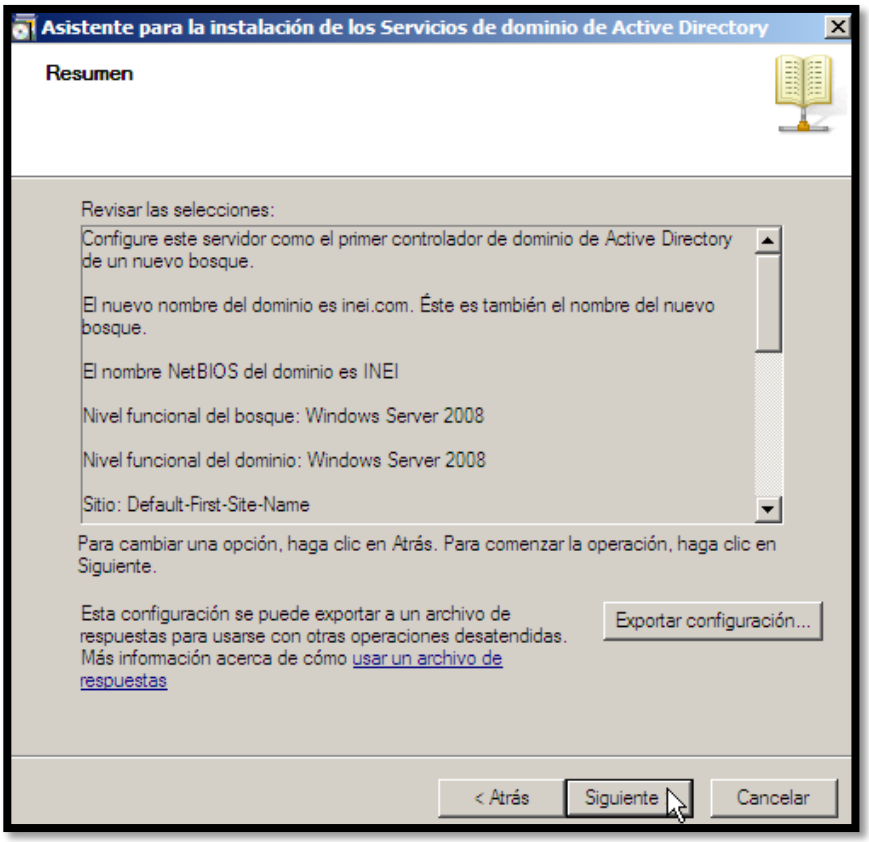
Img 24. Ventana de ubicación de la Base de Datos – Fuente (Elaboración Propia)

Se asignó la contraseña al Administrador de Servicios de Active Directory, para ello es recomendable usar letras mayúsculas, minúsculas y/o números pero de preferencia se sugiere colocar la contraseña del administrador del equipo para evitar olvidos posteriores.



Img 25. Contraseña del Administrador de Active Directory – Fuente (Elaboración Propia)

Seguidamente apareció el resúmen de todos los servicios de dominio, que se han de instalar.



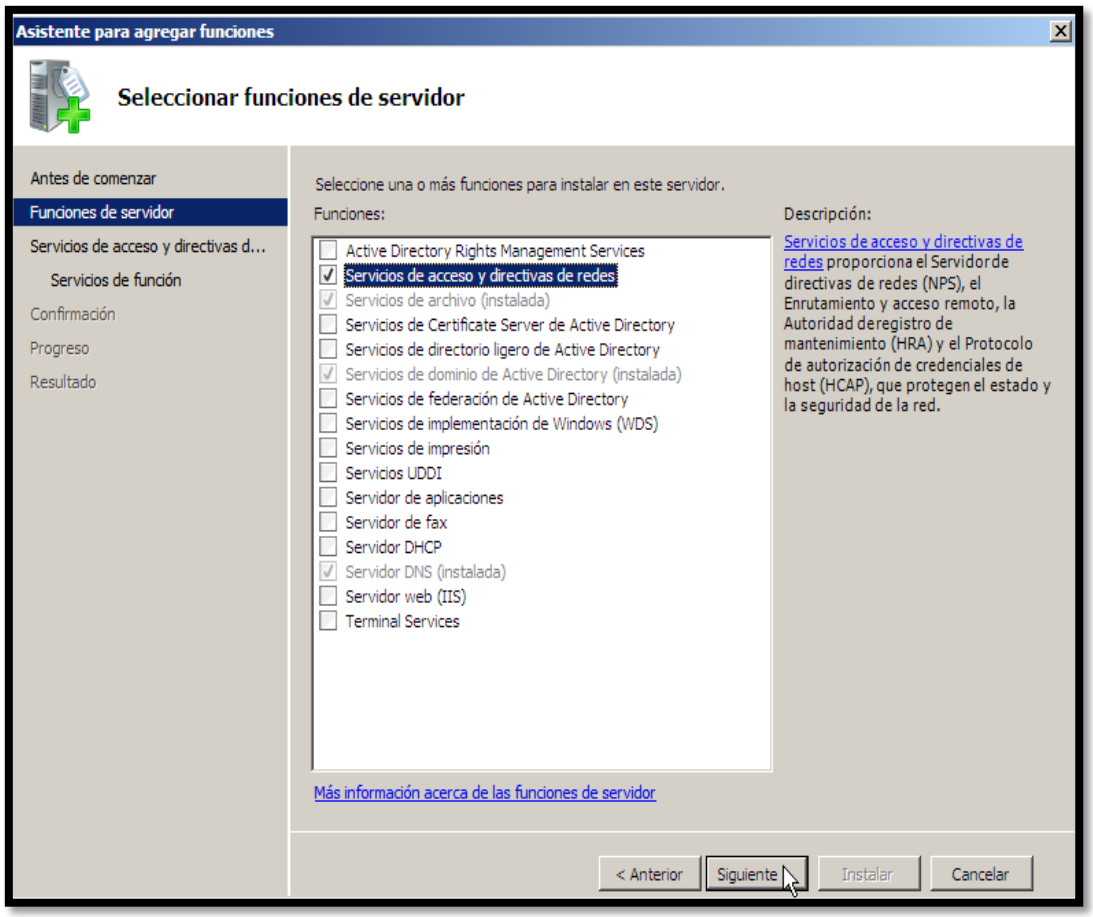
Img 26. Ventana Resúmen para la instalación de Dominio de Active Directory – Fuente (Elaboración Propia)

Para finalizar con el proceso de instalación de los Servicios de Dominio de Active Directory, se reinició el equipo con la finalidad de asegurar que se guarden todas las configuraciones realizadas.

Img 27. Ventana de Instalación de Domino de Active Directory – Fuente (Elaboración Propia)

5.1.5 FUNCIONES DE ADMINISTRADOR DEL SERVIDOR VPN

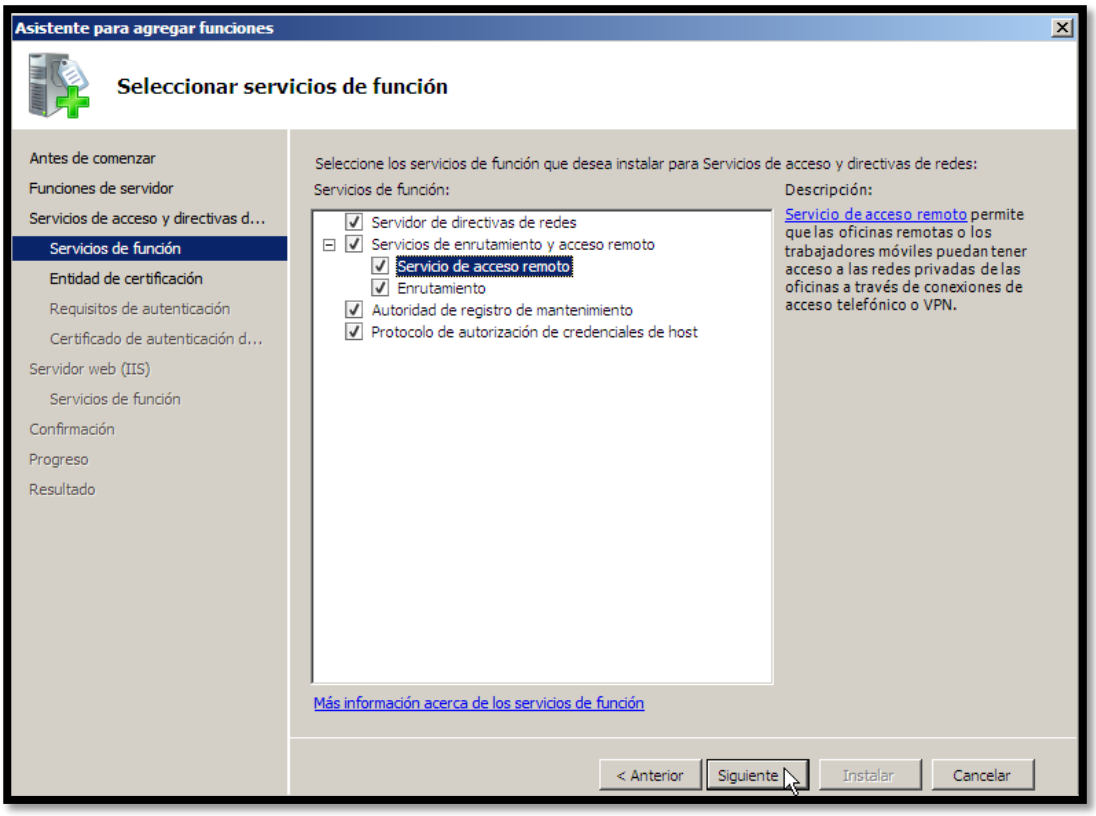
Para definir las funciones del servidor se siguieron los siguientes pasos: Inicio, administrador del servidor (presionar anticlik), agregar funciones. La opción que se eligió fue “Servicios de acceso y Directivas de Redes (NPAS)” para la seguridad de la red.



Img 28. Funciones del Servidor VPN – Fuente (Elaboración Propia)

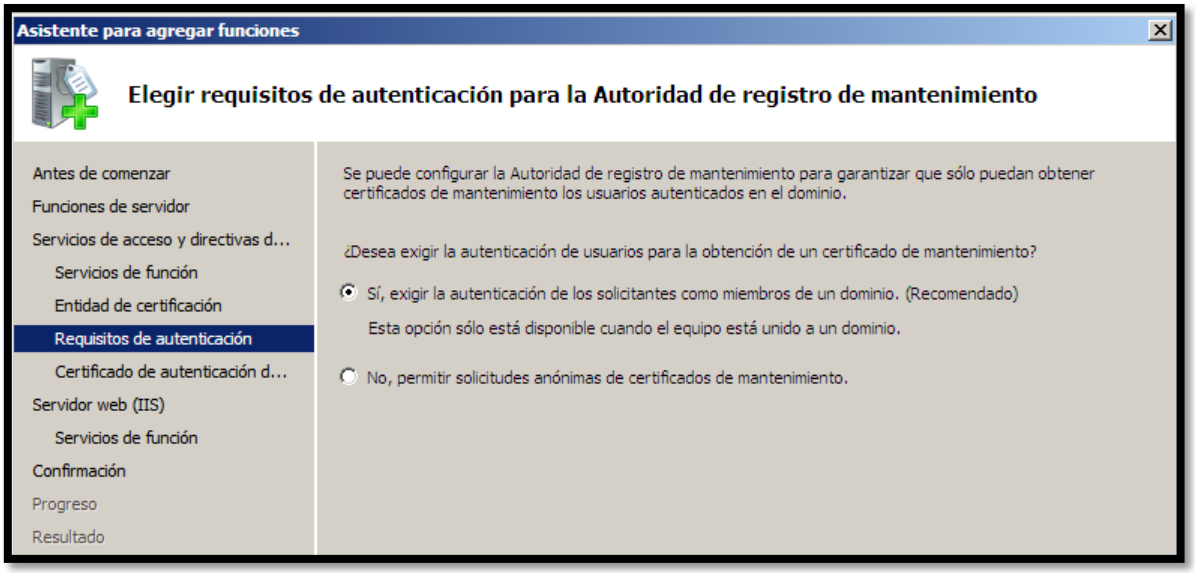
En los Servicios de Función se seleccionó la opción “Servicio de Acceso Remoto”, con la finalidad de que las cuentas para los trabajadores administrativos que posteriormente se han de crear, puedan acceder a la VPN.

En esta ventana ubicar y seleccionar la opción “servicio de acceso remoto”, para que los trabajadores puedan tener acceso a la VPN desde cualquier otro lugar geográfico.



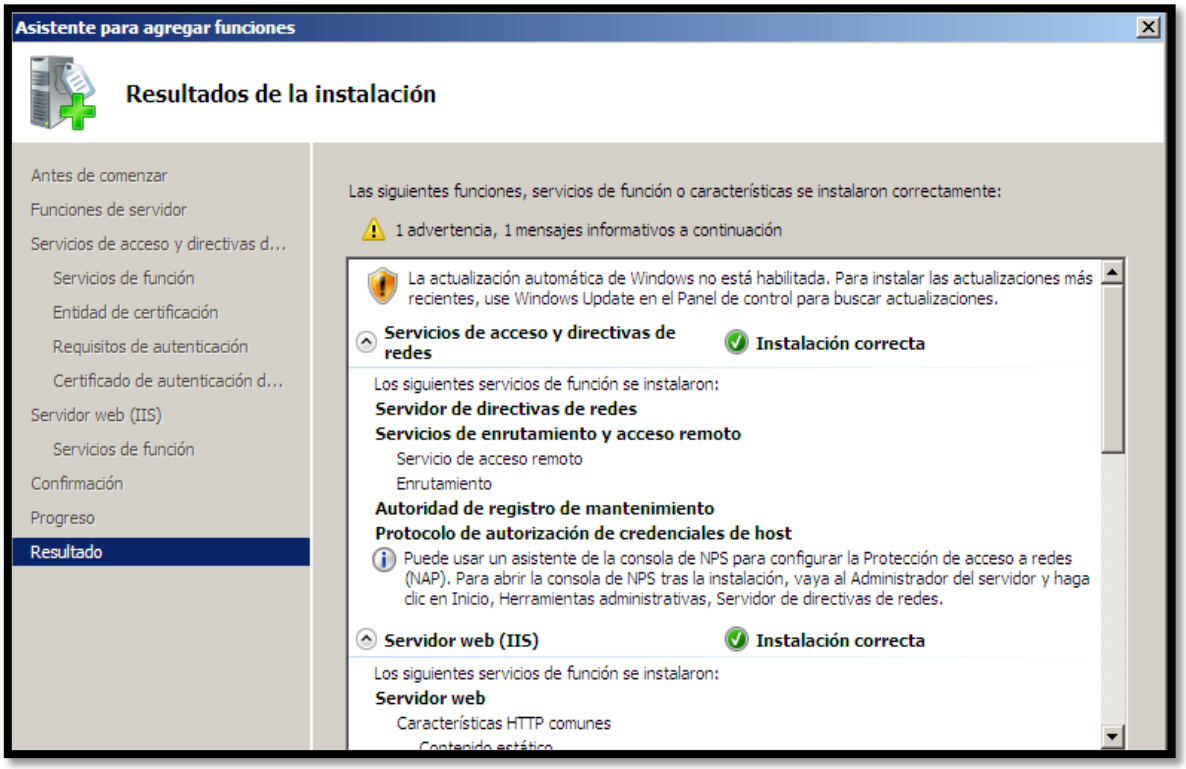
Img 29. Servicios de Función – Fuente (Elaboración Propia)

Se seleccionó la opción recomendada, ya que en pasos anteriores se creó el dominio “inei.com”.



Img 30. Requisitos de Autenticación para el Registro de Mantenimiento – Fuente (Elaboración Propia)

En la siguiente imagen de resultados del resumen de la instalación se podrá observar que además de instalarse los “Servicios de Acceso y Directivas de Redes”, también se instaló por defecto “Servidor web (IIS)” el cual permite compartir información entre usuarios de la intranet.



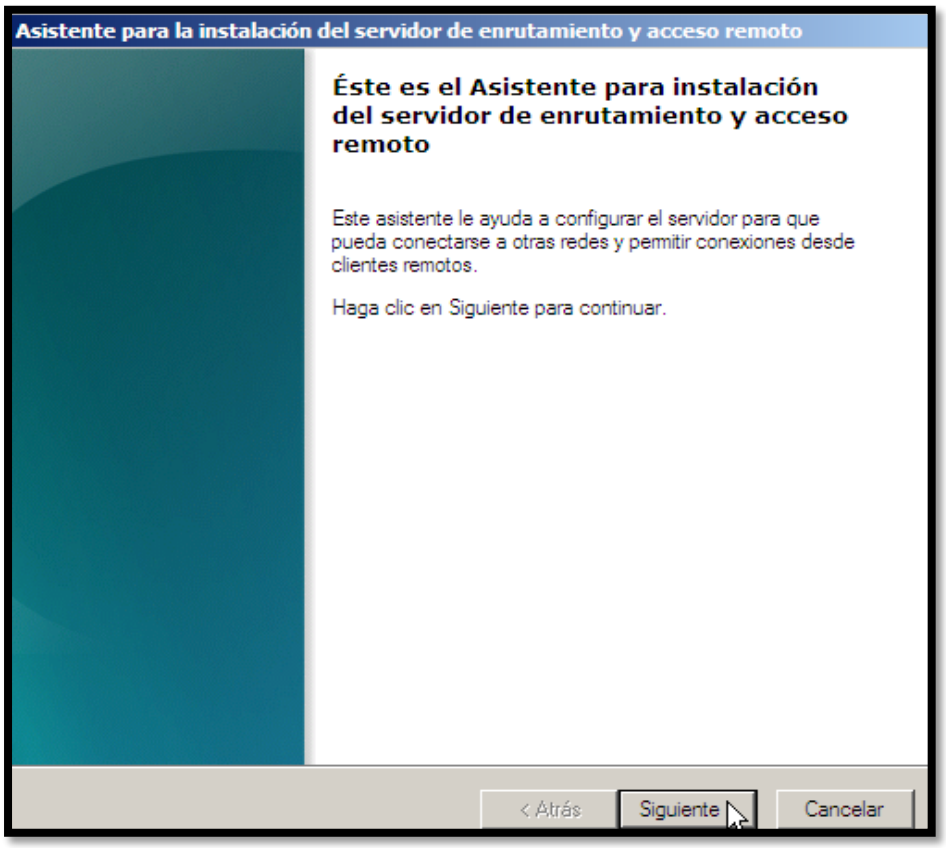
Img 31. Resultados de Instalación de los Servicios de Acceso y Directivas de Redes – Fuente (Elaboración Propia)

Para guardar las configuraciones anteriormente realizadas, se reinició el equipo.

5.1.6 ENRUTAMIENTO Y ACCESO REMOTO

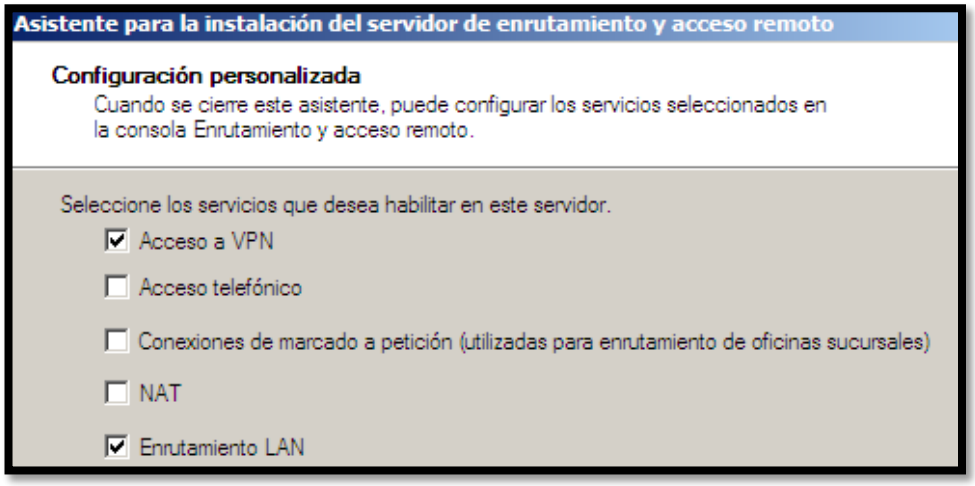
Para la instalación del servidor de enrutamiento se siguieron los siguientes pasos: Inicio, herramientas administrativas, enrutamiento y acceso remoto.

A continuación, ubicó el cursor sobre el nombre del servidor y se eligió la opción "Configurar y Habilitar Enrutamiento y Acceso remoto", es así como se inició con el proceso de la instalación.



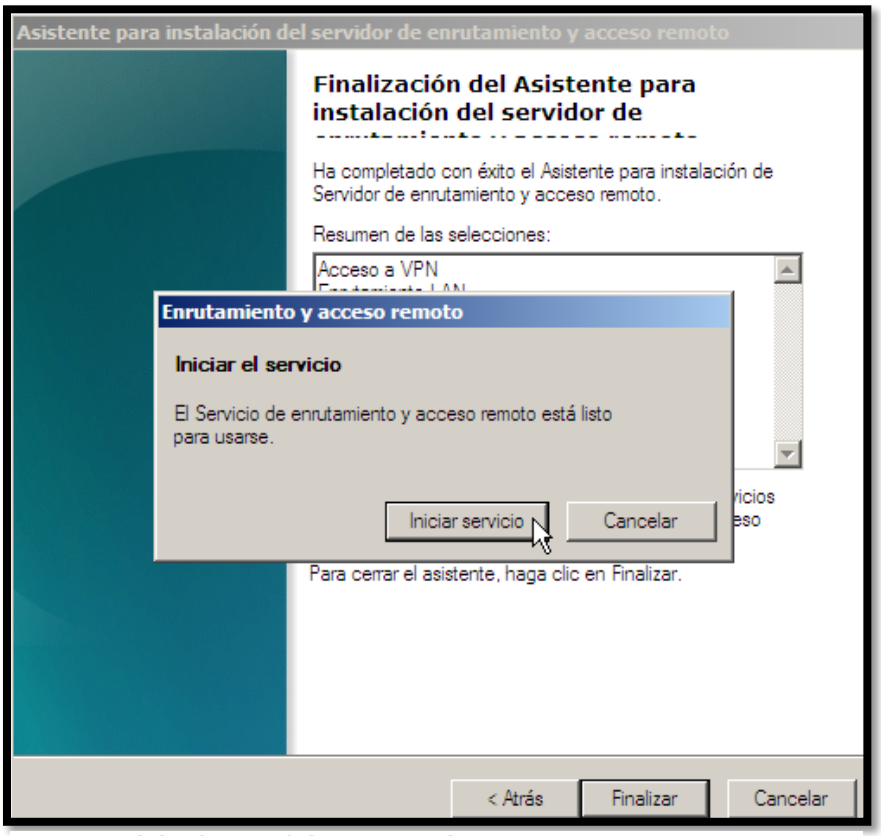
Img 32. Asistente para la Instalación del Servidor de Enrutamiento y Acceso Remoto – Fuente (Elaboración Propia)

Se seleccionó la opción "Personalizada" y la opción "Acceso a VPN" Y "Enrutamiento LAN".



Img 33. Ventana de Configuración de Acceso VPN y Enrutamiento LAN – Fuente (Elaboración Propia)

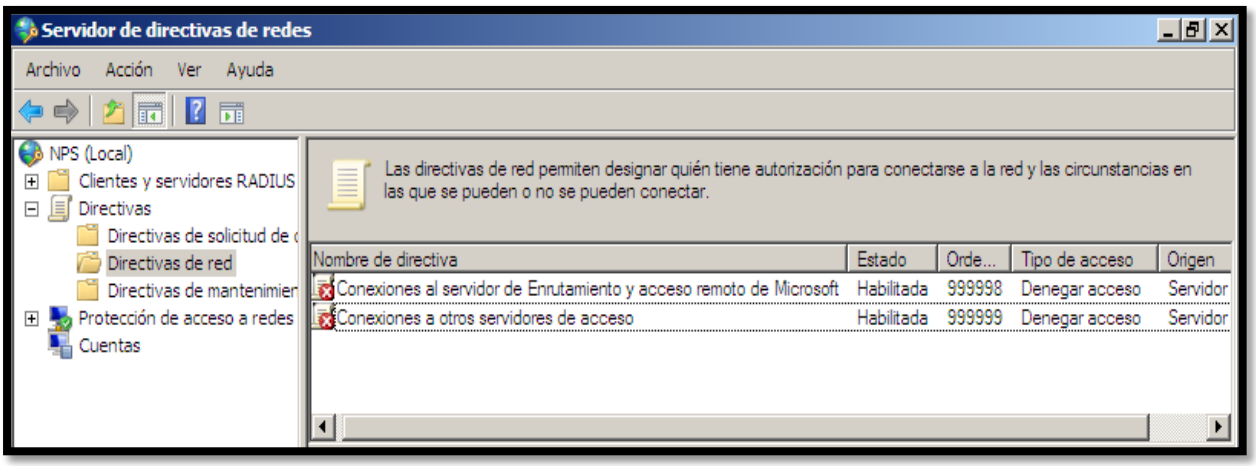
Una vez que el Asistente haya culminado con el proceso de instalación se eleigió la opcion “finalizar” seguido de “Iniciar el Servicio”.



