DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA:

"ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE ADMINISTRACIÓN CENTRALIZADO DE CLAVES BASADO EN LDAP PARA SERVIDORES VIRTUALIZADOS LINUX DE LA COOPERATIVA DE AHORRO Y CRÉDITO "29 DE OCTUBRE "LTDA"

AUTOR: VARGAS PONCE, DANNY OSWALDO

DIRECTOR: ING. RON, MARÍO

SANGOLQUÍ, ENERO - 2016

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÒN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICADO

En mi calidad de Director del Trabajo de titulación: "ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE ADMINISTRACIÓN CENTRALIZADO DE CLAVES BASADO EN LDAP PARA SERVIDORES VIRTUALIZADOS LINUX DE LA COOPERATIVA DE AHORRO Y CRÉDITO "29 DE OCTUBRE" LTDA", elaborado por el Sr. Danny Oswaldo Vargas Ponce, egresado de la Carrera de Ingeniería en Sistemas e Informática, Certifico que fue dirigida observando los aspectos técnicos y reglamentarios de la norma vigente.

Por lo tanto autorizo su presentación ante los organismos pertinentes

Ing. Mario Ron
DIRECTOR DE TESIS

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÒN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Yo, **VARGAS PONCE DANNY OSWALDO**, con cédula de identidad N° 1722548821 declaro que es trabajo de titulación "**ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE ADMINISTRACIÓN CENTRALIZADO DE CLAVES BASADO EN LDAP PARA SERVIDORES VIRTUALIZADOS LINUX DE LA COOPERATIVA DE AHORRO Y CRÉDITO "29 DE OCTUBRE" LTDA"** ha sido desarrollado con base a una investigación exhaustiva respetando los derechos intelectuales de terceros, conforme a las fuentes que se incorpora en la bibliografía. Consecuentemente este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 15 de enero del 2016

VARGAS PONCE DANNY OSWALDO

C.C 1722548821

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÒN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Yo, **VARGAS PONCE DANNY OSWALDO**, Autorizo a la universidad de la fuerzas armadas ESPE publicar en la biblioteca Virtual de la Institución el presente trabajo de titulación "**ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE ADMINISTRACIÓN CENTRALIZADO DE CLAVES BASADO EN LDAP PARA SERVIDORES VIRTUALIZADOS LINUX DE LA COOPERATIVA DE AHORRO Y CRÉDITO "29 DE OCTUBRE" LTDA**", cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 15 de enero del 2016

VARGAS PONCE DANNY OSWALDO

C.C 1722548821

DEDICATORIA

Dedico este proyecto a mis amados y únicos padres Angelito y Mari Carmi, los cuales con su gran esfuerzo, apoyo y sacrificio lograron que alcance junto con ellos el camino a esta gran meta que siempre fue objetivo de toda mi hermosa familia.

Agradezco a Dios porque pese a las noches largas y malos ratos logre llegar a la meta puesta gracias a la fe que mis padres y mi gran hermano nunca perdieron en mí.

A mi querido hermano que con sus consejos y palabras me apoyo en este camino desde un principio, donde también cada paso, cada alegría dada compartía conmigo. Gracias ñaño querido.

Gracias a mi amada familia Vargas Ponce, esto no es solo mío esto es de todos nosotros

Danny Oswaldo Vargas Ponce

AGRADECIMIENTOS

Agradezco a Dios por haberme dado la oportunidad de iniciar y culminar esta meta junto a mi familia en momentos buenos pero por sobre todo los momentos malos estuvieron siempre conmigo dándome apoyo incondicional que siempre tuve y tendré.

A mi Director de Tesis Ing. Mario Ron destacado profesional que con su gran ayuda, paciencia y consejos hicieron posible la realización de este proyecto

A todos mis amigos, profesores, primos que por todo el conocimiento y el gran apoyo brindado en este tiempo de una querida vida universitaria.

Danny Oswaldo Vargas Ponce

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

RESÚMEN

La seguridad de la información es un componente esencial en cualquier organización, para ser efectiva debe estar relacionada con los procesos de negocios. En el sector financiero un buen conjunto de prácticas unidas con la tecnología proporcionan el cuidar los activos de la empresa, resguardando la confidencialidad que asegura la integridad y disponibilidad continua de la información. Las seguridades adoptadas pueden dar diferente enfoque dependiendo del entorno con el que se maneje la organización. Esta tesis, tiene como objetivo principal colaborar con la administración de claves de los usuarios, mismos que tienen acceso al manejo de la información dentro de la Cooperativa. El trabajo le permitirá observar el análisis, diseño e implementación de un modelo centralizado basado en el protocolo LDAP, el cual es utilizado para acceder a los datos almacenados en un directorio de información. Para llevar a cabo este trabajo se ha utilizado tecnologías OpenSource debido a que su código, foros y acceso es libre; dichas tecnologías son Centos, OpenLDAP, MySql y Php. El proyecto cumple con la construcción del directorio LDAP, iniciando con su descarga, configuración del servidor y de las variables de entorno que sirven para la instalación, seguido de su arranque e interrogación que permite añadir o eliminar entradas LDAP. Los resultados permiten acceder a través de una interface web a la información que se encuentra almacenada en el servidor LDAP.

PALABRAS CLAVE: LDAP, OPENSOURCE, CENTOS, OPENLDAP, SERVIDOR, INTERFACE WEB.

ABSTRACT

Information security is an essential component of any organization, to be effective it must be related to business processes. In the financial sector a good set practices together with technology provide care for company assets protecting the confidentiality that ensures the integrity and continuous availability of information. Adoptive assurances can be given different approach depending on the environment in which the organization is managed. This thesis main objective is working with key management of the users themselves who tend Access to information management within the cooperative. Observe the work will allow the design and implementation of a centralized model bassed on the LDAP protocol which is used to access data stored in a directory of information analysis. To carry this work has been used Open Source technologies because their fórums and Access code is free these technologies are Centos, Open LDAP, MySql and Php. The Project complies with the construction of the LDAP directory beginning with download server settings and environment variables used to install followed by the start and interrogation that can add or delete LDAP entries. The results allow Access through a web interface to information that is stored in the LDAP server.

KEYWORDS: LDAP, OPENSOURCE, CENTOS, OPENLDAP, SERVER, WEB INTERFACE.

GLOSARIO DE NOMENCLATURAS

- LDAP: (Lightweight Directory Access Protocol) es un servidor de datos optimizado para la realización rápida de consultas de lectura y orientado al almacenamiento de datos de usuarios a modo de directorio.
- Internet: Es un sistema mundial de redes de computadoras, integrado por las diferentes redes de cada país del mundo y por medio del cual un usuario con los permisos apropiados puede obtener información de un servidor o computadora personal y tener comunicación directa con otros usuarios.
- Open Source (Código abierto o código libre): Software que distribuye de forma libre su código fuente y los desarrolladores pueden hacer variaciones, mejoras o reutilizaciones en otras aplicaciones. También conocido como free software.
- Sitio Web: Conjunto de páginas Web referentes a un tema en particular, que incluye una página inicial de bienvenida, con un nombre de dominio y dirección en Internet. Empleado por las empresas para ofertar sus bienes y servicios.
- Modelo: Es la conceptualización de un evento, un proyecto, una hipótesis, el estado de una cuestión y se representa como un esquema que posee símbolos descriptivos de características y relaciones más importantes.
- Usuario: Ente humano que usa al sistema. Un mismo usuario puede actuar como instancias en varios actores diferentes, es decir, puede jugar diferentes roles

CAPÍTULO 1

INTRODUCCIÓN

Con el avance de la tecnología actual, se busca salvaguardar de la mejor manera la seguridad de la información, la administración para servidores de una organización es un punto primordial al momento de llevar de modo eficiente y optimo dicha seguridad, el poder dar el uso de modelos y nuevas herramientas que faciliten esta tarea.

Las redes corporativas permiten realizar intercambios de información con mayor rapidez pero no de modo seguro, los niveles de privilegios de usuarios varían dependiendo de su cargo en cada empresa, por desconocimiento o por algún otro motivo puede acceder a la información en el servidor y esta puede ser cambiada, modificada o eliminada.

Un punto muy importante acerca de este tema es la garantía que se dé a los usuarios con respecto a la seguridad, la generación de políticas, permisos e ingresos asegura integridad y disponibilidad.

El hecho de tener diferentes servidores cada uno con su rol, función y ejecución especifica determina una instancia a la cual debe enfrentarse el administrador, pérdida de información, un mal rendimiento o un acceso no autorizado al servidor, son algunos aspectos a tomar en cuenta, algo que diagnosticar no siempre es sencillo, ya sea por falta de recursos o por desconocimiento de la administración apropiada.

1.1.Planteamiento del problema

La información que se maneja es un punto crítico, por eso se ha llegado a considerar un activo cada vez más valioso. Razón por la cual se debe establecer un modelo de administración centralizado que sea eficiente para lograr salvaguardarla.

Actualmente en la Cooperativa de Ahorro y Crédito "29 de Octubre" se tiene diferentes servidores virtualizados con su respectivo rol, función específica, servicio asociado y con distinto proveedor lo que genera varios inconvenientes a la hora de la administración de cada uno de ellos; claves temporales, permisos, niveles de privilegio y servicios de tiempo necesitan ser adecuadamente llevados por el departamento y área responsable, a partir de allí se podrá desarrollar los procedimientos de seguridad con mayor precisión.

1.2.Justificación

La información es uno de los factores más importantes que manejan las organizaciones, se debe buscar métodos que permitan administrar y gestionar la misma, esto para que facilite y permita resolver las necesidades, manteniendo una seguridad informática.

Un modelo de administración centralizado de claves basado en LDAP permitirá mejorar la seguridad dentro de la cooperativa, como por ejemplo se conoce que al dar de baja un usuario dentro del servidor se evita desde ese momento que pueda acceder a la información compartida, también se pueden configurar restricciones.

Para la administración de las claves de los servidores virtualizados, existe la necesidad de instalar y centralizar un servidor que permita establecer accesos a la información y niveles de privilegios de ingreso a los servidores.

El beneficio es de tener un único servidor OpenLDAP que se comunique con los distintos servidores y elementos de la red para simplificar la administración

mediante una interfaz web, este se encargará de gestionar los permisos de acceso de los usuarios y de registrar las conexiones a uno u otro servidor al cual se necesite ingresar a ver o modificar.

1.3.Objetivos

1.3.1. Objetivo General

- Realizar un modelo de administración centralizado de claves basado en LDAP para Servidores Virtualizados Linux de la Cooperativa de Ahorro y Crédito “29 de Octubre”

1.3.2. Objetivos Específicos

- Analizar e Identificar los roles y funciones de cada servidor virtualizado Linux con las que cuenta la cooperativa.
- Diseñar el modelo de centralización de servidores basado en LDAP.
- Implementar un servidor de administración centralizada desde la que se gestionen ingresos a los servidores y en la que se obtenga información.
- Configurar permisos otorgando o restringiendo el acceso de los usuarios.

1.4.Alcance

En este proyecto se pretende identificar los roles y servicios que el servidor requiere, así como los recursos tecnológicos necesarios para diseñar el modelo que centralizará los controles de seguridad de acceso de usuarios.

Para el desarrollo del proyecto, de acuerdo con los requisitos administrativos, los requisitos de seguridad y la capacidad técnica, se va a optar por diseñar un modelo de administración centralizado basado en LDAP.

Un modelo administrativo centralizado se caracteriza por un solo grupo administrativo y por una administración del servidor y de las directivas centralizadas. El modelo administrativo es absolutamente independiente de la infraestructura física, de modo que este modelo puede centralizarse aun cuando la cooperativa esté formada por varias sucursales. Sólo puede haber un grupo administrativo, pero puede haber varios grupos.

Mediante un modelo administrativo centralizado se asignará accesos diferentes usuarios, su ingreso al manejo de la información en el servidor depende del privilegio dado, este criterio de seguridad permite establecer un acceso.

El modelo centralizado contara con una interfaz web, que permita la administración de usuarios, misma que incluye funcionalidades como la insertar y eliminar.

En la metodología utilizada, se establece que las fases de implementación de la misma llegan hasta las pruebas, para la implementación de este modelo no se realizará una implantación real del sistema.

1.5.Delimitación Espacial

Este proyecto se lo realizó en la Cooperativa de Ahorro y Crédito “29 de Octubre” LDTA, cantón Quito, provincia Pichincha.

1.6.Delimitación Temporal

El proceso de desarrollo se lo realizó desde enero de 2015 hasta noviembre de 2015, se utilizó el software libre Centos, OpenLDAP, Mysql el cual es adecuado para este tipo de proyectos.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Hardening en Linux

Como hardening se entiende a las medidas aplicables a un servidor con el fin de minimizar el riesgo de intrusión en el mismo. Se incluyen aquí medidas de seguridad local, de red, instalación de herramientas de seguridad proactiva y de integridad de datos. También se ha de conectar a la sonda de monitorización aquellas herramientas cuya salida tenga que ser supervisada. (Llaquet, 2011)

2.1.1. Permisos del sistema de archivos

Linux es un sistema multiusuario, lo que conlleva a mantener la privacidad de estos y un control general para que no todos puedan hacer lo que quieran y comprometer así el sistema. En la familia de los sistemas operativos GNU/LINUX se utilizan los permisos para ello, permitiendo o no realizar acciones concretas al resto de usuarios no propietarios del fichero, o incluso al propio propietario.

Cada usuario tiene un identificador UID (User Identification) y un grupo identificativo GID (Group Identification). Estos usuarios pueden realizar tres acciones distintas en un fichero:

- **Lectura**: del inglés *read* y abreviado como **r**, que indica no solo la posibilidad de leer el archivo, sino también de listarlo con el comando básico **ls**.
- **Escritura**: del inglés *write* y abreviado como **w**, que una vez activo permite al usuario realizar modificaciones en el archivo.
- **Ejecución**: del inglés *execute* y abreviado como **x**, permite al usuario la ejecución del archivo.

Cuando un usuario crea un fichero, el UID y GID propietarios de éste son los del propio usuario, como es lógico. Pero tiene más permisos que pueden ser configurados. (Llaquet, 2011)

Estos permisos indican que el usuario propietario del fichero tiene permisos de Lectura (R), Escritura (W) y Ejecución (X), que no es un directorio y que los miembros del grupo y el resto de usuarios del sistema no pueden hacerle nada.

Existen 9 bits de permiso, más 3 que afectan el modo de operación de los programas ejecutables. Este conjunto de 12 bits es el modo del archivo. El tipo de archivo, fijado al momento de su creación, ocupa 4 bits más, completando una palabra de 16 bits, los permisos se visualizan con ls -l.

Si el bit está en 0 quiere decir que no está activo, por el contrario si el bit está en 1, está activo. Si alguno de estos permisos está desactivado, para efectos del comando **ls** al momento de listar un archivo se le asigna un guion '-'.

- **Setuid, Setgid.** Los valores octales 4000 y 2000 son los bits setuid y setgid. El bit setuid permite ejecutar el programa con el dueño del archivo como propietario del proceso; el bit setgid permite ejecutarlo con el grupo dueño del archivo como grupo propietario del proceso. En algunos sistemas el bit setgid se usa en directorios para fijar el grupo dueño igual al del directorio cuando se crea un nuevo archivo.
- **Sticky bit.** El valor octal 1000 es el "sticky bit". Originalmente indicaba procesos que debían permanecer en memoria; actualmente se usa en algunos sistemas para conferir a los directorios compartidos la propiedad de impedir borrar archivos a otros que no sean el dueño del directorio, el dueño del archivo o el superusuario.
- **Bits de permiso.** Se agrupan en conjuntos de tres bits, representando permisos de lectura, escritura y ejecución. Existen tres grupos de 3 bits, con los respectivos permisos para el usuario, el grupo y otros. El significado de los permisos varía según se trate de un archivo o un directorio:

Para interpretar correctamente esta cadena se debe entender que cada espacio corresponde a un Bit de permisos, y estos al mismo tiempo se pueden agrupar en cuatro bloques tal como se indica a continuación:

Permiso	Símbolo	Binario	Archivo	Directorio
Ninguno	-	000	Ninguno	ninguno
Lectura	r	100	ver contenido	ver nombres de archivos y subdirectorios
Escritura	w	010	modificar contenido, permisos	crear y eliminar archivos y subdirectorios en el directorio
Ejecución	x	001	ejecutar el archivo como programa	acceder al directorio (posicionarse en él o invocar programas)

Los permisos en Linux son una base muy importante para entender cada vez más como funciona el sistema, así como para la comprensión de comandos útiles como **chmod** y una de las opciones de creación de directorios de **mkdir**, entre otros. (Llaquet, 2011)

2.1.2. Modificaciones

Para la modificación de permisos el bit 0 indica si se trata o no de un directorio, no se puede modificarlo, sino que es asignado en el momento de crear el fichero o directorio.

