UNIVERSIDAD NACIONAL DE LOJA

PFC

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

---

CARRERA DE INGENIERÍA EN SISTEMAS

"Implementación de Active Directory aplicando el estándar 802.1x, dentro de la red LAN y WLAN de la Universidad Nacional de Loja"

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO
DE INGENIERO EN SISTEMAS

Autores, compilación y revisión:

- Lenin Sebastián Ocampo Vélez
- Henry Paúl Vivanco Encalada
- Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.

Autorizado por:

- Torres-Carrión, Hernán-Leonardo, Coordinador de la Carrera CIS

Fecha de actualización:

- 17 de julio de 2015

LOJA-ECUADOR
2015

Certificación del Director

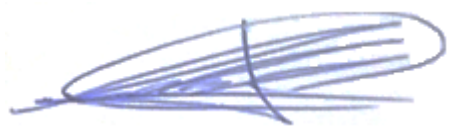
Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.
DOCENTE DE LA CARRERA DE INGENIERIA EN SISTEMAS, DEL ÁREA DE LA ENERGIA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, DE LA UNIVERSIDAD NACIONAL DE LOJA.

CERTIFICA:

Haber asesorado y revisado detenida y minuciosamente durante todo su desarrollo, el proyecto de fin de carrera titulado: **"IMPLEMENTACIÓN DE ACTIVE DIRECTORY APLICANDO EL ESTÁNDAR 802.1x, DENTRO DE LA RED LAN Y WLAN DE LA UNIVERSIDAD NACIONAL DE LOJA".** Realizado por los postulantes Lenin Sebastián Ocampo Vélez y Henry Paúl Vivanco Encalada.

Por lo tanto, autorizo proseguir los trámites legales pertinentes para su presentación y defensa

Loja, Julio 2015



Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.
DIRECTOR DE TESIS

Autoría

Nosotros, **LENIN SEBASTIÁN OCAMPO VÉLEZ** y **HENRY PAÚL VIVANCO ENCALADA**, declaramos ser autores del presente trabajo de tesis y eximimos expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente aceptamos y autorizamos a Universidad Nacional de Loja, la publicación de nuestra tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma:

Cedula: 1105668485

Fecha: 18 de Enero de 2016

Firma:

Cedula: 1105163875

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DE LOS AUTORES, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO

Nosotros, **LENIN SEBASTIÁN OCAMPO VÉLEZ** y **HENRY PAÚL VIVANCO ENCALADA**, declaramos ser autores de la tesis titulada: **"IMPLEMENTACIÓN DE ACTIVE DIRECTORY APLICANDO EL ESTÁNDAR 802.1x, DENTRO DE LA RED LAN Y WLAN DE LA UNIVERSIDAD NACIONAL DE LOJA"**, como requisito para optar el grado de: **INGENIERO EN SISTEMAS**; autorizamos al Sistema Bibliotecario de la Universidad Nacional de Loja, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido, de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dieciocho días del mes de enero del dos mil dieciséis.

Firma:
Autor: Lenin Sebastián Ocampo Vélez.
Cédula: 1105668485
Dirección: Loja (Pasaje Sinchona y Azuay)
Correo Electrónico: lsocampov@unl.edu.ec.
Teléfono: 2576759 **Celular:** 0980326712

Firma:
Autor: Henry Paúl Vivanco Encalada.
Cédula: 1105163875.
Dirección: Loja (Perú y Sevilla de Oro.)
Correo Electrónico: hpvivancoe@unl.edu.ec
Teléfono: 2565983 **Celular:** 0984087221

DATOS COMPLEMENTARIOS

Director de Tesis:	Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.
Tribunal de Grado:	Ing. Hernán Leonardo Torres Carrión, Mg. Sc.
	Ing. Mario Enrique Cueva Hurtado, Mg. Sc.
	Ing. Ángel José Ordoñez Mendieta, Mg. Sc.

Agradecimiento

Al culminar el presente proyecto de tesis, expresamos nuestro agradecimiento especial a Dios, nuestras familias y seres queridos, y un agradecimiento especial a la Universidad Nacional de Loja, por haber abierto sus puertas con el fin de llevar nuestros estudios universitarios.

Un agradecimiento especial a nuestro Directo de Tesis, Ing. Carlos Miguel Jaramillo Castro, por su dedicación, responsabilidad, apoyo y sabias orientaciones, que han permitido culminar con éxito el presente proyecto de tesis.

Así mismo agradecemos a todo el personal que labora en la Dirección de Telecomunicaciones e Información, quienes aportaron con la información y conocimientos necesarios, que permitieron el avance y culminación del proyecto de tesis.

Dedicatoria

El presente proyecto de tesis, va dedicado especialmente a Dios y a nuestras familias que con su apoyo incondicional hemos logrado la culminación del mismo. De la misma manera a todas aquellas personas que de una u otra manera supieron motivarnos y darnos fuerzas para avanzar y lograr culminar con éxito nuestro proyecto de tesis, y por ende nuestros estudios superiores.

Una dedicatoria especial a todos aquellos profesionales, docentes de la carrera de Ingeniería en Sistemas, y ajenos a la misma, quienes con su experiencia y conocimientos sobre el tema, supieron guiarnos para el correcto desarrollo del proyecto de titulación.

A todos y cada uno de ellos gracias sinceras.

Lenin Sebastián Ocampo Vélez

Henry Paúl Vivanco Encalada

AUTORES

1. Título

IMPLEMENTACIÓN DE ACTIVE DIRECTORY APLICANDO EL ESTÁNDAR 802.1X, DENTRO DE LA RED LAN Y WLAN DE LA UNIVERSIDAD NACIONAL DE LOJA

2. Resumen

El proyecto de titulación está basado en la implementación de Active Directory aplicando el estándar de seguridad 802.1x en la red LAN y WLAN de la Universidad Nacional de Loja, con el fin de tener un mecanismo de autenticación para los usuarios que hacen uso de la red de datos de la institución, evitando así diversos problemas en la red; como, uso de la red por personas ajenas a la institución, perdidas de direcciones IP, ataques a servidores de la institución, entre los principales.

Para el correcto desarrollo del proyecto, fue necesario el uso de una metodología propia, la cual consta de cuatro fases cada una de ellas con varios puntos o ítems a cumplir.

En cuanto a procedimientos, fueron necesarias varias técnicas, como entrevistas; una de las principales, se la realizó a la persona encargada de la gestión de redes en la institución, así mismo se realizó entrevistas necesarias para conocimientos de diversos temas en cuantos al manejo, diseño y administración de la red. Se practicó la observación directa y conversaciones personales con diversas autoridades de la institución.

Para la implementación de Active Directory, fue necesario el levantamiento del sistema operativo Windows Server 2012, el mismo que cuenta con licenciamiento, adquirido por parte de la Dirección de Telecomunicaciones e Información, fue necesaria también la configuración de equipos de red, tanto AP's como Switch's, los cuales cumplen la función de autenticador dentro de la red de la institución. Para hacer uso del estándar de seguridad fue necesario el levantamiento de un servidor RADIUS.

Culminando con éxito el proyecto de titulación.

ABSTRACT

This draft is based on qualifications deploying Active Directory using standard 802.1X security on the LAN and WLAN at the National University of Loja. In order to obtain an authentication mechanism for each of the people who use the data network of the institution, thus avoiding various network problems, problems such as addresses IP's losses, attacks on servers of the institution among the main ones.

For the correct development of the aforementioned project it was necessary to use a methodology which consists of four stages each with several points or items to deliver.

As to procedures for project development, various techniques were necessary, such as interviews, a major he's performed the person in charge of network management at the university, also interviews necessary knowledge of various subjects was conducted in few handling, design and network management. Direct observation and personal conversations with various officials of the institution was also performed.

To install the tool, Active Directory, it was necessary to lift the Windows Server 2012 operating system, the same that has acquired licensing by the Telecommunications and Information Unit, configuring network equipment, equipment was needed as well AP's Switch's which are the main provider on the institution. To use the security standard was necessary to create a RADIUS server client.

Successfully completing our graduation project.

Índice

Índice de Figuras

Índice de Tablas

3. Introducción

Las instituciones educativas de nivel superior en Ecuador, y a nivel mundial, han experimentado los grandes cambios tecnológicos que ha sufrido el planeta, por ende contar con una estructura de red basada en las nuevas tecnologías que permita ofrecer a las entidades investigadoras, la posibilidad de enlazar conocimientos con el mundo, es de vital importancia, y de esta manera optimizar sus niveles académicos.

Estos cambios no solo han afectado a las instituciones académicas de nivel superior, sino también a un considerable número de empresas que demandan de la tecnología para poder seguir ampliando sus mercados y mejorando la calidad de servicio. Con ello surgen diversos problemas como: robo de información, acceso ilegal a los recursos tecnológicos y a la intranet, ataques a la infraestructura de red, entre otros. Mostrando así las vulnerabilidades dentro de empresas e instituciones.

Esto ha hecho que surjan nuevos métodos para el acceso o conexión a la red, y así tener el registro total de la información de los usuarios que acceden a la misma.

En la actualidad la Universidad Nacional de Loja cuenta con un diseño de red basado en tres capas de abstracción: acceso, distribución y core; dicha estructura de red requiere mantener un esquema organizado de usuarios, equipos y un mecanismo de autenticación cliente-servidor, que permita a los usuarios el acceso a la red; para esto existen los denominados servicios de directorio y protocolos de autenticación y autorización.

Los servicios de directorio son importantes, ya que proporcionan una manera consistente de nombrar, describir, administrar y asegurar información acerca de los usuarios o recursos tecnológicos, por lo que la implementación de Active Directory dentro de la red de la Universidad Nacional de Loja es considerada como una solución de productividad.

Uno de los principales controles que se realiza en muchas empresas o instituciones para el acceso del personal a la red, es la autenticación y autorización de usuarios utilizando tecnologías adaptables a sus necesidades.

Siendo este un requerimiento que presenta actualmente la red de la Universidad Nacional de Loja, convirtiéndose así un factor de trascendencia.

Con estos antecedentes de la realidad mundial tecnológica y mecanismos para la mejora de la seguridad de la información, en la Universidad Nacional de Loja, que es una institución de Educación Superior, autónoma, de derecho público, con personal jurídico y sin fines de lucro, de alta calidad académica y humanística, es de gran necesidad pensar en la **IMPLEMENTACIÓN DE ACTIVE DIRECTORY APLICANDO EL ESTÁNDAR 802.1x, DENTRO DE LA RED LAN Y WLAN DE LA UNIVERSIDAD NACIONAL DE LOJA**, teniendo en consideración que el acceso a la intranet de la institución, debe ser controlada con un mecanismo que se adapte a sus necesidades actuales, el mismo que ayudará a manejar de manera centralizada la información de los usuarios de la red, y de esta manera mejorar la calidad de servicio a su personal académico, administrativo y colectividad en general.

4. Revisión de Literatura

Para entender mejor el contenido de este documento, a continuación, se presenta de manera breve los principales conceptos relacionados con la implementación de Active Directory como controlador de dominio, y mecanismos de seguridad para el control de acceso a red de datos.

4.1 Servicio de directorio

Un directorio es como una base de datos, pero en general contiene información más descriptiva y basada en atributos. La conclusión que se extrae de esta situación, es que el Servicio de Directorio es un conjunto complejo de componentes que trabajan de forma cooperativa para prestar un servicio. [1]

Es importante, porque proporciona una manera consistente de nombrar, describir, administrar y asegurar información acerca de dichas entidades u objetos, actuando como una capa de abstracción entre los usuarios y los recursos, en la Figura 1 se muestra los componentes de la estructura lógica de un directorio activo. [1]

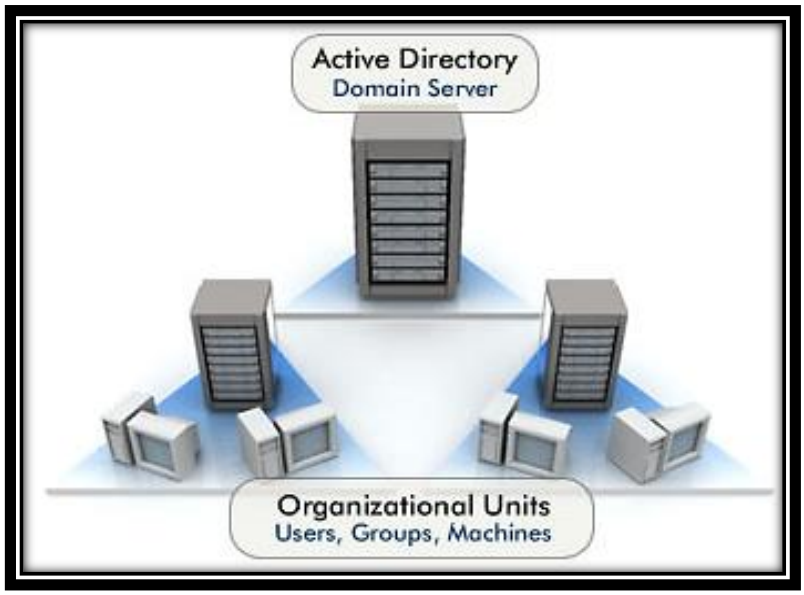


Figura 1. Estructura lógica del directorio activo

Fuente: Jessica Hidalgo (2013)

4.1.1 Protocolos de acceso

El protocolo que en sus inicios otorgaba el acceso a un directorio activo era el Protocolo de Acceso a Directorios DAP, el cual delimitaba los servicios para controlar las

comunicaciones usuario-directorio y viceversa, para que el cliente tenga acceso completo a la información del directorio.

DAP es un protocolo que resultó ser extremadamente pesado, operaba sobre el modelo OSI y requería una cantidad significativa de recursos computacionales; por lo que LDAP nació como respuesta para simplificar el acceso al directorio X.500. [2]

Por otro lado el protocolo ligero de acceso a directorios LDAP opera sobre el modelo de referencia TCP/IP, compartiendo la misma función con su antecesor DAP, cuya ventaja radica en el uso de una menor cantidad de recursos, haciéndolo más viable a la hora de poner en producción un directorio.

LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente. [3]

4.1.2 Software de servicios de directorio

Algunos de los servicios de directorio ofrecidos por los fabricantes son:

- Active Directory para Windows 2000 hasta 2012.
- Apple Open Directory en Mac OS X Server.
- Novell Directory Services (NDS).
- OpenLDAP.
- 389 Directory Server.
- Sun Directory Services.

4.2 Active Directory

Un directorio representa una estructura jerárquica que almacena información acerca de los objetos existentes en la red. Active Directory, proporciona métodos para almacenar los datos del directorio y ponerlos a disposición de los administradores y los usuarios de la red. Por ejemplo, Active Directory almacena información acerca de las cuentas de usuario (nombres, contraseñas, números de teléfono, etc.) y permite que otros usuarios autorizados de la misma red, tengan acceso a esa información, en la Figura 2 se muestra la estructura de Active Directory. [4]

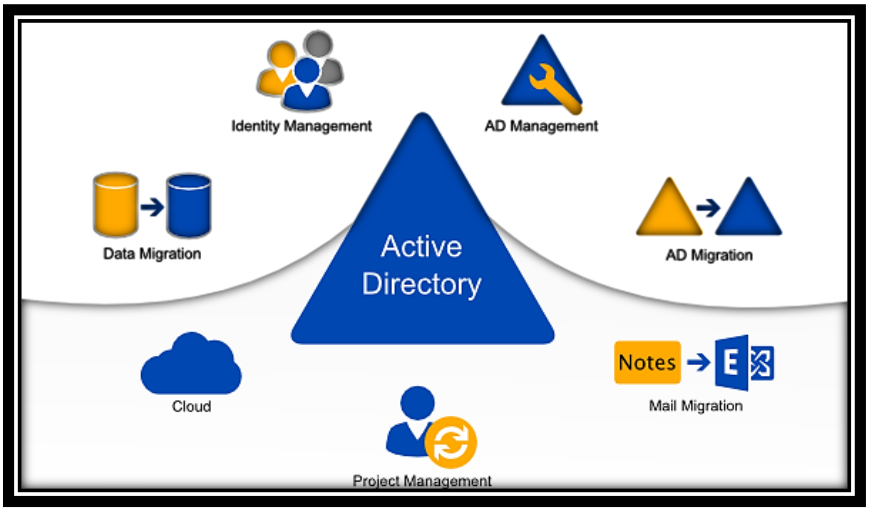


Figura 2. Estructura de Active Directory

Fuente: Jessica Hidalgo (2013)

4.2.1 Estructura lógica

Active Directory como característica global, brinda seguridad ante el almacenamiento de la información de sus clientes, los mismos que representan entidades u objetos dentro de la estructura lógica, En la Figura 3 se muestran los componentes de dicha estructura.

La estructura lógica de Active Directory comprende los siguientes componentes:

a. Objetos

Son los componentes más básicos de la estructura lógica. Cada clase de objetos se define mediante un grupo de atributos, que definen los posibles valores que se pueden asociar a un objeto. Cada objeto posee una única combinación de valores de atributos. [5]

b. Unidades organizativas

Se pueden utilizar estos objetos contenedores para estructurar otros objetos de modo que admitan los propósitos administrativos. Mediante la estructuración de los objetos por unidades organizativas, se facilita su localización y administración. También se puede delegar la autoridad para administrar una unidad organizativa. Las unidades organizativas pueden estar anidadas en otras unidades organizativas, lo que simplifica la administración de objetos. [5]

c. Dominios

Se trata de las unidades funcionales centrales en la estructura lógica de Active Directory que son un conjunto de objetos definidos de forma administrativa y que comparten una base de datos, directivas de seguridad y relaciones de confianza comunes con otros dominios. Los dominios proporcionan un límite administrativo para objetos, un medio de administración de la seguridad para recursos compartidos, una unidad de replicación para objetos. [5]

d. Árboles de dominios

Los dominios que están agrupados en estructuras jerárquicas se denominan árboles de dominios. Al agregar un segundo dominio a un árbol, se convierte en secundario del dominio raíz del árbol. El dominio al que está adjunto un dominio secundario se denomina dominio primario. Un dominio secundario puede tener a su vez su propio dominio secundario. El nombre de un dominio secundario se combina con el nombre de su dominio primario para formar su propio nombre único de Sistema de nombres de dominio (DNS, Domain Name System), como corp.nwtraders.msft. De esta forma, el árbol dispone de un espacio de nombres contiguo. [5]

e. Bosques

Un bosque es una instancia completa de Active Directory y consta de uno o varios árboles. En un árbol de sólo dos niveles, que se recomienda para la mayoría de las organizaciones, todos los dominios secundarios se convierten en secundarios del dominio raíz de bosque para formar un árbol contiguo.

El primer dominio del bosque se denomina dominio raíz de bosque. El nombre de ese dominio se refiere al bosque, como por ejemplo nwtraders.msft. De forma predeterminada, la información de Active Directory se comparte sólo dentro del bosque. De este modo, el bosque es un límite de seguridad para la información contenida en la instancia de Active Directory. Cada árbol de un bosque tiene su propio nombre de espacio único. [5]

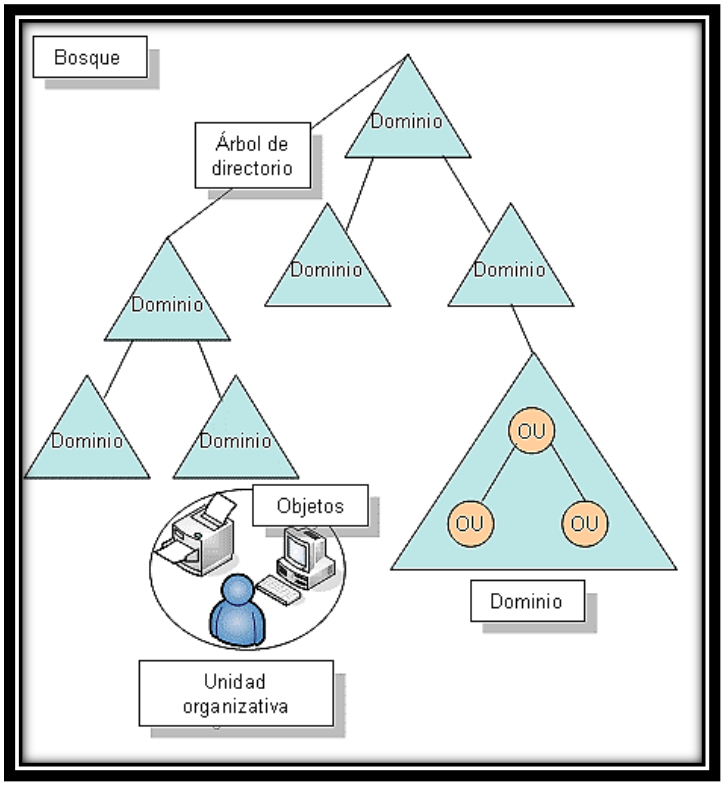


Figura 3. Estructura lógica de Active Directory

Fuente: Eduardo J (2013)

4.2.2 Estructura física

Se necesita entender los componentes de la estructura física del Directorio Activo, para tener un enfoque claro sobre cómo establecer y gestionar el tráfico de red.

En la Figura 4 se puede apreciar los componentes que integran la estructura física de Active Directory, los mismos que se describen a continuación:

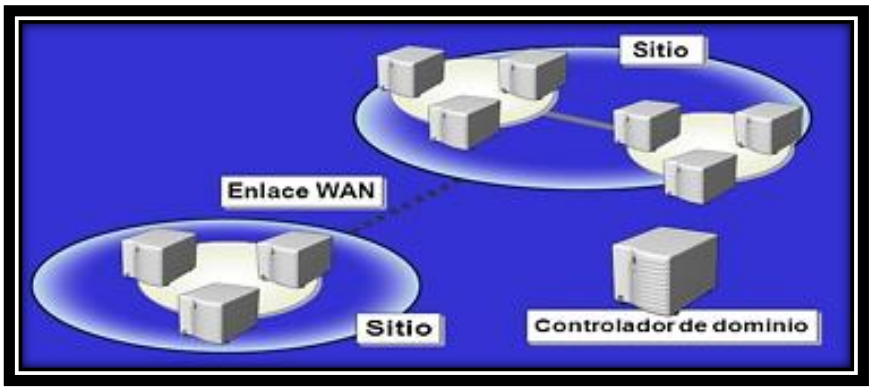


Figura 4. Estructura física de Active Directory

Fuente: Julián Blázquez (2014)

Sitios: Determina la forma que debe replicarse la información de directorio y como debe tratarse las solicitudes de servicio de equipos los que son asignados a sitios, estos son una combinación de una o más subredes IP conectadas en enlaces de alta velocidad, las cuales constituyen una forma sencilla y eficaz para representar agrupamientos en la red. [5]

Controlador de dominio: Es un equipo que ejecuta Windows Server 2012, donde se almacena una copia del directorio, almacenan datos y administran las interacciones entre el usuario y el dominio, como los procesos de inicio de sesión, la autenticación y las búsquedas de directorio. También administra los cambios del directorio y los replica a otros controladores de dominio del mismo dominio. [5]

4.3 Políticas de grupo

Las políticas de grupo del directorio activo definen las configuraciones de grupos de usuarios y equipos, para controlar su acceso a los recursos de red. Utilizándolas se puede crear un entorno de trabajo que se adapte a las necesidades de cada usuario. [6]

Las políticas de grupo se definen de dos formas:

Configuración de equipos: Específica el proceder del sistema operativo, la apariencia del escritorio, la configuración de las aplicaciones, de seguridad y los scripts de iniciar y apagar la computadora. Se aplican cuando se inicia el sistema operativo. [6]

Configuración de usuarios: Configura información específica del usuario, tales como acceso al panel de control, la configuración de red, de escritorio, de Internet Explorer, e instalación de software, etc. Se aplica al momento en que el usuario se conecta a una computadora o a la red con su cuenta y contraseña. [6]

4.3.1 Tipos de políticas de grupo

Las políticas de grupo conceden a un administrador los permisos para establecer los requerimientos necesarios para una entidad u objeto, representada por un usuario o equipo, dichas políticas se cumplen en su totalidad.

Se pueden configurar las siguientes políticas de grupo:

Configuraciones de seguridad: Opciones para equipos locales, dominios y configuraciones de seguridad de la red. [5]

Directrices administrativas: Configuraciones basados en el registro, opciones de configuración de aplicaciones, apariencia del entorno de trabajo, y el comportamiento de los servicios del sistema. [5]

Instalación del software: Administración central de instalación de software, actualizaciones y eliminaciones. [5]

4.4 Protección de Acceso a Redes (NAP)

La Protección de acceso a redes (NAP) es una nueva tecnología incorporada en Windows Vista y Windows Server 2008. NAP incluye componentes de servidor y de cliente que permiten crear y aplicar las directivas de requisitos de mantenimiento que definen las configuraciones de software y de sistema necesarias para los equipos que se conectan a la red. Para aplicar los requisitos de mantenimiento, NAP inspecciona y evalúa el estado de los equipos cliente, limita el acceso a la red cuando se considera que los equipos cliente no cumplen los requisitos y soluciona este incumplimiento de los requisitos por parte de los equipos cliente para que tengan un acceso a la red ilimitado. NAP aplica los requisitos de mantenimiento en los equipos cliente que intentan conectarse a una red. También puede encargarse también de que se sigan cumpliendo estos requisitos mientras el equipo cliente esté conectado a la red. [7]

El cumplimiento NAP depende del método de cumplimiento que se elija. NAP se aplica a:

- Comunicaciones protegidas por el protocolo de seguridad de Internet (IPsec).
- Conexiones autenticadas mediante el estándar 802.1x del IEEE.
- Conexiones VPN.
- Configuración del Protocolo de configuración dinámica de host (DHCP).

En la Figura 5. Se muestra un modelo de ejemplo de alto nivel de Network Access Protection.

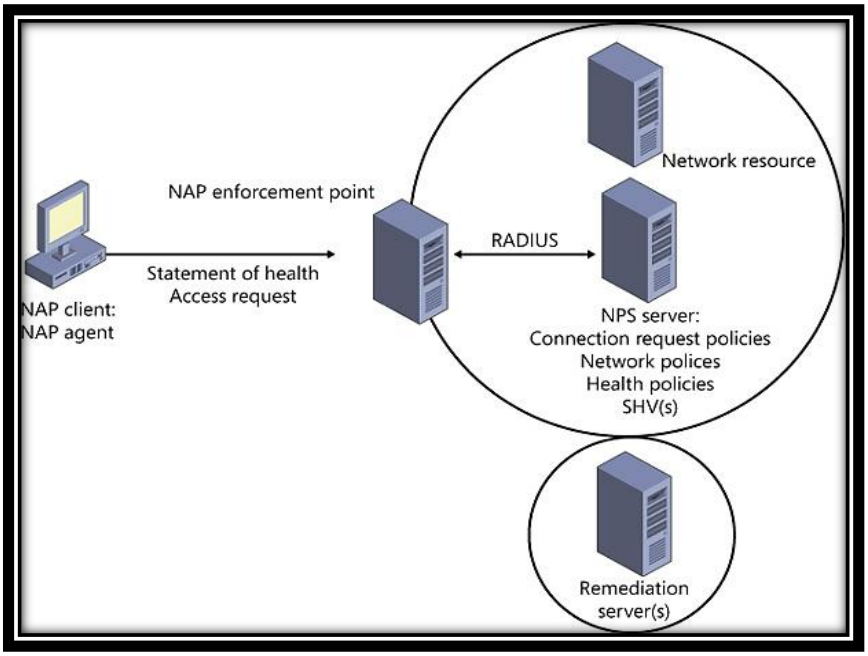


Figura 5. Modelo Network Access Protection (NAP)

Fuente: John Morello (2012)

4.5 Servidor de directivas de redes (NPS)

El Servidor de Directivas de Redes (NPS) de Windows Server 2008 permite crear y aplicar directivas de acceso a la red en toda la organización para fines de mantenimiento de clientes, autenticación y autorización de solicitudes de conexión. [7]

NPS contiene también componentes clave para implementar la Protección de Acceso a Redes (NAP) en la red, y puede implementarse como un servidor de directivas de mantenimiento de NAP. [7]

4.6 Control de acceso

El control de acceso, en sistemas de información, es la capacidad de controlar la interacción de un elemento activo (usuario, dispositivo, servicio) con un recurso informático (red de datos, sistema, servicio). [8]

Se debe tener en claro conceptos adicionales utilizados durante el control de acceso; los cuales son identificación, autenticación y autorización.

4.6.1 Identificación

La identificación es el procedimiento mediante el cual un elemento presenta su identidad a otro componente. Generalmente la identificación puede estar dada por un nombre de usuario, número de identificación o número de cuenta. [8]

4.6.2 Autenticación

Es el proceso de validar la identidad de quien accede o provee un servicio, mediante la verificación de ciertas credenciales o parámetros que debe proveer la entidad que se autentica. [8]

A continuación se describen brevemente los principales protocolos de autenticación de este tipo:

4.6.2.1 PAP (Password Authentication Protocol)

Este protocolo realiza la validación cuando se establece la conexión entre el cliente y el servidor. Utiliza el nombre de usuario y contraseña como credenciales, las cuales son enviadas en texto plano sobre el enlace, por lo que se considera un método poco seguro. [8]

4.6.2.2 CHAP (Challenge Handshake Protocol)

Provee un mejor nivel de seguridad, ya que realiza una validación de tres vías entre cliente y servidor, donde este último envía un parámetro de control a quien se autentica, este lo encripta con su contraseña y lo reenvía al servidor, donde se realiza el mismo procedimiento con la contraseña almacenada y se verifica si se obtiene el mismo resultado. [8]

4.6.2.3 EAP (Extensible Authentication Protocol)

Es un protocolo que permite elevar aún más el nivel de seguridad de la autenticación, permitiendo diversos métodos de autenticación y tipos de credenciales a utilizar. [8]

Los principales tipos de EAP son:

EAP-TLS: Realiza la autenticación estableciendo un túnel cifrado entre los elementos para proteger las credenciales y datos que se intercambian. Utiliza certificados digitales para autenticar a cliente y servidor. [8]

PEAP: Realiza la autenticación en dos fases. Primero establece una sesión TLS para autenticar al servidor y posteriormente se establece un segundo túnel para autenticar al cliente, permitiendo realizar autenticaciones de tipo de manera más segura. [8]

TTLS: También se realiza la autenticación en dos fases, utilizando una sesión de TLS para proteger la autenticación del cliente (similar a PEAP). Puede utilizar tipos de autenticación diferentes a EAP, como CHAP, MS-CHAP y otros. [8]

LEAP: Es un método de autenticación desarrollado por Cisco, que usa contraseña para autenticar al cliente. Generalmente se requiere de hardware/software Cisco para soportarlo. Adicionalmente, es susceptible a ataques de adivinación de contraseñas, y no permite autenticar equipos. [8]

4.6.3 Autorización

La autorización establece lo que un usuario puede o no hacer una vez haya sido identificado y autenticado. [8]

4.7 RADIUS (Remote Authentication Dial-In User Service)

Es un protocolo de autenticación basado en cliente y servidor que le permite a un servidor de acceso remoto comunicarse con un servidor central para poder autenticar usuarios que acceden a la red y autorizar el uso de los servicios requeridos. [8]

Este sistema, generalmente se implementa mediante software, e inicialmente su función principal fue autorizar a los usuarios de acceso conmutado (dial-in) de un proveedor de servicios de Internet (ISP) para permitir su acceso a la red pública.

4.8 Norma IEEE 802.1

La norma 802.1 describe la interrelación entre las partes del documento y su relación con el Modelo de Referencia OSI. También contiene información sobre normas de gestión de red e interconexión de redes. Establece los estándares de interconexión relacionados con la gestión de redes. [9]

En cuanto a las normas asociada a la seguridad de la red se pueden describir los siguientes protocolos:

TABLA I. PROTOCOLOS DE SEGURIDAD

Protocolo 802.1x	Protocolo 802.1AE	Protocolo 802.1AR
Seguridad basada en el puerto de control de acceso de red: Define un "puerto controlado" accesibles sólo después de la autenticación basada en EAP, y un "puerto no controlado", accesible en cualquier momento. [9]	Es el estándar de seguridad de la IEEE MAC define la confidencialidad de los datos sin conexión y la integridad de protocolos de acceso a los medios de comunicación independientes. La gestión de claves y la creación de asociaciones de seguridad están fuera del alcance de 802.1AE, pero se especifica mediante 802.1X. MAC de seguridad: Define una forma de obtener los datos sobre un individuo segmento de LAN, Integrado con el acuerdo y las funciones clave del puerto controlado / no controlado en 802.1X. [9]	Identidad del dispositivo seguro: Define único dispositivo por identificadores, permite a los mecanismos estándar para autenticar la identidad de un dispositivo y facilita el aprovisionamiento dispositivo seguro. [9]

4.8.1 Estándar de autenticación 802.1x

Este protocolo especifica el bloqueo del puerto LAN para autorizar o denegar el acceso a la red, el uso generalmente se da en redes inalámbricas.

En la implementación 802.1x se requieren, mínimo, los siguientes componentes:

- Usuario que intenta acceder a la red, o “suplicante”.
- Punto de acceso que habilita o impide el ingreso del suplicante, también llamado “Autenticador”.
- Servidor de autenticación, quien negocia y valida la identidad del suplicante; y le informa el éxito o fracaso de este proceso al autenticador para que ejecute la acción indicada. [9]

5. Materiales y Métodos

En el desarrollo del presente proyecto de titulación, se hizo uso de diferentes materiales, métodos y técnicas, y una metodología propia; los mismos permitieron la redacción y acopio de información necesaria para el desarrollo del proyecto de titulación, estos recursos se detallan a continuación:

5.1 Materiales

5.1.1 Materiales bibliográficos

- Libros.
- Internet.
- Folletos.
- Artículos Científicos.

Estos fueron fuentes de consulta, permitiendo así la obtención de conocimientos claros y precisos que sirvieron para fundamentar, argumentar y darle forma al proyecto de titulación.

5.1.2 Materiales de oficina

- Resmas de papel.
- Cartuchos de Tinta.

Los materiales de oficina, fueron adquiridos por cada uno de los integrantes del grupo de trabajo.

5.1.3 Equipo informático

- Computadores.
- Impresora.
- Disco USB.

En el desarrollo del proyecto de titulación se hizo uso de diversos equipos informáticos, los cuales son pertenecientes a cada uno de los integrantes del grupo de trabajo.

5.2 Métodos

Los principales métodos aplicados en el desarrollo del proyecto de titulación, son los siguientes:

5.2.1 Método analítico

Fue de mucha utilidad en el análisis de nuestra problemática, visualizando de manera minuciosa los inconvenientes, causas y consecuencias de la no implementación de Active Directory dentro de la red de datos de la Universidad Nacional de Loja.

5.2.2 Método científico

El uso del método científico es de vital importancia, ya que con él se realiza la recolección de conocimientos teóricos necesarios para el desarrollo del proyecto de tesis.

5.3 Técnicas

Las técnicas usadas para el desarrollo del proyecto de titulación se describen a continuación.

5.3.1 Técnica de observación

Se realizó una observación de campo, para poder apreciar los problemas que se encuentran, principalmente, en la seguridad de la red de datos de la Universidad Nacional de Loja.

5.3.2 Técnica de investigación bibliográfica

Mediante la técnica de Investigación Bibliográfica, se logró desarrollar la parte teórica del proyecto de titulación, mediante consultas en diferentes fuentes.

5.3.3 Lectura comprensiva

Se hizo uso de la lectura comprensiva, con el fin de lograr obtener conocimiento ordenado y sistemático, para con ello, poder dar posibles soluciones a los problemas planteados con anterioridad en el proyecto de titulación.

5.3.4 Entrevista

Esta técnica fue aplicada para encontrar el principal problema en red de datos de la Universidad Nacional de Loja, aplicándola a la persona encargada de la sección de Redes y Equipos Informáticos de la Dirección de Telecomunicaciones e Información; Se realizaron también, para tener conocimiento acerca de los servidores y equipos informáticos que se hallan actualmente en la institución.

5.3.5 Experimentación

Mediante la experimentación, se realizó las diferentes pruebas de funcionalidad a nivel de servidor y de estaciones de trabajo.

5.4 Metodología

Se desarrolló una metodología propia de acuerdo a cada uno de los objetivos que se plantearon en el anteproyecto.

5.4.1 Fase 1

Analizar la situación actual de la red LAN y WLAN para la implementación de Active Directory aplicando el estándar de seguridad IEEE 802.1x dentro de la Universidad Nacional de Loja.

- Estudio de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de hosts o recursos tecnológicos implementados actualmente.
- Verificación de la Infraestructura a nivel de servidores.
- Verificación de la infraestructura a nivel de estaciones de trabajo, características de funcionamiento, operatividad y limitaciones que presentan actualmente los recursos tecnológicos.

5.4.2 Fase 2

Analizar los servicios que brinda Active Directory para mejorar la seguridad y administración de los recursos tecnológicos dentro de la red LAN y WLAN de Universidad Nacional de Loja.

- Estudio de las características, ventajas y desventajas de la herramienta.
- Estudio del hardware y software de acuerdo a los requerimientos necesarios para la implementación del servidor.
- Análisis de los servicios de seguridad que brinda el estándar 802.1x.

5.4.3 Fase 3

Analizar las políticas de seguridad y privacidad necesarias para todo el personal académico y administrativo, quienes hacen uso de la red LAN y WLAN de la Universidad Nacional de Loja.

- Determinar los grupos de trabajo según la estructura jerárquica de la red de datos de la Universidad Nacional de Loja.
- Obtención de las necesidades actuales de los usuarios a nivel de servicios de la red, en procesos académicos, como administrativos que se ejecutan en la Universidad Nacional de Loja.
- Determinar las políticas de seguridad y privacidad de acuerdo a las funciones que desempeña el personal tanto académico como administrativo.

5.4.4 Fase 4

Realizar la implementación y pruebas de funcionalidad del servidor, verificando la prestación del servicio como controlador de dominio; dentro del Área de la Energía y los Recursos Naturales no Renovables de la Universidad Nacional de Loja.

- Instalación y configuración de la plataforma operativa en el servidor físico.
- Instalación y configuración de la herramienta Active Directory con las políticas de seguridad y servicios establecidos.
- Pruebas de funcionalidad a nivel de servidor como controlador de dominio.
- Pruebas de funcionalidad a nivel de estaciones de trabajo dentro del Área de la Energía y los Recursos Naturales no Renovables de la Universidad Nacional de Loja.

6. Resultados

6.1 Fase 1: Analizar la situación actual de la red LAN y WLAN para la implementación de Active Directory aplicando el estándar de seguridad IEEE 802.1x dentro de la Universidad Nacional de Loja

6.1.1 Estudio de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de hosts o recursos tecnológicos implementados actualmente

6.1.1.1 Universidad Nacional de Loja

La Universidad Nacional de Loja se encuentra ubicada, en la región sur del país, en la provincia y ciudad de Loja, Ciudadela Universitaria Guillermo Falconí Espinoza (La Argelia).

Es una institución de Educación Superior, laica, autónoma, de derecho público, con personería jurídica y sin fines de lucro, de alta calidad académica y humanística, que ofrece formación en los niveles: técnico y tecnológico superior; profesional o de tercer nivel; y, de postgrado o cuarto nivel; que realiza investigación científico-técnica sobre los problemas del entorno, con calidad, pertinencia y equidad, a fin de coadyuvar al desarrollo sustentable de la región y del país, interactuando con la comunidad, generando propuestas alternativas a los problemas nacionales, con responsabilidad social; reconociendo y promoviendo la diversidad cultural, étnica y la sabiduría popular, apoyándose en el avance científico y tecnológico, en procura de mejorar la calidad de vida del pueblo ecuatoriano.[10]

La Universidad Nacional de Loja posee en la actualidad una oferta educativa que cuenta con 35 carreras distribuidas en cinco áreas Académico-Administrativas:

- Área Jurídica Social y Administrativa.
- Área de la Educación, el Arte y la Comunicación.
- Área Agropecuaria y de Recursos Naturales Renovables.
- Área de la Energía, las Industrias y los Recursos Naturales no Renovables.

- Área de la Salud Humana.

Cuenta también con un Área Administrativa:

- Administración Central.

Además extensiones Académico-Administrativas:

- Teatro Bolívar.
- Extensión Punzara.
- Nivelación Motupe.
- Idiomas.

La institución proyecta su oferta académica a todo el territorio ecuatoriano, por medio de la Modalidad de Estudios a Distancia con nueve carreras. Oferta también un Plan de Contingencia con ocho carreras.

Mediante el convenio suscrito con la SENESCYT la Universidad Nacional de Loja implementó el curso de nivelación para los aspirantes a ingresar en las aulas universitarias.

La Universidad Nacional de Loja con la finalidad de promover profesionales que generen y apliquen conocimientos científico-técnicos, oferta en la actualidad los siguientes programas de postgrado:

- Especialización en Medicina Interna.
- Especialización en Pediatría.
- Especialización en Cirugía General.
- Especialización en Ginecología y Obstetricia.
- Especialización en Ortopedia y Traumatología.
- Especialización en Radiología e Imagen.
- Especialización en Anestesiología.

Misión

La formación académica y profesional de calidad, con sólidas bases científicas y técnicas, pertinencia social y valores; la producción y aplicación de conocimientos científicos, tecnológicos y técnicos, que aporten a la ciencia universal y a la solución de

los problemas específicos del entorno; la generación de pensamiento; la promoción, desarrollo y difusión de los saberes y culturas; la oferta de servicios especializados; y, la gestión participativa e innovadora, con personal idóneo, comprometido institucional y socialmente.[10]

Visión

La Universidad Nacional de Loja es una institución de educación superior pública y laica, abierta a todas las corrientes del pensamiento, orientadora de la conciencia social; referente fundamental para el desarrollo de la Región Sur y del País; con altos niveles de calidad, pertinencia y compromiso, reconocido prestigio nacional e internacional, por el accionar de sus profesionales en respuesta a las exigencias sociales, la generación y aplicación de conocimientos científicos y tecnológicos, el reconocimiento de los saberes y prácticas ancestrales y su permanente interacción con los sectores sociales.[10]

En la Figura 6 se puede apreciar el organigrama estructural de la Universidad Nacional de Loja, aprobado por el Sr. Rector de la institución en Abril del 2012.

Organigrama estructural de la Universidad Nacional de Loja

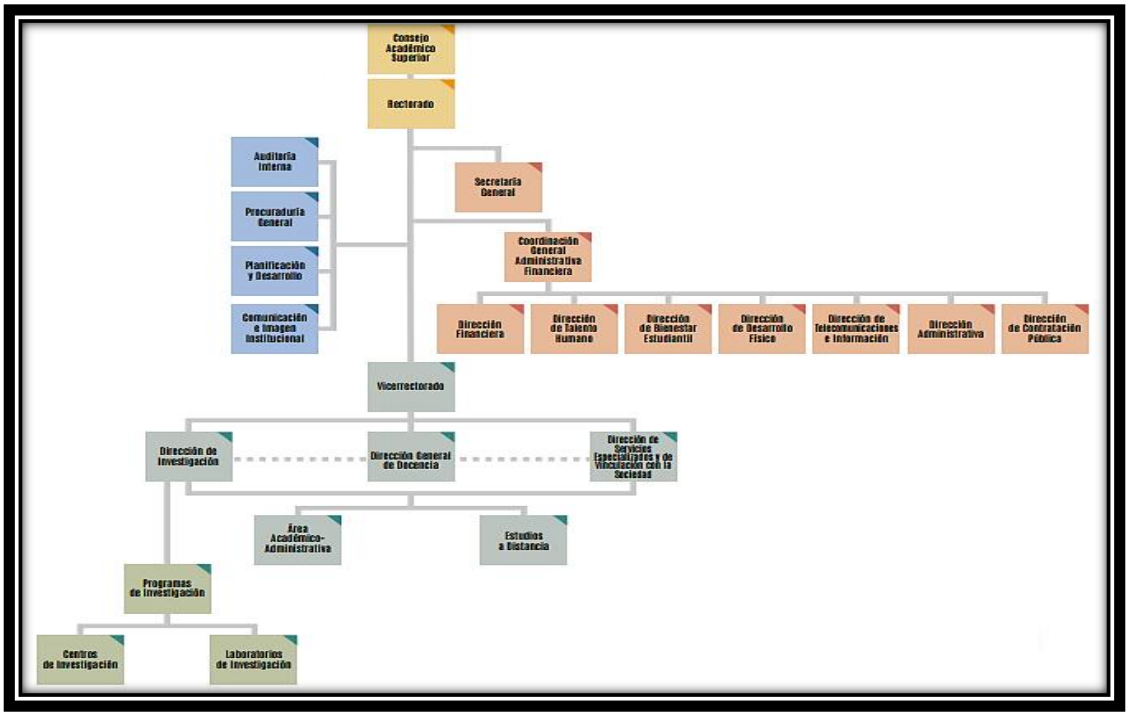


Figura 6. Organigrama estructural UNL

Fuente: Plan estratégico UNL (2012)

Dirección de Telecomunicaciones e Información

La Dirección de Telecomunicaciones e Información de la Universidad Nacional de Loja, se encuentra ubicado en el orgánico estructural, como parte de Coordinación General Administrativa-Financiera. Físicamente está ubicado en el edificio 2 de Administración Central, tercer piso.

Se define como el área de servicios que tiene como usuarios a todas las áreas de la Universidad Nacional de Loja, incluyendo la Modalidad de Estudios a Distancia (MED).

Es una de las unidades prioritarias y de gran importancia para la universidad, ya que tiene mucho que ver con el normal funcionamiento de la institución universitaria. Se encarga de la instalación de software, actualizaciones de antivirus, administración de las claves y configuración de equipos de red y de computación, tanto para el sector administrativo como académico, de toda la universidad.

La Dirección de Telecomunicaciones e Información de la institución se encuentra dirigida por el ingeniero Milton Leonardo Labanda Jaramillo como director de dicha entidad.

Los departamentos o subdirecciones existentes en la Dirección de Telecomunicaciones e Información se detallan a continuación:

- Subdirección de Redes y Equipos Informáticos.
- Subdirección de Desarrollo de Software.

