Pontificia Universidad Católica del Ecuador

Sede Ibarra

ESCUELA DE INGENIERÍA

INFORME FINAL DEL PROYECTO

TEMA:

SISTEMA DE AUTENTICACIÓN Y POLÍTICAS DE SEGURIDAD MEDIANTE UN SERVIDOR AAA, HACIENDO USO DEL ESTÁNDAR IEEE 802.1X Y LOS PROTOCOLOS RADIUS PARA LA RED INSTITUCIONAL DE LA UNIDAD EDUCATIVA “SAN JUAN DIEGO” EN LA CIUDAD DE IBARRA.

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN TEGNOLOGÍAS DE LA INFORMACIÓN

LÍNEAS DE INVESTIGACIÓN:

INNOVACIÓN Y EMPRENDIMIENTO EN TIC´S

AUTOR/A: CHRISTIAN PAOLO SÁNCHEZ ALMEIDA

ASESOR/A:

IBARRA, ABRIL - 2023

Ibarra, 10 de abril de 2023

Mgs. Darwin Marcelo Pillo Guanoluisa
ASESOR
CERTIFICA:

Haber revisado el presente informe final de investigación, el mismo que se ajusta a las normas vigentes en la Escuela de Ingeniería, de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI); en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f:) 

Mgs. Darwin Marcelo Pillo Guanoluisa

C.C.: 1003319660

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El jurado examinador, aprueba el presente informe de investigación en nombre de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI):

(f):
Mgs. Darwin Marcelo Pillo Guanoluisa
C.C.: 1003319660

(f):
Mgs. Galo Hernán Puetate Huera
C.C.: 040137578-7

(f):
Mgs. Juan Carlos Armas Cárdenas
C.: 100168573-2

ACTA DE CESIÓN DE DERECHOS

Yo **CHRISTIAN PAOLO SÁNCHEZ ALMEIDA**, declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: "Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones, a título gratuito u oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia".

Ibarra, 10 de abril de 2023

f): 

Christian Paolo Sánchez Almeida

C.C.: 171801402-8

AUTORÍA

Yo, **CHRISTIAN PAOLO SÁNCHEZ ALMEIDA,** portador de la cédula de ciudadanía N° **171801402-8**, declaro que la presente investigación es de total responsabilidad del autor, y eximo expresamente a la Pontificia Universidad Católica del Ecuador Sede Ibarra de posibles reclamos o acciones legales.

Christian Paolo Sánchez Almeida

C.C.: 171801402-8

DECLARACIÓN y AUTORIZACIÓN

Yo: **CHRISTIAN PAOLO SÁNCHEZ ALMEIDA**, con CC: 171801402-8, autor del trabajo de grado intitulado: **"Sistema de Autenticación y Políticas de Seguridad mediante un Servidor AAA, haciendo uso del estándar IEEE 802.1x y los protocolos Radius para la Red Institucional de la Unidad Educativa "San Juan Diego" en la Ciudad de Ibarra"**, previo a la obtención del título profesional de Ingeniero en Tecnologías de la Información, en la Escuela de Ingeniería

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador Sede- Ibarra, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador Sede Ibarra a difundir a través de sitio web de la Biblioteca de la PUCESI el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ibarra, 10 de abril de 2023

(f.) 

Christian Paolo Sánchez Almeida

C.C. 171801402-8

CERTIFICACIÓN ANTIPLAGIO

Yo Darwin Marcelo Pillo Guanoluisa, declaro que luego del proceso de revisión en el sistema antiplagio TURNITIN el porcentaje de similitud del trabajo de titulación denominado: "**SISTEMA DE AUTENTICACIÓN Y POLÍTICAS DE SEGURIDAD MEDIANTE UN SERVIDOR AAA, HACIENDO USO DEL ESTÁNDAR IEEE 802.1X Y LOS PROTOCOLOS RADIUS PARA LA RED INSTITUCIONAL DE LA UNIDAD EDUCATIVA "SAN JUAN DIEGO" EN LA CIUDAD DE IBARRA**", es del (9%), de acuerdo al documento (1832492416).

En base a lo anterior, considero que el trabajo de titulación NO ☐ SÍ ☒ cumple los requisitos de originalidad y autenticidad, de acuerdo con los requisitos establecidos por la ley.

Ibarra, 08/04/2023

Darwin Marcelo Pillo Guanoluisa

C.C.: 1003319660

DEDICATORIA

Queridos padres y amigos,

Hoy, al culminar este importante proyecto, me siento agradecido y emocionado de tenerlos a mi lado. Su amor, apoyo y aliento incondicional han sido la fuerza impulsora detrás de mi éxito académico y personal.

A mis queridos padres, gracias por ser mi roca durante todas las dificultades. Gracias por su sacrificio y por enseñarme la importancia del trabajo duro, la dedicación y la perseverancia. Ustedes han sido mi guía y modelo a seguir en cada paso de mi camino.

A mis amigos, gracias por ser mi fuente de alegría y motivación. Sus palabras de aliento, su confianza en mí y su constante apoyo han sido invaluables. Gracias por estar a mi lado en las buenas y en las malas, y por ser una parte integral de mi vida.

Esta tesis es una prueba de mi dedicación y compromiso, pero también es un reflejo del amor y el apoyo que he recibido de mis padres y amigos. Este logro es tanto de ustedes como mío, y por eso les dedico este trabajo con todo mi corazón.

¡Gracias por siempre estar ahí para mí!

Con amor y gratitud,

Christian Paolo Sánchez

AGRADECIMIENTOS

Estimados todos,

Me dirijo a ustedes hoy para expresar mi profunda gratitud y agradecimiento por el apoyo que me han brindado durante mi proyecto de tesis. En este momento, siento que mi corazón está lleno de gratitud por todo lo que han hecho por mí.

En primer lugar, me gustaría expresar mi más sincero agradecimiento a mi tutor. Sin su guía, conocimiento y experiencia, nunca hubiera podido completar este proyecto. Su apoyo y orientación constante han sido invaluables, y estoy profundamente agradecido por ello.

También quisiera agradecer a mis padres por su constante apoyo y amor incondicional. Han estado a mi lado durante todo el proceso, brindándome la fuerza y el coraje para seguir adelante cuando las cosas se ponían difíciles. No puedo expresar con palabras lo agradecido que estoy por todo lo que han hecho por mí.

A mis amigos, les doy las gracias por estar siempre ahí para mí, animándome y apoyándome durante todo el proceso. Han sido mi apoyo emocional y han estado ahí para celebrar cada pequeño éxito y consolarme cuando las cosas no iban bien.

En resumen, no puedo expresar lo suficiente lo agradecido que estoy por su apoyo y amor. No podría haber llegado hasta aquí sin ustedes. Espero poder devolverles todo lo que me han dado en algún momento en el futuro. Gracias de todo corazón.

Atentamente,

Christian Paolo Sánchez Almeida

Tabla de contenido

Índice de tabla de contenidos

Índice Tabla de Ilustraciones

RESUMEN

La Unidad Educativa San Juan Diego es una de las instituciones educativas en la ciudad de Ibarra con una estructura adecuada para impartir educación a sus 500 estudiantes. Sin embargo, su tecnología se ha quedado atrás y se puede observar una red de internet precaria que solo se utiliza para la parte administrativa, sin cumplir los niveles de seguridad que debería tener una institución educativa.

Para solucionar los problemas de la red de internet y la seguridad de la misma, en la Unidad Educativa San Juan Diego, se ha propuesto la implementación de un servidor Radius con la implementación del protocolo IEEE 802.1X para el mejoramiento de la seguridad del acceso a las redes inalámbricas con el fin de mejorar la vulnerabilidad de la misma tomando en cuenta que cumpla con los estándares de seguridad 2865 y 2866.

Este estudio se basó en la implementación del protocolo IEEE 802.1X que controlará los accesos y las autenticaciones de los usuarios de la Unidad Educativa San Juan Diego, tomando en cuenta el servidor programado en CentOS, que es el que se encargara de otorgar o denegar los accesos a los dispositivos que quieran conectarse a la red institucional.

La conexión inalámbrica es una de las principales herramientas que se usa en la Unidad Educativa San Juan Diego, pues tanto los docentes como los alumnos la usan para conectarse a la red, el mecanismo que se usaba es la conexión tradicional, buscar la red e ingresar la contraseña que con el tiempo se ha visto que se ha vuelto obsoleta pues no se sabe quien o quienes acceden a ella, pero con la implementación del protocolo IEEE 802.1X se logró el objetivo basado en un modelo de servicio cliente – servidor, donde todos los elementos tecnológicos cumplen con el estándar del protocolo 802.1X para la homogenización de los diferentes mecanismos de seguridad según la necesidad de la institución la principal herramienta que se usó fue el servidor Radius con apoyo de un servidor LDAP, concluyendo así que el proyecto sirvió como aporte para medir y controlar el acceso a la red.

Para la implementación del proyecto se empleó técnicas e instrumentos de recolección de datos, análisis de fuentes y la observación directa.

Palabras claves: Controlar el acceso, protocolo IEEE 802.1X, servidor Radius, Servidor LDAP.

ABSTRAC

The San Juan Diego Educational Unit is one of the educational institutions in the city of Ibarra with a suitable structure to provide education to its 500 students. However, its technology has fallen behind, and a precarious internet network can be observed that is only used for administrative purposes, without meeting the security levels that an educational institution should have.

To solve the problems with the internet network and its security, the San Juan Diego Educational Unit has proposed to implement of a Radius server with the implementation of the IEEE 802.1X protocol to improve the security of access to wireless networks, in order to improve its vulnerability, taking into account compliance with security standards 2865 and 2866.

This study was based on the implementation of the IEEE 802.1X protocol that will control access and authentication of users of the San Juan Diego Educational Unit, taking into account the server programmed in CentOS, which will be responsible for granting or denying access to devices that want to connect to the institutional network.

Wireless connection is one of the main tools used in the San Juan Diego Educational Unit, as both teachers and students use it to connect to the network. The mechanism that was used is the traditional connection, searching for the network and entering the password that has become obsolete over time since it is not known who accesses it. However, with the implementation of the IEEE 802.1X protocol, the objective was achieved based on a client-server service model, where all technological elements comply with the 802.1X protocol standard for homogenization of different security mechanisms according to the institution's needs. The main tool used was the Radius server with the support of an LDAP server, concluding that the project served as a contribution to measuring and controlling access to the network.

To implement the project, data collection techniques and instruments, source analysis, and direct observation were employed.

Keywords: Access control, IEEE 802.1X protocol, Radius server, LDAP server.

INTRODUCCIÓN

Una de las principales herramientas en la época actual es el internet, pues gracias a esta gran tecnología hoy en día se pueden realizar varias acciones desde cualquier parte del mundo y en cualquier campo, siendo uno de estos la educación, pues hoy en día es uno de los cimientos para desarrollar el aprendizaje tanto como de niños y jóvenes que cruzan la etapa de aprendizaje en un centro educativo.

La ciudad de Ibarra cuenta con una diversidad de centros educativos uno de ellos es la Unidad Educativa San Juan Diego, establecimiento que con los años ha ido creciendo exponencialmente pues hoy en día dicho establecimiento cuenta con 500 estudiantes, con una gran estructura con la que satisface las necesidades básicas para impartir una excelente educación. Sin embargo, en la parte de la tecnología se puede ver a simple vista que en vez de actualizarse como debería ser en estos tiempos, donde la tecnología ha sido parte fundamental, lamentablemente en la institución ha ido retrocediendo, pues se puede observar una precaria red de internet que solo sirve para la parte administrativa y no cumple los niveles de seguridad que debería tener dichas institución.

Después de hacer un estudio del funcionamiento de la red de internet y su respectiva seguridad en la institución se ha podido constatar que a pesar de tener un buen ancho de banda, no se le tiene configurado correctamente, y peor aún, no cuenta con las seguridades correspondientes, pues la institución solo cuenta con el Router que proporciona la compañía y ningún otro dispositivo más, viendo estos antecedentes se puede observar que la Red de internet que en este tiempo es fundamental para el aprendizaje didáctico de los estudiantes no funciona correctamente y peor aún no cuenta con las seguridades que se debería tener en una Institución Educativa.

En la Unidad Educativa San Juan Diego, se comienza a ver la precariedad del internet en tiempos de la pandemia, pues antes el internet solo se lo ocupaba para cosas administrativas

mas no como parte del sistema de aprendizaje, pero con este problema de la pandemia se pudo evidenciar que el internet de la unidad estaba muy mal configurado, pues se quería usar el internet para que los docentes se conectaran a las clases virtuales y a cada rato se colgaba tomando en cuenta que el ancho de banda era normal y que si hubiera tenido una buena distribución se hubiera logrado dar clases sin tantos problemas de conexión.

Ahora que se volvió a presencialidad en la institución y se puede ver una gran falla con respecto al internet, se dejó a un lado las clases virtuales, pero se sigue trabajando con las herramientas tecnológicas del internet y ahí se observa una gran deficiencia con respecto a la red de internet, no pueden trabajar ni los alumnos ni los maestros, no hay una red estructurada y el internet se va a cada rato, porque el internet está abierto y todos se conectan no hay una configuración, no hay seguridad, es decir la red de internet de la unidad es sencillamente es obsoleta.

Es por ello que después de investigar y hablar con las autoridades de la institución se les ha propuesto arreglar la red de internet obsoleta implementando un servidor Radius que se basa en los estándares de seguridad 2865 y 2866 que describen el funcionamiento del servidor.

El servidor Radius va ayudar en ciertos requerimientos que se necesitan para tener una buena red de internet utilizando los protocolos PPP (Point to Point Protocol), para establecer un canal seguro punto a punto, también el protocolo PAP para autenticar los usuarios mediante contraseñas, también usar el protocolo CHAP que sirve para establecer una comunicación segura, todo esto con el fin de que en la institución se pueda usar el internet de una forma segura.

Objetivos

Objetivo General

- Implementar un sistema de autenticación y políticas de seguridad mediante un servidor AAA, haciendo uso del estándar IEEE 802.1x y los protocolos Radius para la red institucional de la unidad educativa “San Juan Diego”

Objetivos Específicos

- Seleccionar el servidor de autentificación más óptimo de acuerdo a los parámetros definidos, para implementar un prototipo que se adecue a cualquier tipo de red wifi.

- Estudiar conceptos relacionados con los Servidores de autentificación en redes Wifi para determinar las alternativas más apropiadas que soporten certificados digitales

- Realizar un escenario de pruebas que nos permita determinar cuantitativamente la mejor opción de servidor de autentificación

El presente trabajo está dividido en tres capítulos. En el primer capítulo se describe toda la información teórica o estado del arte para poder tener claro por qué y para qué es necesario la implementación del Servidor Radius AAA con los protocolos de seguridad IEEE 802 1x.

En el segundo capítulo se describe los lineamientos metodológicos con el cual se desarrolló este proyecto.

En el capítulo tres detallan todos los resultados, de la implementación del servidor Radius AAA con el protocolo estándar IEEE 802. 1x, con sus diferentes funcionalidades, y por último se presenta las conclusiones, recomendaciones y los respectivos anexos que dan por finalizado este proyecto.

CAPÍTULO I

1. ESTADO DEL ARTE

En esta sección se presentan los estudios que se han hecho acerca del funcionamiento de un sistema Radius AAA, referenciando algunas investigaciones de autores, los cuales ayudarán a entender como es el funcionamiento y porque es necesario implementar estos sistemas en lugares donde existen muchos usuarios y que tienen acceso a la red de internet.

1.1. Antecedentes de Investigación

En una investigación previa (Yurema & Mora , 2016)mencionan en su trabajo de investigación la elaboración de un modelo que permita el control en el acceso de los usuarios a la red a través de las redes Wireless protegiendo al sistema, así como a los diferentes activos de ataques o accesos no validados a través de un dispositivo autenticador evitando así movimientos laterales o verticales de equipos con un mejor control mediante logs de los inicios de sesión realizados por los usuarios.

Yurema y Mora en el 2016 dan a conocer en su trabajo mencionan la importancia de tener una red segura, pues al tener libre acceso de los usuarios a la red sin tener un control de accesos a los usuarios se puede tener robo de información y otros problemas mas de seguridad, es por ello que mencionan en su investigación la importancia de un modelo de control, que permita el acceso a los usuarios y así evitar ataques o accesos no válidos.

Asimismo, (Sánchez, 2022) en su investigación propone usar una red Wireless mediante un caso práctico realizando la autenticación de forma centralizada a través de protocolos basados en el estándar 802.1x demostrando una eficiencia en cuanto a establecimiento de comunicación utilizando uno de los tres métodos de autenticación en redes Wireless más comunes.

La importancia de los protocolos basados en el estándar 802.1x, en el caso de la comunicación entre Wireless, es de mucha importancia sobre todo para mantener un estándar de seguridad garantizado, así lo afirma Sánchez en el 2016 pues luego de realizar su investigación llega a la conclusión que la forma de garantizar y proteger los datos que viajan por la red es usar protocolos de seguridad en este caso en su trabajo implementó el estándar 802.1x.