Ahora se tiene tres bloques con tres bits cada uno: rwx, para modificarlos se debe usar el comando “chmod” (Change Modes), este comando tiene varias sintaxis y se puede cambiar los permisos de acceso a un fichero o archivo. Sólo el dueño del archivo o el usuario llamado root pueden cambiar los permisos.

Su sintaxis puede variar mucho, ya que existen varias maneras de utilizarlo, siendo la fórmula inicial chmod {categoría} +-. {Permisos} {Archivo].

La manera de utilizar el comando chmod se describe a continuación:

sudo chmod {u, g, a, o} {+, - } {r, w, x } nombre del archivo

u: corresponde al dueño del archivo

g: corresponde al grupo

o - a: corresponde al resto de los usuarios, a para todos (all) y o para otros (others)

Para autorizar o desautorizar el permiso:

+: autoriza

-: desautoriza

=: resetea los permisos

y donde los tipos de permisos son:

r: lectura

w: escritura y

x: ejecución

2.1.3. Asignación coherente

Aunque la asignación de permisos a un fichero es algo prácticamente trivial, hacerlo adecuadamente no lo es tanto. Existe el problema debido a una mala gestión de los permisos en los ficheros sensibles. Empezando por el fichero donde se guardan los usuarios y passwords del sistema encriptados, el fichero **"/etc/shadow"**. Aunque los permisos por defecto varían según la distribución que se esté usando, no es así en cuanto al uso que se hace de éste. (Llaquet, 2011)

Cuando un usuario cambia el password o bien se registra en el sistema, lo hace utilizando el programa **"/bin/login"**, el cual tiene activado el atributo, o bit, SUID. Dicho de otra manera, mientras "login" está en ejecución, el usuario que lo ejecuta es "root".

Puede variar el grupo o incluso los permisos, este fichero solamente será leído y escrito por root, a no ser que el administrador quiera que alguno más lo haga.

En la familia de operativos Unix los usuarios tienen su "home" en "/home/<usuario>/" por defecto. Exceptuando el administrador "root", el home del cual se encuentra en "/root" generalmente. La importancia es mantener la privacidad de todos los usuarios y de cómo proteger el "home" del administrador para que los usuarios no puedan ver que hay dentro de él. Para que esto no ocurra, se asignará permisos de ejecución, lectura y escritura exclusivamente al usuario root:

```
# chmod 700 /root
```

Con esto queda protegido el directorio contra el listado de ficheros. Es recomendable realizar el mismo comando a todos los "homes" de los usuarios para evitar que unos vean el contenido de los otros:

```
# chmod 700 /home/*
```

A continuación se debe configurar los logs del sistema para evitar lecturas por parte de otros usuarios distintos a root o el encargado de los logs, bastará entonces con cambiar el propietario de los logs a "logger" y darle los permisos adecuados, tal y como se ha hecho con los "homes" de los usuarios. Claro que a lo mejor interesa que "logger" solo pueda leer los ficheros, sin llegar a modificarlos, y no es recomendable que pueda cambiarse los privilegios porque entonces podría saltarse esa prohibición.

Dependiendo del tipo de servidor, los permisos deberán ser más o menos restrictivos, eso ya depende de cada caso en concreto y del administrador que esté a cargo.

Lo que sí es generalizable es el minucioso cuidado que se debe tener con los ejecutables con el bit SUID activo, se deben extremar las precauciones y mantenerlo

fuera del alcance de los usuarios. De lo contrario, si existiera un bug en algún ejecutable de este tipo o se hiciera un mal uso de éste, un usuario podría llegar a realizar una escalada de privilegios y ser entonces “root”, lo que comprometería el sistema.

2.1.4. Integridad

La integridad se refiere a la validez y consistencia de los elementos de información almacenados y procesados en el sistema. Basándose en este principio, las herramientas de seguridad deben asegurar que los procesos estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Entre los temas a considerar en primera instancia está la identificación de todos los archivos factibles de ser escritos por todos, los cuales podrían potencialmente poseer un riesgo para la confidencialidad, integridad, o seguridad del sistema y sus datos en caso sean modificados.

2.2. Configuraciones

2.2.1. Seguridad

La seguridad local puede atacarse desde dos puntos de vista, el acceso físico al sistema y el acceso virtual, existen aplicaciones que se encargan de gestionar sucesos. Éstas utilizan, por lo general, el mail local para comunicarse con el administrador del sistema, por esa razón es recomendable un servidor de correo para permitirle dicha comunicación. De lo contrario, algunas aplicaciones podrán no funcionar correctamente. (Llaquet, 2011)

2.2.1.1. Seguridad Física

En contraste con los entornos físicos, los entornos virtuales basan su operación en infraestructura física unificada, es decir, un servidor físico puede contener uno o varios sistemas operativos hospedados en una misma plataforma. Es

aquí donde el tema de seguridad de ambientes virtuales juega un papel muy importante. A diferencia de un equipo físico, están reducidas a un simple archivo, que representa flexibilidad para el administrador, también significa una vulnerabilidad que puede ser explotada para robar la máquina completa, incluyendo su contenido. Se debe Recordar que en los entornos virtuales, varias máquinas virtuales pueden compartir una sola interfaz física en consecuencia, dichos equipos pueden ser víctimas de diversos tipos de ataques entre una máquina virtual y otra residente en el mismo equipo físico, ante esta situación, el administrador debe estar prevenido.

2.2.1.2. Limitando el acceso físico

La seguridad virtual se extiende más allá de las máquinas virtuales, una recomendación es mantener los sistemas de almacenamiento separados del resto de las máquinas virtuales.

En donde se utilizan equipos para ejecutar las tareas de procesamiento de las máquinas virtuales (y su almacenamiento se encuentra en un almacenamiento de red), es fácil ver cómo se ve comprometido todo el sistema de almacenamiento cuando no se contemplan este tipo de riesgos, sobre todo al momento de la instrumentación de entornos virtuales basados en sistemas de almacenamiento separado.

Algunos aspectos para limitar el acceso físico es la aplicación de seguridad en entornos virtuales al inicio de su diseño: clasificación del tráfico e información real entre máquinas virtuales, mecanismos de autentificación, controles de acceso robustos, controles para el acceso y la operación, corrección de vulnerabilidades e instalación de actualizaciones de seguridad, así como configuración de auditoría y escaneo de vulnerabilidades. (Llaquet, 2011)

2.2.2. Seguridad Local

Se deben tener permisos de seguridad de propietario en todos los paquetes de envíos en la red para que no puedan entrar los intrusos permitiéndole a los usuarios desconocidos el permiso de lectura y no de escritura, ni tampoco las dos opciones a la vez que si tiene el propietario o root que es letura y escritura al mismo tiempo, esta opción permite a Linux administrar tanto archivos, carpetas, directorios y cuentas en (admin) para proteger de manera segura.

Desde Linux cada usuario puede tener una clave y un usuario puede permitir que sea más difícil entrar a su sistema y ser jaqueado. Utilizando un cifrado como clave que no sea ni el nombre, ni tampoco algo muy conocido sino más bien dónde sea combinado tanto letras como números que sea muy difícil de cifrar por un espía.

Se debe limitar, el utilizar al usuario principal root solo para tareas concretas, ya que por seguridad es bueno tener un usuario secundario, porqué el usuario principal es donde se tiene muchos registros del sistema que si en un momento dado es jaqueado se perdería el computador y ser secuestrado por otro usuario que logro el objetivo principal como intruso de obtener toda la información del root y ante ello no se podría hacer nada. *(Llaquet, 2011)*

Se puede decir que para eliminar el riesgo en linux se permite utilizar las relaciones de confianza UNIX que consiste en incluir los nombres o direcciones IP de la máquinas de confianza en los ficheros host del servidor.

Además es recomendable desactivar servicios no necesarios en linux y modificar los ficheros /etc/inetd.conf o /etc/xinetd.conf.

Se puede utilizar un método de criptografía asimétrica donde utilice 128 bits donde una cuenta tenga dos claves una pública y una privada que cuando envié algo al receptor se difícil descifrarla aun teniéndose palabras claves o frases.

2.2.2.1. Seguridad del sistema de ficheros

Se tendrá que asignar los permisos adecuados a los directorios sensibles del sistema, para evitar miradas de terceros, tanto propietarios como permisos. De esta manera se asegura la privacidad de los usuarios:

chmod 700 (permisos)

chown : (propietario)

Adicionalmente se puede utilizar un cifrado de cualquier tipo asegurar ficheros concretos o bien montar una partición cifrada de manera que la operación de cifrado sea transparente. Existen algunas herramientas para realizar estas acciones.

2.2.2.2. Cambio periódico de contraseña

Por mucho que se proteja un sistema, algunos usuarios son descuidados y no se preocupan lo suficiente a la hora de asignar una contraseña o bien a la hora de conservarla. Cuando eso ocurre, un potencial atacante ya habría superado la primera barrera, la remota, y por lo tanto tendría acceso al sistema gracias a la cuenta débil proporcionada por el usuario legítimo. Para evitar esta clase de problemas el administrador tendría que obligar a los usuarios a redefinir su contraseña cada cierto periodo de tiempo, así asegura que si el usuario pierde la contraseña u otra persona la posea, al cabo de cierto tiempo esas credenciales se invalidarán, consiguiendo así que el atacante no puedo reutilizarlos.

2.3. OpenSource

Es una expresión de la lengua inglesa que pertenece al ámbito de la informática. Aunque puede traducirse como “fuente abierta”, suele emplearse en nuestro idioma directamente en su versión original, sin su traducción correspondiente.

Se califica como open source a los programas informáticos que permiten el acceso a su código de programación, lo que facilita modificaciones por parte de otros programadores ajenos a los creadores originales del software en cuestión.

Es importante distinguir entre el software open source, que dispone de la mencionada característica de presentar su código abierto, y el software libre que puede descargarse y distribuirse de manera gratuita. Existe software libre que no brinda acceso al código y que, por lo tanto, no puede considerarse como open source, y programas open source que se distribuyen de manera comercial o que requieren de una autorización para ser modificados.

Pese a que ambas nociones suelen confundirse, por lo general la idea de open source está vinculada a una filosofía de trabajo conjunto sobre los programas informáticos. Cuando se brinda acceso al código fuente, la comunidad de programadores puede hacer sus aportes para solucionar eventuales fallos, incrementar la usabilidad y mejorar el programa a nivel general.

2.4. Protocolo LDAP

Es un protocolo estándar que permite administrar directorios, esto es, acceder a bases de información de usuarios de una red mediante protocolos TCP/IP.

Un servidor LDAP, es un servidor de datos optimizado para la realización rápida de consultas de lectura y orientado al almacenamiento de datos de usuarios a modo de directorio. (OpenLDAP, s.f.)

La principal utilidad de un directorio LDAP es como servidor de autentificación para los distintos servicios de un sistema informático estos pueden ser:

- Autentificación para el ingreso a un ordenador
- Ingreso a una aplicación web.
- Acceso a los servidores.

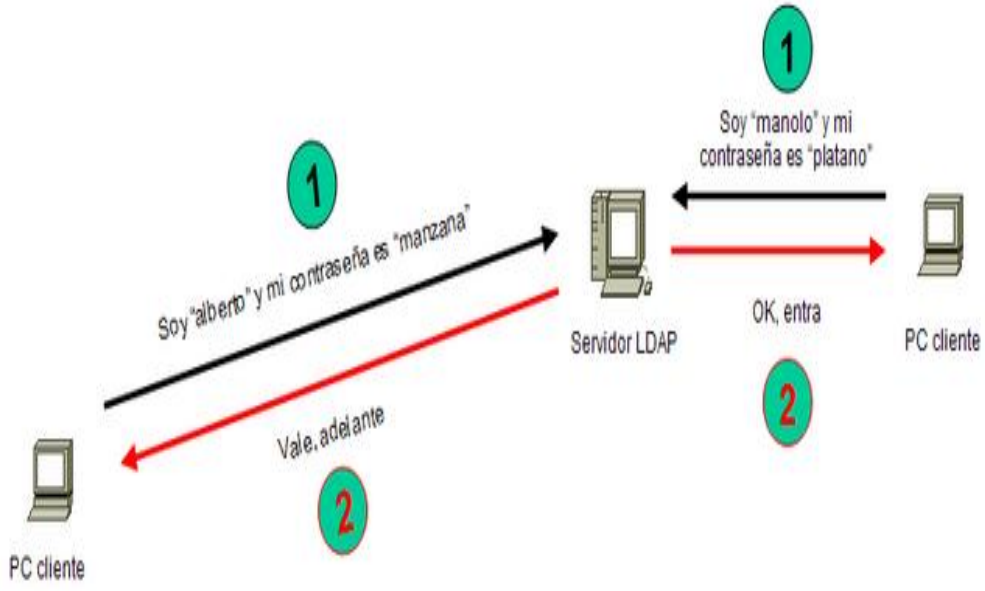

Figura 1 Servidor LDAP

2.4.1. Cómo funciona LDAP

El servicio de directorio LDAP se basa en un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol del directorio LDAP o base de datos troncal. El cliente LDAP se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de dónde puede el cliente hallar más información. No importa con qué servidor LDAP se conecte el cliente, siempre observará la misma vista del directorio, el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP. Es ésta una característica importante de un servicio de directorios universal como LDAP. (Malere, 2000)

Si en la red se dispone de un servidor LDAP y se configura todos los PCs y todos los servicios de la red para que se autentifiquen en él, bastará con crear las cuentas de usuario y grupos de usuarios en el servidor LDAP para que los usuarios puedan hacer uso del sistema y de sus servicios desde cualquier puesto de la red.

Es un sistema ideal para centralizar la administración de usuarios en un único lugar. LDAP presenta la información bajo la forma de una estructura jerárquica de árbol denominada DIT (Árbol de información de directorio), en la cual la información denominada entradas, es representada por bifurcaciones. Una bifurcación ubicada en la raíz de una bifurcación se denomina entrada raíz (Kioskea, 2014).

- Cada entrada en el directorio LDAP corresponde a un objeto abstracto o real.
- Cada entrada está conformada por un conjunto de pares clave/valor denominados atributos.