Img 34. Inicio de Servicio Enrutamiento y Acceso Remoto – Fuente (Elaboración Propia)

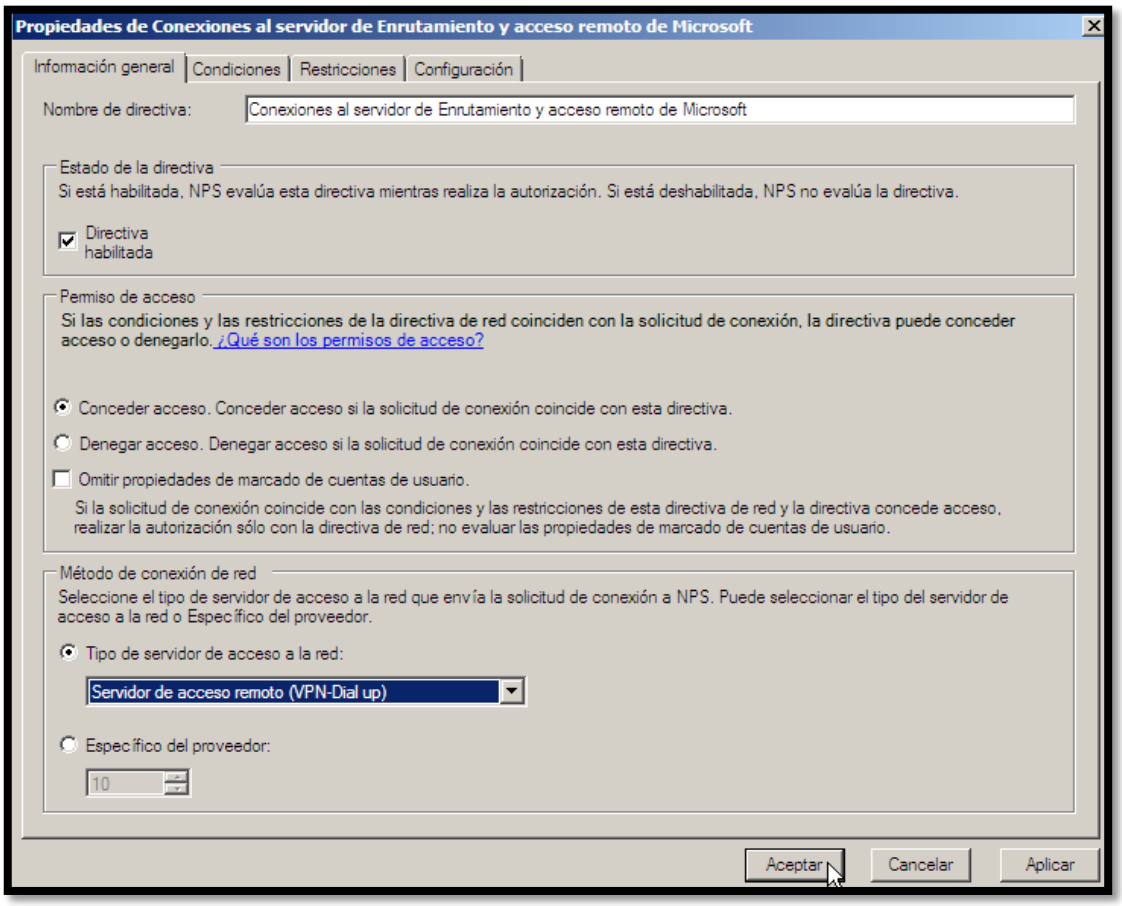
Finalmente para concluir con la configuración del Servidor VPN se habilitaron las directivas de red en “Servidor de Directivas de Redes”, para ello se debieron seguir los pasos: Inicio, herramientas administrativas, servidor de directivas de redes.

Una vez accedido, desdoblar la opción de “Directivas” y pulsar sobre la opción de “Directivas de Red”.



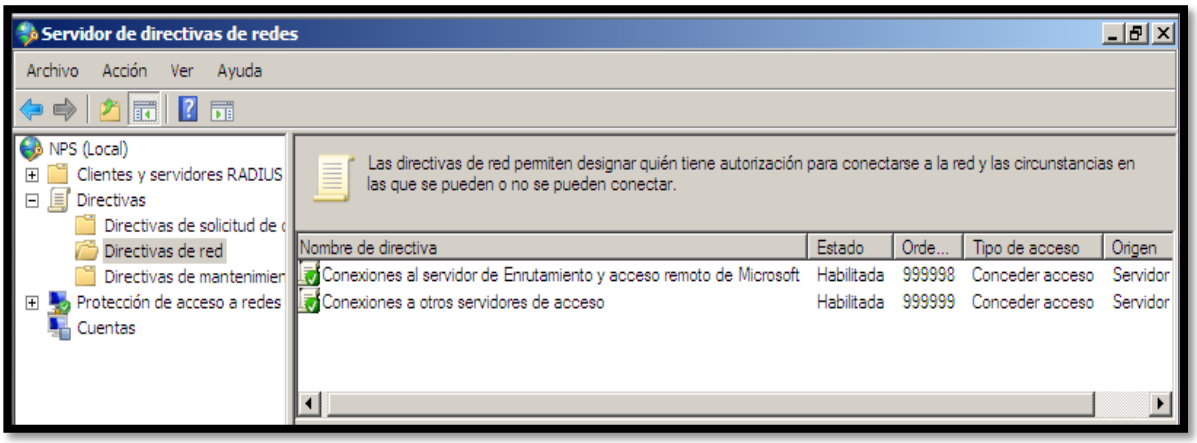
Img 35. Servidor de Directivas de Redes - Directivas Denegadas– Fuente (Elaboración Propia)

Para habilitar ambas directivas que se encuentran en “acceso denegado”, se seleccionó la primera directiva, a continuación apareció la siguiente ventana.



Img 36. Propiedades de conexión para Conceder Acceso a las Directivas de red – Fuente (Elaboración Propia)

Una vez realizado estos cambios en la siguiente imagen se podrá observar que las directivas ya fueron habilitadas.

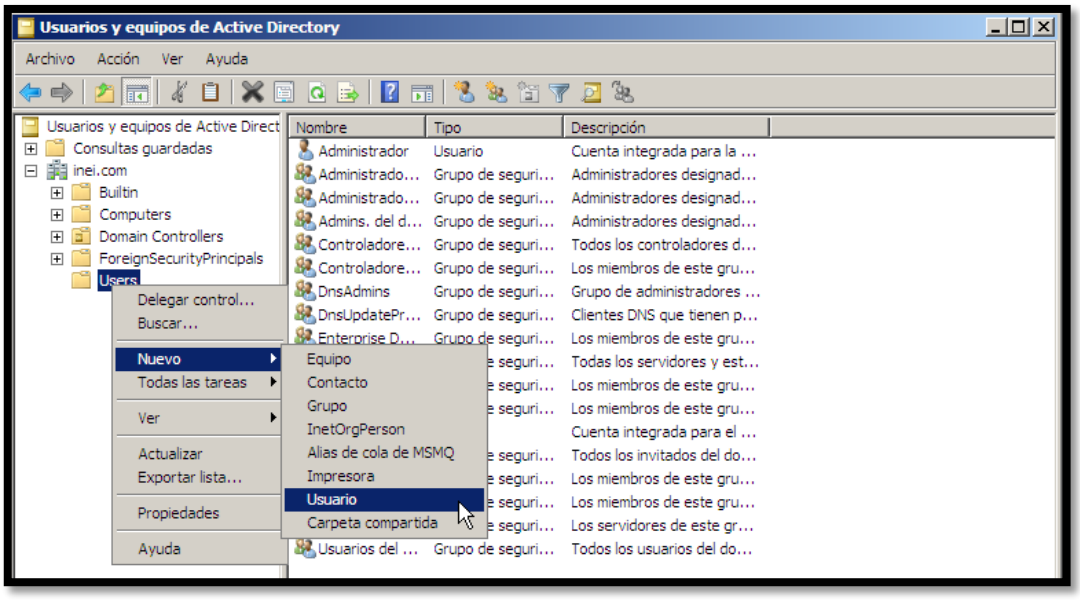


Img 37. Servidor de Directivas de Redes - Directivas Habilitadas – Fuente (Elaboración Propia)

Se reinició el servidor para guardar las configuraciones realizadas y de esta forma ya se culminó con la configuración del Servidor VPN.

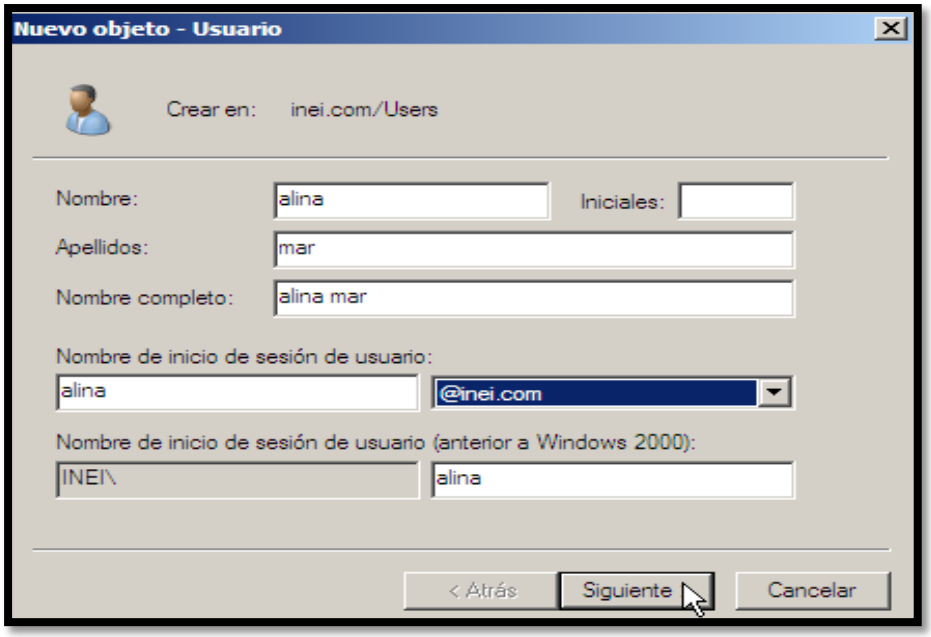
5.1.7 CREACIÓN DE CUENTAS DE CLIENTES VPN (PERSONAL ADMINISTRATIVO)

Para la creación de cada una de las cuentas de los usuarios, se siguieron los siguientes pasos: Inicio, herramientas administrativas, usuarios y equipos de active directory. Seleccionar el dominio “inei.com”, ubicar la carpeta “users”, (presionar anticlick), seleccionar nuevo, usuario.



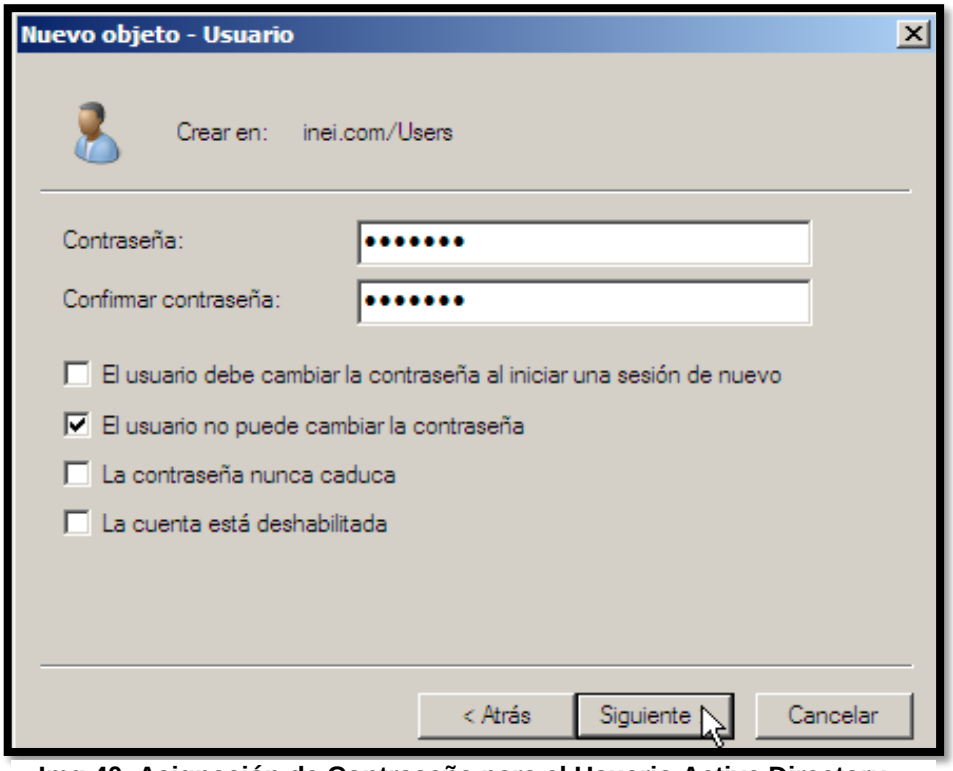
Img 38. Creación de Usuarios Active Directory – Fuente (Elaboración Propia)

Se procedió a la creación de las cuentas con los nombres de cada usuarios, si se tiene el caso de que existan dos trabajadores con el mismo nombre, se recomienda asignar a la cuenta el nombre y el primer apellido del usuario para evitar duplicidad de cuentas, pulsar siguiente.



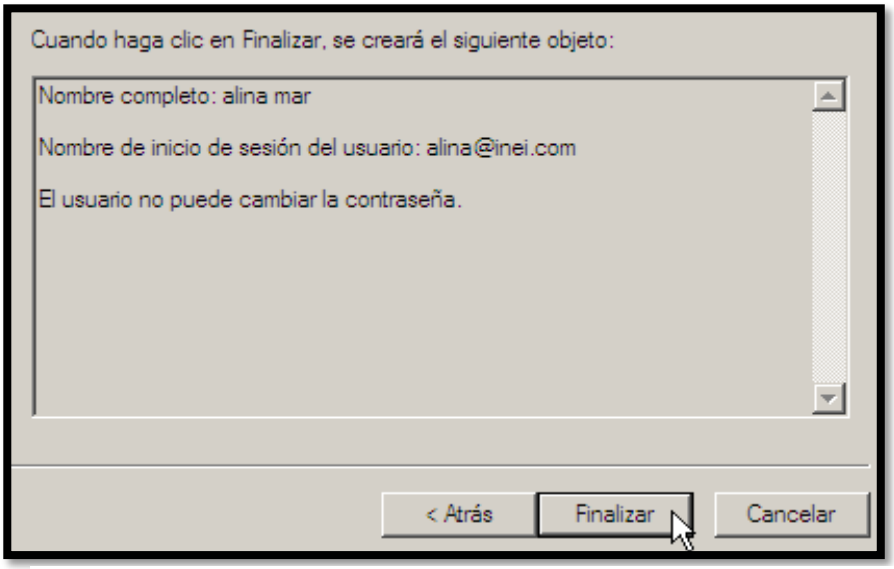
Img 39. Nuevo Usuario Active Directory – Fuente (Elaboración Propia)

Al momento de asignar la contraseña, se recomienda que sea entre una combinación de números y letras, seguidamente se seleccionó la opción “El usuario no puede cambiar la contraseña” ya que las cuentas de usuario sólo podrán ser administradas por el ingeniero de sistemas que se encuentra a cargo en la sede Lima y en la sede Cusco.



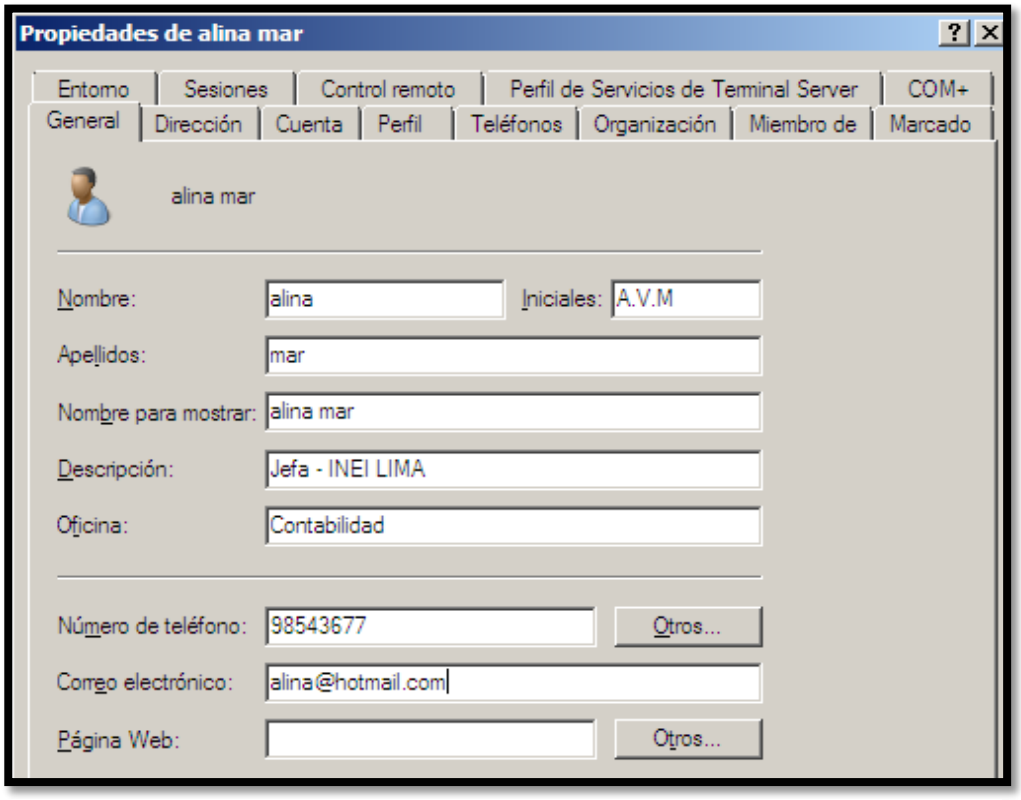
Img 40. Asignación de Contraseña para el Usuario Active Directory – Fuente (Elaboración Propia)

Para concluir con la configuración de la cuenta del usuario “alina mar” con nombre de inicio de sesión “alina@inei.com”, se seleccionó la opción “finalizar”.



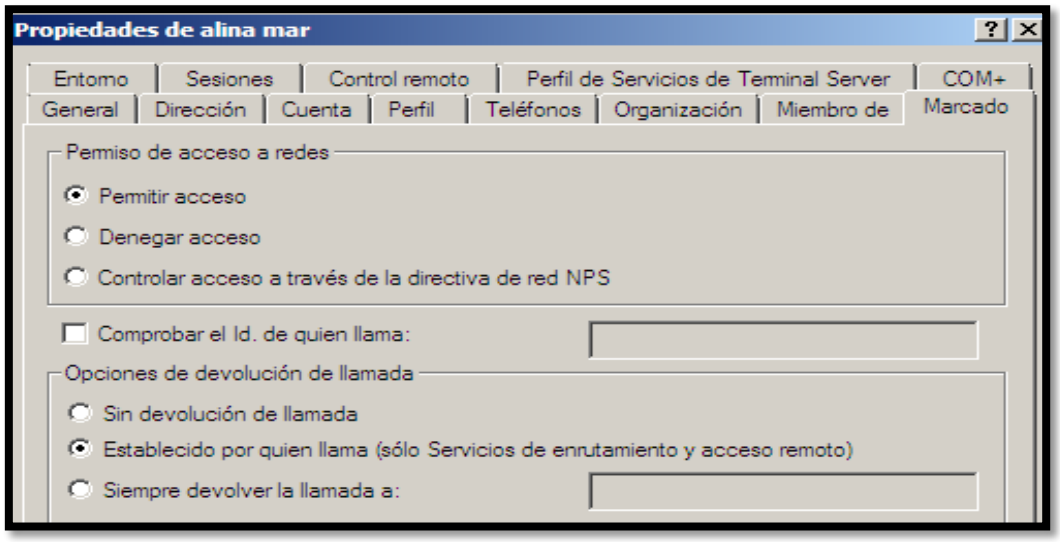
Img 41. Término de la Creación de Usuario de Active Directory – Fuente (Elaboración Propia)

Para detallar de forma específica cada uno de los campos en propiedades de usuario tales como: datos personales, sede al cual corresponde dicho usuario, etc. Se presionó anticlick sobre el usuario creado, en este caso: “alina” y se seleccionó la opción “propiedades”.



Img 42. Propiedades de Cuenta de Usuario – Fuente (Elaboración Propia)

Para el manejo de seguridad en cada una de las cuentas de usuarios, se ingresó a la opción “Propiedades”, “Marcado” y se seleccionó la opción “Permitir Acceso” y “Servicios de Acceso Remoto”, con el fin de administrar con mayor control cada cuenta.



Img 43. Permiso de Acceso a Redes – Fuente (Elaboración Propia)

5.1.8 CONEXIÓN DE CLIENTES VPN A LA INTRANET

Para la conexión de los usuarios al servidor VPN se utilizó el sistema operativo Windows 7, la instalación de dicho sistema operativo se muestra en el **ANEXO 6**.

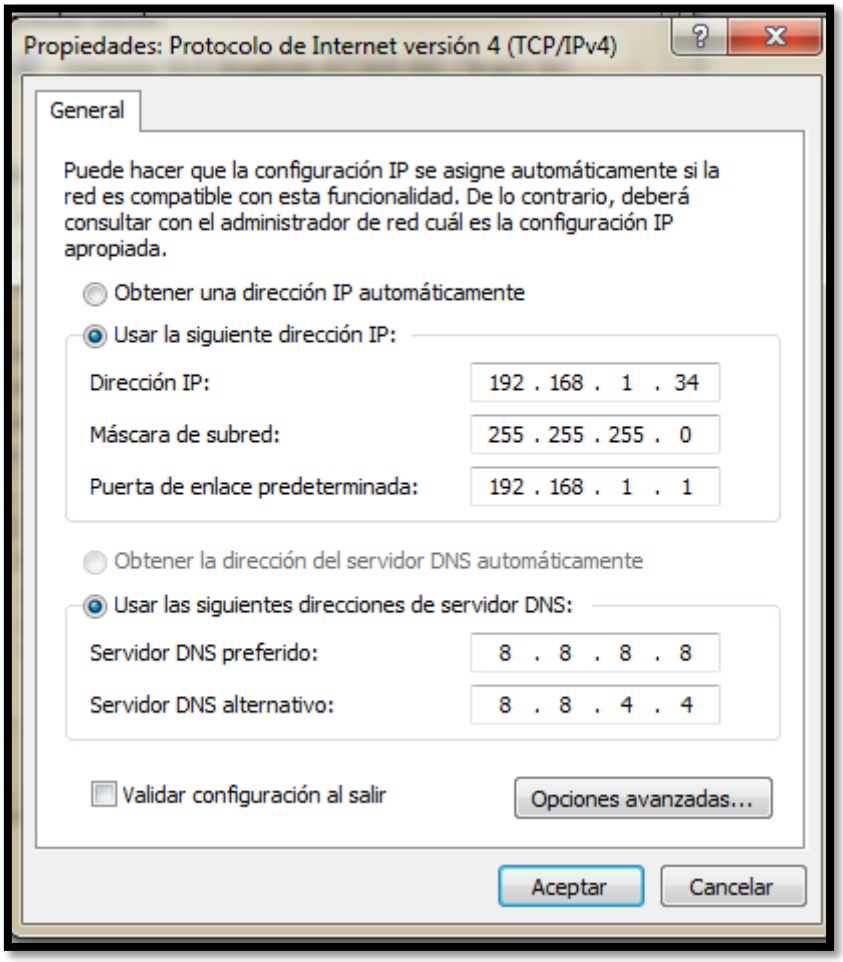
Para llevar a cabo la conexión de los clientes VPN a la intranet, se optó por utilizar Direcciones IP fijas, con la finalidad de tener un uso exclusivo de la dirección IP que se le asigne a cada PC.