Mendoza, Zambrano, Sánchez en el 2021, dan a conocer en la revista Sinapsis la importancia del control de acceso a la red, para controlar el acceso a la red a través de conexiones inalámbricas y remotas, se emplea el sistema de seguridad RADIUS, implementado en un servidor FreeRADIUS, el cual, se encarga de autenticar a los usuarios que accedan a la red ya sea a través delos servicios de accesos remotos o de los puntos de acceso Wifi, generando archivos de texto de registros con información detallada de cada uno de ellos. (Mendoza Navarrete , Zambrano Zambrano, & Sánchez Parrales , 2021)

La importancia de los protocolos de seguridad en cualquier institución con acceso a internet es necesaria, es por ello que este proyecto que se va aplicar en una institución educativa, que al contar varios estudiantes se tiene el problema de seguridad de ingreso libre a la red, pues al no tener estandarizado el acceso a la red, todo tipo de usuarios ingresan, es por ello que se referencia el trabajo de Mendoza en el 2016 pues en su investigación menciona que los el acceso a la red debe tener un método certificado como lo es el protocolos estándar 802.1x de esta forma se taparía los posibles infiltrados en la red.

(Indah & Wardana, 2020) Describen en su investigación la importancia de proteger las redes inalámbricas con un servidor de autenticación. Se puede proteger las redes inalámbricas de la dirección MAC suplantación de identidad y también WEP/WPA crack, es decir, mediante el uso de la autenticación FreeRADIUS. además de mejorar seguridad, este servidor también funciona para la gestión del ancho de banda de cada usuario, de modo que el uso de una red la conexión es más óptima y no es mal utilizada por partes irresponsables.

1.2.Conceptos

1.2.1. ¿Qué es un Servidor?

Con la aparición de las redes informáticas en medio tecnológico aparece la necesidad de usar estas redes para intercambiar información entre puntos distantes entre las diferentes personas que estaban conectadas al en la red, junto con este avance tecnológico nace el problema de como se iban a conectar las personas entre si y nace la solución, que es conectar la red a un computador y esto se le llama servidor, y de esta forma nace lo que conocemos como Servidor que básicamente es conectar un computador con la red y de esta forma poner todos sus recursos a todos los integrantes de la red. (Valdivieso , 2015)

1.2.2. Servidor AAA

El servidor AAA tiene como tarea de verificar que los usuarios sean accesibles para poder ingresar en la red, si está registrado en la Red verifica que este esté registrado en la Base de datos (Directorio activo) por lo tanto si el usuario esta validado no impide que las personas accedan a él y dependiendo del nivel de seguridad aprobado en la red, limita quién puede usar y quien no un qué recurso en particular en la red.

AAA significa autenticación, autorización y Contabilidad, que en español se traduce como (autenticación, autorización y) revisión). Lo que hace este servidor es controlar quien puede tener acceso a la red (autenticación), qué pueden hacer mientras están allí (autorización) y registrar las actividades que realizaron al acceder a la red (auditoría) (Fernandez, 2009).

1.2.3. Servidor Radius

En la actualidad debido al crecimiento de redes y al aumento de información disponible en el mundo de internet, la seguridad ha llegado a ser casi ilimitada, dando como resultado su debilitación y poco control. Los usuarios de las redes van ganando cada vez más experiencia y la información de las vulnerabilidades se encuentra con mayor facilidad, provocando así que más personas las conozcan, volviéndose cada vez más inseguras y por lo tanto muy vulnerables a ataques y robos de información o simplemente dejar inhabilitada la red y es ahí que nace la necesidad de tener un protocolo que ayude a proteger la red. Por estas

razones, las empresas consideran una necesidad primordial de proteger las redes de datos ya que sus usuarios, demandan un control de acceso y privacidad a las redes, así mismo hacer frente a las amenazas como al acceso extremo a la red, ataques a la integridad y confidencialidad de los datos. La solución a estas demandas se puede lograr haciendo uso de un servidor AAA, tal como el servidor RADIUS. (Narvaez & Victor M., 2014)

Como indica el enunciado anterior el motivo por el cual se va implementar un sistema Radius AAA, es por tapar esas grietas de seguridad que las personas que están en el entornos van encontrando, pues cada vez las personas tienen más conceptos informáticos y eso conlleva a que cada tienen más conocimientos y es aquí donde nace la curiosidad y pasan el límite de lo legal y buscan vulnerar ciertos protocolos que si no se les tiene bien definidos será muy fácil el robo de la información de la empresa que sea es por ello que se ha busca tener una red segura por medio de este proyecto.

1.2.4. ¿Qué es PPP?

El protocolo punto a punto (PPP) es un protocolo TCP/IP que se emplea para conectar un sistema informático a otro. Las máquinas emplean PPP para comunicarse por la red telefónica o por Internet. (IBM, 2021)

1.2.5. ¿Qué es CHAP?

La autenticación CHAP utiliza la noción de desafío y respuesta, que significa que el par (autenticador) exige al emisor de llamada (autenticado) que demuestre su identidad. El desafío incluye un número aleatorio y un ID único que genera el autenticador. El emisor de llamada debe utilizar el ID, el número aleatorio y sus credenciales de seguridad de CHAP para generar la respuesta adecuada (reconocimiento) para enviar al par. (Oracle, 2014)

Para entender mejor el concepto de un Servidor Radius, hay que tener claro su funcionamiento es por ello que se ha tomado la información de Cisco donde nos va previamente ya instalaron un proyecto con servidor Radius es así como van dando las pautas de cómo es el funcionamiento y cuáles son sus protocolos como se debe implementar para tener un proyecto optimo, ya que con las ideas claras se puede llevar a cabo el proyecto en la Institución donde se va a implementar el servidor Radius

1.2.6. Seguridad de los Usuarios

En la era del internet, aunque tenga instalado en su Computadora Personal (PC) un programa antivirus que es necesario e importante, este no es suficiente. Los nuevos virus van

apareciendo y de manera más agresiva es su accionar, por lo que debe considerar actualizar permanentemente la base de datos de virus de la aplicación, de acuerdo a sus esquemas de navegación en la red o de la cantidad de dispositivos portables provenientes de fuera que conecte a su equipo. De igual manera el contar con un *firewall* (cortafuegos) que limita el tráfico de datos provenientes de la red evitando ciertos problemas; no es suficiente por tanto debe considerarse una estrategia global que incluya la red interna de la organización. (Alexander, 2011)

1.2.7. ¿Qué es la Autenticación?

La autenticación se entiende como el proceso de identificar a los usuarios y garantizar que los mismos sean quienes dicen ser. Esto evita que cualquiera pueda entrar en un determinado sistema o iniciar sesión en alguna plataforma de forma indebida, sin que realmente sea el usuario legítimo que tiene el poder para hacerlo. (Fernández, 2022)

Esta es la forma en que los usuarios podrán entrar a la red siempre y cuando tengan los permisos pertinentes, que serán validados por el servidor es ahí cuando el usuario podrá ingresar a la red.

1.2.8. Autorización

La autorización es lo que define a qué recursos de sistema el usuario autenticado podrá acceder. Que haya logrado pasar la instancia de la autenticación, no significa que podrá utilizar el sistema por completo como super administrador. (Fernández, 2022)

El hecho de que ya un usuario este autenticado no quiere decir que ya puede entrar directamente, pues dependiendo de los permisos que tenga el usuario podrá ser autorizado entrar a cierta parte dependiendo de los permisos que tenga ese usuario.

1.2.9. ¿Qué es el Protocolo IEEE 802.1x?

Una parte importante que va tener este proyecto es la integración del protocolo estándar 802.1x, el cual es una solución de seguridad ratificada por el IEEE en junio de 2001 que puede autenticar (identificar) a un usuario que quiere acceder a la red (ya sea por cable o inalámbrica). Esto se hace a través del uso de un servidor de autenticación. (lopez, 2021)

1.2.10. ¿Cómo funciona el Protocolo IEEE 802.1x?

El funcionamiento del protocolo IEEE 802.1x es de la siguiente manera:

El controlador de acceso, después de recibir la solicitud de conexión del usuario, envía una solicitud de autenticación.

El usuario envía una respuesta al controlador de acceso, quien enruta la respuesta al servidor de autenticación.

El servidor de autenticación envía un *"challenge*" al controlador de acceso, quien lo transmite al usuario. El *challenge* es un método para establecer la identificación. Si el cliente no puede evaluar el *challenge*, el servidor prueba con otro y así sucesivamente.

El usuario responde al *challenge.* Si la identidad del usuario es correcta, el servidor de autenticación envía la aprobación al controlador de acceso, quien le permite al usuario ingresar a la red o a parte de ella, según los derechos otorgados. Si no se pudo verificar la identidad del usuario, el servidor de autenticación envía un mensaje de denegación y el controlador de acceso le deniega al usuario el acceso a la red. (lopez, 2021)

La importancia del protocolo IEEE 802.1x en la implantación como seguridad de una red es necesaria, pues una red segura implica tener una norma estándar de seguridad que autentifique los usuarios que ingresan a la red, al tener esta seguridad el servidor va permitir el acceso seguro a usuarios que solo estén autenticados. El momento que un usuario entra a la red esta parte de la configuración verifica la identidad del usuario, si es que el usuario no es verificado, se envía un mensaje de denegación, esta la razón porque en este proyecto se va implementar este protocolo estándar, el cual ayudará a tener control sobre quién entra y quien no a la red, es por esta razón que en este proyecto se va implementar este protocolo de seguridad, que al ser una institución educativa se tiene acceso de muchos usuarios y para tener una red segura se implementará un Servidor Radius con el protocolo de seguridad IEEE 802.1x, de esta manera se mantendrá una red segura libre de accesos de usuarios desconocidos.

1.2.11. Seguridad de la red

La ciberseguridad o la (Seguridad en la Red) ayuda a que usuarios maliciosos reemplacen información, puedan leer información o puedan modificar información dirigida a destinatarios específicos, también está parte se encarga de permitir o no el acceso a servicios remotos no autorizados (Morgan , 2019)

En la Unidad Educativa donde se va implementar este sistema la seguridad en la red va ser una parte importante, pues al tener muchos usuarios que ingresan a la red, y no se sabe quien o quienes son usuarios de la institución y quienes son usuarios maliciosos es por este motivo que se busca controlar el acceso de que usuarios son los que deben ingresar y quien no.

1.2.12. Protocolos AAA

Los protocolos AAA son los más utilizados por los administradores de TIC para controlar el acceso de los usuarios en la red, sea a través de una red cableada o de forma inalámbrica este el protocolo se denomina RADIUS + TACACS y su protocolo sucesor es el TACACS+ TACACS y RADIUS son protocolos que se usan para tener un control seguro de acceso a la red, pero cada de estos protocolos tiene diferentes habilidades y funciones, el uso de uno estos protocolos dependerá mucho de la necesidad de la empresa en la que se le va implementar. (Red Seguridad, 2021)

1.2.13. Protocolo RADIUS

RADIUS significa (Remote Authentication Dial-In User Server). Es un protocolo AAA abierto con aplicaciones para el acceso a las redes y movilidad IP. El funcionamiento de este servidor de autenticación es de la siguiente manera, recibe la petición de acceso del usuario con sus credenciales para acceder a la red, por medio del protocolo PPP (Protocolo Punto a Punto), a través del Network Access Server (NAS), quien redirige la petición al servidor de autenticación que opera con el protocolo RADIUS.

El servidor de autenticación previamente ya programado se encarga de comprobar que las credenciales sean correctas mediante mecanismos diferentes de autenticación como por

ejemplo PAP (Protocolo de Autenticación de *Password*), CHAP (Protocolo de Autenticación por Desafío Mutuo), o EAP (Protocolo de Autenticación Extensible). En caso de ser aceptadas se autoriza al usuario acceder a la red y recibir sus respectivos parámetros, a través del servicio de DNS, tales como una dirección IP (Protocolo de Internet).

El protocolo RADIUS encripta las contraseñas durante la transmisión, incluso con el Protocolo de Autenticación de Contraseñas PAP (*Password* Authentication Protocol), usando una operación bastante compleja que involucra la dispersión a través de *Message Digest* 5 (MD5) y una contraseña compartida. Sin embargo, el resto del paquete se envía en texto plano.

RADIUS utiliza el puerto UDP (User *Datagram* Protocol), 1645 o 1812 para la autenticación y el puerto UDP 1646 o 1813 para los registros de auditoría. Este protocolo combina los servicios de autenticación y autorización en un solo proceso, es decir que cuando el usuario se autentica, también está autorizado. (Bedón, 2012 citado por) (Valdivieso , 2015)

1.2.14. Protocolo TACACS+

Para comprender el protocolo TACACS+ debemos saber que antes de este protocolo hay versiones anteriores como TACACS que fue el primer protocolo AAA y que en la actualidad ya es inutilizado ya que siendo CISCO su creador ya no brinda soporte a este protocolo y se ha vuelto casi nulo. TACACS + es un protocolo estándar desarrollado por el Departamento de Defensa de EE. UU., y luego mejorado por Cisco Systems.

TACACS+ (Terminal Access Controller Acces Control System Plus) es un protocolo que ofrece mejores soluciones de control de acceso además se destaca una mejoría en las funciones AAA.

Entre las principales características de este protocolo es que funciona con el protocolo de transporte TCP, varias ventajas del protocolo de transporte de TACACS+ está orientado a la conexión logrando así cifrar el tráfico entre servidores.

TACACS+ es un protocolo que funciona bajo el modelo de cliente/servidor y para su transporte utiliza el protocolo TCP por el puerto 49 y utiliza encriptación de credenciales y

datos mediante el algoritmo de encriptación MD5 lo que lo hace más seguro y confiable de otros protocolos.

Además, que para tener menos carga en el servidor y una mejor detección de caídas en la comunicación puede ser establecida en una sola sesión de cliente/servidor mientras que el servidor o dispositivo de red se encuentren en forma operacional.

Los RFC que tratan sobre TACACS+ son el RFC 1492 de 1993 "Un protocolo de control de acceso, TACACS", RFC 927 "Opción de Telnet para TACACS" y RFC 2975 de 2000 "Introducción a la gestión de contabilidad o arqueo" (Mazzei, 2014 citado por) (Andrade, 2019)

1.2.15. LDAP

LDAP son las siglas de Protocolo Ligero de Acceso a Directorio, o en inglés *Lightweight Directory Access Protocol*. Se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

Un directorio remoto es un conjunto de objetos que están organizados de forma jerárquica, tales como nombre claves direcciones, etc. Estos objetos estarán disponibles por una serie de cliente conectados mediante una red, normalmente interna o LAN, y proporcionarán las identidades y permisos para esos usuarios que los utilicen.

LDAP está basado en el protocolo X.500 para compartir directorios, y contiene esta información de forma jerarquizada y mediante categorías para proporcionarnos una estructura intuitiva desde el punto de vista de la gestión por parte de los administradores. Es, por así decirlo, una guía telefónica, pero con más atributos y credenciales. En este caso utilizamos el término directorio para referirnos a la organización de estos objetos.

De forma general, estos directorios se utilizan básicamente para contener información virtual de usuarios, para que otros usuarios accedan y dispongan de información acerca de los contactos que están aquí almacenados. Pero es mucho más que esto, ya que es capaz de

comunicarse de forma remota con otros directorios LDAP situados en servidores que pueden estar en el otro lado del mundo para acceder a la información disponible. De esta forma se crea una base de datos de información descentralizada y completamente accesible.

La versión actual se denomina LDAPv3 y se encuentra definida en una hoja de documentación RFC 4511 accesible de forma pública. (Castillo, 2019)

1.2.16. Funcionamiento de LDAP

LDAP es un protocolo basado en la conexión entre cliente y servidor. En el servidor LDAP se almacenarán los datos relativos al directorio, el cual podrá usar una amplia variedad de bases de datos para este almacenamiento, llegando a ser de grandes dimensiones.

El funcionamiento de acceso y administración es muy similar a Active Directory de Windows. Cuando el cliente LDAP se conecta con el servidor, podrá realizar dos acciones básicas, bien consultar y obtener información del directorio, o modificarla.

Si un cliente consulta la información el servidor LDAP puede conectarla directamente si tienen un directorio alojado en él, o bien redirigir la solicitud hasta otro servidor que efectivamente tenga esta información. Este podrá ser local, o remoto.

Si un cliente quiere modificar la información del directorio, el servidor comprobará si el usuario que está accediendo a este directorio tiene permisos de administrador o no. Entonces, la información y gestión de un directorio LDAP se podrá hacer de forma remota.

El puerto de conexión para el protocolo LDAP es el TCP 389, aunque por supuesto, se podrá modificar por el usuario y establecerlo en el que desee si así se lo indica al servidor. (Castillo, 2019)

CAPITULO II

2. MATERIALES Y METODOS

2.1. Descripción del área física de la implementación del sistema Radius AAA en la Unidad Educativa San Juan Diego

La Unidad Educativa san Juan Diego se encuentra ubicada en la ciudad de Ibarra en las calles Secundino Peñafiel 2-80 y Emilio Grijalva, su estructura consta de cuatro edificios en los cuales funcionan las diferentes áreas con las que consta la Unidad Educativa.

2.2. Topología de la Red

2.2.1. Data center

El data center de la Unidad educativa san Juan Diego, esta ubicado en el edificio 1 de la institución, edificio central donde funciona la parte administrativa, aquí se encuentra instalados los equipos principales que componen la infraestructura que controla los accesos de los usuarios que ingresan a la red.

Los equipos que se tiene instalados esta descrito en la siguiente tabla

Tabla 1 Dispositivos con los que cuenta el data center

Ítem	Cantidad	Descripción	Numero de Parte	Fabricante
1	1	Router Huawei		Huawei
2	1	Switch de 4 puertos	TE100-S5/AS	Trendnet
3	1	Router TP-Link		Tp-link
4	1	Computador Asus	X542U	Asus VivoBook

2.2.2. Equipos de comunicación (Accesos de red)

Dentro de cada edificio que conforman la Unidad Educativa San Juan Diego se encuentran ubicados los equipos que conforman el mecanismo de acceso seguro de red, continuación se detallan los equipos instalados en cada uno de los edificios.