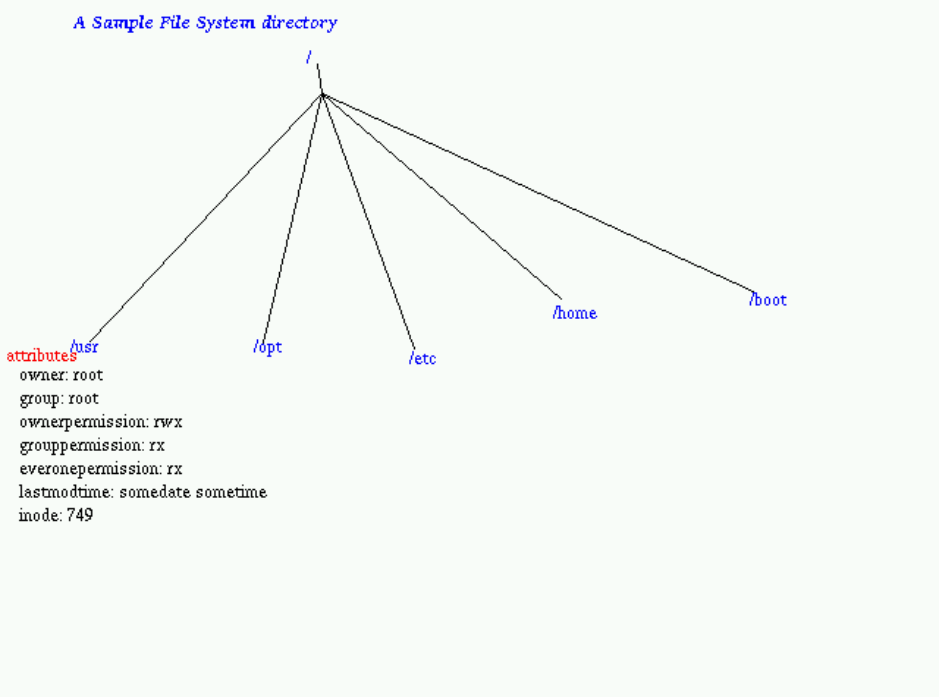

Figura 2 Diagrama del Directorio de Sistema de Ficheros

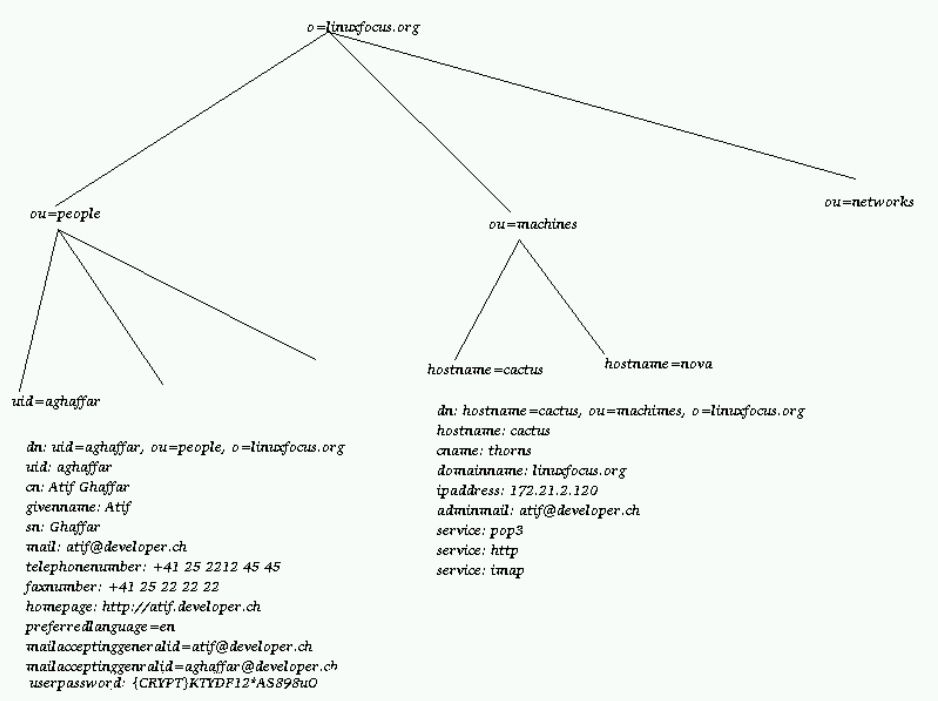

Figura 3 Diagrama del directorio LDAP

Cada entrada está compuesta por un conjunto de atributos (pares clave/valor) que permite caracterizar el objeto que la entrada define. Existen dos tipos de atributos:

- Atributos normales: éstos son los atributos comunes (apellido, nombre, etc.) que distinguen al objeto.
- Atributos operativos: éstos son atributos a los que sólo el servidor puede acceder para manipular los datos del directorio (fechas de modificación, etc.).

2.4.2. Atributos de Entrada

Una entrada se indexa mediante un nombre completo (DN) que permite identificar de manera única un elemento de la estructura de árbol. (Kioskea, 2014)

Un DN se constituye tomando el nombre del elemento denominado Nombre distintivo relativo y agregándole el nombre entero de la entrada principal.

Se trata de utilizar una serie de pares clave/valor para poder localizar una entrada de manera única. A continuación se ve una serie de claves generalmente utilizadas:

- uid (id de usuario), ésta es una identificación única obligatoria
- cn (nombre común), éste es el nombre de la persona
- givenname, éste es el nombre de pila de la persona
- sn (apellido), éste es el apellido de la persona
- (organización), ésta es la compañía de la persona
- u (unidad organizacional), éste es el departamento de la compañía para la que trabaja la persona

En LDAP, una clase de objetos define la colección de atributos que pueden usarse para definir una entrada. El estándar LDAP proporciona estos tipos básicos para las clases de objetos: (Malere, 2000)

- Grupos en el directorio, entre ellos listas no ordenadas de objetos individuales o de grupos de objetos.
- Emplazamientos, como por ejemplo el nombre del país y su descripción.
- Organizaciones que están en el directorio.
- Personas que están en el directorio.

Una entrada determinada puede pertenecer a más de una clase de objetos. Por ejemplo, la entrada para personas se define mediante la clase de objetos person, pero también puede definirse mediante atributos en las clases de objetos inetOrgPerson, groupOfNames y organization. La estructura de clases de objetos del servidor (su esquema) determina la lista total de atributos requeridos y permitidos para una entrada concreta.

Los datos del directorio se representan mediante pares de atributo y su valor. Cualquier pieza de información específica se asocia con un atributo descriptivo.

2.4.3. Consulta de datos

LDAP brinda un conjunto de funciones para llevar a cabo solicitudes en los datos para buscar, cambiar y eliminar entradas en los directorios.

A continuación se describe las principales operaciones que puede realizar LDAP:

Funcionamiento	**Descripción**
Abandon (Abandonar)	Cancela la operación previa enviada al servidor
Add (Agregar)	Agrega una entrada en el directorio
Bind (Enlazar)	Inicia una nueva sesión en el servidor LDAP
Compare (Comparar)	Compara las entradas en un directorio según los criterios
Delete (Eliminar)	Elimina una entrada de un directorio
Extended (Extendido)	Realiza operaciones extendidas
Rename(Cambiar nombre)	Cambia el nombre de una entrada
Search (Buscar)	Busca entradas en un directorio
Unbind (Desenlazar)	Finaliza una sesión en el servidor LDAP

2.4.4. El formato Ldif

LDIF es un formato que se utiliza para la importación y exportación de datos independientemente del servidor LDAP que se esté utilizando.

Cada servidor LDAP tiene una o varias maneras de almacenar físicamente sus datos en el disco, por esto que Ldif provee una manera de unificar la manera de tratar

los datos y así poder migrar de un servidor a otro sin importar que clase de implementación es.

El formato Ldif es simplemente un formato de texto Ascii para entradas LDAP, que tiene la siguiente forma: (Pentima, 2007)

dn: <nombre distinguido>
<nombre_atributo>: <valor>
<nombre_atributo>: <valor>
<nombre_atributo>: <valor>

En un archivo Ldif puede haber más de una entrada definida, cada entrada se separa de las demás por una línea en blanco. A su vez, cada entrada puede tener una cantidad arbitraria de pares <nombre_atributo>: <valor>.

Este formato es útil tanto para realizar copias de seguridad de los datos de un servidor LDAP, como para importar pequeños cambios que se necesiten realizar manualmente en los datos, siempre manteniendo la independencia de la implementación LDAP y de la plataforma donde esté instalada.

A continuación se ve un formato Ldif para cuenta de un usuario.

dn: uid=jperez,ou=People,dc=ejemplo,dc=com
uid: jperez
cn: Juan Perez
objectclass: account
objectclass: posixAccount
objectclass: top
loginshell: /bin/bash
uidnumber: 512
gidnumber: 300
homedirectory: /home/jperez
gecos: Juan Perez,,,,
userpassword: {crypt}LPnaOoUYN57Netaac

2.5. Virtualización

2.5.1. Introducción

La virtualización de servidores, sistemas operativos y redes juega un papel fundamental tanto para los administradores de sistemas como para los expertos en seguridad informática. Para los administradores de sistemas brinda una herramienta perfecta para separar unos servicios de otros y ganar en seguridad, ya que si un hacker compromete un servicio no tendrá acceso a todo el sistema.

Desde el punto de vista del hacking ético esta herramienta dará la posibilidad de crear entornos virtuales para poder hacer pruebas. Otra de las ventajas de la virtualización es que si se quiere probar un sistema operativo antes de decidir si instalarlo en el disco duro modificando el sistema de arranque se podrá instalarlo sin necesidad de hacer ningún cambio en tu PC, tal y como si fuera un programa más. (cursohacker.es, 2015)

2.5.2. Qué es la virtualización

La virtualización consiste en términos generales en emular mediante algún programa un hardware sobre el que montar un servicio, servidor o red. De esta forma se crea lo que se conoce como una máquina virtual. Así con un solo ordenador se puede crear varias máquinas virtuales e instalar en cada una de ellas el software ya sea un Windows, una distribución de Linux, o MacOS. (cursohacker.es, 2015)

Esto es importante no solo para el usuario que se dedica de forma profesional a la informática sino para todos los usuarios, si el usuario de Windows necesita en algún momento trabajar con un programa pero este sólo se encuentra disponible para Linux, se podrá mediante una máquina virtual instalar un Linux dentro del Windows y trabajar con el programa que se necesite.

La idea principal es la de permitir ejecutar varios sistemas operativos simultáneamente sobre el mismo hardware. Para ello, separa las dos funciones básicas que realiza un sistema de tiempo compartido: multiprogramación y abstracción del hardware. El corazón del sistema es conocido como monitor de máquina virtual, y se ejecuta sobre el hardware proporcionando varias máquinas virtuales al siguiente nivel de software. Por eso cada una puede estar ejecutando un sistema operativo distinto. (cursohacker.es, 2015)

- **Hosting:** cada vez son más los ISP que ofrecen servidores virtuales usando estas tecnologías.
- **Consolidación de servidores:** se trata de agrupar todos los servidores de una empresa en una sola máquina. La idea se basa en aprovechar mejor los recursos del servidor, ya que es habitual el desaprovechamiento de los recursos del hardware, en estos casos, se utilizan máquinas virtuales, la realización de copias de seguridad de cada una de las maquinas resulta muy fácil, puesto que en general supondrá la copia de un solo fichero.
- **HoneyPots:** Máquinas puestas en internet para que los Hackers 'jueguen' con ellas. se usan en genera para aprender los comportamientos y las nuevas técnicas que usan los intrusos informáticos.
- **Máquinas de desarrollo y pruebas:** Siempre es mejor probar las cosas en una máquina que no es crítica para el negocio y que, como en el caso de las máquinas virtuales, se pueden recuperar en muy poco tiempo.

2.5.3. Ventajas de la Virtualización

Como administrador de sistemas o redes trabajar virtualizando servidores, aplicaciones o servicios es una estrategia que cada día se pone en práctica con más énfasis. Los beneficios de la virtualización para los administradores se pueden dividir en grupos. (cursohacker.es, 2015)

- **Seguridad**

Si se escoge una solución virtualizada se creará un servidor en 2 máquinas virtuales. En la primera se instalaría el servidor LAMP, y en la segunda se instalaría el servidor de archivos. En este escenario un hacker que consiga encontrar una vulnerabilidad en la web solo tendría acceso a la máquina virtual que aloja el servidor LAMP y aunque lograría conseguir comprometer en la web los archivos de la empresa aún seguirían aislados y seguros. Es por este motivo por el que para muchos administradores la solución ideal es crear una máquina virtual por cada servicio que tenga un riesgo medio alto de ser vulnerado. (cursohacker.es, 2015)

- **Copias de seguridad**

La mayoría de los servicios que se utiliza hoy en día disponen de mecanismos para hacer copias de seguridad y poder restaurarlas en caso de fallos. Pero también es cierto que las copias de seguridad a veces no son completas, contienen datos pero no guardan configuraciones o perfiles específicos.
Si se utiliza máquinas virtuales, se puede programar en el servidor de forma automática que cada día haga una copia de la máquina virtual, de modo que si quiere restaurar una copia de seguridad bastará con arrancar la máquina que tiene copiada y funcionará sin tener que tomar ninguna medida más.

- **Protección contra errores hardware**

Uno de los problemas que más daño puede crear a un administrador de sistemas es que falle un componente crítico del servidor, si esto ocurre y hay que sustituir este elemento habrá que reinstalar todo el sistema operativo, configurarlo, instalar los programas, configurarlos y cargar las copias de seguridad para poder seguir trabajando. Todo esto tiene un coste en tiempo y esfuerzo bastante alto. Sin embargo si se está trabajando con máquinas

virtuales si falla el servidor se podrá sustituirlo, copiarle las máquinas virtuales y arrancarlas**.** Esta solución no llevará mucha parte de tiempo que si se tuviera en el caso de reconfigurarlo todo de nuevo.

- **Migración de servidores sin reconfiguraciones**

Aplicando el punto anterior si el servidor se queda sin espacio y se requiere uno con mayor capacidad, tan solo se necesitará conectarlo pasarle las máquinas virtuales y empezar a trabajar nuevamente, sin necesidad de reconfigurar todo lo que se tenía hecho en el servidor que se quedó sin espacio.

- **Realizar Pruebas sin riesgo**

Una de las características más interesantes de la virtualización es que se puede hacer "puntos de retorno" o "Snapshots". Esto significa que si se está dudando sobre si instalar un programa o no, se creará un punto de retorno "snapshot", instalar lo que se requiera y si se detecta alguna incompatibilidad lo mejor habría sido no instalarlo, pues se podrá volver al punto de retorno y la máquina virtual volverá al estado en el que se hizo el snapshot, sin quedar ningún rastro de todo lo que se haya hecho tras el punto de retorno. (cursohacker.es, 2015)

- **Privacidad y Protección**

El problema de cifrar la partición en el que se está instalando el sistema operativo es que si se corrompe no se podrá utilizar herramientas para repararlo ya que al estar cifrado las herramientas no podrán acceder al contenido. Una forma de trabajar utilizando la criptografía disminuyendo el riesgo de no poder reparar el sistema operativo es precisamente cifrar la máquina virtual así no se tendrá el problema de estar sin poder reparar el sistema operativo pero nadie será capaz de ejecutar la máquina virtual sin conocer la clave de descifrado.

Otro punto extra que ofrecen las máquinas virtuales es que como permiten virtualizar cualquier sistema operativo se puede tener un sistema operativo en el que no aparezcan datos sobre alguien en especial, que no aparezca el nombre real, y no se haya introducido ningún dato personal. Con este sistema operativo "neutro" se podrá navegar por internet sin dejar rastro de nombres.

Como usuarios de la red y programas a veces se encuentra que no se está seguro si algún programa trae malware incrustado, se sospecha que quizá por la procedencia el programa no está limpio.

Si se instala en algún ordenador tal cual se lleva el riesgo de que se vea infectado por el malware que contenga, si no se lo instala no se puede hacer uso del programa. En este punto las máquinas virtuales también resultan de gran ayuda ya que se instalará el programa dentro de la máquina virtual, analizando si traía malware y decidir si instalarlo en el sistema operativo de trabajo o dejarlo virtualizado.

2.6. Administración de cuentas de usuarios y acceso a recursos

La administración de cuentas de usuario y grupos es una parte esencial de la administración de sistemas dentro de una organización. Pero para hacer esto efectivamente, el administrador de sistemas primero debe entender lo que son las cuentas de usuario y los grupos y cómo funcionan. (Red Hat, 2005)

La razón principal para las cuentas de usuario es verificar la identidad de cada individuo utilizando un computador. Una razón secundaria es la de permitir la utilización personalizada de recursos y privilegios de acceso.

Los recursos incluyen archivos, directorios y dispositivos. El control de acceso a estos dispositivos forma una gran parte de la rutina diaria de un administrador de sistemas; a menudo el acceso a un recurso es controlado por grupos. Los grupos son construcciones lógicas que se pueden utilizar para enlazar a usuarios para un propósito común. Por ejemplo, si una organización tiene varios administradores de sistemas, todos ellos se pueden colocar en un grupo

administrador del sistema. Luego se le pueden dar permisos al grupo para acceder a recursos claves del sistema.

De esta forma, los grupos pueden ser una herramienta poderosa para la administración de recursos y acceso.

2.6.1. Administración de cuentas de usuarios

Como se dice anteriormente, las cuentas de usuarios es la forma a través de la cual se identifica y autentifica a un individuo con el sistema. Las cuentas de usuarios tienen diferentes componentes. Primero, está el nombre de usuario. Segundo, está la contraseña seguida de la información de control de acceso. (Red Hat, 2005)

2.6.2. El nombre de usuario

Desde el punto de vista del sistema, el nombre de usuario es la respuesta a la pregunta "quién es usted". Como tal, los nombres de usuarios tienen un requerimiento principal deben ser únicos. Es decir cada usuario debe tener un nombre de usuario que sea diferente a todos los otros usuarios en ese sistema.

Debido a este requerimiento, es vital determinar cómo se crean los nombres de usuario. De lo contrario, puede encontrarse en la posición de ser forzado a reaccionar cada vez que un nuevo usuario solicita una cuenta.

Lo que necesita es una convención de nombres para sus cuentas de usuarios.

2.6.3. Convenio de nombres

Mediante la creación de un convenio de nombres para los usuarios, se puede ahorrar varios problemas. En vez de inventar nombres cada vez, el convenio de

nombres puede ser muy simple, o solamente su descripción puede tomar muchas páginas.