Las direcciones IP para cada cliente VPN, fueron distribuidas de la siguiente manera:

ÁREAS	CANTIDAD DE MÁQUINAS DE ESCRITORIO POR ÁREA		DIRECCIONES IP	
	SEDE LIMA	SEDE CUSCO	SEDE LIMA	SEDE CUSCO
Jefatura	**1**	**1**	192.168.1.40	192.168.1.116
Oficina Técnica de Administración	**15**	**2**	**De:** 192.168.1.41 **A:** 192.168.1.56	**De:** 192.168.1.117 **A:** 192.168.1.118
Oficina Técnica de Informática	**18**	**1**	**De:** 192.168.1.57 **A:** 192.168.1.75	192.168.1.119
Oficina Técnica de Estadísticas Departamentales	**11**	**2**	**De:** 192.168.1.76 **A:** 192.168.1.87	**De:** 192.168.1.120 **A:** 192.168.1.121
Escuela Nacional de Estadística e Informática	**4**	**1**	**De:** 192.168.1.88 **A:** 192.168.1.92	192.168.1.122
Dirección Técnica de Indicadores Económicos	**11**	**2**	**De:** 192.168.1.93 **A:** 192.168.1.104	**De:** 192.168.1.123 **A:** 192.168.1.124
Dirección Nacional de Censos y Encuestas	**9**	**3**	**De:** 192.168.1.105 **A:** 192.168.1.114	**De:** 192.168.1.125 **A:** 192.168.1.127
Secretaría General	**1**	**1**	192.168.1.115	192.168.1.128

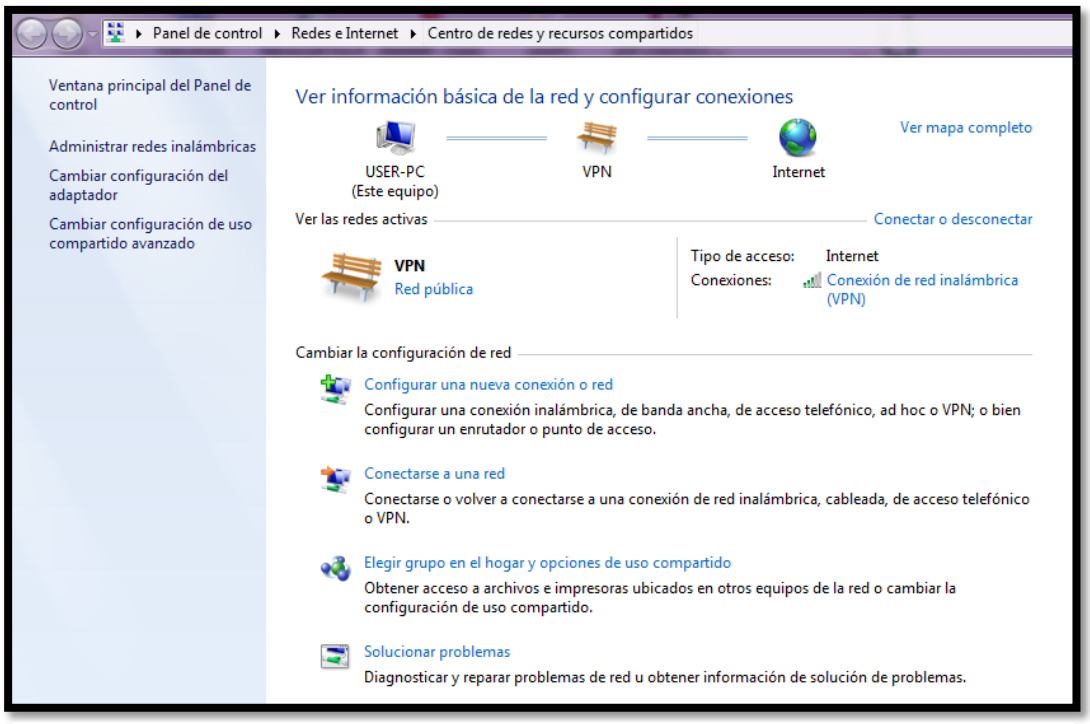
Tabla 23. Distribución de Direcciones IP para Clientes VPN – Fuente (Elaboración Propia)

Para el caso del cliente anteriormente creado “alina” en Usuarios Active Directory, se le asignó la siguiente dirección IP: **192.168.1.34**, para establecer dicha dirección IP se siguieron los siguientes pasos: presionar anticlick en mis sitios de red, propiedades, conexión de área local (presionar anticlick), propiedades, aceptar.



Img 44. Asignación de Dirección IP al cliente VPN – Fuente (Elaboración Propia)

Una vez asignada la dirección IP, se dirigió a propiedades de red y se seleccionó la opción “Configurar una Nueva Conexión”.

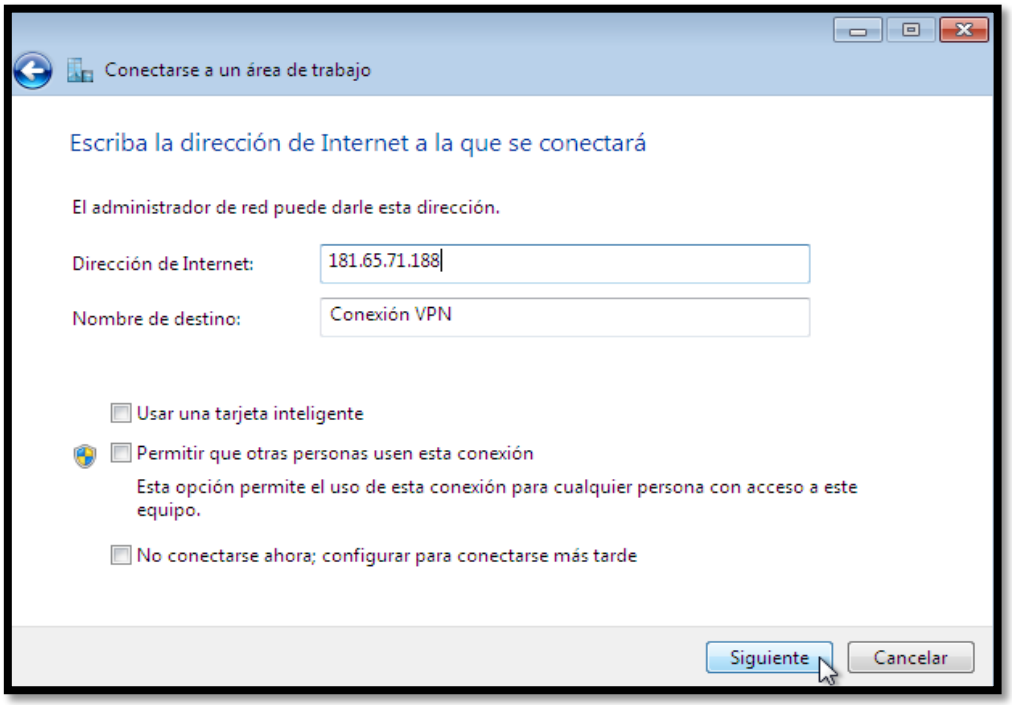


Img 45. Configuración para una Nueva Conexión – Fuente (Elaboración Propia)

Se seleccionó la opción “Conectarse a un area de trabajo” y seguidamente la opción “Usar mi conexión a internet (VPN)”.

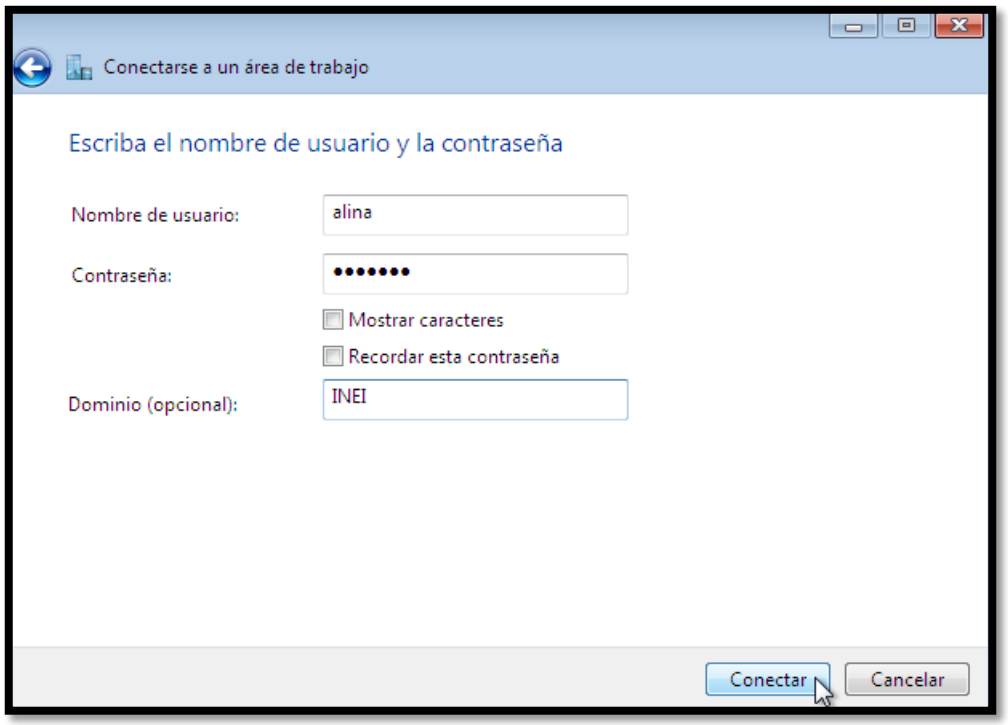
Img 46. Tipo de Conexión para Acceder a la VPN – Fuente (Elaboración Propia)

Para establecer la conexión con el servidor VPN, en la siguiente ventana se asignó la Dirección IP Pública del equipo donde se encuentra configurado el servidor VPN. Tener en cuenta que la IP pública cambiara todos los días a menos que la institución del INEI solicite a telefónica una IP pública fija.



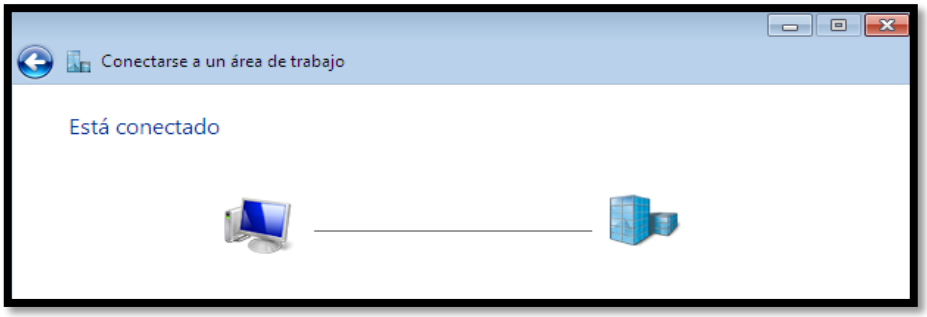
Img 47. Conexión al Servidor VPN – Fuente (Elaboración Propia)

Para establecer la conexión del cliente VPN con el servidor, se ingresó el nombre de usuario, la contraseña y el nombre del dominio (INEI).



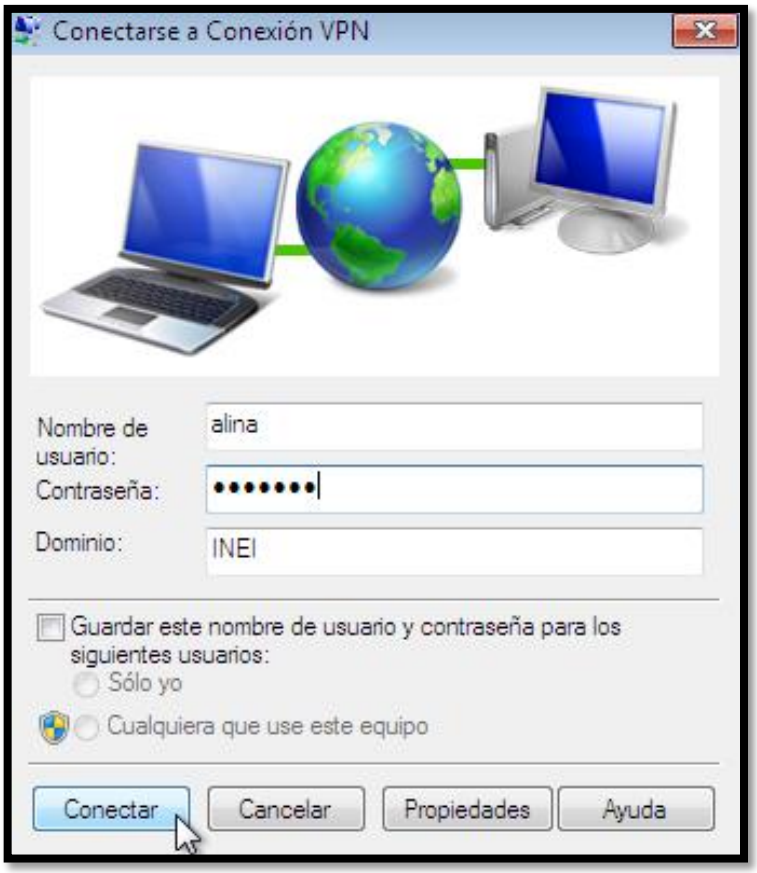
Img 48. Nombre de Usuario y Contraseña – Fuente (Elaboración Propia)

Finalmente se esperó a que se valide el nombre de usuario y la contraseña asignada.



Img 49. Conexión Satisfactoria Cliente - Servidor VPN – Fuente (Elaboración Propia)

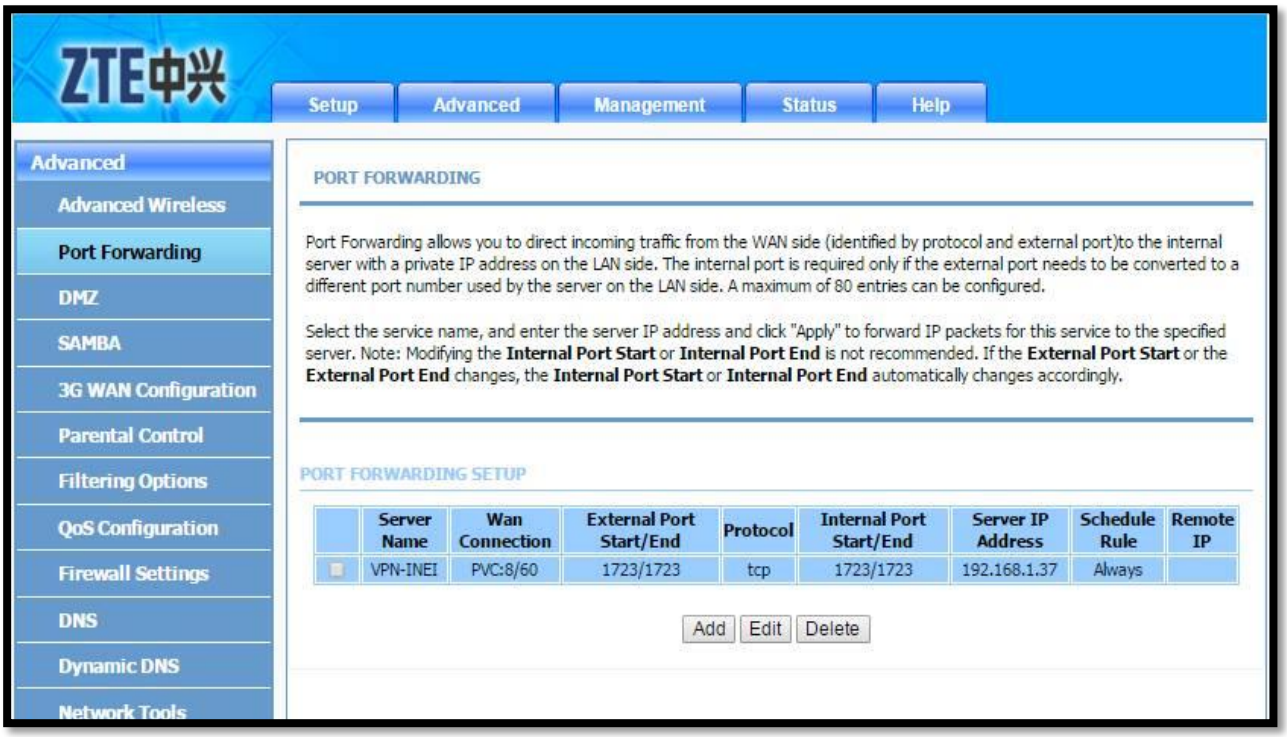
Una vez terminada la configuración, para poder volverse a conectar a la intranet apareció la siguiente ventanilla, lista para ingresar los la cuenta del cliente VPN.



Img 50. Autenticación de Usuario – Fuente (Elaboración Propia)

5.1.9 HABILITAR PUERTO VPN

Una vez terminado el proceso de configuración se procedió a configurar el protocolo TCP, para ello se habilitó el puerto VPN - TCP 1723, indicando la dirección IP de donde se encuentra configurado el servidor, en este caso la IP: 192.168.1.37, con la finalidad de establecer conexión de los clientes con el servidor VPN.



Img 51. Habilitar el puerto VPN – Fuente (Elaboración Propia)

A su vez al momento de habilitar el puerto, se tuvo la opción de poder decidir por cuánto tiempo se desea que el servidor este activo, ya sea por horas o días específicos, en este caso se configuró en el router, que el servidor este siempre "activo" ya que el personal en algunas áreas administrativas tales como: la escuela ENEI laboran también los días domingos.

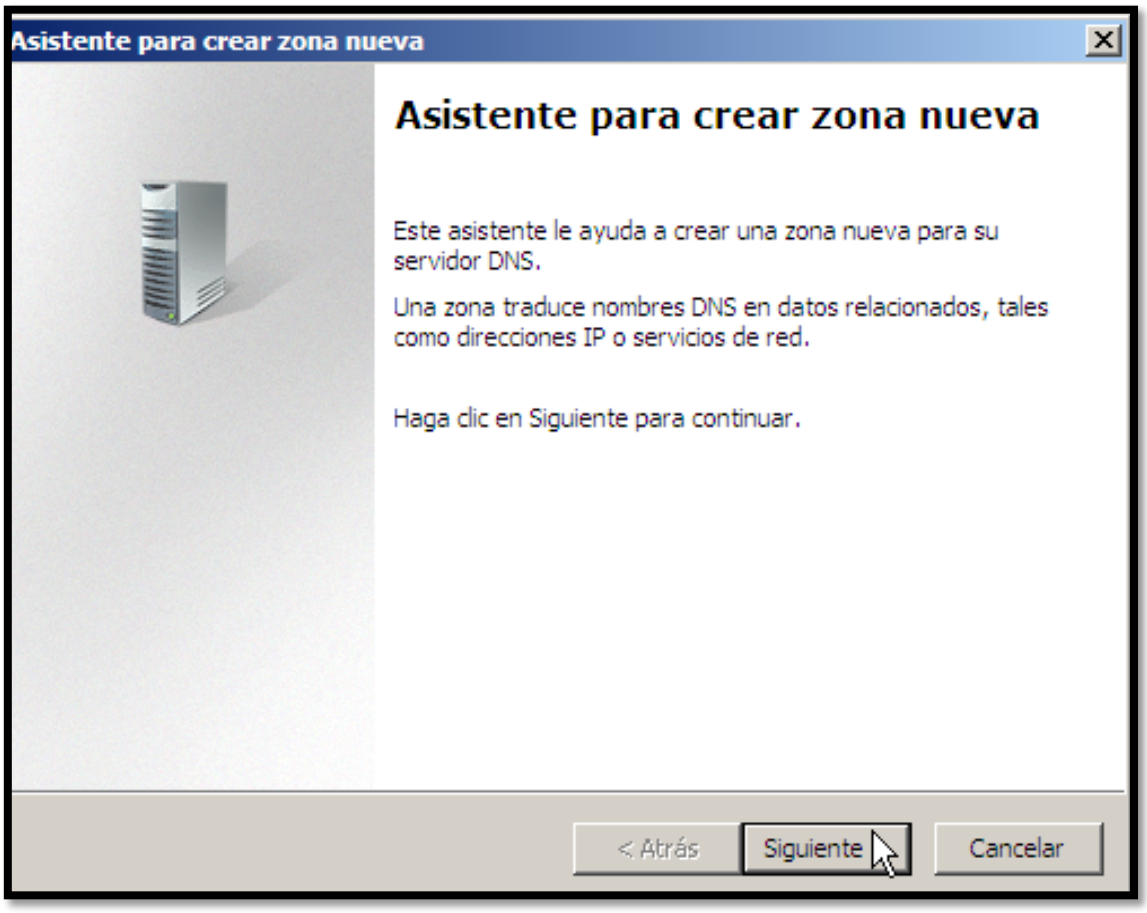
5.2 CONFIGURACIÓN SERVIDOR DE CORREOS

Como anteriormente ya se configuraron los Servicios de Dominio de Active Directory, se procedió a configurar el DNS, con la finalidad de hacer uso del dominio “inei.com” anteriormente configurado.

5.2.1 CREACIÓN DE ZONA NUEVA

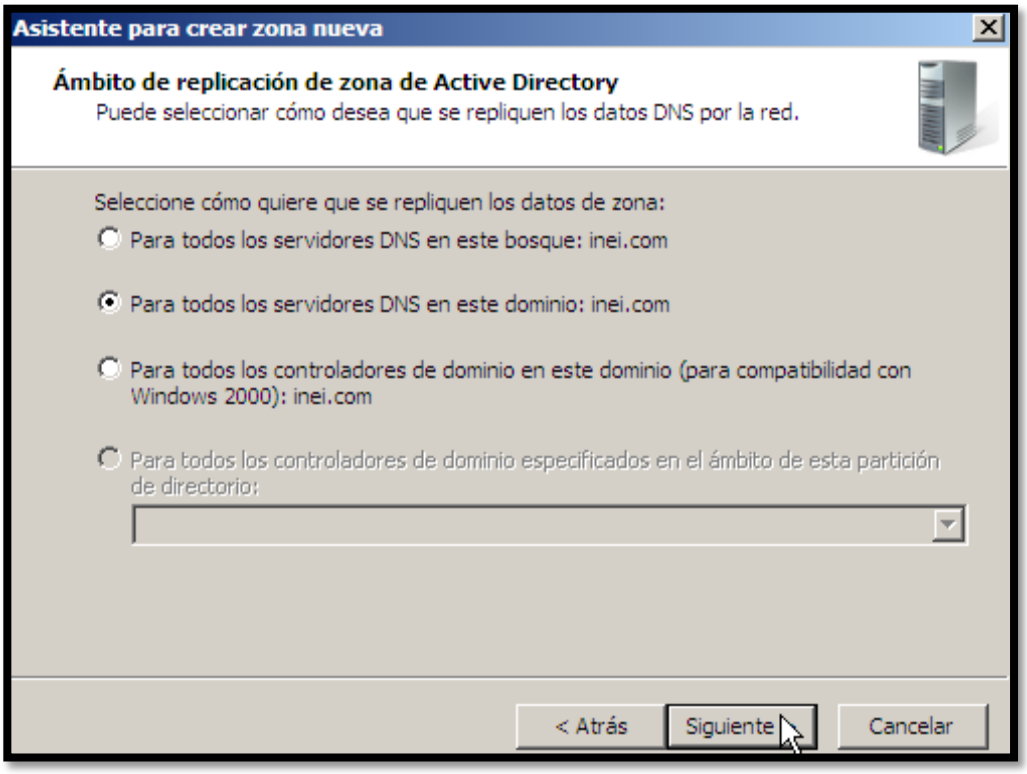
La creación de una zona nueva, se realizó con la finalidad de que el sistema de nombres de dominios DNS, permitirá a un espacio de nombre DNS ser dividido en zonas, en este caso cada zona se encargó de almacenar toda la información del dominio “inei.com”.

Para iniciar con la configuración del servidor DNS y con la creación de una nueva zona de búsqueda inversa, se siguieron los siguientes pasos: Inicio, herramientas administrativas, dns, zona de búsqueda inversa, zona nueva.