2.2.3. Edificio 2 (Básica Elemental y Básica Media)

El edificio dos de la unidad educativa es el lugar donde funciona la básica elemental y la básica media, en el primer piso de dicho edificio se encuentra instalado un Router. La información de dicho equipo se encuentra detallado dentro de la siguiente tabla.

Tabla 2 Características Del Router del edificio 2

Marca	Modelo	**Versión**	**Funciones**	**Estándares Inalámbricos**	**Velocidad Inalámbrica**	**Protocolos de Seguridad**
1	TL-WR941HP	V6	Router Repetidor, Punto de acceso	IEEE 802.11n/b/g	450 Mbps	SPI WPA WPA2 WEP DMZ

2.2.4. Edificio 3 (básica media y la básica elemental)

El edificio tres de la unidad educativa es el lugar donde funciona la básica media y la básica elemental, en el segundo piso de dicho edificio se encuentra instalado un Router.

La información de dicho equipo se encuentra detallado dentro de la siguiente tabla.

Tabla 3 Características Del Router del edificio 3

Marca	Modelo	**Versión**	**Funciones**	**Estándares Inalámbricos**	**Velocidad Inalámbrica**	**Protocolos de Seguridad**
1	TL-WR941HP	V6	Router Repetidor, Punto de acceso	IEEE 802.11n/b/g	450 Mbps	SPI WPA WPA2 WEP DMZ

2.2.5. Edificio 4 (Básica Superior y Bachillerato)

El edificio cuatro de la unidad educativa es el lugar donde funciona la Básica Superior y Bachillerato, en el segundo piso de dicho edificio se encuentra instalado un Router.

La información de dicho equipo se encuentra detallado dentro de la siguiente tabla.

Tabla 4 Características Del Router del edificio 4

Marca	Modelo	**Versión**	**Funciones**	**Estándares Inalámbricos**	**Velocidad Inalámbrica**	**Protocolos de Seguridad**
1	TL-WR941HP	V6	Router Repetidor, Punto de acceso	IEEE 802.11n/b/g	450 Mbps	SPI WPA WPA2 WEP DMZ

2.2.6. Diseño de la LAN

El diseño de la red de la Unidad Educativa San Juan Diego está basado en una topología de red de tipo estrella, los detalles se ilustra en la figura

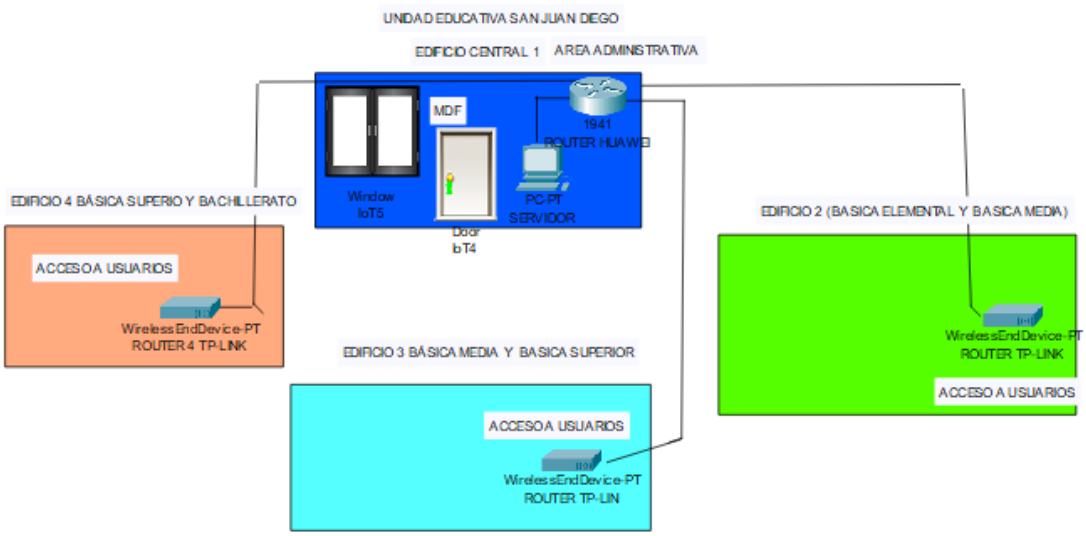


Ilustración 1 Topología de la red de la Unidad Educativa San Juan Diego

2.2.7. Comunicación de los Equipos

Los diferentes equipos de red con los que cuenta la Unidad Educativa se encuentran conectados de la siguiente manera.

Cada edificio tiene un Router TP-Link los cuales están conectados al Switch principal que está ubicado en el edificio principal, tal como se detallo en las tablas anteriores.

La interconexión entre los diferentes equipos se lo realizó por medio de cable UTP Categoría 6, el cableado esta de forma interna del edificio principal hacia los diferentes edificios de la Unidad Educativa de esta manera se encuentra enlazados los diferentes equipos de cada edificio que forma parte de la red de la unidad educativa.

2.2.8. Dispositivos que conforman la WLAN

Los dispositivos que conforman la WLAN son 4 Reuters TP-Link que están distribuidos en los 4 edificios que forman parte de la Unidad Educativa San Juan Diego los cuales brindan el servicio de red inalámbrica, los mismos que están conectados hacia el Switch principal que está ubicado en el edificio principal (Edificio Administrativo).

A continuación, se detallan los Reuters que brindan el servicio de red inalámbrica en la Unidad Educativa San Juan Diego.

- 3 Reuters TP-Link modelo TL-WR941HP

2.3.Topología lógica de la red

2.3.1. Redes

Dentro de la topología de la red de la Unidad Educativa San Juan Diego se contempla conectar tres Reuters TP-Link los mismos que permitirán tener un acceso especifico y distribuido de acuerdo a la necesidad de los usuarios que se conectan a la red donde los Reuters fueron configurados con IP Estáticas.

2.3.2. Mecanismos de acceso seguro a la red

La información que se maneja dentro de la Unidad educativa San Juan Diego va tener dos mecanismos de acceso seguro de red, tanto a nivel local como a nivel de internet.

2.3.3. Acceso seguro a la red local

El dispositivo principal para el funcionamiento con el cual se va manejar el mecanismo seguro de acceso a la red local de la Unidad Educativa san Juan Diego va ser un computador

Asus, en el cual se va instalar VMware, que es una de las herramientas más populares que se utilizan para virtualizar diferentes máquinas virtuales.

El proceso de autenticación, autorización y registro de usuarios debe cumplir el siguiente procedimiento:

1. Un usuario para que pueda tener acceso a la red, previamente debe ser registrado en el directorio activo de la empresa, donde cada usuario tendrá asignado un usuario y una contraseña (de ser necesario se puede cambiar la contraseña si el usuario lo requiere).
2. Cada usuario se conectará de forma inalámbrica a la red de la Unidad Educativa san Juan Diego.
3. Una vez que se conecta los usuarios a través de los diferentes Routers estos enviarán las credenciales hacia el servidor el cual se encargará mediante LDAP, de comparar en su base de datos local si estos datos son correctos y concuerdan con las credenciales del usuario.
4. Si las credenciales son positivas se asignará una dirección IP a través del DNS que se encuentra configurado en el servidor y de esta forma el usuario registrado tendrá el respectivo permiso para ingresar a la red y acceder a los servicios requeridos, en caso de coincidir con las credenciales el usuario automáticamente no podrá acceder a la misma.

2.3.4. Acceso seguro red de conexión a internet

La Unidad Educativa San Juan Diego tiene salida internet por medio de la ISP Xtrem el cual provee internet con un ancho de banda de 50Mbps.

El dispositivo principal para la conexión a internet de la unidad educativa San Juan Diego es un computador portátil, marca (Asus Core 17. 8G, 16 RAM) en el cual esta instalado VMware que sirve para visualizar máquinas, y dentro de la cual esta virtualizado los servidores Radius y LDPA.

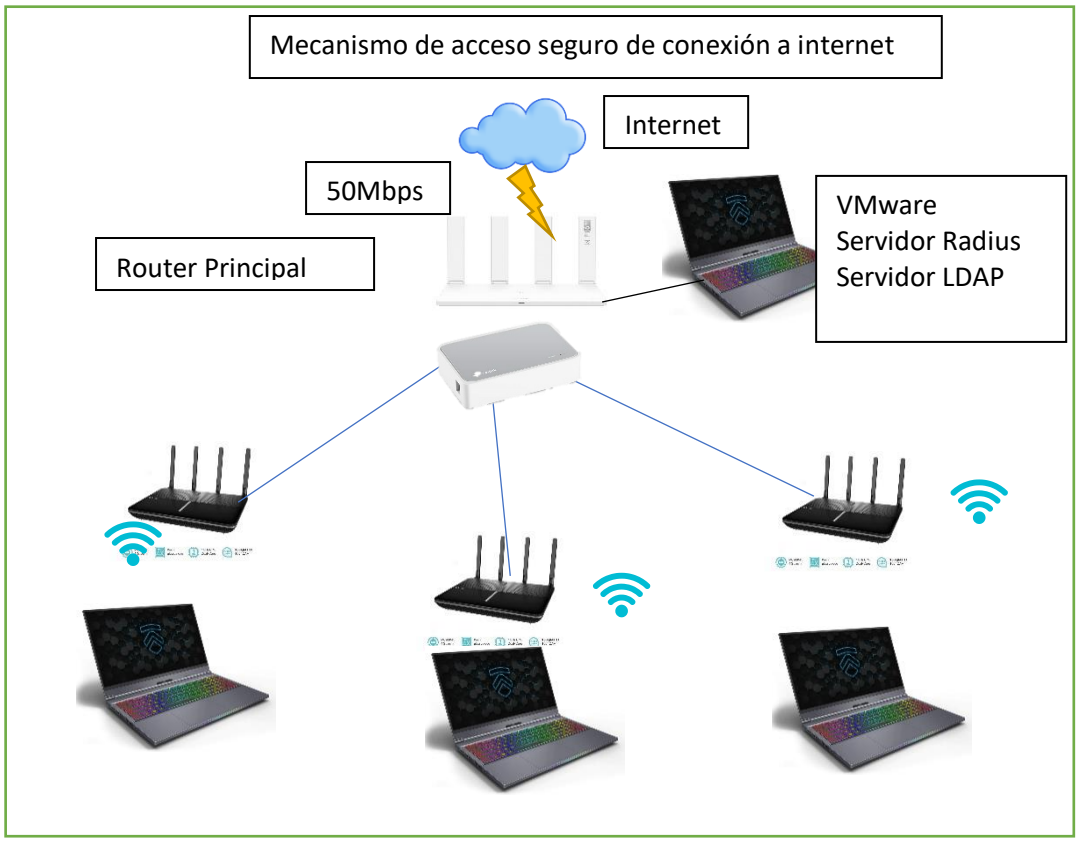


Ilustración 2 Mecanismo de acceso seguro de conexión a internet

2.3.5. Acceso al servidor de autenticación

El administrador de red, previamente debe ingresar los datos del usuario, y este para poder ingresar abrirá la red creada por el administrador, en donde ingresará su usuario y contraseña y si está bien las credenciales podrán tener ingreso a la red de internet.

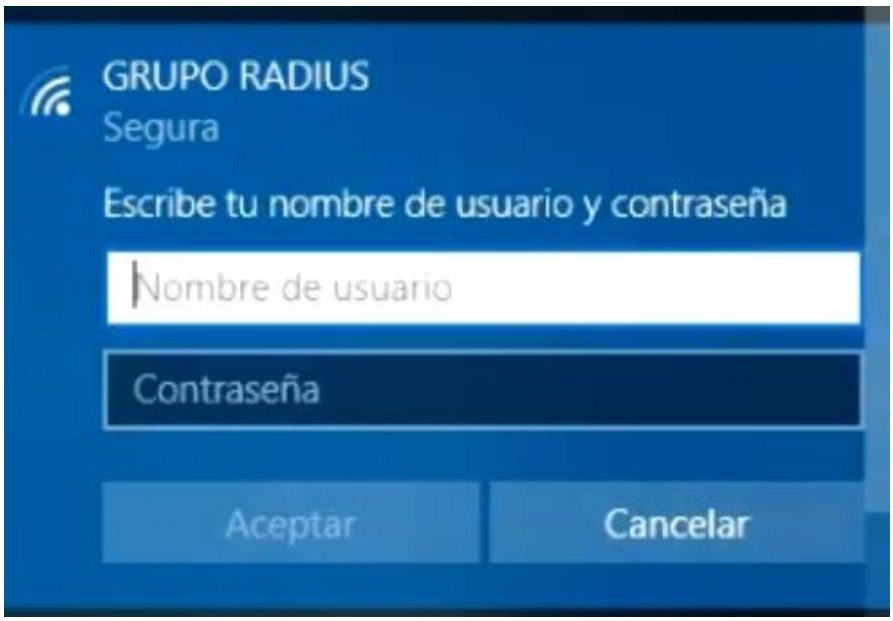


Ilustración 3 Acceso al servicio de autenticación

2.3.6. Usuarios con acceso a servicios web

En la siguiente figura se observa el proceso que debe seguir el usuario para que tenga acceso a la web, el servidor verifica el usuario si esta correcto al momento de ingresar el usuario y la contraseña.

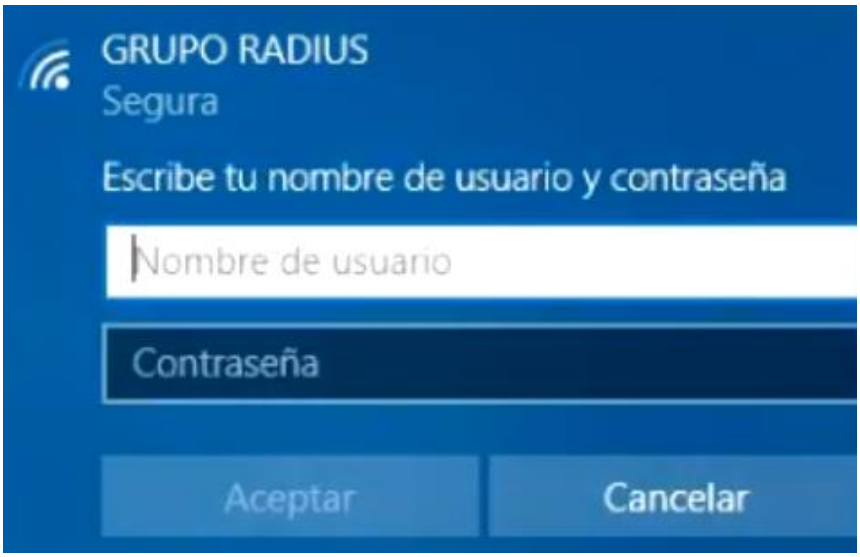


Ilustración 4 validación de usuario y contraseña

Como se observa en la figura anterior se puede ver como el usuario está ingresando sus credenciales y si la validación fue positiva el usuario puede acceder a los servicios web de la red.

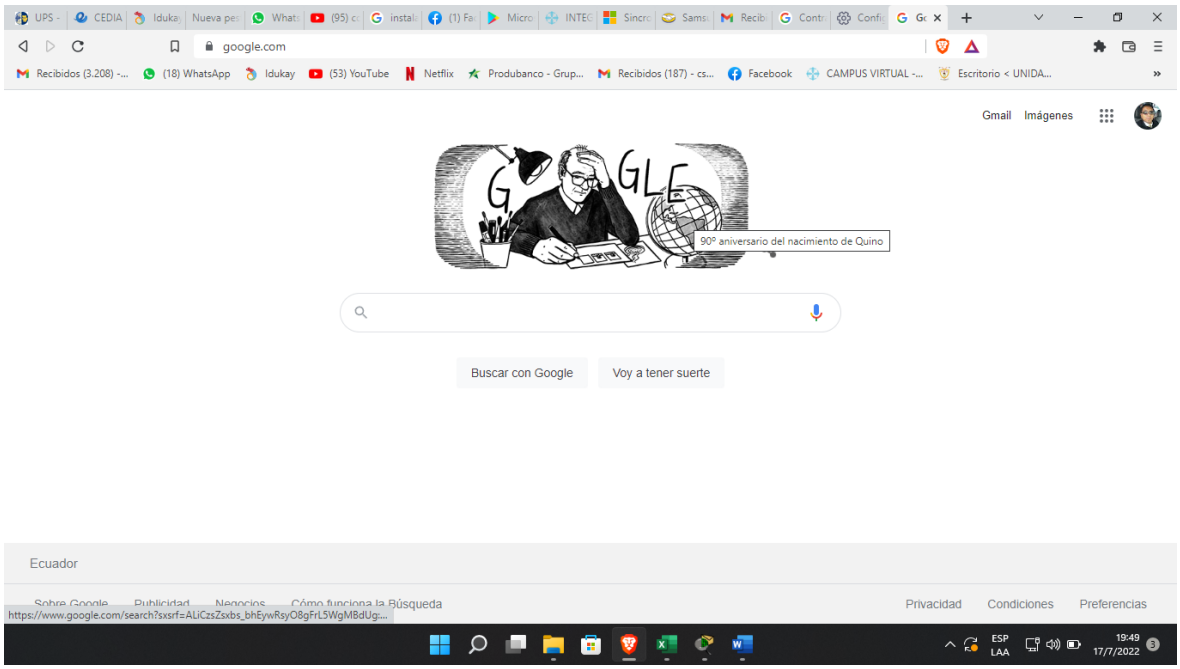


Ilustración 5 Validación de usuario y acceso a Internet

CAPITULO III

3. IMPLEMENTACIÓN

3.1. Implementación del Servidor Virtual CentOS 7

Para la implementación del sistema Radius se lo instalo en una máquina virtual, virtualizada en el programa VMware. El sistema de software libre que se usó es CentOS 7. Para la instalación del Sistema Operativo CentOS 7 se siguió los siguientes pasos:

Se descargó el archivo ISO del Sistema Operativo CentOS 7

Se instaló el programa para virtualizar VMware en la computadora portátil Asus

Se procedió a crear la máquina virtual con el sistema operativo CentOS 7

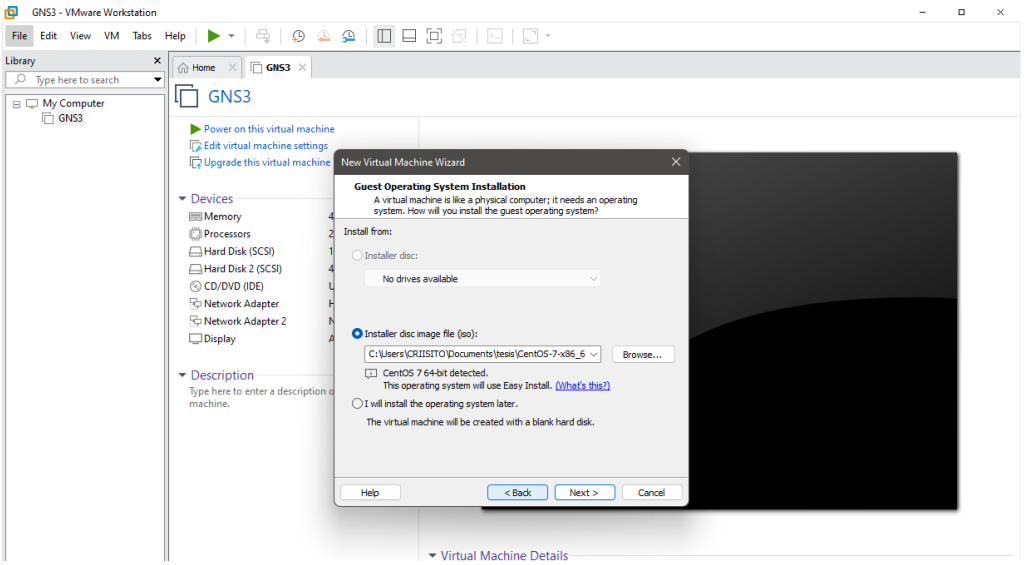


Ilustración 6 Instalación de CentOS 7

La ubicación donde se instaló en la máquina virtual es en el disco D:

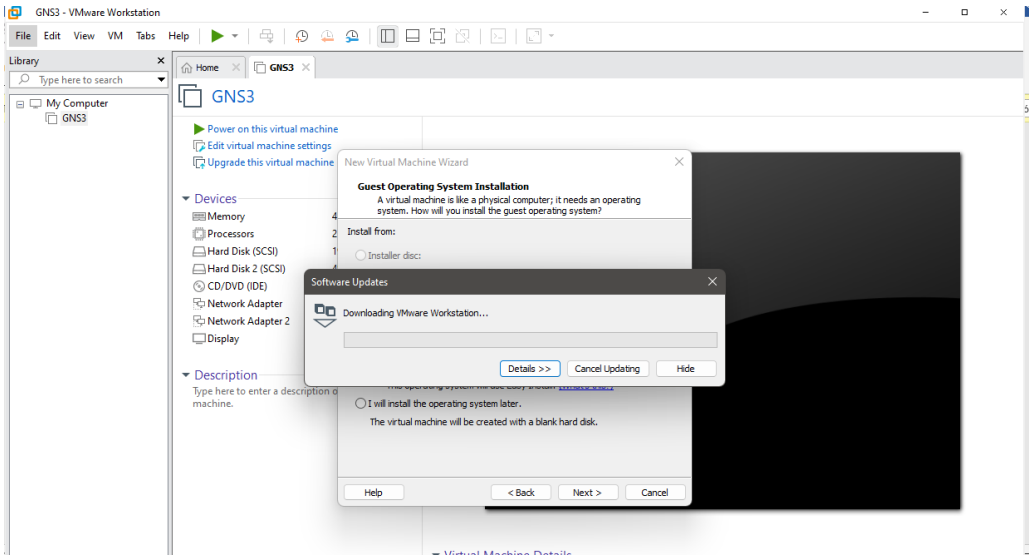


Ilustración 7Configuraciones de Instalación

Para el buen funcionamiento de la máquina virtual creada para CentOS se determinó parte de memoria RAM y procesadores.

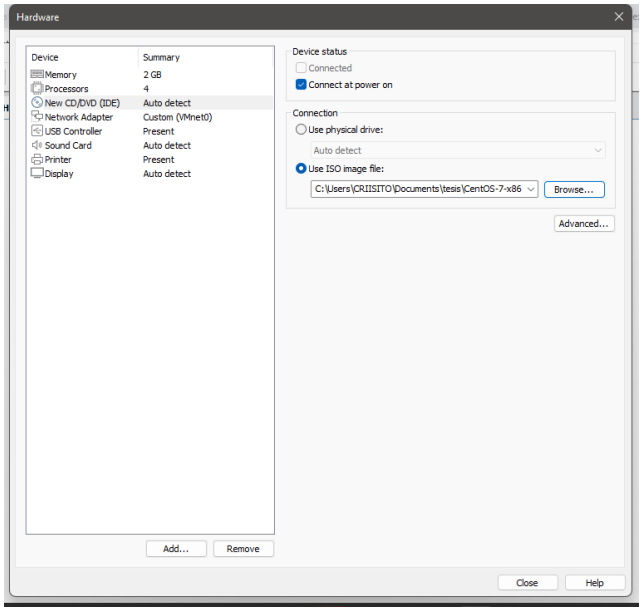


Ilustración 8 Configuración de Recursos

Después de las respectivas configuraciones ya se puede ingresar a la máquina virtual donde se instalo el sistema CentOS 7

Ilustración 9 Configuración Final de CentOS 7

3.2. Instalación de FreeRADIUS

Terminada la instalación del Sistema Operativo CentOS 7, se procedió a instalar FreeRADIUS, para ello se usó los siguientes pasos:

Se abrió un terminal y se puso en modo Root con el siguiente comando:

Su – root

3.2.1. Actualizamos el sistema CentOS/RHEL, con la siguiente línea de comando

sudo yum -y update

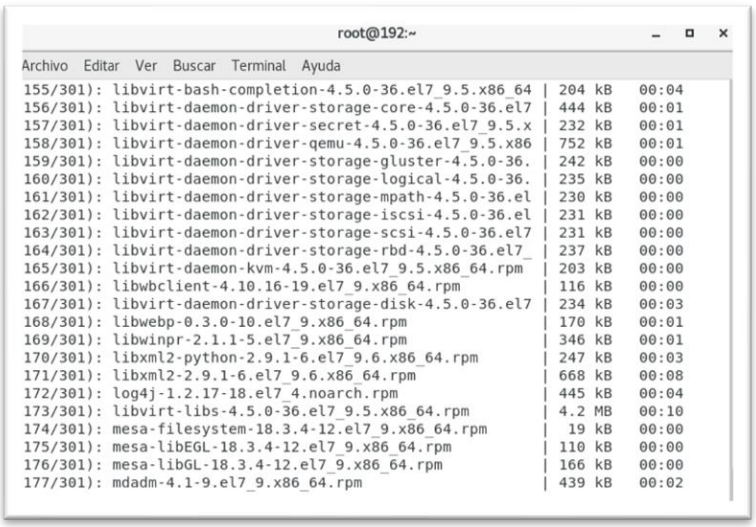


Ilustración 10 Instalación de FreeRADIUS

3.2.2. Reiniciamos el sistema con la siguiente línea de código

sudo reboot

Para poder trabajar sin ningún problema en las diferentes instalaciones se va deshabilitar el SELinux que es el sistema que controla la seguridad y que restringe el acceso a módulos Kernel específicos. Para ello se entro a la siguiente dirección:

sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config

3.2.3. Verificamos que este deshabilitad con la siguiente línea de comando;

/usr/sbin/sestatus -v

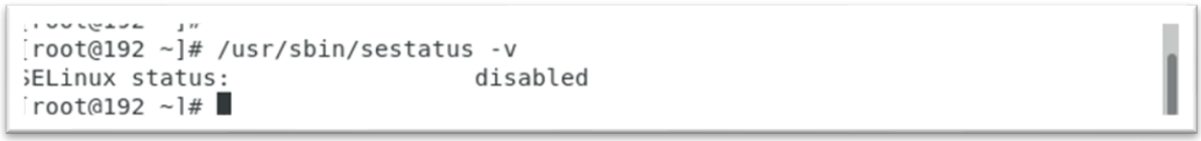


Ilustración 11 Comprobación de SELINUX

Se verifico el estado el firewall y se le cambio a deshabilitado para poder agregar reglas, para verificar el estado se usó la siguiente línea de comando;

firewall-cmd –state

Se apago el firewall y se apago el arranque para iniciar firewall con la siguiente línea de comando;

Systemctl stop firewalld.service

Aquí se abre la siguiente ventana y cambiamos el estado de SELinux a deshabilitado.

3.3.Instalación de FreeRADIUS

3.3.1. Instalación

Para instalar FreeRadius se uso la siguiente línea de comando

sudo yum -y install freeradius freeradius-utils freeradius-mysql

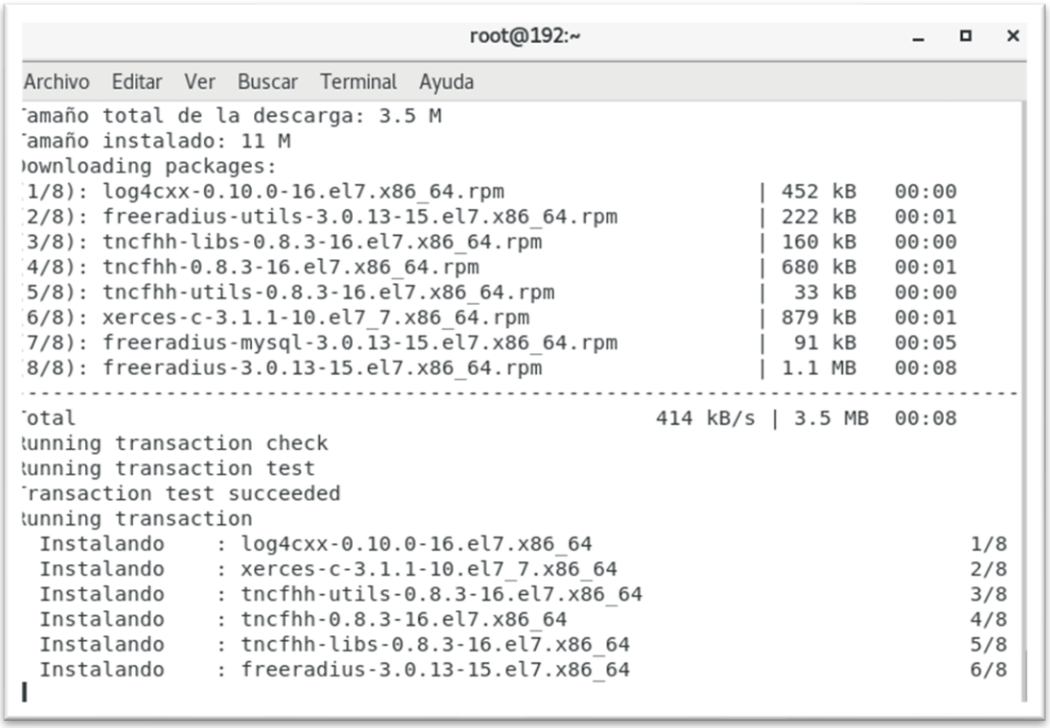


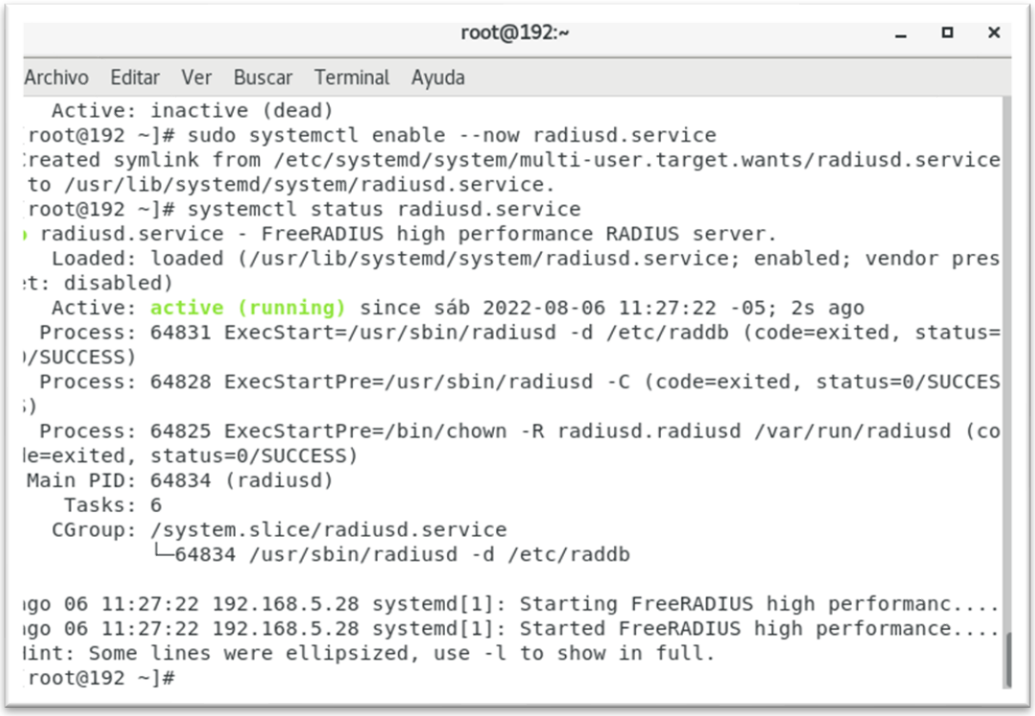
Ilustración 12 Instalación de FreeRADIUS

Se reinició freeradius para que se inicie en el arranque con la siguiente línea de código

sudo systemctl enable --now radiusd.service

Comprobamos el estado con la siguiente línea de código;

systemctl status radiusd.service



Comprobación del servidor si está funcionando con la siguiente línea de código

sudo ss -tunlp | grep radiusd

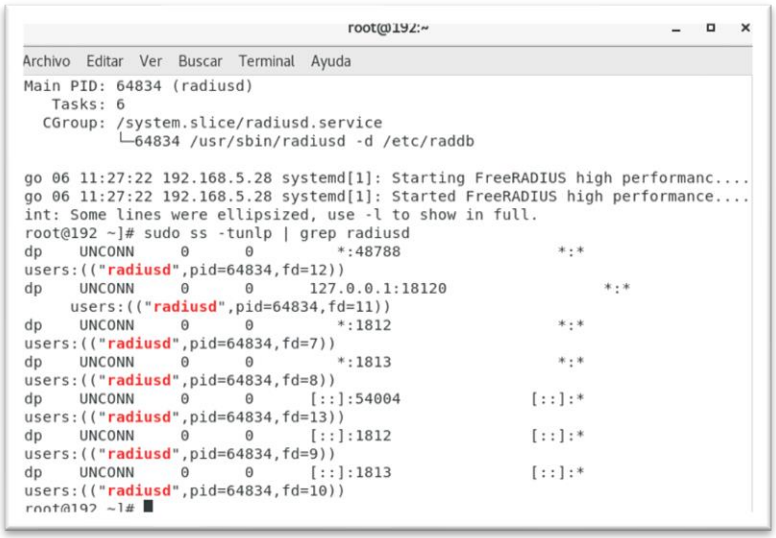


Ilustración 13 FreeRADIUS funcionando

3.4.Instalación y Creación de Usuarios en LDAP

3.4.1. Configuración e instalación de LDAP

Para la creación de los usuarios se descargó LDAP en el Servidor para ellos primero se instaló el servidor LDAP para ello se configuró de esta manera, instalamos las diferentes los diferentes servicios

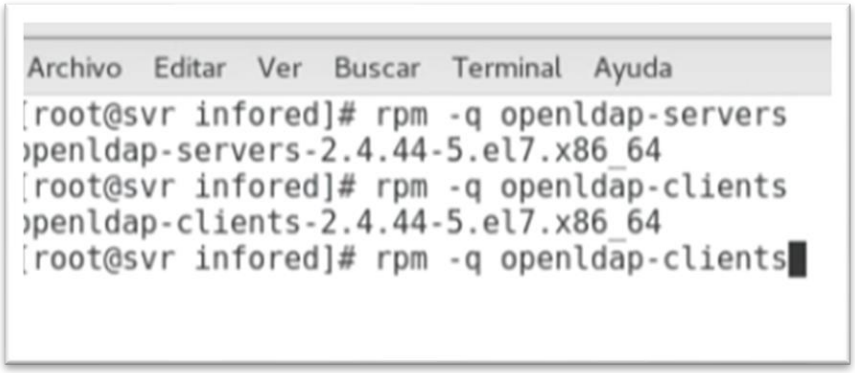


Ilustración 14 servicios Ldap-servers-utils-migration

Durante la instalación del paquete, se pidió que ingrese la contraseña para la entrada de administrador en su directorio LDAP, ahí se estableció una contraseña segura

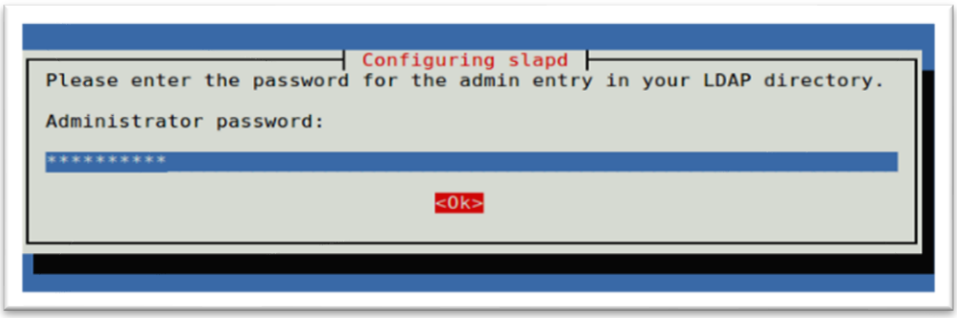


Ilustración 15 Configuración slapd-contraseña segura

1. Se verificó si se habilito y que se inicie automáticamente en el momento del arranque. Para ello se utilizó los siguientes comandos:

   $ sudo systemctl start slapd

   $ sudo systemctl enable slapd

   $ sudo systemctl status slapd

2. Se permitió las solicitudes del servidor LDAP a través del firewall

   # firewall-cmd --add-service=ldap

   $ sudo ufw allow ldap

3.4.2. Configuración del servidor LDAP

3. Se creo un usuario administrativo en OpenLDAP y se asignó una contraseña para ese usuario. En el siguiente comando, se creó un valor hash para la contraseña dada, este se usará en el archivo de configuración LDAP.