La naturaleza exacta de su convenio de nombres debe tomar varios factores en cuenta:

- El tamaño de su organización
- La estructura de su organización
- La naturaleza de su organización

El tamaño de la organización importa, pues dicta cuántos usuarios puede soportar su convención para nombres. Una compañía quizás pueda permitir que todo el mundo utilice su primer nombre. Para una organización mucho más grande, este convenio no funciona.

La estructura de la organización también puede tener influencia sobre el convenio de nombres más apropiado. Para organizaciones con una estructura bien definida puede ser adecuado incluir elementos de esa estructura en la convención de nombres, puede incluir los códigos de los departamentos como parte del nombre de usuario. (Red Hat, 2005)

2.6.4. Manejo de cambios de nombres

Si la organización utiliza una convención de nombres que está basada en el nombre de cada usuario, es de esperarse que eventualmente tendrá que enfrentarse a cambios de nombres. Aún si el nombre de la persona realmente no cambia, de vez en cuando se le pedirá que modifique el nombre de usuario. Las razones pueden variar desde un usuario que no le gusta su nombre de usuario hasta un empleado con más jerarquía en la organización que prefiere un nombre de usuario "más acorde".

No importa cuál sea la razón, hay muchos aspectos a tener en mente cuando se cambie un nombre de usuario:

- Mantener constante toda la información subyacente del usuario.

- Cambiar la propiedad de todos los archivos y otros recursos específicos al usuario.
- Manejar los problemas relacionados con el correo electrónico.

Es importante estar seguros de que el nuevo nombre de usuario es propagado a todos los sistemas donde se utilizaba el nombre original. De lo contrario, cualquier función del sistema operativo que esté vinculado con el nombre de usuario, funcionará en algunos sistemas y en otros no. Ciertos sistemas operativos utilizan técnicas de control de acceso basadas en nombres de usuarios. (Red Hat, 2005)

Muchos sistemas operativos utilizan algún tipo de número de identificación de usuarios para la mayoría de los procesamientos específicos al usuario. Para minimizar los problemas generados a partir de un cambio de nombre de usuario, tratar de mantener este número de identificación constante entre el nuevo y el viejo nombre de usuario. Si no se hace esto, puede producir un escenario en el que el usuario ya no puede acceder a sus archivos y otros recursos que ellos poseían anteriormente bajo el nombre de usuario original.

Si se debe cambiar el número de identificación del usuario, es necesario cambiar la propiedad para todos los archivos y recursos específicos al usuario para reflejar la nueva identificación del usuario. Este puede ser un proceso muy susceptible a errores, ya que pareciera que siempre hay algo en alguna esquina olvidada del sistema que se ignora al final. (Red Hat, 2005)

Los problemas relacionados al correo electrónico probablemente sean donde el cambio de un nombre de usuario es más difícil. La razón para esto es que a menos que se tomen las medidas para evitarlo, los correos electrónicos dirigidos al viejo nombre de usuario no se entregaran al nuevo.

Los problemas alrededor del impacto de los cambios de nombres de usuario en el correo electrónico tienen múltiples dimensiones. En su forma más básica, un cambio de nombre de usuario implica que la gente ya no conoce el nombre de usuario correcto de esa persona. A primera vista, esto puede parecer como que no es gran cosa notificar a todo el mundo en su organización (Red Hat, 2005)

Se le puede indicar al usuario que debe alertar a todas las personas que su nombre de usuario ha sido modificado. A medida que el tiempo pasa, menos y menos mensajes serán entregados usando el alias y eventualmente podrá eliminarlo.

2.6.5. Contraseñas

Si el nombre de usuario responde a la pregunta "¿Quién es usted?", la contraseña es la respuesta a la pregunta que inevitablemente sigue:

En términos más prácticos, una contraseña proporciona una forma de probar la autenticidad de la persona que dice ser el usuario con ese nombre de usuario. La efectividad de un esquema basado en contraseñas recae en gran parte sobre varios aspectos de la contraseña:

- La confidencialidad de la contraseña
- La resistencia de adivinar la contraseña
- La resistencia de la contraseña ante un ataque de fuerza bruta

Las contraseñas que efectivamente toman en cuenta estos problemas se conocen como contraseñas robustas, mientras que aquellas que no, se les llama débiles. Es importante para la seguridad de la organización crear contraseñas robustas, mientras más robustas sean las contraseñas, hay menos chances de que estas sean descubiertas o que se adivinen. Hay dos opciones disponibles para reforzar el uso de contraseñas robustas: (Red Hat, 2005)

- El administrador del sistema puede crear contraseñas para todos los usuarios.
- El administrador del sistema puede dejar que los usuarios creen sus propias contraseñas, a la vez que se verifica que las contraseñas sean lo suficientemente robustas.

Al crear contraseñas para todos los usuarios asegura que estas sean robustas, pero se vuelve una tarea pesada a medida que crece la organización. También incrementa el riesgo de que los usuarios escriban sus contraseñas.

Por estas razones, la mayoría de los administradores de sistemas prefieren dejar que los usuarios mismos creen sus contraseñas. Sin embargo, un buen administrador de sistemas tomará los pasos adecuados para verificar que las contraseñas sean robustas.

La necesidad de mantener secretas las contraseñas debería ser una parte arraigada en la mente de un administrador de sistemas. Este punto se pierde con frecuencia en muchos usuarios. De hecho, muchos usuarios ni siquiera entienden la diferencia entre nombres de usuarios y contraseñas. Dado este hecho, es de vital importancia proporcionar cierta cantidad de educación para los usuarios, para que así estos puedan entender que sus contraseñas se deberían mantener tan secretas como su sueldo. (Red Hat, 2005)

Las contraseñas deberían ser tan difíciles de adivinar como sea posible. Una contraseña robusta es aquella que un atacante no podrá adivinar, aún si el atacante conoce bien al usuario.

Un ataque de fuerza bruta sobre una contraseña implica el intento metódico de cada combinación de caracteres posible con la esperanza de que se encontrará la contraseña correcta eventualmente. Una contraseña robusta se debería construir de manera tal que el número de contraseñas potenciales a probar sea muy grande, forzando al atacante a tomarse un largo tiempo buscando la contraseña.

2.6.6. Información de control de acceso

Junto con un nombre de usuario y contraseña, las cuentas de usuario también contienen información de acceso. Esta información toma formas diferentes de acuerdo al sistema operativo o servidor utilizado. Sin embargo, los tipos de información a menudo incluyen:

- Identificación específica al usuario global al sistema

- Identificación específica al grupo global al sistema
- Lista de los grupos/capacidades adicionales a los cuales el usuario es miembro
- Información de acceso por defecto a aplicar para todos los archivos y recursos creados por el usuario

En algunas organizaciones, la información de control de acceso quizás nunca se necesite tocar. Este caso es más frecuente con estaciones de trabajo personales y sistemas independientes, los recursos compartidos a los largo de la red entre diferentes grupos de usuarios, requieren que la información de control de acceso se modifique con frecuencia. (Red Hat, 2005)

La carga de trabajo requerida para mantener apropiadamente la información de control de acceso de sus usuarios varía de acuerdo a cuan intensivamente su organización utiliza las funcionalidades de control de acceso. Mientras que no está mal contar con estas funcionalidades, implica que el entorno de sistema puede requerir más esfuerzo para ser mantenido y que cada cuenta de usuario pueda tener más formas en las cuales pueda ser mal configurada.

Por lo tanto, si la organización requiere de ese tipo de entorno, se debería documentar los pasos exactos requeridos para crear y correctamente configurar una cuenta de usuario. De hecho, si hay diferentes tipos de cuentas de usuario, debería documentar cada una.

2.7. Introducción a Php

PHP es el lenguaje de lado servidor más extendido en la web. Nacido en 1994, se trata de un lenguaje de creación relativamente reciente, aunque con la rapidez con la que evoluciona Internet parezca que ha existido toda la vida. Es un lenguaje que ha tenido una gran aceptación en la comunidad de desarrolladores, debido a la potencia y simplicidad que lo caracterizan, así como al soporte generalizado en la mayoría de los servidores de hosting. (Alvarez, 2002)

PHP permite embeber pequeños fragmentos de código dentro de la página HTML y realizar determinadas acciones de una forma fácil y eficaz, combinando lo que se sabe del desarrollo HTML. Es decir, con PHP se escribe scripts dentro del código HTML. Por otra parte, es aquí donde reside su mayor interés con respecto a los lenguajes pensados para los CGI, PHP ofrece un sinfín de funciones para la explotación de bases de datos de una manera llana, sin complicaciones.

2.7.1. Tareas Principales de Php

En un principio diseñado para realizar poco más que un contador y un libro de visitas, PHP ha experimentado en poco tiempo una verdadera revolución y a partir de sus funciones, en estos momentos se pueden realizar una multitud de tareas útiles para el desarrollo del web: (Alvarez, 2002)

- **Funciones de correo electrónico**

Se puede con facilidad enviar un e-mail a una persona o lista parametrizando toda una serie de aspectos tales como el e-mail de procedencia, asunto, persona.

Otras funciones menos frecuentes pero de indudable utilidad para gestionar correos electrónicos son incluidas en su librería.

- **Gestión de bases de datos**

El lenguaje PHP ofrece interfaces para el acceso a la mayoría de las bases de datos comerciales y por ODBC a todas las bases de datos posibles en sistemas, a partir de las cuales podremos editar el contenido de nuestro sitio con absoluta sencillez.

- **Gestión de archivos**

Crear, borrar, mover, modificar, cualquier tipo de operación más o menos razonable puede ser realizada a partir de una amplia librería de funciones para la gestión de archivos por PHP. También se puede transferir archivos por FTP a partir de

sentencias en el código, protocolo para el cual PHP ha previsto también gran cantidad de funciones.

- **Tratamiento de imágenes**

Puede resultar cansado uniformar en tamaño y formato miles de imágenes recibidas día tras día. Todo este procedimiento puede ser también automatizado eficazmente mediante PHP.

También puede ser útil el crear botones dinámicos, es decir, botones en los que se utilice el mismo diseño y solo cambiamos el texto.

2.8. Amenazas a la seguridad de servidores

La seguridad en los servidores es tan importante como la seguridad de la red debido a que los servidores usualmente contienen una gran cantidad de información vital de la organización.

Si un servidor está comprometido, todos sus contenidos pueden estar disponibles para que un pirata los manipule o robe a su gusto. (Red Hat, 2005)

2.8.1. Servicios inutilizados

Una instalación completa contiene más de 1000 aplicaciones y bibliotecas de paquetes. Sin embargo, la mayoría de los administradores de servidores optan por no instalar todos los paquetes de la distribución, prefiriendo realizar una instalación base de paquetes, incluyendo varias aplicaciones de servidor.

Es común que los administradores de sistemas realicen una instalación del sistema operativo sin prestar atención a qué programas están siendo realmente instalados. Esto puede ser problemático puesto que se pueden instalar servicios innecesarios, configurados con sus valores por defecto y, posiblemente activados por defecto. Esto puede causar que servicios no deseados, tales como DHCP, o DNS, se

ejecuten en un servidor o estación de trabajo sin que el administrador se llegue a enterar, lo cual en consecuencia puede causar tráfico indeseado al servidor, o más aún, un camino de entrada potencial para cualquier acceso no autorizado.

2.9. Metodología

Los métodos a utilizar para el proceso de requerimientos serán los métodos empíricos, esto debido a que los datos que se obtendrán para plantear el desarrollo de la propuesta están basados en el estudio, planificación y de entrevistas. (Mizner, 2008-2015)

2.9.1. Método empírico

Este modelo empírico – analítico es un modelo de investigación científica, que se basa en la lógica empírica y que junto al método fenomenológico es el más usado en el campo de las ciencias sociales y en las ciencias descriptivas.

El término empírico deriva del griego antiguo (Aristóteles utilizaba la reflexión analítica y el método empírico como métodos para construir el conocimiento) de experiencia es decir, llevando a cabo el experimento o las pruebas. Por lo tanto los datos empíricos son sacados de las pruebas acertadas y de los errores. Su aporte al proceso de investigación es resultado fundamentalmente de la experiencia. Estos métodos posibilitan revelar las relaciones esenciales y las características fundamentales del objeto de estudio, accesibles a la detección, a través de procedimientos prácticos con el objeto y diversos medios de estudio, su utilidad destaca en la entrada en campos inexplorados o en aquellos en los que destaca el estudio descriptivo. (Mizner, 2008-2015)

- **Corriente Lógica**

La lógica empírica es la base del razonamiento empírico y por lo tanto del método empírico, su origen se deduce a través de la observación de las relaciones entre los objetos la convierte en la base ideal para las leyes del conocimiento. Su aparición provoca la definitiva separación entre las ciencias formales de las ciencias

empíricas, su paso a través de la historia provoca el descubrimiento de la lógica experimental que se mantiene en estos días.

- **Características**

- Es un método factico es decir se ocupa de los hechos que realmente acontecen
- Se vale de la verificación empírica: no pone a prueba la hipótesis mediante el mero sentido común sino mediante una cuidadosa contrastación por medio de la percepción
- Es auto correctivo y progresivo, la ciencia se construye a partir de la superación gradual de sus errores. No considera sus conclusiones finales, este método está abierto a la incorporación de nuevos conocimientos y procedimientos con el fin de asegurar un mejor acercamiento a la verdad

- **Clasificaciones**

Entre los métodos empíricos se encuentran:

- Experimental: Es el más complejo y eficaz de los métodos empíricos, por lo que a veces se utiliza erróneamente como sinónimo de método empírico.
- Algunos lo consideran una rama tan elaborada que cobra fuerza como otro método científico independiente con su propia lógica, denominada lógica experimental.
- En este método el investigador interviene sobre el objeto de estudio modificando a este directa o indirectamente para crear las condiciones necesarias que permitan revelar sus características fundamentales y sus relaciones esenciales bien sea:
- Aislando el objeto y las propiedades que estudia de la influencia de otros objetos
- Reproduciendo el objeto de estudio en condiciones controladas

- Modificando las condiciones bajo las cuales tiene lugar el proceso o fenómeno que se estudia

Así, los datos son sacados de la manipulación sistemática de variables en un experimento, una diferencia clara con el método empírico en general es que este además trata de considerar los errores de modo que una inferencia pueda ser hecha en cuanto a la casualidad del cambio observado. (Mizner, 2008-2015)

- **Pasos generales del Método Empírico – Analítico**

Existen varias maneras de formalizar los pasos de este método. De entre ellas se menciona:

- Forma Convencional
    a. Identificación de un problema de investigación
    b. Formulación de la hipótesis
    c. Prueba de hipótesis
    d. Resultados
- Formulación de Neil J. Salkind
    a. Formulación de un problema
    b. Identificar factores importantes
    c. Formulación de hipótesis de investigación
    d. Recopilación de información
    e. Probar la hipótesis
    f. Trabajar con la hipótesis
    g. Reconsideración de la teoría
    h. Confirmación o refutación

2.9.2. Metodología de la especificación de requerimientos

En esta fase se permite conocer las expectativas del usuario, se identifican los grupos de usuarios reales y posibles con su área de aplicación, se revisa la documentación existente, se analiza el entorno operativo y sus requerimientos de

procesado y se realizan entrevistas a los usuarios. Para este proceso existen técnicas formalizadas de especificación de requerimientos que concuerden con las siguientes:

Se identifican las entradas del problema, los resultados deseados o salidas y cualquier requerimiento o restricción adicional en la solución.

- **Obtener información acerca de lo que los usuarios desean**

Los requerimientos son el punto en donde el usuario y el proyecto se unen, dicha unión es necesaria para poder configurar un servidor que satisfaga las necesidades del usuario.

Si los requerimientos de enfocan a describir las necesidades del usuario, entonces es lógico la obtención de esta información de primera mano, esto por medio de entrevistas con el usuario o revisando la documentación que describa la manera que el usuario desea que funcione la solución de la propuesta.

Las necesidades de los requerimientos del usuario son cambiantes con el tiempo y cada cambio involucra un costo. Por eso es necesario tener la documentación original del usuario, así como cada revisión o cambio que se ejecute.

Como cada necesidad del usuario es tratada de forma diferente, es importante clasificar necesidades para saber cuáles de esas necesidades serán satisfechas por el proyecto.

- **Clasificar y estructurar requerimientos**

El clasificar a los requerimientos es una manera de organizarlos de mejor manera, esto debido a que no todos los requerimientos son tratados de la misma manera por sus características.

Los requerimientos pueden ser clasificados dependiendo de cada proyecto:

- Requerimientos del entorno

El entorno es todo lo que rodea a la aplicación podemos decir que pueden ser sistemas operativos, sistema de archivos, herramientas de seguridad.