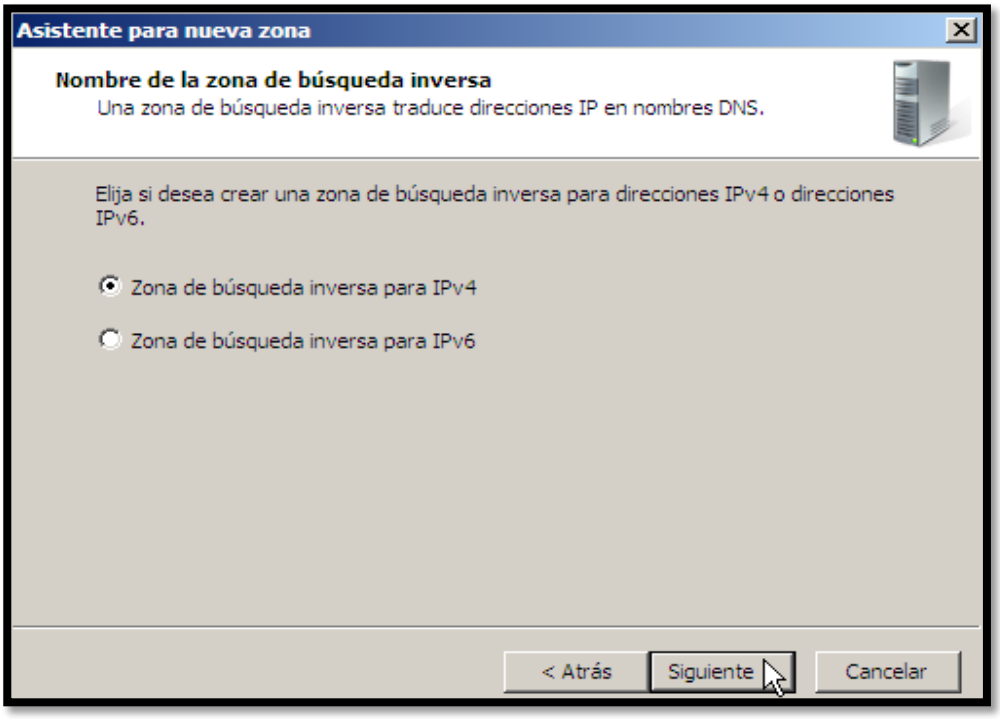
Img 52. Asistente para la Creación de una Nueva Zona – Fuente (Elaboración Propia)

Se seleccionó la opción “Para todos los servidores DNS en este domino: inei.com”, ya que lo que se configuro anteriormente es un dominio.



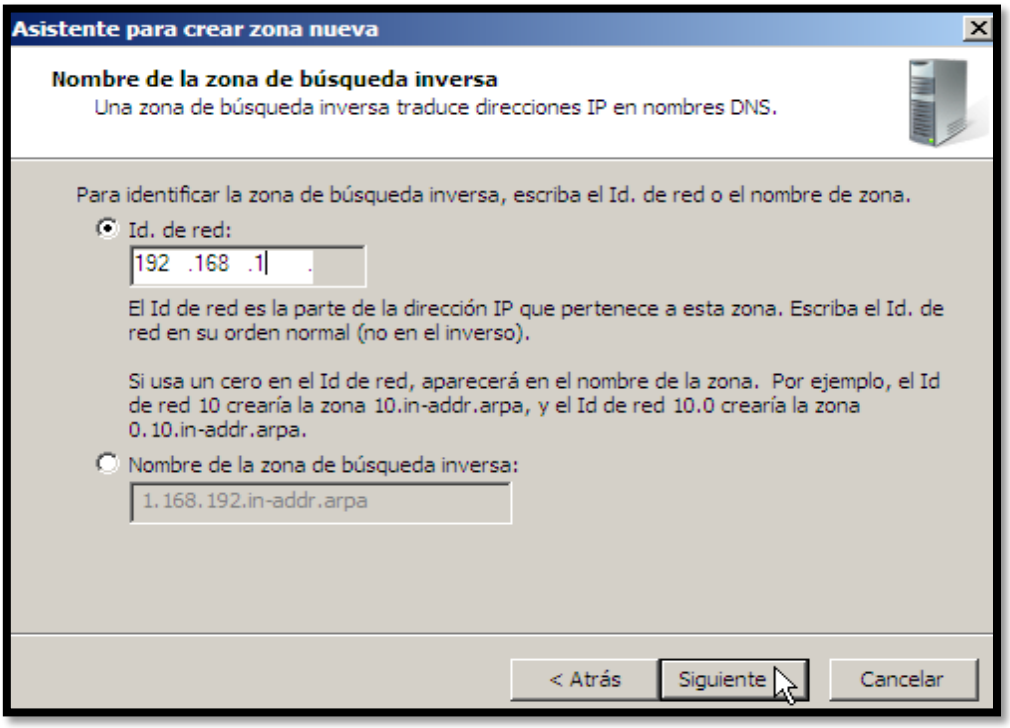
Img 53. Ámbito de Replicación de Zona de Active Directory – Fuente (Elaboración Propia)

Se seleccionó “Zona Principal” y el tipo de zona elegida fue el la de búsqueda inversa para IPv4, debido a que con las IPv4.



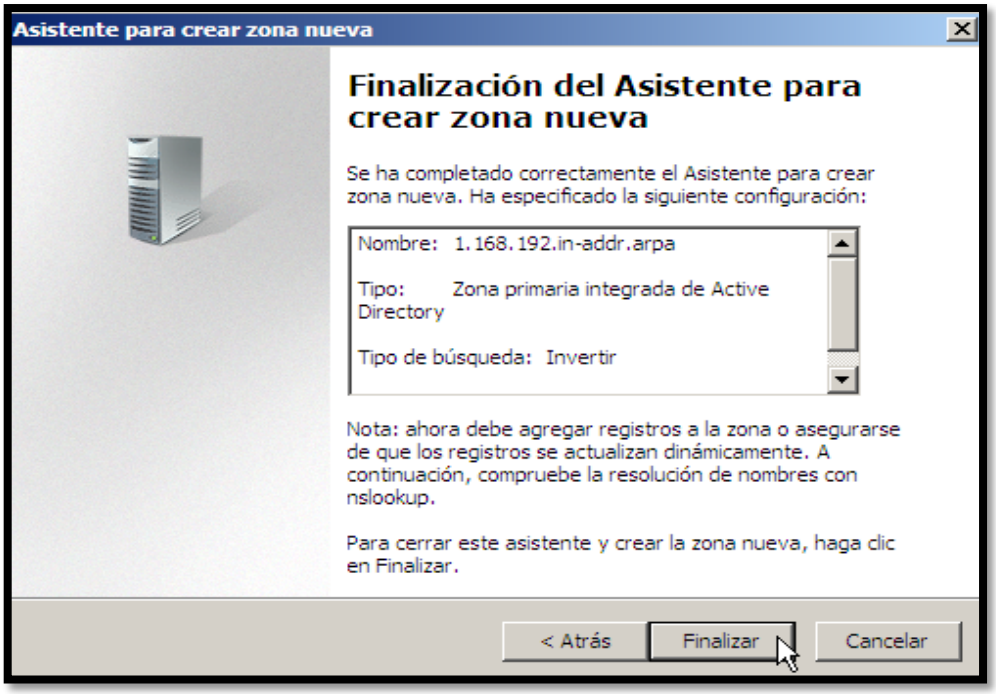
Img 54. Tipo de Zona – Fuente (Elaboración Propia)

Se escribió el Id. de red en su forma normal para la creación de dicha zona, en este caso fue el 192.168.1 y el nombre de la zona de búsqueda inversa tomó el nombre de: 1.192.168.in-addr.arpa.



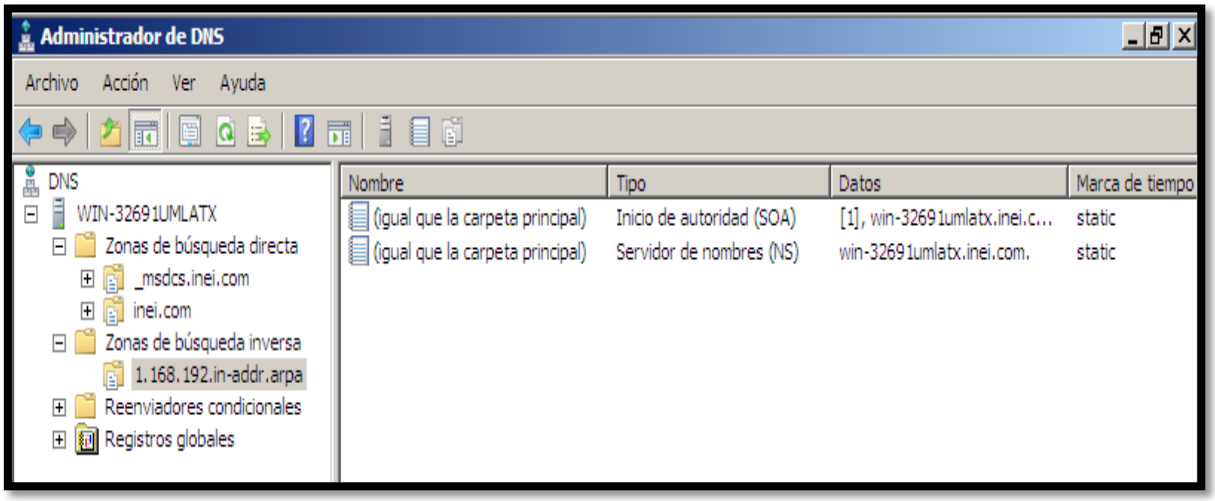
Img 55. Nombre de la Zona de Búsqueda Inversa – Fuente (Elaboración Propia)

Se seleccionó la actualización "dinámica segura" la cual esta como opción recomendada y pulsar en siguiente para concluir con la creación de la zona.



Img 56. Finalización del Asistente para Crear Zona Nueva – Fuente (Elaboración Propia)

Para verificar que la zona de búsqueda inversa se ha creado correctamente, se ingresó al administrador de DNS, realizando los siguientes pasos: inicio, herramientas administrativas, dns.



Img 57. Zona de Búsqueda Inversa Creada – Fuente (Elaboración Propia)

Una vez finalizado con la creación de la zona, se procedió a instalar el servidor web IIS, con la finalidad de que los clientes VPN puedan compartir información por medio de la intranet, para la instalación se siguió los siguientes pasos: Inicio, administrador del servidor (presionar anticlick), agregar funciones de servidor, seleccionar la opción “Servidor web IIS” y reiniciar el equipo para guardar las configuraciones realizadas.

5.2.2 INSTALACIÓN Y CONFIGURACIÓN DE EXCHANGE SERVER

Se consideró la instalación de Server Exchange como parte para la configuración del servidor de correos, debido a que Windows server 2008 no tiene incluido protocolo de red para correo electrónico POP3.

Para iniciar con la instalación de Server Exchange, primero tuvo que ejecutarse en modo administrador y automaticamente la instalacion inició apartir el paso 4: “instalación de Microsoft Exchange”.

Img 59. Instalación Exchange Server – Fuente (Elaboración Propia)

Se aceptó los términos del contrato de licencia, se vio por conveniente elegir la instalación típica ya que es la opción más completa.

Img 58. Tipo de Instalación Exchange Server 2010 – Fuente (Elaboración Propia)

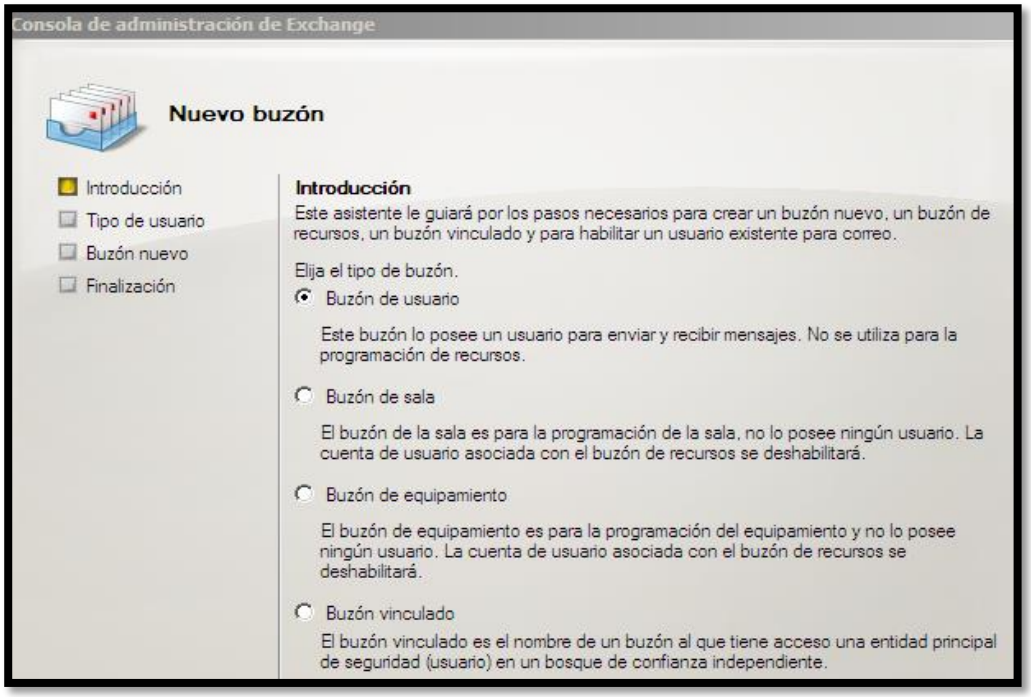
Se indicó el nombre de la organización, en este caso fue “INEI”.

Img 60. Nombre de la organización de Exchange – Fuente (Elaboración Propia)

Finalmente se esperó a que la instalación del server exchange haya finalizado.

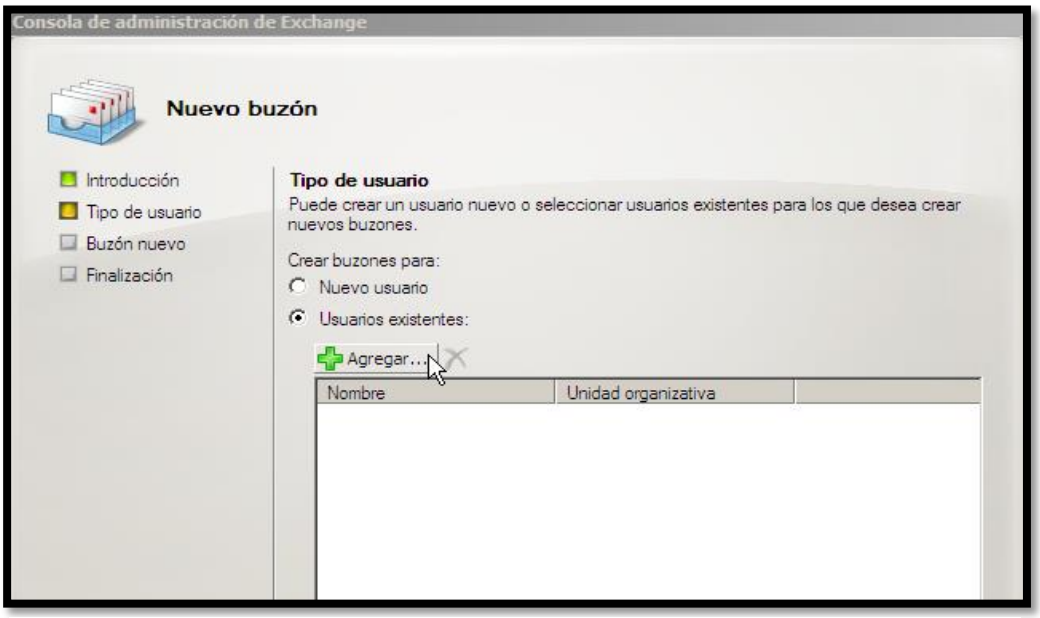
Img 61. Img. 54 Finalización de la Instalación de Exchange Server – Fuente (Elaboración Propia)

Una vez culminada la instalación, se reinició el equipo para guardar los cambios efectuados, seguidamente se procedió a la creación de un nuevo buzón el cual se encarga de albergar las cuentas de los destinatarios, para ello se siguió los siguientes pasos: abrir la consola de administración de Exchange, buzón (anticlick), buzón nuevo.



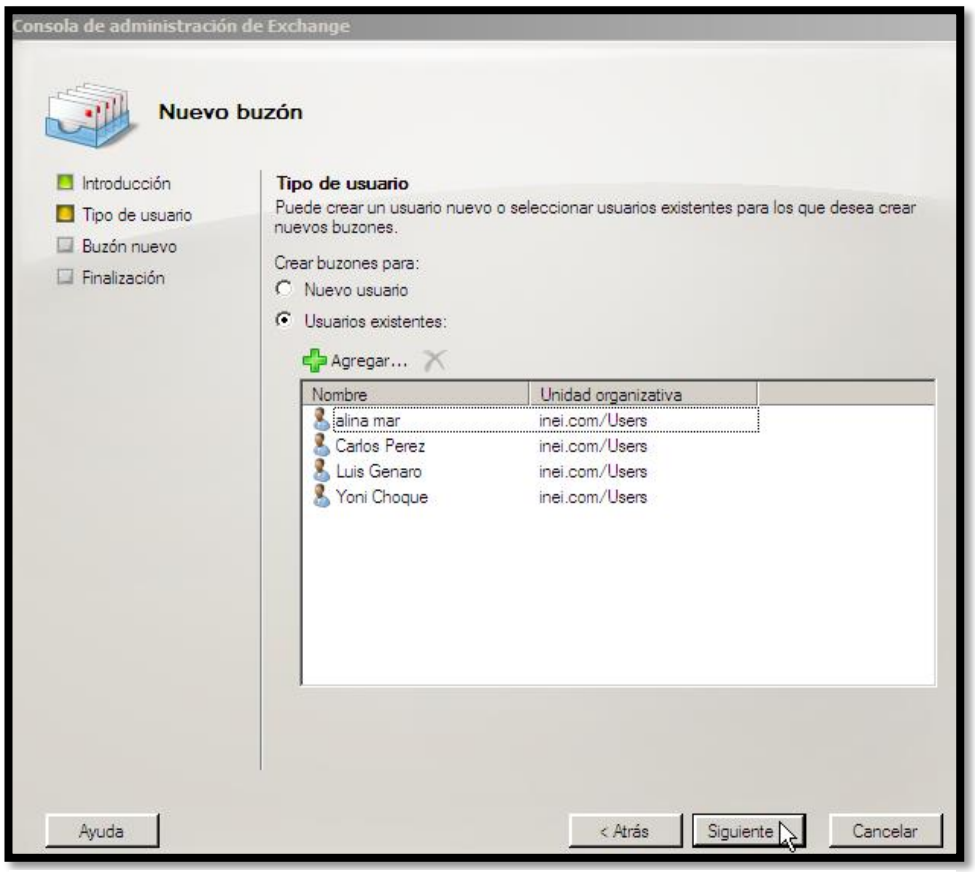
Img 62. Creación de Buzón de Usuario – Fuente (Elaboración Propia)

El tipo de usuario que se vio por conveniente elegir fue “Usuarios Existentes” ya que anteriormente para la creación de la intranet se crearon las cuentas con los nombres de los trabajadores.



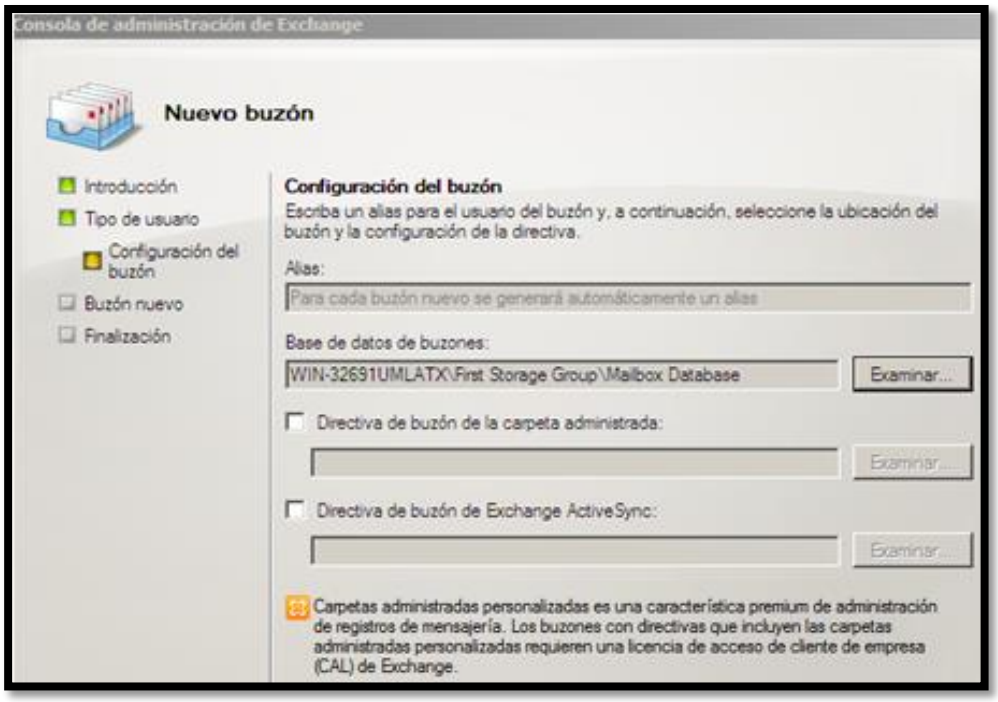
Img 63. Selección tipo de usuario para la creación de un Nuevo Buzón – Fuente (Elaboración Propia)

Se seleccionó y agrego a los usuarios anteriormente configurados.



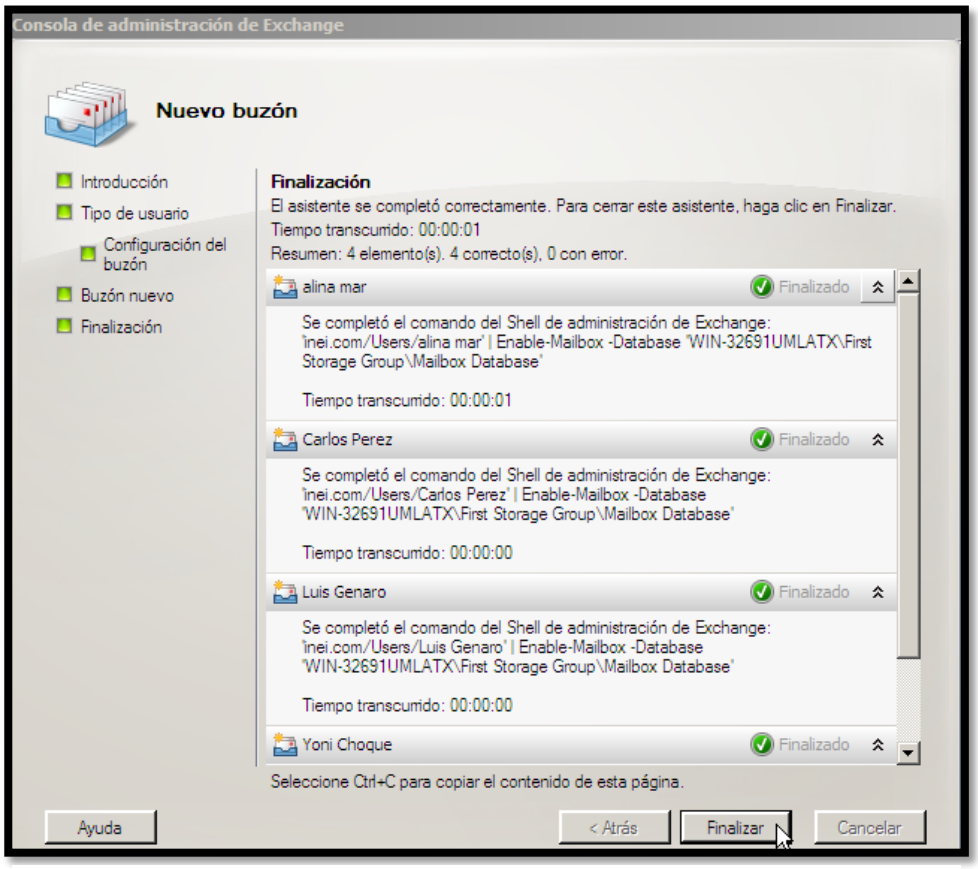
Img 64. Selección de usuarios a agregar – Fuente (Elaboración Propia)

Se ubicó el nombre de la base de datos que esta por defecto en la configuración del buzón de Exchange server, para el almacenamiento de los buzones de cada usuario.