En la Figura 7 se indica la organización estructural de la Dirección de Telecomunicaciones e Información, mediante un organigrama estructural.

Organigrama estructural de la Dirección de Telecomunicaciones e Información

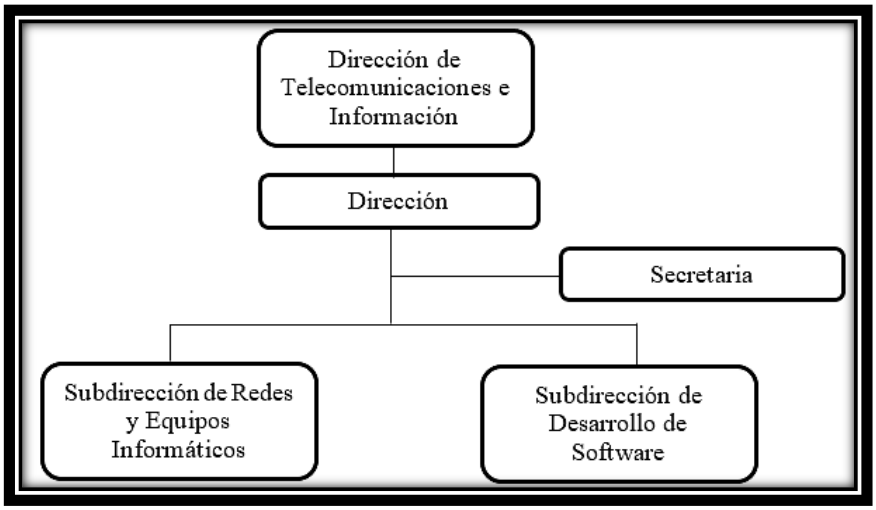


Figura 7. Organigrama estructural

Fuente: Autor

Subdirección de Redes y Equipos Informáticos

Las actividades esenciales que se realizan en la subdirección son:

- Planificar, coordinar, controlar y evaluar los estudios, diseños, implementación, construcción y mantenimiento de redes informáticas, según los requerimientos académicos y administrativos institucionales.
- Planificar, coordinar y evaluar la adquisición y/o renovación de los equipos informáticos de propiedad de la Universidad Nacional de Loja.
- Planificar, organizar, coordinar y controlar el apoyo técnico a los centros de cómputo y laboratorios informáticos de las áreas académicas y centros especializados, para garantizar el funcionamiento adecuado de sus redes y equipos informáticos.
- Planificar, organizar y coordinar el soporte técnico y el mantenimiento preventivo y correctivo a las redes y equipos de los sistemas informáticos de la Universidad Nacional de Loja.
- Coordinar la elaboración de los términos de referencia de los pliegos para la adquisición de equipos informáticos y materiales para su mantenimiento.

- Coordinar la capacitación a los usuarios internos en la operación de los equipos informáticos y TIC's, en coordinación con los responsables de las otras secciones de la unidad administrativa.

Misión

Planificar, coordinar y controlar la implementación y mantenimiento de redes informáticas; así como la renovación y mantenimiento de los equipos informáticos; para el efectivo cumplimiento de las actividades académicas y administrativas de la Universidad Nacional de Loja.

La persona responsable de la subdirección, es el Ingeniero John Alexander Calderón Sanmartín.

6.1.1.2 Red de datos

En cuanto al servicio prestado por parte de la Dirección de Telecomunicaciones e Información, destacamos varios puntos que serán indispensables para el correcto desarrollo del proyecto de titulación.

En la Universidad Nacional de Loja, existe un cuarto de equipos de red, este cuarto se encuentra ubicado en la Subdirección de Redes y Equipos Informáticos de la Dirección de Telecomunicaciones e Información, desde esta sección se administra y distribuye el internet hacia las demás áreas.

La Universidad Nacional de Loja, posee una red de datos interna, que permite la comunicación entre usuarios de la red.

El Internet llega a la Universidad Nacional de Loja a través de fibra óptica, la empresa encargada de brindar este servicio es TELCONET. El ancho de banda que posee actualmente es de 300 megas.

La estructura tecnológica actual de la Universidad Nacional de Loja es jerárquica, se ha considerado el uso de las 3 capas de red Enterprise: Acceso, Distribución y Core.

Actualmente se encuentra basada en una topología, estrella extendida, donde cada facultad y área tiene asignado un Switch de distribución y conectados a él, los Switch's de acceso, los mismos que permiten la conexión al usuario final.

En la parte inalámbrica la universidad cuenta actualmente con cuatro redes principales, las mismas que llevan el nombre de: CAMPUS UNL, UNL, EDUROAM e INVITADOS UNL.

La red de datos tanta cableada como inalámbrica se halla libre, es decir cualquier persona perteneciente o no a la institución, puede conectarse a la misma sin restricción alguna.

Para facilitar la comprensión del diagrama de redes indicado en la Figura 8, es necesario tener conocimiento de los símbolos que se emplean, para ello se debe tomar en cuenta la simbología de la TABLA II.

TABLA II. SIMBOLOGÍA PARA INTERPRETACIÓN DE DIAGRAMAS

SIMBOLO	DESCRIPCIÓN
	100baset hub
	workgroup Switch
	wireless Router
	Modem
	Need layer 3 switch network (CORE)
	L2/L3 distribution
	layer 3 switch
	workgroup switch
	Router
	layer 2 remote switch
	Firewall
	Enlace inalámbrico

Topografía física

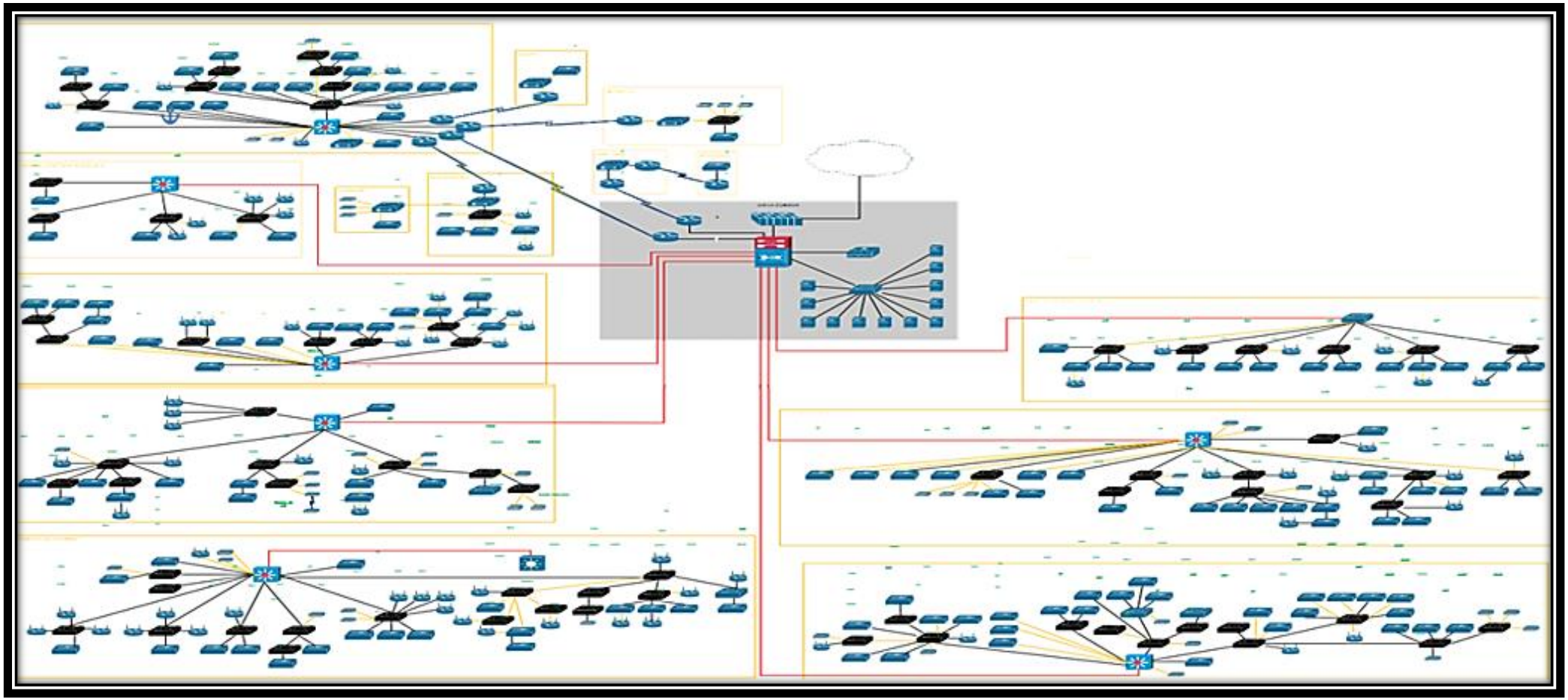


Figura 8. Topografía física

Fuente: Daniel Jiménez (2015)

Distribución de Switch’s, VLAN’s y subredes por área

La distribución de Switch’s se la realiza de manera unificada, etiquetando los mismos dependiendo como se hallen ubicados y conectados, existe una clasificación por cada área de la institución como primer nivel de categorización, en el segundo nivel se especifica el número de bloque, dependiendo de la organización de cada área y como tercer nivel el número de piso de cada bloque o edificio.

Área de la Salud

- Bloque 1: Aula Virtual, Piso 2; Bloque 2: Laboratorios Piso 3; Bloque 3: Bodega Piso 1,

Administración Central

- Bloque 1: Piso1, Piso 2, Piso 3, Piso 4; Bloque 2: Piso1, Piso 2, Piso 3, Piso 4.

Área de la Energía

- Bloque 2: Piso 1; Bloque 3: Piso 1; Bloque 8: Piso 1; Bloque 7: Piso 1, Piso 2.

Área Educativa

- Bloque 1: Piso 1, Piso 2, Piso 3; Bloque 3: Piso 1; Bloque 6: Piso 1; Bloque 7: Piso 1, Piso 2, Bloque 8: Piso 1, Piso 2, Bloque 11: Piso 1, Piso 2, Bloque 9: Piso 1, Piso 2.

Área Jurídica

- Bloque 6: Piso 1, Piso 2; Bloque 5: Piso 2; Bloque 4: Piso 2; Bloque 2: Piso 2; Bloque 4: Piso 1; Bloque 12: Piso 2.

Área Agropecuaria

- Bloque 8: Piso 1; Bloque 12: Piso 1; Bloque 24: Piso 2, Piso 3; Bloque 20: Piso 1; Bloque 7: Piso 1; Bloque 10: Piso 2; Bloque 1: Piso 1; Bloque 23: Piso 1, Piso 2, Piso 3; Bloque 7: Piso 1.

La distribución de VLAN's y subredes pertenecientes a cada área de conexión se encuentra distribuida de la siguiente manera.

En cada área de la institución se maneja, un swicth administrable L3 de distribución que replica las configuraciones de las VLAN's manejadas actualmente en la institución, las áreas comprendidas son:

Área de la Salud

TABLA III. DISTRIBUCIÓN DE PUERTOS SALUD: SW-L3-SALUD_1.0

Item	Vlan ID	Descripción	Red	Gateway/SVI	Rango DHCP
1	Vlan 1	Maludnagment	X.X.81.X	X.X.81.X	N/A
2	RESERVA	RESERVA	X.X.82.X	X.X.82.X	X.X.82.X
3	Vlan 20	Profesores	X.X.83.X	X.X.83.X	X.X.83.X
4	Vlan 30	Estudiantes	X.X.84.X	X.X.84.X	X.X.84.X
5	Vlan 40	Voz IP	X.X.85.X	X.X.85.X	X.X.85.X
6	Vlan 50	Biometrico/Impresoras	X.X.86.X	X.X.86.X	X.X.86.X
7	Vlan 60	Cámaras	X.X.87.X	X.X.87.X	X.X.87.X
8	Vlan 70	Laboratorios	X.X.88.X	X.X.88.X	X.X.88.X
9	Vlan 10	Administrativo	X.X.89.X	X.X.89.X	X.X.89.X
10	Vlan 200	Default Linksys	X.X.90.X	X.X.90.X	X.X.90.X
11	Vlan 120	Biblioteca	X.X.91.X		
12	RESERVA	RESERVA	X.X.92.XX		

Administración Central

TABLA IV. DISTRIBUCIÓN DE PUERTOS ADMINISTRACIÓN CENTRAL BLOQUE 1: SW-L3-ADMCENTRAL-B1_1.0

Item	Vlan ID	Descripción	Red	Gateway/SVI	Rango DHCP
1	Vlan 1	Managment	X.X.17.X	X.X.17.X	N/A
2	RESERVA	RESERVA	X.X.18.X	X.X.18.X	X.X.18.X
3	Vlan 20	Profesores	X.X.19.X	X.X.19.X	X.X.19.X
4	Vlan 30	Estudiantes	X.X.20.X	X.X.20.X	X.X.20.X
5	Vlan 40	Voz IP	X.X.21.X	X.X.21.X	X.X.21.X
6	Vlan 50	Biométrico/Impresoras	X.X.22.X	X.X.22.X	X.X.22.X
7	Vlan 60	Cámaras	X.X.23.X	X.X.23.X	X.X.23.X
8	Vlan 70	Laboratorios	X.X.24.X	X.X.24.X	X.X.24.X
9	Vlan 10	Administrativo	X.X.25.X	X.X.25.X	X.X.25.X
11	Vlan 200	Default Linksys-Dlink	X.X.26.X	X.X.26.X	X.X.26.X
12	Vlan 120		X.X.27.X		
13	RESERVA	RESERVA	X.X.28.X		

Área de la Energía

TABLA V. DISTRIBUCIÓN DE PUERTOS ENERGÍA: SW-L3-ENERGIA_1.0

Item	Vlan ID	Descripción	Red	Gateway/SVI	Rango DHCP
1	Vlan 1	Managment	X.X.1.X	X.X.1.X	N/A
2	RESERVA	RESERVA	X.X.2.X	X.X.2.X	X.X.2.X
3	Vlan 20	Profesores	X.X.3.X	X.X.3.X	X.X.3.X
4	Vlan 30	Estudiantes	X.X.4.X	X.X.4.X	X.X.4.X
5	Vlan 40	Voz IP	X.X.5.X	X.X.5.X	X.X.5.X
6	Vlan 50	Biometrico/Impresoras	X.X.6.X	X.X.6.X	X.X.6.X
7	Vlan 60	Cámaras	X.X.7.X	X.X.7.X	X.X.7.X
8	Vlan 70	Laboratorios	X.X.8.X	X.X.8.X	X.X.8.X
9	Vlan 10	Administrativo	X.X.9.X	X.X.9.X	X.X.9.X
10	Vlan 200	Default Linksys-Dlink	X.X.10.X	X.X.10.X	X.X.10.X
11	Vlan 120	Biblioteca	X.X.11.X		
12	RESERVA	RESERVA	X.X.12.X		

Área Educativa

TABLA VI. DISTRIBUCIÓN DE PUERTOS EDUCATIVA: SW-L3-EDUCACTIVA_1.0

Item	Vlan ID	Descripción	Red	Gateway/SVI	Rango DHCP
1	Vlan 1	Managment	X.X.145.X	X.X.145.X	N/A
2	RESERVA	RESERVA	X.X.146.X	X.X.146.X	X.X.146.X
3	Vlan 20	Profesores	X.X.147.X	X.X.147.X	X.X.147.X
4	Vlan 30	Estudiantes	X.X.148.X	X.X.148.X	X.X.148.X
5	Vlan 40	Voz IP	X.X.149.X	X.X.149.X	X.X.149.X
6	Vlan 50	Biométrico	X.X.150.X	X.X.150.X	X.X.150.X
7	Vlan 60	Cámaras	X.X.151.X	X.X.151.X	X.X.151.X
8	Vlan 70	Laboratorios	X.X.152.X	X.X.152.X	X.X.152.X
9	Vlan 10	Administrativo	X.X.153.X	X.X.153.X	X.X.153.X
10	Vlan 200	Linksys-Dlink	X.X.154.X	X.X.154.X	X.X.154.X
11	Vlan 120	Biblioteca	X.X.155.X		
12	RESERVA	RESERVA	X.X.156.X		

Área Jurídica

TABLA VII. DISTRIBUCIÓN DE PUERTOS BLOQUE 10 JURÍDICA: SW-L3-B10-JURIDICA_1.0

Item	Vlan ID	Descripción	Red	Gateway/SVI	Rango DHCP
1	Vlan 1	Managment	X.X.129.X	X.X.129.X	N/A
2	RESERVA	RESERVA	X.X.130.X	X.X.130.X	X.X.130.X
3	Vlan 20	Profesores	X.X.131.X	X.X.131.X	X.X.131.X

4	Vlan 30	Estudiantes	X.X.132.X	X.X.132.X	X.X.132.X
5	Vlan 40	Voz IP	X.X.133.X	X.X.133.X	X.X.133.X
6	Vlan 50	Biométrico	X.X.134.X	X.X.134.X	X.X.134.X
7	Vlan 60	Cámaras	X.X.135.X	X.X.135.X	X.X.135.X
8	Vlan 70	Laboratorios	X.X.136.X	X.X.136.X	X.X.136.X
9	Vlan 10	Administrativo	X.X.137.X	X.X.137.X	X.X.137.X
10	Vlan 200	Linksys-Dlink	X.X.138.X	X.X.138.X	X.X.138.X
11	Vlan 120	Biblioteca	X.X.139.X		
12	RESERVA	RESERVA	X.X.140.X		

Área Agropecuaria

TABLA VIII. DISTRIBUCIÓN DE PUERTOS AGROPECUARIA: SW-L3-AGROPECUARIA_1.0

Item	Vlan ID	Descripción	Red	Gateway/SVI	Rango DHCP
1	Vlan 1	Managment	X.X.65.X	X.X.65.X	N/A
2	RESERVA	RESERVA	X.X.66.X	X.X.66.X	X.X.66.X
3	Vlan 20	Profesores	X.X.67.X	X.X.67.X	X.X.67.X
4	Vlan 30	Estudiantes	X.X.68.X	X.X.68.X	X.X.68.X
5	Vlan 40	Voz IP	X.X.69.X	X.X.69.X	X.X.69.X
6	Vlan 50	Biometrico/Impresoras	X.X.70.X	X.X.70.X	X.X.70.X
7	Vlan 60	Cámaras	X.X.71.X	X.X.71.X	X.X.71.X
8	Vlan 70	Laboratorios	X.X.72.X	X.X.72.X	X.X.72.X
9	Vlan 10	Administrativo	X.X.73.X	X.X.73.X	X.X.73.X
10	Vlan 100	Default Linksys-Dlink	X.X.74.X	X.X.74.X	X.X.74.X
11	Vlan 120	Biblioteca	X.X.75.X		
12	RESERVA	RESERVA	X.X.76.X		

Topología lógica

La topología lógica se halla dada por medio de segmentación o VLAN's, las cuales permiten crear redes lógicas independientes dentro de una misma red física.

Estas son útiles para reducir el tamaño del dominio de difusión, y ayudan en la administración de la red, separando segmentos lógicos de una red de área local, que no deberían intercambiar datos usando la red local.

Equipos

Figura 9. Cuarto de máquinas

Fuente: Autor

En el cuarto de máquinas, que se halla ubicado en un espacio de la Dirección de Telecomunicaciones e Información, se encuentran 3 armarios o RACK's como se muestra en la Figura 9, de los cuales 2 de ellos se destinan directamente a servidores.

Mientras que, en el RACK número 03, existen diferentes equipos destinados a brindar internet a la comunidad universitaria, entre estos equipos se hallan:

UPS's

Dos equipos UPS de marca POWERCOM, los cuales son los encargados de almacenar energía en sus baterías para ser usada al momento de tener fallas eléctricas o escases de energía en la universidad, evitando así perdida de servicio.

Router Cisco

Este equipo permite la interconexión con internet. El manejo de este equipo es de uso exclusivo del proveedor de internet para la universidad es decir TELCONET.

Switch Cisco

Existen tres equipos Cisco, en uno de ellos se hallan conectados los servidores internos de la Dirección de Telecomunicaciones.

En el otro equipo están conectados los servidores públicos para la Universidad Nacional de Loja, servidores como:

- Servidor WEB.

- Servidor para la Radio Universitaria.
- Servidor DNS.

El tercer equipo se encuentra destinado únicamente al Firewall que maneja la universidad.

Switch Cisco Wireless Controller

Se encuentra destinado a la interconexión de las redes inalámbricas que alberga la institución, realizando así el control de estas redes.

Las redes inalámbricas que abarca la controladora son: UNL, CAMPUS UNL, EDUROAM e INVITADOS UNL.

Cisco Systems

Es el equipo principal proveedor de internet para toda la universidad, es conocido como Switch CORE, del mismo se hallan ramificaciones conectadas a Switch's de distribución en toda la institución.

Estos son los principales equipos que se hallan dentro del cuarto de máquinas, fuera del mismo, en toda la universidad se hallan diversos armarios o RACK's, en ellos se hallan los Switch's de distribución.

Para las conexiones de acceso se tiene diversos Switch's Dlink, principalmente, mientras para las conexiones inalámbricas se la hace atreves de Puntos de Acceso (AP) Cisco.

Todos los equipos implementados son configurados de manera uniforme, además los equipos Cisco de distribución cuentan con el estándar de seguridad 802.1x.

6.1.2 Verificación de la infraestructura a nivel de servidores

En el cuarto de máquinas de la Dirección de Telecomunicaciones e Información, los RACK's o armarios 04 y 02 son destinados a los servidores de la Universidad Nacional de Loja.

En el RACK 04 se halla el BLADE el mismo que está distribuido físicamente de la siguiente manera:

- 24 Cuchillas de 450 Gb.
- 8 Cuchillas de 146 Gb.
- 4 Cuchillas de 306 Gb.

En el BLADE existe un porcentaje estimado del 70% disponible del total de su capacidad.

En el RACK 02 existen tres CPU's destinados como servidores.

Los servidores que se encuentran abarcados en la Universidad Nacional de Loja son:

6.1.2.1 Firewall

Permite tener la barrera entre la red pública y la red privada de datos, aquí constan las reglas que optimizan el uso del internet en la Universidad Nacional de Loja.

Las características principales del Firewall son:

- Sistema Operativo Linux.
- Intel(R) Xeon (TM) CPU 3.2GHz.
- Memoria 1 Gb.
- Disco 160 Gb.

6.1.2.2 Servidor web

En el servidor Web se encuentra la página web de la Universidad Nacional de Loja. La cual brinda servicio de información, dentro de cada una de las áreas que abarca la universidad, en la misma constan sistemas de: matriculación, desempeño de los docentes, entro otros sistemas más.

Las características principales del servidor se describen a continuación:

- Sistema Operativo Linux.
- Intel(R) Xeon (TM) CPU 3.2GHz.
- Memoria 1 Gb.
- Disco 160 Gb.

6.1.2.3 Servidor moodle

Es utilizado para brindar servicio de educación a distancia vía internet. De igual manera, como el servidor web, permite matriculación e información respecto a la educación a distancia y cursos de la misma índole, cursos tanto de inglés como de educación física. Actualmente se halla inactivo.

Las principales características del servidor Moodle son:

- Sistema Operativo Linux.
- Intel(R) Xeon (TM) CPU 3.2GHz.
- Memoria 1Gb.

6.1.2.4 Servidor de correo

El servidor de correo se encuentra manejado directamente por gmail, el mismo que permite contar con direcciones de correo electrónico bajo un dominio de la universidad, por ejemplo: sistemas@unl.edu.ec

Sus características principales son:

- Sistema Operativo Linux.
- Intel(R) Xeon (TM) CPU 3.2GHz.
- Memoria 1 Gb.
- Disco 160 Gb.

6.1.2.5 Servidor DHCP

El servidor DHCP permite asignar dinámicamente direcciones de red a los computadores de la universidad, por medio de la MAC de la interfaz de red.

Esto se realizaba con anterioridad, hoy en día se halla libre para cualquier persona que pueda acceder a un punto de red.

Las características principales se detallan a continuación.

- Sistema Operativo Linux.
- Intel(R) Pentium (r) D CPU 3.4GHz.
- Memoria 1 Gb.

- Disco 160 Gb.

6.1.2.6 Servidor para la radio universitaria

Se encarga principalmente de replicar o transmitir la señal de “Radio Universitaria”, a través de internet, transmitiendo en vivo todos los programas que ofrece.

Se lo realiza con la finalidad de que todos los radioescuchas puedan acceder a la transmisión de la radio.

Como características principales se detalla las siguientes:

- Sistema Operativo Linux.
- Intel(R) Pentium (r) D CPU 3.4GHz.
- Memoria 1Gb.
- Disco 160Gb.

Recientemente se adquirió la licencia del Sistema Operativo Windows Server 2012, el mismo que tiene un espacio definido en el BLADE.

Cuenta con las siguientes características:

- Sistema Operativo Windows Server 2012 Standard.
- Intel(R) Pentium (r) D CPU 3.4GHz.
- Memoria 2 Gb.

6.1.3 Verificación de la infraestructura a nivel de estaciones de trabajo, características de funcionamiento, operatividad y limitaciones que presentan actualmente los recursos tecnológicos

La institución cuenta con computadores tanto portátiles y de escritorio, que son entregados a docentes y administrativos que colaboran en la universidad, los equipos son entregados por peticiones, es decir si un docente o administrativo, prefiere un computador portátil en vez de un computador de escritorio, se hace la petición del mismo para su próxima entrega, siendo así que cada equipo o computador queda a cargo de la persona a la que se entregó el bien.

Los equipos son entregados de manera permanente, si el responsable del mismo, por diversas razones, deja de laborar para la institución, el equipo debe ser entregado a

Bodega General, para su contabilidad y una próxima entrega si fuese necesario. Si este equipo tiene fallos tanto físicos como a nivel de software, debe ser entregado a la Subdirección de Redes y Equipos Informáticos en la Dirección de Telecomunicaciones e Información, para su posterior revisión.

La mayor parte de estos bienes trabajan con sistema operativo de Microsoft en la plataforma de Windows, las principales versiones de esta plataforma son: Windows 7, 8, 8.1 y Windows Vista; en máquinas con bajos recursos es instalado Windows XP. Existen además computadores en la plataforma Linux, principalmente con el sistema operativo Ubuntu, los computadores con este sistema operativo se hallan principalmente en los laboratorios de la Universidad Nacional de Loja.

Acerca de la forma de llevar la contabilidad o inventario de los equipos, este se lo realiza de manera manual, teniendo en cuenta que Bodega General no se encarga de llevar el inventario de todos ellos. Cada área educativa y administrativa de la institución cuenta con una bodega, en donde, cada una de ellas lleva el inventario de los recursos tecnológicos.

El número de equipos informáticos (computadores), que trabajan con sistemas operativos privativos y sistemas operativos libres, en cada una de las áreas se especifican en la TABLA IX.

TABLA IX. EQUIPOS INFORMATICOS DE LA UNL

	Sistema Operativo Privativo	**Sistema Operativo Propietario**	**Total**
Área Jurídica Social y Administrativa	132	33	165
Área Agropecuaria y de Recursos Naturales Renovables	112	28	140
Área de la Educación Arte y Comunicación	165	42	207
Área de la Energía las Industrias y los Recursos Naturales no Renovables	165	42	207
Área de la Salud Humana	112	28	140
Administración Central	192	48	240
TOTAL	**878**	**221**	**1099**

En su totalidad la Universidad Nacional de Loja cuenta con aproximadamente 1099 equipos informáticos (computadores), entre computadores de escritorio o mesa y computadores personales o portátiles. De los cuales, aproximadamente, 878 equipos trabajan bajo software privativo, mientras que 221, se hallan bajo distribución libre.

6.2 Fase 2: Analizar los servicios que brinda Active Directory para mejorar la seguridad y administración de los recursos tecnológicos dentro de la red LAN y WLAN de Universidad Nacional de Loja

6.2.1 Estudio de las características, ventajas y desventajas de la herramienta

Figura 10. Herramientas a comparar (Active Directory, OpenLDAP)

Fuente: Autor

Para el desarrollo del proyecto de tesis, fue necesario realizar la selección de la herramienta de directorio activo a implementarse, esto se efectuó a través de un análisis comparativo de las características, ventajas y desventajas de las herramientas con mayor demanda como las que se indica en la Figura 10, una de ellas de software propietario o libre como OpenLDAP y la otra herramienta de software privativo como es Active Directory.

Estas herramientas fueron comparadas entre sí, respecto a tres criterios de evaluación los cuales se especifican a continuación.

Características administrativas: Para realizar una evaluación de herramientas que presten el servicio de directorio, se necesita identificar las características que posee cada una de estas, para lograr una facilidad en la administración del servicio de directorio y asegurar su contenido e manera confiable.

Rendimiento: El rendimiento de las herramientas a comparar es un criterio importante que permite medir que tan competente es una herramienta comparada con otra, en cuanto a los resultados que se espera o se desea al implementar la misma.

Costos: El costo es un criterio importante a tomar en cuenta para la implementación de una herramienta en una empresa o institución, ya que dependiendo del capital con que cuenta puede ser factible realizar la implementación, en cuanto a este criterio, se pretende medir principalmente el valor de la herramienta, así como también los costos que originan el soporte de la misma.

Estos criterios son presentados en una serie de tablas en donde cada fila indica un criterio específico a analizarse. Cada uno de estos criterios tiene un valor asociado, el cual se representa por un numero entero del 1 al 10, de esta forma se especifica la importancia del criterio especifico.

En la parte derecha de cada uno de los criterios específicos, se define las columnas para evaluar tanto a la herramienta Active Directory como OpenLDAP, a cada una de las herramientas se le da una valoración con un número de 0 al 10 por cada uno de los criterios específicos, teniendo un valor resultante para cada herramienta.

Cada uno de los valores de los criterios específicos, es tomado de acuerdo a un análisis ya realizado de manera minuciosa, acerca de estas dos herramientas de directorio activo.

El análisis nombrado, fue realizado por Cesar Romero, estudiante de la Facultad de Ingeniería en Electricidad y Computación de la Escuela Superior Politécnica del Litoral, Guayaquil. La información completa del análisis, puede ser encontrado en la siguiente referencia bibliográfica [2].

6.2.1.1 Características administrativas

TABLA X. CARACTERÍSTICAS ADMINISTRATIVAS

Características Administrativas					
		ACTIVE DIRECTORY		**OPENLDAP**	
Criterio	**Valor**	**Evaluación**	**Resultado**	**Evaluación**	**Resultado**
Ambiente Grafico	10	8	80	0	0
Control de Acceso	6	8	48	8	48
Escalabilidad	7	9	63	8	56
Utilidades de Respaldo	8	6	48	5	40
Utilidades de	9	7	63	5	45

Restauración					
Fácil Administración	10	10	100	8	80
TOTAL			**402**		**269**

Mientras mayor sea el valor total de una herramienta es mucho más factible u ofrece mejores características administrativas que la otra herramienta.

Ambiente gráfico: Active Directory posee un ambiente gráfico propio de la herramienta, que facilita al administrador de red, realizar las tareas relacionadas a la administración de la organización, a diferencia de OpenLDAP que no posee un ambiente gráfico propio del producto, su utilización está basada en el terminal.

Control de acceso: Tanto Active Directory como OpenLDAP, disponen de mecanismos de seguridad para controlar el acceso a la información del directorio, dichos mecanismos se establecen a través de listas de control de acceso, las cuales consisten en listas que otorgan permisos a un objeto.

Escalabilidad: Active Directory tiende a ser más escalable con respecto a OpenLDAP, debido a que este expone que por un determinado número de máquinas se necesita establecer una nueva controladora de dominio.

Utilidades de respaldo: La utilidad slapcat, usada por OpenLDAP al momento de realizar un respaldo, tiene la limitante de que el servicio debe ser detenido antes de realizar el proceso para garantizar la consistencia de la base de datos, mientras que con la utilidad provista por Active Directory denominada ntbackup, es posible realizar dicho proceso mientras el servicio de directorio está ejecutándose. Por lo que la máxima puntuación fue otorgada a Active Directory.

Utilidades de restauración: Active Directory es mejor en cuanto a su utilidad de restauración, debido a que no conlleva pasos involucrados con el sistema operativo tal como lo efectúa OpenLDAP.

Fácil administración: Active Directory se muestra más fácil de administrar que OpenLDAP, fundamentado, en que las tareas relacionadas a la administración como es el caso de creación, modificación y eliminación de usuarios o grupos del directorio, se la realiza de forma amigable al usuario. Active Directory es simple de administrar mediante las facilidades gráficas.

Al medir cada uno de los parámetros establecidos en cuanto a las características

administrativas, Active Directory es la herramienta adecuada para la implementación del directorio activo, teniendo como característica principal un ambiente gráfico, su control de acceso es similar al de OpenLDAP, mientras que en los demás criterios específicos Active Directory se encuentra por encima de OpeonLDAP.

6.2.1.2 Rendimiento

TABLA XI. CARACTERÍSTICAS DE RENDIMIENTO

Rendimiento					
		ACTIVE DIRECTORY		OPENLDAP	
Criterio	**Valor**	**Evaluación**	**Resultado**	**Evaluación**	**Resultado**
Tiempo de Login	6	8	48	7	42
Manejo de conexiones LDAP	7	7	49	7	49
Procesamiento de las Operaciones	8	7	56	5	40
TOTAL			**153**		**131**

En cuanto al rendimiento, mientras mayor es el valor total de una herramienta es mejor en el ámbito del rendimiento respecto a la otra herramienta.

Tiempo de login: En Active Directory, el tiempo de login que se produce respecto a 1 cliente es igual a 0,27 segundos aproximadamente; respecto a 10 clientes es aproximadamente igual a 1,39 segundos.

En OpenLDAP, el tiempo de login que se produce respecto a 1 cliente es igual a 0,46 segundos aproximadamente, y el tiempo total de login de los 10 clientes es aproximadamente de 2,19 segundos.

Valores que favorecen en esta característica a Active Directory, debido a que los tiempos reflejados en el login son menores a los obtenidos por OpenLDAP.

Manejo de conexiones LDAP: En el manejo de conexiones LDAP, existe un buen nivel en ambas herramientas dado que ambas saben manejar estas conexiones.

Procesamiento de las operaciones: Claramente se visualiza a Active Directory como una herramienta de directorio muy fuerte frente a la herramienta OpenLDAP, al analizar el criterio relacionado al tiempo de procesamiento de las operaciones dentro del servicio de directorio.

En cuanto al rendimiento, Active Directory es la herramienta adecuada, ya que la misma se halla por encima de OpenLDAP, de acuerdo a los criterios del tiempo de login y en

el procesamiento de las operaciones; mientras que en cuanto al criterio de manejo de conexiones LDAP es similar en las dos herramientas.

6.2.1.3 Costos

TABLA XII. CARACTERÍSTICAS DE COSTOS

Costos					
		ACTIVE DIRECTORY		OPENLDAP	
Criterio	**Valor**	**Evaluación**	**Resultado**	**Evaluación**	**Resultado**
Software	7	10	70	0	0
Hardware	7	7	49	7	49
Implementación	7	5	35	8	56
Mantenimiento	8	5	40	6	48
TOTAL			**194**		**153**

El resultado final, después de analizar los valores asignados a cada uno de los criterios en cuanto a los costos, determina que mientras mayor es el valor total es mucho más costoso la implementación de esta herramienta.

Costo de software: En cuanto al costo en software, se detalla el valor de evaluación de OpenLDAP, con un valor de 0, ya que este es de código propietario o libre, es decir Active Directory resulta más costoso frente a OpenLDAP; dado que es necesario adquirir el sistema operativo.

Costo del hardware: Al considerar el costo de hardware del servidor, para implementar un servicio de directorio, se puede decir que tanto para usar Active Directory, como OpenLDAP, no se requiere de una arquitectura de hardware compleja ni especializada.

Costo de implementación: Si consideramos el costo de implementación como el costo de efectuar el proceso que soporta la instalación, configuración y pruebas respectivas sobre el directorio; la implementación de Active Directory resulta un proceso sencillo, basado en el tiempo que conlleva realizarlo.

Costo de mantenimiento: Los costos por mantenimiento serán los valores reflejados en el pago al personal encargado, quien es el responsable del funcionamiento del servidor en el que reside el servicio de directorio. En este caso el encargado de la sección de redes percibe el mismo salario ya que se trata de una institución pública. En tal caso será más factible aplicar Active Directory, ya que es mucho más fácil su administración, mientras que para OpenLDAP, sería necesario una persona experta en el área de sistemas operativos libres o propietarios.

En cuanto al costo, OpenLDAP es la mejor opción, ya que no posee costo en su licenciamiento, en lo referente al hardware tanto OpenLDAP como Active Directory requieren hardware similar, Active Directory es mucho más económico en cuanto a la implementación y el mantenimiento, sin embargo OpenLDAP es el mejor, ya que el costo de la licencia es el criterio más significativo en la comparación de las herramientas.

Una vez analizados cada uno de los criterios, podemos concluir o seleccionar la herramienta a usar para el proyecto de fin de carrera, la cual en base a las puntuaciones obtenidas se deduce que es Active Directory la herramienta adecuada para el desarrollo exitoso del proyecto de titulación.

Para tener una noción clara de lo que es, y ofrece Active Directory, se especifica a continuación características, ventajas y desventajas de la misma.

6.2.1.4 Características de Active Directory

Active Directory es un servicio de directorio de tipo empresarial y escalable, se ha creado a partir de cero mediante tecnologías estándar de Internet y está totalmente integrado en el sistema operativo, simplifica la administración y permite a los usuarios buscar recursos con mayor facilidad.

Active Directory proporciona una amplia gama de características y capacidades como:

Mejor replicación y capacidades de pruebas de diagnóstico de DNS: Ofrece avisos automáticos de copia de seguridad de los servicios de directorio, mayor protección contra errores de replicación, mejoras para instalar desde medios, capacidades de pruebas de diagnóstico de DNS, y acceso a una nueva plataforma para ejecutar controladores de dominio en equipos virtuales en Microsoft. [11]

Administración simplificada de usuarios y recursos de red: Se puede utilizar Active Directory para crear estructuras de información jerárquicas, que simplifican el control de las credenciales administrativas y otras opciones de seguridad, permite a los usuarios localizar recursos de red, como archivos e impresoras, con mayor facilidad. [11]

Sistemas de autenticación y autorización flexibles y seguras: Los servicios de autenticación y autorización, flexibles y seguros, proporcionan protección para los datos al mismo tiempo que reducen las barreras. Active Directory admite numerosos protocolos de autenticación. [11]

Consolidación de directorios: Es posible organizar y simplificar la administración de usuarios, equipos, aplicaciones y dispositivos, y facilitar a los usuarios la búsqueda de la información que necesitan. [11]

Infraestructura y aplicaciones habilitadas para el uso de directorios: Las características de Active Directory facilitan la configuración y administración de las aplicaciones y otros componentes de red habilitados para el uso de directorios. [11]

Escalabilidad sin complejidad: Puede escalarse hasta llegar a tener millones de objetos por cada dominio y utiliza tecnología de indización y técnicas de replicación avanzadas para aumentar el rendimiento. [11]

Uso de los estándares de Internet: Proporciona acceso mediante LDAP y utiliza un espacio de nombres basado en el Sistema de Nombres de Dominio (DNS). [11]

Un entorno de desarrollo eficaz: Ofrece un entorno de desarrollo eficaz mediante las Interfaces de Servicio de Active Directory (ADSI), que le proporciona una interfaz orientada a objetos. [11]

Replicación y supervisión de confianza: Proporciona clases de Instrumental de Administración de Windows (WMI) que supervisan si los controladores de dominio replican correctamente la información de Active Directory y si las relaciones de confianza funcionan adecuadamente. [11]

Listas de distribución de Servicios de Message Queue Server: Permite enviar mensajes a listas de distribución alojadas en Active Directory. [11]

6.2.1.5 Características para la administración de equipos con Active Directory

Directivas de usuario

Active Desktop

- **Quitar del escritorio el icono de equipo**

Esta opción oculta Equipo en el escritorio y en el nuevo menú Inicio. También oculta los vínculos a Equipo en la vista web de todas las ventanas del Explorador de Windows y oculta Equipo en el panel del árbol de carpetas del Explorador. Si el usuario llega a

Equipo con el botón "Arriba" mientras esta opción está habilitada, verá una carpeta Equipo vacía. Esta opción permite a los administradores impedir que los usuarios vean Equipo en el espacio de nombres de shell, lo que les permite ofrecer a los usuarios un entorno de escritorio más sencillo.

Si se habilita esta opción, Equipo estará oculto en el escritorio, en el nuevo menú Inicio, en el panel del árbol de carpetas del Explorador y en las vistas web del Explorador. Si el usuario consigue llegar a Equipo, la carpeta estará vacía.

Si se deshabilita esta opción, Equipo se mostrará con normalidad en el escritorio, el menú Inicio, el panel del árbol de carpetas y las vistas web, a no ser que otra opción lo impida.

- **Quitar el elemento propiedades del menú contextual del elemento equipo**

Si habilita esta opción, la opción Propiedades no aparecerá cuando el usuario haga clic con el botón secundario en Equipo o haga clic en Equipo y vaya el menú Archivo. Asimismo, Alt+Entrar no realizará ninguna acción cuando Equipo esté seleccionado.

Si deshabilita esta opción o no la configura, el elemento Propiedades se mostrará con normalidad.

- **Quitar el elemento propiedades del menú contextual del elemento documentos**

Si habilita esta configuración de directiva, el comando de menú Propiedades no se mostrará cuando el usuario realice una de las acciones siguientes:

Hacer clic con el botón secundario en el icono Mis documentos.

Hacer clic con el botón secundario en el icono Mis documentos y, a continuación, abrir el menú Archivo.

Hacer clic con el botón secundario en el icono Mis documentos y, a continuación, presionar Alt+Entrar.

Si deshabilita o no establece esta configuración de directiva, el comando de menú Propiedades se mostrará.

- **Quitar del escritorio el icono de la papelera de reciclaje**

Esta opción quita el icono Papelera de reciclaje del escritorio, del Explorador de archivos, de los programas que usan las ventanas del Explorador de archivos y del cuadro de diálogo estándar Abrir.

Esta opción no impide que el usuario use otros métodos para obtener acceso al contenido de la carpeta Papelera de reciclaje.

- **No guardar la configuración al salir**

Si habilita esta opción, los usuarios pueden cambiar el escritorio, pero algunos de los cambios, como la posición de las ventanas abiertas o el tamaño y la posición de la barra de tareas, no se guardarán cuando los usuarios cierren la sesión. No obstante, los accesos directos que se encuentren en el escritorio se guardarán siempre.

- **Prohibir el ajuste de la barra de herramientas del escritorio**

Impide que los usuarios ajusten la longitud de las barras de herramientas del escritorio. Además, los usuarios no podrán colocar elementos ni barras de herramientas en las barras de herramientas acopladas.

Esta opción no impide que los usuarios agreguen o quiten barras de herramientas en el escritorio.

- **Activar Active desktop**

Esta opción impide que los usuarios intenten habilitar o deshabilitar Active Desktop mientras una directiva lo controla.

Si deshabilita esta opción o no la configura, Active Desktop se deshabilita de forma predeterminada, pero los usuarios pueden habilitarlo.

- **Papel tapiz**

Especifica el fondo de escritorio ("papel tapiz") que se mostrará en los escritorios de todos los usuarios.

Esta opción le permite especificar el papel tapiz que aparecerá en los escritorios de los usuarios e impide que los usuarios puedan cambiar la imagen o su presentación. El

papel tapiz que especifique puede almacenarse como un archivo de mapa de bits (*.bmp) o JPEG (*.jpg).

Para usar esta opción, escriba el nombre y la ruta de acceso completos del archivo en el que se almacena la imagen del papel tapiz. Puede escribir una ruta de acceso local, como C:\Windows\web\wallpaper\inicio.jpg o una ruta UNC, como \\servidor\recursoCompartido\Corp.jpg. Si el archivo especificado no está disponible cuando el usuario inicia la sesión, no aparecerá ningún papel tapiz. Los usuarios no pueden especificar un papel tapiz alternativo. También puede usar esta opción para especificar que la imagen del papel tapiz debe aparecer centrada, en forma de mosaico o expandida. Los usuarios no pueden cambiar esta especificación.

Componentes de Windows

- **Administrador de datos adjuntos**
    - **Lista de inclusión de archivos de alto riesgo**

Esta configuración de directiva permite configurar la lista de tipos de archivos de alto riesgo. Si los datos adjuntos de archivo están en la lista de tipos de archivo de alto riesgo y proceden de una zona restringida, Windows impide que el usuario tenga acceso al archivo. Si el archivo está en la zona de Internet, Windows avisa al usuario antes de que tenga acceso al archivo. Esta lista de inclusión tiene preferencia sobre las listas de inclusión de riesgo bajo y moderado (cuando una extensión aparece en más de una lista de inclusión).

- **Administrador ventanas de Windows**
    - **No permitir animaciones en las ventanas**

Esta configuración de directiva controla el aspecto de las animaciones de las ventanas, como las que pueden aparecer al restaurar, minimizar y maximizar las ventanas.

    - **No permitir invocación Flip 3D**

Esta configuración de directiva permite configurar la accesibilidad de la característica Flip 3D. Flip 3D permite que el usuario pueda ver los elementos en el escritorio de Windows mientras se voltean en tres dimensiones.

Menú de inicio y barra de tareas

- **Desactivar menús personalizados**

Windows personaliza menús largos moviendo elementos recientemente usados al principio del menú y ocultando elementos que no se han usado recientemente. Los usuarios pueden mostrar los elementos ocultos haciendo clic en una flecha para extender el menú.

Si habilita esta opción, el sistema no personaliza los menús. Todos los elementos del menú aparecen y permanecen en orden estándar. Esta opción de configuración también quita la opción "Usar menús personalizados" para que los usuarios no traten de cambiar la opción de configuración mientras esté activa una opción.