- Requerimientos funcionales

Son los que describen lo que el proyecto debe de hacer, estos tipos de requerimientos se convierten en la lógica de las configuraciones necesarias.

- Requerimientos de desempeño

Estos requerimientos indican las características de desempeño que debe tener el servidor.

- Disponibilidad

Este tipo de requerimientos se refieren a la durabilidad, degradación, portabilidad y flexibilidad. Este tipo de requerimiento es importante en servicios de tiempo real.

- Entrenamiento

Estos requerimientos se enfoca en las personas que van administrar la solución propuesta, son importantes en el desarrollo ya que facilitan la introducción y aceptación del servicio en donde será implementado.

2.9.3. Método teórico analítico

- **FASE 1 Situación actual**

Actualmente, existe la necesidad de mejorar la administración de la información de la cooperativa, se destaca la incorrecta manipulación de la organización frente a la seguridad de acceso a los servidores virtualizados dejando

huecos informáticos que permiten el ingreso de personas no autorizadas sobre su información.

Para determinar la situación actual se recopilará la información existente sobre los servidores en la COOPERATIVA DE AHORRO Y CRÉDITO “29 de Octubre” para poder tener criterio del estado, funcionamiento y permisos de los diferentes servidores virtualizados.

Posteriormente se instalará un servidor demo el cual servirá para poder administrar la creación de usuarios y sus permisos de acceso a los servidores, con estos permisos se sabrán quienes manipulan la información dentro de la institución.
El acceso a los servidores de la cooperativa está integrado en varios puntos a nivel nacional, algunos de estos puntos se conectan directamente sin ningún control de acceso arriesgando la integridad de la información a nivel nacional.

Todos los puntos de la cooperativa “29 de Octubre” deben acceder a un sistema que se encuentra centralizado en Quito, las maquinas o usuarios que necesiten acceso al servidor, deberán ser creados por el administrador y este asignará permisos de acceso a la oficina virtual que se requiera. Una vez creado el usuario este ingresará sus datos de autentificación para ser validado por el servidor LDAP.

- **FASE 2 Rol y Servicio de los servidores**

Se llevará a cabo un análisis de cada servidor. Se identifica su rol, función y servicio, con lo cual se define una primera aproximación del diseño que se va a implementar.

La introducción de cambios en la administración de los servidores puede resultar costosa si no se hace una debida planificación, el manejo y acceso a la información de la cooperativa es sumamente delicada por lo cual el servidor demo de la implementación debe estar supervisado por parte de miembros de la organización.

Primero se realizará el levantamiento del diagrama de los servidores, con el fin de tener un punto de inicio del diseño a implementar. Lógicamente se analizará la configuración de los servidores para evaluar la operatividad de los mismos.

- **FASE 3 Análisis**

En lo que se refiere al análisis, se va a utilizar los estudios realizados anteriormente como punto de inicio, con la finalidad de entender la necesidad de centralizar la administración de servidores virtualizados basado en LDAP.

- **FASE 4 Implementación**

Con los resultados de la fase de análisis se considerarán aspectos como el fundamento de un modelo administrativo centralizado en la institución los cuales estarán acorde a las necesidades del proyecto. Se configurará el servidor base Centos, LDAP, Mysql, Php, y OpenLDAP, se realizará pruebas de aplicación, interfaz, facilidad de uso, navegación, configuración, seguridad, desempeño y de consultas lo cual garantizará el correcto funcionamiento del proyecto.

2.10. Herramientas de desarrollo

Centos V.6

Es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, operándose de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto, estable y fácil de instalar y utilizar.

Oracle VM VirtualBox

Es un software de virtualización para arquitecturas x86/amd64, actualmente es desarrollado por Oracle Corporation como parte de su familia de productos

de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como sistemas invitados, dentro de otro sistema operativo anfitrión, cada uno con su propio ambiente virtual.

OpenLDAP 2.4.42

Es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol LDAP desarrollada por el proyecto OpenLDAP.

MySql 5.6.21

Es un sistema de administración de base de datos relacionales y multiusuario diseñado para entornos de producción críticos.

Php 5.4.33

Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

Ext JS

Es una biblioteca de JavaScript para el desarrollo de aplicaciones web interactivas usando tecnologías como AJAX, DHTML y DOM. Fue desarrollada por Sencha. En la actualidad puede usarse como extensión para la biblioteca jQuery y Prototype, puede ejecutarse como una aplicación independiente.

CAPÍTULO 3

ANÁLISIS Y DISEÑO

3.1. Situación Actual

El modelo centralizado de administración será realizado para el administrador de la red de la Cooperativa “29 de Octubre”, tomando en cuenta que tendrá la potestad de asignar los usuarios y permisos de acceso a los servidores virtualizados.

El administrador de la red estará involucrado con el servidor centralizado desde una interfaz web el cual le permitirá administrar los usuarios, permisos y los accesos al servidor que se requiera o asigne.

Dicho modelo centralizado se basa en el protocolo LDAP, mismo que permitirá centralizar la administración, los usuarios son miembros de la cooperativa estos pueden ser cajeros, asistentes operativos, asesores. No todos tienen la necesidad de acceder a la información de los servidores, si fuese el caso se les asignará permisos solo de lectura mas no de escritura, esta decisión queda a cargo del administrador salvo mejor criterio de la dirección quien es responsable de las seguridades.

3.1.1. Perspectivas del producto

- La aplicación de administración proporcionará una herramienta que permite acceder y manipular la información en el servidor LDAP.
- Por otra parte integrará una interfaz web, la que permite al administrador un acceso y manipulación de datos de manera más intuitiva.

El producto a ser realizado estará sobre un dominio en un servidor virtualizado dentro de la cooperativa por lo que acceder a la interfaz administración

se puede dar desde cualquier lugar sin tener inconvenientes ya que el servidor estará en ejecución a cada momento.

3.2. Rol y Servicio de los servidores

Rol de Administrador

El administrador tiene acceso al servidor openLDAP desde un sitio web, en este sitio se ingresa y elimina usuarios, dichos usuarios creados también se les asigna permisos de acceso a los servidores u oficinas virtuales, se pone el ejemplo de que un cajero necesite ingresar a la información de clientes almacenados en el servidor de Quito su permiso de acceso fuese solo de lectura ya que necesita consultar y fijarse mas no modificar, en cambio para el otro caso un asistente operativo de la cooperativa necesita dar de baja a un cliente el cual se encuentra almacenado en el servidor de Quito si poseer de permisos de escritura lo que le permitirá eliminar al o los cliente , además la actualización de la información en el servidor será en tiempo real, lo que le facilitaría el ingreso de otro usuario al mismo tiempo que este ingresando al servidor proceder con las consulta ya con los datos actualizados en el servidor.

Rol de Usuario

El usuario puede ingresar al servidor virtual dependiendo del permiso que se le asignó al momento en el que fue creado por el administrador, puede acceder a un servidor o ambos si es el caso necesario.

Si el usuario ingresa con permisos de solo lectura podrá visualizar la información de los clientes almacenados en ese servidor, si los permisos son de lectura y escritura puede crear y eliminar los clientes si fuese el caso necesario, dichos ingresos o eliminaciones actualizaran automáticamente a la información del servidor.

3.3. Análisis de Servidores Virtualizados

3.3.1 Servidores Virtualizados de la Cooperativa

Como entidad financiera la Cooperativa de Ahorro y Crédito “29 de Octubre” posee varios servidores virtualizados los cuales son utilizados para diferentes propósitos, el servidor de correo zimbra esta implementado en Centos 5.0, este servidor administra todos los usuarios y grupos especiales de la cooperativa.

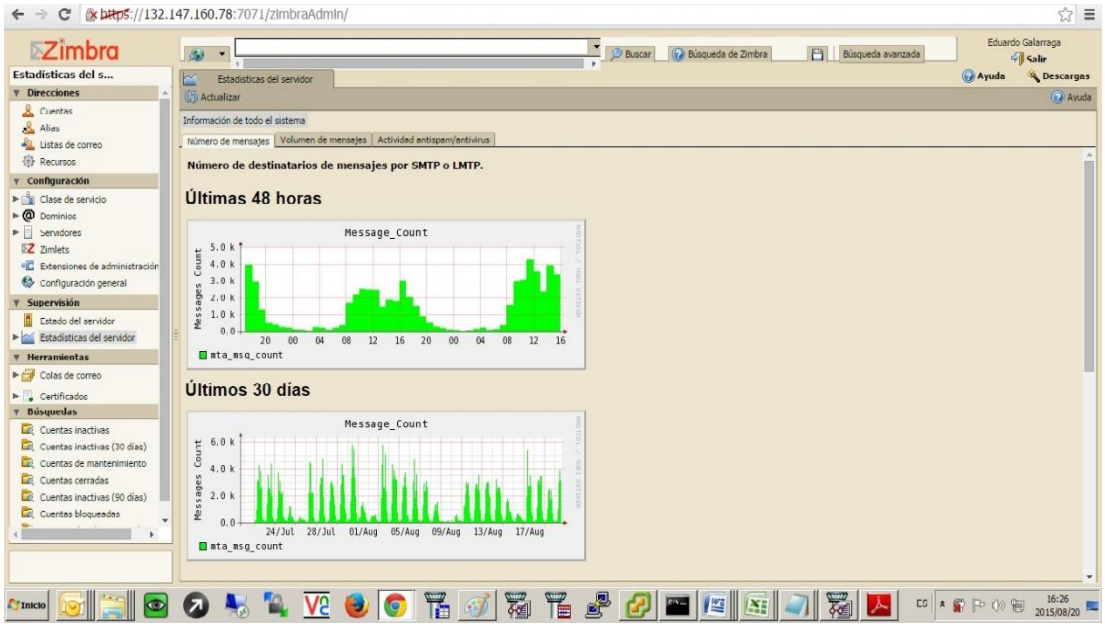

Figura 4 Servidor de Correo Zimbra

Como servidor de correo se puede administrar de manera ordenada grupos estratégicos que eviten estar escogiendo uno por uno los destinatarios de los grupos, también en el servidor se asigna permisos es decir una cuenta de correo puede estar con permisos de administrador lo cual le daría oportunidad de modificar cuentas, por aquello el administrador debe de controlar algún tipo de ingreso no autorizado, ya que esto generaría la violación de cuentas privadas en la organización.

Además se tiene un servidor de aplicaciones y de un servidor Bpm mismos que se encuentras virtualizados y son administrados de manera separada.

Para el servidor de aplicaciones se cuenta con diferentes ambientes, como lo son el ambiente de pruebas y el ambiente de producción ambos son virtualizados y uno es respaldo del otro.

En el servidor de aplicaciones ambiente de pruebas se realizan los cambios de librerías mediante FTP, una vez actualizadas las librerías y levantado todos los servicios se procede a realizar pruebas con el encargado de la administración, se prueba accesibilidad, tiempos de respuesta y manejo de la información sensible y delicada ya que son datos de cuentas económicas y algún error o una mala manipulación puede generar inconvenientes graves para el administrador del sistema.

Figura 5 Servidor de Correo Bpm

Los usuarios de la cooperativa que tienen acceso a los diferentes servidores virtualizados lo hacen con el objetivo de consultar la información mas no modificarla o eliminarla, el acceso es creado y dado por el administrador por cada servidor.

La ventaja de tener algunos servidores virtualizados en la cooperativa son que se los tienen agrupados en un mismo hardware lo que reduce tiempos en acceder a alguno de ellos, el proceso de las copias de seguridad (backup) es mucho mejor, ya

que se lo puede realizar periódicamente, en caso de que el hardware falle por calentamiento o por falta de espacio o de memoria.

Figura 6 Servidor de Aplicaciones

Dichos servidores antes mencionados están bajo un dominio de la Cooperativa, el servidor LDAP a ser implementado va a estar igual bajo un dominio pero bajo un ambiente demo, es decir será administrado para pruebas locales antes de poder implementarlo en otro ambiente, esto debido a que las políticas de procesos de seguridad de la información en la institución son de carácter privado.

Por ser una entidad financiera la gestión de riesgos es muy alta, se debe cuidar la información interna de manera total.

3.3.2. Seguridad de la Información

Se debe decir que el manejo de información o los accesos no autorizados estan controlados y regidos por la cooperativa, toda información manejada y procesada sobre algun activo, usuario, proceso o aplicacion debe tener la autorización por las coordinaciones y direcciones encargadas de salvagaurdarla.

Debido a que la información que se encuentra en los servidores virtualizados de la la cooperativa es manejada con privacidad y confidencialidad para evitar cualquier manipulacion no autorizada, el modelo a ser implementado sera un demo que demuestra como se autentifica el usuario aplicando el protocolo LDAP, dicho demo tendra acceso una interfaz web de nuestro servidor openLDAP el cual administra a los usuarios y sus accesos a los otros servidores virtuales que para el proyecto será realizado con 2 servidores virtuales de pruebas que tambien seran llamadas oficinas virtuales.

La implementación de modelo centralizado de claves como se menciona antes sera sobre servidores de pruebas de la cooperativa, lss cuales son permitidos el acceso teniendo en cuenta la supervision de un miembro de la cooperativa el cual se hizo presente en todo el proceso del proyecto, desde el levantamiento de información requerida, analisis, permisos, accesos, implementación llegando hasta las respectivas pruebas realizadas sobre el modelo propuesto.

3.3.3. Distribución de Sistema Operativo en el Servidor LDAP

Analizando los diferentes servidores virtualizados que se encuentran en la entidad financiera, el modelo basado en LDAP a ser implementado y centralizado toma como distribución de sistema operativo a Centos, esto debido a que sobre este Sistema Operativo se encuentran implementados algunos servidores de la cooperativa.

3.3.4. Función y Rol del Servidor LDAP

La función dentro del servidor LDAP es de administrar a los usuarios y sus permisos al servidor, aplicando los conceptos de LDAP y de su estructura, cada rama o nodo del directorio del sistema de ficheros LDAP tiene como mínimo un atributo único, el cual permite diferenciar los unos atributos de los otros.

El modelo de LDAP está basado en varias entradas, una entrada es una colección de atributos que tienen un único y global Nombre Distinguido el cual se utiliza para referirse a una entrada. Cada atributo de una entrada posee un tipo y uno o más valores.

Los tipos son normalmente palabras nemotécnicas, como “cn” para el tipo de nombre común, o “mail” para una dirección de correo.

El rol del servidor LDAP es de centralizar en un solo lugar la autentificación, lo cual nos da como beneficios un único punto de administración, con menos posibilidad de errores, de igual manera disminuye los datos duplicados por todas las partes o por las ramas del árbol LDAP, además da la facilidad de realizar backups de manera rápida bajo cierto tiempo planificado.

3.4. Diseño del modelo de administración centralizado

3.4.1. Almacenamiento de la Información en el Servidor LDAP

Las entradas están organizadas en una estructura jerárquica como ya lo mencionamos tipo árbol. Cada rama o nodo de datos se lo denomina “entrada”. Cada entrada tiene una denominación, que se forma de la concatenación de los nombres distinguidos relativos, desde las entradas “padre” hasta llegar a la entrada “raíz” del árbol.

LDAP define operaciones para interrogar y actualizar el directorio. Provee operaciones para añadir y borrar entradas del directorio, se utiliza para buscar información almacenada en el directorio. Las operaciones de búsqueda de LDAP permiten buscar entradas que concuerdan con algún criterio especificado por un filtro de búsqueda. La información puede ser solicitada desde cada entrada que concuerde con dicho criterio.