Img 65. Base de Datos de Buzones – Fuente (Elaboración Propia)

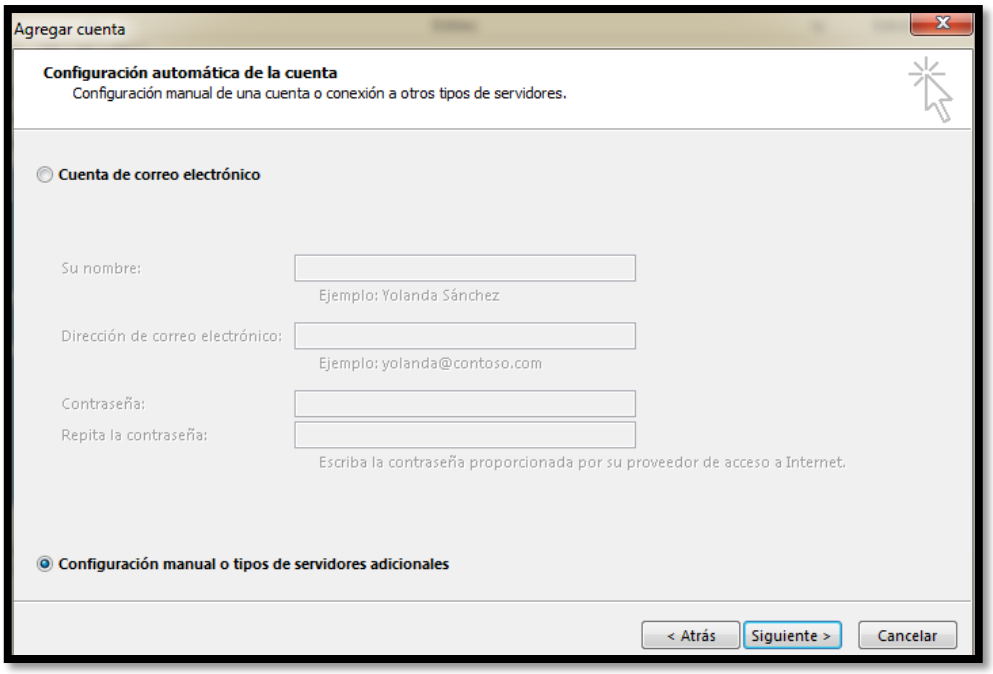
Finalmente se esperó a que se culmine con la creación de cada buzón para los usuarios seleccionados.



Img 66. Creación de Buzones de Correo – Fuente (Elaboración Propia)

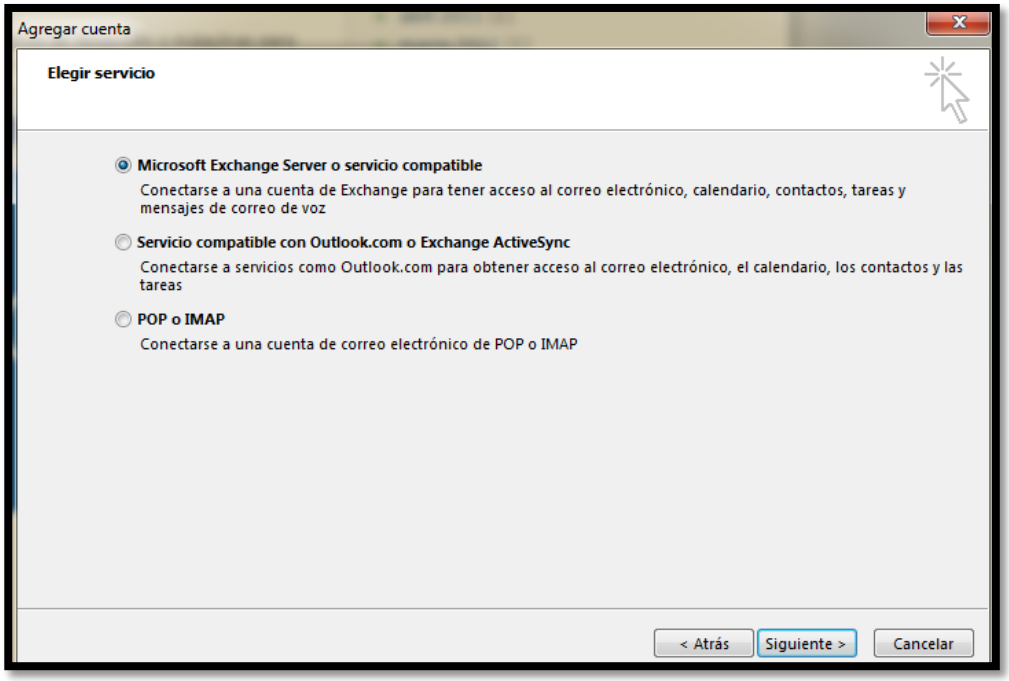
5.2.3 CREACIÓN DE CUENTAS EN OUTLOOK

Una vez finalizado la instalación y configuración de los buzones de correo para cada uno de los trabajadores autorizados de las sedes Lima – Cusco del INEI, se procedió a crear las cuentas en outlook (correo de escritorio), los pasos que se siguieron para la creación de dichas cuentas fueron outlook fueron: Abrir el servicio de correo electrónico y seleccionar la opción “Configuración Manual”.



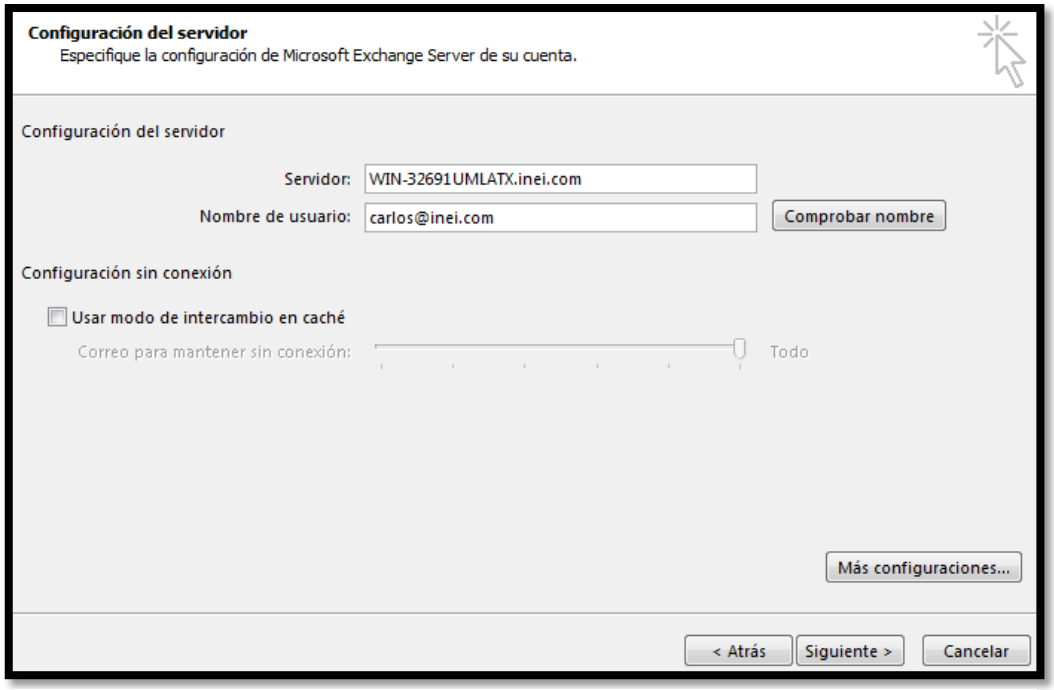
Img 68. Configuración Manual para la Cuenta en Outlook – Fuente (Elaboración Propia)

El tipo de servicio que se eligió fue de Microsoft Exchange, debido a que en él se encuentra configuradas las cuentas de correo.



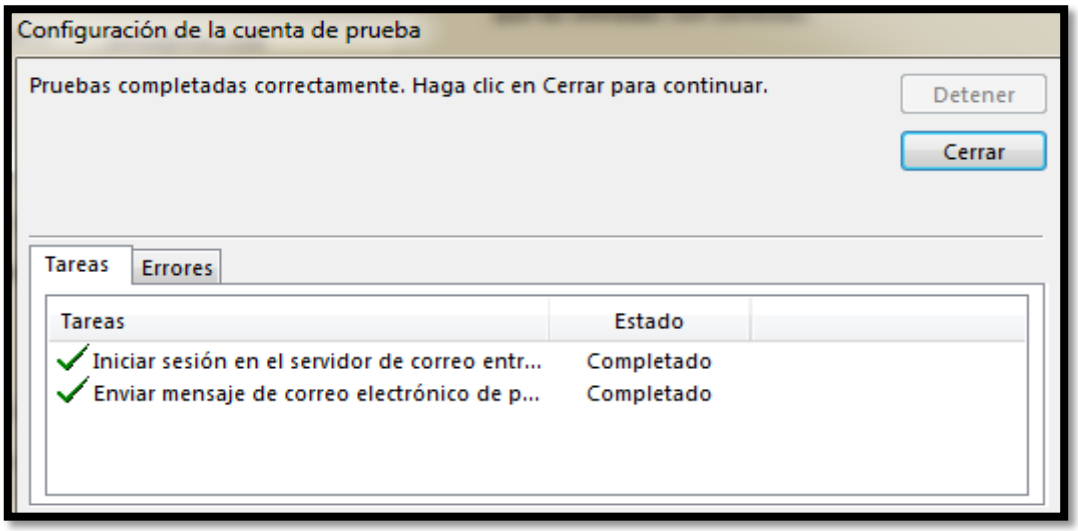
Img 67. Tipo de Servicio para la Creación de la Cuenta de Correo – Fuente (Elaboración Propia)

Para la creación de la cuenta “carlos@inei.com y demás usuarios en outlook, se indicó el nombre del servidor y el nombre del usuario anteriormente citado en el Exchange Server, en este caso para el usuario “carlos”.



Img 69. Configuración de Microsoft Exchange de la Cuenta – Fuente (Elaboración Propia)

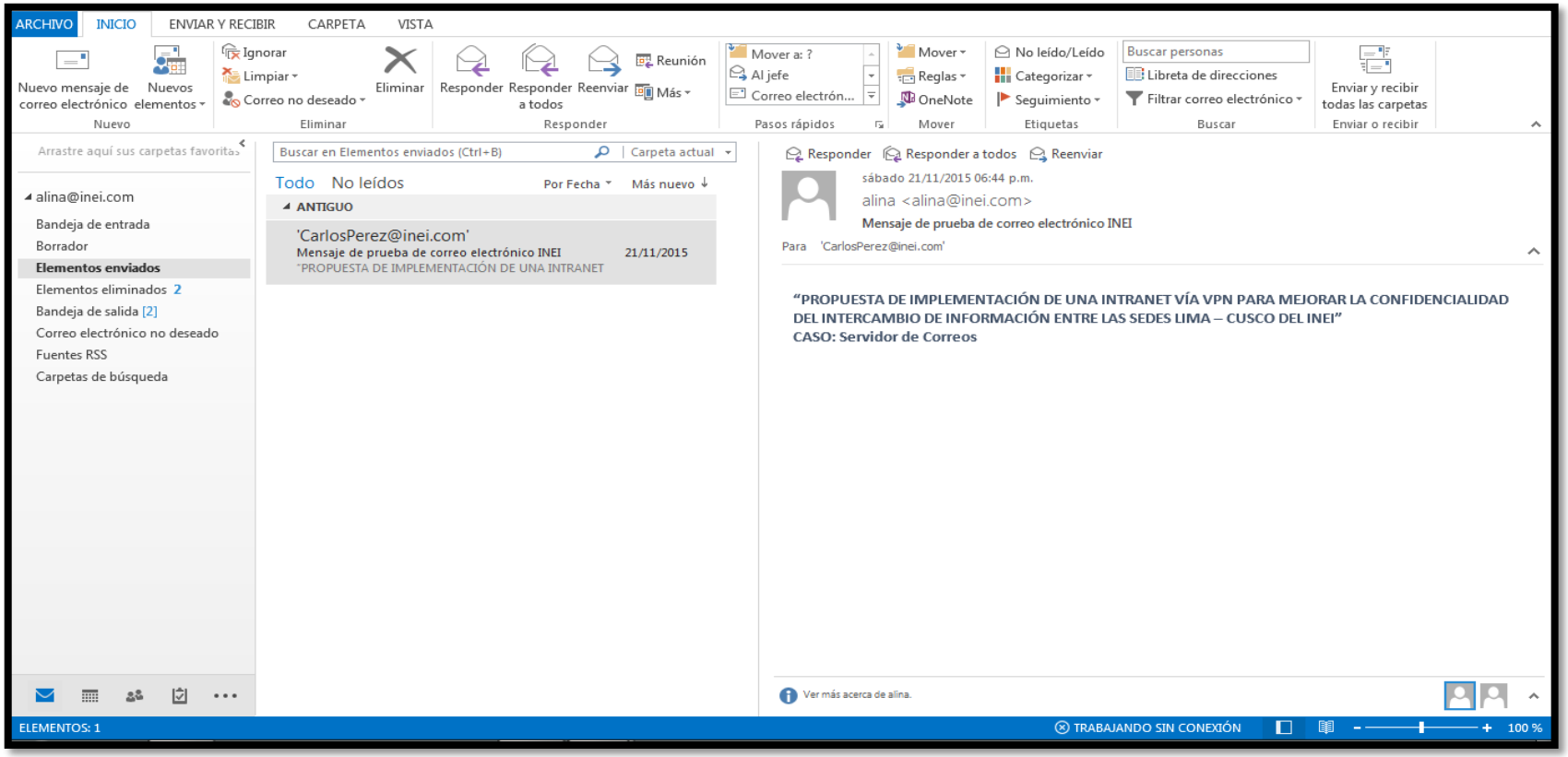
Finalmente para comprobar la conexión de una determinada cuenta con el Exchange Server, se pulsó sobre la opción “comprobar nombre”, y a continuación se observa que la conexión ha sido exitosa.



Img 70. Configuración de la Cuenta de Prueba – Fuente (Elaboración Propia)

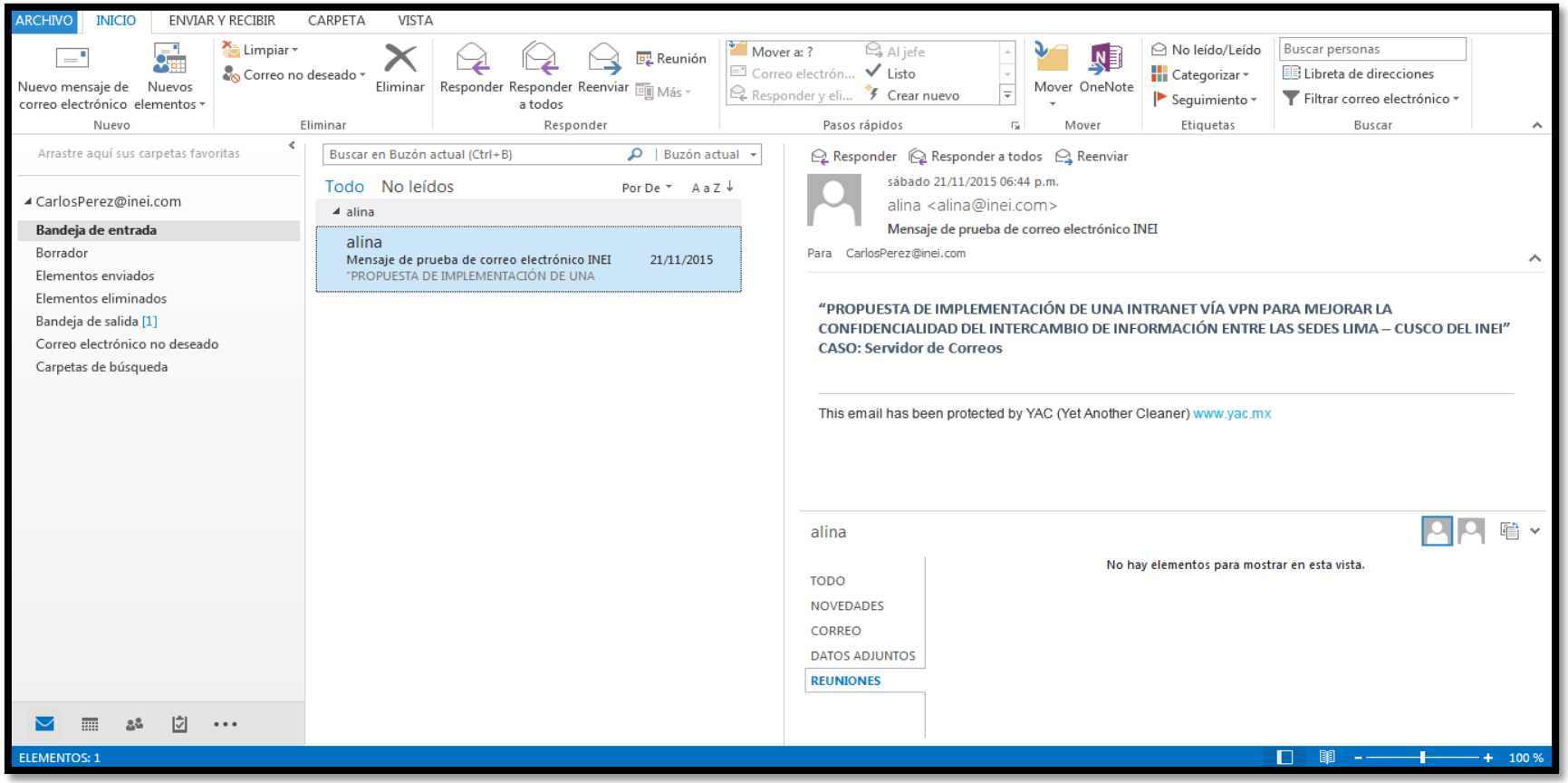
5.2.4 PRUEBA DE ENVÍO Y RECEPCIÓN DE MENSAJES

Una vez culminado con todas las configuraciones anteriormente realizadas, se procedió a realizar pruebas de envío y recepción de mensajes de los correos entre los usuarios alina@inei.com y CarlosPerez@inei.com, donde alina@inei.com envía el mensaje de prueba a CarlosPerez@inei.com



Img 71. Prueba Envío de mensaje alina@inei.com a la cuenta CarlosPerez@inei.com -Fuente (Elaboración Propia)

Mensaje de prueba enviado por alina@inei.com , recibido en la cuenta de correo de CarlosPerez@inei.com.



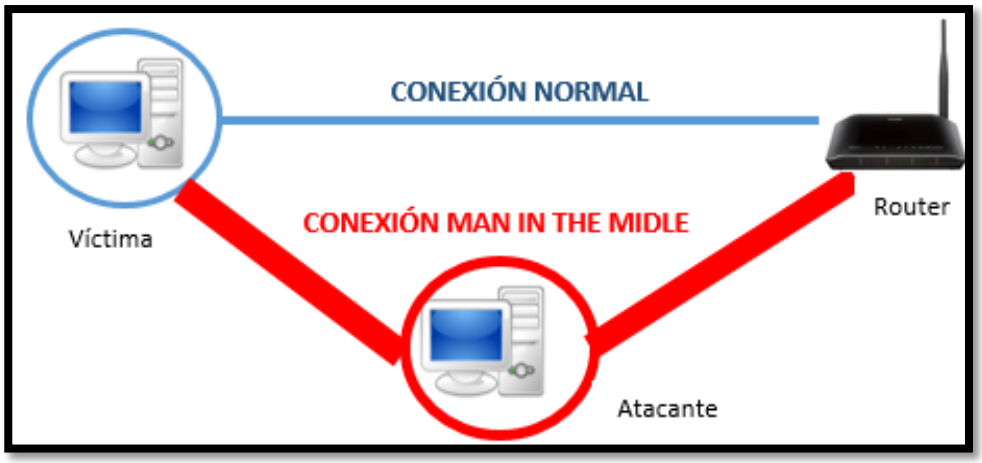
Img 72. Prueba de Recepción del mensaje de la cuenta alina@inei.com -Fuente (Elaboración Propia)

Una vez realizada la prueba de envío y recepción de la información a través del correo, se tiene que la información enviada por la cuenta de alina (alina@inei.com - img. 72), fue recibida con éxito por su destinatario (CarlosPerez@inei.com – img.73), demostrando no sólo la integridad de la información enviada sino también la disponibilidad de ésta para cuando el destinatario lo requiera.

CAPÍTULO VI

6.1 PRUEBAS DE LA INTRANET

Para poner a prueba la seguridad de la intranet vía VPN, se realizó el ataque “man in the middle”, utilizando para esto el sistema operativo kali Linux en su versión 2.0, haciendo uso de la técnica arpspoof y la herramienta sslstrip. Asimismo se realizaron dos ambientes de prueba para realizar los ataques, una sin conexión a la intranet la cual es como actualmente se viene utilizando en las sedes Lima – Cusco del INEI y otra prueba con conexión a la intranet, para verificar que tan eficiente es la VPN, éstos ataques se trabajaron con la siguiente topología:



Img 73. Topología de ataque "Man in the middle"- Fuente (Elaboración Propia)

Antes de iniciar con las pruebas, es necesario señalar que las cuentas que se utilizaron como víctimas para llevar a cabo los ataques man in the middle fueron: alina@inei.com y CarlosPerez@inei.com (clientes VPN anteriormente configurados en la intranet), a continuación se indicarán las direcciones IP´s tanto el atacante como el de las víctimas.

- **Dirección IP del atacante:** 192.168.1.38

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:16:d1:c6
          inet addr:192.168.1.38  Bcast:192.168.1.255  Mask:255.255.255.0
```

Img 74. Dirección IP del atacante – Fuente (Elaboración Propia)

- **Dirección IP de la víctima “alina”:** 192.168.1.34

```
Dirección IPv4. . . . . . . . . . . . : 192.168.1.34
Máscara de subred . . . . . . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.1.1
```

Img 75. Dirección IP de la víctima “alina” – Fuente (Elaboración Propia)

- **Dirección IP de la víctima “CarlosPerez”:** 192.168.1.40

```
Dirección IPv4. . . . . . . . . . . . : 192.168.1.40
Máscara de subred . . . . . . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.1.1
```

Img 76. Dirección IP de la víctima “CarlosPerez” – Fuente (Elaboración Propia)

6.1.1 PRUEBA SIN CONEXIÓN A LA INTRANET

Para iniciar con la prueba del ataque sin conexión intranet se ingresó en modo root o súper-usuario para tener todos los privilegios de administrador, seguidamente se realizaron los siguientes pasos:

- Se puso en modo promiscuo el equipo del atacante para filtrar y escuchar todo el tráfico que pasa por la red, seguidamente se corroboró que la tarjeta de red efectivamente se encontraba en modo promiscuo.

```
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
0
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
```

Img 77. Cambio de modo normal a modo promiscuo – Fuente (Elaboración Propia)

- Se escribió el comando arpspoof para generar el envenenamiento al equipo de la víctima “alina”, con la finalidad de hacer que todo el tráfico que éste mande al router primero pase por la máquina del atacante para así poder robar o vulnerar su información, cuentas de usuario y contraseñas, es así que la víctima nunca se dará cuenta que está siendo vigilada por alguien más ya que el atacante se ésta haciendo pasar por el router.