   $ slappasswd.

4. Luego creó un archivo LDIF que se usó para agregar una entrada al directorio LDAP.

   $ sudo vim ldaprootpasswd.ldif

   Como lo muestra la figura luego ingresamos al siguiente directorio y cambiamos el dominio por el dominio creado

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 d13ca249
dn: olcDatabase={2}hdb
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=my-domain,dc=com
olcRootDN: cn=Manager,dc=my-domain,dc=com
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
structuralObjectClass: olcHdbConfig
entryUUID: 2f3b37b2-40e7-1038-9360-77031092c702
creatorsName: cn=config
createTimestamp: 20180830212704Z
entryCSN: 20180830212704.482976Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20180830212704Z
```

Ilustración 16 Configuraciones

5. A continuación, agreguó la entrada LDAP correspondiente especificando el URI que hace referencia al servidor ldap y al archivo anterior.
   $ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f ldaprootpasswd.ldif

3.4.3. Configurar la base.ldif

6. Se copió los siguientes archivos en el siguiente en directorio base.ldif, donde se agrego el dominio ya creados anteriormente

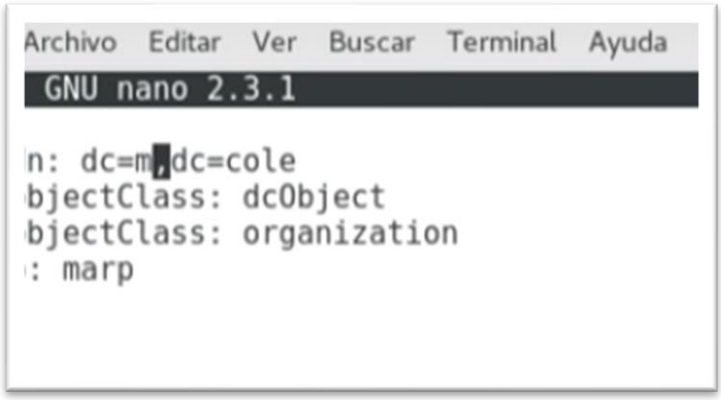


Ilustración 17 Comfiguracion archivo base.ldif

7. Luego copio todos los archivos. ldif al siguiente directorio

```
[root@svr schema]# ldapadd -Y EXTERNAL -H ldapi:/// -f dyngroup.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=dyngroup,cn=schema,cn=config"

[root@svr schema]# ldapadd -Y EXTERNAL -H ldapi:/// -f inetorgperson.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"

[root@svr schema]# ldapadd -Y EXTERNAL -H ldapi:/// -f java.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=java,cn=schema,cn=config"
```

3.5.Configuración de la Organización, Grupos, Usuarios

3.6.Añadir la Unidad Organizativa

Se ingresó al siguiente directorio

cd /home/UESJD/Escritorio/

3.7.Editamos la unidad organizativa creada con el siguiente comando

nano unidadorganizativa.ldif

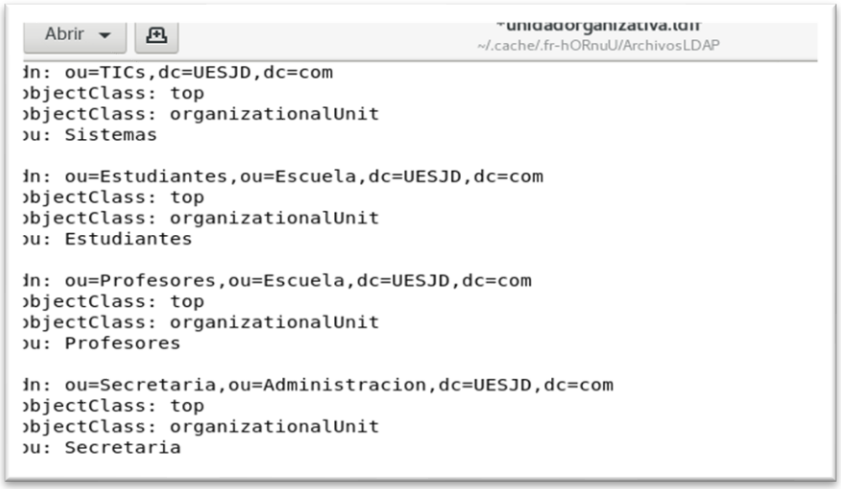


Ilustración 18 Creación de organizaciones

3.8. Siguiente paso se va cargar los grupos e ingresamos al directorio con el siguiente comando

#cp grupo.ldif /root/

cp users.ldif /root/

3.9.Configuración de Grupos

Realizamos el paso como en el anterior procedimiento se las organizaciones

```
# nano grupo.ldif
```

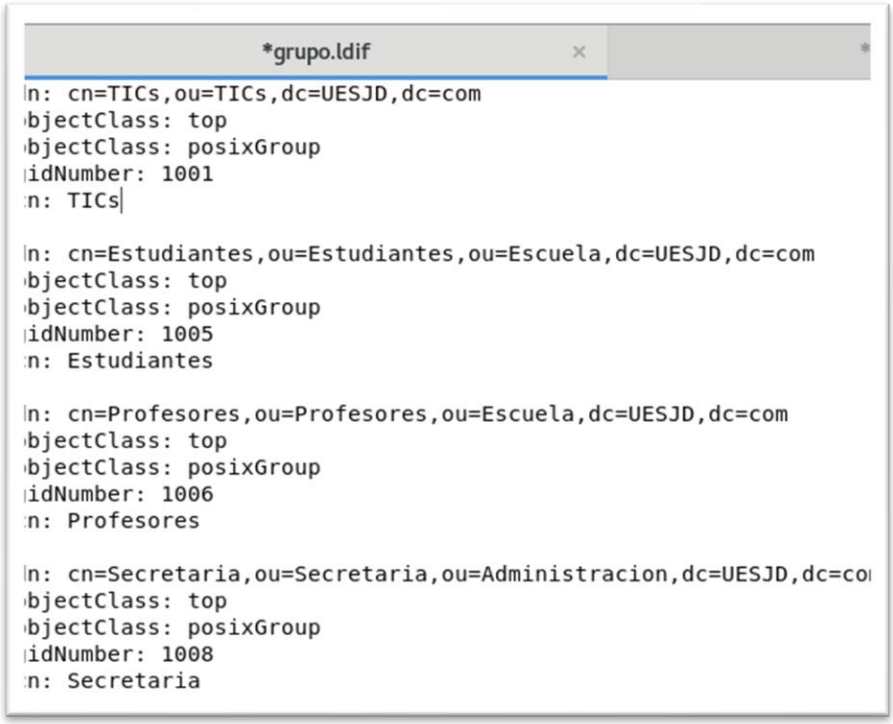


Ilustración 19 Creación de grupos

3.10. Configuración de Usuarios

Cargamos los usuarios con la siguiente línea de código

```
# gedit user.ldif
```

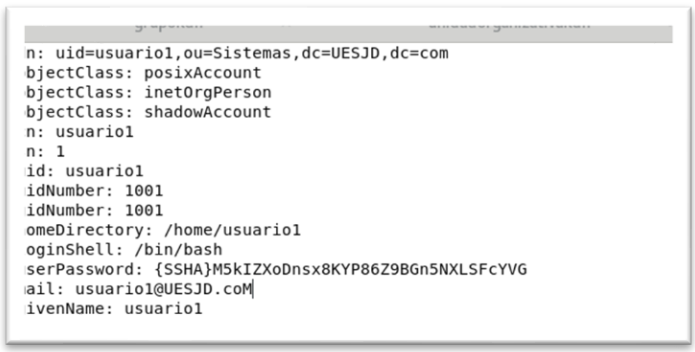


Ilustración 20 Creación de Usuarios

3.11. Instalación de Phpldapadmin

Para instalar phpldapadmin se uso el siguiente comando

sudo apt-get install phpldapadmin

```
================================================================================
 Package              Arquitectura   Versión                 Repositorio  Tamaño
================================================================================
Instalando:
 phpldapadmin         noarch         1.2.5-1.el7             epel         797 k
Instalando para las dependencias:
 php                  x86_64         5.4.16-48.el7           base         1.4 M

Resumen de la transacción
================================================================================
Instalar  1 Paquete (+1 Paquete dependiente)