Para el modelo el árbol LDAP queda estructurado de la siguiente manera:

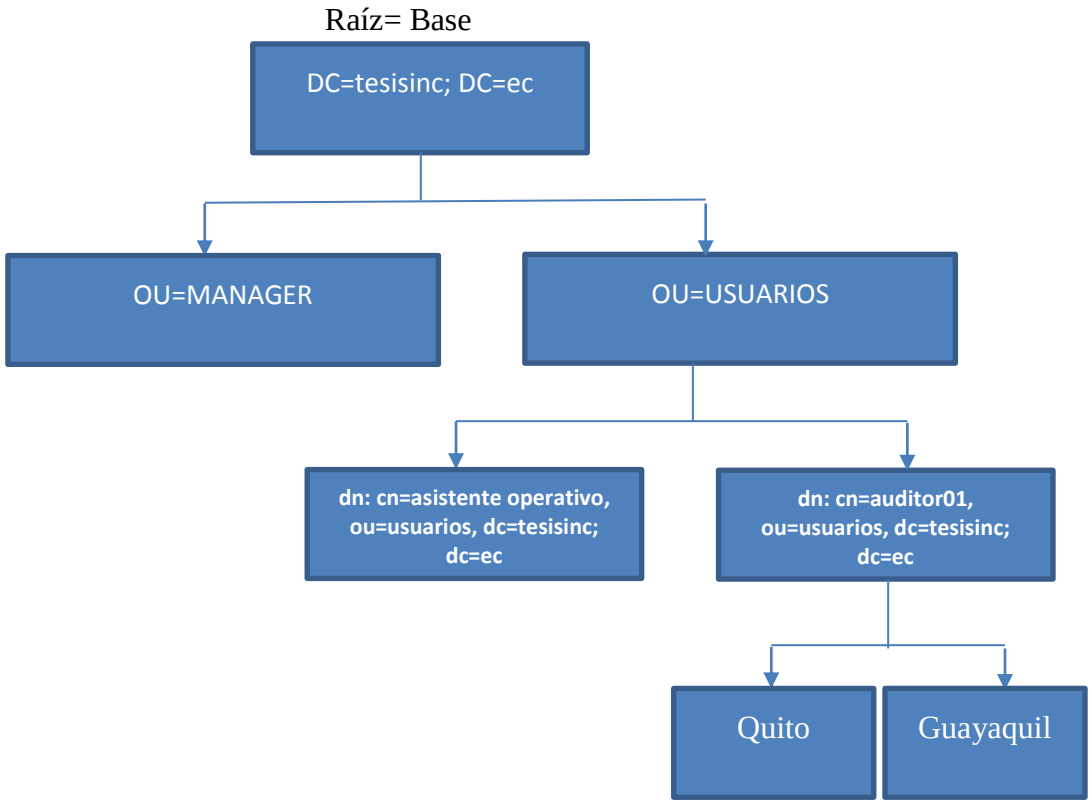

Figura 7 Estructura de los objetos del directorio LDAP

En donde:

dc=tesisinc, dc=ec	es nuestra raiz
ou= Usuarios	es nuestro grupo
cn=Asistente Operativo	es nuestro usuario
o= Quito	es nuestra organización (Servidor virtual)

en la cual la rama quedará de la siguiente manera:

o=Quito, cn=Asistente Operativo, ou= Usuarios, dc= tesisinc, dc=ec

La estructura de LDAP se puede modificar dependiendo de las necesidades a ser utilizadas, si es fuese el caso uno o mas grupos el árbol se puede extender y de igual

manera si existiese la necesidad de crear mas nodos se lo puede realizar acorde a lo que se requiera manejar y manipular.

El modelo funcional de LDAP describe como acceder a los datos en el directorio a través de operaciones que se pueden llevar a cabo usando el protocolo LDAP.

Las operaciones del modelo funcional de LDAP están divididas en tres grupos:

- Las operaciones de consulta, que permiten realizar búsquedas en el directorio y la recuperación de datos del mismo.
- Las operaciones de actualización, que permiten agregar, borrar, renombrar o cambiar entradas en un directorio.
- Las operaciones de autentificación y control, que permiten a los clientes ser identificados ante el servidor de directorios y por tanto controlar ciertos aspectos de la sesión, el restringir o permitir el acceso a ciertas entradas.

Además de estas operaciones, el protocolo LDAP define una manera para agregar nuevas operaciones que permitan hacer búsquedas o recuperaciones de datos especializados. Estas operaciones se llaman las operaciones extendidas de LDAP.

3.4.2. Operación del Servidor LDAP

La forma de operar del servidor LDAP empieza cuando un cliente inicie sesión en el servidor desde aquí el cliente se autentifica y envía la solicitud al servidor de directorio este emite una respuesta solo bastará con crear las cuentas de usuario y grupos de usuarios en el servidor LDAP para que los usuarios puedan hacer uso del sistema y de sus servicios desde cualquier punto de la red. Como resultado se centraliza la administración de usuarios en un único punto.

La operación primaria con la que se puede probar al servidor LDAP es Bind, este es el proceso de "conectar" enviando un usuario con su contraseña y esperar la respuesta de autenticación.

La manera por la cual se mueven los datos por el servidor LDAP, se llama Ldif (LDAP Data Interchange Format), aquí los datos son movidos desde el cliente al servidor y viceversa utilizando el dialecto propio de LDAP.

A continuación se ve el modelo por el cual los usuarios de la cooperativa van a consultar al servidor LDAP si están autentificados y si tienen acceso a uno o más servidores esto depende de su privilegio de ingreso.

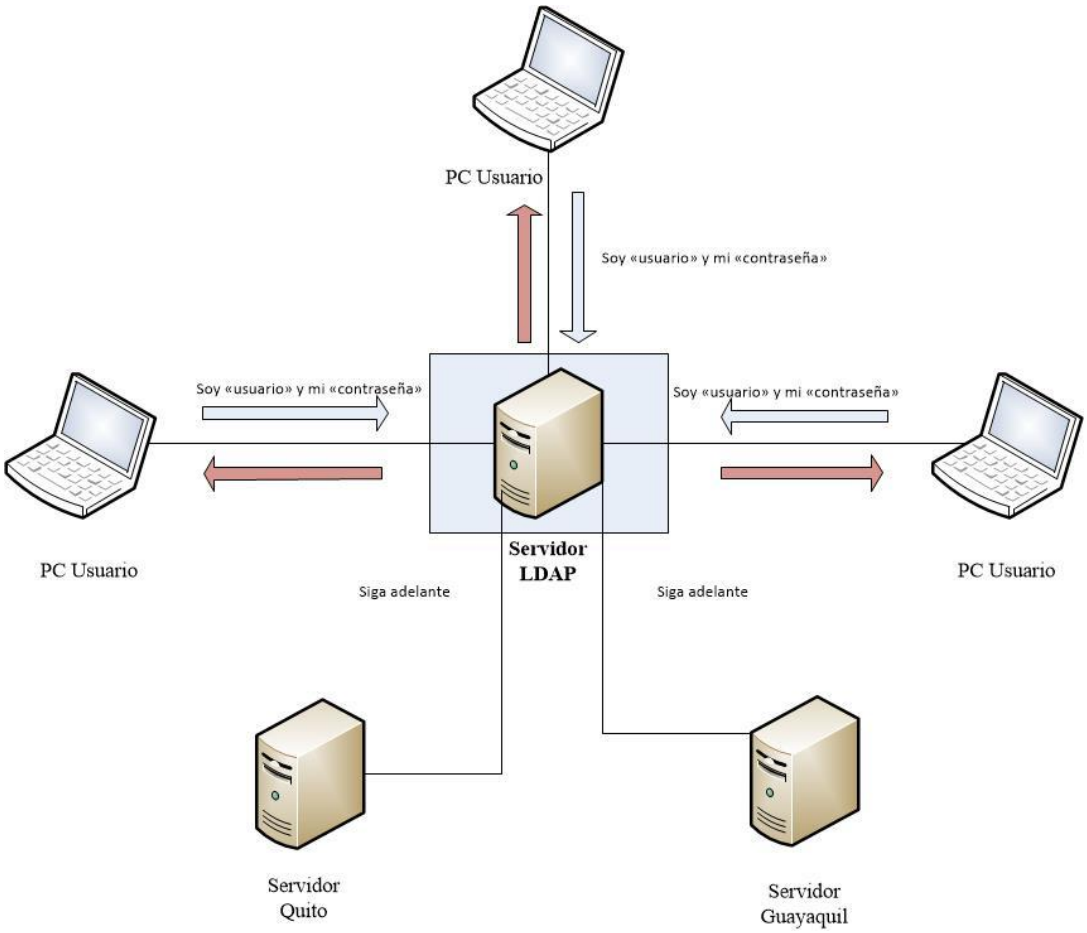

Figura 8 Diseño Propuesto del Modelo Centralizado de Autentificación

Modelo Centralizado de Autentificación

En el modelo se realiza la pregunta al servidor LDAP desde cualquier punto mediante el acceso web de administración.

La respuesta del servidor LDAP consiste en autentificar nombre de usuario y de contraseña del mismo, si la respuesta es correcta puede ingresar al servidor especificado sino la respuesta será de no autorizado el acceso.

Al especificar el servidor se le especifica el tipo de permiso que tiene el usuario lo cual le permita acceder a la información de dicho servidor.

Cabe decir que se puede acceder a cualquier equipo que se encuentre dentro de la red, siempre y cuando este especificado en la estructura LDAP por ejemplo:

dn: cn=Asistente Operativo, ou= Usuarios, dc= tesisinc, dc=ec
cn: Asistente Operativo
ccn: Contraseña Asistente
domainname: tesisinc.ec
ipaddress: 132.140.160.79:8080
adminmail: admin@manager.es
service: pop3
service: http
service: imap

Por seguridades de la entidad se debe tener claro que el acceso a un servidor o equipo en la red debe ser acompañada por las configuraciones de seguridad las cuales evitaran ataques de terceros.

Es decir si un nuevo empleado entra a la organización normalmente se le debe dar accesos y varios recursos dependiendo de las responsabilidades que vaya a ejercer, talvez se le puede dar acceso a uno o mas equipos de la cooperativa como administrador la responsabilidad de verificar los permisos debe ser de manera rapida.

Para esto el administrador se tiene que ayudar de los procedimientos de la organización el cual le notificará el ingreso del nuevo de usuario.

Seguido de este la supervision del nuevo usuario al momento de la creacion de su cuenta y sus permisos respectivos.

Es conocido el hecho de que habrá usuarios que ingresen o dejen la organización, en cualquier caso, es vital que se le informe de la situación para que así pueda tomar las acciones adecuadas.

Como mínimo, las acciones apropiadas deben incluir:

- Inhabilitar el acceso del usuario a todos los sistemas y recursos relacionados (usualmente mediante el cambio o bloqueo de la contraseña)
- Hacer una copia de seguridad de los archivos del usuario, en caso de que contengan algo importante
- Coordinar el acceso del usuario

El propósito del modelo de seguridad de LDAP es proteger la información de un directorio contra los accesos no autorizados.

La autentificación de un cliente LDAP en el servidor es parte de la seguridad de un directorio, el modelo de autentificación forma parte de este. Otra parte del modelo de seguridad de LDAP la conforman los controles de acceso, que son la forma en la cual se especifican los privilegios que poseen algunos usuarios, después de ser autentificados con éxito.

Es claro que los tipos de privilegios básicos a asignar a clientes sobre determinados DN de un directorio son escritura y/o lectura.

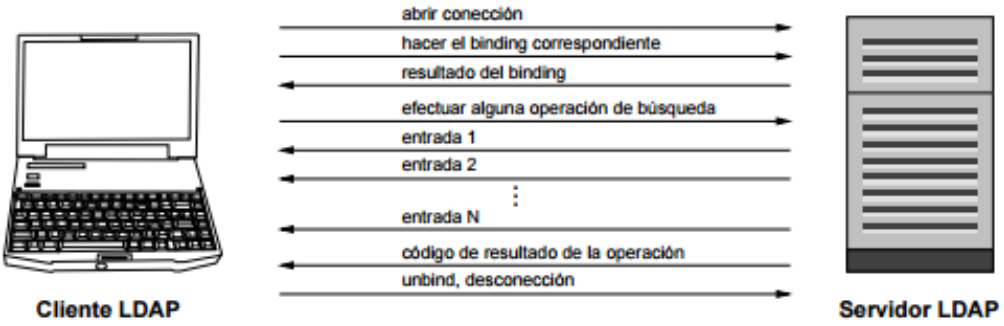

Figura 9 Cliente efectuando búsqueda en el Servidor LDAP

3.5. Caracterisiticas de OpenLDAP

OpenLDAP es una implementación libre y de código abierto del protocolo LDAP, desarrollada por el proyecto OpenLDAP.

OpenLDAP se encuentra compuesto por 3 componentes:

- SLAPD: Es el servidor DSA y sus herramientas utilitarias
- Bibliotecas que implementan el protocolo LDAP y el Backend de almacenamiento y/o interacción con los datos
- Programas cliente.

Un DSA se compone de un Front-End que gestiona las conexiones y el procesamiento de las soluciones LDAP y un Backend que maneja exclusivamente el tratamiento de los datos; la arquitectura de OpenLDAP es de modular y le permite interactuar con varios y diversos backends.

3.6. Directorio LDAP

Para poder levantar el directorio OpenLDAP en el servidor se debe seguir los siguientes pasos:

3.6.1. Descargar e instalar OpenLDAP

Para descargar OpenLDAP se debe ingresar a la dirección web www.openLDAP.com e instalar según la documentación o instalar un paquete de binarios pre compilados.

En dicha dirección web se encuentran tutoriales, manuales y ejemplos de código libre los cuales pueden ayudar a cualquier necesidad.

3.6.2. Configuración del Servidor OpenLDAP

OpenLDAP tiene un usuario principal llamado "rootdn" (Root Distinguished Name o Nombre Distinguido de Root) el cual está definido dentro de la aplicación. Al contrario que el usuario root clásico de Unix, al usuario rootdn se le deben asignar los permisos adecuados. El usuario principal solo se puede utilizar en el contexto de la configuración y también en la definición del directorio.

En este caso un usuario puede autenticarse a sí mismo como rootdn con la contraseña usada en la configuración y la contraseña basada en el árbol o estructura de LDAP.

Las contraseñas de usuario para propósitos de verificación se pueden almacenar como test en claro o aplicando un hash. Se dispone de varios algoritmos hash, sin embargo no se recomienda el uso de algoritmos débiles.

Una vez descargado el paquete comprimido de LDAP se lo descomprime en la carpeta específica y se levanta las configuraciones que contiene el paquete, utilizamos la siguiente línea de comandos.

tar zxvf openLDAP-2.4.42.tgz

Ahora es necesario editar la configuración LDAP del servidor en /etc/openLDAP/slapd.conf. El fichero slapd.conf que se muestra es de las fuentes originales de openLDAP.

Archivo **/etc/openLDAP/slapd.conf**

```
include /etc/openLDAP/schema/core.schema
include /etc/openLDAP/schema/cosine.schema
include /etc/openLDAP/schema/inetorgperson.schema
include /etc/openLDAP/schema/nis.schema
include /etc/openLDAP/schema/misc.schema

pidfile /var/run/openLDAP/slapd.pid
argsfile /var/run/openLDAP/slapd.args

 ## ## ServerID se utiliza cuando haya réplicas
serverID 0
loglevel 0

## ## Sección de Certificados y SSL
TLSCipherSuite normal
TLSCACertificateFile /etc/openLDAP/ssl/LDAP.crt
TLSCertificateFile /etc/openLDAP/ssl/LDAP.pem
TLSCertificateKeyFile /etc/openLDAP/ssl/LDAP.key
TLSVerifyClient never

## ## Controles de acceso
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
   by self write
   by users read
   by anonymous read

## ## Definición de la base de datos
database bdb
suffix " dc=tesisinc,dc=ec"
checkpoint 32 30
rootdn "cn=Manager, dc=tesisinc,dc=ec "
## ## Contraseña para root generada previamente con la orden slappasswd
rootpw "{SSHA}EzP6I82DZRnW+ou6lyiXHGxSpSOw2XO4"
directory "/var/lib/openLDAP-data"
```

```
index objectClass eq

## ## Sincronización (desde otro servidor LDAP)
syncrepl rid=000
  provider=LDAP://LDAP2.genfic.com
  type=refreshAndPersist retry="5 5 300 +"
  searchbase=" dc=tesisinc,dc=ec "
  attrs="*,+"
  bindmethod="simple"
  binddn="cn=LDAPreader, dc=tesisinc,dc=ec "
  credentials="LDAPsyncpass"

index entryCSN eq
index entryUUID eq

mirrormode TRUE

overlay syncprov
syncprov-checkpoint 100 10
```

Se edita el fichero **/etc/openLDAP/LDAP.conf**, este fichero pertenece al cliente de LDAP

Se inicia el servidor LDAP.

/etc/rc.d/LDAP start
/usr/local/libexec/slapd

3.6.3. Administración de OpenLDAP

Una vez instalado y configurado el servidor OpenLDAP, lo siguiente que deberá hacer es la del diseño de la estructura y la introducción de datos en el directorio, el servidor debe almacenar usuarios para su autentificación, crear una estructura que inicie de la base del directorio LDAP, para almacenar dicha información.

Para acceder al directorio LDAP se tiene dos maneras, la primera es de trabajar con comandos y con archivos ldif para crear y eliminar elementos del directorio LDAP, la segunda forma es más práctica y es la de utilizar un explorador de directorios LDAP.