```
root@kali:~# arpspoof -i eth0 -t 192.168.1.34 192.168.1.1
8:0:27:16:d1:c6 74:e5:43:39:17:89 0806 42: arp reply 192.168.1.1 is-at 8:0:27:16
:d1:c6
8:0:27:16:d1:c6 74:e5:43:39:17:89 0806 42: arp reply 192.168.1.1 is-at 8:0:27:16
:d1:c6
8:0:27:16:d1:c6 74:e5:43:39:17:89 0806 42: arp reply 192.168.1.1 is-at 8:0:27:16
:d1:c6
8:0:27:16:d1:c6 74:e5:43:39:17:89 0806 42: arp reply 192.168.1.1 is-at 8:0:27:16
:d1:c6
8:0:27:16:d1:c6 74:e5:43:39:17:89 0806 42: arp reply 192.168.1.1 is-at 8:0:27:16
:d1:c6
8:0:27:16:d1:c6 74:e5:43:39:17:89 0806 42: arp reply 192.168.1.1 is-at 8:0:27:16
:d1:c6
8:0:27:16:d1:c6 74:e5:43:39:17:89 0806 42: arp reply 192.168.1.1 is-at 8:0:27:16
```

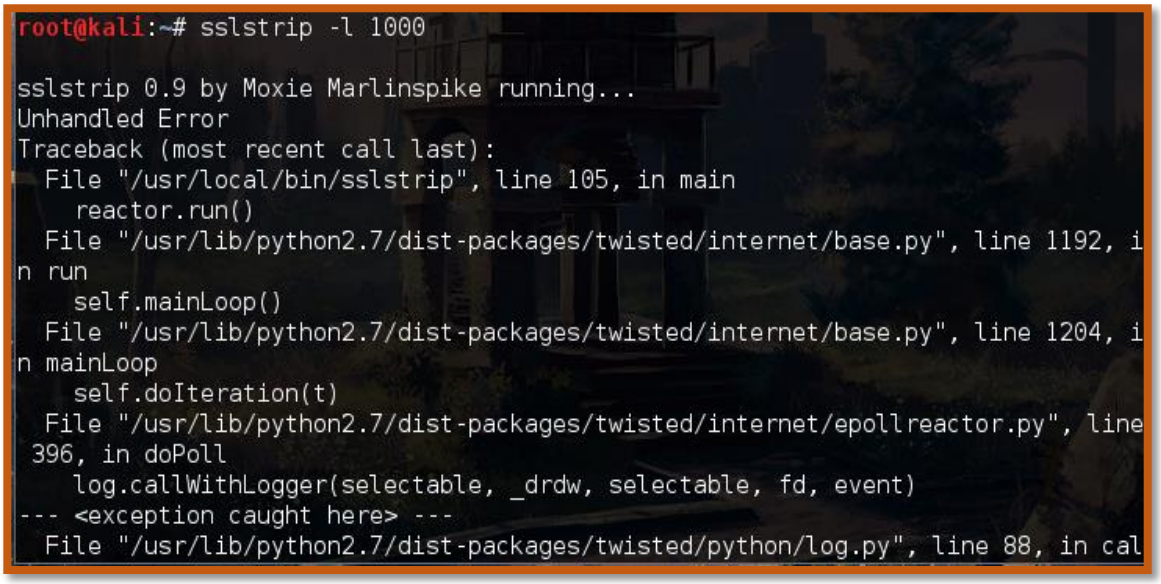
Img 78. Envenenamiento al equipo de la víctima “alina” – Fuente (Elaboración Propia)

- Se utilizó el comando iptables para redireccionar que todo el tráfico que realice la víctima pase de estar del puerto 80 (utilizado por defecto en el sistema), pase al puerto 1000.

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 1000
```

Img 79. Redireccionamiento del puerto 80 al puerto 1000 – Fuente (Elaboración Propia)

- Seguidamente se ejecutó el comando sslstrip para que éste pueda escuchar el tráfico y pueda descifrar el tráfico https y la información de la víctima pase de ser segura a ser vulnerable.

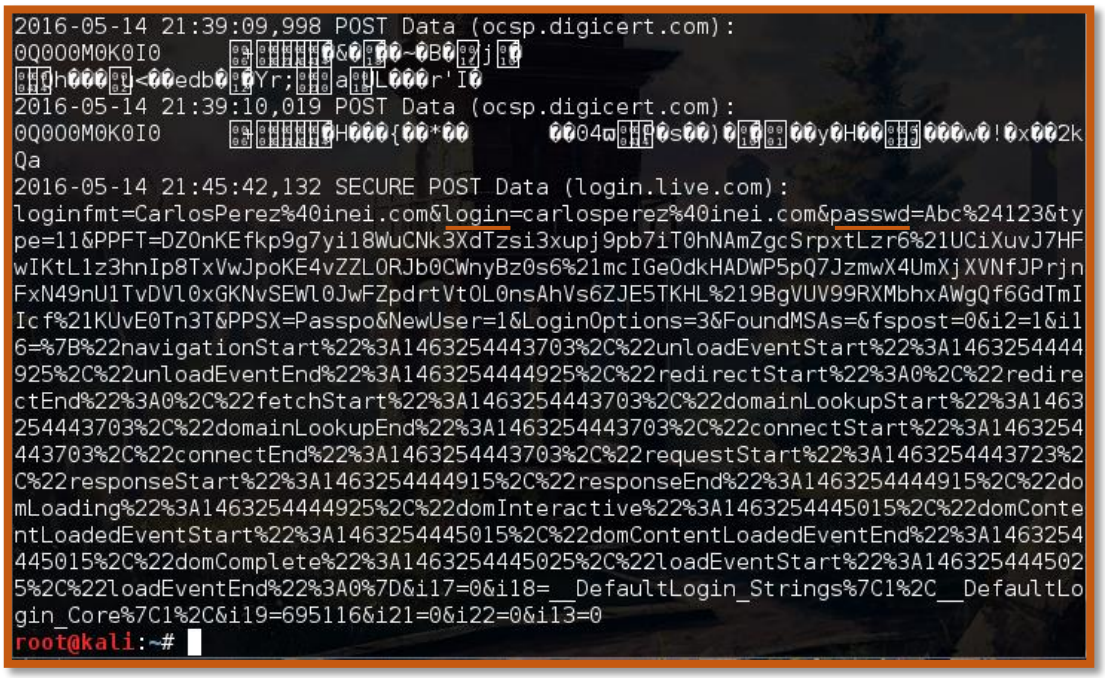


Img 80. Pasar la información segura a ser vulnerable – Fuente (Elaboración Propia)

- Finalmente para poder visualizar el usuario y la contraseña que la víctima colocó al momento de autenticarse en su cuenta de correo, se ejecutó el siguiente comando: "cat sslstrip.log", ya que es ahí donde sslstrip almacena toda la información del tráfico que generó la víctima.

Img 81. Cuenta hackeada de la víctima "alina" – Fuente (Elaboración Propia)

- Para el caso de la segunda víctima “CarlosPerez”, de la misma manera se siguieron los pasos anteriores, con la diferencia que se cambió la dirección IP del equipo en el que éste se encontraba situado.



Img 82. Cuenta hackeada de la víctima CarlosPerez – Fuente (Elaboración Propia)

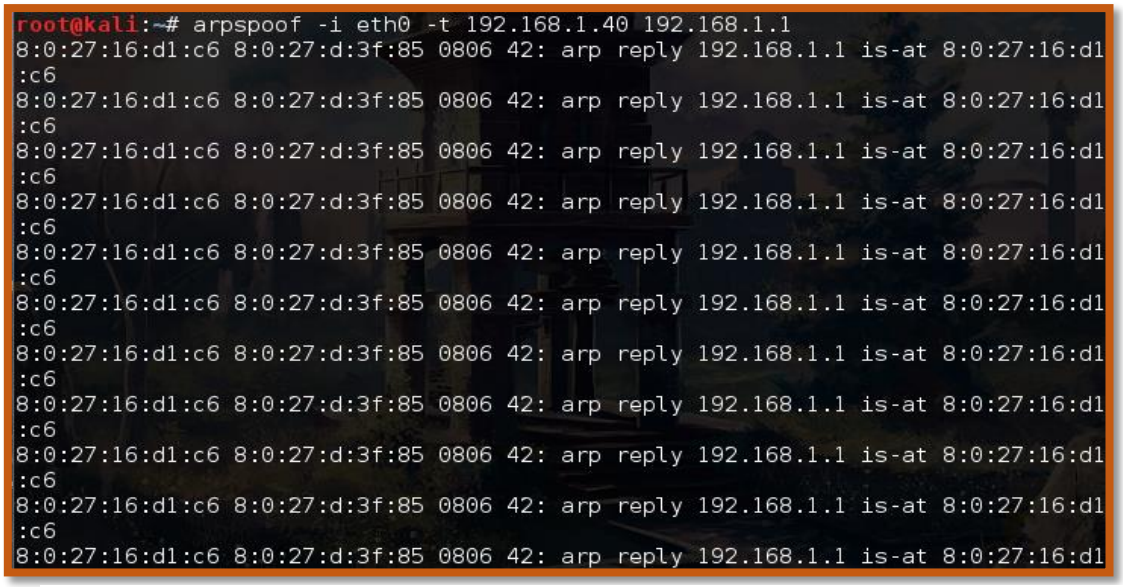
6.1.2 PRUEBA CON CONEXIÓN A LA INTRANET

Para realizar las pruebas con la conexión a la VPN, primeramente la víctima se conectó a la intranet indicando su cuenta y su contraseña asignada como cliente VPN, seguidamente se realizaron los siguientes pasos:

- Ingresar en modo súper-usuario para tener los privilegios de administrador y se puso en modo promiscuo el equipo del atacante.

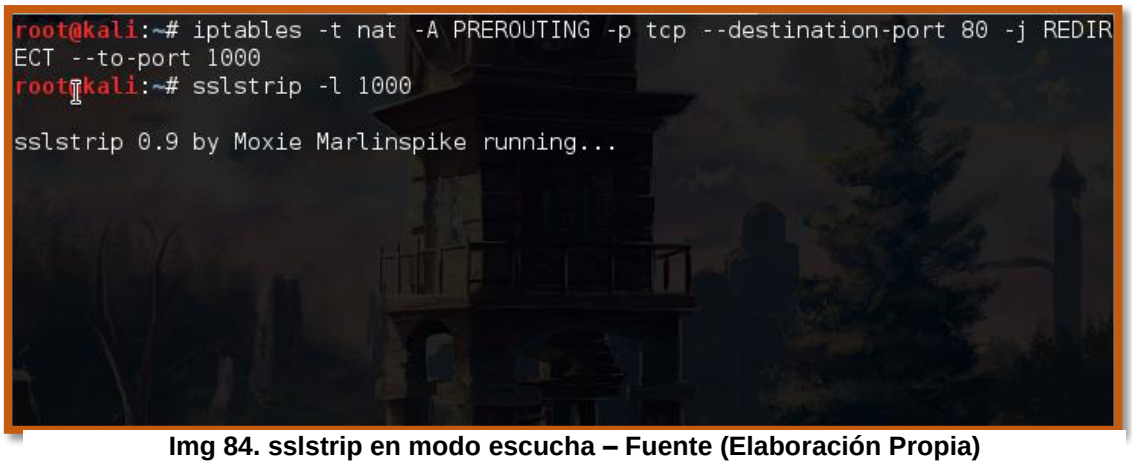
Img 83. Cambio a modo promiscuo de la tarjeta de red– Fuente (Elaboración Propia)

- Ejecutar el comando arpspoof para envenenar el equipo de la víctima “CarlosPerez” y hacer que todo el tráfico que éste realice que pase por el equipo del atacante y así este pueda observar todo lo que la víctima esté realizando en su equipo.



Img 85. Envenenamiento al equipo de la víctima "CarlosPerez" – Fuente (Elaboración Propia)

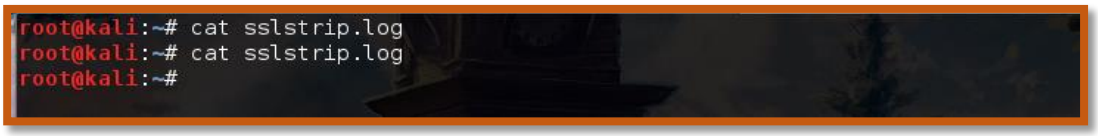
- Se ejecutó los comandos iptables y sslstrip, iptables para redireccionar todo el tráfico que realice la víctima pase de estar del puerto 80 pase al puerto 1000 y sslstrip para hacer que éste escuche y descifre el tráfico https pasándolo a http.



Img 84. sslstrip en modo escucha – Fuente (Elaboración Propia)

Como se pudo observar en la anterior imagen sslstrip no pudo captar el tráfico que la víctima estuvo realizando (ingresar a su cuenta de correo), para poder corroborar que el atacante no pudo obtener nada del tráfico que ocasionó la víctima se ejecutó el siguiente comando:

Como se pudo observar no se registra absolutamente ningún dato.



Img 86. Almacén del tráfico que guardó sslstrip generada por la víctima – Fuente (Elaboración Propia)

6.2 DISCUSIÓN DE RESULTADOS

Una vez realizado cada una de las pruebas, se procedió a comparar los resultados obtenidos.

- **Resultados del ataque "man in the middle" sin conexión a la intranet**

Img 87. Resultados de ataque sin conexión a intranet – Fuente (Elaboración Propia)

Como se pudo observar en la imagen anterior, se puede ver claramente la cuenta de usuario y la contraseña de correo de la víctima "alina", donde:

Cuenta de correo: alina@inei.com

Contraseña: 123%40Abc

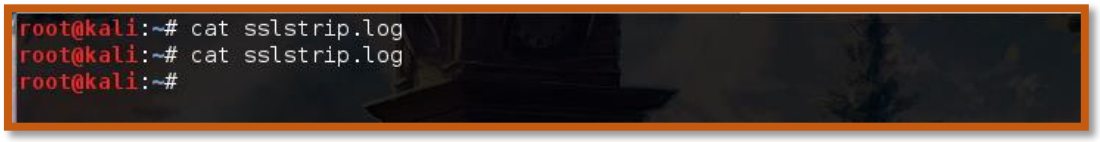
Una vez realizado el ataque se muestra que $ está expresado con el código: %40.

Con el resultado obtenido sin la conexión a la intranet según muestra la imagen 88, se puede observar que con el ataque man in the midle el atacante no sólo pudo observar el tráfico que generó la víctima sino que a su vez éste pudo extraer la cuenta de usuario y la contraseña de la víctima a quien se realizó el ataque.

CONCLUSIÓN

Sin una conexión VPN la información de la víctima puede ser fácilmente extraída y vulnerada por el atacante.

- **Resultados del ataque "man in the middle" con conexión a la intranet**



Img 88. Resultados de ataque con conexión a intranet – Fuente (Elaboración Propia)

Con el resultado obtenido con la prueba del ataque man in the middle con una conexión a la intranet según muestra la imagen 89, se puede observar que el atacante no pudo captar absolutamente nada del tráfico que realizó la víctima "alina".

CONCLUSIÓN

Con una conexión VPN no sólo se asegura la información sino que a su vez se mejora la confidencialidad de la misma, dando fé que la hipótesis anteriormente señalada al inicio del presente informe es verdadera.

CAPÍTULO VII

COSTOS

7.1 COSTOS DE INVESTIGACIÓN DEL PROYECTO

	CANTIDAD	ESPECIFICACIONES		COSTO UNITARIO	COSTO GENERAL
HADWARE	2	PC´s de escritorio	Pc1	S/. 2507.00	S/. 4757.00
			Pc2	S/. 2250.00	
	2	Laptops	Laptop1	S/. 2350.00	S/. 5240.00
			Laptop2	S/. 2890.00	
	2	Routers	ZTE	S/. 70.00	S/. 108.00
			TP - LINK	S/. 38.00	
	2	Cables de red		S/.3.00	S/. 6.00
SOFTWARE	3	Windows Server 2008 r2		S/.0.00	S/.0.00
		Windows 7 Professional		S/.0.00	
		Kali Linux		S/.0.00	
SERVICIOS	Servicio de Luz (S/.65.00 por año y medio)				S/. 1170.00
	Servicio de Internet (S/.96.30 por año y medio)				S/.1733.40
OTROS	Papelería				S/. 500.00
COSTO TOTAL					S/. 13514.40

Tabla 24. Costos de Investigación del proyecto – Fuente (Elaboración Propia)

7.2 COSTOS DE IMPLEMENTACIÓN DEL PROYECTO

		ESPECIFICACIONES	CANTIDAD	COSTO ESPECÍFICO	COSTO GENERAL
	HADWARE	Router Cisco[29]	2	**$.** 206.48 (Tipo de cambio del dólar 3.34)[30]	**S/.** 1379.28
				S/. 689.64	
	SOFTWRAE (PAGO ANUAL)	Windows Server 2008 r2[31]		**$.** 1500.00 (Tipo de cambio del dólar 3.34)[32]	**S/.** 5460.90
				S/. 5010.00	
		Windows 7 Professional[33]		**$.** 135.00 (Tipo de cambio del dólar 3.34) (Cuanto cuesta el dólar, 2016)	
				S/. 450.90	
SEDE CUSCO	SERVICIOS	Servicio de Luz (pago mensual aproximado)[34]		**S/.** 3200.00	**S/.** 7900.00
		Servicio de Internet (pago mensual: 2Mb) (INEI, 2016)[35]		**S/.** 2500.00	
		Recursos Humanos – Ing. Sistemas (pago mensual)[36]		**S/.** 2200.00	
SEDE LIMA	SERVICIOS	Servicio de Luz (pago mensual aproximado)		**S/.** 5000.00	**S/.** 12000.00.
		Servicio de Internet (pago mensual: 4Mb)		**S/.** 4500.00	
		Recursos Humanos – Ing. Sistemas (pago mensual)		**S/.** 2500.00	
	COSTO TOTAL				**S/. 26740.18**

Tabla 25. Costos de Implementación del proyecto – Fuente (Elaboración Propia)

[29] (Amazon, Amazon, 2016)
[30] (Cuanto cuesta el dólar, 2016)
[31] (Amazon, Amazon.es, 2016)
[32] (Cuanto cuesta el dólar, 2016)
[33] (Amazon, Amazon.es, 2016)
[34] (INEI, 2016)
[35] (INEI, 2016)
[36] (INEI, 2016)

- # DESCRIPCIÓN DE COSTOS

  - **COSTOS DE INVESTIGACIÓN DEL PROYECTO**

    Algunos de los costos señalados en el cuadro de costos de investigación del proyecto, son referenciales debido a que ya se contaba con algunos de ellos (Pc´s de escritorio, laptops, routers, cables de red), con referencia los softwares el costo señalado es de S/. 0.00 debido a que ya se tenían instalados en las maquinas utilizadas y finalmente en cuanto a los servicios y al costo de papelería sí señalan el costo real utilizado.

  - **COSTOS DE IMPLEMENTACIÓN DEL PROYECTO**

    Los precios señalados de los servicios de las sedes Lima – Cusco del INEI, fueron extraídos tomando como referencia los datos Internos de la institución, en cuanto al costo señalado de la licencia de Windows 7 Professional es con referencia de Microsoft pero cabe señalar que actualmente las máquinas de los trabajadores de las áreas administrativas ya cuentan con dicha licencia en ambas sedes, finalmente en cuanto al costo del router y a la licencia de Windows server 2008, serían la única inversión que realizaría la entidad para la implementación de la intranet vía VPN.

GLOSARIO

- **INEI** : Instituto Nacional de Estadística e Informática
- **ISO** : International Organization for Standardization
- **TCP** : Transmission Control Protocol
- **VPN** : Virtual Private Network
- **PPTP** : Point To Point Tunneling Protocol
- **PC** : Computadora Personal
- **DNS** : Domain Name System
- **CISCO** : Empresa Líder en Tecnologías de la Información
- **HTTP** : Protocolo de Transferencia de Hipertexto
- **HTTPS** : Versión segura del Protocolo http
- **L2TP** : Layer 2 Tunneling Protocol
- **LAN** : Local Area Network
- **IPSEC** : Ip Security
- **SSL** : Secure Socket Layer
- **IIS** : Internet Information Services
- **AD** : Active Directory
- **SMTP** : Simple Mail Transfer Protocol
- **DNS** : Domain Name System
- **NPS** : Servidor de Directivas de redes
- **NPAS** : Servicio de Acceso y Directivas de Redes

CONCLUSIONES

1. Se elaboró la propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI, donde se pudo observar que, sin la conexión a la intranet vía VPN el atacante no solo pudo observar el tráfico que generó su víctima sino que éste a su vez pudo extraer con facilidad la información de ésta (cuenta de usuario y contraseña vista en la imagen 88), en cambio con los resultados obtenidos con la conexión a la intranet vía VPN realizada por la víctima, el atacante no pudo tener acceso al tráfico que generó su víctima ni a su cuenta de usuario y contraseña (vista en la imagen 89), por ende queda demostrado que con la implementación de una intranet vía VPN sí se mejora la confidencialidad de la información.
2. Se simuló el intercambio de información por medio del servidor de correos entre las cuentas alina@inei.com y CarlosPerez@inei.com (clientes VPN), dando como resultado una comunicación exitosa entre ambas cuentas.
3. Se configuró un servidor de correos para la prueba de funcionalidad de la intranet, para ello se realizaron los ataques man in the middle en dos escenarios de prueba con conexión a la intranet y sin conexión a la intranet vía VPN, en donde se obtuvo que con la conexión a la intranet (vista en la imagen 89), el atacante no pudo observar absolutamente nada del tráfico que generó la víctima, ni su cuenta de usuario, ni su contraseña, por ende se puede decir que la VPN asegura toda la información que maneje un cliente VPN en su cuenta de correo.
4. La VPN aseguró la integridad de la información enviada del emisor al receptor, para demostrar dicha afirmación se realizó una prueba de envío y recepción de información entre dos cuentas, alina@inei.com (emisor – Img.72) para CarlosPerez@inei.com (destinatario – Img. 73), en donde se puede dar fé de la

integridad de la información, es decir que: tal como “alina” envió la información al destinatario “Carlos Perez”, éste recibió el mensaje conforme “alina” lo envió.

5. Se verificó la disponibilidad de la información por medio del servidor del correos según la prueba de envío de la información realizada por alina@inei.com para el destinatario CarlosPerez@inei.com (vista en la imagen 73), donde se pudo observar que la información queda a la disponibilidad del receptor cuando éste lo requiera en su bandeja de entrada.

6. Se determinaron los costos de investigación del proyecto donde señalan los costos del hardware, software y servicios utilizados durante tiempo de investigación del proyecto, dando un total de **S/. 13514.40**.

7. Se determinaron los costos de implementación del proyecto, dando la posibilidad de que el proyecto pueda ser adquirido por el INEI, ya que ésta institución por pertenecer al estado, éste podría aportar económicamente para la adquisición del presente gracias a la mejora de la confidencialidad de información que ofrece, el costo total de implementación es de **S/. 26740.18**.

RECOMENDACIONES

1. Implementar en el INEI algunas de las políticas de seguridad estipuladas en estándares o normativas de gestión de seguridad de la información.
2. Si se deseara realizar la implementación de una intranet vía VPN para interconectar las demás sedes del INEI las cuales se encuentran ubicadas a nivel nacional, se recomienda utilizar L2TP para maximizar la seguridad y confidencialidad de la información.
3. Se recomienda adquirir dos routers uno para cada sede del INEI (sede Lima - Cusco) para el uso exclusivo de la intranet vía VPN.

REFERENCIAS

Alfonso, E. V. (15 de Julio de 2015). Redes Digitales Blog-spot. Obtenido de http://redesdigitales-vpn-6im9.blogspot.pe/

Amazon. (10 de Junio de 2016). Amazon. Obtenido de https://www.amazon.com/Cisco-RV325-Gigabit-Router-RV325-K9-NA/dp/B00GSQJI4E

Amazon. (22 de Junio de 2016). Amazon.es. Obtenido de https://www.amazon.es/Microsoft-Windows-Professional-Sp1-Licencia/dp/B004Q86D8U

Amazon. (26 de Junio de 2016). Amazon.es. Obtenido de https://www.amazon.es/Microsoft-Windows-Professional-Sistema-Operativo/dp/B00H09BXI2/ref=sr_1_1?ie=UTF8&qid=1467605721&sr=8-1&keywords=licencia+windows+7+professional+64

Andrew, T. (2010). Redes de Computadoras, 4ta Edicion. Pearson Prentice Hall.

Bustamante, O. (2014). Metodologia Para La Implementacion De Redes Privadas Virtuales Con Internet Como Red De Enlace.

Curso de hackers. (10 de Mayo de 2016). Obtenido de http://www.cursodehackers.com/ManInTheMiddle.html

Cisco. (03 de marzo de 2015). Cisco. Obtenido de http://www.cisco.com/web/LA/soluciones/la/vpn/index.html

Cisco. (08 de Junio de 2016). Cisco. Obtenido de http://www.cisco.com/c/en/us/products/routers/rv325-dual-gigabit-wan-vpn-router-wf/index.html

CopolInformática. (18 de Junio de 2015). CopolInformática. Obtenido de https://sites.google.com/site/copolinformaticabi2015/tema-3-redes/aspectos-basicos-de-redes/3-1-4-identificar-las-tecnologias-necesarias-para

Dennis, F. (2012). Virtual Private Networks: Making the right connection, 1ra Edicion. Morgan Kaufmann Publishers.