- **Quitar y evitar el acceso a los comandos Apagar, Reiniciar, Suspender**

Si se habilita esta configuración de directiva, el botón de encendido y los comandos Apagar, Reiniciar, Suspender e Hibernar se quitan del menú Inicio. También se quita el botón de encendido de la pantalla de Seguridad de Windows, que aparece cuando se presiona CTRL+ALT+DELETE.

Si se deshabilita o no se configura esta configuración de directiva, el botón de encendido y los comandos Apagar, Reiniciar, Suspender e Hibernar estarán disponibles en el menú Inicio. El botón de encendido también estará disponible en la pantalla de Seguridad de Windows.

- **Quitar el vínculos de juegos del menú de inicio**

Si habilita esta directiva, el menú Inicio no mostrará un vínculo a la carpeta Juegos.

Si deshabilita o no configura esta directiva, el menú Inicio mostrará un vínculo a la carpeta Juegos, a menos que el usuario elija quitarla en el panel de control del menú Inicio.

- **No guardar el historial de documentos abiertos recientemente**

Si habilita esta opción, el sistema y los programas de Windows no crearán accesos directos a los documentos abiertos mientras esté activa la opción. Además, retendrán pero no mostrarán los accesos directos a documentos ya existentes. El sistema vaciará

el menú Elementos recientes del menú Inicio y los programas de Windows no mostrarán los accesos directos en la parte inferior del menú Archivo. Además, las Jump List de programas del menú Inicio y la barra de tareas no mostrarán listas de archivos, carpetas o sitios web usados recientemente.

Si deshabilita o no configura esta opción, el sistema mostrará accesos directos a archivos, carpetas o sitios web usados recientemente y usados con mayor frecuencia.

- **Quitar el icono de música del menú de inicio**

Quita el icono Música del menú Inicio.

- **Cambiar el botón de encendido del menú inicio**

Si habilita esta opción, el menú Inicio establecerá el botón de encendido a la acción elegida y no permitirá al usuario cambiarla.

Si establece el botón de encendido a Suspender o Hibernar y el equipo no admite ese estado, el botón volverá a Apagar.

- **No permitir el anclado a la barra de tareas**

Si habilita esta opción, los usuarios no podrán cambiar los programas que están anclados actualmente a la barra de tareas. Continuarán mostrándose en la barra de tareas los programas que ya estén anclados a la misma. Sin embargo, los usuarios no podrán desanclar estos programas ya anclados a la barra de tareas, ni anclar nuevos programas.

Si deshabilita o no configura esta opción, los usuarios podrán anclar programas, de forma que los accesos directos a los programas permanezcan en la barra de tareas.

- **Bloquear toda la configuración de la barra de tareas**

Si habilita esta opción, el usuario no podrá tener acceso al panel de control de la barra de tareas. Tampoco podrá cambiar el tamaño, mover ni reorganizar barras de herramientas de la barra de tareas correspondiente.

Si deshabilita o no configura esta opción, el usuario podrá establecer cualquier configuración de la barra de tareas permitida por otra configuración de directiva.

- **Quitar el menú Ejecutar**

Permite quitar el comando Ejecutar del menú Inicio, Internet Explorer y el Administrador de tareas.

Si se habilita esta opción, se producirán los siguientes cambios:

1. Se quita el comando Ejecutar del menú Inicio.
2. El comando Nueva tarea (ejecutar) se quita del Administrador de tareas.
3. Se impedirá al usuario lo siguiente en la barra de direcciones de Internet Explorer:
    a. Escribir una ruta de acceso UNC: \\<servidor>\<recursoCompartido>
    b. Tener acceso a unidades locales: por ejemplo, C:
    c. Tener acceso a carpetas locales: por ejemplo, \temp>

Además, los usuarios con teclados extendidos ya no podrán seguir mostrando el cuadro de diálogo Ejecutar presionando la tecla de aplicación (la tecla con el logotipo de Windows) + R.

Panel de control

- **Ocultar elementos específicos del panel de control**

Esta opción quita elementos del Panel de control (como, por ejemplo, "Mouse", "Sistema" o "Personalización") de la ventana Panel de control y el menú Inicio.

Para ocultar un elemento del Panel de control, haga clic en Mostrar. En el cuadro de diálogo Mostrar contenido, en la columna Valor, escriba el nombre canónico del elemento del Panel de control (por ejemplo, "Microsoft.Mouse", "Microsoft.System" o "Microsoft.Personalization").

- **Agregar o quitar programas**
    - **Ocultar la página configurar acceso y programas predeterminados**

El botón Configurar acceso y programas predeterminados permite a los administradores especificar los programas predeterminados para ciertas actividades, como exploración de Internet o envío de correo electrónico, así como los programas que a los que se tiene acceso desde el menú Inicio, el escritorio y otras ubicaciones.

Si deshabilita esta opción o no la configura, el botón Configurar acceso y programas predeterminados está disponible para todos los usuarios.

- **Impresoras**
    - **Buscar impresoras en la red**

Si habilita esta opción o no la configura, cuando los usuarios elijan agregar impresora de red con el botón de radio "Una impresora de red o una impresora conectada a otro equipo" en la página 2 del Asistente para agregar impresoras y seleccionen el botón de radio "Conectarse a esta impresora (o para buscar una, seleccionar esta opción y hacer clic en Siguiente)" en la página 3, sin especificar el nombre de la impresora en el cuadro de texto "Nombre", el asistente mostrará la lista de las impresoras compartidas en la red e invitará a elegir una.

Si deshabilita esta opción, la página de búsqueda de impresoras se quita del Asistente para agregar impresoras; de este modo, los usuarios no pueden buscar en la red y deben escribir el nombre de una impresora.

- **Impedir la eliminación de impresoras**

Si un usuario intenta eliminar una impresora, por ejemplo, con la opción Eliminar del elemento Impresoras del Panel de control, aparecerá un mensaje que explica que existe una opción que impide esta acción.

Esta opción no impide que los usuarios ejecuten otros programas para eliminar una impresora.

Si esta directiva está deshabilitada o sin configurar, los usuarios pueden eliminar impresoras mediante los métodos descritos anteriormente.

Personalización

- **Impedir cambiar la combinación de colores**

Si habilita esta opción, el usuario no podrá cambiar la combinación de colores del tema de escritorio actual.

Si deshabilita o no configura esta opción, el usuario podrá cambiar la combinación de colores del tema de escritorio actual.

En Windows 7 y posterior, use la opción "Impedir cambiar el color y la apariencia de las ventanas".

- **Impedir cambiar el tema**

Si habilita esta opción, los usuarios no podrán cambiar ni guardar un tema. No obstante, se podrán cambiar los elementos de un tema, como fondo de escritorio, color de ventanas, sonidos y protector de pantalla (a menos que las directivas los hayan desactivado).

Si deshabilita o no configura esta opción, no se produce ningún efecto.

- **Impedir cambiar el estilo visual de ventanas y botones**

Si se habilita en Windows XP y sistemas posteriores, esta opción impide que se cambie el estilo visual desde la línea de comandos. Además, el usuario no podrá aplicar un estilo visual distinto al cambiar el tema.

- **Prohibir seleccionar el tamaño de fuente del estilo visual**

Si se habilita esta opción, se deshabilita la lista desplegable "Tamaño de fuente" en la ficha Apariencia de Propiedades de pantalla.

Si se deshabilita o no se configura esta opción, un usuario puede cambiar el tamaño de fuente mediante la lista desplegable “Tamaño de fuente” en la ficha Apariencia.

- **Impedir cambiar el color y la apariencia**

Esta configuración impide a los usuarios usar el Panel de control para cambiar el color del estilo visual Glass, los colores del sistema o la combinación de colores del escritorio y las ventanas.

Si se ha deshabilitado o no se ha definido esta configuración, la página Color de ventana o el diálogo Combinación de colores estarán disponibles en el Panel de control de personalización o pantalla.

- **Impedir cambiar el fondo de pantalla**

Impide que los usuarios agreguen o cambien el diseño de fondo del escritorio.

De forma predeterminada, los usuarios pueden usar la página Fondo de escritorio del Panel de control de personalización o pantalla para agregar un diseño de fondo (papel tapiz) al escritorio.

Si habilita esta opción, el usuario no podrá cambiar ninguna de las opciones de Fondo de escritorio.

Para especificar un papel tapiz para un grupo, use la opción "Tapiz del escritorio".

- **Impedir cambiar los iconos del escritorio**

De forma predeterminada, los usuarios pueden usar el cuadro de diálogo Configuración de iconos de escritorio del Panel de control de personalización o pantalla para mostrar, ocultar o cambiar los iconos del escritorio.

Si habilita esta opción, el usuario no podrá cambiar ninguno de los iconos del escritorio.

En sistemas anteriores a Windows Vista, esta configuración también oculta la ficha escritorio en el Panel de control de Pantalla.

- **Impedir cambiar punteros del mouse**

De forma predeterminada, los usuarios pueden usar la ficha Punteros del Panel de control del mouse para agregar, quitar o cambiar los punteros del mouse.

Si habilita esta opción, el usuario no podrá cambiar ninguna de las opciones de la combinación de punteros del mouse.

- **Impedir cambiar protector de pantalla**

Impide que el cuadro de diálogo Protector de pantalla se abra en el Panel de control de personalización o pantalla.

Esta configuración impide que los usuarios usen el Panel de control para agregar, configurar o cambiar el protector de pantalla del equipo. No impide que se ejecute un protector de pantalla.

- **Impedir cambiar sonidos**

De forma predeterminada, los usuarios pueden usar la ficha Sonidos del Panel de control de sonido para agregar, quitar o cambiar la combinación de sonidos del sistema.

Si habilita esta opción, el usuario no podrá cambiar ninguna de las opciones de la combinación de sonidos.

Programas

- **Ocultar la página “programas y características”**

Si esta opción está deshabilitada o no está configurada, "Programas y características" estará disponible para todos los usuarios.

Esta opción no impide que los usuarios usen otros métodos y herramientas para ver o desinstalar programas. Tampoco impide que los usuarios establezcan vínculos con características relacionadas del panel de control Programas, como Características de Windows, Obtener programas o Windows Marketplace.

- **Sistema**
    - **Quitar administrador de tareas**

Si esta opción está habilitada y los usuarios intentan iniciar el Administrador de tareas, aparece un mensaje que explica que hay una directiva que impide realizar la acción.

El Administrador de tareas permite a los usuarios iniciar y detener programas, supervisar el rendimiento de sus equipos, ver y supervisar todos los programas que se ejecutan en sus equipos (incluidos los servicios del sistema), buscar los nombres de los archivos ejecutables de los programas y cambiar la prioridad del proceso en el que se ejecutan los programas.

    - **Quitar bloqueo de equipo**

Cuando el sistema está bloqueado, el escritorio permanece oculto y no se puede usar el sistema. Únicamente el usuario que bloqueó el sistema o el administrador del sistema pueden desbloquearlo.

Sugerencia: para bloquear un equipo sin configurar ninguna opción, presione Ctrl+Alt+Supr y, a continuación, haga clic en "Bloquear este equipo".

- **Desactivar el cmd**

6.2.1.6 Ventajas y desventajas de Active Directory

A simple vista Active Directory parece una buena opción a la hora de promocionar un dominio, pero también tiene sus desventajas.

En la TABLA XIII se puede apreciar las principales ventajas y desventajas que ofrece hoy por hoy Active Directory.

TABLA XIII. VENTAJAS Y DESVENTAJAS DE ACTIVE DIRECTORY

Active Directory	
Ventajas	**Desventajas**
Multitud de herramientas de configuración (gráfica y terminal).	Requiere tener un tamaño mayor de disco duro.
Mayor Seguridad frente a los servidores NT.	Requerimiento de memoria
Mejoras en el rendimiento del sistema	Un equipo servidor
Control sobre las instalaciones que tienen los usuarios.	Se requiere tener los sistemas de archivos en NTFS.
Control sobre los tipos de accesos que tendrán cada usuario.	Puede tornarse un tanto lento dependiendo de cuantos servidores se tenga instalados. Puede verse saturado y será necesario disponer de suficiente memoria.
Seguridad en los datos.	

6.2.2 Estudio del hardware y software de acuerdo a los requerimientos necesarios para la implementación del servidor

Una vez seleccionada la herramienta para la implementación del directorio activo en la red de datos de la Universidad Nacional de Loja, se debe tener claro que software y hardware son necesarios para el levantamiento de la misma y el correcto desarrollo del proyecto de tesis.

6.2.2.1 Software

Active Directory es una herramienta de directorio activo perteneciente a Microsoft, exclusivamente pertenece a Windows Server en todas sus versiones. La versión a ser usada para el proyecto de tesis es Windows Server 2012 Standard.

Windows Server 2012 es la versión más reciente del sistema operativo Windows Server, ofrece a las empresas y los proveedores de hospedaje una infraestructura escalable,

dinámica y para varios inquilinos. [12] Proporciona varias características y capacidades nuevas con respecto a las versiones anteriores en cuanto Active Directory, entre las principales características se detallan las siguientes:

Descripción del rol: Los Servicios de certificados de Active Directory (AD CS) proporcionan servicios personalizables para emitir y administrar certificados de infraestructura de clave pública (PKI) usados en sistemas de seguridad de software que emplean tecnologías de clave pública. El rol de servidor de AD CS incluye seis servicios de rol: [13]

- Entidad de certificación (CA).
- Inscripción web.
- Servicio de respuesta en línea.
- Servicio de inscripción de dispositivos de red.
- Servicio web de directivas de inscripción de certificados.
- Servicio web de inscripción de certificados.

Funcionalidad nueva o modificada: Existen varias funcionalidades nuevas disponibles en la versión Windows Server 2012 de AD CS. Incluyen:

- **Integración con el administrador del servidor:** El Administrador del servidor proporciona una interfaz gráfica de usuario centralizada para instalar y administrar el rol de servidor de AD CS y sus seis servicios de rol. [13]
- **Funcionalidades de administración e implementación desde Windows PowerShell:** Mediante el uso de los cmdlets de implementación de AD CS de Windows PowerShell, pueden configurarse todos los servicios de roles de AD CS o pueden quitarse sus configuraciones. El cmdlet de administración de AD CS permite administrar el servicio de rol Entidad de certificación. [13]
- **Todos los servicios de roles de AD CS se ejecutan en cualquier versión de Windows server 2012:** Todas las versiones de Windows Server 2012 permiten instalar todos los servicios de roles de AD CS. [13]
- **Todos los servicios de rol de AD CS pueden instalarse y ejecutarse en Server Core:** Los seis servicios de roles de AD CS de Windows Server 2012 pueden instalarse y ejecutarse en instalaciones Server Core de Windows Server 2012 o las opciones de instalación de la interfaz de servidor básica. [13]

- **Compatibilidad con la renovación basada en claves:** Los Servicios web de inscripción de certificados es una característica que se agregó en Windows 7 y Windows Server 2008 R2. Esta característica permite que las solicitudes de certificados en línea provengan de dominios de Servicios de Dominio de Active Directory (AD DS) que no sean de confianza o incluso de equipos que no estén unidos a un dominio. AD CS en Windows Server 2012 aprovecha los Servicios web de inscripción de certificados agregando la capacidad de renovar certificados automáticamente para los equipos que son parte de dominios de AD DS.[13]
- **Compatibilidad con plantillas de certificado:** AD CS en Windows Server 2012 presenta plantillas de certificado de la versión 4. Estas plantillas presentan varias diferencias con respecto a las versiones anteriores. Las plantillas de certificado de la versión 4: [13]
    - Admiten proveedores de servicios de cifrado (CSP) y proveedores de servicios de claves (KSP).
    - Se pueden configurar para requerir la renovación con la misma clave.
    - Solamente están disponibles para su uso por parte de Windows 8 y Windows Server 2012.
    - Especifican los requisitos mínimos de entidad de certificación y sistemas operativos de cliente de certificados que puede usar la plantilla.
- **Renovación de certificados con la misma clave:** AD CS en Windows Server 2012 aumenta la seguridad exigiendo la renovación de un certificado con la misma clave. Esto permite mantener el nivel de seguridad de la clave original durante todo su ciclo de vida. Windows Server 2012 admite la generación de claves protegidas mediante el módulo de plataforma segura (TPM) mediante el uso de proveedores de almacenamiento de claves (KSP) basados en TPM. La ventaja de usar KSP basados en TPM es la auténtica imposibilidad de exportar claves respaldadas por el mecanismo de protección contra ataques de repetición (hammering) de los TPM. Los administradores pueden configurar plantillas de certificado para que Windows 8 y Windows Server 2012 les proporcionen prioridad más alta a los KSP basados en TPM para generar claves. Además, al usar la renovación con la misma clave, los administradores pueden estar seguros de que la clave permanecerá en el TPM tras la renovación. [13]
- **Compatibilidad con nombres de dominio internacionalizados:** Los nombres internacionalizados son nombres que contienen caracteres que no se pueden

representar en ASCII. AD CS en Windows Server 2012 admite nombres de dominio internacionalizados (IDN) en diversos escenarios. [13]

- **Mayor seguridad habilitada de manera predeterminada en el servicio de rol Entidad de certificación:** Cuando una autoridad de certificación (CA) recibe una solicitud de certificado, la CA puede forzar el cifrado para la solicitud a través de RPC_C_AUTHN_LEVEL_PKT. En Windows Server 2008 R2 y versiones anteriores, esta configuración no está habilitada de manera predeterminada en la CA. En una CA de Windows Server 2012, esta configuración de seguridad mejorada está habilitada de manera predeterminada. [13]
- **Reconocimiento de sitios de AD DS para AD CS y clientes PKI:** Los servicios de certificados en Windows 8 y Windows Server 2012 se pueden configurar de forma que utilicen sitios de Servicios de dominio de Active Directory (AD DS) para optimizar las solicitudes de cliente de servicios de certificados. Esta funcionalidad no está habilitada de forma predeterminada en los equipos cliente de entidad de certificación (CA) o de infraestructura de clave pública (PKI). [13]

6.2.2.2 Hardware

Requisitos de disco

Como mínimo, un controlador de dominio necesita espacio de disco disponible para la base de datos de los Servicios de Dominio de Active Directory (AD DS), los archivos de registro de AD DS, SYSVOL y el sistema operativo.

Los siguientes puntos sirven de guía para determinar cuánto espacio de disco se debe asignar para la instalación de AD DS: [14]

- En la unidad que va a contener la base de datos de AD DS, NTDS.dit, de debe designar como un mínimo de 0,4 Gb por cada 1.000 usuarios.
- En la unidad que contiene los archivos de registro de AD DS, se debe designar al menos 500 Mb.
- En la unidad que contiene la carpeta compartida SYSVOL, se debe designar al menos 500 Mb.
- En la unidad que contiene los archivos del sistema operativo, para ejecutar el programa de instalación, se debe designar como mínimo entre 1,25 Gb y 2 Gb.

Requisitos de memoria

- Si se tiene de 1 a 499 usuarios el mínimo en memoria RAM es de 512 Mb.
- Si se tiene de 500 a 999 usuarios el mínimo en memoria RAM es de 1 Gb.
- Si se tiene más de 1000 usuarios el mínimo en memoria RAM es de 2 Gb. [15]

Requisitos del procesador

La recomendación general es que para los sitios con menos de 500 usuarios, se inicia con un solo procesador; para los sitios con más de 10.000 usuarios, se debe comenzar con procesadores duales y luego escalar desde allí. Esto supone que el trabajo principal del directorio es la autenticación de usuarios. [15]

Requisitos de red

Por lo general, un solo adaptador de red es suficiente para manejar todo el tráfico de red, a, o desde el servidor. Si se espera que el tráfico de red sea extremadamente alta, entonces puede ser necesario realizar pruebas para ver si se requieren múltiples adaptadores de red. [15]

La Universidad Nacional de Loja cuenta con aproximadamente 10000 usuarios de la red de datos, tanto estudiantes, docentes y administrativos.

Teniendo en consideración los puntos a tomar en cuenta para la determinación de hardware adecuado para la implementación de Active Directory, y la cantidad de usuarios que hacen uso de la red de la institución se puede indicar que los requisitos mínimos, adecuados y recomendados de hardware para el levantamiento de Active Directory son los siguientes:

Requisitos mínimos

- Procesador: Procesadores duales.
- Memoria RAM: 2 GB.
- Espacio en disco: 50 GB.

Requisitos adecuados

- Procesador: Procesadores duales.
- Memoria RAM: 4 GB.

- Espacio en disco: 100 GB.

Requisitos recomendados

- Procesador: Procesadores duales.
- Memoria RAM: 6 GB.
- Espacio en disco: 480 GB.

En cuanto al hardware, no surgen problemas al momento de realizar la instalación del sistema operativo y el levantamiento de Active Directory, ya que el servicio de directorio activo será implementado en la Universidad Nacional de Loja, la institución cuenta ya con un espacio adecuado para el levantamiento del servicio.

Plan de contingencia

Para el correcto funcionamiento del Directorio Activo dentro de la Universidad Nacional de Loja, se debe poner en marcha un plan de contingencia, ya que con este se puede evitar pérdidas tanto en equipos físicos, como en tiempo por cada uno de las personas que hacemos uso de la red de datos, ya que Active Directory se aplica a la red de la institución, y si por a o b razones llegase a fallar, ningún usuario podría seguir con sus cargos ya que no tendrían acceso a la red de la institución.

El plan de contingencia viene dado tanto en hardware como en software, se recomienda los siguientes puntos para evitar molestias posteriores.

A nivel de Hardware:

- Dos líneas eléctricas.
- Dos UPS una conectada a cada línea eléctrica.
- Los servidores con 2 Fuentes de alimentación y cada una conectada a una UPS.
- En cada servidor mínimo 2 discos en RAID 1. (Espejos).
- Una unidad de backup.

A nivel de Software:

- Un segundo servidor como controlador de dominio.

6.2.3 Análisis de los servicios de seguridad que brinda el estándar 802.1x

6.2.3.1 Estándar 802.1x

Es un estándar del IEEE para realizar el control de acceso a una red mediante un proceso de autenticación que habilita o impide el acceso de los dispositivos que se conectan a un puerto de red LAN. Este estándar puede implementarse en redes cableadas al igual que en redes inalámbricas 802.11. [8]

En la implementación 802.1x se requieren, mínimo, los siguientes componentes:

- Usuario que intenta acceder a la red, o “suplicante”.
- Punto de acceso que habilita o impide el ingreso del suplicante, también llamado “Autenticador”.
- Servidor de autenticación, quien negocia y valida la identidad del suplicante; y le informa el éxito o fracaso de este proceso al autenticador.

Por otro lado 1x hace referencia al uso del protocolo de autenticación extensible EAP entre el suplicante, el autenticador y los servidores de autenticación. [8]

6.2.3.2 Porque 802.1x

Muchas prácticas se han establecido como recomendables para minimizar los riesgos asociados al acceso indebido en redes alámbricas e inalámbricas. Entre las principales recomendaciones de este tipo se encuentran:

- Evitar la difusión del identificador de red.
- Establecer listas de control de acceso por direcciones físicas o de MAC de los dispositivos que acceden a la red.
- Utilizar cifrado en las conexiones.
- Segmentar los puntos de acceso inalámbricos en zonas de seguridad administradas por un firewall.
- Establecer redes privadas virtuales o VPN’S en las conexiones inalámbricas.

De estas prácticas, algunas se han implementado directamente en dispositivos alámbricos e inalámbricos, como el uso de cifrado. Inicialmente surgió el protocolo WEP el cual utiliza una clave secreta estática que es compartida por el punto de acceso y

todos los clientes que accedan a través de este a la red, y con la cual se realiza la autenticación a la red y la protección de los datos.

Muchos fabricantes entonces, decidieron integrar esta funcionalidad y compatibilidad con WEP para ofrecer un mecanismo de seguridad para las redes inalámbricas, sin embargo, no pasó mucho tiempo para que se empezaran a detectar y difundir las debilidades o fallas de este mecanismo. Realmente WEP tiene debilidades de seguridad debido al manejo estático de su llave y al uso de un vector de inicialización que se puede identificar en los paquetes transmitidos, de manera periódica; lo que hace que este protocolo sea susceptible a ataques que permitan encontrar la llave de cifrado a partir de un tráfico capturado; más aún, hoy en día no se requiere una cantidad extremadamente grande de datos capturados ni de conocimiento para llevar a cabo este proceso. [8]

Este estándar incluye los mecanismos más adecuados para realizar el control de acceso y protección de datos en ambientes alámbricos e inalámbricos ya que integra mecanismos fuertes de autenticación, control de acceso, integridad y confidencialidad.

WPA utiliza 802.1x como mecanismo de control de acceso y autenticación a la red, y para generar y entregar las llaves de sesión WPA a los usuarios autenticados.

El principal problema de WPA radica en que es un estándar que aún se encuentra en proceso de adopción, donde muchas tecnologías inalámbricas no están habilitadas para poder implementarlo. Adicionalmente el estándar 802.11i (también conocido como WPA2) aún se está ratificando y posteriormente se requerirá una actualización en el hardware y software de acceso inalámbrico para cumplir con este estándar.

La implementación de 802.1x para redes inalámbricas utiliza un servidor de autenticación como el RADIUS, el cual no solo es quien valida la identidad de quien accede a la red si no que es quien fuerza, con cierta frecuencia, la generación de una nueva clave de cifrado para la conexión establecida, haciendo que la probabilidad de que un ataque identifique de la clave de cifrado, sea mínima. [8]

Otra ventaja de la implementación de 802.1x en redes alámbricas e inalámbricas es los costos asociados, ya que se puede utilizar servidores de autenticación que ya existen en las organizaciones y no se requiere actualizaciones firmware o compatibilidad con WPA en los dispositivos utilizados.

Finalmente, este tipo de implementación es fácilmente adaptable a los cambios o crecimientos de las infraestructuras tecnológicas y también se pueden utilizar modelos de autenticación distribuidos para organizaciones con varias sedes o varias redes LAN.

6.2.3.3 Análisis de requerimientos

Una vez se haya decidido la implementación de un sistema de control de acceso a la red de datos basado en el estándar 802.1x, se debe determinar cuáles son los requerimientos de funcionalidad que se deben cumplir así como los requerimientos técnicos que implica la implementación de este tipo de solución, con lo cual se definirá el diseño y la selección del tipo de autenticación a utilizar.

A continuación se describen los principales requerimientos funcionales y técnicos:

Funcionalidad

La implementación de una infraestructura de acceso inalámbrico a la red de datos de una organización puede ser conducida por diferentes requerimientos funcionales, algunos de los más comunes son:

- Ofrecer acceso a los servicios tecnológicos al creciente número de usuarios de la organización.
- Brindar acceso a algunos servicios para invitados, clientes o socios de negocio que visitan instalaciones habilitadas para el acceso inalámbrico.
- Ofrecer servicios de acceso a la red pública (Internet) y ofrecer servicios de valor agregado (ISP).
- Habilitar el acceso a los recursos informáticos para usuarios que requieren movilidad dentro de las instalaciones de la organización.

Cada uno de estos escenarios requiere la infraestructura alámbrica e inalámbrica adecuada con los mecanismos de seguridad adecuados, por lo cual, la selección de estos componentes puede variar ampliamente de un escenario a otro.

Seguridad requerida

El grado de seguridad requerido es una de las consideraciones en el momento de seleccionar el mecanismo de control de acceso y autenticación a la red.

Este grado de seguridad puede variar ampliamente entre una y otra organización; en otras palabras, si el nivel de riesgo que representa la infraestructura inalámbrica contra la integridad, confidencialidad y disponibilidad de la información no es considerable o se ha disminuido con otras medidas, tales como la autenticación en el acceso a servicios y aplicaciones, políticas de grupo, cifrado de información u otras; se puede seleccionar mecanismos de autenticación menos complejos pero acordes a dicho nivel de riesgo.

También el tamaño de las organizaciones y su limitación en recursos pueden conllevar a que se implementen mecanismos de seguridad menos robustos pero que disminuyen el riesgo a niveles aceptables.

Requerimientos técnicos

Si funcionalmente ya se delimitaron los posibles tipos de autenticación a implementar, es importante validarlos y seleccionar el más indicado con base en los requerimientos técnicos que implica la implementación de estos posibles tipos de autenticación.

Integración y compatibilidad

En el momento de la implementación las organizaciones ya pueden contar con un servicio de autenticación de usuarios, el cual requiere mantener y poder integrar a la nueva infraestructura de acceso inalámbrico. Para esto, dichas organizaciones deben validar si estos servicios de autenticación son compatibles con 802.1x, y si es así, determinar los tipos de autenticación EAP que soportan.

Sin embargo, si el servicio de autenticación a la red con el que se cuenta no es compatible con los nuevos requerimientos para asegurar el acceso inalámbrico, se debe verificar si realizando una actualización del servicio este quede habilitado para implementar 802.1x, o si por el contrario se requiere implementar uno nuevo de las muchas alternativas comerciales y gratuitas disponibles que brindan amplias capacidades y compatibilidad con 802.1x

Otro punto importante es considerar la estructura de dominio de usuarios con la que se cuenta y si se pretende utilizar la misma base de datos de usuarios para validar la autenticación a la red en la implementación de 802.1x a realizar.

Generalmente, la mayoría de servidores de autenticación que soportan 802.1x permiten integrarse con las bases de datos de usuarios de la organización, para poder así utilizar

las mismas credenciales almacenadas en estas, para la autenticación a nivel de acceso a la red. Sin embargo, es necesario verificar esta compatibilidad en el servidor de autenticación que se pretende utilizar, u optar por manejar una base de datos alterna, implementada sobre el mismo servidor, de acuerdo a las opciones que este brinde para realizar dicho proceso.

En los usuarios (suplicantes)

Desde el punto de vista de los clientes de acceso inalámbricos, más exactamente sobre los requerimientos de la conexión, se debe validar si las plataformas utilizadas en los clientes soportan el tipo de autenticación elegido o si por el contrario requieren un componente de software que los habilite para realizarla.

En la TABLA XIV se presenta el tipo de soporte disponible en algunos sistemas operativos para los diferentes métodos de autenticación EAP:

TABLA XIV. SOPORTE DE EAP EN LOS PRINICIPALES SISTEMAS OPERATIVOS COMO CLIENTE

Sistema Operativo	Versión del S.O	EAP-TLS	EAP-TTLS	PEAP	LEAP
Windows XP, Vista, 7, 8, 8.1	Todas	Cliente Nativo	Cliente de Tercero	Cliente Nativo	Cliente de Tercero
Linux(Ubuntu/Fedora)	Desde la 6.06 LTS a la versión estable más actual 15.04	Cliente de Tercero	Cliente de Tercero	Soportado	Soportado
Mac	Todas	Cliente de Tercero	Cliente de Tercero	Soportado	Soportado
Android	Basado en el núcleo de Linux Todas	Cliente de Tercero	Cliente de Tercero	Soportado	Soportado
IOS	Desde la versión 3.0 a la más actual IOS 8.4	Cliente de Tercero	Cliente de Tercero	Soportado	Soportado

Es posible que organizaciones con diferentes plataformas a nivel de clientes prefieran implementar un mismo cliente 802.1x para tener un sistema homogéneo y facilitar su administración.

En los Access Points (autenticadores)

Entre los principales requerimientos, sobre estos dispositivos, para poder implementar un mecanismo de seguridad para el control del acceso inalámbrico, se encuentran:

- Compatibilidad con 802.11 y soporte de cifrado (WEP al menos)
- Capacidad de implementar el servicio de control de acceso 802.1x

En el servidor de autenticación

Los principales requerimientos en este componente, para poder implementar la solución de seguridad basada en 802.1x, son:

- Compatibilidad con 802.1x.
- Soporte de diversos tipos de autenticación EAP (TLS, TTLS, PEAP)
- Capacidad de registro (Accounting).
- Soporte para el control de acceso en redes inalámbricas.
- Flexibilidad para validar a los suplicantes mediante varios métodos (Base de datos de usuarios local, directorio de usuarios LDAP, certificados, entre otros).
- Adicionalmente, en este componente se deben verificar las capacidades de integración con otros servicios de la red.

Finalmente se muestra en breves palabras, mediante un cuadro descriptivo, en la TABLA XV, las principales características del protocolo de seguridad 802.1x.

TABLA XV. RESUMEN ESTANDAR 802.1x

Estándar 802.1X					
Puntos Clave	Realiza el control de acceso a una red mediante un proceso de autenticación.	Requiere de: Usuario o “suplicante”, Punto de acceso o “Autenticador” y Servidor de autenticación.	Hace referencia al uso del protocolo de autenticación extensible EAP.	La implementación de 802.1x para redes inalámbricas utiliza un servidor de autenticación como el RADIUS.	
Porque 802.1X	Evitar la difusión del identificador de red o SSID.	Establecer listas de control de acceso por direcciones físicas.	Utilizar cifrado en las conexiones.	Segmentar los puntos de acceso inalámbricos	Combinar mecanismo de autenticación a la red y cifrado de datos.

Ventajas	Costos asociados, ya que se puede utilizar servidores de autenticación (RADIUS, IAS6).	Es fácilmente adaptable a los cambios o crecimientos de las infraestructuras tecnológicas.	Se pueden utilizar modelos de autenticación distribuidos para organizaciones con varias sedes o varias redes LAN.
Funcionalidad	Ofrecer acceso a los servicios tecnológicos.	Brindar acceso a algunos servicios para invitados, clientes o socios de negocio.	Habilitar el acceso a los recursos informáticos para usuarios que requieren movilidad.
Seguridad Requerida	Puede variar ampliamente entre una y otra organización.	Tamaño de las organizaciones y su limitación en recursos pueden conllevar a que se implementen mecanismos de seguridad menos robustos.	

6.3 Fase 3: Analizar las políticas de seguridad y privacidad necesarias para todo el personal académico y administrativo, quienes hacen uso de la red LAN y WLAN de la Universidad Nacional de Loja

6.3.1 Determinar los grupos de trabajo según la estructura jerárquica de la red de datos de la Universidad Nacional de Loja

Para la determinación de los grupos de trabajo dentro de la Universidad Nacional de Loja, es necesario conocer quiénes son los usuarios finales de la red de datos, ya sean estos usuarios pertenecientes o ajenos a la misma.

La Universidad Nacional de Loja cuenta con diferentes áreas tanto académicas como administrativas. En cada una de estas áreas existe un número significativo de usuarios de la red de datos. Los principales tipos de usuarios que hacen uso de la red de datos de la institución son los siguientes:

- **Docentes:** Se especifica a cada uno de los profesionales que son encargados de impartir conocimientos a los estudiantes
- **Administrativos:** Se hallan todas las personas que trabajan para la institución fuera del cargo de brindar conocimiento a los alumnos de la misma.
- **Trabajadores:** Colaboradores en la institución, que no llevan la denominación de administrativos.

- **Estudiantes:** Especifica cada una de las personas que se hallan adquiriendo conocimiento dentro de la Institución
- **Invitados:** Específica a todas aquellas personas ajenas a la Institución que por a o b razones hacen uso del servicio de internet.

La organización de los grupos, dentro de Unidades Organizativas (UO), viene dada de acuerdo al organigrama estructural actual de la institución, el cual se indica en la Figura 7.

En cuanto a la red de datos LAN o cableada, los tipos de usuarios que hacen uso de la misma son: Docentes y Administrativos. Es por ello que este tipo de conexión se ofrece, con prioridad a estos dos tipos de usuarios.

En cuanto a los equipos existentes en laboratorios y bibliotecas de cada una de las áreas académico-administrativas, estos cuentan con este tipo de conexión, pero no han sido considerados como grupo de usuarios, ya que estos equipos son de uso tanto de personal académico como administrativo.

Mientras que en el tipo de conexión Inalámbrico o WLAN, hacen uso todos los tipos de usuarios que presenta la institución.

La Universidad Nacional de Loja cuenta con diversas redes de conexión inalámbrica, cada una de ellas destinadas a cada tipo de usuario, se pretende que las redes UNL, CAMPUS UNL y EDUROAM se hallen restringidas por el mecanismo de autenticación, ya que las mismas son principalmente para brindar servicio de internet a los usuarios pertenecientes a la institución; mientras que la red INVITADOS se halle libre para cualquier usuario que desee una conexión a internet, principalmente para el tipo de usuario Invitados, ya que los mismos no contaran con una cuenta en el directorio activo.

La institución cuenta con diversos tipos de usuarios a los cuales se los ha integrado en las diferentes Unidades Organizativas, de acuerdo al organigrama estructural de la institución.

6.3.2 Obtención de las necesidades actuales de los usuarios a nivel de servicios de la red, en procesos académicos, como administrativos que se ejecutan en la Universidad Nacional de Loja

Para conocer las necesidades actuales de los usuarios a nivel de servicios de red, es necesario tener claro los usuarios de la misma. Siendo así dichos usuarios se pueden apreciar en dos categorías los mismos que son: Usuario Administrador y Usuarios Finales.

El o los Usuarios Administradores, son los encargados, como su nombre lo dice, de administrar la herramienta; creando: Unidades Organizativas y usuarios finales, administrando contraseñas y configurando políticas o directivas, para cada una de las UO existentes en el Directorio Activo.

Por otra parte los Usuarios Finales de la red de la Universidad Nacional de Loja, son todos y cada uno de los inmersos en las UO, estos usuarios básicamente son: Docentes, Estudiantes, Administrativos y Trabajadores, Invitados corresponde también a usuarios finales de la red de datos, con la diferencia que ellos no se hallan inmersos en las UO.

Dentro de la Universidad Nacional de Loja se ejecutan diversos procesos tanto académicos como administrativos, procesos que hacen uso de la red de datos que brinda la institución, a continuación se especifica los principales procesos que son llevados por cada uno de los usuarios finales de la red.

Los procesos académicos son llevados principalmente por los usuarios finales: Docentes y Estudiantes.

Docentes, realizan los siguientes procesos académicos con uso de la red de datos.

- Investigación de nuevos conocimientos para impartir a los estudiantes de la Universidad Nacional de Loja.
- Trabajo en nuevos proyectos para difundir sus resultados, ampliando la reputación de la Institución.
- Acceso al Sistema de Gestión Académica (SGA) de la Universidad Nacional de Loja, con el fin de publicar calificaciones y asistencias de los estudiantes.
- Inmersión en la base de datos de consultas científicas que ofrece la Universidad Nacional de Loja.

En cuanto a Estudiantes, realizan los siguientes procesos.

- Desarrollo y envió de trabajos o consultas, enviadas por los docentes de la institución.
- Investigación personal, accediendo a la base de datos de consultas científicas que ofrece la Universidad Nacional de Loja.
- Uso del correo Institucional para consultar información enviada por cada uno de los docentes.
- Acceso al SGA, para consultas respecto a calificaciones y asistencias en el transcurso del periodo académico.
- Ingreso al SGA para obtención de matrícula del siguiente periodo académico.

Los procesos administrativos son ejecutados principalmente por cada uno de los usuarios finales denominados Administrativos, estos procesos depende del cargo que ocupe cada usuario, entre los principales, los siguientes:

- Admisión y Matriculación de estudiantes.
- Homologación para cambios en las carreras por parte de los estudiantes.
- Expedición de títulos y certificaciones.
- Autorizaciones, acreditaciones e inscripciones.
- Ayudas, becas.
- Convenios.
- Procedimientos en Tesorería.
- Ingresos de Derecho Público.
- Operaciones con Bienes.
- Selección, Contratación de Personal y Provisión de puestos.
- Elaboración de Disposiciones.

Los usuarios finales, Trabajadores, normalmente no desempeñan labores académicas o administrativas, principalmente son colaboradores en las diferentes áreas académico-administrativas de la institución.

Las necesidades actuales son enfocadas de acuerdo al Usuario Administrador, ya que mediante estas, se realizan las configuraciones necesarias en Active Directory, tanto en la creación de Unidades Organizativas, usuarios y políticas o directivas para cada uno de ellos.

Luego de una plática personal con la persona encargada de la red en ese momento, Ing. Nohelia Alfonsina Bustamante Pardo, se pudo conocer las siguientes necesidades en cuanto al uso de los servicios de la red, por parte de los usuarios finales.

- Cada uno de los usuarios finales debe pertenecer a una UO, para así poder manejar políticas específicas para cada uno de ellos.
- Debe existir un método de autenticación y autorización de usuarios en la red, ya que mediante el mismo se evitara diversos problemas en la misma.
- La autenticación de usuarios debe ser segura.
- Se debe contralar el tiempo de conexión de cada uno de los usuarios, aplicando intervalos de tiempo de acuerdo al uso necesario de la red.
- Evitar que cualquier usuario ajeno (Invitados) a la Universidad Nacional de Loja, pueda tener uso excesivo de la red.

6.3.3 Determinar las políticas de seguridad y privacidad de acuerdo a las funciones que desempeña el personal tanto académico como administrativo

En base al alcance del proyecto, las políticas de seguridad aplicables actualmente dentro de la red de la Universidad Nacional de Loja, se encuentran basadas en el Servidor de Directivas de Redes de Active Directory.

El Servidor de directivas de redes (NPS), permite crear y aplicar directivas de acceso a la red de la Universidad Nacional de Loja, con fines de conexión mediante autenticación y autorización. Permite configurar y administrar de forma centralizada directivas de autenticación de acceso a la red, autorización y mantenimiento de clientes, aplicando las siguientes directivas o políticas de seguridad:

6.3.3.1 Política de acceso a la red mediante RADIUS server

El servidor de políticas de red realiza la autenticación, autorización y administración de conexiones de forma centralizada para los conmutadores de autenticación inalámbricos.

Cuando se usa NPS como un servidor RADIUS, se configuran los servidores de acceso a la red, como clientes RADIUS en NPS. Además, se configuran las directivas de redes que usa NPS para autorizar las solicitudes de conexión. También puede configurar la administración de cuentas RADIUS para que NPS registre la información de las cuentas.

6.3.3.2 Política Network Access Protection (NAP) policy server.

Cuando se configura NPS como un servidor de directivas de NAP, NPS evalúa los informes de mantenimiento enviados por equipos clientes compatibles con NAP que desean conectarse a la red. NPS también actúa como un servidor RADIUS cuando está configurado con NAP, realizando tareas de autenticación y autorización para las solicitudes de conexión. Se puede configurar directivas y opciones de NAP en NPS, lo que incluye validadores de mantenimiento del sistema, directivas de mantenimiento y grupos de servidores de actualizaciones que permiten a los equipos cliente actualizar su configuración para ser compatibles con la directiva de red de la organización.

Se puede configurar NPS con cualquier combinación de las características anteriores. Por ejemplo, un servidor NPS para que actúe como un servidor de directivas NAP con uno o varios métodos de cumplimiento.

6.3.3.3 Políticas de seguridad aplicadas al usuario final

Estas políticas se determinaron en base a los requerimientos obtenidos específicamente para los usuarios finales de la red de datos de la Universidad Nacional de Loja, y se listan a continuación.

Directivas de contraseña

Esta directiva se aplica a todos los usuarios en el dominio unl.edu.ec, todas las cuentas de los usuarios finales contaran con una longitud mínima de ocho caracteres, la complejidad queda deshabilitada, para que cada uno de los usuarios ingrese su contraseña a su parecer.

La contraseña por defecto es el número de cedula de cada uno de los usuarios finales de la red.

Todos los usuarios de la red de datos de la Universidad Nacional de Loja, al realizar la primera conexión de red, deberán hacer el cambio de su contraseña obligatoriamente.

Directivas de sesión

Esta directiva permite administrar el tiempo que el usuario puede mantener sesión o ser excluido, además ofrece la opción de dar de baja o colocar una fecha de caducidad a la cuenta de cada uno de los usuarios finales.

El nombre de usuario para cada uno de ellos es correo electrónico institucional por ejemplo: pedro.ramirez@unl.local

Las características implementadas en el dominio unl.edu.ec se listan a continuación:

Docentes, Administrativos y Trabajadores

Directiva por defecto

- El tiempo de sesión será durante los días laborables, estos son de lunes a viernes estipulados por los organismos superiores de la Universidad Nacional de Loja en horario de 7:00 a 22:00 horas.
- Caducidad de la cuenta: anualmente.

Directivas opcionales

- En días estipulados como feriados por los organismos competentes se determina la suspensión del servicio de autenticación, como medida de seguridad.
- En días no laborables estipulados como día normal de trabajo por los organismos competentes, se determina la habilitación del servicio de autenticación.
- Si el servicio se encuentra suspendido, como medida se seguridad, el usuario mediante oficio y detallando sus actividades, deberá solicitar la habilitación del mismo, en la Dirección de Telecomunicaciones e Información.

Estudiantes

Directiva por defecto

- El tiempo de sesión será durante los días laborables, estos son de lunes a viernes estipulados por los organismos superiores de la Universidad Nacional de Loja en horario de 7:00 a 21:00 horas.
- Caducidad de la cuenta: cada seis meses.

Cada una de las cuentas de los usuarios finales, tienen fecha de caducidad, ya que en un lapso de tiempo usuarios finales dejan de pertenecer a la institución e ingresan nuevos usuarios a la misma.

Al existir un administrador del Directorio Activo, este puede realizar la configuración de las directivas opcionales, de acuerdo a las estipulaciones indicadas, de la misma manera en la caducidad de las cuentas, deberá cargar la base de datos de todos los usuarios finales al ser caducadas las mismas, de acuerdo a las directivas por defecto.

6.3.3.4 Políticas establecidas para la administración de equipos

En vista que la Universidad Nacional de Loja, no cuenta con políticas o directivas aplicables a los usuarios de la institución para la administración de los equipos, se ha determinado las siguientes políticas, como propuesta, en base a los perfiles de los usuarios tanto administrativos, docentes y estudiantes.