Tamaño total de la descarga: 2.1 M
Tamaño instalado: 6.8 M
Downloading packages:
(1/2): php-5.4.16-48.el7.x86_64.rpm                          | 1.4 MB   00:00
(2/2): phpldapadmin-1.2.5-1.el7.noarch.rpm                   | 797 kB   00:00
--------------------------------------------------------------------------------
Total                                              2.5 MB/s | 2.1 MB  00:00
Running transaction check
```

Ilustración 21 Instalador de Phpldapadmin

En la figura que se muestra a continuación se observa Se ingreso en la siguiente ruta. Donde se agregó el dominio creado anteriormente

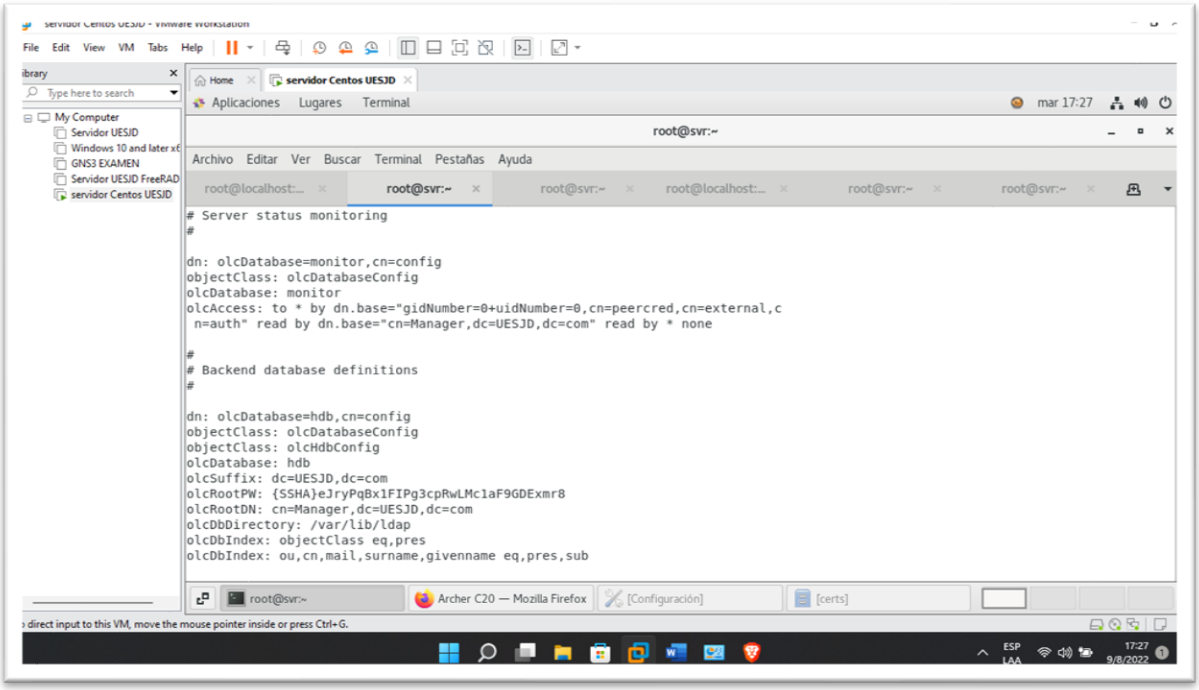


Ilustración 22 Configuración phpldapadmin

3.12. Interfaz de Phpldapadmin

En la siguiente imagen se muestra la la interfaz grafica de phpldapadmin, que ayudará de una forma mas sencilla a ingresar los nuevos usuarios para ello colocamos en la red local la IP del DNS creado y en una ventana del navegador ingresamos la IP del DNS seguido de la palabra phpldapadmin/login y nos ingresa a la siguiente página.

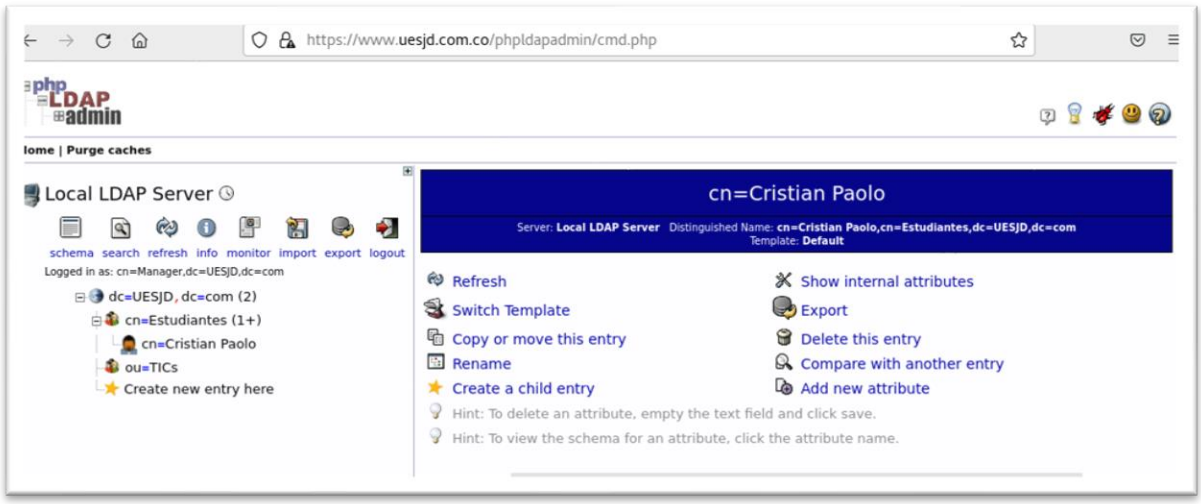


Ilustración 23 Página de ingreso a phpldapadmin

CAPITULO 4

4. PRUEBAS Y RESULTADOS

En este capítulo se va describir las pruebas y las autenticaciones que se realizaron después de la implementación del Servidor Radius, en la Unidad Educativa San Juan Diego.

4.1. Usuarios registrados en el dominio

En la figura 21 se puede ver los usuarios que van a ingresar a la red de la Unidad Educativa San Juan Diego, deben ser previamente registrados en el dominio que se creó para este fin en este caso el dominio creado es UESJD.edu.ec., este proceso está a cargo del departamento de Tics, que son las personas que van a poder añadir o eliminar usuarios y dar los permisos necesarios.

Ilustración 24 Dominio creado para la Unidad Educativa San Juan Diego

En la figura 22 se puede ver la configuración que se le va tomar en cuenta para que puedan autenticarse los usuarios que van a ingresar a la Red de la Unidad Educativa San Juan Diego. Para ello en el Router se ha configurado con WPA/WPA2-Empresarial, de esta manera los usuarios que van a autenticarse en el Servidor Radius debe cumplir los requerimientos de seguridad que en este caso es identificarse y el servidor Radius revisa que este registrado y le permite el ingreso a la red.

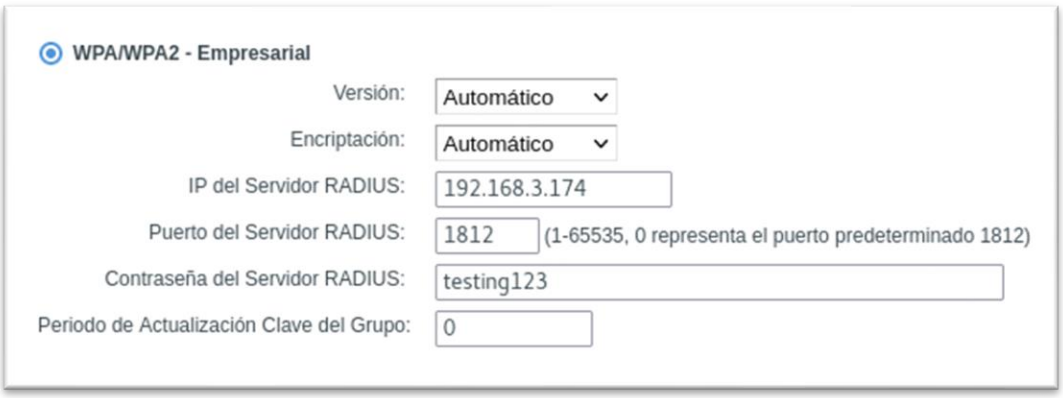


Ilustración 25 Seguridad para poder autenticarse en Radius

4.2 Autenticación Radius

La autenticación Radius se implementó para que los usuarios de la Unidad Educativa San Juan Diego, puedan conectarse desde cualquier dispositivo de una forma segura a la red de la institución, para ello toda la información de los usuarios se está almacenando en servidor Ldap que trabajará como la base de datos local

A continuación, se muestra el proceso que se realizó para el funcionamiento del Servidor Radius, conjuntamente con Ldap.

4.2.1. Protocolo Estándar IEEE 802.1x

El protocolo estándar IEEE 802.1x, es parte esencial para la seguridad en la autenticación de usuarios, y casi todos los equipos actuales, enrutadores, puntos de acceso, Router, etc. tienen ya incluido en sus equipos estos protocolos, es por ello que para cumplir con la todas las seguridades se complementó perfectamente el servidor Radius con el protocolo IEEE 802.1x pues de esta forma la seguridad al momento de la autenticación cumplirá con todos los requerimientos pedidos para tener una buena conexión.

4.2.2. Autenticación de Usuario en la Red LAN

En la figura 23 se muestra como un usuario para conectarse a la red institucional es necesario tener sus credenciales como lo es su usuario y su contraseña, que son previamente entregados al usuario por el departamento de Tics.

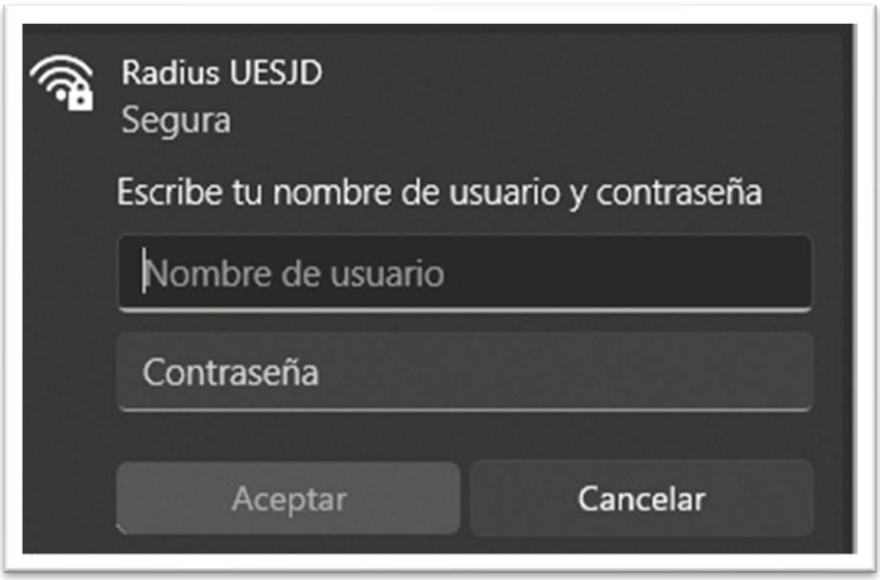


Ilustración 26 Autentificación Usuario y Contraseña

4.2.3. Registro de Usuarios en Phpldapadmin

En la figura 24 se muestra como es el ingreso de los usuarios, al grupo de usuarios que previamente se creó en Ldap. Como se trabajó en el sistema Operativo Centos7, todas las configuraciones se la hacen por medio de comandos.

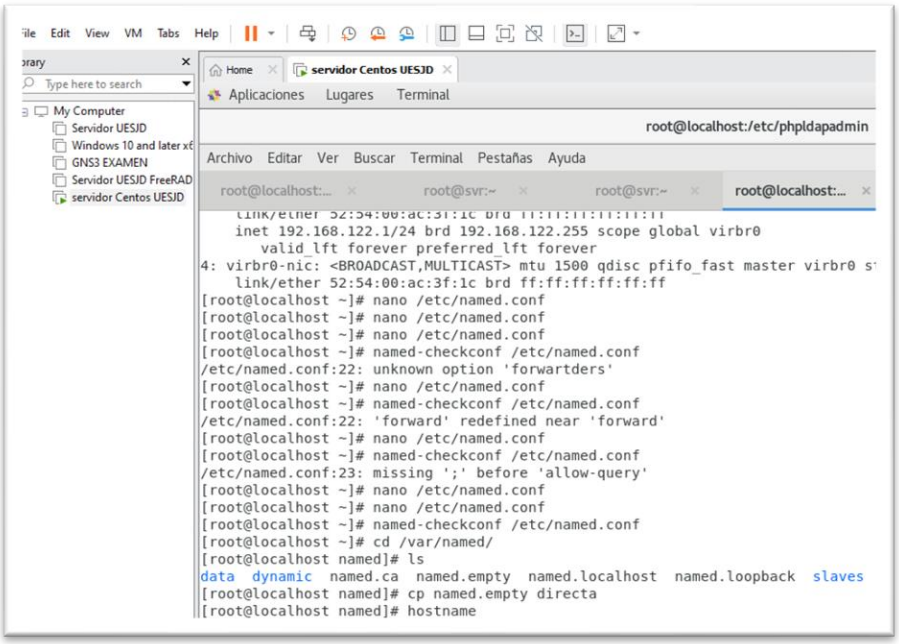


Ilustración 27 Comandos Instalación FreeRADIUS

El proceso para el ingreso de usuarios en centos7 es por medio de comandos, que, si se ingresa mal una línea, va dar error y no va poder configurarse correctamente, es por ello que se instaló Phpldapadmin, como lo indica la figura 25;

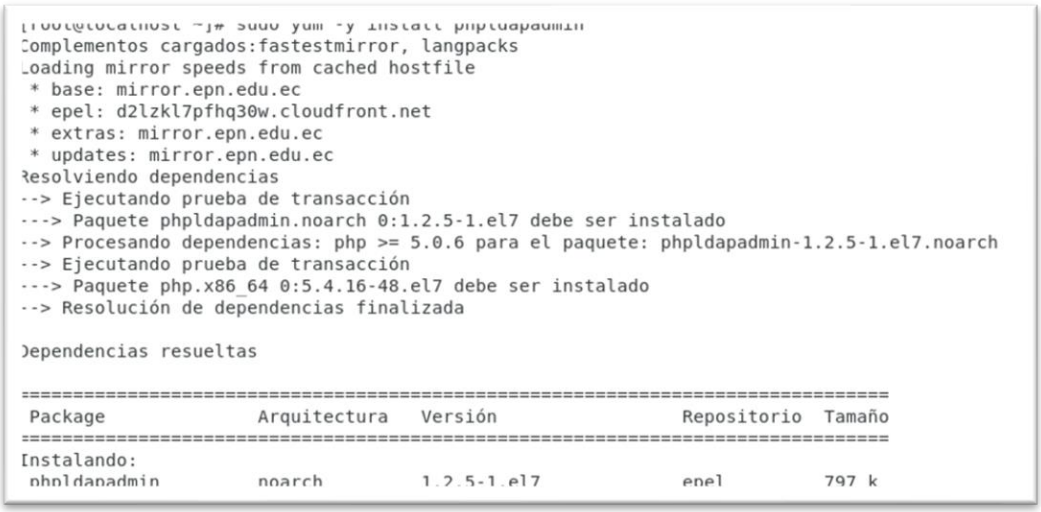


Ilustración 28 Instalación de Phpldapadmin

4.2.4. Ingreso a Phpldapadmin

Ya instalado Phpldapadmin se procedió a configurar y al finalizar la configuración se pudo ingresar al sitio Web de Phpldpadmin, como lo muestra la siguiente figura.

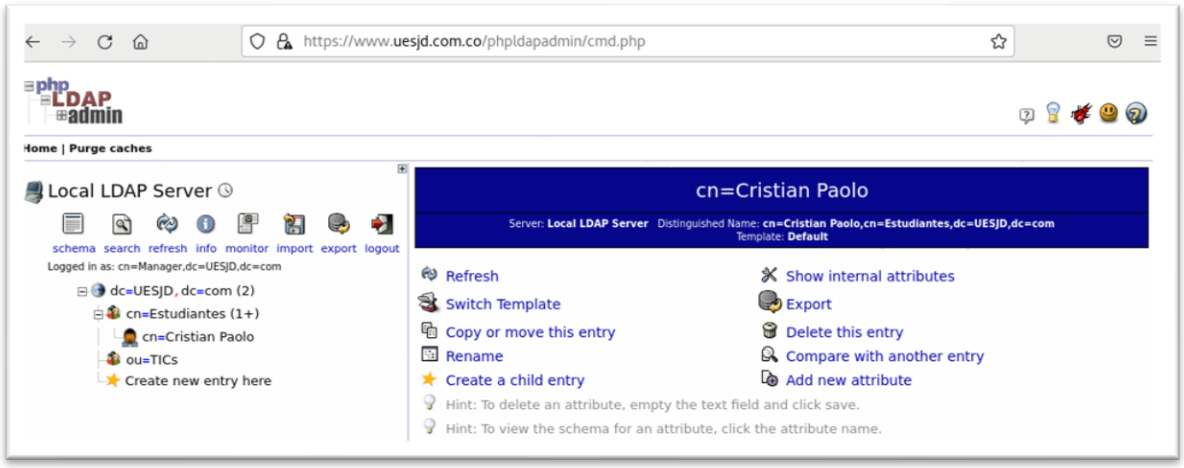


Ilustración 29 Ingreso al Sitio Web Phpldapadmin

4.2.5. Ingreso de usuarios en phpldapadmin.

Ya que se ingresó al sitio web de phpldapadmin, se observa que se tiene una interfaz sencilla pero excelente en recursos para trabajar con los usuarios. Como ya se había creado los diferentes departamentos, se puede agregar usuarios para ello basta ubicarse en el grupo creado y luego en la parte derecha ingresar en la opción créate a *child entry* como se mira en la siguiente imagen.

Ilustración 30 Interfaz de creación de usuarios en phpldapadmin

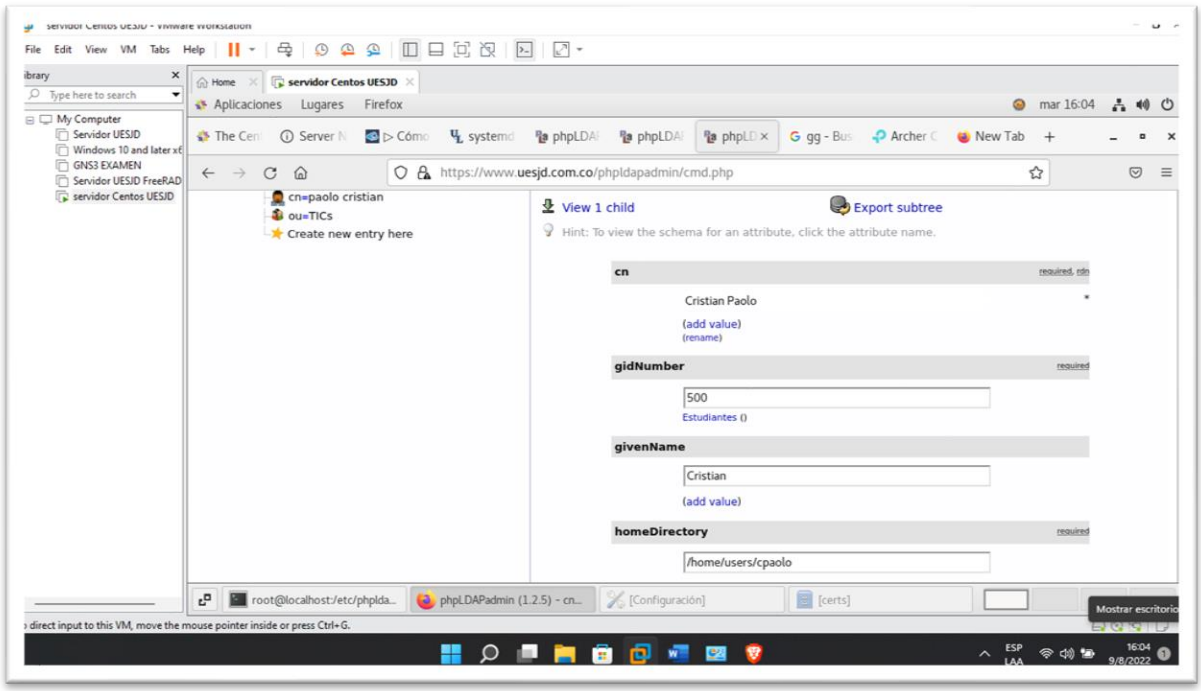


Ilustración 31 Creación de usuario de forma gráfica en phpldapadmin

4.2.6. verificación de usuarios en Ldap

Para verificar si los usuarios ingresados en phpldapadmin se ingresaron correctamente se verifica por medio de consola en centos7, como lo podemos ver en la siguiente imagen, donde se ingresó el usuario Cristian y se puede verificar que esta subida la información correctamente.

```
dn: cn=paolo cristian,dc=UESJD,dc=com
givenName: paolo
sn: cristian
cn: paolo cristian
uid: pcristian
userPassword:: e1NTSEF9ZUQ1K3AyNXYxakswQkhaY1NRVk1qdUt0RGxnRU1BdGM=
uidNumber: 1001
gidNumber: 500
homeDirectory: /home/users/pcristian
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
```

Ilustración 32 Verificación de Usuario en Ldap

4.2.7. Prueba de testeo de Usuario autenticación correcta

Para saber si el usuario esta correctamente validado se puede hacer una prueba de testeo con el comando radtest como se lo muestra en la siguiente imagen, en el cual se nos indica que esta correctamente aceptado por el servidor Radius

```
[root@svr /]# radtest cpaolo cristian 192.168.3.174 1812 testing123
Sent Access-Raquest Id 202 from 0.0.0.0:37390 to 192.168.3.174:1812 lengt 79
        User-Name = "cpaolo"
        User-Password = "cristian"
        NAS-IP-Address = 192.168.3.174
        NAS-Port = 1812
        Mesagge-Authenticator = 0x00
        Cleartext-Password = "cristian"
Received Access-Accept Id 202 from 192.168.3.174:1812 to 0.0.0.0:0 length 20
[root@svr /]#
```

Ilustración 33 Aceptación de usuario correctamente validado por el servidor Radius

4.2.8. Autenticación fallida de ingreso a la red

En la figura 28 en una prueba de testeo se muestra la autentificación fallida que tiene un usuario cuando previamente no está registrado correctamente