INDECOPI-CNB, I. (1 de Noviembre de 2009). Sistemas de Gestión de Seguridad de la Información. Norma Técnica Peruana NTP-ISO/IEC 27001, págs. 11-12.

INEI. (2016). Datos internosde la Institución.

Linux GNU Blog. (15 de Mayo de 2016). Obtenido de http://linuxgnublog.org/envenamiento-de-las-tablas-arp-arp-spoofing/

Microsoft. (04 de febrero de 2015). Obtenido de Microsoft: https://msdn.microsoft.com/es-es/library/cc786563%28v=ws.10%29.aspx

Microsoft. (05 de Noviembre de 2015). Microsoft. Obtenido de https://msdn.microsoft.com/es-ar/library/cc488021(v=vs.90).aspx

Microsoft. (06 de Noviembre de 2015). Microsoft. Obtenido de http://licenciamiento-microsoft.com/category/windows7/

Microsoft. (04 de febrero de 2015). Microsoft. Obtenido de https://msdn.microsoft.com/es-es/library/cc786563(v=ws.10).aspx

Microsoft. (20 de Mayo de 2015). Microsoft. Obtenido de https://msdn.microsoft.com/es-es/library/cc786563(v=ws.10).aspx

Mircrosoft. (26 de Agosto de 2015). Mircrosoft. Obtenido de https://social.technet.microsoft.com/Forums/es-ES/f0ce940a-9f2c-4d75-9134-6f0c47e56a91/dns-directa-e-inversa?forum=windowsserveres

Ramirez Limari, V. H. (2010). Protocolos De Seguridad Para Redes Vpn.

Sampieri, E. (Mayo de 2015). Tipos de Metodologias. Obtenido de http://www.academia.edu/6399195/Metodologia_de_la_investigacion_5ta_Edicion_Sampieri

Seguridad Informática. (17 de Mayo de 2016). Obtenido de http://www.redeszone.net/seguridad-informatica/sslstrip/

Servicios de Aacceso y Directivas de Redes. (mayo de 2015). Obtenido de https://technet.microsoft.com/es-es/library/cc731321.aspx

Stallings, W. (2012). Data and Computer Networks, 8va Edicion. Pearson Prentice Hall.

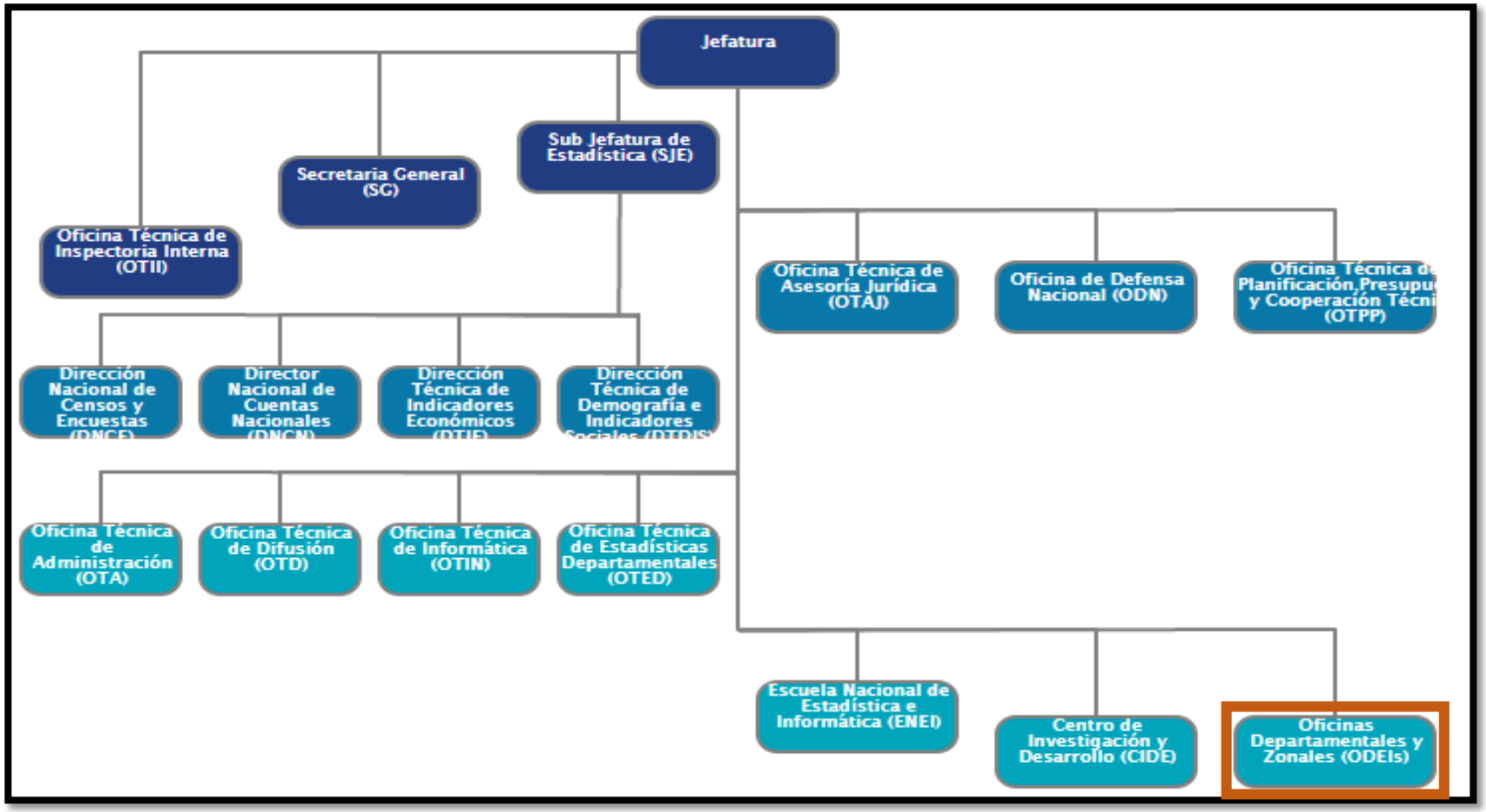
VyprVPN. (27 de Marzo de 2015). VyprVPN. Obtenido de https://www.goldenfrog.com/ES/vyprvpn/features/vpn-protocols

ANEXOS

Br. JENNY MAR SEGUNDO

ANEXO 1

ORGANIGRAMA INEI SEDE LIMA



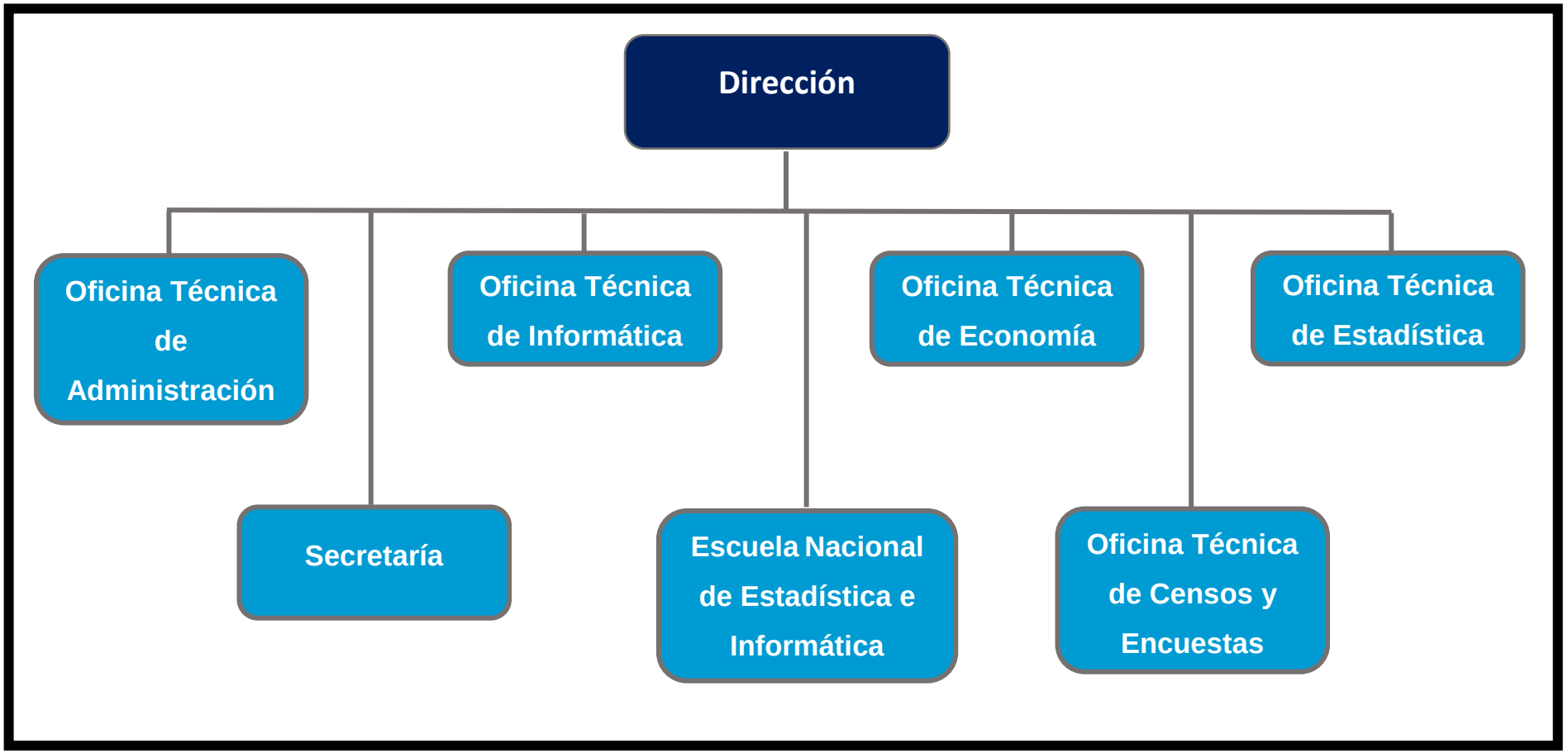
Img 89. ANEXO 1 - Organigrama INEI sede Lima, Fuente (INEI)

Cabe señalar que las sedes del INEI que se encuentran ubicadas a nivel nacional se encuentran dentro del área de ODEIs.[37]

[37] (INEI, 2016)

ANEXO 2

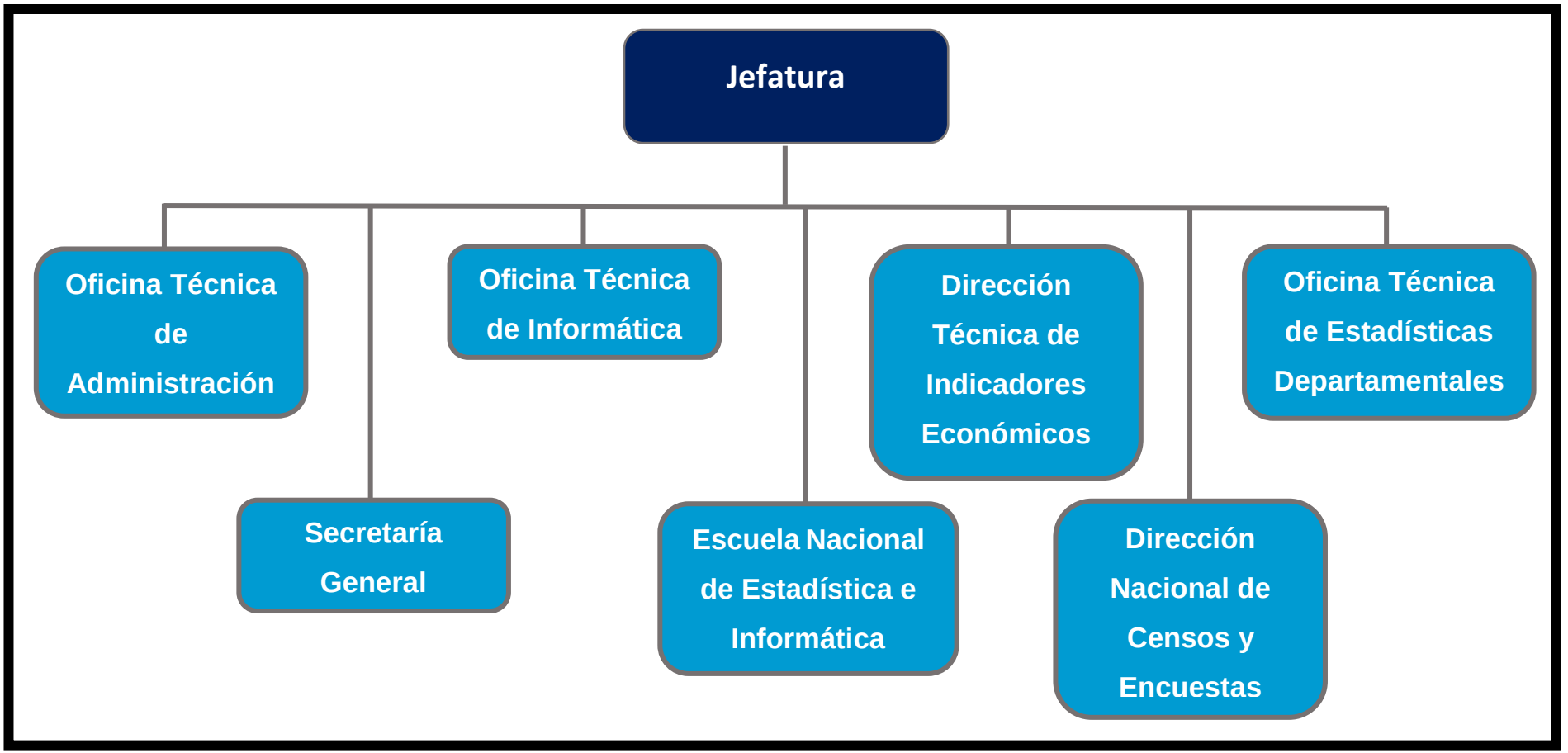
ORGANIGRAMA INEI SEDE CUSCO



Img 90. ANEXO 2 - Organigrama INEI sede Cusco, Fuente (INEI)

ANEXO 3

ORGANIGRAMA DE ÁREAS ADMINISTRATIVAS EN COMÚN SEDES LIMA – CUSCO DEL INEI



Img 91. ANEXO 3 - Organigrama de áreas administrativas en común del INEI sedes Lima - Cusco, Fuente (Elaboración Propia)

ANEXO 4

CUESTIONARIO PARA EL PERSONAL ADMINISTRATIVO EN COMÚN DE LAS SEDES LIMA – CUSCO DEL INEI

TITULO DE LA TESIS

Propuesta de implementación de una Intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI

CASO: Servidor de Correos

OBJETIVO DEL CUESTIONARIO

Verificar de qué manera actualmente se lleva a cabo el intercambio de información entre las sedes Lima – Cusco del INEI.

NOMBRES Y APELLIDOS

……..

CARGO QUE OCUPA

……..

Las siguientes preguntas se realizaron a los trabajadores de las áreas administrativas de las sedes Lima – Cusco del INEI.

1) ¿Actualmente en la institución se utilizan correos no institucionales para el envío y recepción de información confidencial?

Si ( ) -> Hotmail ( ) Gmail ( ) otros ( )

No ( ) ¿Por qué?

……..…

……..

2) ¿Ud. Posee una cuenta de correos institucional?

Si ( )

No ( ) ¿Por qué?

……..…

……..

3) ¿Utiliza su cuenta de correo no institucional para el envió de información laboral y confidencial?

Si ( )

No ( ) ¿Por qué?

……..…

……...

4) ¿Qué información confidencial es la que se envía por estas cuentas?

a) Acuerdos de proyectos a nivel nacional a realizar

b) Envío del monto económico por cobrar

c) Agenda a tratar en reunión

d) Otros…….

5) ¿Le gustaría que se implemente un correo institucional para el envío y recepción de información netamente institucional?

Si ( )

No ( ) ¿Por qué?

……..…

……...

Las siguientes preguntas se realizaron sólo al personal de las áreas informáticas de las sedes Lima – Cusco del INEI.

6) ¿Existen antecedentes de vulnerabilidades de información anteriormente realizadas a alguna cuenta?

Si ( ) ¿Como cuáles?

No ( )

……..…

……...

7) ¿Se cuenta con medidas de seguridad en caso de posibles ataques?

Si ( ) ¿Como cuáles?

No ( ) ¿Por qué?

……..…

……...

8) ¿Estaría de acuerdo con la implementación de una intranet vía VPN para interconexión de las sedes Lima – Cusco del INEI?

Si ( ) ¿Por qué?

No ( ) ¿Por qué?

……..…

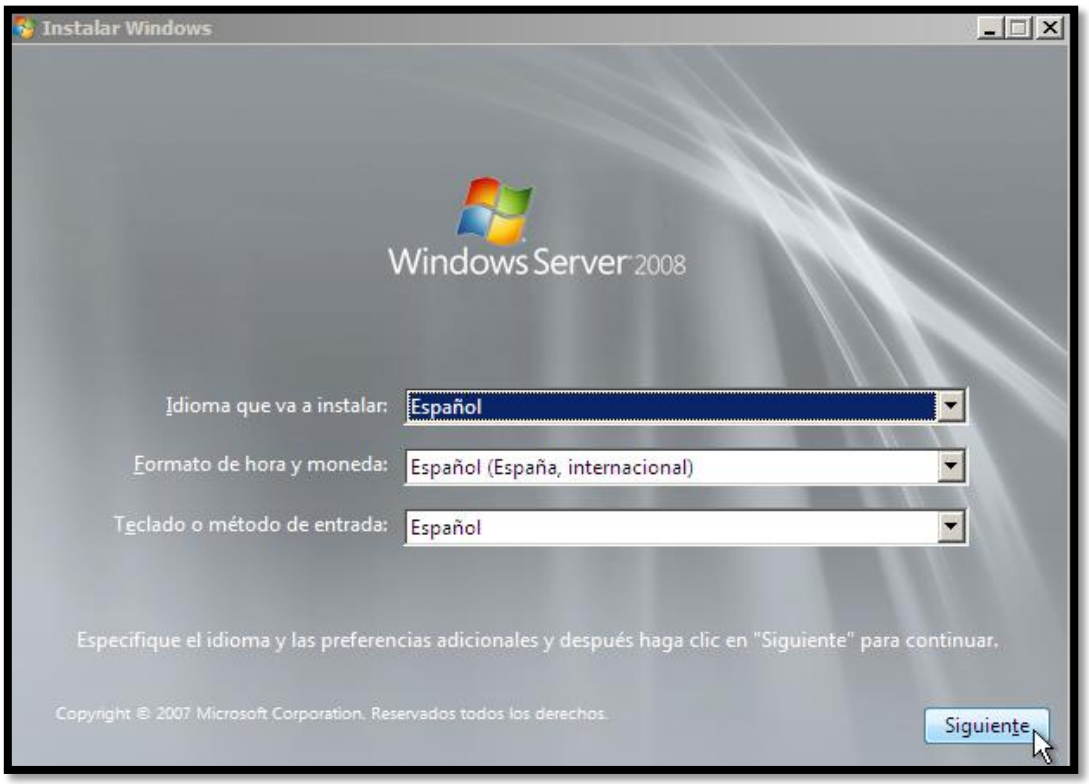
……...

ANEXO 5

INSTALACIÓN DEL SISTEMA OPERATIVO: WINDOWS SERVER 2008 R2

Para inicializar la instalación del sistema operativo Windows server 2008, ejecutar el CD, seguidamente realizar los siguientes pasos

Seleccionar el tipo de idioma, formato de hora – moneda y finalmente elegir el tipo de configuración del teclado, según se muestra en la siguiente imagen.

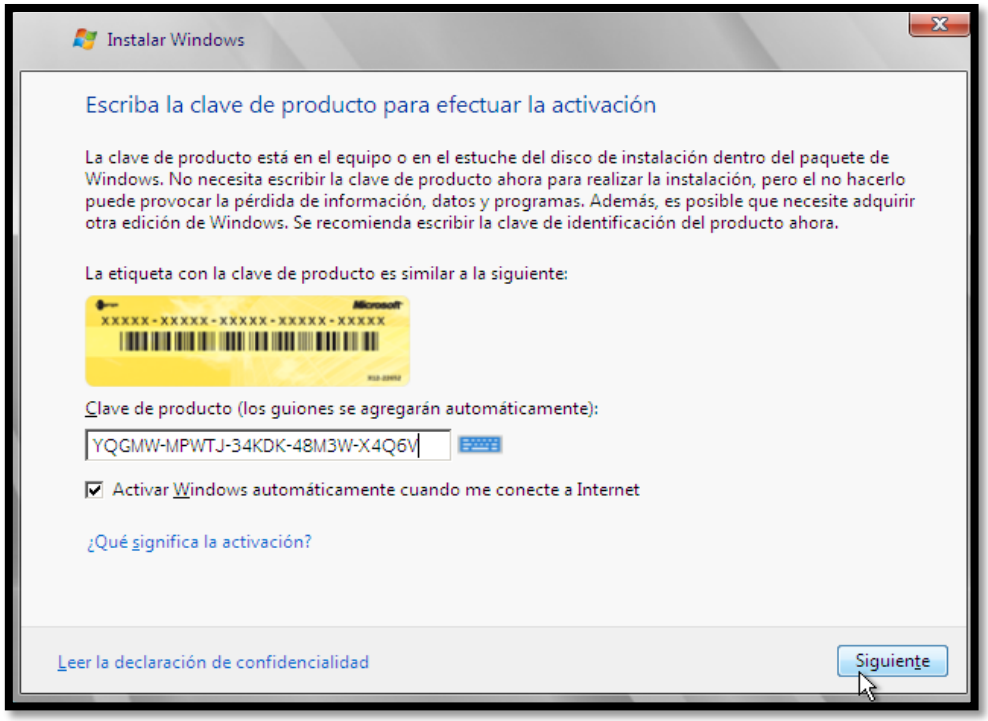


Img 92. Idioma, Formato de hora y teclado de entrada de Windows Server 2008 – Fuente (Elaboración Propia)

Pulsar sobre la opción “instalar ahora” para poder iniciar con el proceso de instalación del sistema operativo.

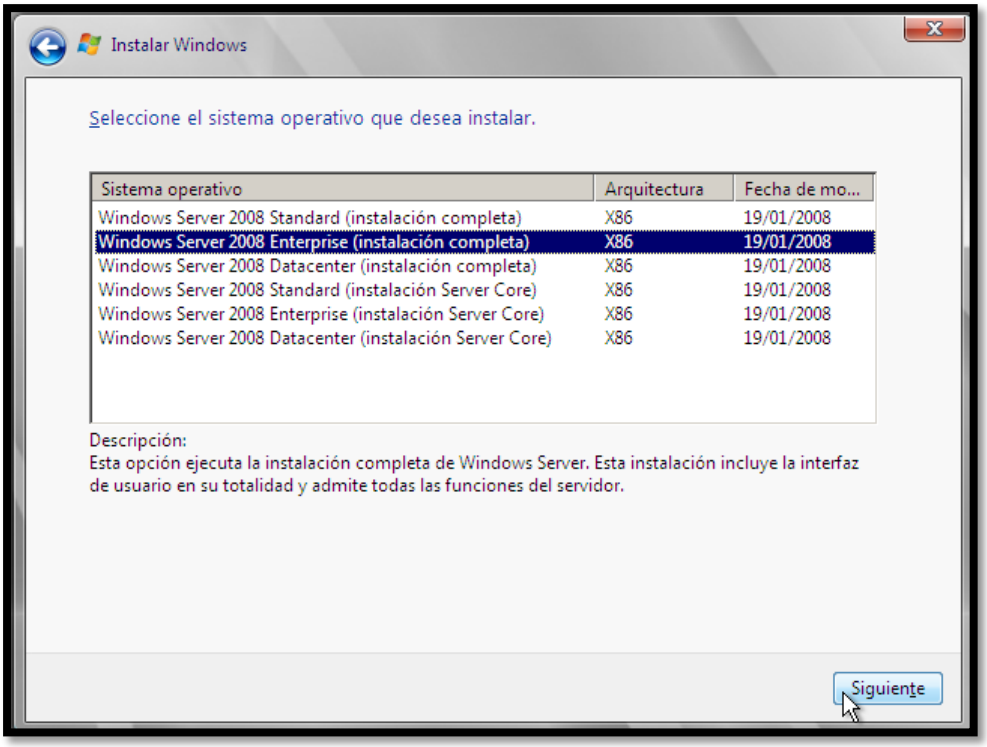
Img 93. Inicio de Instalación Windows Server 2008 – Fuente (Elaboración Propia)

Indicar la clave del producto para su activación.