TABLA XVI. POLÍTICAS PARA LA ADMINISTRACIÓN DE EQUIPOS

Directiva	Administrativo	Docente	Estudiante
Quitar del escritorio el icono de equipo.	No aplica.	No aplica.	Aplica
Quitar el elemento propiedades del menú contextual del elemento equipo.	Aplica	Aplica	Aplica
Quitar el elemento propiedades del menú contextual del elemento documentos.	No aplica	No aplica	Aplica
Quitar del escritorio el icono de la papelera de reciclaje.	Aplica	Aplica	Aplica
No guardar la configuración al salir.	Aplica	Aplica	Aplica
Prohibir el ajuste de la barra de herramientas del escritorio.	Aplica	Aplica	Aplica
Activar Active desktop.	Aplica	Aplica	Aplica
Lista de inclusión de archivos de alto riesgo.	Aplica	Aplica	Aplica
No permitir animaciones en las ventanas.	Aplica	Aplica	Aplica
Desactivar menús personalizados.	Aplica	Aplica	Aplica
Quitar y evitar el acceso a los comandos Apagar, Reiniciar, Suspender.	No aplica	No aplica	Aplica
Quitar el vínculo de juegos del menú de inicio.	Aplica	Aplica	Aplica
No guardar el historial de documentos abiertos recientemente.	No aplica	No aplica	Aplica
Quitar el icono de Música del menú de inicio.	No aplica	No aplica	Aplica
Cambiar el botón de encendido del menú inicio.	No aplica	No aplica	Aplica
No permitir el anclado a la barra de tareas.	No aplica	No aplica	Aplica
Bloquear toda la configuración de la barra de tareas.	Aplica	No aplica	Aplica
Ocultar elementos específicos del Panel de Control.	Aplica	Aplica	Aplica
Ocultar la página Configurar acceso y programas predeterminados.	No aplica	No aplica	Aplica
Buscar impresoras en la red.	Aplica	Aplica	No aplica
Impedir la eliminación de impresoras.	Aplica	Aplica	Aplica
Impedir añadir impresoras.	No aplica	No aplica	Aplica
Impedir cambiar la combinación de colores.	Aplica	Aplica	Aplica

Impedir cambiar el tema.	Aplica	Aplica	Aplica
Impedir cambiar el estilo visual de ventanas y botones.	Aplica	Aplica	Aplica
Prohibir seleccionar el tamaño de fuente del estilo visual.	Aplica	Aplica	Aplica
Impedir cambiar el color y la apariencia.	Aplica	Aplica	Aplica
Impedir cambiar el fondo de pantalla.	Aplica	Aplica	Aplica
Impedir cambiar los iconos del escritorio.	No aplica	No aplica	Aplica
Impedir cambiar punteros del mouse.	Aplica	Aplica	Aplica
Impedir cambiar protector de pantalla.	Aplica	Aplica	Aplica
Impedir cambiar sonidos.	Aplica	Aplica	Aplica
Ocultar la página “Programas y características”.	No aplica	No aplica	Aplica
Quitar administrador de tareas.	No aplica	No aplica	Aplica
Quitar bloqueo de equipo.	No aplica	No aplica	Aplica
Desactivar el cmd.	No aplica	No aplica	Aplica
Quitar el menú Ejecutar	No aplica	No aplica	Aplica

6.4 Fase 4: Realizar la implementación y pruebas de funcionalidad del servidor, verificando la prestación del servicio como controlador de dominio; dentro del Área de la Energía y los Recursos Naturales no Renovables de la Universidad Nacional de Loja

6.4.1 Instalación y configuración de la plataforma operativa en el servidor físico

La instalación de Windows Server 2012, fue en un equipo físico (Blade), en la Dirección de Telecomunicaciones e Información, las características de este fueron dadas por el Ing. Milton Palacios, ex Director de la Dirección de Telecomunicaciones, siendo estas las que se muestran en la Figura 11.

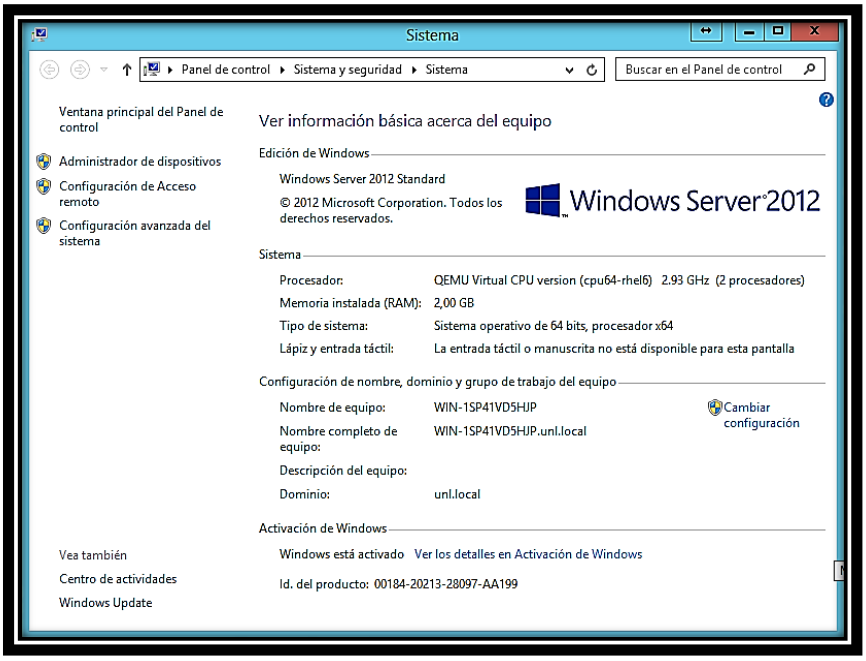


Figura 11. Información básica del equipo (Windows Server 2012 Standard)

Fuente: Autor

Cabe recalcar, que para la manipulación del servidor se lo hace mediante control remoto.

Para realizar la instalación de Windows Server 2012, Microsoft aconseja tomar en cuenta las siguientes recomendaciones:

- **Desconectar los dispositivos SAI (UPS):** Si se tiene conectado un sistema de alimentación ininterrumpida (SAI o UPS) al equipo de destino, se debe desconectar el cable serie antes de ejecutar el programa de instalación. El programa de instalación intenta detectar automáticamente los dispositivos conectados a los puertos serie, y los equipos SAI o UPS pueden causar problemas en el proceso de detección.
- **Realizar una copia de seguridad de los servidores:** Las copias de seguridad deben incluir todos los datos y toda la información de configuración que necesita el equipo para funcionar. Es importante que se realice una copia de seguridad de la información de configuración de los servidores, sobre todo de aquellos que proporcionan la infraestructura de red, como los servidores de protocolo de configuración dinámica de host (DHCP). Cuando se realice las copias de seguridad, no se debe olvide incluir las particiones de arranque y del sistema, así como los datos del estado del sistema. Otra forma de realizar copias de

seguridad de la información de configuración es crear un conjunto de copia de seguridad para la Recuperación automática del sistema.

- **Deshabilitar el software de protección antivirus:** El software de protección antivirus puede interferir en la instalación. Por ejemplo, puede ralentizar en gran medida la instalación al examinar cada uno de los archivos que se copia localmente en el equipo.
- **Ejecutar la Herramienta de diagnóstico de memoria de Windows:** Se debe ejecutar esta herramienta para probar la memoria RAM del equipo.
- **Proporcionar los controladores de almacenamiento masivo:** Para proporcionar el controlador durante la instalación, en la página de selección de disco, se debe hacer clic en cargar controlador o presionar F6. Puede buscar el controlador o dejar que el programa de instalación lo busque en el medio.
- **Tener en cuenta que Firewall de Windows esté activado de manera predeterminada:** Las aplicaciones de servidor que deben recibir conexiones de entrada no solicitadas generarán errores hasta que cree reglas de firewall de entrada que las admitan.

Debido a que la instalación de Windows Server 2012 es sencilla, se la realiza de igual manera que para la instalación de cualquier otro sistema operativo proporcionado por Microsoft, no se presentan imágenes referentes a la instalación del mismo.

6.4.2 Instalación y configuración de la herramienta Active Directory con las políticas de seguridad y servicios establecidos

Una vez instalado el Sistema Operativo Windows Server 2012 podemos observar la primera vista que este muestra, como se lo representa en la Figura 12.

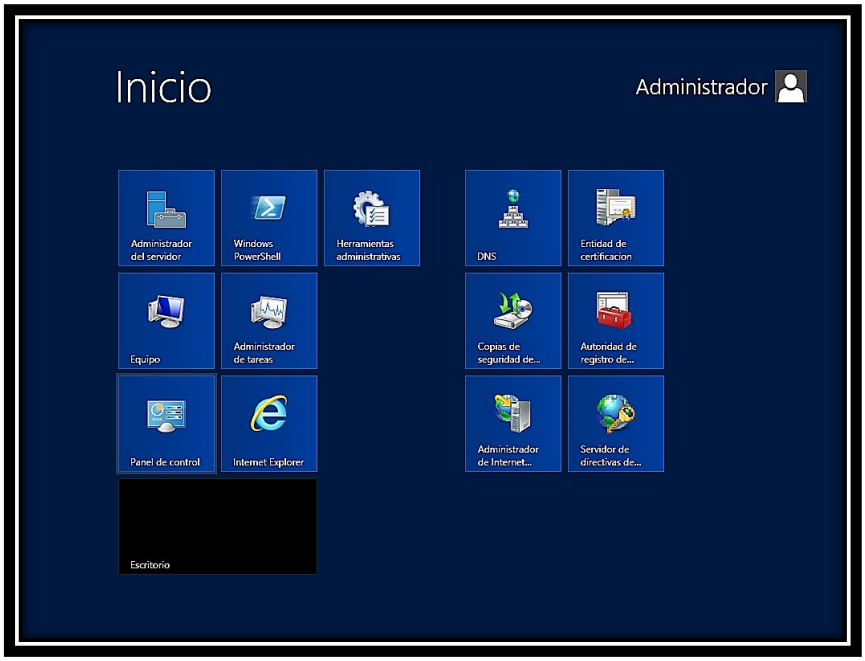


Figura 12. Primera vista del sistema operativo

Fuente: Autor

La dirección IP del servidor fue dada por el antiguo director de Dirección de Telecomunicaciones, Ing. Milton Palacios.

6.4.2.1 Instalación de Servicios de Active Directory (AD DS)

En la Figura 13 se observa el Asistente de configuración que implementa Windows Server 2012 Standard, dentro de las opciones que presenta se debe seleccionar: Agregar roles y características.

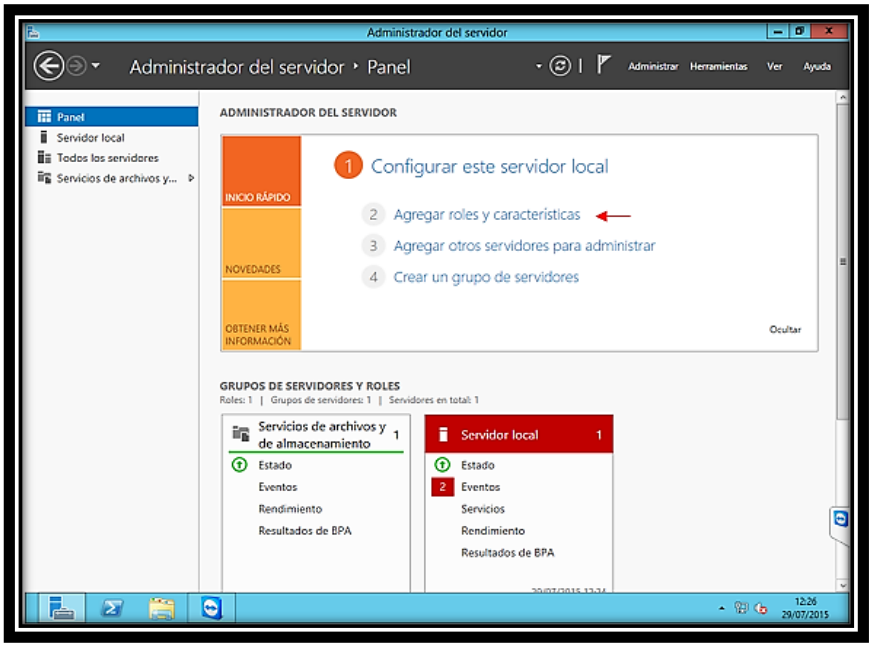


Figura 13. Instalación de Active Directory AD DS

Fuente: Autor

Una vez seleccionado el ítem Agregar roles y características, se desplegara una ventana denominada: Asistente para agregar roles y características, como se muestra en la Figura 14, lo único que se hace en este asistente es hacer en clic en siguiente para continuar con la instalación.

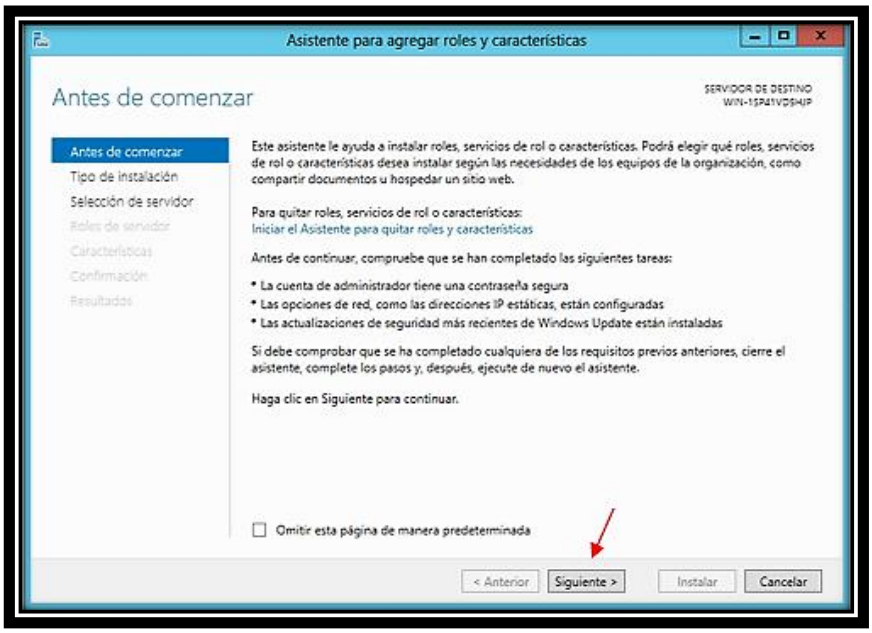


Figura 14. Asistente para agregar roles y características

Fuente: Autor

Al hacer clic en siguiente, se debe seleccionar el tipo de instalación que se realizara, se selecciona Instalación basa en características o roles como se indica en la Figura 15. Una vez seleccionado este ítem pinchamos en siguiente.

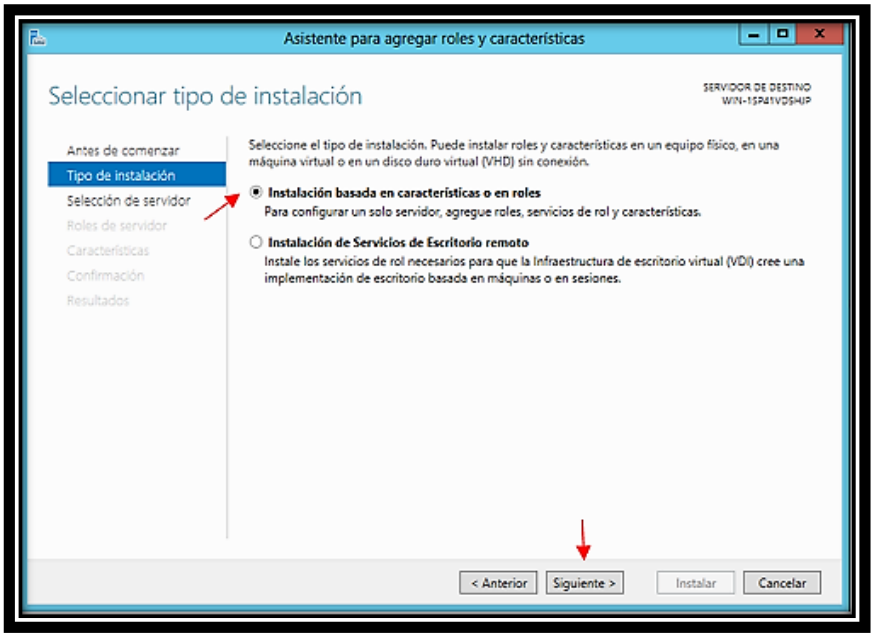


Figura 15. Tipo de instalación

Fuente: Autor

Una vez seleccionado el tipo de instalación, se debe seleccionar el servidor para ello aplicamos el ítem: Seleccionar un servidor del grupo de servidores, como se indica en la Figura 16, al activar este ítem, se mostrara nuestro servidor, al cual se selecciona y se pincha en siguiente.

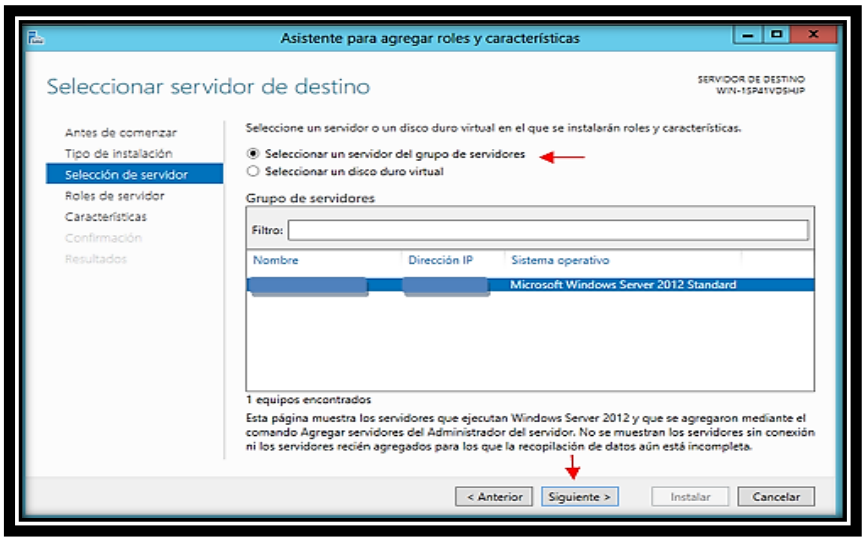


Figura 16. Selección de servidor

Fuente: Autor

Ahora se debe agregar roles al servidor, para ello se selecciona el ítem: Servicios de dominio de Active Directory, al seleccionar este ítem, se desplegará una ventana emergente, en la cual se indica las características a ser instaladas, como se muestra en la Figura 17, se pincha en el botón Agregar características para continuar con la instalación.

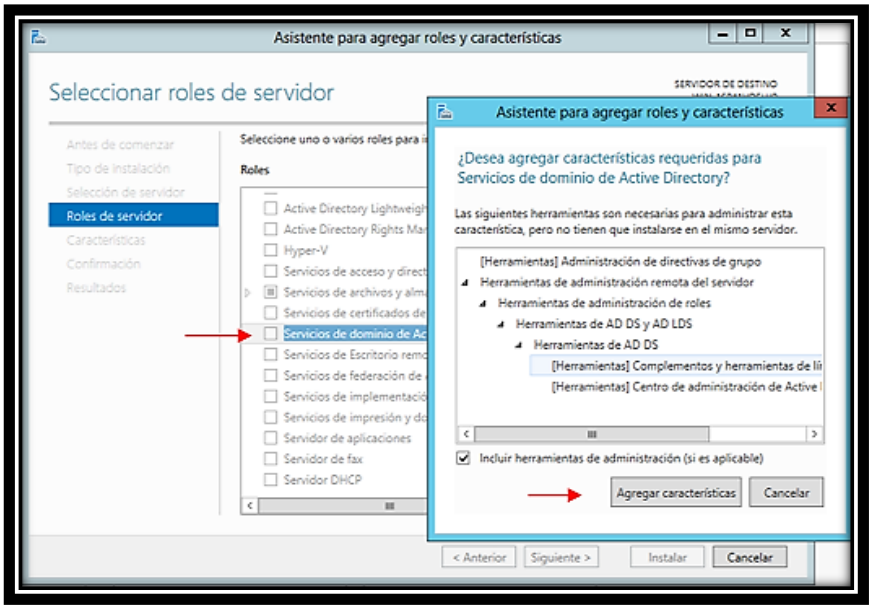


Figura 17. Roles de servidor

Fuente: Autor

Al hacer clic en Agregar características, se muestra las características instaladas, en la ventana siguiente se selecciona el ítem Administración de directivas de grupo, y se da clic en Siguiente. Como se puede visualizar en la Figura 18.

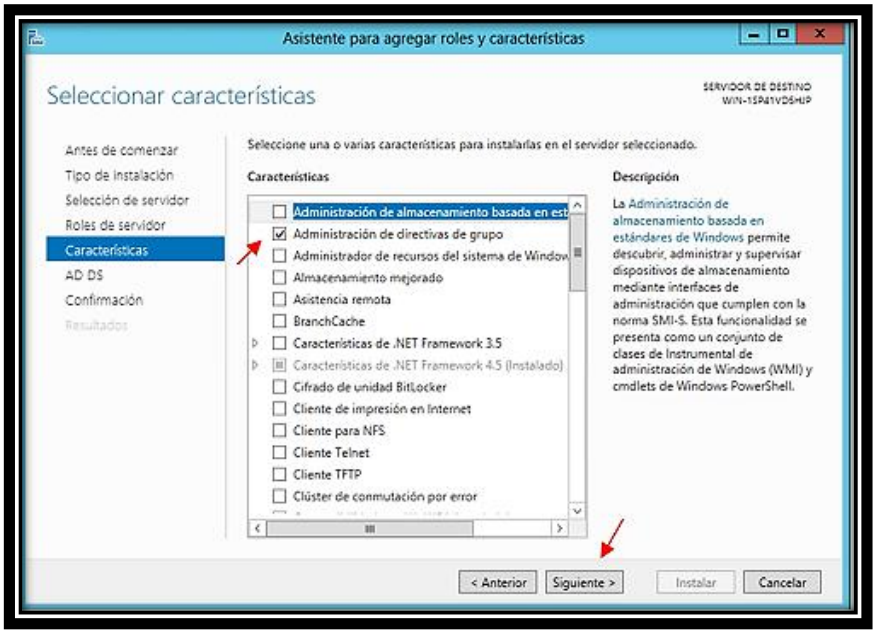


Figura 18. Características del servidor

Fuente: Autor

La Figura 19, muestra información acerca de los servicios del directorio activo y unas observaciones del mismo, lo único que se realiza aquí es dar clic en Siguiente.

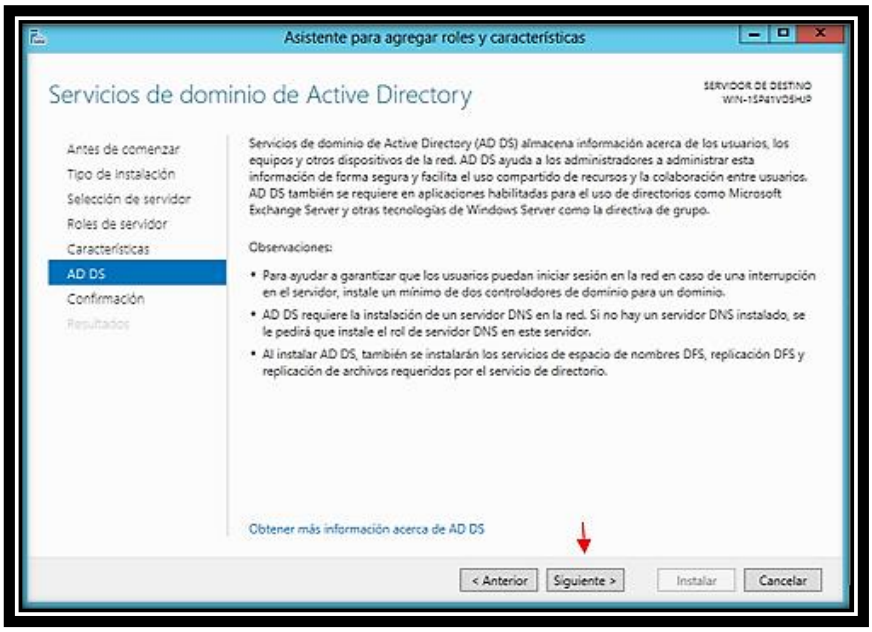


Figura 19. Información y observaciones servicios de dominio de Active Directory

Fuente: Autor

La ventana de Confirmar selecciones de instalación, muestra las características que instalar en el servidor, para continuar con la instalación, se da clic en Instalar como indica la Figura 20.

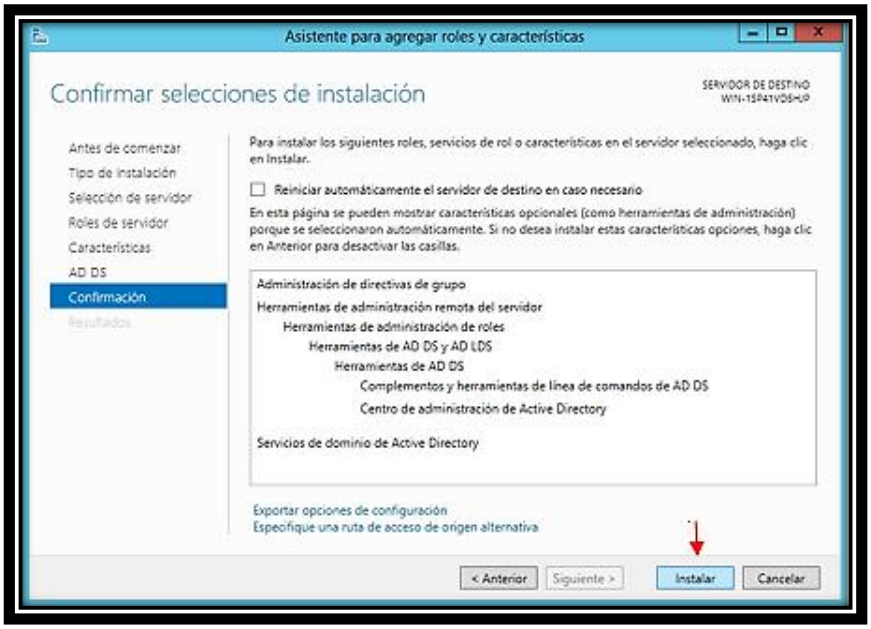


Figura 20. Confirmar selecciones de instalación

Fuente: Autor

Al momento de dar clic en instalar en la Figura 20, se muestra el proceso de instalación, como se detalla en la Figura 21, aquí esperamos un momento que esta culmine.

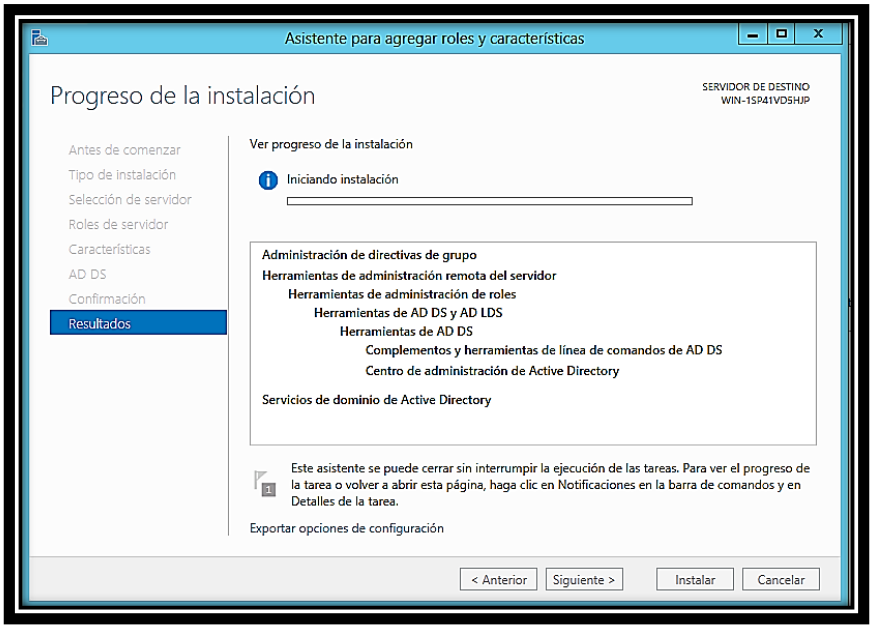


Figura 21. Proceso de instalación

Fuente: Autor

6.4.2.2 Instalación del controlador de dominio

Una vez finalizada la instalación de las características agregadas, se hace clic en Promover este servidor a controlador de dominio como indica la Figura 22.

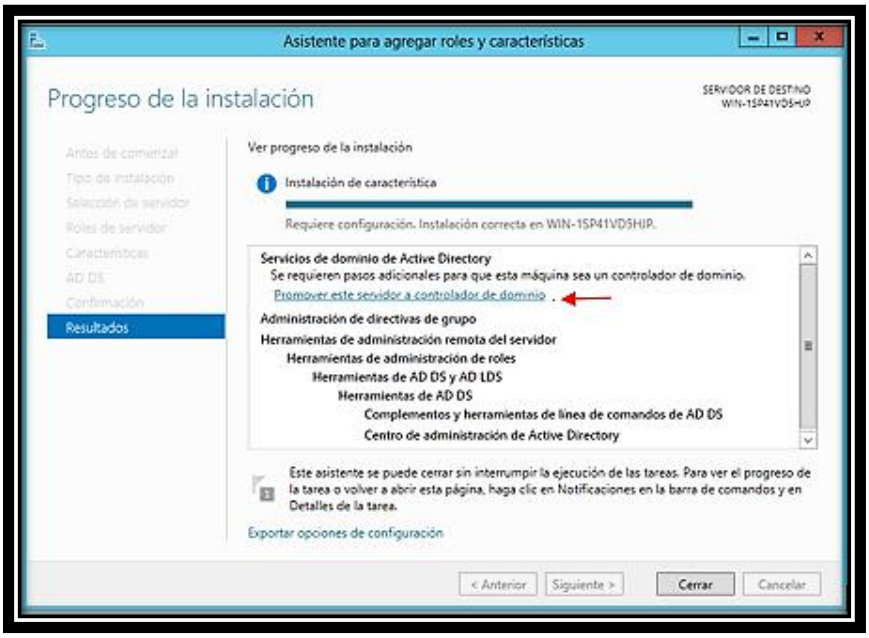


Figura 22. Promover este servidor a controlador de dominio

Fuente: Autor

Para promover el servidor como controlador de dominio se debe agregar un nuevo bosque e ingresar el nombre del dominio raíz en este caso unl.edu.ec, y dar clic en siguiente, como en la Figura 23.

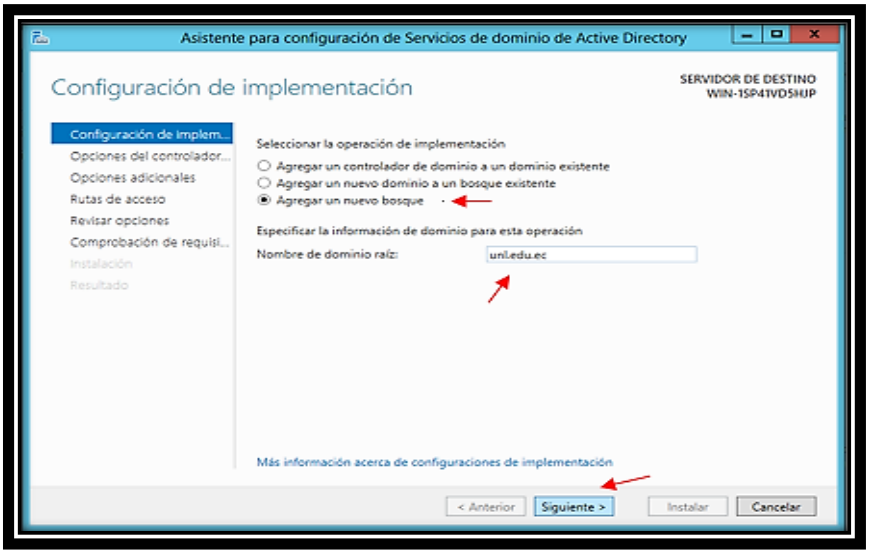


Figura 23. Configuración de implementación

Fuente: Autor

En Opciones del controlador de dominio, se debe asegurar que el nivel funcional del bosque y del dominio, sea Windows Server 2012, en capacidades del controlador de dominio viene marcado el ítem Catalogo Global, La razón de esto es que es el primer controlador de dominio (DC) de la selva de AD y al menos uno debe ser un GC. Por último se establece la contraseña de modo de restauración de servicios de directorio como se muestra en la Figura 24, y se da clic en Siguiente.

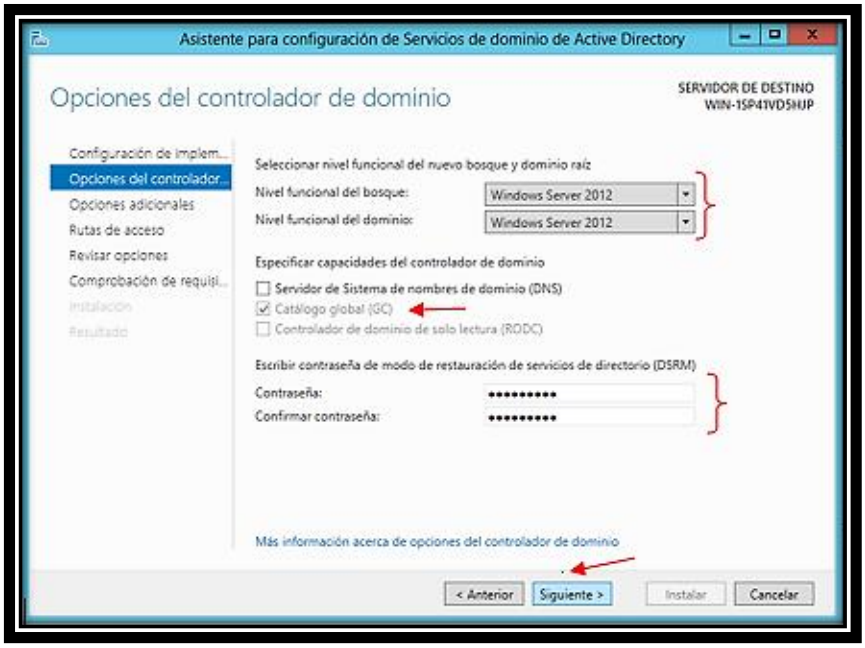


Figura 24. Opciones del controlador de dominio

Fuente: Autor

En opción de DNS simplemente se da clic en Siguiente, para continuar con la configuración.

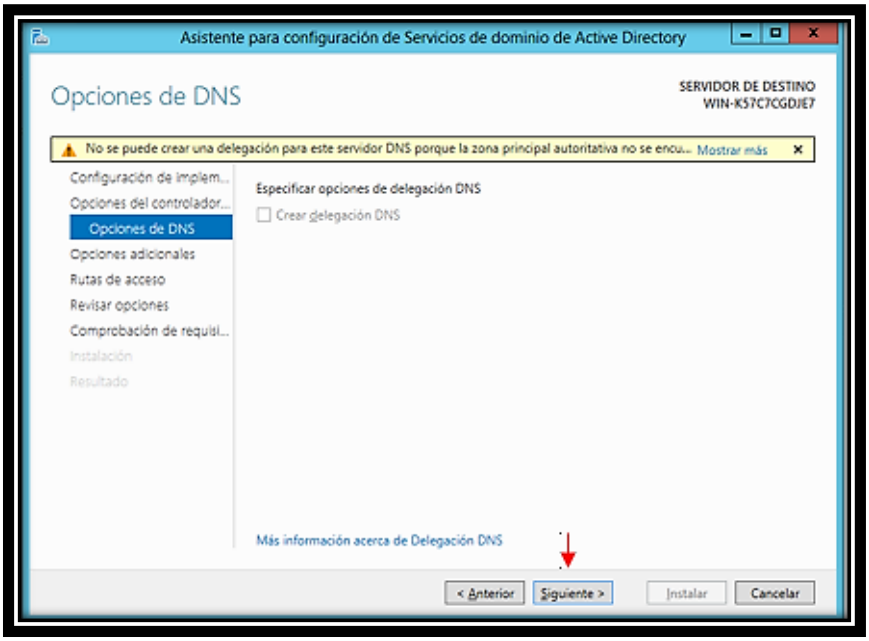


Figura 25. Opción de DNS

Fuente: Autor

En la Figura 26 se pide el nombre del dominio NetBIOS, el cual por defecto se coloca en el campo requerido.

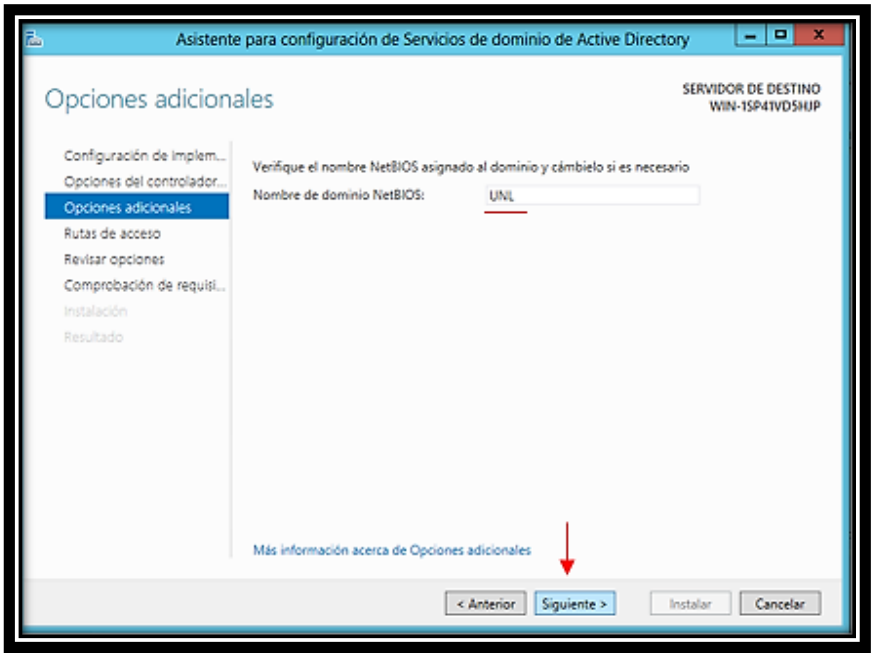


Figura 26. Opciones adicionales

Fuente: Autor

De la misma manera, automáticamente, se especifican las rutas de las carpetas de la base de datos, archivos de registro y carpeta SYSVOL, en la Figura 27 se detalla ello, para continuar se debe dar clic en Siguiente.

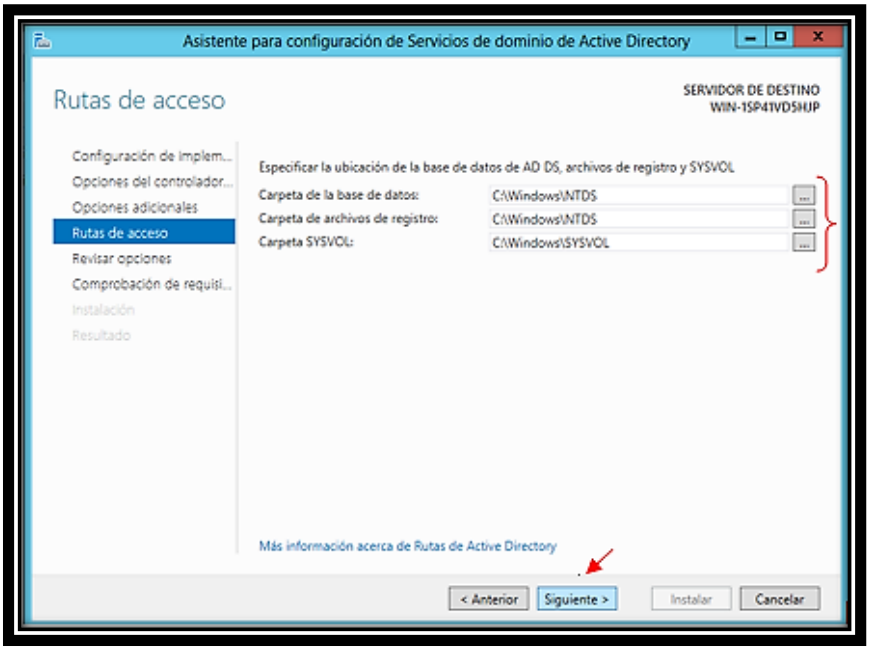


Figura 27. Rutas de acceso

Fuente: Autor

En la ventana Revisar opciones lo unico que muestra se las caracteristicas principales; como el nombre de dominio, nombre de NetBIOS y los niveles funcionales. Esto se describe en la Figura 28. Para continuar se debe hacer clic en Siguiente.

Figura 28. Revisar opciones

Fuente: Autor

Antes de realizar la instalacion se realiza la comprobación de requisitos previos, una ves realizada esta comprobación de manera exitosa, como en la Figura 29, se da clic en instalar.

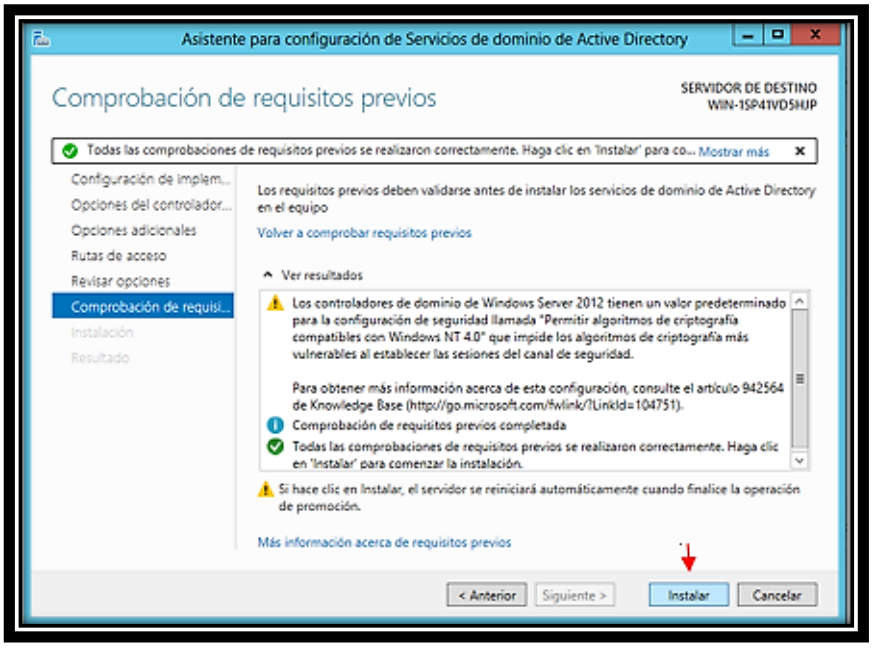


Figura 29. Comprobación de requisitos previos

Fuente: Autor

Al culminar la instalación el equipo se reiniciara automaticamente como indica en la Figura 30.

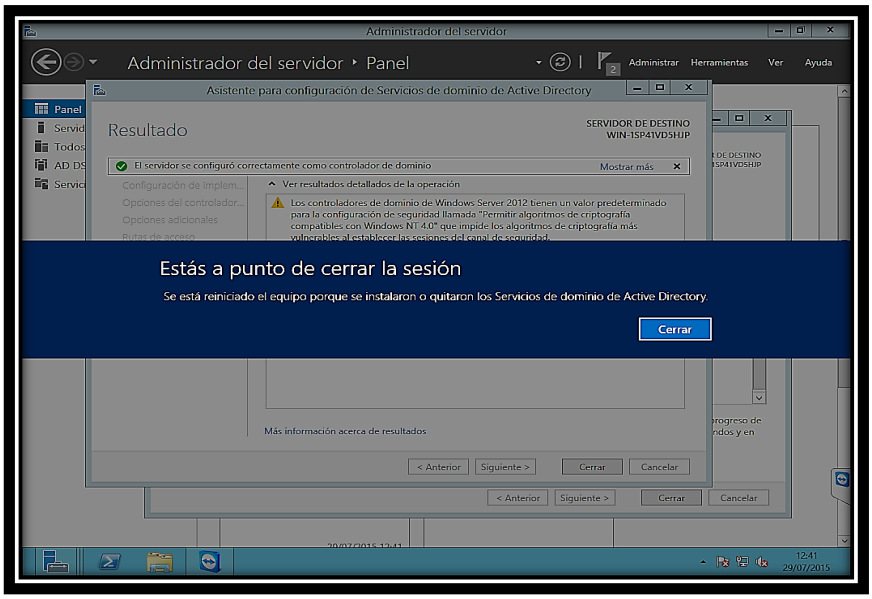


Figura 30. Reinicio automatico del equipo

Fuente: Autor

6.4.2.3 Instalación de Servicios de Certificados de Active Directory

Activo nuevamente el equipo, ingresamos a instalar un nuevo rol en el servidor, activando el item Servicios de certificados de Active Directory, la Figura 31 indica las caracteristicas a instalarse al activar ese item, se da clic en Agregar caracteristicas para continuar con la instalacion.

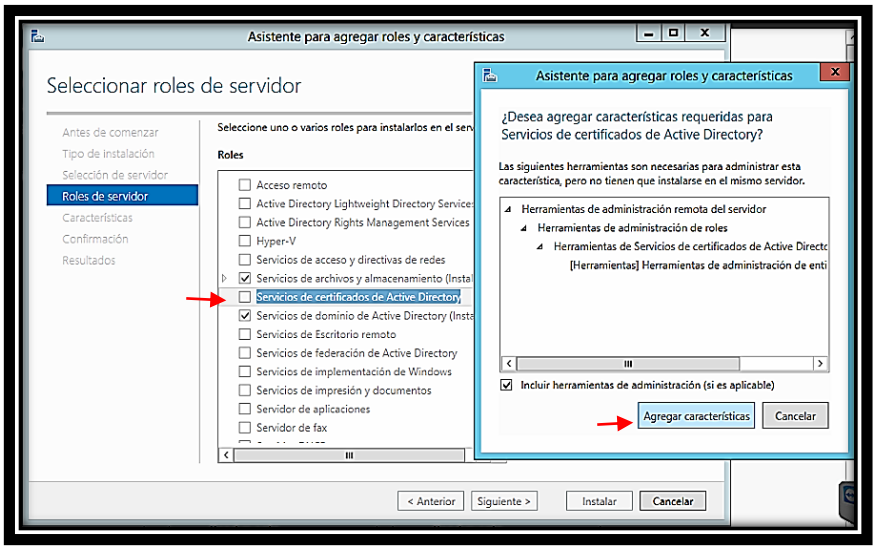


Figura 31. Servicios de certificados de Active Directory

Fuente: Autor

Al agregar las caracteristicas, se muesta una ventana como la Figura 32, en ella se debe hacer clic en Siguiente para continuar.