```
[root@svr ~]# radtest acarlos 12345 192.168.10.2 1812 testing123
Sent Access-Request Id 176 from 0.0.0.0:35296 to 192.168.10.2:1812 length 77
        User-Name = "acarlos"
        User-Password = "12345"
        NAS-IP-Address = 192.168.10.2
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Cleartext-Password = "12345"
Sent Access-Request Id 176 from 0.0.0.0:35296 to 192.168.10.2:1812 length 77
        User-Name = "acarlos"
        User-Password = "12345"
        NAS-IP-Address = 192.168.10.2
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Cleartext-Password = "12345"
Sent Access-Request Id 176 from 0.0.0.0:35296 to 192.168.10.2:1812 length 77
        User-Name = "acarlos"
        User-Password = "12345"
        NAS-IP-Address = 192.168.10.2
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Cleartext-Password = "12345"
(0) No reply from server for ID 176 socket 3
```

Como se puede verificar aquí no hay una validación de usuario, es decir no está registrado y sin estar registrado al momento de ingresar el usuario y la contraseña no le va dejar ingresar a la red de la Unidad Educativa san Juan Diego, en la red Radius UESJD

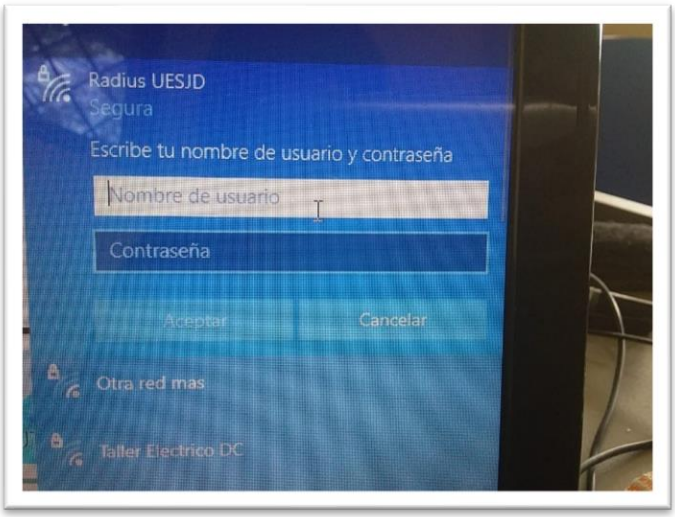


Ilustración 34 No se puede ingresar a la red Institucional

Cuando el usuario no es el correcto salta y regresa a pedir nuevamente el usuario y la contraseña

CONCLUSIONES

El diseño de una solución 4utilizando el servidor de autenticación FreeRADIUS AAA conjuntamente con dispositivos de acceso de red, compatibles con los servicios de autenticación propuestos por el servidor el cual tiene incorporados de fabrica los protocolos RADIUS, IEEE 802IX, facilitó la creación de usuarios, grupos y la asignación de políticas de seguridad para el administrador de red.

Como conclusiones se puede mencionar que para este proyecto se buscó tanto el equipo físico y lo mismo del software, para que funcione el proyecto de la mejor manera, es por ello que con los equipos necesarios y las políticas de seguridad y autenticación se pudo tener éxito en la implementación de este sistema, tomando en cuenta que se usó, software libre y no se gastó cumpliendo así las metas propuestas.

Para integrar todo este sistema, se revisó los diferentes servidores de autenticación y se eligió de entre todos centos7, pues al ser software libre, se adecuo muy bien a los objetivos planteados y se pudo trabajar sin dificultades de licencias y ese tipo de barreras que se tiene al usar software de paga, y de esta forma tanto el servidor como los equipos se fusionaron de manera correcta cumpliendo así con los objetivos.

Para poder constatar la eficacia del sistema, se realizó diferentes pruebas de testeo ingresando usuarios por medio de consola y luego por medio de la interfaz gráfica Phpldapadmin, se usó diferentes dispositivos, como lo es portátiles, celulares, Tablet, para poder realizar las pruebas de autentificación, de esta forma probar que funciona y que no haya problemas después de entregar el sistema en la Unidad Educativa San Juan Diego.

RECOMENDACIONES

Se recomienda no hacer actualizaciones del sistema pues no se sabe si las actualizaciones puedan dañar las configuraciones, es por ello recomendable no hacer actualizaciones sin las debidas precauciones.

Se recomienda tener un encargado que este siempre pendiente del sistema, pues se ha creado los grupos de usuarios, y más adelante se va ingresar más usuarios, es por ellos que se recomienda tener un encargado capacitado previamente que este monitoreando el sistema instalado.

Es recomendable como acción extra para el acceso a red inalámbrica, realizar el procedimiento de filtrado usando las MAC, de esta forma y mejorar la seguridad en el acceso a la red

Referencias

Alexander, H. R. (2011). La Seguridad Informática . *Ciencia UNEMI*, 31.

Andrade, G. (2019). Análisis de prestaciones de los protocolos de autenticación remota Radius y Tacacs+ en infraestructura de comunicaciones corporativas. *(Ingeniero en Electrónica Telecomunicaciones y Redes).* Escuela Superio Politecnica de Chimborazo, Riobamba.

Castillo, J. A. (05 de 01 de 2019). *Profesional Review*. Obtenido de Profesional Review: https://www.profesionalreview.com/2019/01/05/ldap/

Cisco. (19 de 01 de 2006). *Cisco*. Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Fernández, L. (10 de 06 de 2022). *RZ Redes Zone*. Obtenido de https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/

Fernandez, Y. (2009). *AAA / RADIUS / 802.1x, Sist. Basados en la Autenticacion en Windows y Linux/GNU.* España: Alfaomega Ra-Ma.

IBM. (14 de 04 de 2021). *IBM Corporation*. Obtenido de https://www.ibm.com/docs/es/i/7.2?topic=concepts-what-is-ppp

Indah, K., & Wardana, I. (2020). The implementation of radius server for wifi pass using the mechanism of access point controller in Department of Electrical Engineering building, Bali State Polytechnic. *Journal of Physics: Conference Series*, 10.

lopez, C. (17 de 02 de 2021). *CCM*. Obtenido de https://es.ccm.net/contents/785-802-1x-eap

Mendoza Navarrete , M. L., Zambrano Zambrano, T. M., & Sánchez Parrales , L. V. (19 de Junio de 2021). Manejo de servicio de autenticación de usuarios con servidores Radius. *Sinapsis, 1*, 3. Obtenido de https://revistas.itsup.edu.ec/index.php/sinapsis/article/view/549/874

Morgan , K. (2019). *Seguridad de las Redes Informáticas para Principiantes: La Guía de Ciberseguridad para Aprender con un enfoque Top-Down las Acciones Defensivas para Protegerse de los Peligros de la Red.* Independently Published.

Narvaez, L. E., & Victor M., C. (2014). Servidor Radius. *Informate* , 9.

Oracle. (07 de 07 de 2014). *Gestión de redes seriales con UUCP y PPP en Oracle® Solaris 11.2*. Obtenido de

https://docs.oracle.com/cd/E56339_01/html/E53885/pppsvrconfig.reference-21.html

Red Seguridad. (21 de 05 de 2021). *Red Seguridad*. Obtenido de Red Seguridad: https://www.redseguridad.com/actualidad/protocolos-aaa-gestion-eficaz-de-la-red-y-la-ciberseguridad_20210512.html

Roldan, J. M. (2012). *Servidor Radius.* IES. JACARANDÁ.

Sánchez, E. (2022). Analisi de factibilidad del uso de autenticación Radius en Redes Wireles mediante la valiodación de usuario. *(Tesis de Ingeniería).* Universidad de Guayaquil, Guayaquil.

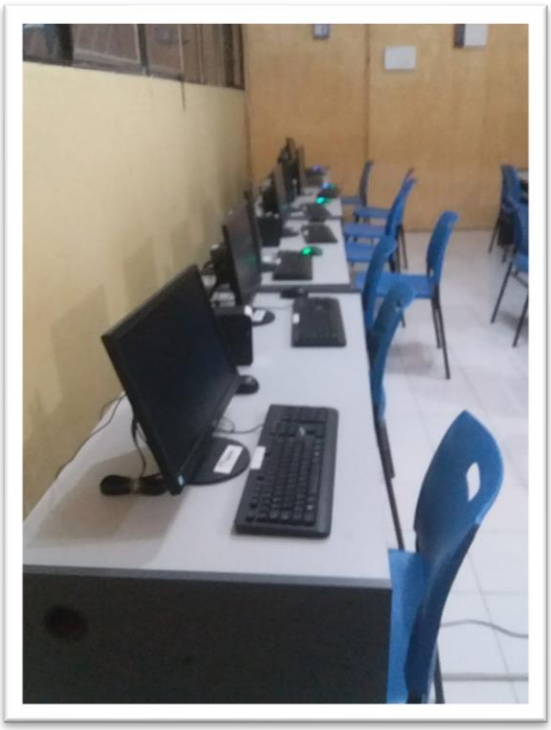
Valdivieso , A. A. (2015). Diseño e implementación de un sistema de autenticación y políticas de seguridad mediante un servidor AAA, haciendo uso del estándar IEEE 802.1x y los protocolos Radius y tacacs+ para la red corporativa de la empresa proyectos integrales del Ecuador PIL S. *(Tesis de Ingenería).* Universidad Técnica Salesiana Sede Quito, Quito.

Yurema, T., & Mora , G. (2016). Implementación de un servidor RADIUS en Windows Server para centralizar la administración de nuevos Access Points en las oficinas remotas de Galpones y Huertos del Gobierno Autónomo Descentralizado del Guayas. *(Tesis de Ingeniería).* Universidad Politécnica Salesiana Sede Guayaquil., Guayaquil.

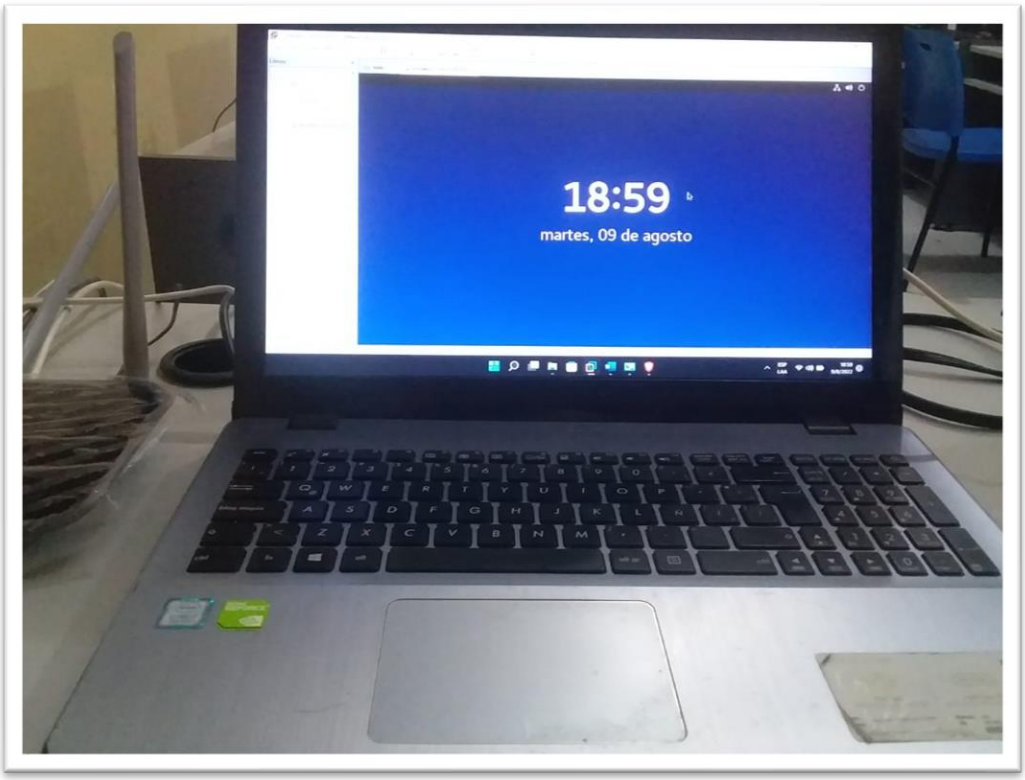
ANEXOS

Unidad Educativa San Juan Diego

Equipos de prueba

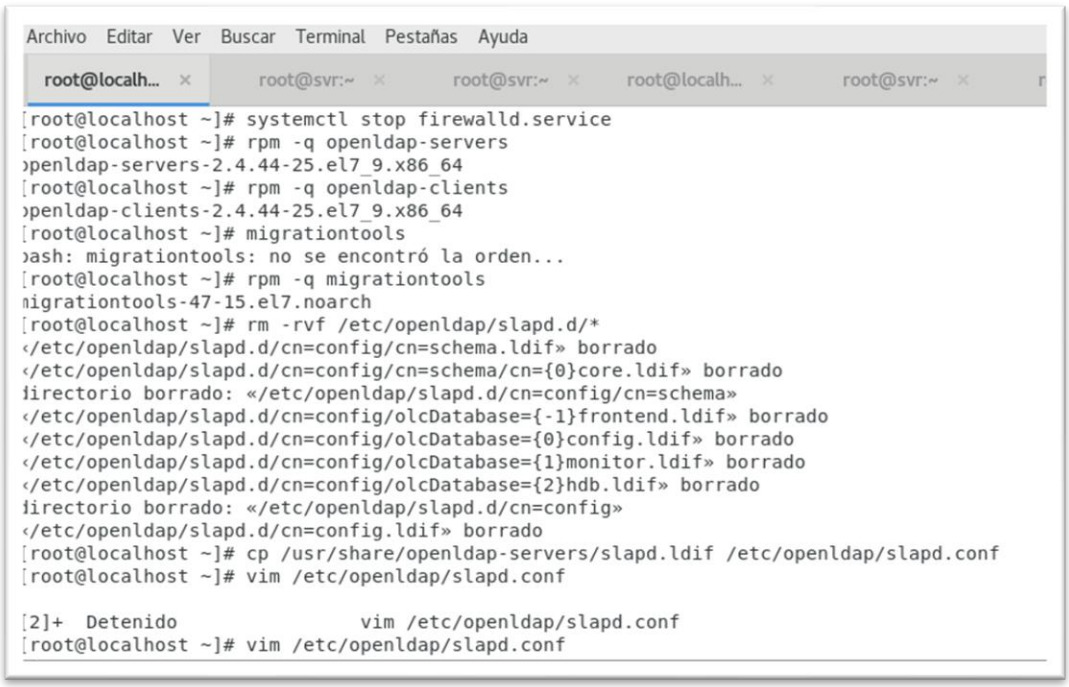


Laptop, (maquina Asus usada como maquina principal donde se virtualizó Centos7

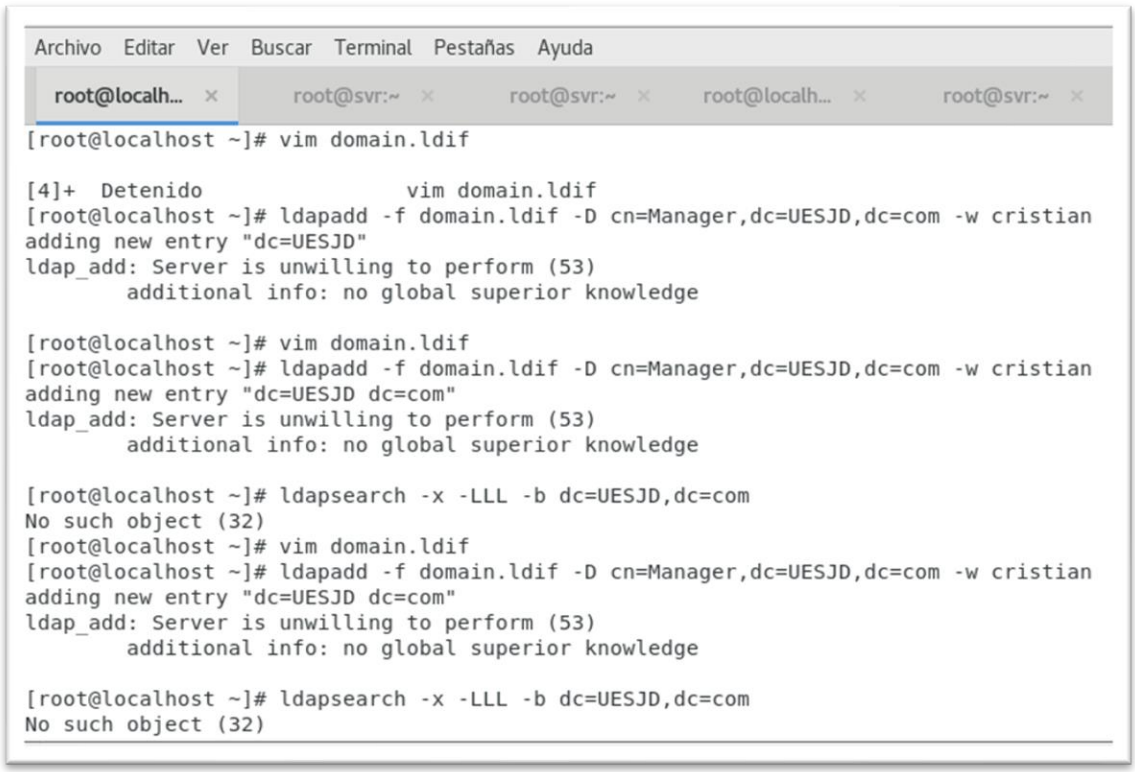


Uno de los Router de Testeo

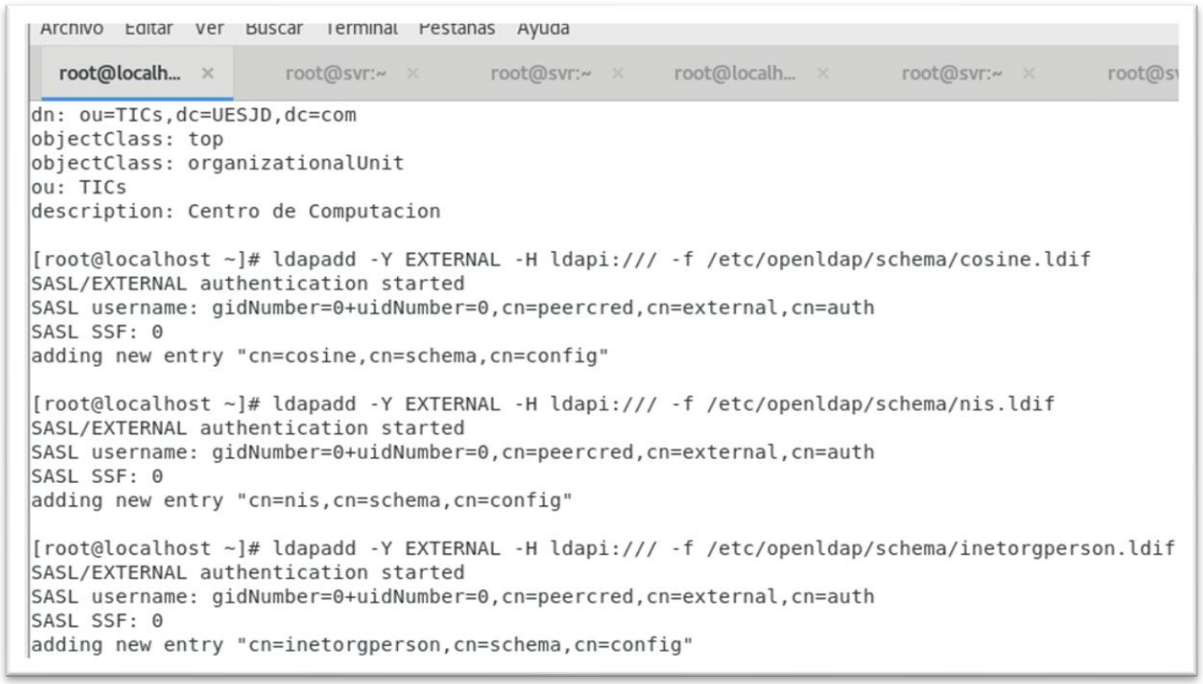
Historial de comando usados en las configuraciones “Instaladores de paquetes” yum install



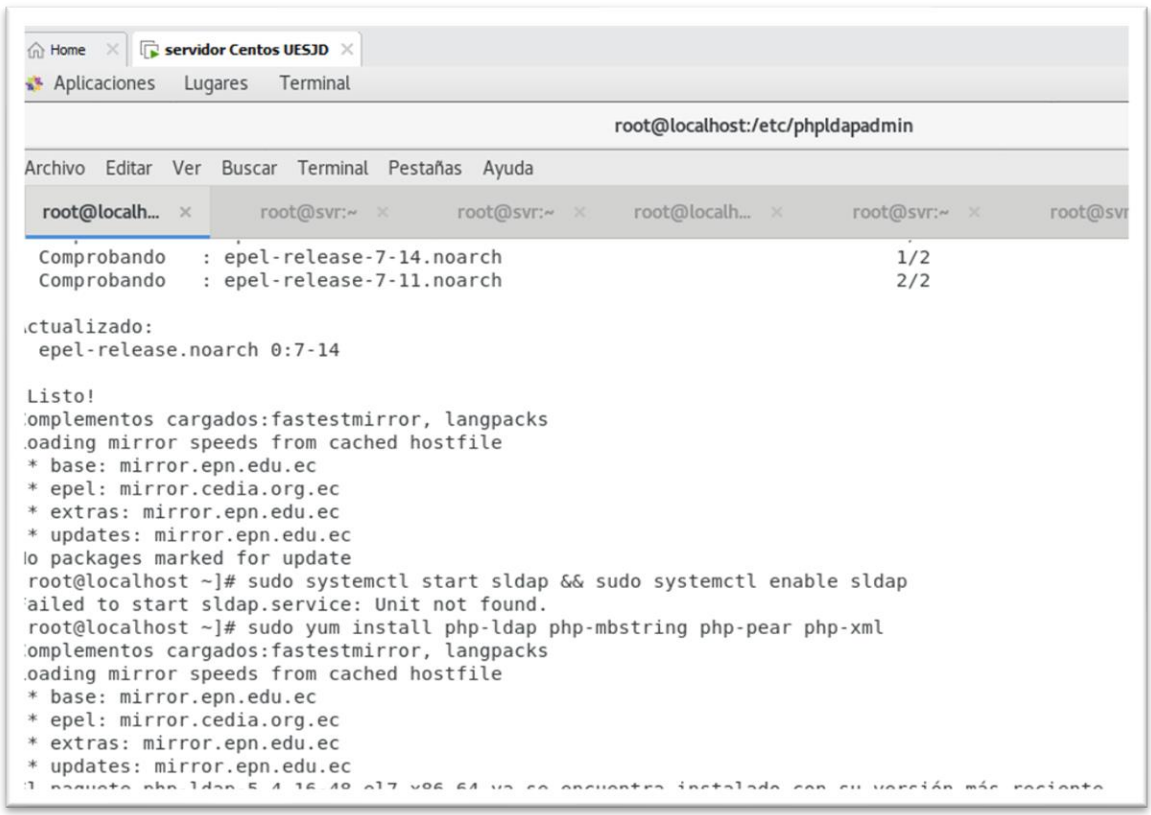
Comando vi para editar archivos



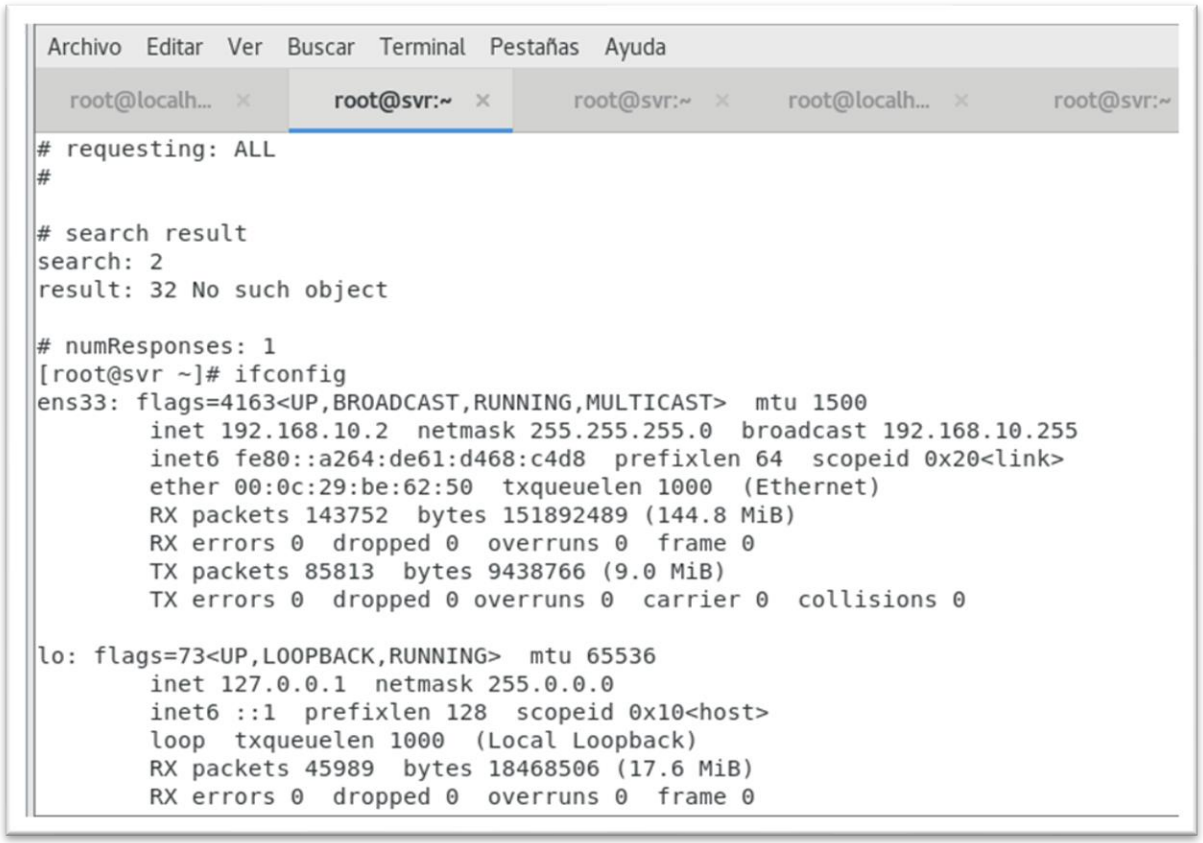
Comando dapadd para agregar archivos



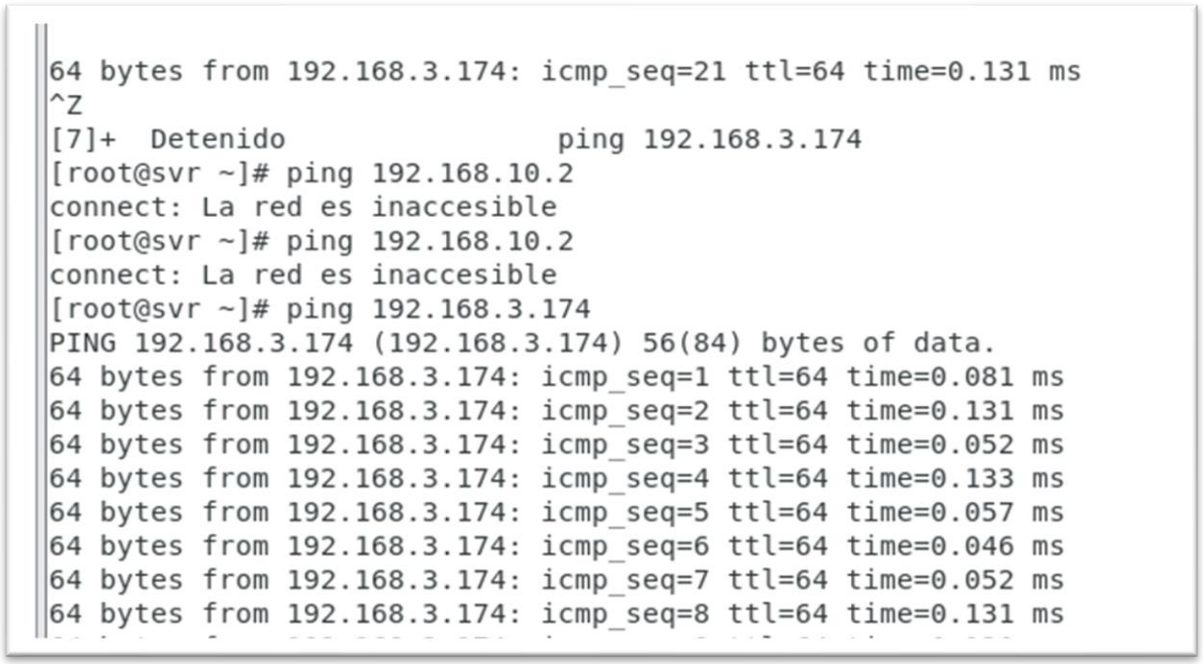
Comando systemctl para iniciar, ver estados de los paquetes



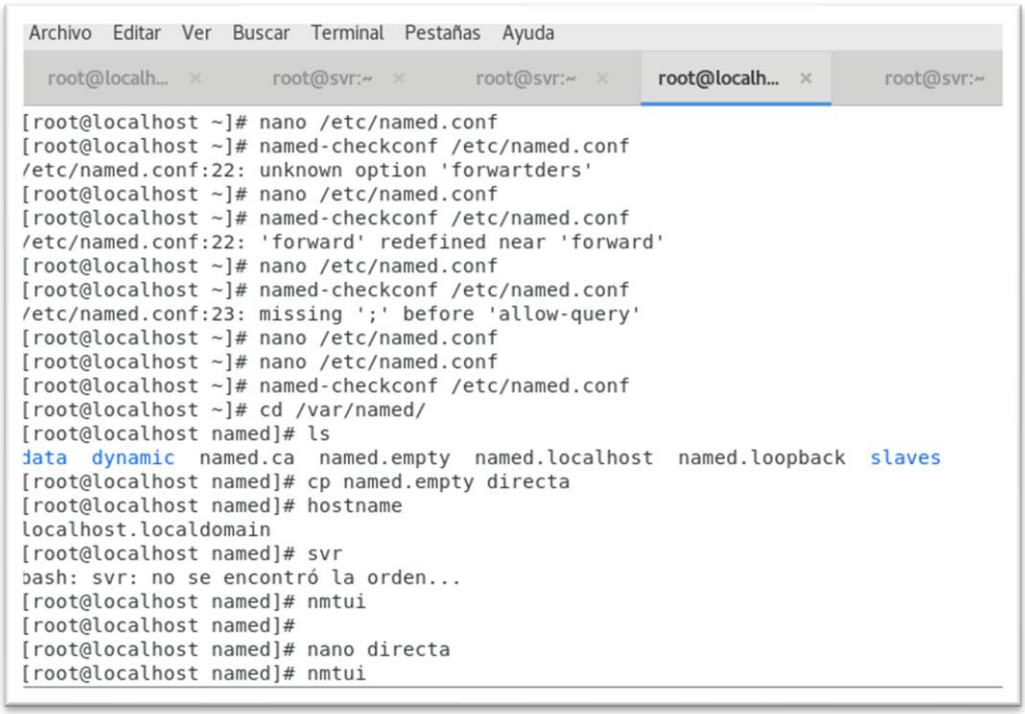
Comando Ifconfig para conocer las IP de las tarjetas de red



Comando Ping para ver si hay conexión entre maquinas



Comando nano para editar archivos



Comando ldapsearch para hacer búsquedas