Existen varios exploradores LDAP tanto pagados como libres, la que se utilizara en este proyecto es phpLDAPadmin.

Para instalar phpLDAPadmin, al igual que otras aplicaciones web, se debe descargarla desde http://phpLDAPadmin.sourceforge.net/ y descomprimirla dentro del Root de apache, dentro de la carpeta **/var/www/phpLDAPadmin**.

wget
http://nfsi.dl.sourceforge.net/sourceforge/phpLDAPadmin/phpLDAPadmin-1.1.0.7.tar.gz

tar -zxvf phpLDAPadmin-1.1.0.7.tar.gz

sudo cp -R phpLDAPadmin-1.1.0.7 /var/www/html/phpLDAPadmin

sudo cp /var/www/html/phpLDAPadmin/config/config.php.example /var/www/html/phpLDAPadmin/config/config.php

Para ejecutarlo, se requiere tener un servidor web con php y un servidor mysql con una base de datos para el phpLDAPadmin**,** dirigiéndose a la carpeta anterior en donde se descomprimió, después se debe ir a la dirección url http://ip_del_servidor_web/phpLDAPadmin/ el navegador se posesionará sobre la página principal de la aplicación.

Figura 10 Instalación de phpLDAPadmin

A continuación de este paso se debe de dar clic en la palabra conectar seguido de la identificación con el usuario principal.

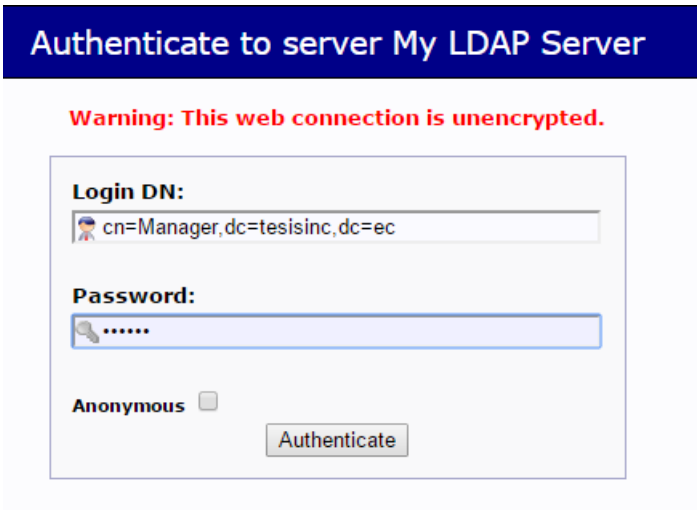

Figura 11 Autentificación de servidor LDAP

CAPÍTULO 4

IMPLEMENTACIÓN CENTRALIZADA Y PRUEBAS

4.1. Implementación

4.1.1. Instalación de Sistema Base Centos

CentOS es una distribución de Linux basada en Red Hat EnterpriseLinux. Cada versión de CentOS es mantenida durante 7 años. Las versiones nuevas son liberadas cada 2 años y actualizadas regularmente para el soporte de hardware nuevo.

La instalación se realizara sobre una máquina virtual en este caso se utilizará Oracle VM Virtualbox.

Figura 12 Instalación CentOS

La versión del CentOS que se va a instalar es la 6.4 la cual se puede descargar desde la página oficial en esta indicara si se desea verificar la integridad del medio de instalación

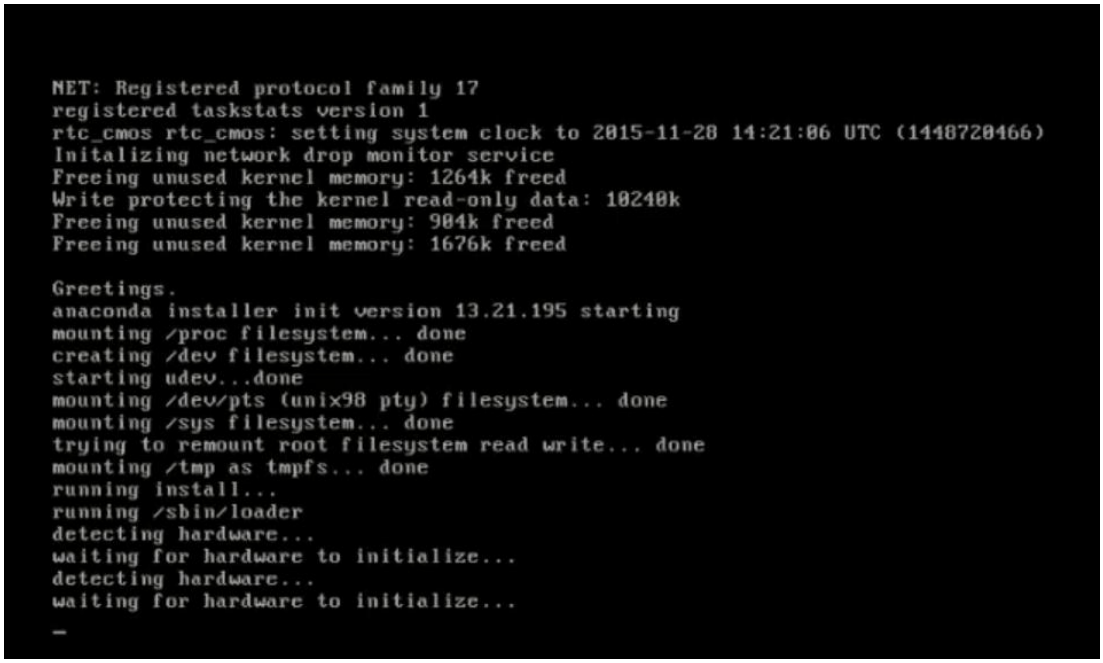

Figura 13 Inicialización del kernel

Figura 14 Pantalla de verificación

El asistente para la instalación de CentOS pedirá aceptar o no verificaciones de integridad, particiones, capacidad del equipo o limitaciones para seguir con el proceso, de igual manera en el proceso de instalación se reiniciara la instalación.

En la siguiente pantalla se debe seleccionar el idioma con el que se proseguirá con la instalación.

Figura 15 Selección de Idioma

Se define el nombre de anfitrión en el siguiente el formato: nombre.dominio.tld. Este preferiblemente debe estar resuelto en un servidor DNS.

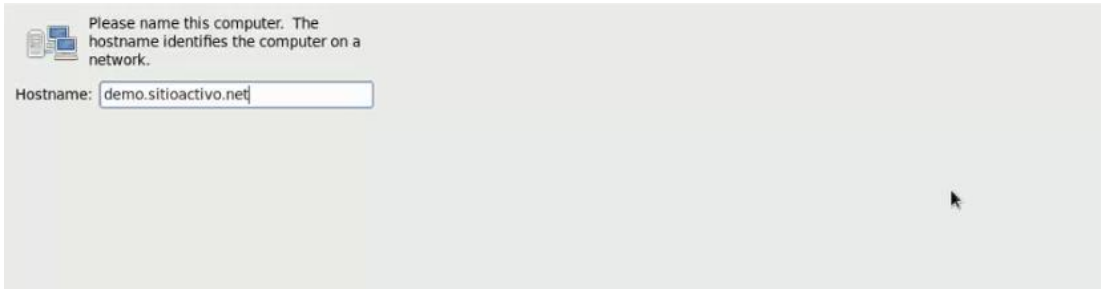

Figura 16 Nombre de Anfitrión

A continuación se deberá seleccionar la zona horaria que corresponda la localidad, para esto se dará clic sobre cualquier punto en el mapamundi.

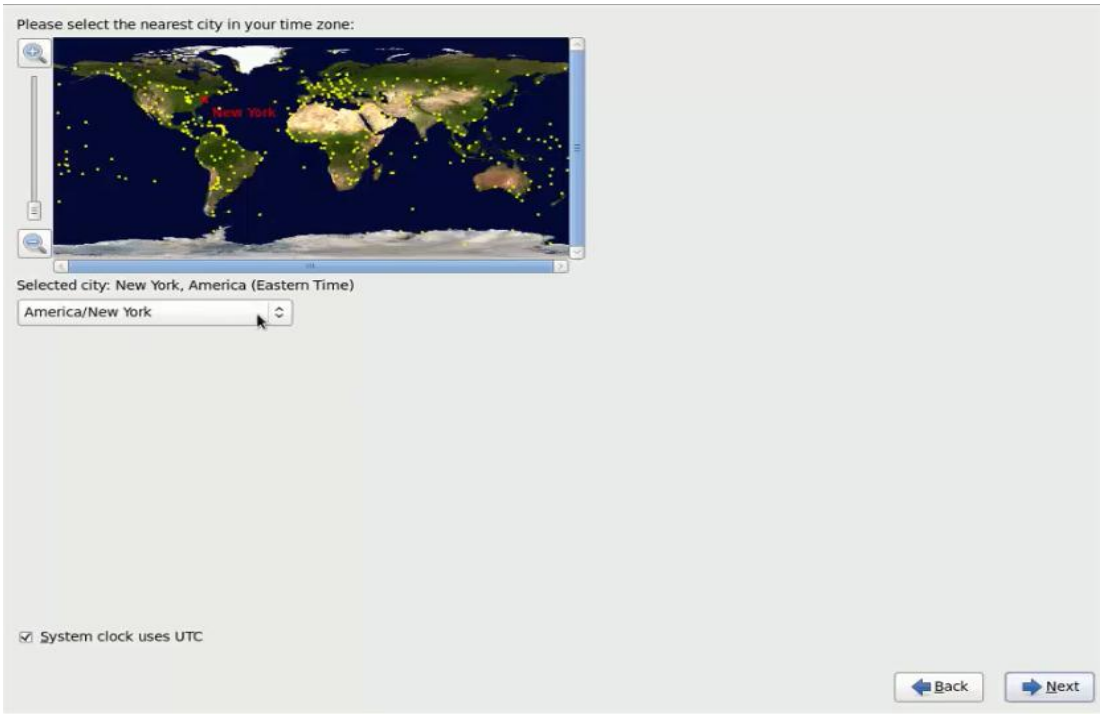

Figura 17 Selección de zona horaria

Ahora se debe definir y confirmar la contraseña para root, cuenta que será utilizada para la administración del sistema

Figura 18 Definición de contraseña para el root

En la siguiente pantalla se debe elegir las opciones para crear las particiones en el disco duro. Salvo que se necesite crear un diseño personalizado, las opciones que aparecen en pantalla indican lo siguiente:

- Usar todo el espacio.- Eliminará cualquier partición de cualquier otro sistema operativo presente y creará de forma automática las particiones necesarias.
- Reemplazar sistema(s) Linux existente(s).- Sólo eliminará todas las particiones Linux existentes y creará de forma automática las particiones necesarias.
- Achicar el sistema actual.- Cambiará el tamaño de las particiones existentes de otros sistemas operativos como Windows, haciendo el espacio necesario para poder instalar un diseño predeterminado de particiones Linux.
- Usar espacio libre.- Creará de forma automática las particiones necesarias en el espacio disponible, basándose sobre un diseño predeterminado.
- Crear un diseño personalizado.- Permitirá elegir las particiones estándar o volúmenes lógicos, que se requiera.

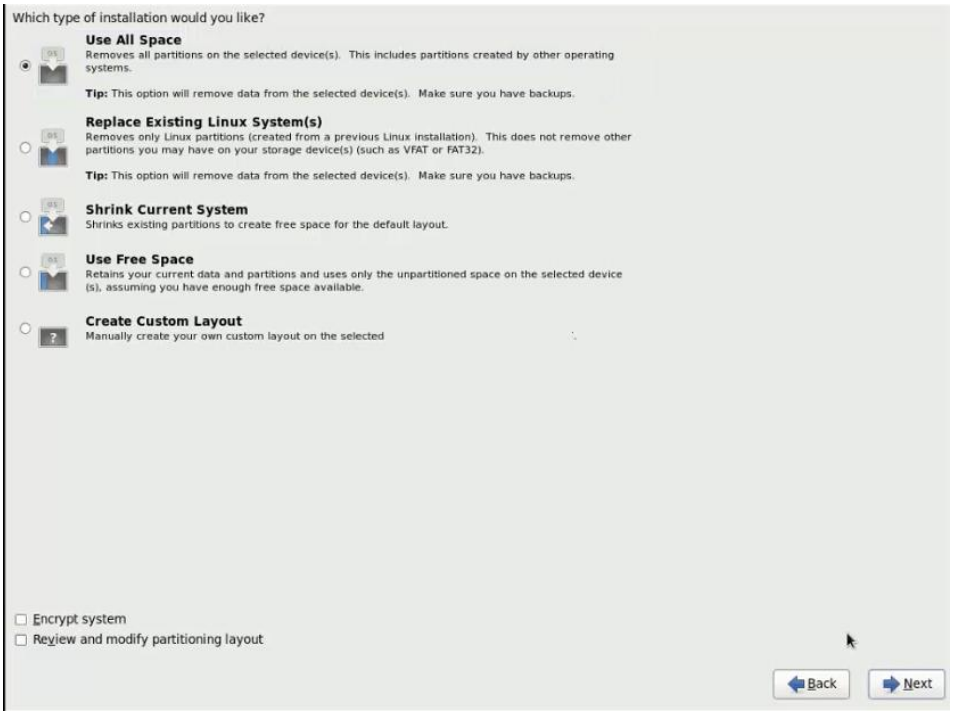

Figura 19 Particiones de disco duro

En la próxima pantalla se especifica la casilla de opción denominada Personalizar ahora con la cual se puede elegir grupos específicos de paquetes.

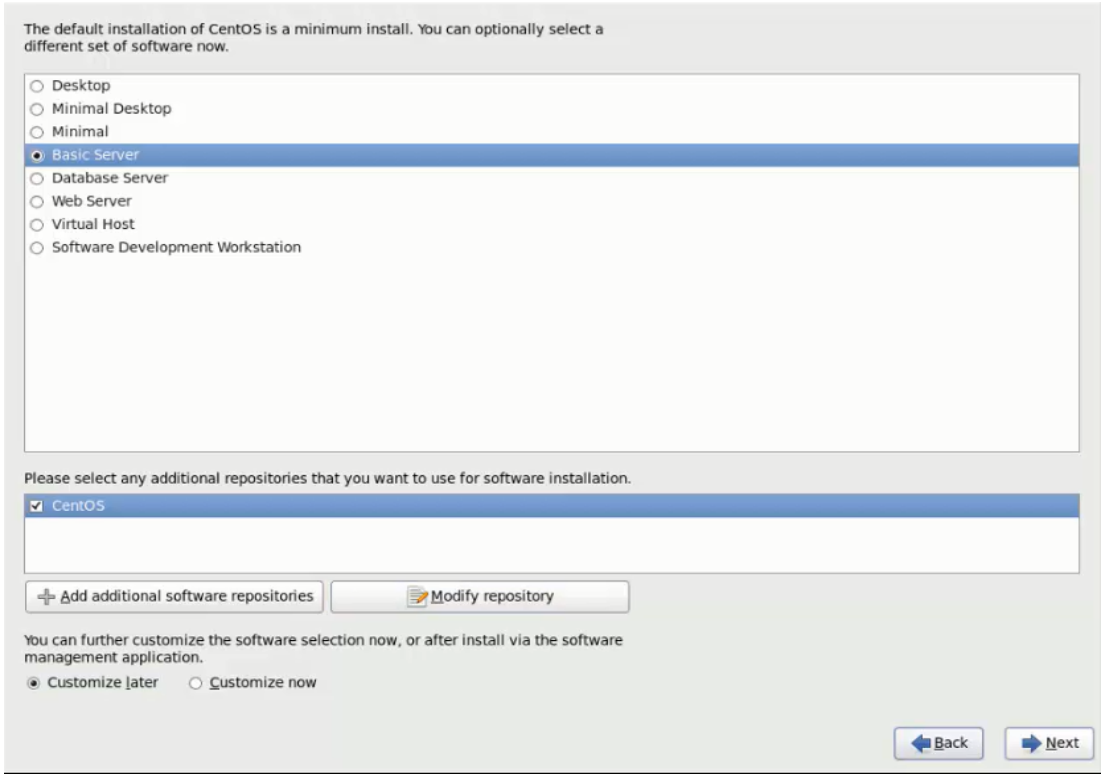

Figura 20 Tipo de Servidor

Una vez realizadas las configuraciones se reiniciará el servidor virtual

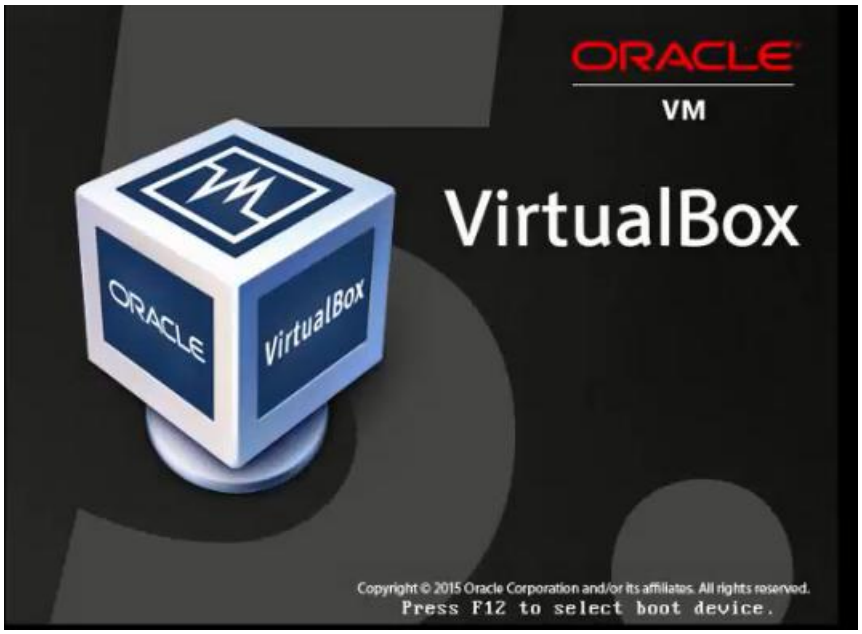

Figura 21 Servidor Virtual reiniciando

Se podrá seleccionar cualquier grupo de paquetes que sirva para las necesidades particulares.