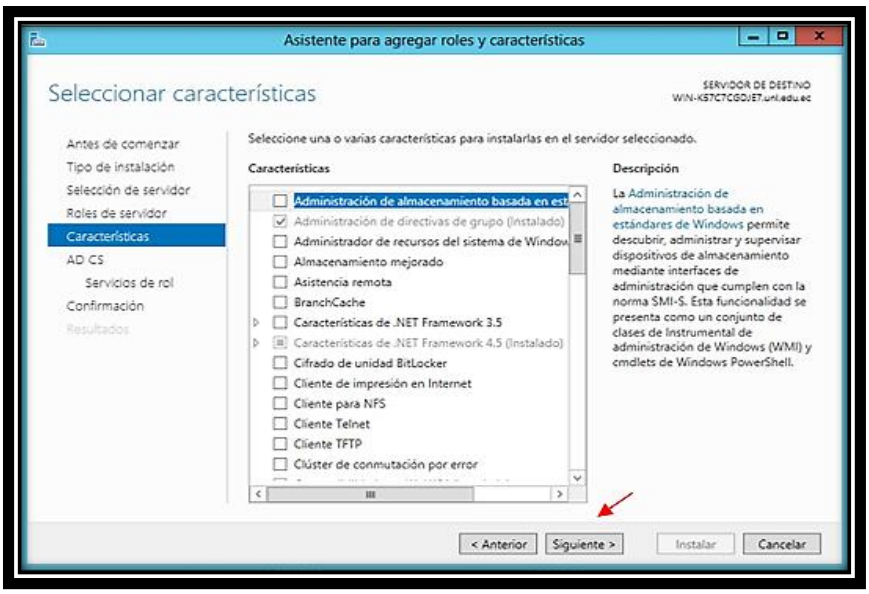


Figura 32. Seleccionar caracteristicas

Fuente: Autor

Al instalar las caracteristicas, se muestra una ventana en donde se indica una serie de informacion respecto a los certificados de Active Directory, en la Figura 33 se da clic en Siguiente.

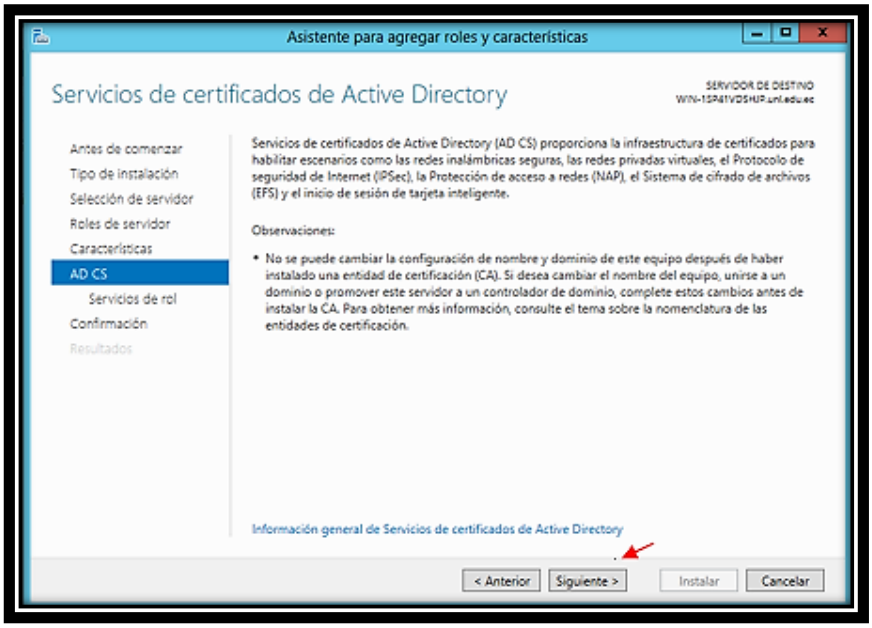


Figura 33. Servicios de certificados de Active Directory

Fuente: Autor

Se debe seleccionar el rol, en la Figura 34 se muesta un listado en el cual se debe activar la casilla Entidad de certificacion, y a continuacion clic en Siguiente.

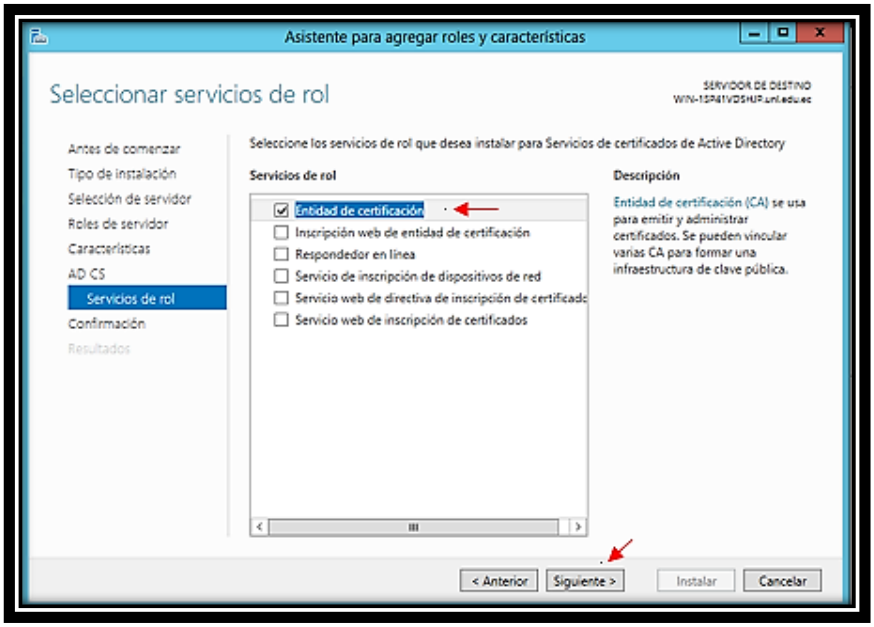


Figura 34. Seleccionar servicos de rol

Fuente: Autor

Luego de seleccionar el rol se debe confirmar el mismo, en la Figura 35 se indica lo mencionado, al tener en claro las caracteristicas a instalarse de debe pinchar el botón Instalar.

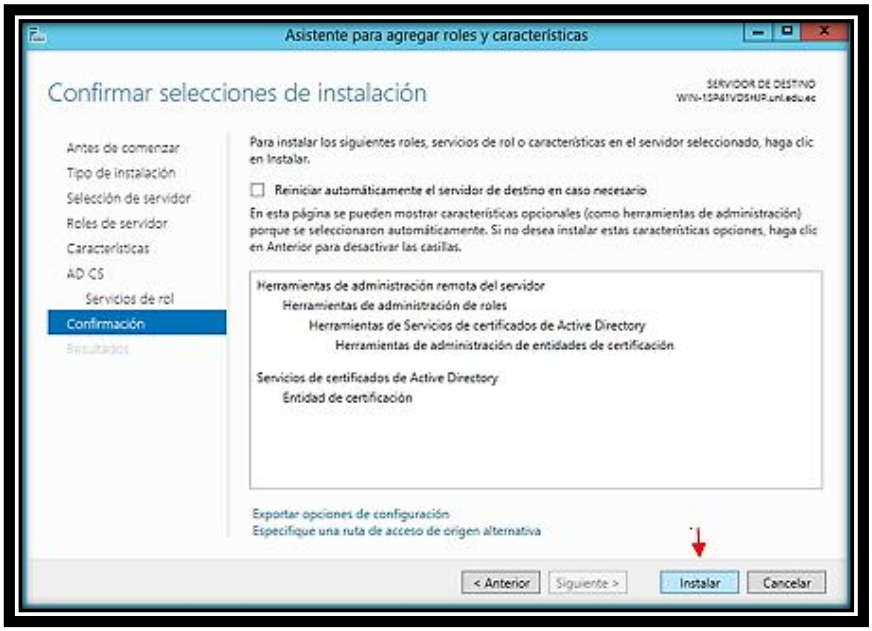


Figura 35. Confirmar selecciones de instalación

Fuente: Autor

Al finalizar la instalación se debe hacer clic en Configurar Servicios de certificados de Active Directory en el servidor de destino, como se indica en la Figura 36.

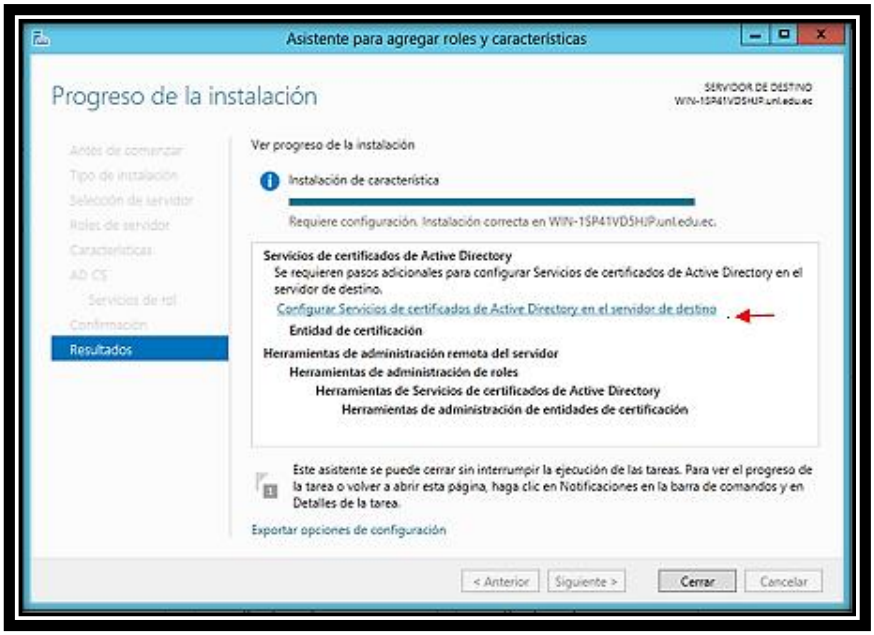


Figura 36. Proceso de instalación

Fuente: Autor

Al hacer clic en configurar los servicios de certificados se muestra un pantalla como la Figura 37, en la cual se especifican las credenciales para configurar servicios de rol, automáticamente se complete el campo de las credenciales, se debe hacer clic en el botón Siguiente.

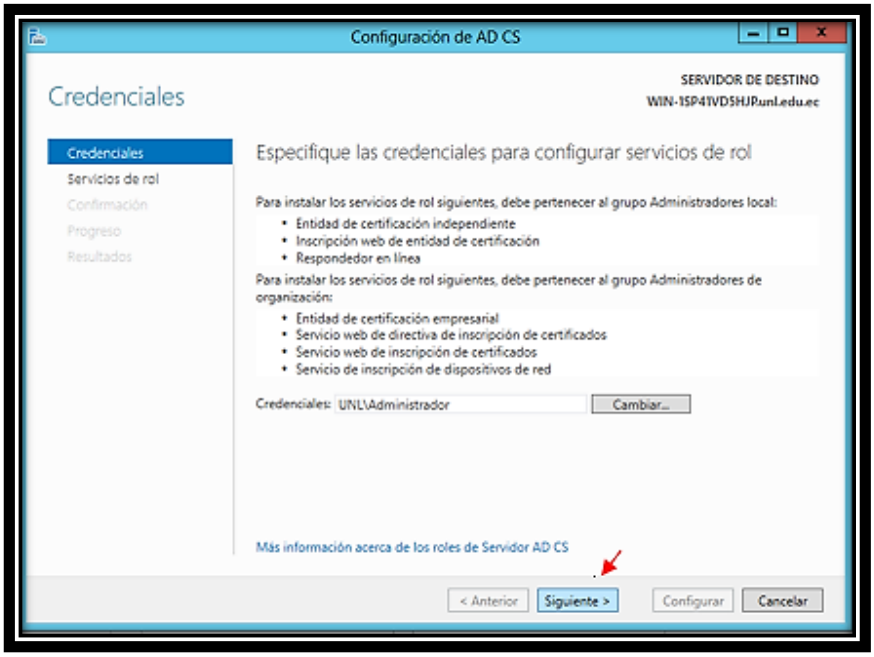


Figura 37. Credenciales

Fuente: Autor

En los servicios de rol se debe seleccionar los servicios de rol que se configurar en la lista que se muestra, se debe seleccionar el ítem Entidad de certificación, como en la Figura 38, una vez seleccionado este ítem se da clic en siguiente para continuar.

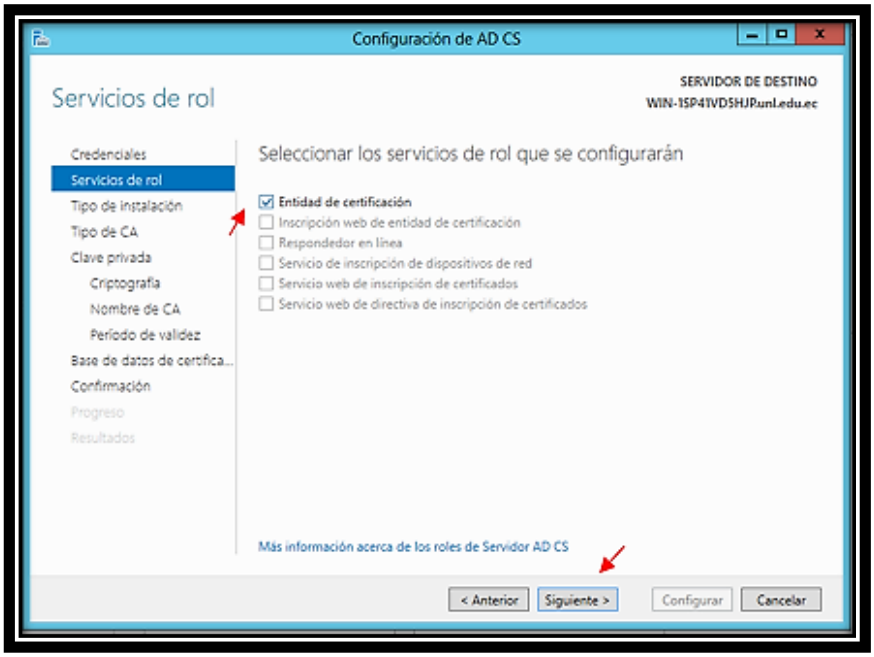


Figura 38. Servicios de rol

Fuente: Autor

En la Figura 39, se muestra el tipo de instalación requerido de la Certificación de Autorización (CA), para ello seleccionamos el ítem CA empresarial, ya que todos nuestros usuarios deben pertenecer al dominio, luego de selección el ítem mencionado, se da clic en siguiente para continuar con la instalación y configuración.

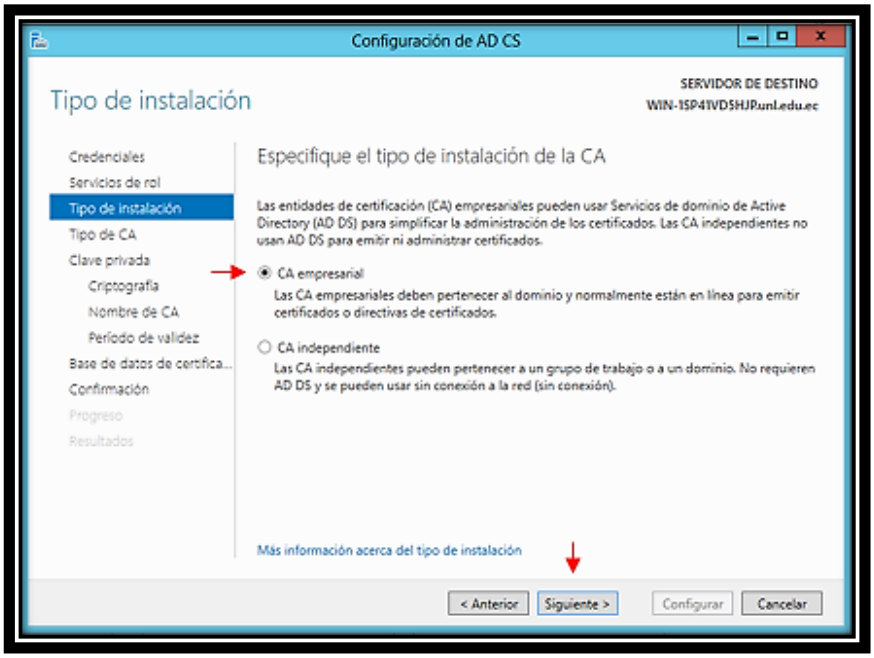


Figura 39. Tipo de instalación

Fuente: Autor

Ahora se necesita seleccionar el tipo de CA, para ello seleccionamos el ítem CA raíz, damos clic en Siguiente, como se indica en la Figura 40.

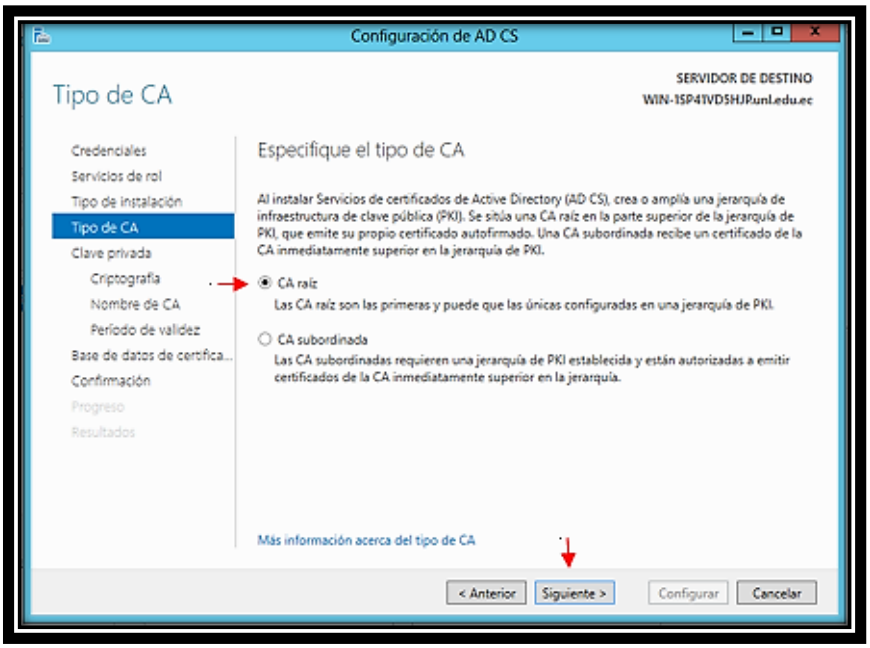


Figura 40. Tipo de CA

Fuente: Autor

Debemos también especificar el tipo de clave privada, para ello se selecciona el ítem Crear una clave privada nueva, ya que es primera vez que se realiza estas configuraciones, una vez seleccionado este ítem damos clic a siguiente, tal como se indica en la Figura 41.

Figura 41. Clave privada

Fuente: Autor

Para la criptografía, se deja los valores por defecto como se indica en la Figura 42. Y se da clic en el botón Siguiente.

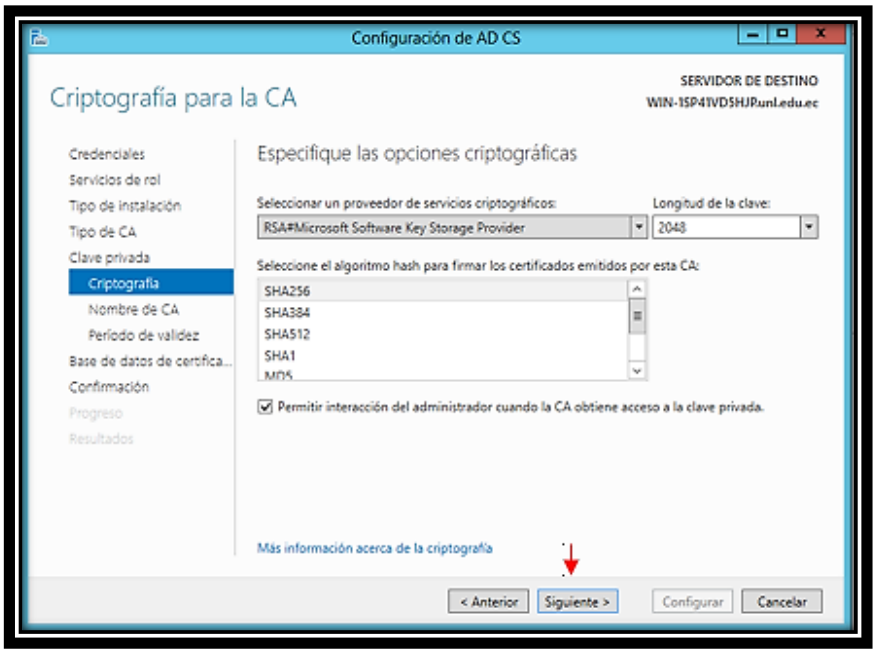


Figura 42. Criptografia para la CA

Fuente: Autor

En la instalación, se requiere el nombre de CA, de igual manera dejamos estos valores por defecto como en se puede apreciar en la Figura 43, así mismo se pincha en el botón Siguiente y se continua con las demás configuraciones.

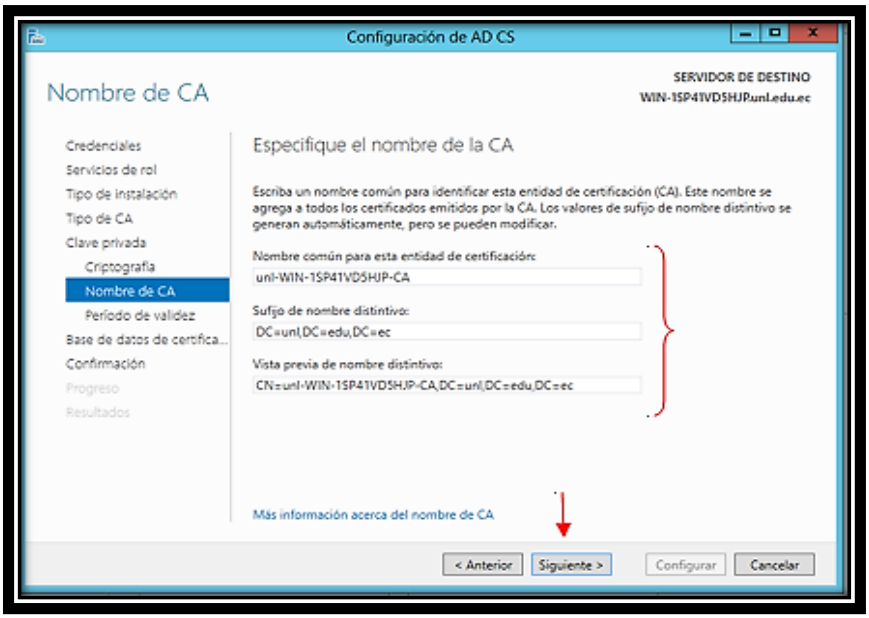


Figura 43. Nombre de CA

Fuente: Autor

A la selección del periodo de validez dejamos por defecto que son de 5 años. Como se indica en la Figura 44, se da clic en siguiente.

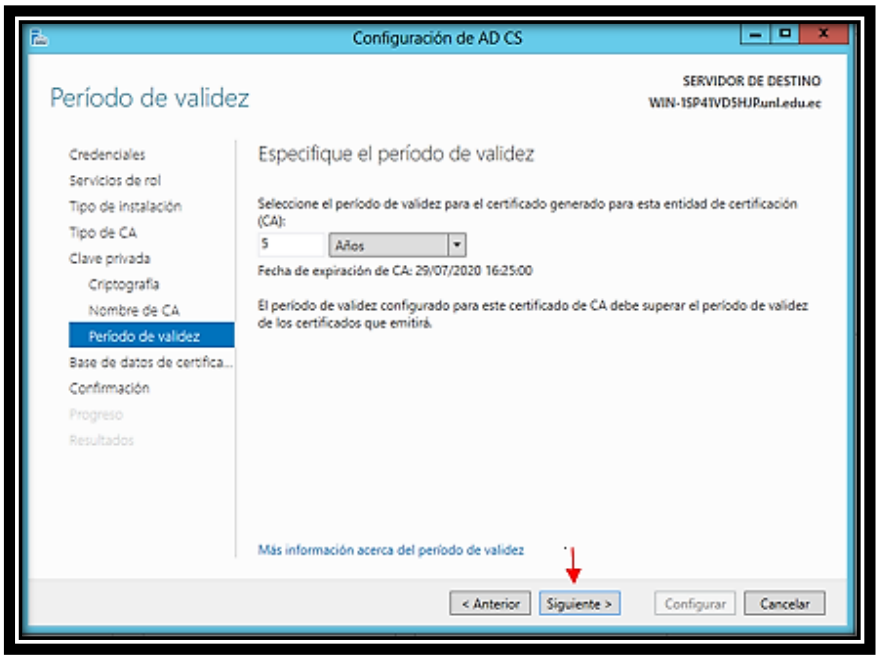


Figura 44. Periodo de validez

Fuente: Autor

La ubicación de la base de datos de certificados y del registro de la base de datos de certificados, viene dada por defecto, si se desea puede ser cambiada, en la Figura 45 se tomó los valores dados por defecto, se da clic en siguiente para continuar.

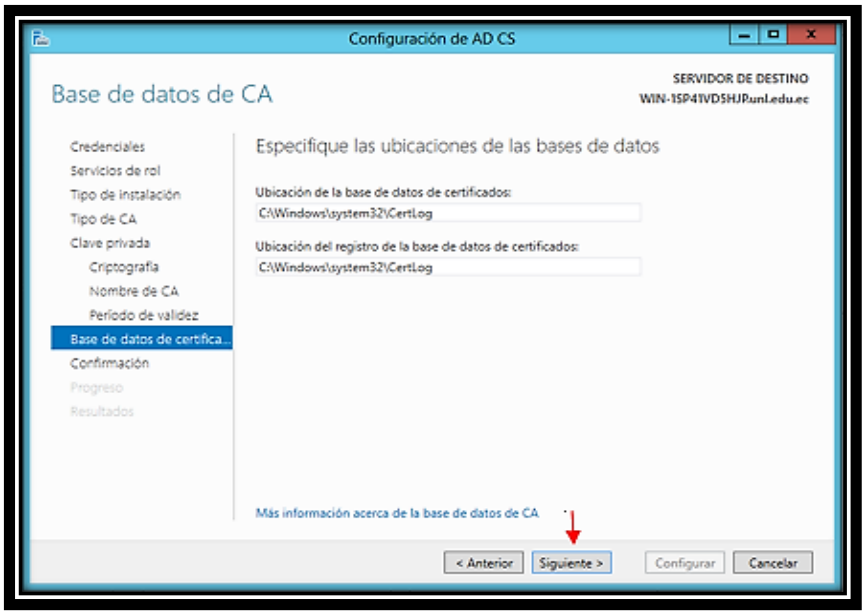


Figura 45. Base de datos de CA

Fuente: Autor

Para finalizar debemos realizar la configuración final para ello, se presenta una pantalla, Configuración, como la de la Figura 46, en ella indica la información ingresada con anterioridad, para finalizar se da clic en Configurar.

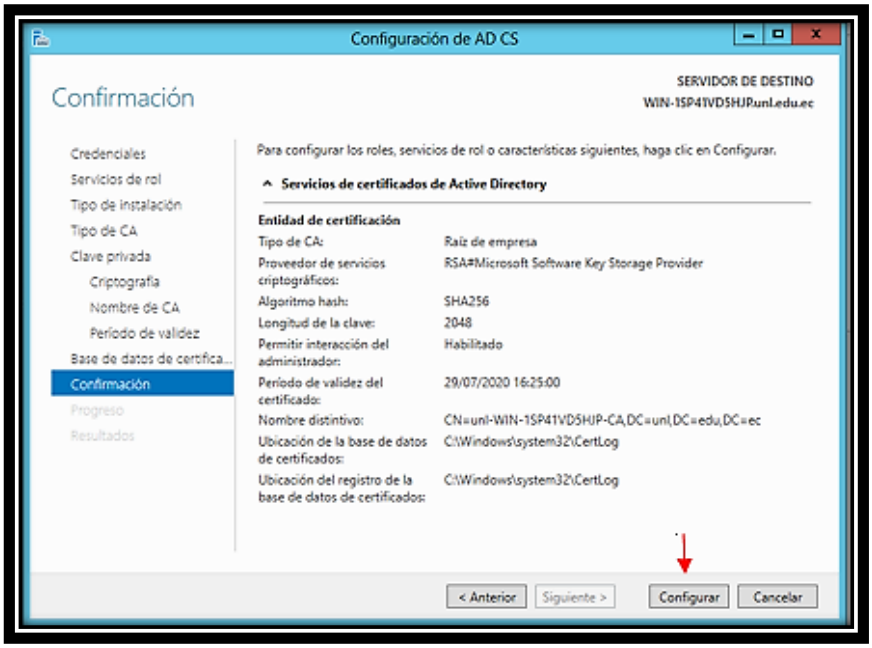


Figura 46. Confirmación

Fuente: Autor

Finalmente se muestra una pantalla como la Figura 47, con los resultados exitosos de la configuración de CA, para cerrar el asistente únicamente se da clic en Cerrar.

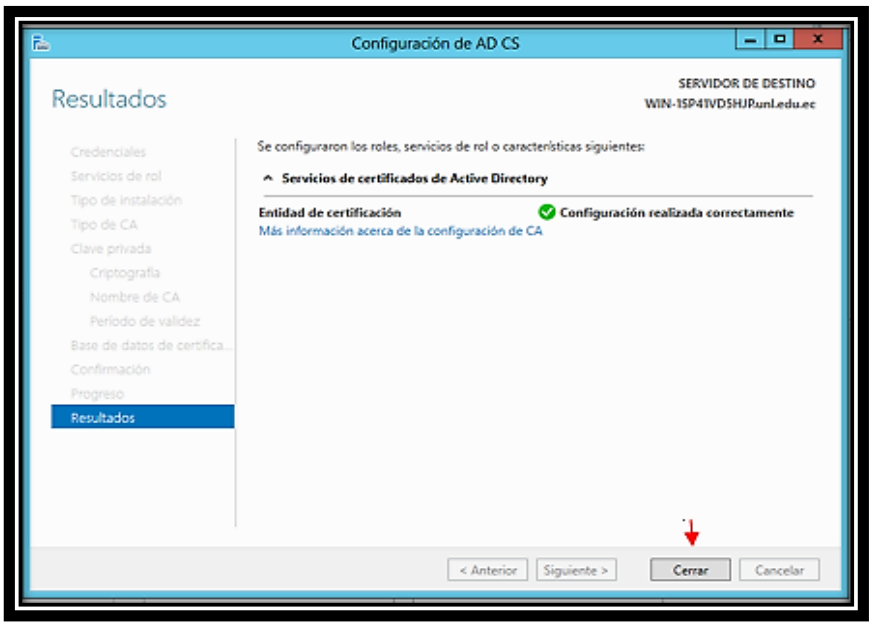


Figura 47. Resultados

Fuente: Autor

6.4.2.4 Configuración de Servidor de Acceso y Directivas de Redes

Para la configuración del Servidor de Acceso y Directivas de Redes, se realiza el mismo procedimiento de agregar roles y características, en el activamos el ítem Servicios de acceso y directivas de redes, como lo indica la Figura 48, al activar este ítem, se arroja una ventana emergente indicando las características a instalarse, se hace clic en el botón Agregar características para continuar con la instalación.

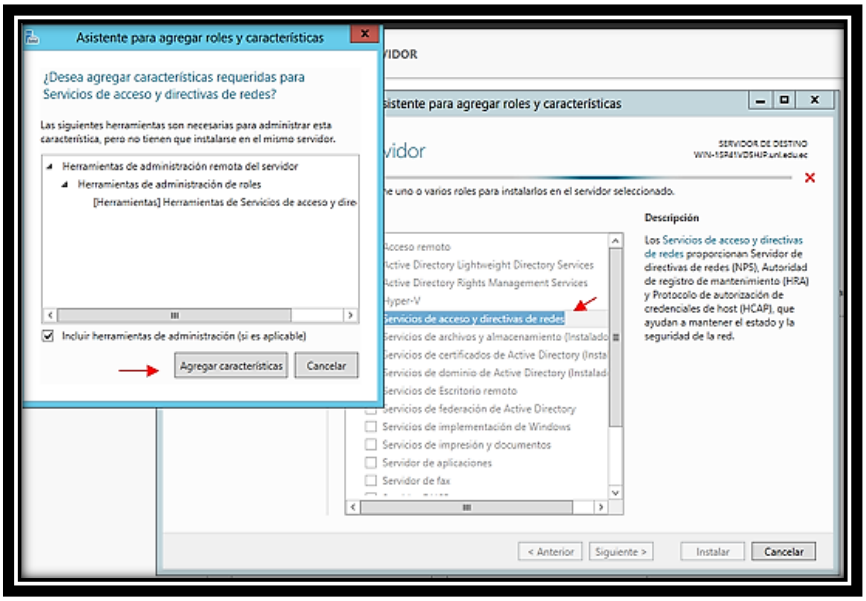


Figura 48. Servidor de acceso y directivas de redes

Fuente: Autor

Al agregar las características, nos indica cuales son estas, como la Figura 49, únicamente se hace clic en el botón Siguiente.

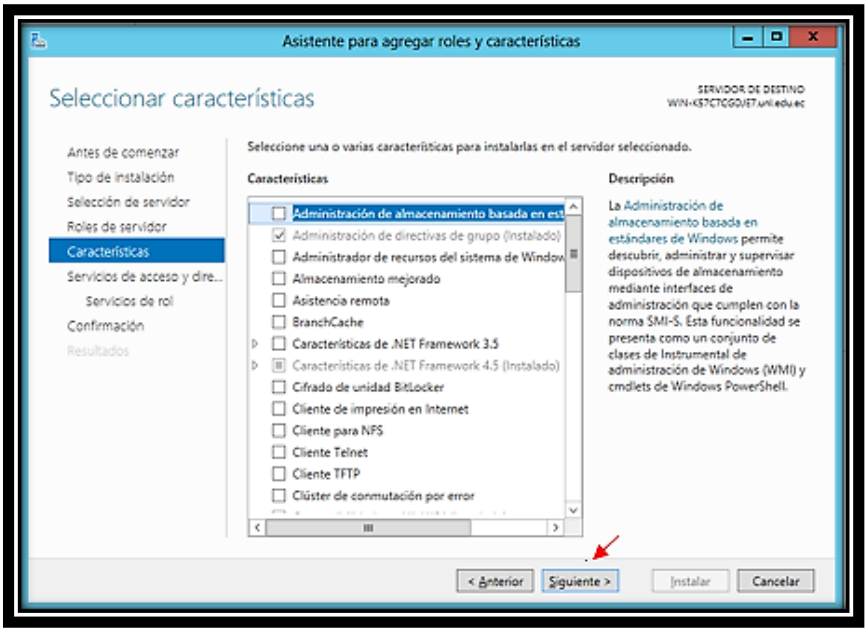


Figura 49. Seleccionar características

Fuente: Autor

Se debe seleccionar los servicios de rol, como la Figura 50, se selecciona el ítem Servidor de Directiva de Redes y se da clic en Siguiente.

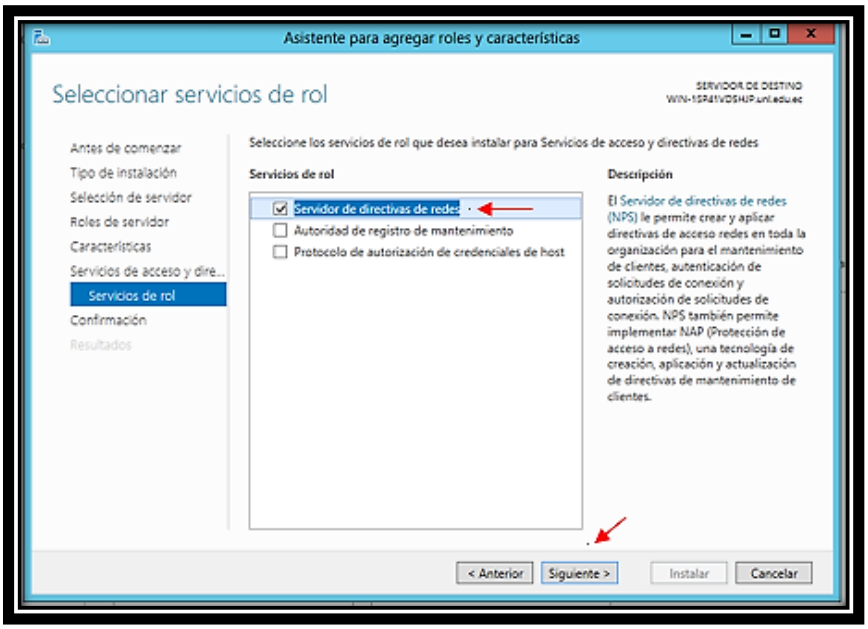


Figura 50. Seleccionar servicios de rol

Fuente: Autor

Una vez seleccionado el rol, únicamente falta realizar la instalación, en la Figura 51 se muestra información de las características a instalarse, si se está de acuerdo con ellas, se da clic en Instalar.

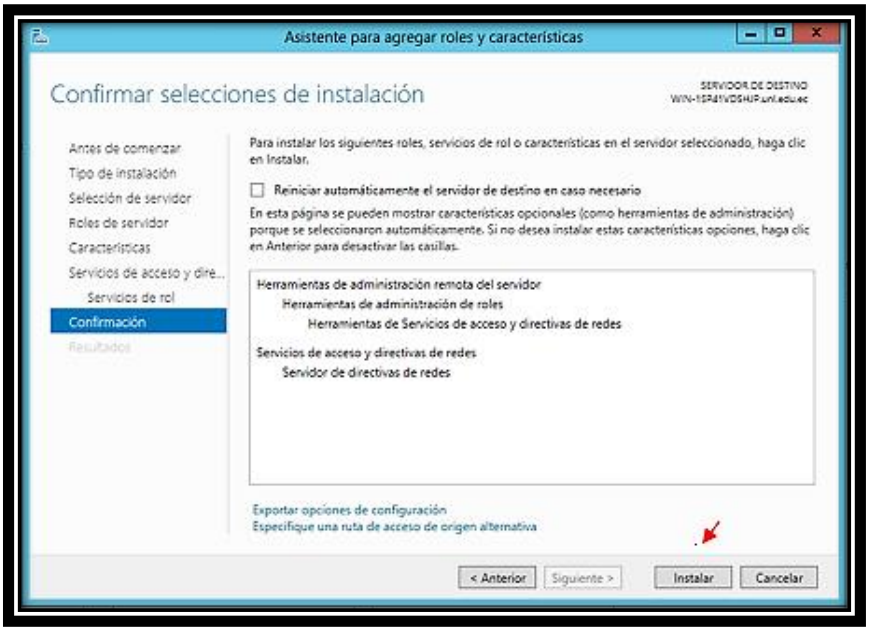


Figura 51. Confirmar selecciones de instalación

Fuente: Autor

En la Figura 52 se puede apreciar la instalación, una vez finalizada la misma se puede cerrar el asistente haciendo clic en Cerrar, y de esta manera se culmina con la instalación.

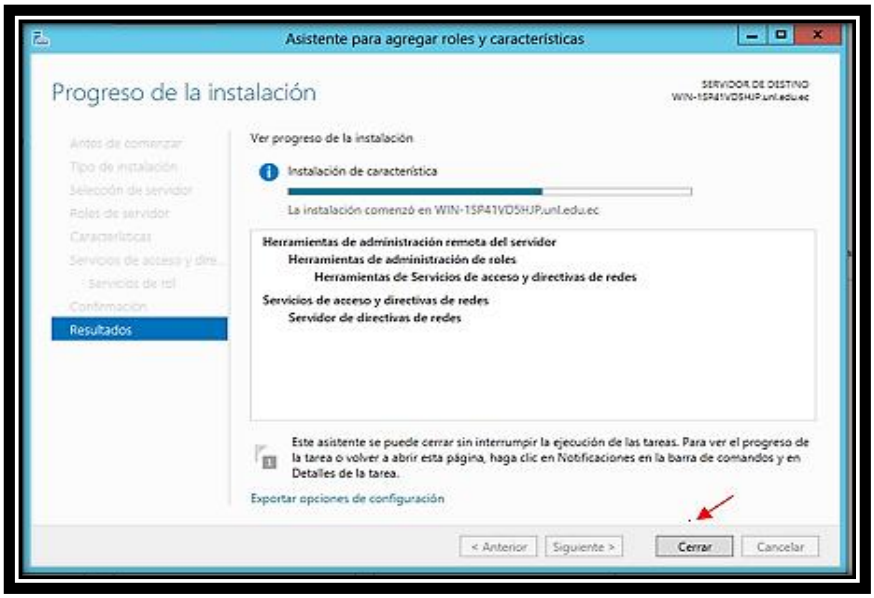


Figura 52. Proceso de instalación

Fuente: Autor

Una vez finalizadas todas estas configuraciones, el servidor se halla configurado correctamente y listo para agregar los usuarios al directorio activo, aplicando la autenticación para cada uno de ellos, agregando políticas o directivas mencionadas con anterioridad.

6.4.2.5 Configuración de usuarios y cuentas

Para ingresar los usuarios al directorio activo y configurar sus cuentas con todas las políticas planteadas, se debe ingresar en inicio, Usuarios y equipos de Active Directory, como se muestra en la Figura 53.

Figura 53. Usuarios y equipos de Active Directory

Fuente: Autor

Una vez dentro de la ventana Usuarios y equipos de Active Directory, se debe crear las Unidades Organizativas, que son a manera de carpetas o directorios en donde constaran tanto los grupos como usuarios pertenecientes a cada uno de ellos, en la Figura 54 se muestra la estructura de estas unidades organizativas de acuerdo al organigrama estructural de la Universidad Nacional de Loja.

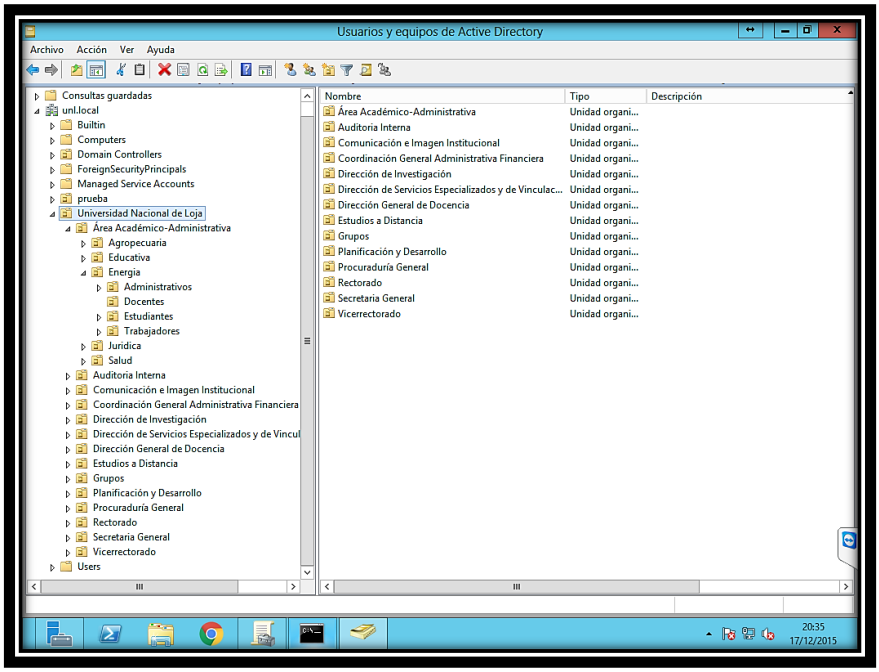


Figura 54. Organización de usuarios

Fuente: Autor

La creación de usuarios dentro del directorio activo, fue realizada de manera masiva mediante una herramienta llamada ActiveRoles Management Shell for Active Directory, utilizando una plantilla en formato .csv, se ingresaron los nombres completos, cedula, correo electrónico, teléfono, cargo, nombre de usuario para su cuenta y la contraseña de la cuenta, entre otros campos. En la Figura 55 se muestra la información básica del usuario Jaramillo Castro Carlos Miguel, docente de la carrera de Ingeniería en Sistemas, al hacer clic en la pestaña Cuenta, accedemos a ella para poder aplicar las políticas de la misma, cabe recalcar que estas políticas se las puede realizar masivamente seleccionando todos los usuarios pertenecientes a una UO en particular.