```
[administrador@svr ~]$ ldapsearch -x -LLL -b dc=UESJD,dc=com
dn: dc=UESJD,dc=com
objectClass: dcObject
objectClass: organization
dc: UESJD
o: UESJD

dn: ou=TICs,dc=UESJD,dc=com
objectClass: top
objectClass: organizationalUnit
ou: TICs
description: Centro de Computacion

dn: cn=Estudiantes,dc=UESJD,dc=com
cn: Estudiantes
gidNumber: 500
objectClass: posixGroup
objectClass: top
```

Certificado Turniting

Turnitin Informe de Originalidad

Procesado el: 09-ago.-2022 22:30 -05
Identificador: 1832492416
Número de palabras: 9437
Entregado: 2

TESIS CHRISTIAN PAOLO SANCHEZ ALMEIDA Por CHRISTIAN PAOLO SANCHEZ ALMEIDA

Índice de similitud	Similitud según fuente	
9%	Internet Sources:	9%
	Publicaciones:	1%
	Trabajos del estudiante:	3%

1% match (Internet desde 09-jul.-2016)
https://www.scribd.com/doc/314071124/19-67-1-PB-pdf

1% match (Internet desde 11-jun.-2022)
https://es.scribd.com/document/577268954/Anthony-Sebastian-Benalcazar-Cabrera

1% match (Internet desde 01-feb.-2022)
https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/

1% match (Internet desde 30-nov.-2020)
http://repositorio.utn.edu.ec/bitstream/123456789/4241/1/05%20%20FECYT%20%202170%20TESIS.pd

1% match (Internet desde 14-may.-2020)
https://id.scribd.com/doc/178659101/033380-tesis-pdf

1% match (Internet desde 20-jul.-2020)
https://docs.oracle.com/cd/E56339_01/html/E53885/pppsvrconfig.reference-21.html

1% match (Internet desde 06-feb.-2022)
https://revistas.itsup.edu.ec/index.php/sinapsis/article/download/549/873

1% match (trabajos de los estudiantes desde 22-oct.-2020)
Submitted to Universidad Técnica de Machala on 2020-10-22

1% match (Internet desde 09-sept.-2018)
http://bibliotecavirtualoducal.uc.cl/vufind/Record/oai:localhost:123456789-1003473

1% match (Internet desde 20-jun.-2019)
http://mendillo.info/gestion/tesis/Mazzei.pdf

< 1% match (Internet desde 08-ene.-2022)
https://www.ibm.com/docs/es/ssw_ibm_i_72/rzaiy/rzaiypdf.pdf

< 1% match (Internet desde 28-jun.-2022)
https://sl.linux-console.net/?p=2372

Pontificia Universidad Católica del Ecuador Sede Ibarra ESCUELA DE INGENIERÍA INFORME FINAL DEL PROYECTO TEMA: SISTEMA DE AUTENTICACIÓN Y POLÍTICAS DE SEGURIDAD MEDIANTE UN SERVIDOR AAA, HACIENDO USO DEL ESTÁNDAR IEEE 802.1X Y LOS PROTOCOLOS RADIUS PARA LA RED INSTITUCIONAL DE LA UNIDAD EDUCATIVA "SAN JUAN DIEGO" EN LA CIUDAD DE IBARRA. PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TEGNOLOGÍAS DE LA INFORMACIÓN LÍNEAS DE INVESTIGACIÓN: INNOVACIÓN Y EMPRENDIMIENTO EN TIC´S AUTOR/A: CHRISTIAN PAOLO SÁNCHEZ ALMEIDA ASESOR/A: IBARRA, ENERO- 2022 Ibarra, 25 de agosto de 2020 Mgs. ASESOR CERTIFICA: Haber revisado el presente informe final de investigación, el mismo que se ajusta a las normas vigentes en la Escuela de Ingeniería, de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI); en consecuencia, autorizo su presentación para los fines legales pertinentes. (f:) ..... Mgs. C.C.: iii PÁGINA DE APROBACIÓN DEL TRIBUNAL El jurado examinador, aprueba el presente informe de

Certificado de Cumplimiento

Unidad Educativa "San Juan Diego"

URBANIZACIÓN YACUCALLE : CALLE PROFESOR SECUNDINO PEÑAFIEL 2-60 Y AV. RICARDO SÁNCHEZ
TELF: 06-2-585-787
IBARRA - ECUADOR

"Hacemos Escuela y Educamos Personas"

Ibarra, 10 de abril del 2023
S.J.D. Nro. 135

El suscrito Rev. P. Rolando Carrión Ortiz,
Rector de la Unidad Educativa "San Juan Diego"

CERTIFICA:

El Sr. **Christian Paolo Sánchez Almeida con Nro. C.I. 1718014028,** estudiante de la escuela de Ingeniería, carrera Tecnologías de la Información, entregó a la Institución el software en perfectas condiciones y hemos comprobado su correcto funcionamiento y su adecuación a nuestras necesidades pedagógicas.

El sistema entregado es un "SISTEMA DE AUTENTICACIÓN Y POLÍTICAS DE SEGURIDAD MEDIANTE UN SERVIDOR AAA, HACIENDO USO DEL ESTÁNDAR IEEE 802.1X Y LOS PROTOCOLOS RADIUS PARA LA RED INSTITUCIONAL DE LA UNIDAD EDUCATIVA "SAN JUAN DIEGO" EN LA CIUDAD DE IBARRA" que consta de un Servidor programado con CentOS que monitorea las personas que ingresan en la red de la institución, y servidor LDAP que es la base de datos donde se guardando todos los procesos y usuarios que ingresan a la red de la Institución.

El software educativo que nos han entregado es una herramienta muy valiosa para el desarrollo de las competencias digitales de nuestro alumnado y para el enriquecimiento de los procesos de enseñanza y aprendizaje. El software cuenta con una interfaz amigable, y de fácil uso tanto para alumnos como docentes.

Queremos felicitarle por el excelente trabajo que han realizado y por el profesionalismo y seriedad que han demostrado en todo momento. Esperamos seguir contando con su colaboración y apoyo en futuros proyectos educativos. Les enviamos un cordial saludo.

Atentamente,

P. Rolando Carrión O.
RECTOR

UNIDAD EDUCATIVA SAN JUAN DIEGO SECRETARÍA IBARRA - ECUADOR

RED EDUCATIVA DIOCESANA

Unidad Educativa "San Juan Diego"
www.unsjd.edu.ec