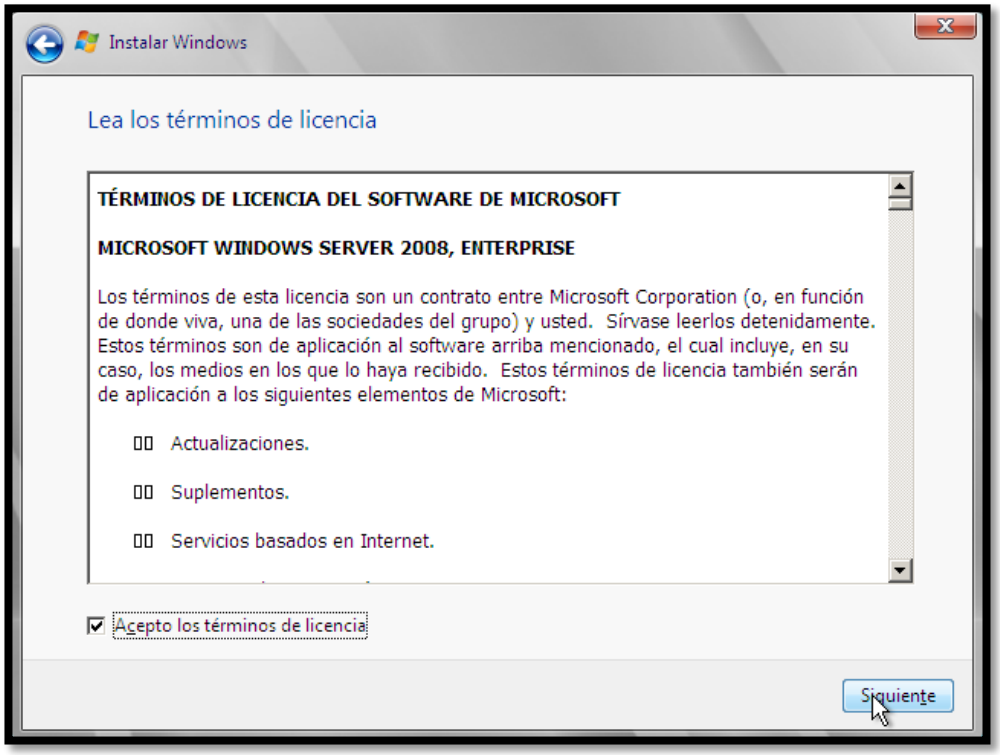
Img 94. Serial para Activación Windows Server 2008 – Fuente (Elaboración Propia)

Seleccionar la versión “Windows Server 2008 Enterprise (Instalación Completa)”, para tener una interfaz gráfica y llevar a cabo las configuraciones.



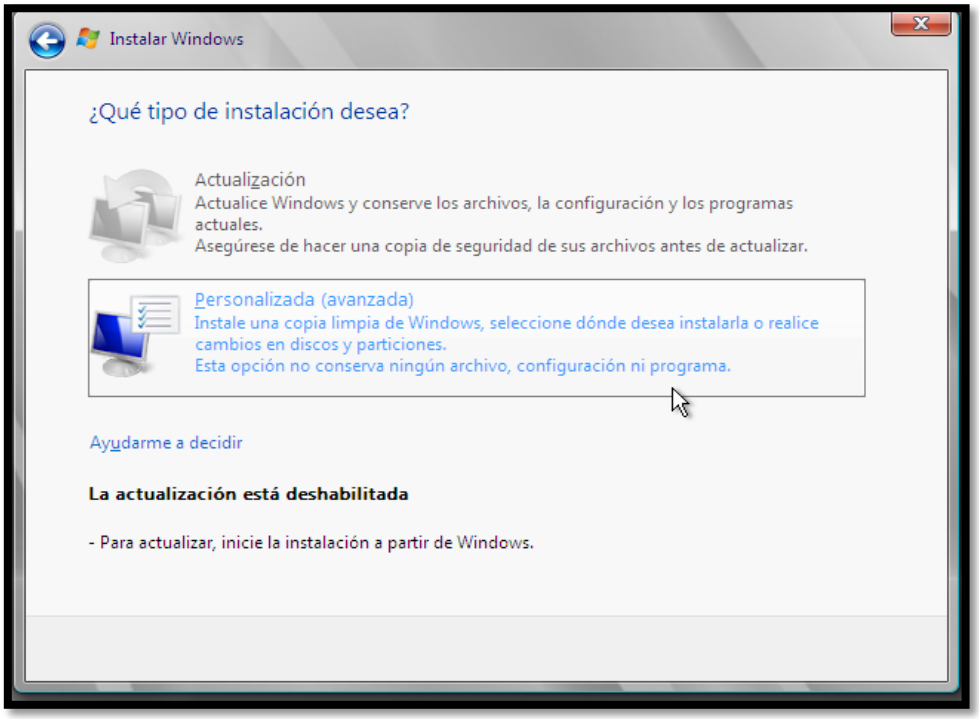
Img 95. Versión Windows Server 2008 Enterprise – Fuente (Elaboración Propia)

Aceptar los términos de licencia.



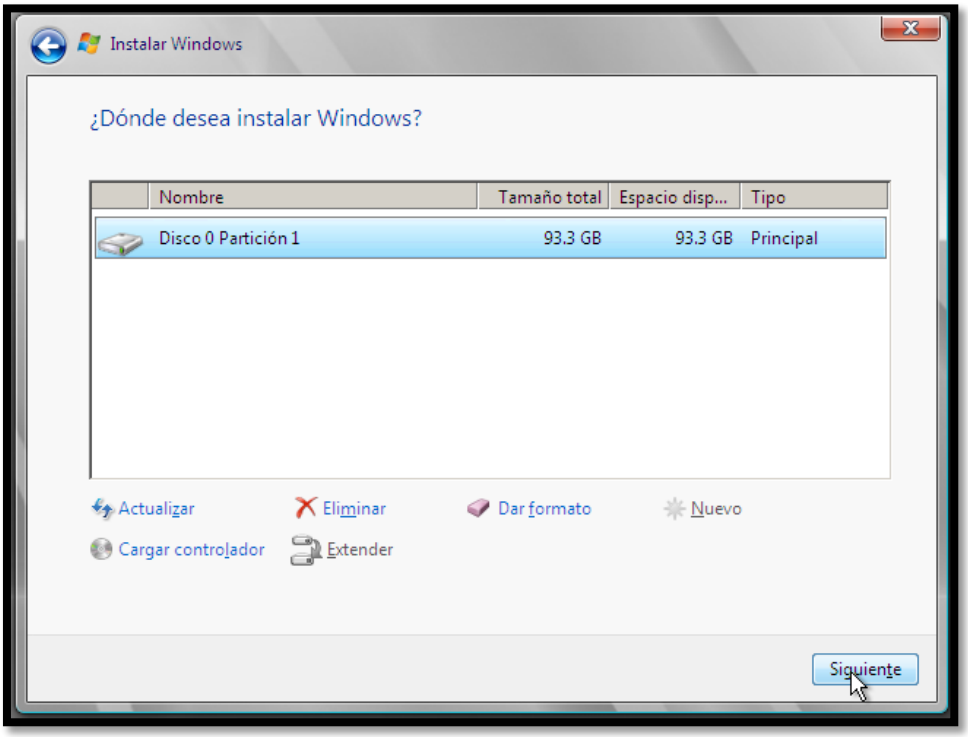
Img 96. Términos de Licencia Windows Server 2008 – Fuente (Elaboración Propia)

El tipo de instalación que se ha de elegir es “Personalizada (Avanzada)”.



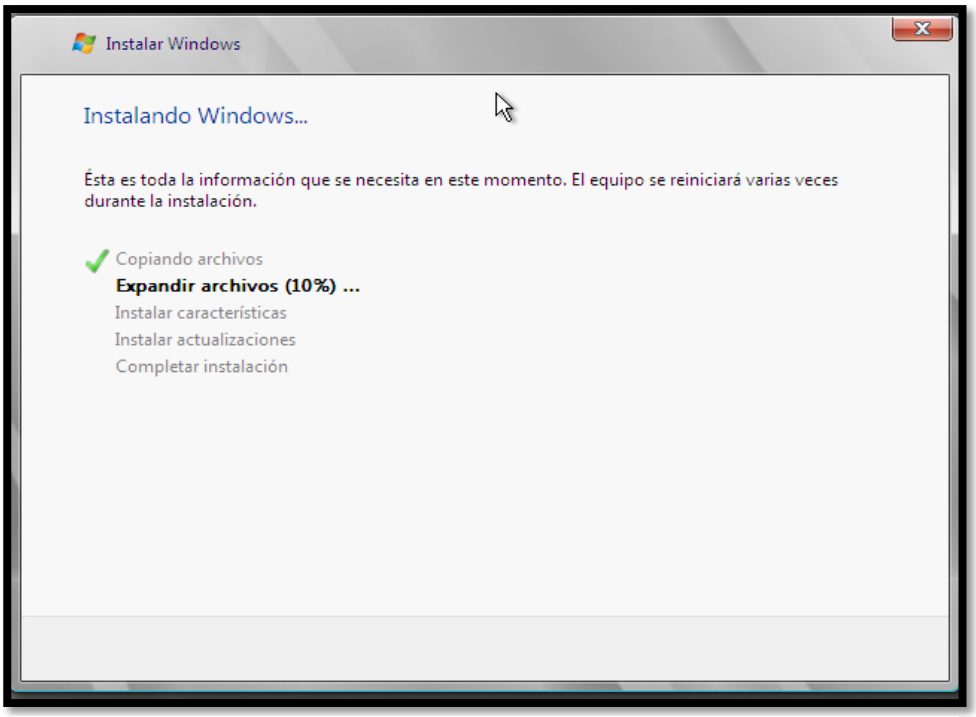
Img 97. Tipo de Instalación – Fuente (Elaboración Propia)

Seleccionar y asignar tamaño a la partición en donde se ha de instalar el sistema operativo.



Img 98. Seleccionar Partición para la Instalación Windows Server 2008 – Fuente (Elaboración Propia)

Esperar a que se lleve a cabo el proceso de instalación y finalización del Sistema Operativo Windows Server 2008 r2 Enterprise.



Img 99. Proceso de Instalación y Finalización de Windows Server 2008 – Fuente (Elaboración Propia)

ANEXO 6

INSTALACIÓN DEL SISTEMA OPERATIVO: WINDOWS 7

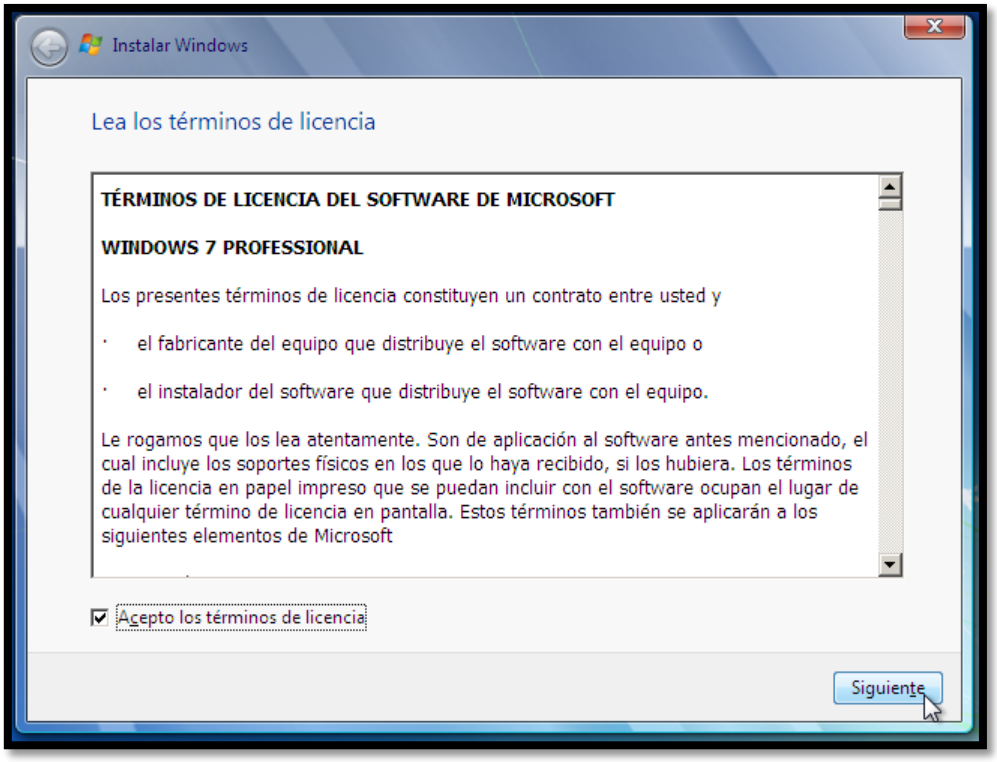
Ejecutar el DVD de instalación de Windows 7, configurar el idioma, formato de fecha - hora y el tipo de teclado, según se muestra en la siguiente imagen.

Img 100. Configuración de Idioma, Fecha y Tipo de teclado – Fuente (Elaboración Propia)

Pulsar sobre la opción instalar ahora, para dar inicio al proceso de instalación de Windows 7.

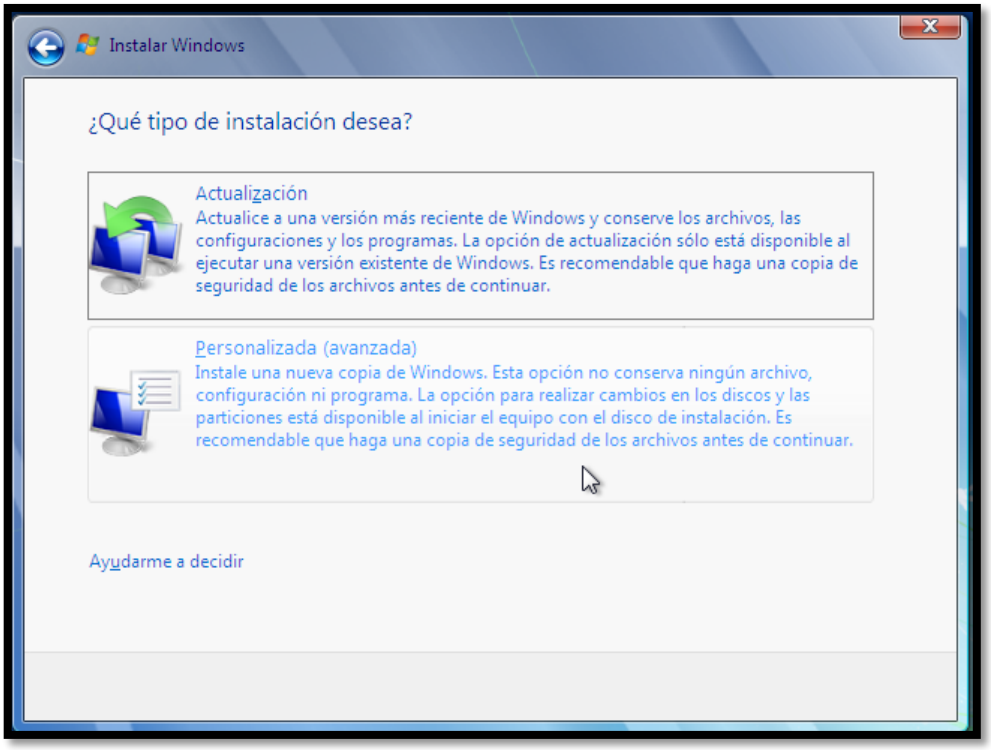
Img 101. Inicio de Instalación de Windows 7 – Fuente (Elaboración Propia)

Aceptar los términos de licencia.



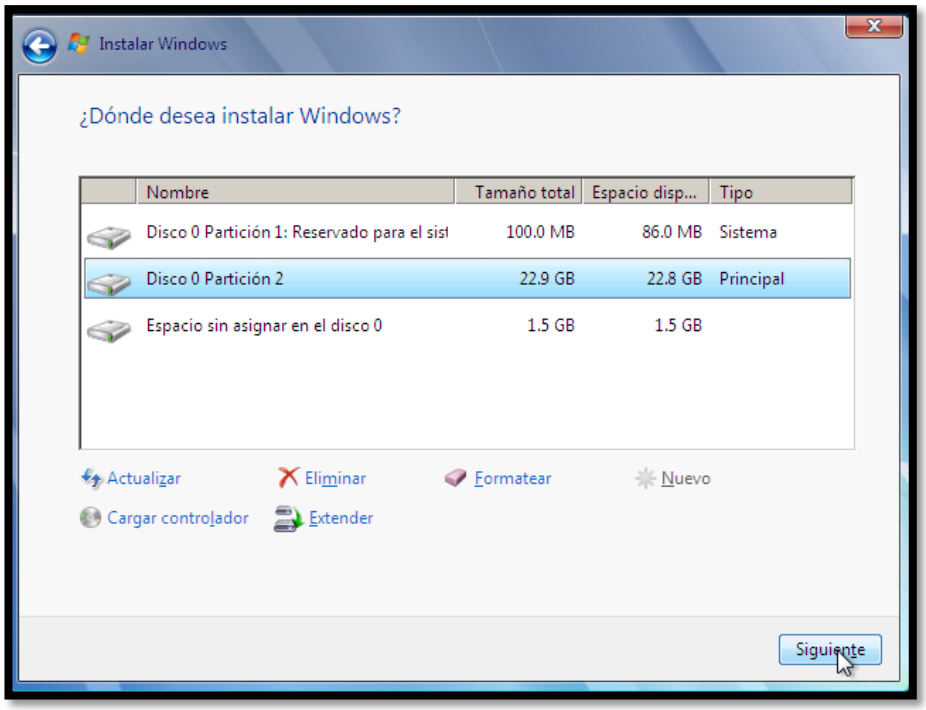
Img 102. Términos de Licencia Windows 7 – Fuente (Elaboración Propia)

Seleccionar el tipo de instalación “Personalizada (Avanzada)”.



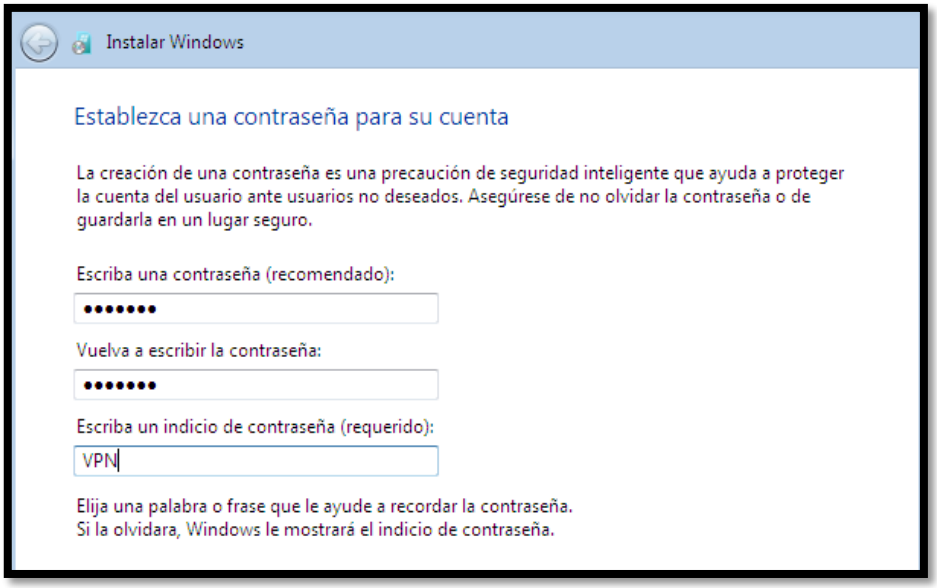
Img 103. Tipo de Instalación Windows 7 – Fuente (Elaboración Propia)

Para la instalación del sistema operativo, crear una nueva partición, para ello, seleccionar “Opciones de unidad”, nuevo, asignar tamaño y aplicar.



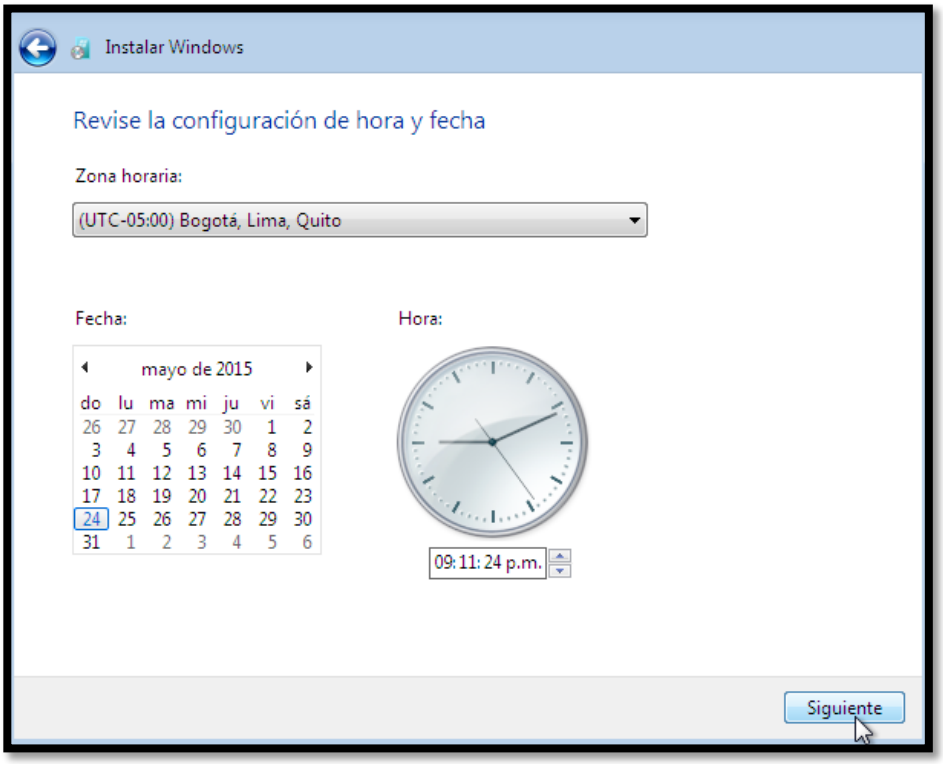
Img 104. Partición Asignada para Windows 7 – Fuente (Elaboración Propia)

Esperar a que el sistema operativo se instale, asignar un nombre de usuario y nombre de equipo a la máquina de escritorio del cliente, se recomienda colocar el nombre de la persona que hará uso de la máquina en los campos de nombre de usuario y nombre del equipo. Seguidamente asignar una contraseña a la cuenta del cliente, de preferencia utilizar letras mayúsculas, minúsculas, números.



Img 105. Asignación de contraseña a la máquina del cliente – Fuente (Elaboración Propia)

Configurar la fecha – hora y la zona horaria.



Img 106. Configuración de Fecha, Hora y Zona Horaria – Fuente (Elaboración Propia)

Finalmente indicar la contraseña anteriormente establecida para el inicio de sesión.

ANEXO 7 : PRUEBA ALFA DE CRONBACH

	# Preguntas	Alternativas	CANTIDAD DE TRABAJADORES (1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68)	TOTAL	0 al 5	
				TOTAL DE 0 AL 5	VARIANZA (Vi)
PERSONAL ADMINISTRATIVO (68)	ITEM 1	si	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	68	5	0.00
		no	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0	0	0.00
	ITEM 2	si	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0	0	0.00
		no	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	68	5	0.00
	ITEM 3	si	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	68	5	0.00
		no	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0	0	0.00
	ITEM 4	Acuerdos	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	39	3	0.24
		Monto economico	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	16	1	0.18
		Agenda	1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	10	1	0.13
		Otros	1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3	0	0.04
	ITEM 5	si	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	39	3	0.24
		no	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	29	2	0.24
	ITEM 6	si	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0	65	5	0.04
		no	1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3	0	0.04
					1.17

0 5 68 100%

DONDE:

k	numero de items
Vi	varianzas individual
Vt	varianza total (0 al 5)

seccion 1 seccion 2

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

k	6
Suma Vi	1.17
Vt	4.4

seccion 1	1.2
seccion 2	0.7

ALFA DE CRONBACH	0.88