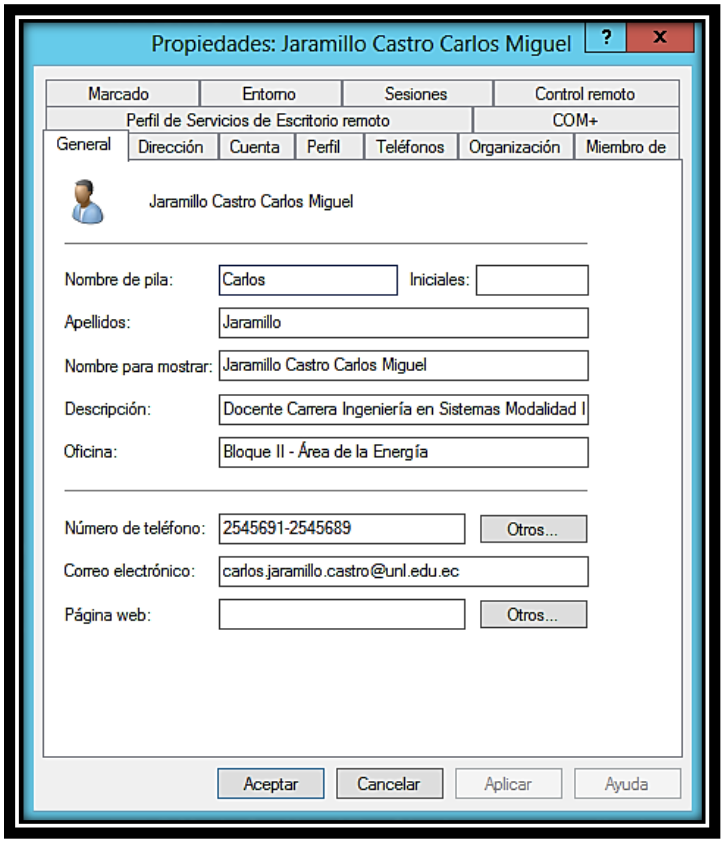


Figura 55. Propiedades del usuario

Fuente: Autor

En la pestaña Cuenta podemos visualizar el nombre de usuario para la misma, en Opciones de Cuenta se despliega una lista de diferentes opciones, en ellas se selecciona la primera, ya que esta es una política aplicada, así mismo en la parte final de la ventana se puede observar la fecha de cuando expira la cuenta del usuario, finalmente para restringir las horas de inicio de sesión se debe hacer clic en el botón Horas de inicio de sesión como se puede observar en la Figura 56.

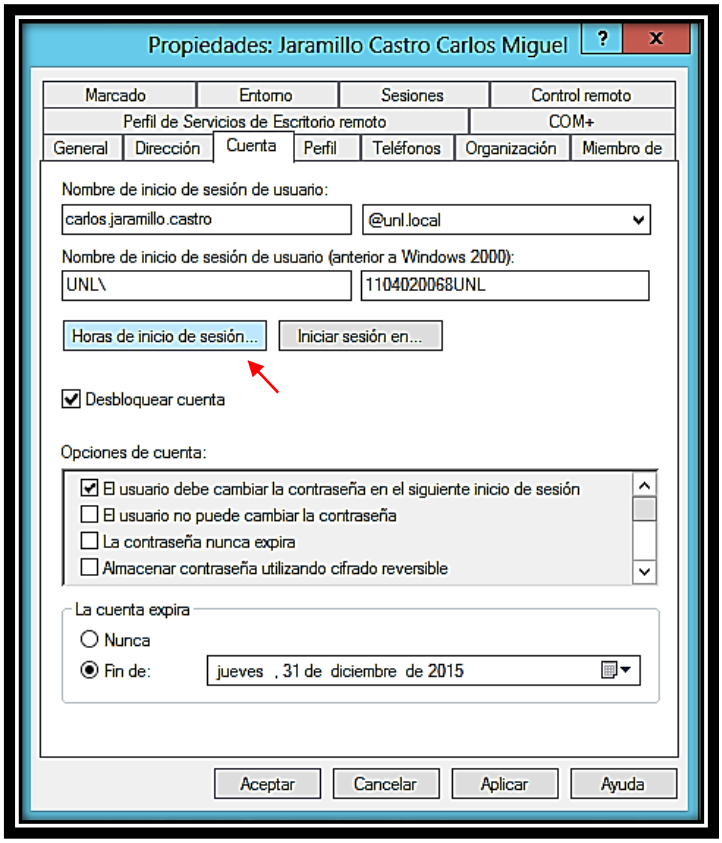


Figura 56. Cuenta del usuario

Fuente: Autor

En las Horas de inicio de sesión se muestra un panel como en el de la Figura 57, en él se aprecia los días de la semana y las horas de cada día, se debe seleccionar el horario que se pretende brindar o quitar el servicio, dependiendo de la política planteada, y mediante los ítems del costado derecho aplicamos lo dicho.

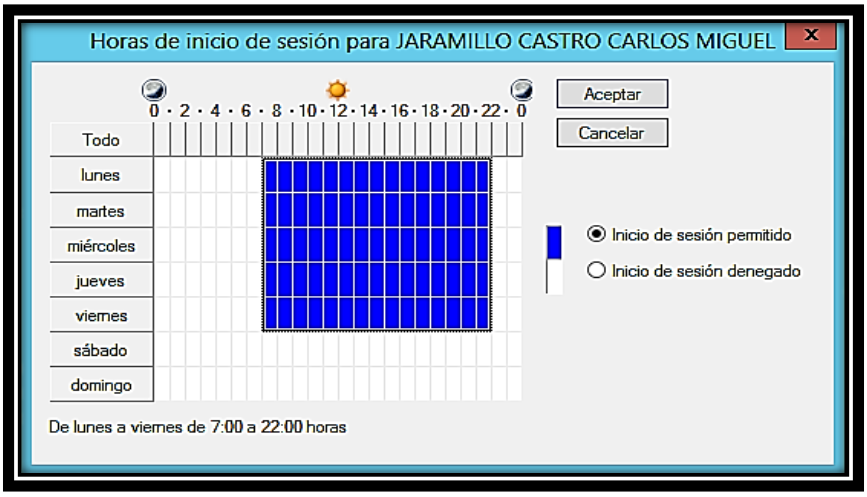


Figura 57. Horas de inicio de sesión

Fuente: Autor

6.4.2.6 Configuración de autenticación 802.1x

Para realizar la autenticación de usuarios mediante 802.1x, se debe ingresar a NAP, al obtener nuestro servidor, se hace clic derecho en el mismo y se abre el Servidor de directiva de roles, como se puede apreciar en la Figura 58.

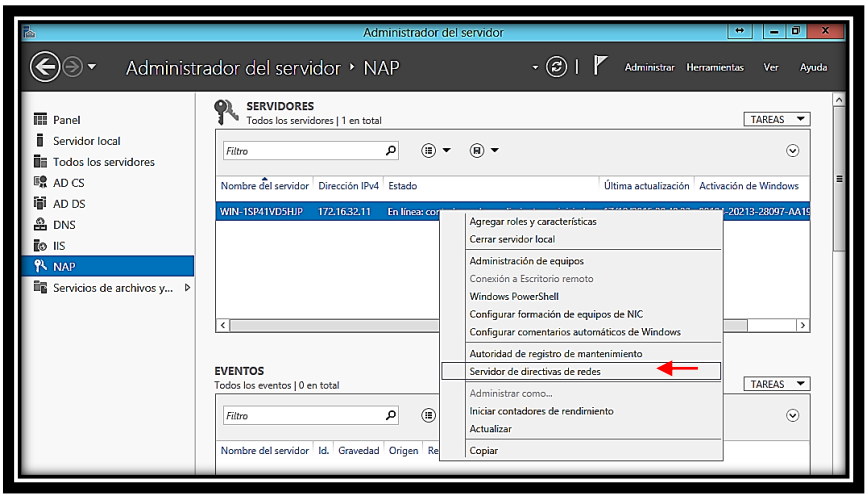


Figura 58. Administrador del servidor NAP

Fuente: Autor

Una vez dentro de NPS, se debe seleccionar el escenario de configuración, en este caso se selecciona Servidor RADIUS para conexiones cableadas o inalámbricas 802.1x, como se muestra en la Figura 59, una vez seleccionado el escenario se da clic en la opción Configurar 802.1x.

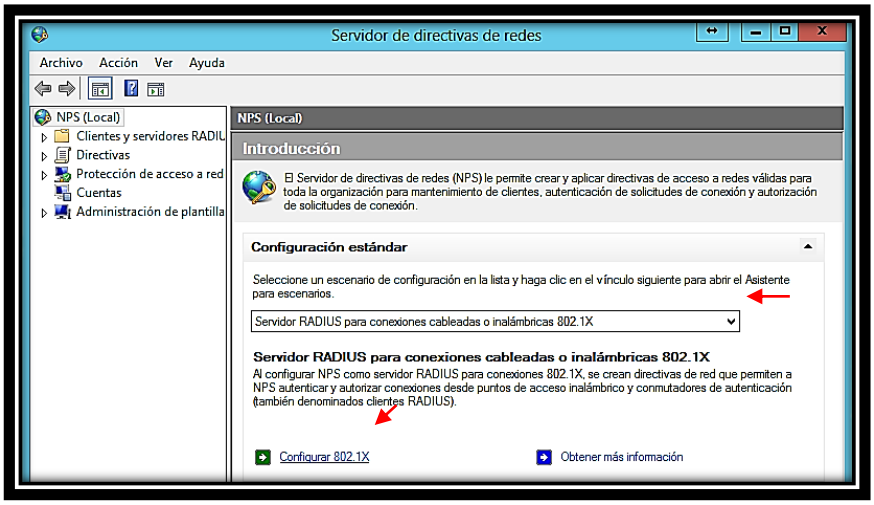


Figura 59. Configurar 802.1x

Fuente: Autor

Dentro de la configuración de 802.1x, se debe seleccionar el tipo de conexión, ya sea conexiones inalámbricas o conexiones cableadas (Ethernet), seleccionado el tipo de conexión, se aplica un nombre descriptivo y se da clic en Siguiente para continuar con la configuración, en la Figura 60 se ha seleccionado conexiones inalámbricas seguras, cabe destacar que es prácticamente el mismo proceso para conexiones cableadas, hay una pequeña diferencia para este tipo de conexión que será indicado con posterioridad.

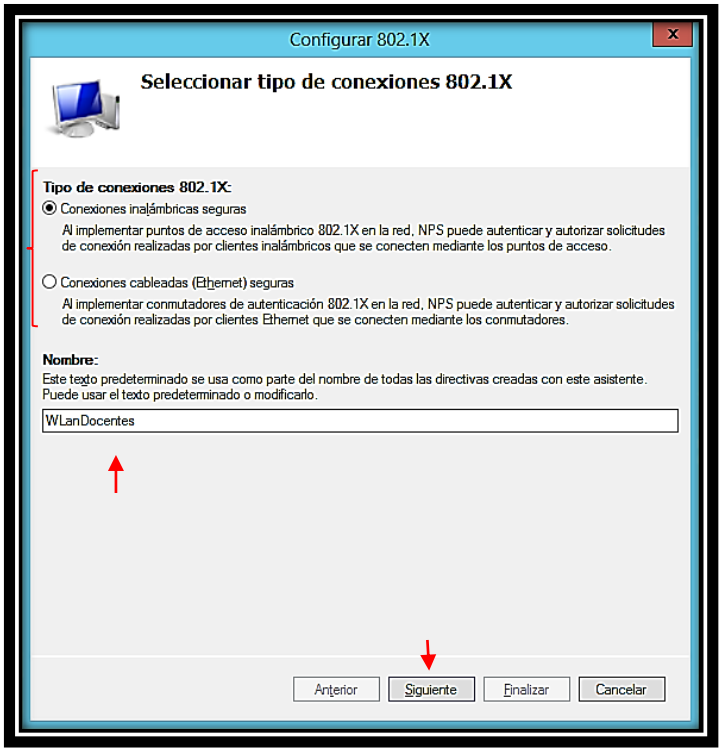


Figura 60. Seleccionar el tipo de conexiones 802.1x

Fuente: Autor

Habiendo seleccionado el tipo de conexión se debe agregar el cliente RADIUS, para ello simplemente se da clic en Agregar como se indica en la Figura 61.

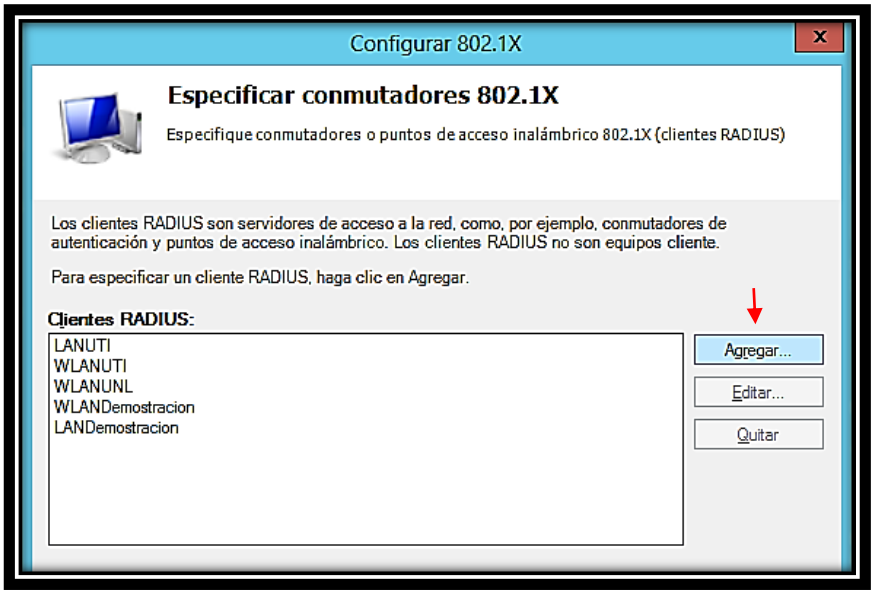


Figura 61. Especificar conmutadores 802.1x

Fuente: Autor

Al agregar un cliente RADIUS se despliega una ventana en la cual se debe ingresar un nombre descriptivo, la dirección IP del conmutador, es decir del medio de transmicion ya sea este un AP para conexiones inalámbricas o un Switch para conexiones cableadas, finalmente se debe agregar un secreto compartido, en la Figura 62 se indica estos datos, se debe tener en cuenta que el secreto compartido será configurado en los medios de transmisión.

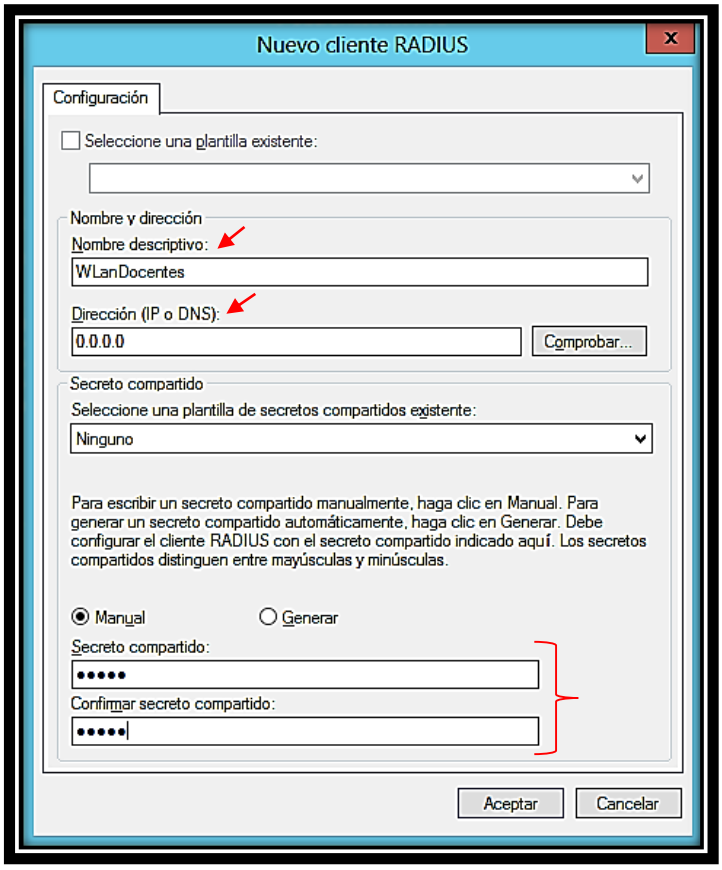


Figura 62. Propiedades del cliente RADIUS

Fuente: Autor

Se debe también configurar el método de autenticación, para ello se seleccionar el método de contraseña segura (EAP-MASCHP v2), como se muestra en la Figura 63, seleccionado el método de autenticación se da clic en siguiente.

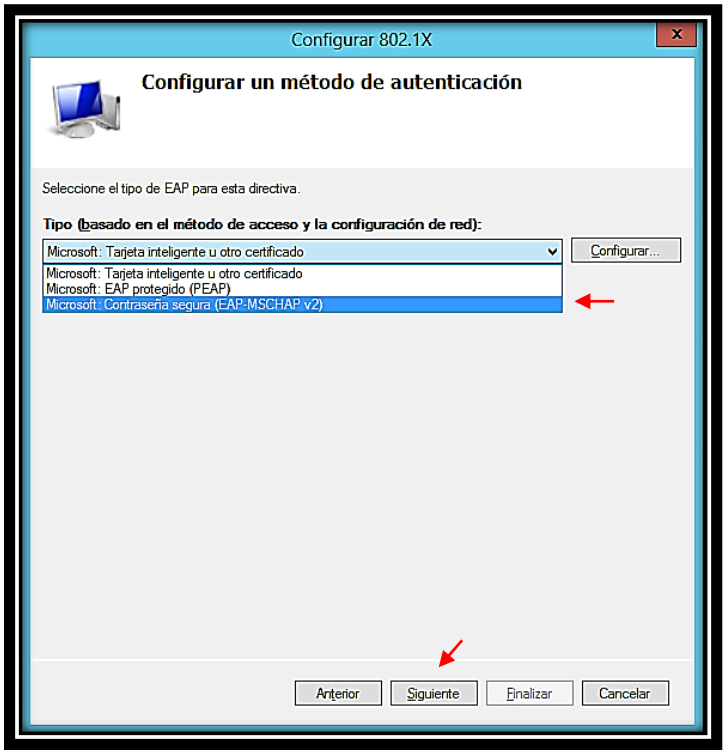


Figura 63. Configurar un método de autenticación

Fuente: Autor

Una vez configurado el método de autenticación, se debe agregar el o los grupos de usuarios que van a ser pertenecientes a este cliente RADIUS, para ello se pulsa el botón Agregar, como indica la Figura 64.

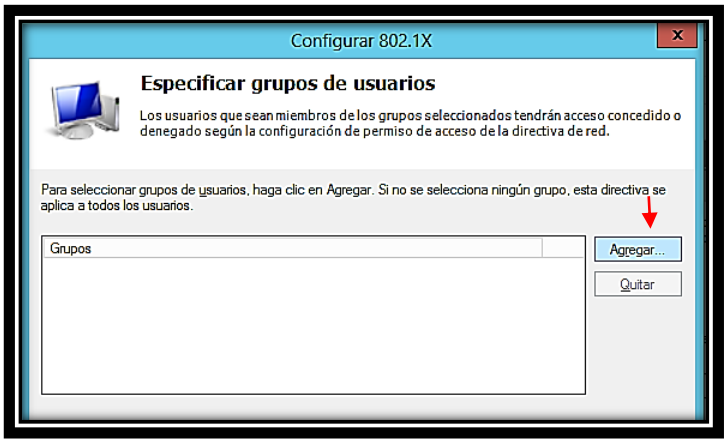


Figura 64. Especificar grupos de usuarios

Fuente: Autor

Se debe seleccionar el grupo de usuarios, para ello se debe escribir el nombre del mismo, si se desea se lo puede buscar mediante la ubicación en las UO, y luego se presiona aceptar, en la Figura 65 se puede apreciar esto.

Figura 65. Seleccionar grupo

Fuente: Autor

Teniendo el grupo de usuarios para la autenticación, únicamente se debe finalizar la configuración, en la Figura 66 se puede apreciar la información básica de este servidor RADIUS, se da clic en finalizar para terminar con la configuración.

Figura 66. Finalización de los clientes RADIUS

Fuente: Autor

Ahora se debe agregar los tipos de EAP, ya que muchos dispositivos cuentan con métodos de autenticación diferentes al establecido, para ello en la parte izquierda, dentro de Directivas encontramos Directivas de red, allí se halla el cliente RADIUS configurado, se da doble clic en el mismo y se despliega una ventana con las propiedades de este cliente, en ella ingresamos a la opción de Métodos de autenticación , una vez allí en la parte de Tipos de EAP, se presiona el botón Agregar, es allí donde agregamos todos las opciones que se nos da, finalmente se presiona el botón aceptar para concluir con la configuración. Esto se puede apreciar en la Figura 67.

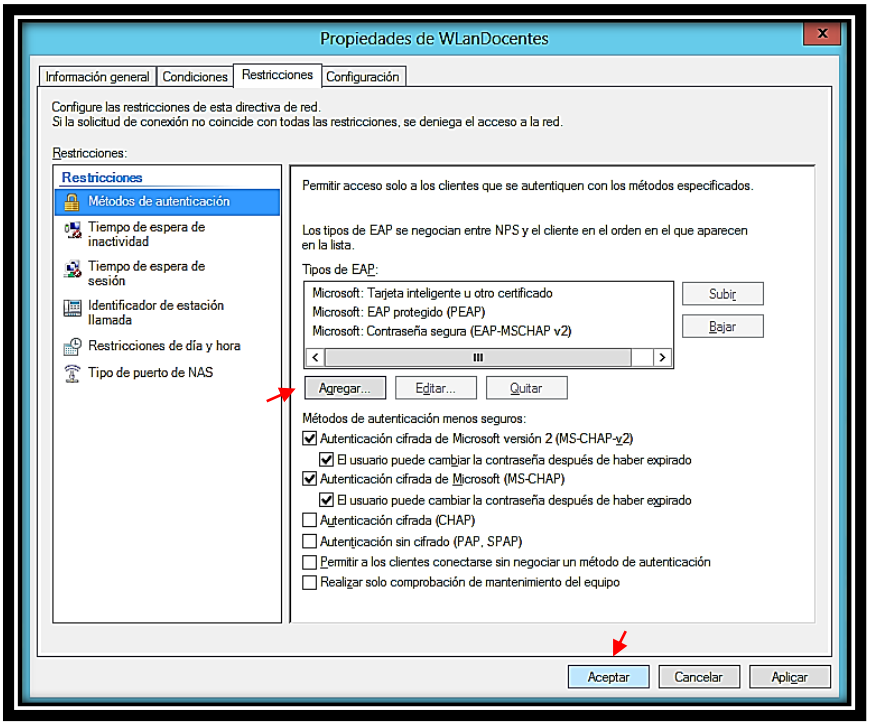


Figura 67. Propiedades del cliente RADIUS

Fuente: Autor

En un apartado anterior se menciono que hay una pequeña diferencia para conexiones cableadas, y este se especifica en la Figura 68, en ella se puede apreciar que se agrega el Tipo de puerto de NAS, dentro de esta opcion, debemos agregar Ethernet en los Tipos de tunel de conexión 802.1x, finalmente se da clic en Aceptar y se termina con la configuración.

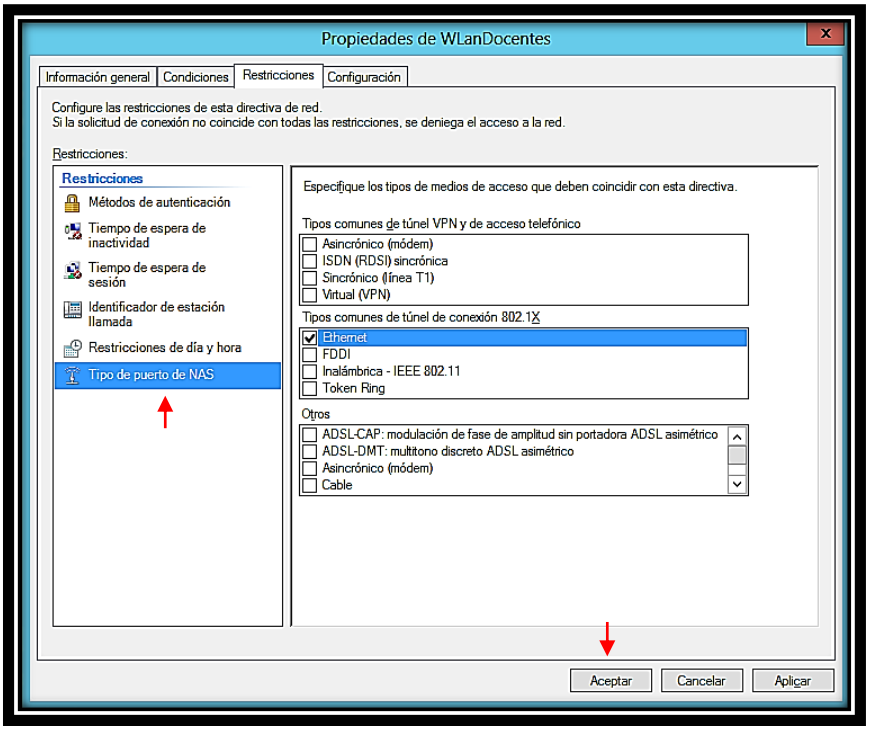


Figura 68. Tipo de Puerto de NAS

Fuente: Autor

6.4.2.7 Configuración de equipos de red

Configuración del Switch CATALYST 2960-X

Para configurar la autenticación basada en puertos 802.1x, debe activar la autenticación, autorización y contabilidad (AAA) y especificar la lista de métodos de autenticación.

Este es el proceso AAA 802.1x:

TABLA XVII. CONFIGURACIÓN DE SWITCH

	Comando	Propósito
Paso 1	configure terminal	Entrar en el modo de configuración global.
Paso 2	aaa nuevo modelo	Habilitar AAA.
Paso 3	dot1x autenticación aaa {default} metodo1	Crear una lista de métodos de autenticación 802.1x. Para crear una lista predeterminada a usar cuando una lista con nombre no se ha especificado en el comando de autenticación, se utiliza la palabra clave default seguida por el método

		a utilizar en situaciones predeterminadas. La lista método por defecto se aplica automáticamente a todos los puertos. Para el metodo1, se debe introducir las palabras clave group radius para utilizar la lista de todos los servidores RADIUS para la autenticación. **Nota:** Aunque otras palabras clave son visibles en la ayuda en cadena de la línea de comandos, sólo se admiten las palabras clave group radius.
Paso 4	dot1x system-auth-control	Habilitar la autenticación 802.1x a nivel global en el interruptor.
Paso 5	radius-server host ip-address	Especificar la dirección IP del servidor RADIUS.
Paso 6	radius-server key string	Especificar la clave de autenticación y encriptación utilizado entre el interruptor y el servidor RADIUS.
Paso 7	interface interface-id	Especifiar el puerto conectado al cliente para habilitar la autenticación 802.1x, y entrar en el modo de configuración de interfaz.
Paso 8	switchport mode access	Configurar el puerto a acces mode, sólo si ha configurado el servidor RADIUS en el Paso 6 y el Paso 7.
Paso 9	authentication port-control auto o dot1x port-control auto	Habilitar la autenticación 802.1x en el puerto.
Paso 10	end	Fin Volver al modo EXEC privilegiado.
Paso 11	show authentication or show dot1x	Verificar las entradas.
Paso 12	copy running-config startup-config	(Opcional) Guardar las entradas en el archivo de configuración.

Configuración del router Inalámbrico CISCO LINKSYS

Para configurar este router inalámbrico con el nuevo tipo de autenticación basado en el estándar 802.1x se necesita seguir los siguientes pasos.

La configuración del este equipo se la realiza vía administración web.

TABLA XVIII. CONFIGURACIÓN DEL ROUTER

	Comando	Propósito
Paso 1	Ingresar User y pass	Ingresar al router como administrador.
Paso 2	Seleccionar Configuración Inalámbrica	Observar los parámetros actuales de configuración y
Paso 3	Seleccionar el tipo de red de 2.4 GHz o 5 GHz	Determinar a qué red se le desea aplicar la configuración.
Paso 4	Seleccionar editar	Permite cambiar la configuración actual de la red.
Paso 5	Colocar nombre de red (SSID)	Nombre con que los clientes podrán identificar la red.
Paso 6	Colocar Ip del radius server	Ingresar la dirección IPv4 que se encuentra asignada al servidor radius
Paso 7	Colocar Puerto Radius	Se ingresa el puerto del servidor radius 1812
Paso 8	Colocar clave compartida	Se ingresa la clave compartida entre el servidor y el autenticador (router). **Nota:** Esta clave se encuentra ingresada previamente en el servidor radius.
Paso 9	Modo de seguridad	Se habilita el modo WPA2 enterprise ya que este modo soporta la autenticación de 802.1x RADIUS.

En la Figura 69 muestra un ejemplo demostrativo de la configuración del router inalámbrico linksys.

Figura 69. Configuración autenticación 802.1x Router Cisco Linksys

Fuente: Autor

6.4.2.8 Configuración de directivas para la administración de equipos

Para realizar la configuración de las directivas o políticas para la adminitracion de equipos se debe seguir los siguientes pasos, los mismos se indican de manera grafica en las Figuras 70,71,72,73 y 74:

1. Para crear una nueva directiva de grupo (GPO) realizamos clic derecho sobre el vínculo Objetos de directiva de grupo.
2. Luego clic en el vínculo Nueva.

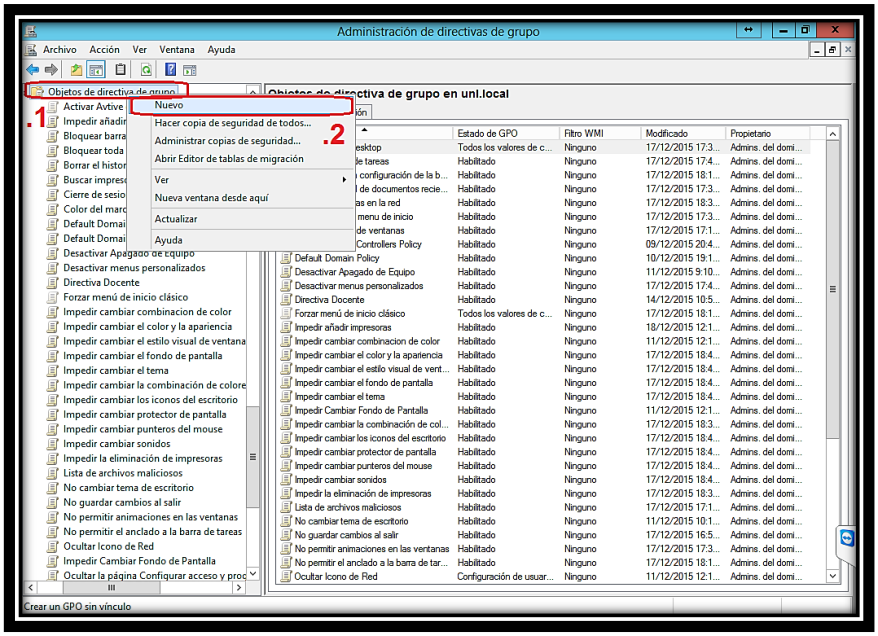


Figura 70. Nueva directiva de grupo

Fuente: Autor

3. Colocar un nombre descriptivo de la directiva.

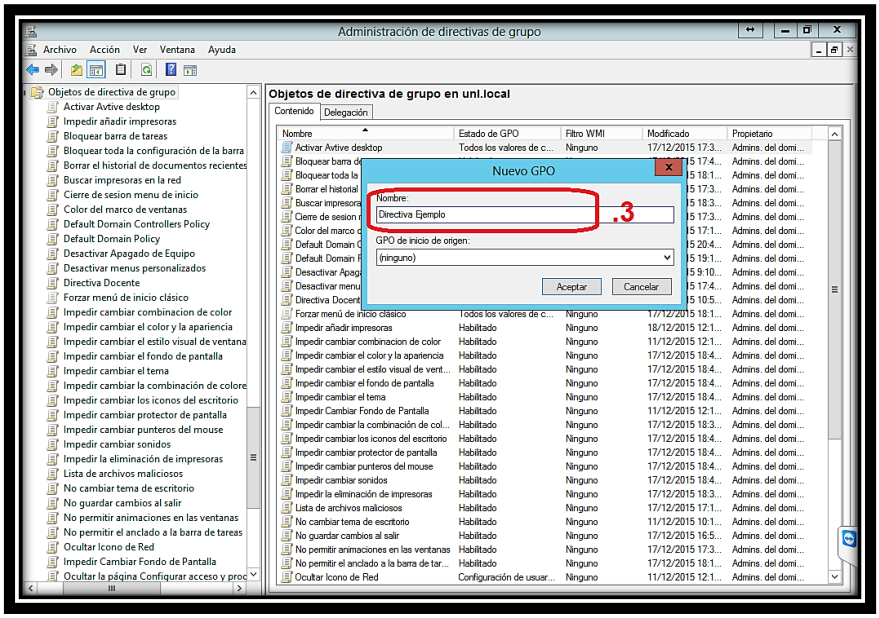


Figura 71. Nuevo GPO

Fuente: Autor

4. Buscamos la directiva, creada en este caso con el nombre “Directiva Ejemplo”, seguido clic derecho y editamos su configuración.

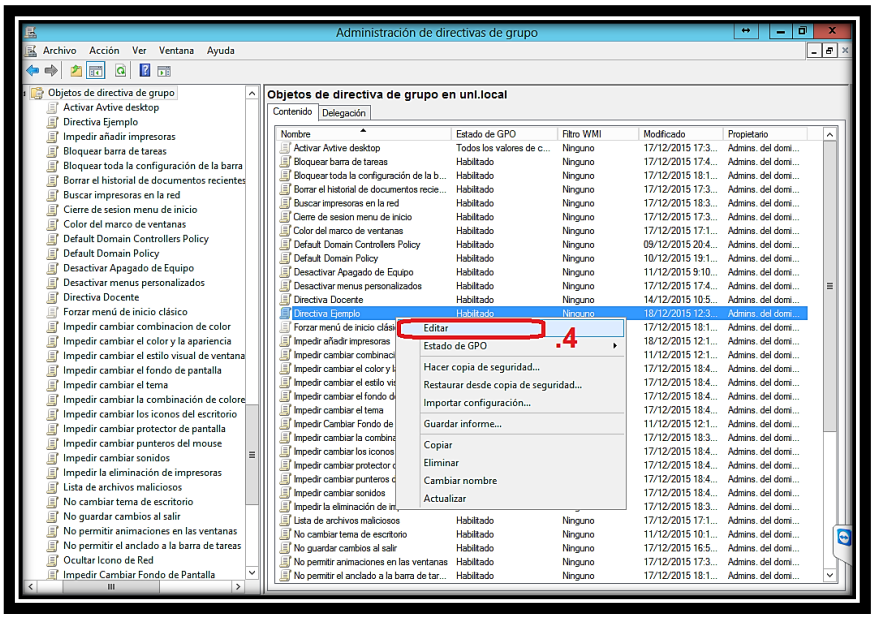


Figura 72. Editar GPO

Fuente: Autor

4.1 Buscamos en el menú desplegable de la izquierda “Configuración de Usuario” – “Directivas” – “Plantillas Administrativas” en la ventana Editor de Administración de directivas de grupo, seleccionamos en este caso la directiva “Quitar del

escritorio el icono de la papelería de reciclaje", realizamos click derecho en la directiva y posterior click en la opción de Editar.

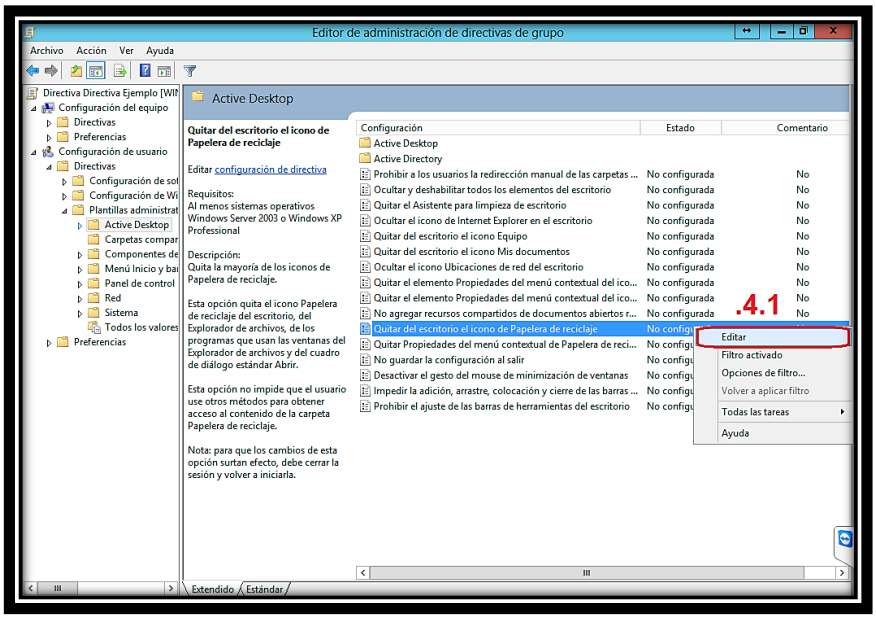


Figura 73. Editar directiva

Fuente: Autor

5 En la ventana de opciones de la directiva, seleccionamos la opción de habilitada, esto permite activar la configuración en los clientes o usuarios.

6 Seleccionamos Aplicar.

7 Seleccionamos Aceptar para que se guarde las configuraciones realizadas.

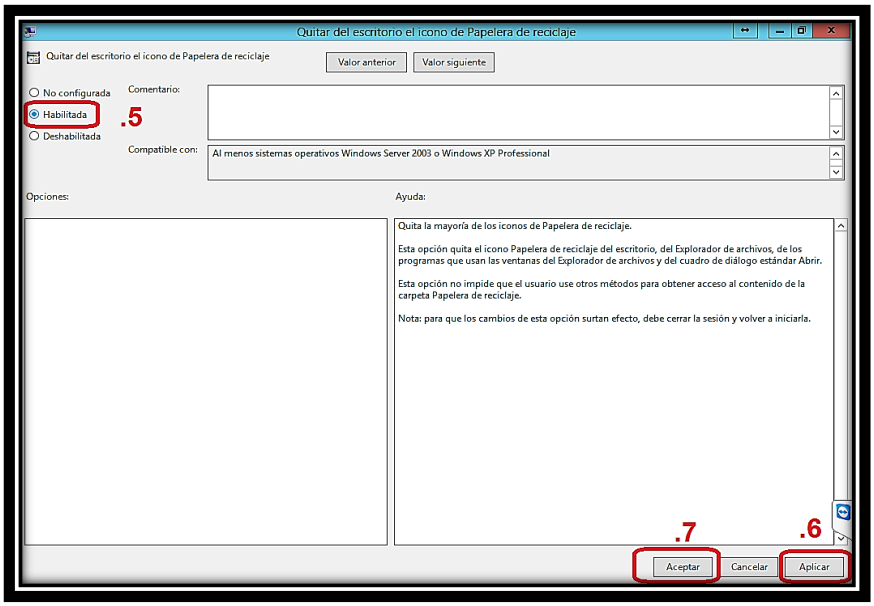


Figura 74. Habilitar directiva

Fuente: Autor

6.4.3 Pruebas de funcionalidad a nivel de servidor como controlador de dominio

Para realizar las pruebas de funcionalidad del servidor como controlador de dominio existen diversas herramientas propias de Active Directory, una de ellas llamada Utilidad de Diagnóstico de Directorio Activo “DCDIAG”, esta herramienta realiza diversas pruebas al servidor brindando información rápida y necesaria para conocer el estado del directorio activo, y si hay problemas, indicarnos en donde los hay, para hacer uso de esta herramienta lo único que se debe hacer, es escribir la palabra “*dcdiag*” en el símbolo del sistema del servidor, cabe recalcar que para ello se debe estar con privilegios de “Administrador”.

A continuación se indica las pruebas que realiza DCDIAG al servidor.

6.4.3.1 Diagnóstico del servidor de directorio

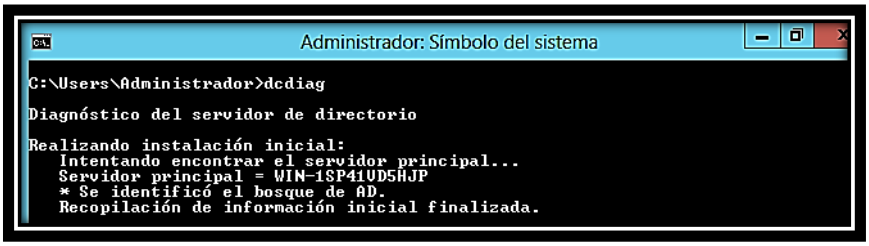


Figura 75. Diagnóstico del servidor de directorio

Fuente: Autor

Como se muestra en la Figura 75. El primer análisis realizado es para encontrar el servidor principal, en este caso dicho servidor se denomina “WIN-1SP41VD5HJP”, el nombre del servidor principal fue dado por el ex director de la Dirección de Telecomunicaciones, Ing. Milton Palacios.

6.4.3.2 Pruebas requeridas iniciales

Figura 76. Pruebas requeridas iniciales

Fuente: Autor

La principal prueba requerida inicial que se lleva a cabo en el servidor es la prueba de Connectivy, como se muestra en la Figura 76, esta prueba testea los DC que están registrados en DNS, así como si se accede a ellos por LDAP y RDP.

6.4.3.3 Pruebas principales

```
Realizando pruebas principales

   Probando servidor: Default-First-Site-Name\WIN-1SP41VD5HJP
      Iniciando prueba: Advertising
         ......................... WIN-1SP41VD5HJP superó la prueba Advertising
      Iniciando prueba: FrsEvent
         ......................... WIN-1SP41VD5HJP superó la prueba FrsEvent
      Iniciando prueba: DFSREvent
         ......................... WIN-1SP41VD5HJP superó la prueba DFSREvent
      Iniciando prueba: SysVolCheck
         ......................... WIN-1SP41VD5HJP superó la prueba SysVolCheck
      Iniciando prueba: KccEvent
         ......................... WIN-1SP41VD5HJP superó la prueba KccEvent
      Iniciando prueba: KnowsOfRoleHolders
         ......................... WIN-1SP41VD5HJP superó la prueba
         KnowsOfRoleHolders
      Iniciando prueba: MachineAccount
         ......................... WIN-1SP41VD5HJP superó la prueba
         MachineAccount
      Iniciando prueba: NCSecDesc
         ......................... WIN-1SP41VD5HJP superó la prueba NCSecDesc
      Iniciando prueba: NetLogons
         ......................... WIN-1SP41VD5HJP superó la prueba NetLogons
      Iniciando prueba: ObjectsReplicated
         ......................... WIN-1SP41VD5HJP superó la prueba
         ObjectsReplicated
      Iniciando prueba: Replications
         ......................... WIN-1SP41VD5HJP superó la prueba
         Replications
      Iniciando prueba: RidManager
         ......................... WIN-1SP41VD5HJP superó la prueba RidManager
```

Figura 77. Pruebas principales

Fuente: Autor

En la Figura 77, se muestran diferentes pruebas que se realizan en el servidor, las mismas se describen a continuación.

Advertising.- Comprueba si cada uno de los “Directory System Agent” (DSA) se informa a sí mismo de su estado. [16]

FrsEvent.- Comprueba si hay errores en el sistema de replicación de archivos. (Si se falla la replicación del recurso compartido SYSVOL puede causar problemas de directiva.) [17]

DFSREvent.- Detecta un error durante la comunicación con un asociado de replicación durante la replicación. [18]

SysVolCkeck.- Consiste en comprobar el Visor de sucesos para asegurarse de que el servicio de replicación de archivos se inicia correctamente. [17]

KccEvent.- Esta prueba comprueba que el Knowledge Consistency Checker (KCC) está funcionando y si está produciendo errores, algo así como un comprobador de coherencia. [16]

NCSecDesc.- Contexto de nomenclatura de Seguridad Prueba Descriptores (NcSecDesc). [19]

NetLogons.- Se usa este procedimiento para asegurarse de que el servicio de replicación de sistema de archivos distribuidos (DFS) se inicia correctamente y luego asegurarse de que la carpeta sysvol compartida y de sesión se crea y se comparten. [17]

Replications.- La topología de replicación minimiza el uso de enlaces potencialmente lentos o costosos de ancho de red de área extensa (WAN) entre sitios. [20]

RidManager.- El pariente Identificación gerente (RID) es responsable de proporcionar los números que se utilizan para crear identificadores de seguridad únicos (SID) para cada cuenta en un dominio. [21]

6.4.3.4 Pruebas de partición

```
Ejecutando pruebas de partición en: ForestDnsZones
   Iniciando prueba: CheckSDRefDom
      ......................... ForestDnsZones superó la prueba
      CheckSDRefDom
   Iniciando prueba: CrossRefValidation
      ......................... ForestDnsZones superó la prueba
      CrossRefValidation

Ejecutando pruebas de partición en: DomainDnsZones
   Iniciando prueba: CheckSDRefDom
      ......................... DomainDnsZones superó la prueba
      CheckSDRefDom
   Iniciando prueba: CrossRefValidation
      ......................... DomainDnsZones superó la prueba
      CrossRefValidation

Ejecutando pruebas de partición en: Schema
   Iniciando prueba: CheckSDRefDom
      ......................... Schema superó la prueba CheckSDRefDom
   Iniciando prueba: CrossRefValidation
      ......................... Schema superó la prueba CrossRefValidation

Ejecutando pruebas de partición en: Configuration
   Iniciando prueba: CheckSDRefDom
      ......................... Configuration superó la prueba CheckSDRefDom
   Iniciando prueba: CrossRefValidation
      ......................... Configuration superó la prueba
      CrossRefValidation

Ejecutando pruebas de partición en: unl
   Iniciando prueba: CheckSDRefDom
      ......................... unl superó la prueba CheckSDRefDom
   Iniciando prueba: CrossRefValidation
      ......................... unl superó la prueba CrossRefValidation
```

Figura 78. Pruebas de partición

Fuente: Autor

En la Figura 78 se muestran diversas pruebas de partición las mismas se detallan a continuación.

ChecksDRefDom.- Comprueba que todas las particiones de directorio de aplicaciones tienen descriptor de seguridad adecuado hacer referencia a dominios. [17]

CrossRefValidation.- Comprueba la validez de las referencias cruzadas. [17]

6.4.3.5 Pruebas de empresa

```
Ejecutando pruebas de empresa en: unl.edu.ec
   Iniciando prueba: LocatorCheck
      ......................... unl.edu.ec superó la prueba LocatorCheck
   Iniciando prueba: Intersite
      ......................... unl.edu.ec superó la prueba Intersite

C:\Users\Administrador>_
```

Figura 79. Pruebas de empresa

Fuente: Autor

En la Figura 79 se muestran las pruebas de empresa, estas se detallan a continuación:

LocatorCheck.- Hace una comprobación para asegurarse que los DC con funciones FSMO son conocidos y, sobre todo, accesibles. [16]

Intersite.- Realiza una serie de test para ver si hay algún problema con los DC BridgeHead. [16]

6.4.4 Pruebas de funcionalidad a nivel de estaciones de trabajo dentro del Área de la Energía y los Recursos Naturales no Renovables de la Universidad Nacional de Loja

6.4.4.1 Plan de pruebas funcionales para la conexión a la red

En este apartado se pretende probar el funcionamiento de las estaciones de trabajo como clientes del servidor RADIUS, y a su vez objetos del servidor controlador de dominio en cuatro escenarios diferentes.

Cada escenario es representado por un sistema operativo diferente, y se listan a continuación.

- Sistema Operativo Nativo Windows 8.1.
- Ubuntu 14.10 LTS Sistema Operativo bajo licencia Libre.
- Android 5.1.1 Sistema Operativo para dispositivos móviles.
- IOS 8.4 Sistema Operativo para dispositivos móviles.

Para ello se ha elegido cuatro casos de uso, uno por cada acción específica que realiza el cliente en el proceso de autenticación, ya sea solicitada en la red inalámbrica o

cableada. La manera de probar la funcionalidad de los clientes u objetos es realizando los siguientes casos de usos.

- Tarjeta de red configurada correctamente.
- Solicitar al cliente el ingreso de su usuario y contraseña.
- Solicitar al cliente el cambio de contraseña inicial con la complejidad establecida.
- Autenticación del cliente exitosa.

Si se desea conocer cómo se configura la tarjeta de red ya sea de área local o inalámbrica puede consultarse el ANEXO 1.

Estás pruebas se realizaron para escenario o sistema operativo presente en el cliente o estación de trabajo, buscando cubrir todos los casos posibles y buscando evaluar todos los aspectos del funcionamiento de cada elemento.

Las pruebas fueron realizadas en diversos lugares del campos de la Universidad Nacional de Loja, principalmente se realizaron en los laboratorios de la carrera de Ingeniería en Sistemas tomando como clientes a los alumnos de los décimos módulos de la carrera, así mismo se realizó en la Dirección de Telecomunicaciones e Información.

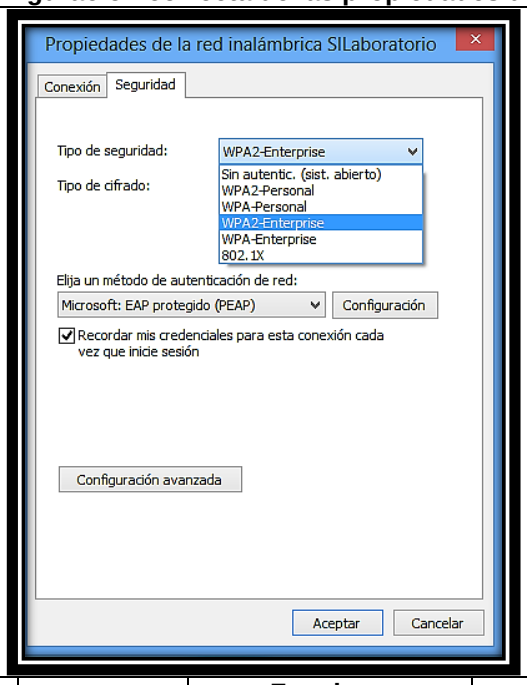
Cabe indicar que al realizar las pruebas de funcionalidad a nivel de estaciones de trabajo, se pudo conocer que el cambio de contraseña obligatorio, se lo puede realizar únicamente desde un computador, AD no permite realizar este cambio de contraseña desde un dispositivo móvil.

Los resultados y detalles de las pruebas de funcionalidad, están descritas en las siguientes tablas.

Escenario 1: Sistema operativo nativo Windows 8.1

TABLA XIX. CONFIGURACIÓN CORRECTA DE LA TARJETA DE RED INALÁMBRICA

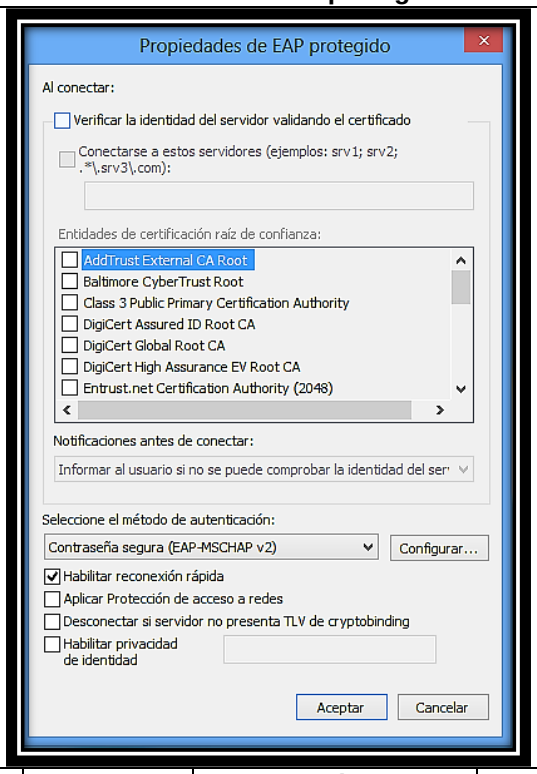
Verificación y configuración correcta de las propiedades de la tarjeta de red



Acciones	Escenario	Funciono correctamente		Comentarios
		SI	NO	
¿Norma de Seguridad WPA2-Enterprise establecida?	1	*		Este modo soporta la autentificación de 802.1x RADIUS.
¿Método de autenticación de red EAP establecido?	1	*		Método de autenticación para clientes que tratan de conectarse a la red a través de los siguientes tipos de servidores de acceso a la red: Puntos de acceso inalámbrico 802.1x y Conmutadores de autenticación 802.1x.
¿Recordar las credenciales cada vez que inicie sesión?	1	*		Permite recordar la credencial del cliente, para que en futuras conexiones no solicite la información de autenticación nuevamente.

TABLA XX. CONFIGURACIÓN CORRECTA DEL PROTOCOLO DE AUTENTICACIÓN EAP PROTEGIDO (PEAP)

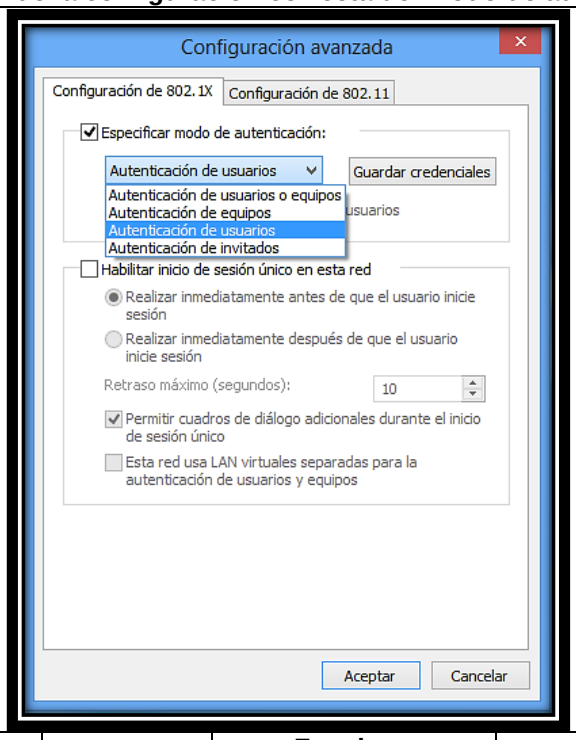
Verificación y configuración correcta de las propiedades del protocolo de autenticación EAP protegido



Acciones	Escenario	Funciono correctamente		Comentarios
		SI	NO	
¿Al conectar verificar la identidad del servidor verificando el certificado?	1	*		Verifica la entidad de certificación en este caso no se verifica ya que el certificado se emite.

TABLA XXI. CONFIGURACIÓN CORRECTA DEL PROTOCOLO DE AUTENTICACIÓN EAP PROTEGIDO (PEAP)

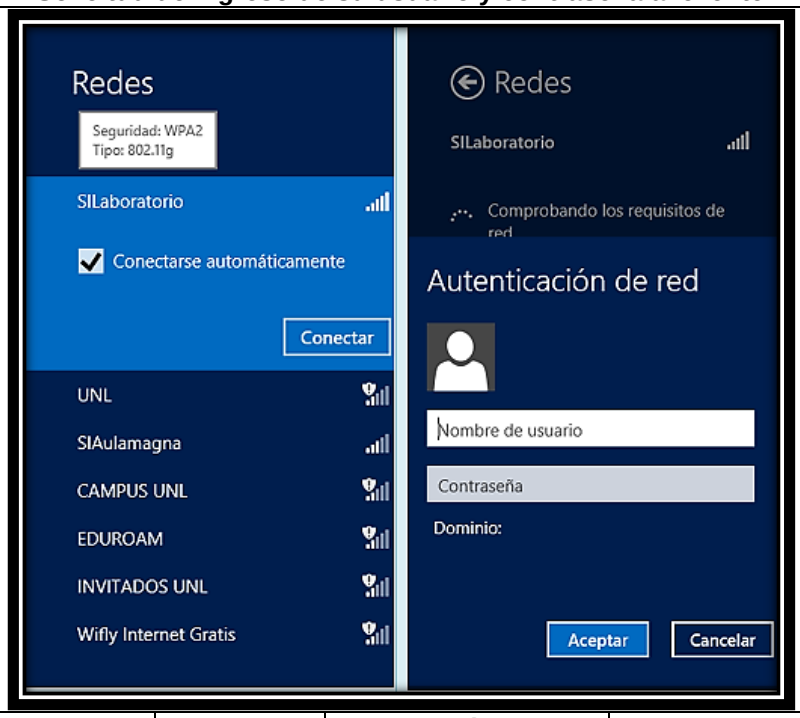
Verificación de la configuración correcta del modo de autenticación



Acciones	Escenario	Funciono correctamente		Comentarios
		SI	NO	
¿El modo de autenticación establecido permite que dicho proceso se realice con éxito?	1	*		El modo de autenticación estable el tipo objeto creado en el servidor controlador de dominio, en este caso es una autenticación de usuarios.

TABLA XXII. SOLICITUD DE DATOS PERSONALES EN LA RED PARA LA POSTERIOR AUTENTICACIÓN

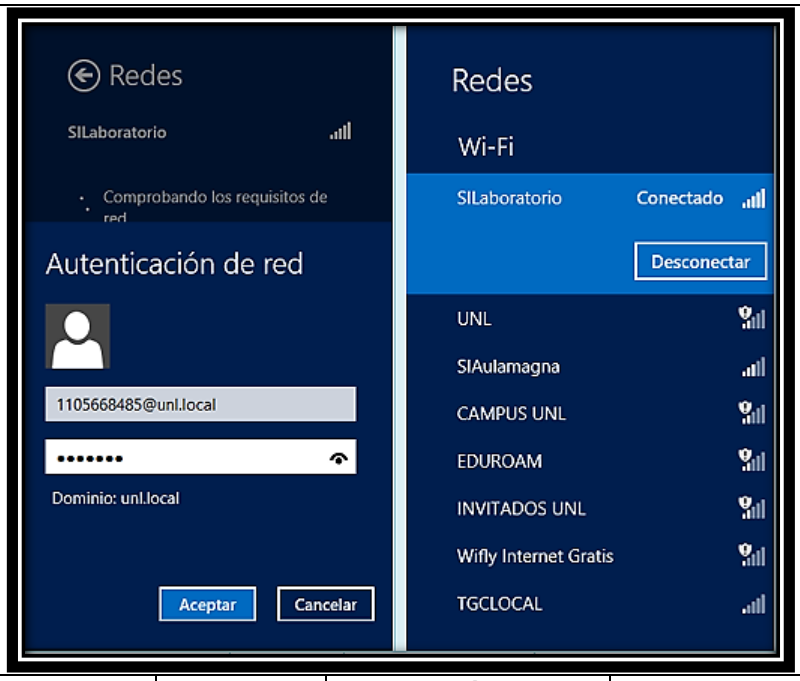
Solicitud de ingreso de su usuario y contraseña al cliente



Acciones	Escenario	Funciono correctamente		Comentarios
		SI	NO	
¿La solicitud de ingreso de datos (usuario y contraseña) dentro del dominio se mostró correctamente?	1	*		Al seleccionar la red se observa el tipo de seguridad establecida y a su vez requerido para la autenticación exitosa, en consecuencia se muestra a continuación que se pide al cliente el ingreso de datos exitosamente.
¿La solicitud de ingreso de datos (usuario y contraseña) dentro del dominio se mostró correctamente?	1		*	Si la solicitud de ingreso de datos no se muestra revisar el ANEXO 1.

TABLA XXIII. VERIFICACIÓN DE LA AUTENTICACIÓN DEL CLIENTE EXITOSA

Verificación de la autenticación del cliente exitosa

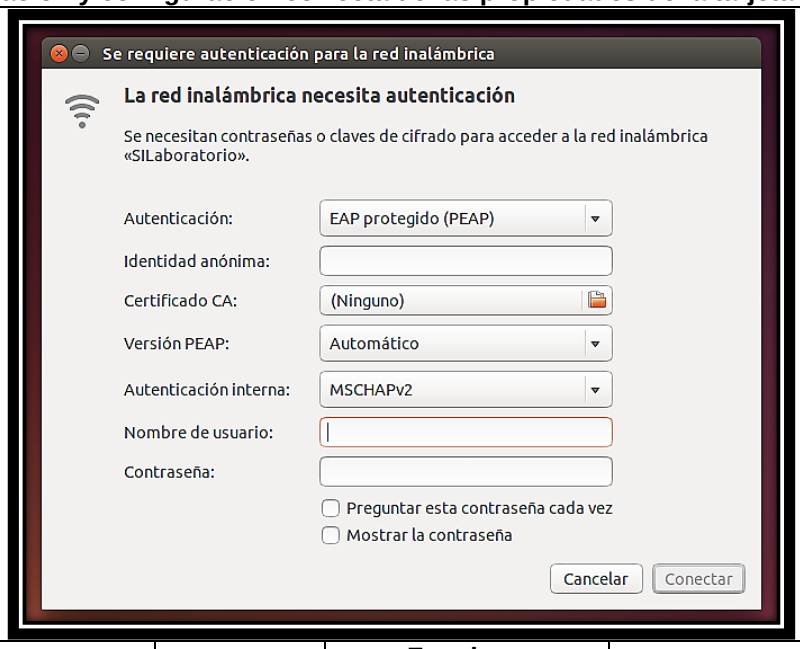


Acciones	Escenario	Funciono correctamente		Comentarios
		SI	NO	
¿La autenticación y posterior conexión a la red se realizó con éxito?	1	*		Al ingresar los datos de usuario y contraseña, verificando que el dominio y sus datos personales sean los correctos, la autenticación y conexión a la red se dio con éxito.
¿La autenticación y posterior conexión a la red se realizó con éxito?	1		*	Si la autenticación falla verificar: a) Que los datos personales ingresados sean los correctos. b) Revisar que el usuario exista dentro del dominio.

Escenario 2: Ubuntu 14.10 LTS sistema operativo bajo licencia Libre

TABLA XXIV. CONFIGURACIÓN CORRECTA DE LA TARJETA DE RED INALÁMBRICA

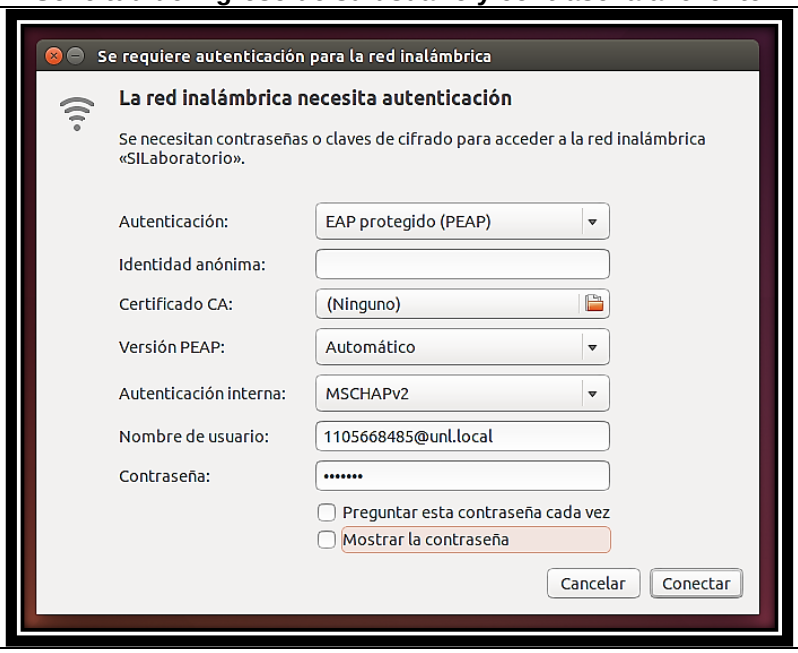
Verificación y configuración correcta de las propiedades de la tarjeta de red



Acciones	Escenario	Funciono correctamente		Comentarios
		SI	NO	
¿Método de autenticación de red EAP protegido (PEAP) establecido?	2	*		Método de autenticación para clientes que tratan de conectarse a la red a través de los siguientes tipos de servidores de acceso a la red: Puntos de acceso inalámbrico 802.1x y Conmutadores de autenticación 802.1x.
¿Autenticación interna establecida con el protocolo MSCHAP v2?	2	*		En la autenticación interna se establece con el Protocolo de autenticación por desafío mutuo de Microsoft versión 2.

TABLA XXV. SOLICITUD DE DATOS PERSONALES EN LA RED PARA LA POSTERIOR AUTENTICACIÓN

Solicitud de ingreso de su usuario y contraseña al cliente



Acciones	Escenario	Funciono correctamente		Comentarios
		SI	NO	
¿La solicitud de ingreso de datos (usuario y contraseña) dentro del dominio se mostró correctamente?	1	*		Al seleccionar la red se observa el tipo de seguridad establecida y a su vez requerido para la autenticación exitosa, en consecuencia se muestra a continuación que se pide al cliente el ingreso de datos exitosamente.
¿La solicitud de ingreso de datos (usuario y contraseña) dentro del dominio se mostró correctamente?	1		*	Si la solicitud de ingreso de datos no se muestra revisar el ANEXO 1.

Escenario 3: Android 5.1.1 sistema operativo para dispositivos móviles

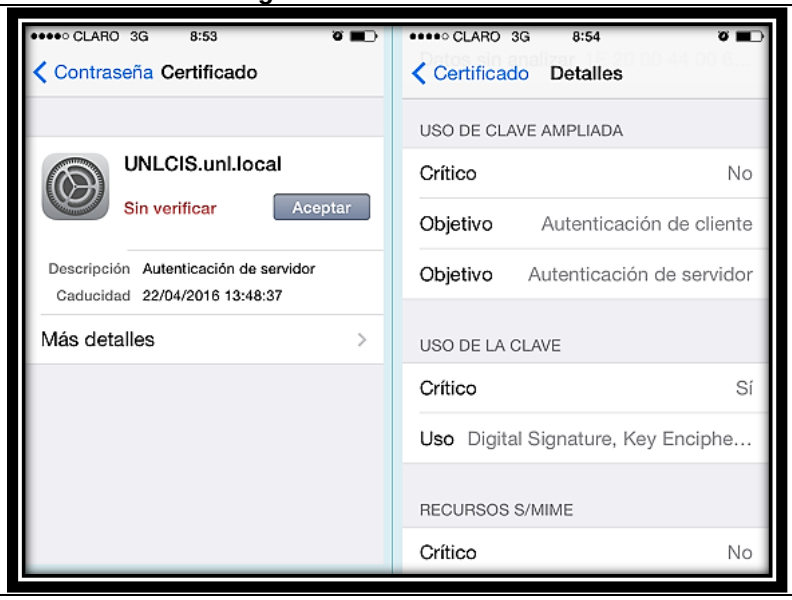
TABLA XXVI. ESCENARIO ANDROID 5.1.1 DISPOSITIVOS MOVILES

Verificación de la configuración correcta del modo de autenticación

Observaciones:
El método de autenticación EAP protegido (PEAP) se encuentra establecido por defecto ya que este sistema operativo actualiza por defecto la configuración de red, según los requerimientos de la red a la que se desea acceder. Se observa en la figura en el punto 1. Método EAP se encuentra establecido por defecto PEAP necesario para autenticación exitosa y en el punto 2. La autenticación de la fase 2 con el Protocolo de autenticación por desafío mutuo de Microsoft versión 2.

Escenario 4: IOS 8.4 sistema operativo para dispositivos móviles

TABLA XXVII. IOS 8.4 DISPOSITIVOS MOVILES

Verificación de la configuración correcta del modo de autenticación

Observaciones:
El método de autenticación EAP protegido (PEAP) se encuentra establecido por defecto ya que este sistema operativo actualiza por defecto la configuración de red, según los requerimientos de la red a la que se desea acceder. Se observa en la figura que pide al usuario o cliente únicamente aceptar el certificado emitido por el dominio UNLCIS.unl.local, en los detalles del certificado se observa que existe adecuadamente los objetivos necesarios para la autenticación de cliente y autenticación de servidor.

6.4.4.2 Pruebas de las directivas aplicadas

Para realizar las pruebas necesarias, respecto a la administración de equipos, es necesario ligar el equipo al servidor de dominio, como se muestra en el ANEXO 2.

Las pruebas fueron realizadas en un equipo con sistema operativo Windows 7, tomando como muestra las principales directivas aplicadas para los usuarios, tanto administrativos, docentes y estudiantes.

Administrativos

Como muestra se ha tomado al usuario Juan Pablo Ramón Sarango, técnico de la Dirección de Telecomunicaciones e Información, en la Figura 80, se puede apreciar las principales directivas aplicadas a los usuarios administrativos, en ella se puede notar que el símbolo de sistema (CMD) se halla activo, el cambio de tema, colores, sonidos y protector de pantalla se encuentra desactivado para que no se pueda realizar cambios

en la personalización de pantalla, se puede observar también que el icono de juegos en el inicio no se halla en el mismo, el botón de apagado se encuentra normal ya que no se han realizado cambios en el mismo.

Figura 80. Cuenta administrativo

Fuente: Autor

Docentes

Respecto a docentes se ah tomando como muestra la cuenta del Ing. Mario Enrique Cueva Hurtado, en la Figura 81, se puede apreciar las directivas más significativas aplicadas a la parte de docencia de la institución, entre ellas se puede observar el CMD activo, el botón de apagado del equipo normal, el icono de juegos no se aprecia en el menú de inicio, de la misma manera que el usuario administrativo, se puede notar también que se puede acceder con normalidad a programas y características que es en donde se muestran todos los programas instalados en el equipo.

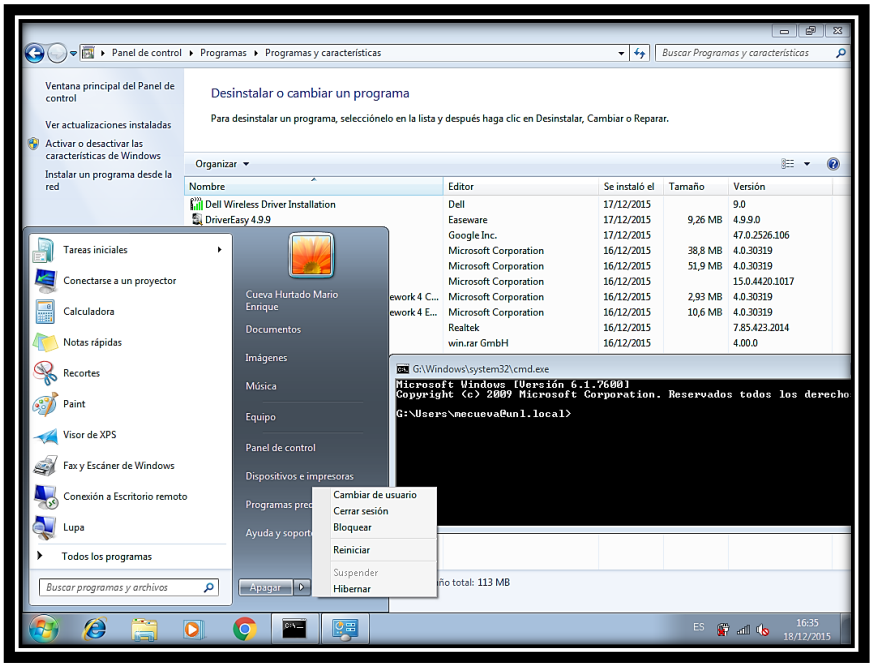


Figura 81. Cuenta docente

Fuente: Autor

Estudiantes

Para realizar las pruebas con cuenta de estudiantes, se ha tomado como muestra a Henry Paúl Vivanco Encalada, en la Figura 82, se puede notar al símbolo de sistema deshabilitado, programas y características de la misma manera, lo que no sucedía con administrativos y docentes, el icono de juegos no se halla en el menú inicio y por último el botón de apagado del equipo se haya modificado, es decir no se presenta el apagado del mismo, en su lugar se encuentra la opción de cerrar sesión, los estudiantes no tendrán la facultad de apagar los equipos usados con sus cuentas.

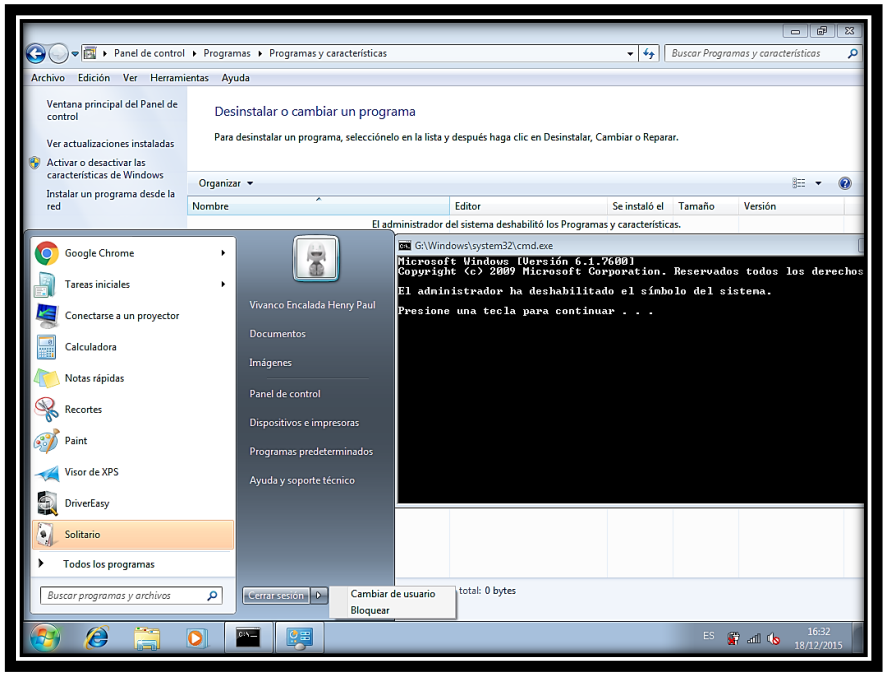


Figura 82. Cuenta estudiante

Fuente: Autor

7. Discusión

Como resultado de la implementación de Active Directory, aplicando el estándar de seguridad 802.1x en la red de datos de la Universidad Nacional de Loja, se obtuvo como resultado la autenticación de cada uno de los usuarios finales que hacen uso de este servicio brindado por la institución, el mecanismo de autenticación aplicado es satisfactorio, ya que mediante el mismo se reducen considerablemente los problemas que se tenían con anterioridad.

Cada persona inmersa en la institución cuenta con un usuario y contraseña propia para su autenticación, ya sea en su computador o dispositivo móvil, sin dar mayor importancia al sistema operativo, gracias a la implementación de un servidor RADIUS, el cual mediante el estándar de seguridad 802.1x hace posible las conexiones del cliente hacia el servidor.

Para hacer posible la autenticación de usuarios mediante Active Directory y el estándar de seguridad 802.1x, se llevó a cabo diversos procedimientos, tales como:

- Levantamiento del servidor, instalando y configurando el sistema operativo Windows Server 2012.
- Configuración de Active Directory, con todas sus unidades organizativas, grupos, usuarios y políticas o directivas para cada uno de ellos.
- Configuración de servidor RADIUS, el cual es el encargado de realizar la conexión entre el servidor como controlador de dominio y usuario final.
- Configuración de los equipos proveedores de internet, tanto AP´S como Switch´s, aplicando el estándar de seguridad 802.1x.

Realizados estos pasos o secuencia de procedimientos, se obtuvo como resultado lo que se esperaba, la autenticación exitosa y segura de usuarios finales dentro de la red de la Universidad Nacional de Loja.

7.1 Desarrollo de la propuesta alternativa

Cada uno de los objetivos planteados, tanto general como específicos, fueron cumplidos con éxito, obteniendo los resultados esperados. Los objetivos específicos fueron parte fundamental de las fases del proyecto de titulación, los cuales se detallan a continuación

indicando los procesos que se llevaron a cabo para el cumplimiento exitoso de los mismos:

7.1.1 Objetivo Especifico 1: Analizar la situación actual de la red LAN y WLAN para la implementación de Active Directory aplicando el estándar de seguridad IEEE 802.1X dentro de la Universidad Nacional de Loja

- **Estudio de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de host o recursos tecnológicos implementados actualmente**

Para el estudio de la situación actual de la Universidad Nacional de Loja en cuanto a la red de datos, fue necesario realizar entrevistas a la ex subdirectora de la Sección de Redes y Equipos Informáticos de la Dirección de Telecomunicaciones e Información, la Ing. Nohelia Alfonsina Bustamante Pardo.

Una vez realizadas las entrevistas obteniendo información importante, brindada por la institución, en cuanto a la estructura de la red de la Universidad Nacional de Loja, se puso conocer la realidad que atraviesa la institución en cuanto al servicio que brinda a todos los usuarios finales de la red de datos.

Como primer punto, se realizó un estudio de la estructura de la institución en la parte académica y administrativa, obteniendo como resultado que la Universidad Nacional de Loja, cuenta con cinco áreas académicas-administrativas, junto con sus extensiones, y un área administrativa, que es la encargada del funcionamiento administrativo de la institución.

De la misma manera se logró conocer la misión y visión de la institución, adjuntando además el organigrama estructurar que es manejado hoy por hoy en la Universidad.

Ya que el proyecto de tesis se basa en la parte de la red de datos de la institución, se definió la sección encargada de brindar el servicio, indicando sus principales funciones dentro de la Universidad.

Para una mejor comprensión del diagrama o topografía general en cuanto a la red de la Universidad Nacional de Loja, se adjuntó una tabla descriptiva con la simbología usada en el diagrama.

Se indicó de manera breve como se hallan distribuidos los Switch's, VLAN'S y Subredes por cada una de las áreas que conforman la institución, anexando información importante que respalde la veracidad del proyecto de titulación.

Por último, la institución cuenta con un cuarto de máquinas, en el cual se almacenan diversos equipos para brindar servicios a la universidad, de manera breve y concisa se indicó la importancia y funcionamiento que tiene cada uno de estos equipos dentro de la institución a nivel de servicios de red.

- **Verificación de la infraestructura a nivel de servidores**

Para conocimiento de la infraestructura de los servidores existentes en la Universidad Nacional de Loja y los servicios que cada uno de ellos presta, fue necesario realizar una entrevista a la persona encargada de los mismos, brindándonos información necesaria de que servicios brinda cada uno de ellos, indicándonos así mismo el hardware que es soportado para cada uno de los servidores existentes en la institución.

El principal motivo de la verificación de la infraestructura a nivel de servidores, fue conocer si existe algún servidor de Microsoft en la institución, o percatarnos de la existencia de espacio necesario para el levantamiento del directorio activo.

- **Verificación de la infraestructura a nivel de estaciones de trabajo, características de funcionamiento, operatividad y limitaciones que presentan actualmente los recursos tecnológicos**

En cuanto a la verificación de la infraestructura a nivel de estaciones de trabajo, indicando las características de cada uno de ellos, se realizó una entrevista a la persona encargada de la sección de mantenimiento de la institución, indicándonos diversos puntos indispensables para el cumplimiento del proyecto de titulación.

Cada una de las áreas académico-administrativas, cuentan con una bodega principal, en las mismas fue necesario realizar una petición personal a las personas encargadas de estas, para que se nos brinde información que constate la existencia de los equipos informáticos o computadores, tanto de escritorio como portátiles, que existen en la Universidad Nacional de Loja.

El principal motivo de este punto, es el conocimiento de los sistemas operativos principales que se manejan en la institución.

7.1.2 Objetivo Específico 2: Analizar los servicios que brinda Active Directory para mejorar la seguridad y administración de los recursos tecnológicos dentro de la red LAN y WLAN de Universidad Nacional de Loja

- **Estudio de las características, ventajas y desventajas de la herramienta**

Antes de decidir la herramienta para el levantamiento del servidor de dominio, fue necesario realizar una comparación entre dos herramientas de mayor demanda, una de ella privativa como es Active Directory, y OpenLDAP propietaria o de código abierto.

El análisis comparativo entre estas dos herramientas se lo realizó en base a características administrativas, rendimiento y costos, obteniendo como resultado la mejor opción para el levantamiento del servidor de dominios a Active Directory.

Una vez elegida la herramienta idónea para la ejecución del proyecto de tesis, fue necesario conocer las principales características de la herramienta y directivas de usuario para la administración de equipos, así mismo cuales son las ventajas y desventajas que trae consigo la implementación de Active Directory como controlador de dominio.

- **Estudio del hardware y software de acuerdo a los requerimientos necesarios para la implementación del servidor**

Para el desarrollo éxito, y cumplimiento de este ítem fue necesario realizar diversas consultas en fuentes confiables, consultas en cuanto al hardware y software necesario para la implementación del servidor de dominio.

De acuerdo al número de usuarios finales con los que cuenta la Universidad Nacional de Loja, se realizó consultas del hardware mínimo, adecuado y recomendado, para con ello conocer si la institución cuanta con el hardware adecuado para la implementación de Active Directory sin tener molestias o problemas posteriores a su implementación.

- **Análisis de los servicios de seguridad que brinda el estándar 802.1x**

Al realizar la implementación de Active Directory como controlador de dominio, se debe conocer también el estándar de seguridad con el que va a contar. Para ello y para cumplir

con éxito el presente ítem se tuvo que realizar diversas consultas sobre todos los servicios, a nivel de seguridad que ofrece 802.1x.

Se indicó también por qué usamos este estándar de seguridad, además de ello se realizó un análisis comparativo entre 802.1x y otro estándares de seguridad, para con ello poder tener en claro cuáles son los principales beneficios de usar 802.1x.

7.1.3 Objetivo Específico 3: Analizar las políticas de seguridad y privacidad necesarias para todo el personal académico y administrativo, quienes hacen uso de la red LAN y WLAN de la Universidad Nacional de Loja

- **Determinar los grupos de trabajo según la estructura jerárquica de la red de datos de la Universidad Nacional de Loja**

Al implementar Active Directory, se debe conocer cuáles serán los grupos de trabajo inmersos en el directorio activo. Para conocer cuáles son los grupos de trabajo o UO, y que usuarios finales pertenecen a cada grupo de usuarios, se realizó una consulta personal a la persona encargada de la administración de la red de la Universidad Nacional de Loja, sabiéndonos indicar, que la estructura de las UO deben ser de acuerdo al orgánico estructural que maneja la institución.

La red de datos de la institución se halla formada por diversas VLAN´S, y cada una de ellas pertenece a un grupo específico de usuarios, es por ello que los grupos de usuarios inmersos en Active Directory, son los mismos grupos pertenecientes a cada una de las VLAN´S de la red de la institución.

- **Obtención de las necesidades actuales de los usuarios a nivel de servicios de red, en los procesos académicos, como administrativos que se ejecutan en la Universidad Nacional de Loja**

Para el correcto cumplimiento de este ítem fue necesario especificar los tipos de usuarios que se tiene, uno de ellos es el Usuario Administrador y los Usuarios Finales quienes son los que obtienen el servicio que ofrece la institución.

Los procesos tanto académicos como administrativos, son llevados a cabo por los usuarios finales de la red, dependiendo del usuario y el grupo al que pertenece, este puede realizar procesos académicos o administrativos, se detalló cuáles son los

procesos académicos que se cumplen y que grupo de trabajo los realiza, de la misma manera para los procesos administrativos.

Para obtener las necesidades actuales, nos enfocamos al usuario administrador, el mismo será la persona encargada de la administración de la red de la institución, para obtener estas necesidades se realizó un dialogo con dicha persona, sabiéndonos manifestar las principales necesidades a nivel de servicios de red.

- **Determinar las políticas de seguridad y privacidad de acuerdo a las funciones que desempeña el personal tanto académico como administrativo**

Las políticas de seguridad y privacidad planteadas se hallan determinadas en base al Servidor de Directivas de Redes que brinda Active Directory, utilizando el manual que ofrece Microsoft en cuanto a las políticas que pueden aplicarse mediante NPS, y de acuerdo a directivas aplicables para la administración de equipos se detalló cuáles son cada una de ellas y que función cumplen en el directorio activo.

Entre las principales políticas de acceso a la red, que fueron planteadas se encuentran: cambio de contraseña al iniciar sesión, tiempo de expedición de la cuenta, horas y días en los que se puede acceder a la red, en cuanto a políticas o directivas aplicadas a los usuarios para la administración de equipos se implementaron las siguientes, entre las principales: bloqueo o acceso al símbolo de sistema, denegación de cambio de pantalla, tema o colores, bloqueo del programas y características, modificación del botón de apagado, bloqueo de propiedades tanto del equipo como de la barra de tareas.

Todas ellas dependiendo el tipo de usuario final, es decir docente, estudiante, administrativo o trabajador.

7.1.4 Objetivo Especifico 4: Realizar la implementación y pruebas de funcionalidad del servidor, verificando la prestación del servicio como controlador de dominio, dentro del Área de la Energía las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja

- **Instalación y configuración de la plataforma operativa en el servidor físico**

Como parte final del proyecto de titulación se ha planteado el ítem de instalación y configuración de la plataforma operativa en el servidor físico.

Para el cumplimiento exitoso de este ítem fue necesaria la autorización de un espacio físico en el BLADE que posee la Universidad Nacional de Loja; esta autorización fue otorgada por parte del ex director de la Dirección de Tecnología e Información, el Ingeniero Milton Ricardo Palacios Morocho, cabe recalcar que la institución, por medio de las autoridades correspondientes se hizo la adquisición de la licencia de la plataforma operativa.

Como se indicó con anterioridad la plataforma operativa o software necesario para la implantación de Active Directory, es Windows Server (se hace uso la versión Standard 2012).

Para la instalación del Sistema Operativo se hizo uso de manuales y tutoriales que indican detalladamente como se puede realizar la instalación de este con sus principales configuraciones.

- **Instalación y configuración de la herramienta Active Directory con las políticas de seguridad y servicios establecidos**

Al tener instalada la plataforma operativa, solo restaba configurar Active Directory con todas las políticas de seguridad para el acceso a la red y las directivas para la administración de equipos, aquí también se realizó la configuración de servidor RADIUS, así mismo la configuración necesaria en cada uno de los equipos que proveen de internet a la institución, todo ello para poder realizar el mecanismo de autenticación usando el protocolo de seguridad nombrado con anterioridad.

Todo esto se lo llevo a cabo mediante estudio en diferentes fuentes, las cuales nos permitieron realizar estas configuraciones con éxito, obteniendo los resultados requeridos.

Tanto el mecanismo de autenticación como los perfiles de los usuarios administrativos, fueron puestos en marcha en la Dirección de Telecomunicaciones e Información mediantes los dos tipos de conexión (cableado, inalámbrico).

Habiendo instalado y configurando la herramienta, se ha logrado cumplir con éxito parte de este objetivo.

- **Pruebas de funcionalidad a nivel de servidor como controlador de dominio**

Para cumplir con éxito este ítem, se realizaron las pruebas mediante una herramienta propia que brinda Active Directory, esta herramienta permite conocer cuál es el estado del servidor aplicando diversas pruebas.

La herramienta aplicada se denomina DCDIAG, para hacer uso de ella simplemente se escribe en el CMD o consola la palabra "*dcdiag*"; para la ejecución del comando se debe estar en modo "Administrador".

- **Pruebas de funcionalidad a nivel de estaciones de trabajo dentro del Área de la Energía las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja**

Para cumplir exitosamente con este ítem, que se basa en la realización de pruebas de funcionalidad a nivel de estaciones de trabajo, se realizaron dichas pruebas con diferentes sistemas operativos, realizando un proceso en cada uno de ellos.

Para realizar las pruebas necesarias a nivel de estaciones de trabajo, fue necesario la configuración de 2 equipos Switch administrables, uno de ellos el encargado de brindar internet al segundo equipo, en este primer equipo fue necesario configurar el puerto del cual sería tomada la cascada hacia el segundo equipo, poniéndolo en modo Trunk, para permitir el paso de diversas VLAN's, en el segundo equipo, se realizó la configuración del puerto al cual llegaba el internet, configurándolo al mismo en modo Trunk para permitir la llegada de las VLAN's, después de realizar las configuraciones necesarias

para el estándar 802.1x, en todos los puertos del equipo, solamente restaba asignar diferentes VLAN's en los puertos del switch.

Los resultados de cada una de las pruebas en los diferentes sistemas operativos, aplicando los procesos adecuados, se plasmaron en tablas en las cuales se indica una imagen o captura de pantalla del proceso llevado, se indicó también la acción y si esta fue cumplida con éxito, cada una de estas acciones trae consigo comentarios indicando puntos claves en la ejecución de cada acción.

De esta manera se cumplió con éxito cada uno de los ítems y objetivos planteados en el proyecto de titulación.

7.2 Valoración técnica económica y ambiental

7.2.1 Valoración técnica económica

En el desarrollo del proyecto de titulación, fueron necesarios recursos tanto humanos, técnicos y materiales; a continuación se detallan cada uno de ellos.

7.2.1.1 Talento humano

TABLA XXVIII. TALENTO HUMANO

Rol	Número de Horas	Valor Hora ($)	Valor Total ($)
Director: Ing. Carlos Jaramillo	200	0.00	0.00
Investigador 1: Lenin Ocampo	400	5.00	2000.00
Investigador 2: Henry Vivanco	400	5.00	2000.00
Total ($)			**4000.00**

7.2.1.2 Recursos técnicos

TABLA XXIX. RECURSOS TECNICOS

Descripción	Cantidad	Valor Unitario ($)	Valor Total ($)	Depreciación Anual
Hardware				
Computador	2	900.00	1800.00	600.00
Impresora	2	100.00	200.00	66.66
Disco USB	2	10.00	20.00	6.60
Software				
Windows Server Estándar 2012 (UNL)	1	988.00	988.00	0.00

Google Drive	2	0.00	0.00	0.00
Dropbox	2	0.00	0.00	0.00
Total ($)			**3008.00**	**673.26**

La depreciación referida en la TABLA XXIX se obtiene dividiendo el costo total del activo fijo para el número de años de vida útil que tiene el mismo. [22], [23]. La vida útil se ha tomado de referencia de 3 años para cada uno de los elementos hardware.

7.2.1.3 Recursos materiales

TABLA XXX. RECURSOS MATERIALES

Descripción	Cantidad	Valor Unitario($)	Valor Total ($)
Cartuchos de Tinta	4	25.00	100.00
Resma de Papel	1	4.00	4.00
Transporte	80	0.30	24.00
Internet	500 h	0.50	250.00
Copias	200	0.02	4.00
Varios	-----	20.00	20.00
Total ($)			**402.00**

7.2.1.4 Total de recursos

TABLA XXXI. TOTAL DE RECURSOS

Recurso	Subtotal ($)
Recurso Humano	4000.00
Recurso Técnico	673.26
Recurso Material	402.00
Improvistos (5%)	253.76
Total ($):	**5329.023**

Para el cálculo de los imprevistos referidos en la TABLA XXXI, se ha considerado el 5% del Valor total del presupuesto. [24]

7.2.2 Valoración ambiental

Al evitar pérdidas de direcciones IP destinadas a personas ajenas a la institución mediante el mecanismo de autenticación implementado, se minimiza considerablemente el uso de energía eléctrica en cada uno de los equipos de los usuarios ajenos la Universidad Nacional de Loja, ya que al no lograr conectarse al internet se minimiza considerablemente el uso del computador y dispositivos móviles, ayudando así al medio ambiente en la reducción de energía innecesaria.

Por la razón antes mencionada nuestro proyecto de titulación es justificado en cuanto a la valoración ambiental.

8. Conclusiones

- En base al estudio realizado a la infraestructura tecnológica de la Universidad Nacional de Loja, se pudo determinar que la institución cuenta con una red de datos óptima, para la implementación de Active Directory.
- Al implementar Active Directory y en base a las pruebas realizadas, se puede indicar que este servicio de directorio ha permitido mejorar y facilitar la administración de usuarios y equipos.
- Las directivas o políticas de seguridad aplicadas a la institución, ayudaron al control de acceso a la red y administración de equipos tecnológicos.
- La implementación de Active Directory como controlador de domino ayuda a las PYMES e instituciones, a centralizar la seguridad y administración de los recursos tecnológicos.
- El estándar 802.1x permitió fortalecer las seguridades, administrando de forma eficiente el acceso a red de acuerdo a los permisos que han sido establecidos.

9. Recomendaciones

- A los responsables de la gestión y control del personal administrativo, docentes y estudiantes de la Universidad Nacional de Loja, el levantamiento total de los datos personales complementarios para que se integren al directorio activo.
- Actualización continúa de mecanismos de autenticación haciendo uso del estándar de seguridad 802.1x, para lograr proteger la red ante nuevas amenazas.
- Implementación de un servidor de pruebas como medida de precaución antes de poner en producción el servidor final.
- Actualización continua de la información de los recursos tecnológicos pertenecientes a la Institución.
- Etiquetado total de los equipos y puntos de red, para facilitar su identificación y ubicación.
- Elaboración de un plan de directivas o políticas aplicables a los usuarios de la red y equipos tecnológicos de la institución, por parte de las autoridades correspondientes.
- A la Dirección de Telecomunicaciones e Información se implemente mecanismos para la sincronización de la información de los diferentes servidores de la institución.

10. Bibliografía

Referencias bibliográficas

[1] C. Pradas, Rafael, “Introducción al Servicio de Directorio”, *Red académica y de investigación nacional*, [online], 2014, Disponible en: https://www.rediris.es/ldap/doc/ldap-intro.pdf.

[2] C.F. Romero, “*Análisis Comparativo entre Productos que proveen Servicio de Directorio pertinentes a Tecnologías Propietaria y de Libre Acceso, aplicado a laboratorios en ambientes educativos*”, Trabajo Fin de Carrera, Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica del Litoral, Guayaquil, 2008.

[3] M. Suarez, “Sistemas Informáticos Avanzados Open LDAP”, *Redes Linux*. [online] 2004.

[4] V. Emmanuel, Exchange Server 2010 Preparación para la certificación MCTS 70-66. s.l. : Ediciones Eni, 2010.

[5] TechNet, Microsoft. Introducción a las infraestructuras de Active Directory. Microsoft TechNet. [online] 2008.

[6] Institute, Sans. Global Information Assurance Certification Paper. INTRODUCCIÓN A LA ESTRUCTURA DEL DIRECTORIO ACTIVO. [online] 2003.

[7] Microsoft, Technet. Network Policy and Access Services. Technet Microsoft. [online] 4 de 2009. https://technet.microsoft.com/es-es/library/cc754521(v=ws.10).aspx.

[8] Chamorro, Juan M. Consideraciones para la implementación de 802.1x. SANS information security training. [online] 2012. https://www.sans.org/reading-room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlans-1607.

[9] IEEE 802 Standards Committee. IEEE 802 LAN/MAN Standards Committee. IEEE 802. [online] 2012. http://www.ieee802.org/1/.

[10] Pagina Web Universidad Nacional de Loja, Nosotros, [online] (2015), Disponible en: http://unl.edu.ec/universidad/nosotros.

[11] Microsoft, *Características de Active Directory*, [online], 2015 Disponible en: https://msdn.microsoft.com/es-es/library/cc737139(v=ws.10).aspx.

[12] Windows Server, *Windows Server 2012*, [online], 2015 Disponible en: https://technet.microsoft.com/es-es/Windowsserver/2012r2.aspx

[13] Microsoft, *Novedades en AD CS*, [online], 2015 Disponible en: https://technet.microsoft.com/es-es/library/hh831373.aspx

[14] Microsoft, *Novedades en Windows Server 2012*, [online], 2015 Disponible en: https://technet.microsoft.com/library/hh831769.aspx

[15] Microsoft, *Dimensionar Hardware para servidores para Active Directory en Windows Server 2012*, [online], 2015 Disponible en: https://social.technet.microsoft.com/Forums/es-ES/b1684ae3-50e2-4ae9-bd40-0e4f0bf252f7/dimencionar-hardware-para-servidores-para-active-directory-en-Windows-server-2008-r2?forum=wsades

[16] *Diagnostico de Directorio Activo-DCDIAG*, [online], 2010, Disponible en: https://masrobeznoquenunca.wordpress.com/2010/02/25/diagnostico-de-directorio-activo-%E2%80%93-dcdiag/

[17] Windows Server, *Dcdiag*, [online], 2015, Disponible en: https://technet.microsoft.com/es-es/library/cc731968(v=ws.10).aspx.

[18] Microsoft, *DsfReplication*, [online], 2015, Disponible en: http://social.technet.microsoft.com/wiki/contents/articles/1207.dfsr-event-5002-dfs-replication.aspx#Summary

[19] Microsoft Support, *Dcdiag fails for NCSecDesc test*, [online], 2015, Disponible en: https://support.microsoft.com/en-us/kb/967482

[20] Microsoft TechNet, *How Active Directory Replication Toology Works*, [online], 2015, Disponible en: https://technet.microsoft.com/en-us/library/cc755994(v=ws.10).aspx

[21] Windows Server, *RID Manager*, [online], 2015, Disponible en:

https://technet.microsoft.com/en-us/library/cc756626(v=ws.10).aspx.

[22] Servicio de Rentas Internas, *Reglamento de Aplicación de la Ley de Régimen Tributario Interno*, [online], 2010 Disponible en: http://www.sri.gob.ec/web/guest/ depreciacion-acelarada-de-activos-fijos.

[23] Aguirre Espinoza, Edison Leonardo E. Aguirre "*Diseño de una metodología para el aprovechamiento ´óptimo de los activos fijos de CASABACA S.A. en el área administrativa, contable, tributaria y financiera*", Tesis Pregrado, Contabilidad y Auditoría, Universidad Politécnica Salesiana, Ecuador, 2010.

[24] J. Toro, *Formulación y Evaluación de Proyectos*, Contribuciones a la Economía, ISSN 1696-8360, pp. 17, Mayo. 2009.

11. Anexos

ANEXO 1: Configuración de clientes para la conexión a la red

Windows (Windows 8.1)

Los pasos para configuración de clientes, en Windows 8.1 se puede apreciar en la Figura 83.

- **Paso 1.-** Verificación y configuración correcta de las propiedades de la tarjeta de red.
- **Paso 2.-** Verificar el tipo de seguridad WPA2-Enterprese.
- **Paso 3.-** Método de autenticación de red EAP protegido (PEAP).
- **Paso 4.-** (Opcional) Recordar credenciales permite que al autenticarse con éxito y cerrar la sesión, este no volverá a pedir una nueva autenticación (ingreso de usuario y contraseña).
- **Paso 5.**- Ingresar a configuración avanzada.

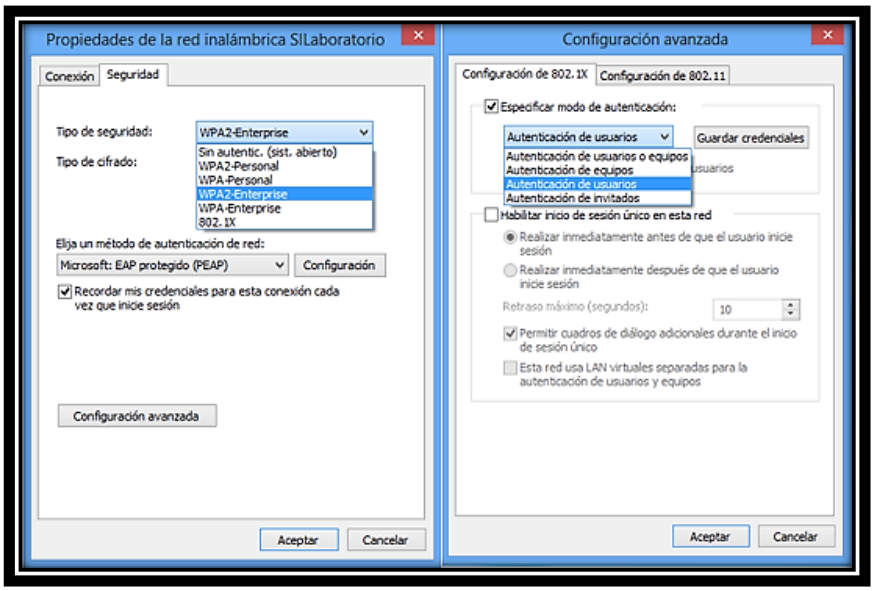


Figura 83. Configuración Tarjeta de red Windows 8.1

Fuente: Autor

Linux (Ubuntu 14.10)

Los parámetros que se muestran en la Figura 84. Son los valores predeterminados con los que se realiza una autenticación exitosa pero se recomienda verificar que sean los correctos antes de realizar el proceso de autenticación.

- **Paso 1.-** Verificar en el campo Autenticación el método de autenticación de red sea EAP protegido (PEAP).
- **Paso 2**. Verificar el campo Autenticación interna este seleccionado el método de autenticación MSCHAPv2.

En los campos vacíos se debe colocar la siguiente información:

- **Identidad anónima:** Se refiere a un alias del usuario, el cual no se está manejando actualmente, el campo debe dejarse vacío.
- **Nombre de usuario:** En este campo se debe colocar la cuenta del usuario ejemplo: sistemas@unl.local.
- **Contraseña:** Se debe escribir la contraseña de la cuenta del usuario (número de cedula).

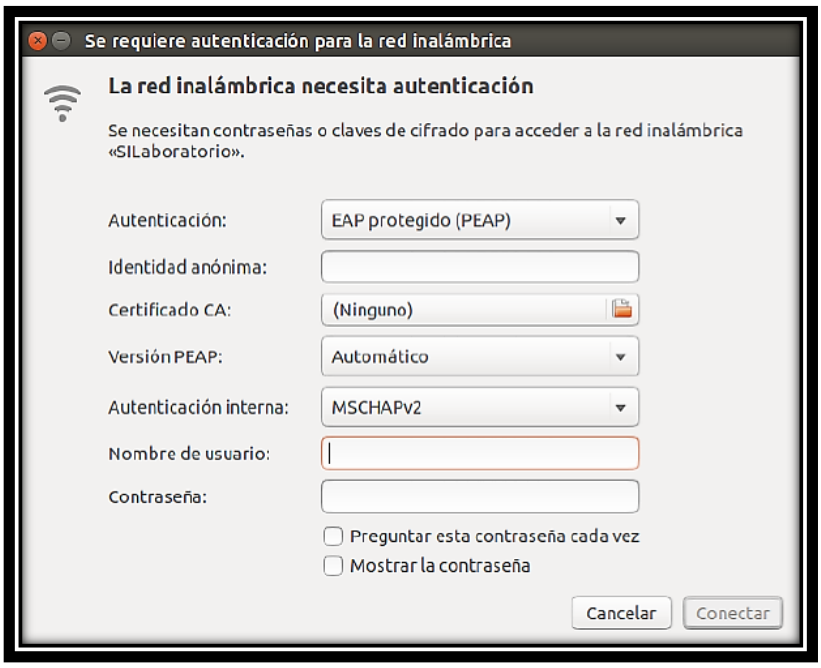


Figura 84. Autenticación red inalámbrica Ubuntu 14.10

Fuente: Autor

Android (Android 5.0.1)

Los parámetros que se muestran en la Figura 85. Son los valores predeterminados con los que se realiza una autenticación exitosa pero se recomienda verificar que sean los correctos antes de realizar el proceso de autenticación.

- **Paso 1.-** Verificar en el campo Método PEAP el método de autenticación de red sea PEAP.
- **Paso 2.**- Verificar el campo Autenticación de fase2 este seleccionado el método de autenticación MSCHAPv2.

La conexión para Android es la misma que para el sistema operativo Ubuntu, los campos que deben ser llenados son los siguientes:

- **Identidad anónima:** Se refiere a un alias del usuario, el cual no se está manejando actualmente, el campo debe dejarse vacío.
- **Nombre de usuario:** En este campo se debe colocar la cuenta del usuario ejemplo: sistemas@unl.local.
- **Contraseña:** En el campo contraseña, se debe escribir la contraseña de la cuenta del usuario (número de cedula).

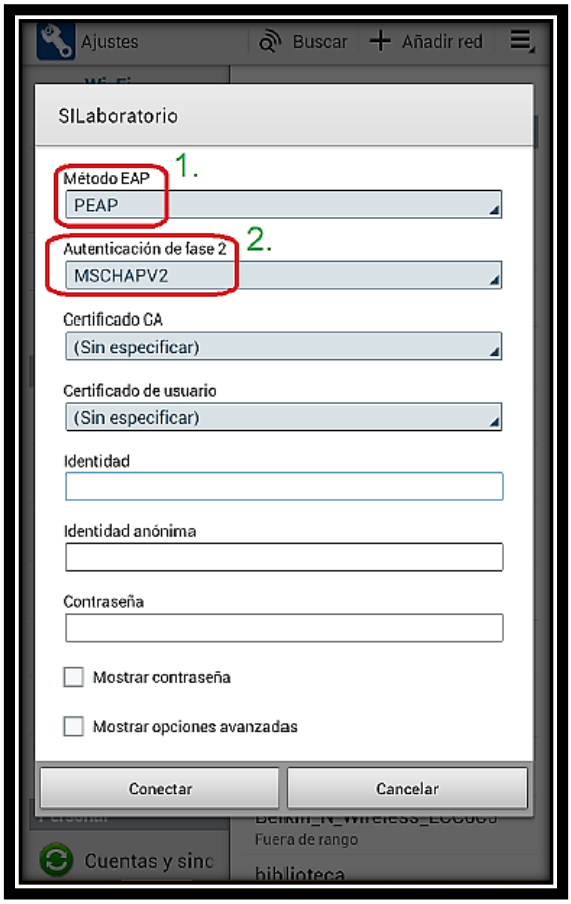


Figura 85. Autenticación red Android

Fuente: Autor

IOS (IOS 8.4)

Los parámetros que se muestran en la Figura 86. Son los valores predeterminados con los que se realiza una autenticación exitosa.

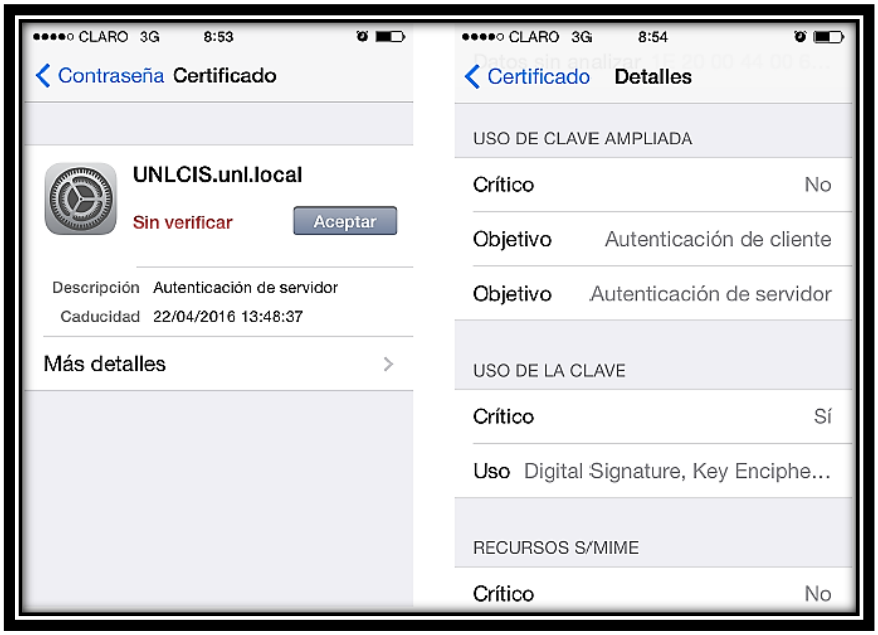


Figura 86. Autenticación red Iphone

Fuente: Autor

ANEXO 2: Configuración de clientes para unirse al dominio

Para lograr la conexión exitosa al dominio debe realizarse los siguientes pasos:

Antes que nada se debe enlazar con el servidor de dominios, para ello se debe modificar la dirección del servidor DNS preferido, ingresando la dirección IP del servidor, se lo realiza ingresando al centro de redes y recursos compartidos, una vez allí, se debe ingresar a Cambiar configuración del Adaptador, allí debemos fijarnos en el tipo de conexión que estemos (cableada o inalámbrica), dependiendo de ello se debe modificar este adaptador como se muestra en la Figura 87, en este caso la configuración se realiza en la tarjeta d red inalámbrica (el mismo proceso para tarjeta de red Ethernet).

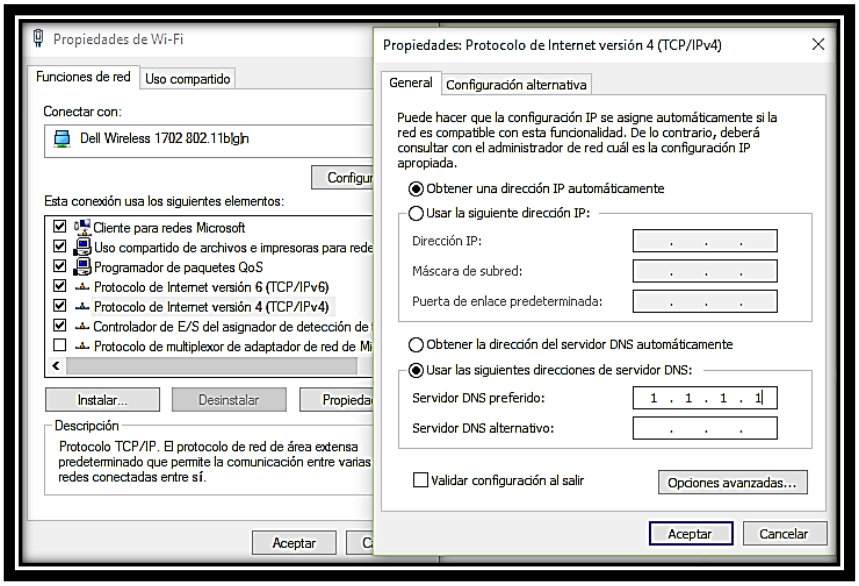


Figura 87. Cambiar configuración adaptador de red

Fuente: Autor

Una vez enlazado el equipo al servidor, se realiza el cambio o unió al dominio, para ello se debe ingresar a propiedades del equipo y cambiar configuración como se muestra en la Figura 88.

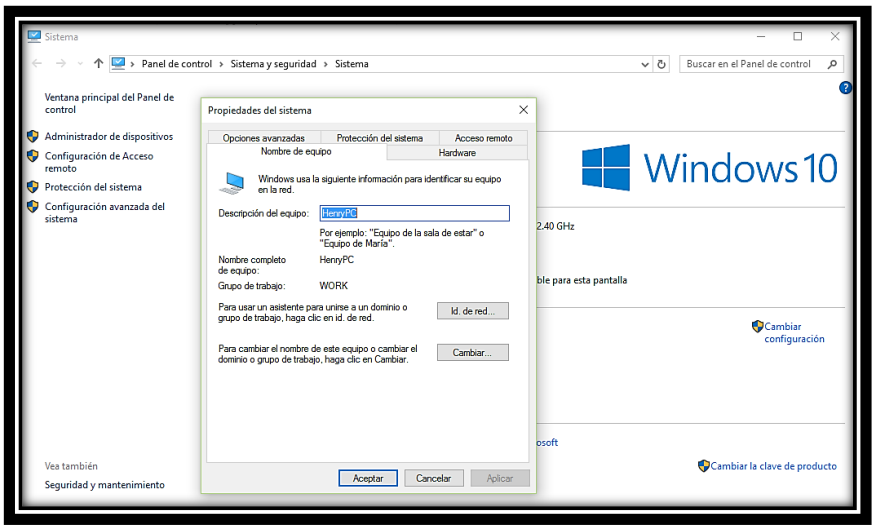


Figura 88. Cambiar configuración del equipo

Fuente: Autor

Una vez en la ventana de Propiedades del Sistema se debe dar clic en el botón cambiar que se muestra en la Figura 89, dando clic en dicho botón aparecerá una ventana denominada cambios en el dominio o el nombre del equipo, como muestra la Figura 81,

en ella, tenemos el nombre del equipo, en el campo de Miembro del: activamos el ítem Dominio e ingresamos el dominio a unirse, y aceptamos.

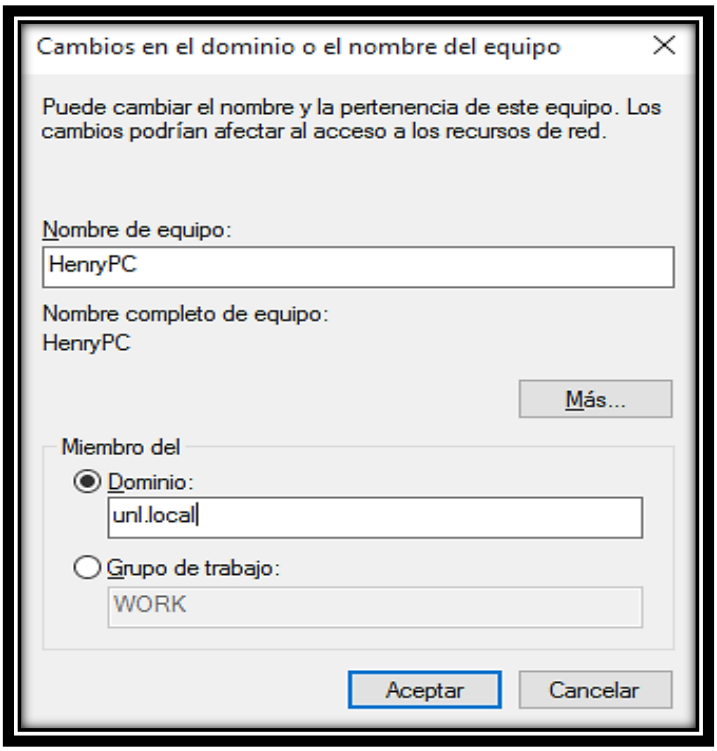


Figura 89. Cambios en el dominio

Fuente: Autor

Una vez aceptado el dominio pedirá ingresar los datos de la cuenta, como se muestra en la Figura 90, en esta ventana ingresamos la cuenta del administrador con su contraseña, para así poder ligar este equipo con diferentes cuentas de usuarios.

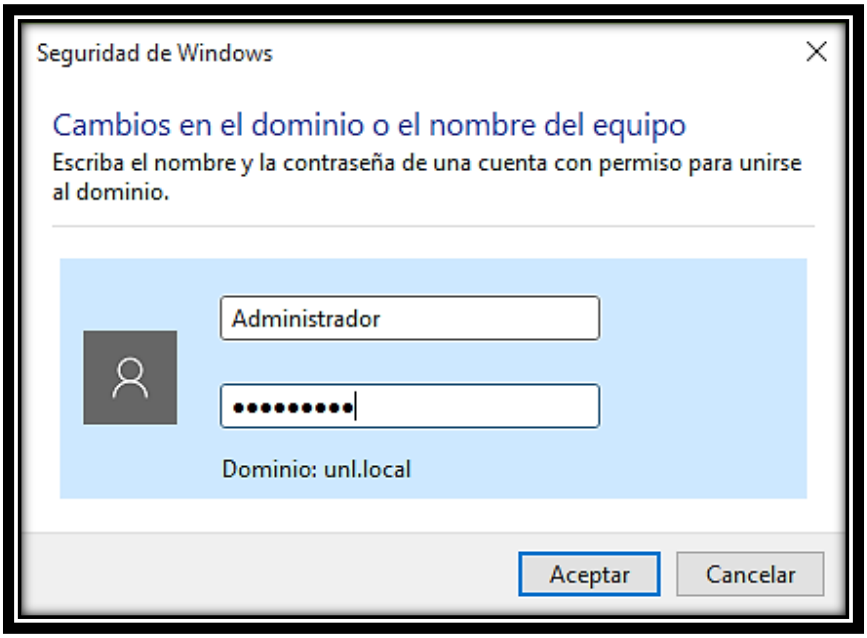


Figura 90. Cuenta de Administrador

Fuente: Autor

Si la cuenta de usuario ingresada, es la correcta se mostrara un mensaje de unión de dominio exitosa como se muestra en la Figura 91, para realizar los cambios el equipo pedirá reiniciar el mismo.

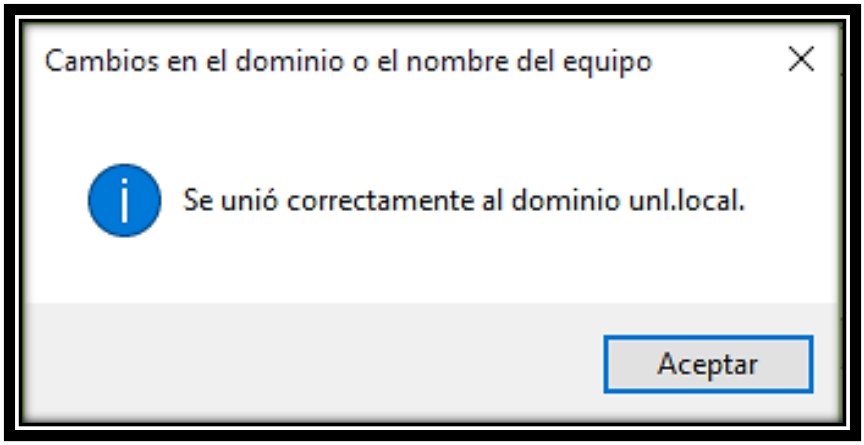


Figura 91. Unión correcta al dominio

Fuente: Autor

Una vez reiniciado el equipo, se debe ingresar al mismo aplicando otra cuenta de usuario, allí se debe ingresar la cuenta de usuario y contraseña, si estos son correctos se podrá acceder al mismo.

Los pasos indicados, son los mismos para cualquier sistema operativos de Microsoft.

ANEXO 3: Glosario

Termino	Definición
1. Capa de abstracción	Es una manera de ocultar los detalles de implementación de la funcionalidad de un sistema en particular.
2. CHAP: Challenge Handshake Protocol	Protocolo de seguridad que realiza una validación de tres vías entre cliente y servidor.
3. DAP: Directory Access Protocol	Es un estándar dentro de las redes de ordenadores que ha sido promulgado por la ITU-T y por la ISO en 1998 para el acceso de un servicio de directorio X.500.
4. DHCP : Dynamic Host Configuration Protocol	Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.
5. DNS: Domain Name System	Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
6. EAP: Extensible Authentication Protocol	Es un framework de autenticación usado habitualmente en redes WLAN Point-to-Point. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas.
7. EAP-TLS	Realiza la autenticación estableciendo un túnel cifrado entre los elementos para proteger las credenciales y datos que se intercambian. Utiliza certificados digitales para autenticar a cliente y servidor.
8. IEEE: Institute of Electrical and Electronics Engineers	Es una asociación mundial de técnicos e ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas.
9. IP: Internet Protocol	Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP.
10. ISP: Proveedor de servicios de Internet	Es la empresa que conecta a sus usuarios a Internet a través de diferentes tecnologías como Línea de abonado digital (DSL), GSM, dial-up, etc.
11. LAN: Local area network	Es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
12. LEAP	Es un método de autenticación desarrollado por Cisco, que usa contraseña para autenticar al cliente. Generalmente se requiere de hardware/software Cisco para soportarlo. Adicionalmente, es susceptible a ataques de adivinación de contraseñas, y no permite autenticar equipos
13. LDAP: Protocolo Ligero de Acceso a Directorios	Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
14. MAC: Media Access Control	Es el conjunto de mecanismos y protocolos a través de los cuales varios dispositivos en una red, se ponen de acuerdo para compartir un medio de transmisión común.
15. NAP: Control de acceso a red	Es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales, usuario o sistema de autenticación y reforzar la seguridad de la red de acceso.
16. NPS: Servidor de directivas de redes	Permite crear y aplicar directivas de acceso a la red en toda la organización para fines de mantenimiento de clientes y autenticación y autorización de solicitudes de conexión
17. OSI: modelo de interconexión de sistemas abiertos	Es el modelo de red descriptivo, que fue creado en el año 1980 por la Organización Internacional de Normalización (ISO).

18. PAP: Password Authentication Protocol	Este protocolo realiza la validación cuando se establece la conexión entre el cliente y el servidor.
19. PEAP: EAP-Protegido	Realiza la autenticación en dos fases. Primero establece una sesión TLS para autenticar al servidor y posteriormente se establece un segundo túnel para autenticar al cliente, permitiendo realizar autenticaciones de tipo CHAP (como el de Microsoft “MS-CHAP”) de manera más segura. Es un protocolo comúnmente soportado por tecnologías de Microsoft.
20. RADIUS: Remote Authentication Dial-In User Service.	Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.
21. SSID: Service Set Identifier	Es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.
22. Suplicante	Usuario que requiere autenticarse en la red.
23. TCP: Transmission Control Protocol	Protocolo utilizado para crear conexiones entre sí a través de las cuales puede enviarse un flujo de datos
24. TTLS	También se realiza la autenticación en dos fases, utilizando una sesión de TLS para proteger la autenticación del cliente (similar a PEAP). Puede utilizar tipos de autenticación diferentes a EAP, como CHAP, MS-CHAP y otros.
25. VPN: Virtual Private Network	Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
26. WEP: Wired Equivalent Privacy o "Privacidad Equivalente a Cableado".	Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite a cifrar la información que se transmite.
27. WLAN: Red de área local inalámbrica	Es un sistema de comunicación inalámbrica flexible, muy utilizada como alternativa a las redes de área local cableada o como extensión de éstas.

ANEXO 4: Entrevistas

Entrevista UTI

Universidad Nacional de Loja

En los tesoros de la sabiduría, está la glorificación de la vida.

Entrevista dirigida a la Sección de Mantenimiento en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Estimado Encargado(a)

Con la finalidad de obtener conocimiento acerca de los equipos informáticos o computadores que se hallan en la Universidad Nacional de Loja, nos permitimos realizar la presente entrevista. Sus opiniones serán importantes para el exitoso desarrollo de nuestro Proyecto de Titulación.

Le pedimos contestar las siguientes preguntas:

CÓDIGO	PREGUNTAS
N°1	**¿Qué equipos informáticos tanto computadores portátiles como de escritorio dispone actualmente la Institución en el área administrativa, investigación y desarrollo?**
	Comentarios: Se dispone actualmente con computadores de escritorio y portátiles para docentes y administrativos, estos equipos son entregados según la petición del mismo, es decir si un docente o administrativo hace la petición de un computador portátil en vez de un computador de escritorio se hace la entrega del mismo. Cada equipo queda a responsabilidad del peticionario.
N°2	**¿Cuáles son los principales sistemas operativos con los que cuentan los equipos informáticos?**
	Comentarios: Los principales sistemas operativos que se tiene en la Universidad son en la plataforma WINDOWS en sus diferentes versiones: Windows 7, Windows 8 y 8.1, en máquinas con pocos recursos es instalado Windows XP. También existen computadores en la plataforma de LINUX, principalmente se hace uso del Sistema Operativo UBUNTU.

N°3	**¿Existe equipo informático asignado permanentemente al personal que labora en la institución?**
	Comentarios: Todos los equipos son entregados de manera permanente, cada equipo queda a responsabilidad de la persona que lo adquiere, si dicha persona por diversas circunstancias ya no laborara en la Universidad el equipo debe ser entregado a bodega general, Si el equipo tiene algún fallo es entregado a mantenimiento para su revisión.
N°4	**¿Existe inventario del equipo informático entregado al área correspondiente?**
	Comentarios: Si existe un inventario manual en donde constan los equipos existentes y ah que personas son entregados los mismos al momento se cuenta con una cantidad aproximada de 500 máquinas entre portátiles y de escritorio.

Loja, 05 de Mayo de 2015

.....
Ing. Livia Celi

UNIVERSIDAD NACIONAL DE LOJA
JEFATURA DE INFORMATICA

Universidad Nacional de Loja

En los tesoros de la sabiduría, está la glorificación de la vida.

Entrevista dirigida a la Sección de Redes y Equipos Informáticos de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Estimado/a de la Sección de Redes y Equipos Informáticos:

Con la finalidad de la realización del proyecto de Titulación en la Carrera de Ingeniería en Sistemas, nos permitimos realizar la presente entrevista. Sus opiniones serán importantes para la determinación del tema del Proyecto de Titulación.

Le pedimos contestar las siguientes preguntas:

CÓDIGO	PREGUNTAS
N° 1	**¿Existe vulnerabilidades en la red de datos cableada e inalámbrica?**
	Comentarios: Existen diversas vulnerabilidades en cuanto a la red, una de las principales es la infección de equipo, se dan también ataques de DNS, inyecciones de DHCP, muchas personas ajenas a la universidad puede hacer uso de la red inalámbrica ya que la misma se halla libre, realizando así ataques a la página web de la universidad, para finalizar no existe un control de las instalaciones que se hace en los equipos de trabajo. **Sugerencias:** La principal sugerencia es la actualización de la licencia del Firewall, y un método de autenticación para usuarios de la red.
N° 2	**¿Existen mecanismos para la autenticación y gestión de usuarios dentro de la red de datos?**
	Comentarios: No existe un mecanismo para la autenticación y gestión de usuarios dentro de la red LAN y WLAN, lo único que se conoce son las paginas a las cuales se conectan los usuarios. Por lo general las conexiones se hacen a la red social

	Facebook y YouTube. **Sugerencias:** Es necesario un mecanismo de autenticación sobre todo en la red WLAN debido a que el campus de la UNL no se halla en un solo lugar, por ejemplo hay instalaciones en Motupe, Idiomas, Salud y el teatro Bolívar, es necesario también un control de FILTER URL, el firewall existente permite realizar esto, pero el mismo no se halla actualizado. Se necesita control de programas que se instalan en los computadores ya que gracias a ello se obtiene demasiados equipos infectados.
N° 3	**¿Existe un mecanismo que facilite el flujo de trabajo de los usuarios de la red de datos?**
	Comentarios: Ah manera de mecanismos se puede decir que la red se halla segmentada, además existen VLAN´S con grupos de usuarios para la no existencia de congestión, gracias a ellos se puede designar un cierto ancho de banda, determinar privilegios o procesos. **Sugerencias:** Control de acceso a los usuarios de la red, control URL, además de control de software que se instala en los computadores de cada usuario.

Loja, 16 de Abril de 2015

UNIVERSIDAD NACIONAL DE LOJA
JEFATURA DE INFORMÁTICA

Alfonsina Bustamante

Ing. Nohelia Alfonsina Bustamante

Universidad Nacional de Loja

Entrevista dirigida a la Sección de Redes y Equipos Informáticos de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Estimado/a de la Sección de Redes y Equipos Informáticos:

Con la finalidad de obtener conocimiento acerca del estado actual de la Red de Datos tanto Cableada como Inalámbrica, nos permitimos realizar la presente entrevista. Sus opiniones serán importantes para el exitoso desarrollo de nuestro Proyecto de Titulación.

Le pedimos contestar las siguientes preguntas:

CÓDIGO	PREGUNTAS
N°1	**¿Especifique brevemente como se encuentra estructurada la red de datos LAN y WLAN?**
	Comentarios: La red que cubre el campus universitario es jerárquica se halla estructurada por 3 niveles: Core, Distribución y acceso. Cada facultad y área tiene asignado un switch de distribución y conectados a él, los switches de acceso. En la parte de la red WLAN actualmente se consta de cuatro redes principales que son: CAMPUS UNL, UNL, EDUROAM e INVITADOS UNL.
N°2	**¿Qué equipos tecnológicos dispone actualmente la Institución en cuanto a la red de datos LAN y WLAN?**
	Comentarios: La mayoría de equipos tanto switch como puntos de acceso son pertenecientes a la marca CISCO. Además existe switch DLink y HP que están siendo utilizados.
N°3	**¿Los equipos cuentan con estándares de configuración, es decir configurados de manera segura y con uniformidad?**

	Comentarios: Todos los equipos implementados con configurados de manera uniforme además todo estos cuenta ya con el estándar de seguridad 802.1X.
N°4	**¿Qué servicios de comunicación ofrece, mediante la infraestructura de red a la Institución?**
	Comentarios: Los principales servicios que ofrece UTI a la comunidad universitaria son de datos, voz y video.
N°5	**¿Qué porcentaje del campus universitario se halla acogido por el servicio de red LAN y WLAN?**
	Comentarios: En la parte de la red LAN se halla cubierta 100% mientras que en la parte inalámbrica o la red WLAN se halla un 80% cubierto, esperando que posteriormente sea cubierto 100%

Loja, 16 de Abril de 2015

UNIVERSIDAD NACIONAL DE LOJA
JEFATURA DE INFORMATICA

Alfonsina Bustamante

Ing. Nohelia Alfonsina Bustamante

ANEXO 5: Fichas de Observación

Universidad Nacional de Loja

En los tesoros de la sabiduría, está la glorificación de la vida.

Ficha de Observación:

Sección de Redes y Equipos Informáticos de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Estimado (a) Encargado (a):

Con la finalidad de la realización del proyecto de Titulación en la Carrera de Ingeniería en Sistemas, nos permitimos realizar la presente observación en cuanto a problemas que se tenga en la Red de Datos que cubre el campus universitario.
El aporte derivado de la siguiente observación es importante para la valoración del desarrollo del proyecto.

Luego de la observación respectiva se ubicará la apreciación que sobre el objeto observado se tenga, utilizando la siguiente escala de valoración.

Totalmente de acuerdo	**Mayoritariamente de acuerdo**	**Parcialmente de acuerdo**	**En desacuerdo**	**No sabe**
Se cumple plenamente	Se cumple aceptablemente	Se cumple insatisfactoriamente	No se cumple	No hay información
4	3	2	1	0

CODIGO	**INDICADOR**	**ESCALA**				
		4	**3**	**2**	**1**	**0**
FO.SREI.01	**Control a las diversas vulnerabilidades que se hallan tanto en la red de datos cableada como inalámbrica.**				X	
	Comentarios: Las principales vulnerabilidades que se pudieron apreciar son: • Infecciones en los equipos. • Ataques de DNS. • Inyecciones DHCP. • Libertad en la red inalámbrica y cableada. • Ataques a la página web de la universidad. **Sugerencias:**					

	De acuerdo a las vulnerabilidades observadas en la red de datos de la universidad se realiza la sugerencia de la actualización de la licencia del Firewall para el control de estas, además se sugiere un método de autenticación para los usuarios de la red.					
FO.SREI.02	**Existen mecanismos para la autenticación y gestión de usuarios dentro de la red de datos.**				X	
	Comentarios: Mediante la observación se pudo apreciar la inexistencia de un mecanismo para la autenticación de usuarios dentro de la red de datos tanto cableada como inalámbrica. **Sugerencias:** Se sugiere realizar la implementación de un mecanismo de autenticación de usuarios sobre todo en la red de datos inalámbrica ya que todo el personal que labora o estudia no se halla en su totalidad en el campus universitarios (Argelia), sino que se halla en diferentes lugares de la ciudad, afectando a la red siendo que cualquier persona puede hacer uso del servicio minimizándolo así para las personas inmersas en la universidad.					
FO.SREI.03	**Existe un mecanismo que facilite el flujo de trabajo de los usuarios de la red de datos.**			X		
	Comentarios: Un mecanismo podría ser que la res de datos se halla segmentada, además hay existencia de VLAN´S, se puede decir que gracias a ello se puede dividir en grupos de usuarios. **Sugerencias:** Para facilitar el flujo de trabajo dentro de la universidad se recomienda control de acceso a los usuarios.					

Fecha, 06 mayo 2015

Universidad Nacional de Loja

En los tesoros de la sabiduría, está la glorificación de la vida.

Ficha de Observación:

Sección de Redes y Equipos Informáticos de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Estimado (a) Encargado (a):

Con la finalidad de la realización del proyecto de Titulación en la Carrera de Ingeniería en Sistemas, nos permitimos realizar la presente observación en cuanto a la infraestructura actual de la Red de Datos que cubre el campus universitario.

El aporte derivado de la siguiente observación es importante para la valoración del desarrollo del proyecto.

Luego de la observación respectiva se ubicará la apreciación que sobre el objeto observado se tenga, utilizando la siguiente escala de valoración.

Totalmente de acuerdo	**Mayoritariamente de acuerdo**	**Parcialmente de acuerdo**	**En desacuerdo**	**No sabe**
Se cumple plenamente	Se cumple aceptablemente	Se cumple insatisfactoriamente	No se cumple	No hay información
4	3	2	1	0

CODIGO	**INDICADOR**	**ESCALA**				
		4	**3**	**2**	**1**	**0**
FO.SREI.01	**La red que cubre el campus universitario es jerárquica se halla estructurada por 3 capas de red Enterprise: Acceso, Distribución y Core. Cada facultad y área tiene asignado un switch de distribución y conectados a él, los switches de acceso, y a estos las estaciones de trabajo o Aps.**	**X**				
	Comentarios: En la parte de la red WLAN actualmente se consta de cuatro redes principales que son: CAMPUS UNL, UNL, EDUROAM e INVITADOS UNL.					
FO.SREI.02	**Los equipos de la red de datos, que permiten el envío y recepción de la información, manejan la tecnología 802.1X, para la autenticación.**		X			
	Comentarios:					

	La mayoría de equipos tanto switch como puntos de acceso son pertenecientes a la marca CISCO, los mismos que manejan dicho protocolo 802.1X. Además existe switch DLink y HP que están siendo utilizados.					
FO.SREI.03	**La red LAN y WLAN acoge a todo el campus universitario, incluyendo sus extensiones administrativas y académicas.**		X			
	Comentarios: La parte de la red LAN se halla cubierta en un 100%, donde se incluye las extensiones académico-administrativas de la UNL, mientras que en la parte inalámbrica o la WLAN se halla un porcentaje de cobertura del 80%, esperando que posteriormente se amplié al 100%					

Fecha, 06 mayo 2015

Ficha de Observación:

Universidad Nacional de Loja

En los tesoros de la sabiduría, está la glorificación de la vida.

Sección de Redes y Equipos Informáticos de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Estimado (a) Encargado (a):

Con la finalidad de la realización del proyecto de Titulación en la Carrera de Ingeniería en Sistemas, nos permitimos realizar la presente observación en cuanto a la situación actual de la estructura de red a nivel de servidores.

El aporte derivado de la siguiente observación es importante para determinar los servicios actuales de la red de datos, la capacidad de almacenamiento y procesamiento de los servidores actuales.

Luego de la observación respectiva se ubicará la apreciación que sobre el objeto observado se tenga, utilizando la siguiente escala de valoración.

Totalmente de acuerdo	Mayoritariamente de acuerdo	Parcialmente de acuerdo	En desacuerdo	No sabe
Se cumple plenamente	Se cumple aceptablemente	Se cumple insatisfactoriamente	No se cumple	No hay información
4	3	2	1	0

CODIGO	INDICADOR	ESCALA				
		4	3	2	1	0
FO.SREI.01	**Todos los servicios actualmente disponibles en la red de datos, se encuentran alojados en los servidores disponibles.**		X			
	Comentarios: Los principales servicios alojados actualmente en los servidores son: ● Firewall. ● Servidor WEB ● Servidor Moodle (Educacion Virtual a Distancia). ● Servidor para la radio universitaria. ● Servidor DNS. ● Servidor de Correos ● Servidor de Control de Contenido ● Servidor Financiero ● Servidor DHCP.					

FO.SREI.02	**Se encuentra actualmente disponible mecanismos para la gestión y administración de los servidores físicos.**		X			
	Comentarios: Actualmente algunos servicios se encuentran montados en máquinas cpu, pero recientemente se adquirió un servidor blade que pretende centralizar todos los servicios.					
FO.SREI.03	**El espacio disponible dentro del servidor físico es óptimo para la implementación de Windows Server 2012.**		X			
	Comentarios: Actualmente se encuentran disponibles aproximadamente dos cuchillas de 450 GB cada una dentro del servidor blade para la implementación de nuevos servicios para la seguridad de la red de datos.					

Fecha, 06 de Mayo

ANEXO 6: Declaración Confidencial

LENIN SEBASTIAN OCAMPO VELEZ Y HENRY PAÚL VIVANCO ENCALADA, ESTIDIANTES Y TESISTAS DE LA UNIVERSIDAD NACIONAL DE LOJA, DEL ÁREA DE LA ENERGIA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, DE LA CARRERA DE INGENIERIA EN SISTEMAS.

SE DECLARA:

Que en el proyecto de tesis titulado **IMPLEMENTACIÓN DE ACTIVE DIRECTORY APLICANDO EL ESTÁNDAR 802.1X, DENTRO DE LA RED LAN Y WLAN DE LA UNIVERSIDAD NACIONAL DE LOJA,** los datos utilizados en pruebas, configuraciones y experimentaciones tienen fines académicos y no serán divulgados con otros propósitos.

Loja, 17 julio 2015

Atentamente,

Lenin Sebastián Ocampo Vélez
1105668485

Henry Paúl Vivanco Encalada
1105163875

ANEXO 7: Certificación de la Traducción del Resumen

THE CANADIAN HOUSE CENTER

THE CANADIAN HOUSE CENTER

El que suscribe, en representación de **THE CANADIAN HOUSE CENTER CIA. LTDA**, con **RUC Nº 1191723364001,** el cual está aprobado por el **Ministerio de Educación del Ecuador** según resolución Ministerial **Nº 320 - 15.**

CERTIFICA.-

Que el resumen de tesis titulada **"IMPLEMENTACIÓN DE ACTIVE DIRECTORY APLICANDO EL ESTÁNDAR DE SEGURIDAD 802.1X EN LA RED LAN Y WLAN DE LA UNIVERSIDAD NACIONAL DE LOJA"** realizado por LENIN SEBASTIÁN OCAMPO VÉLEZ Y HENRY PAÚL VIVANCO ENCALADA estudiantes de la **CARRERA DE INGENIERIA EN SISTEMAS** de la Universidad Nacional de Loja, ha sido debidamente traducido por el Lic. Ross Sampayo docente coordinador de nuestra prestigiosa entidad especializada en la buena enseñanza del idioma inglés.

Se expide el presente documento, de acuerdo a la Ley, para los fines necesarios.

Loja, 19 de Noviembre de 2015

ROYAL INTERNATIONAL LANGUAGE ACADEMY UK CIA. LTDA. THE CANADIAN HOUSE CENTER

Lic. Ross Sampayo
COORDINADOR GENERAL
THE CANADIAN HOUSE CENTER

ROYAL INTERNATIONAL LANGUAGE ACADEMY UK CIA. LTDA.
RUC: 1191756777001
DIR: VENEZUELA 19-77 Y AV. PIO JARAMILLO ALVARADO / TEL. 2584334

www.thecanadianhousecenter.com
Loja Matriz: Venezuela 19-77 Entre José María Peña y Av. Pío Jaramillo Alvarado • Loja-Ecuador • Teléfonos: 2584334/2584450
Loja Centro: Miguel Riofrío 14-35 Entre Bolívar y Sucre • Loja-Ecuador • Teléfono: 2571800
/CHCU
@CHC

ANEXO 8: Licencia Creative Commons.