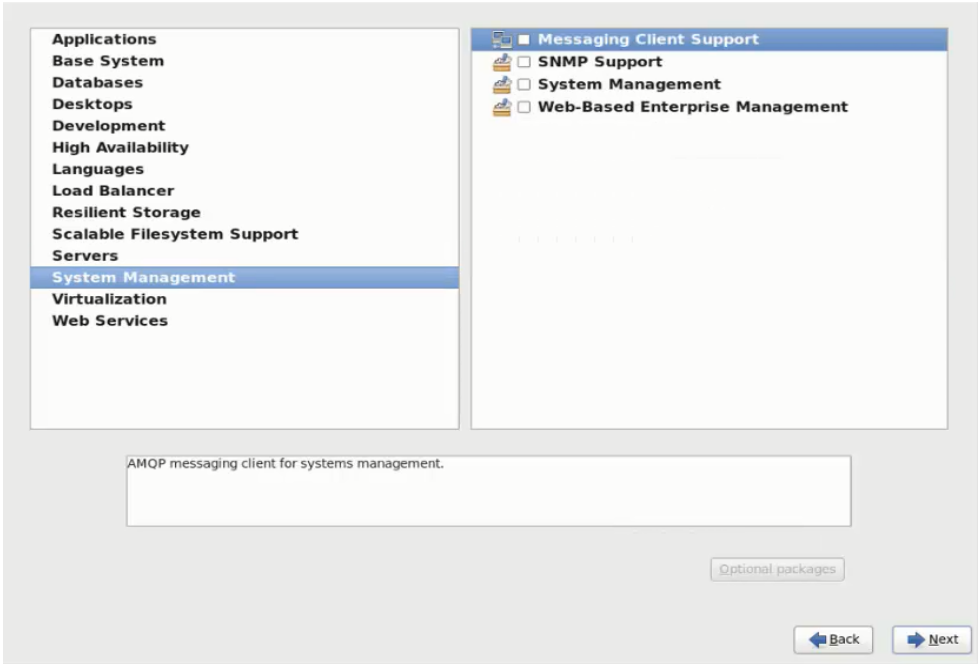

Figura 22 Grupo de paquetes a instalar

Haciendo clic sobre el botón siguiente se estará confirmando que se terminó de seleccionar los grupos de paquetes, esto dará inicio el proceso de instalación de paquetes. El tiempo que demore el proceso depende de la cantidad de grupos y paquetes que se haya seleccionado.

Figura 23 Inicialización de instalación

Una vez culminado el tiempo de todo el grupo de paquetes lo queda es reiniciar la instalación.

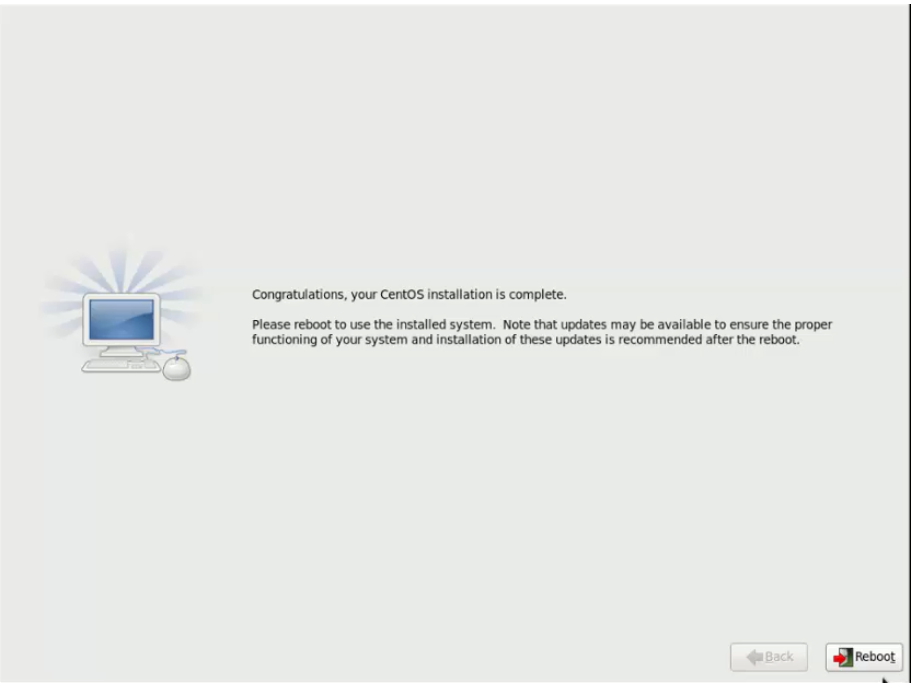

Figura 24 Reinició de Instalación

Una vez terminada la instalación de CentOS 6 existen varios ajustes que se recomienda realizar dependiendo de las necesidades. Todos los procedimientos se los debe realizar como root.

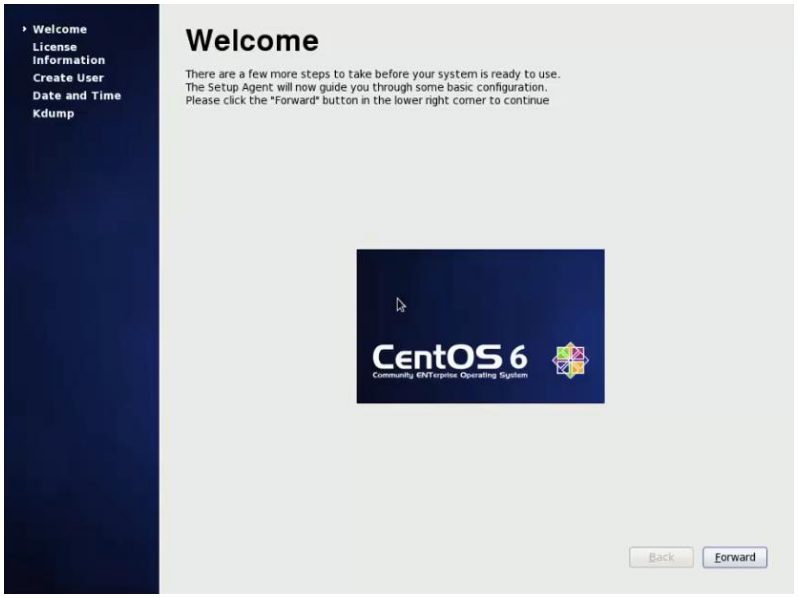

Figura 25 Pantalla de bienvenida de CentOS

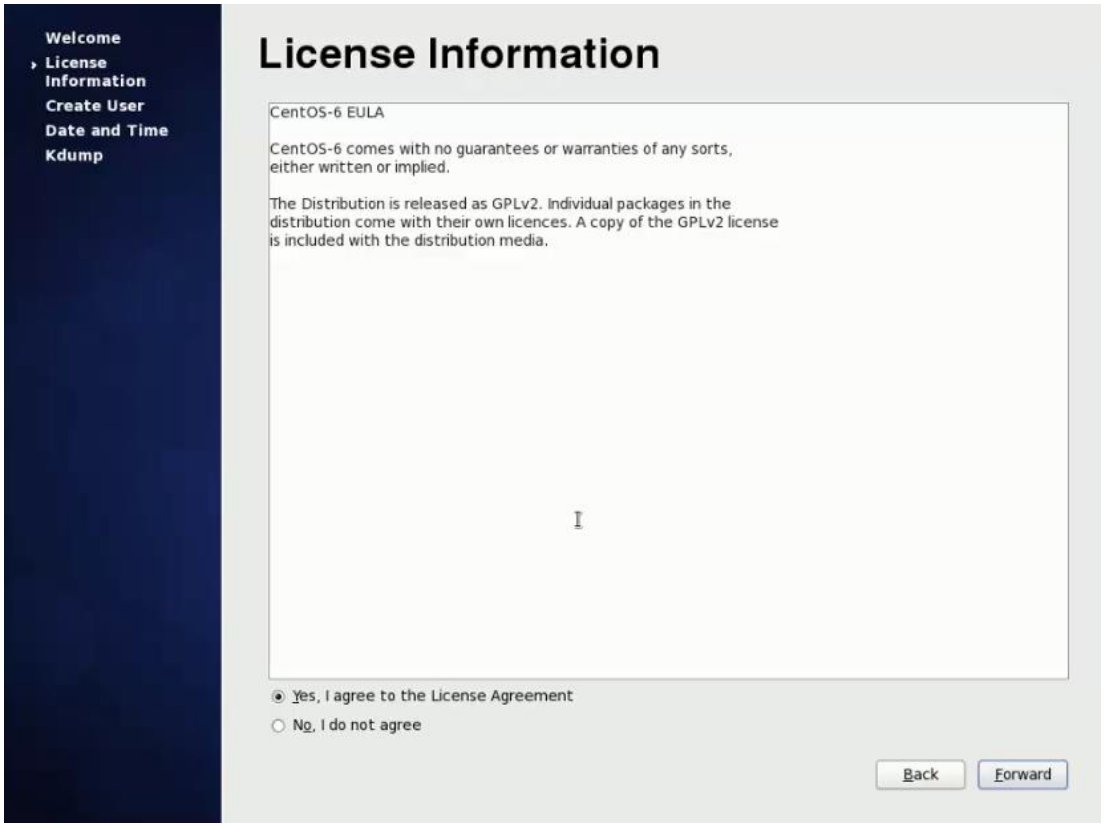

Figura 26 Información de licencia

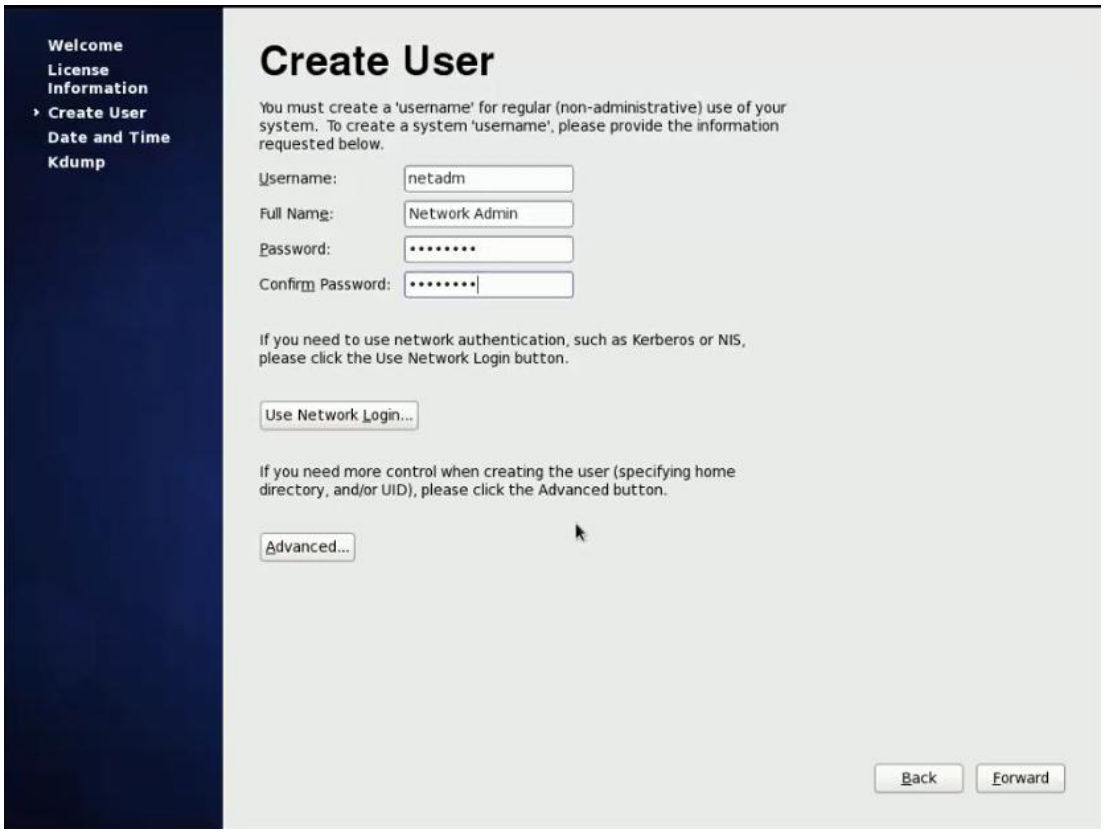

Figura 27 Creación de Usuario

4.1.2. Configuración del Sistema Base

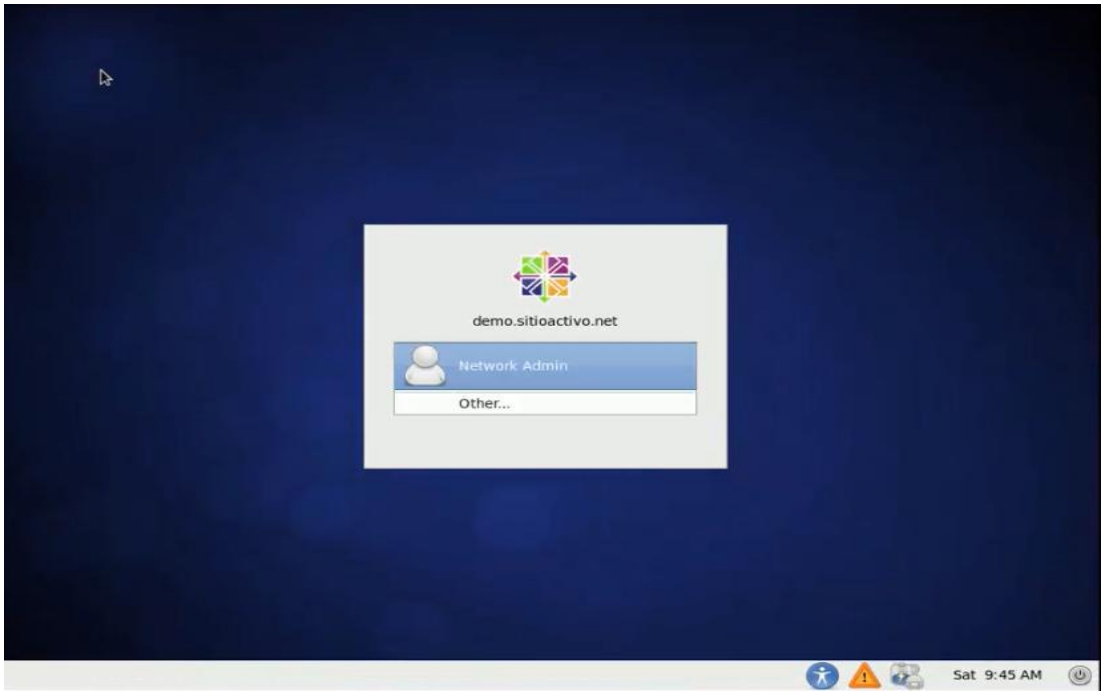

Figura 28 Pantalla de Acceso

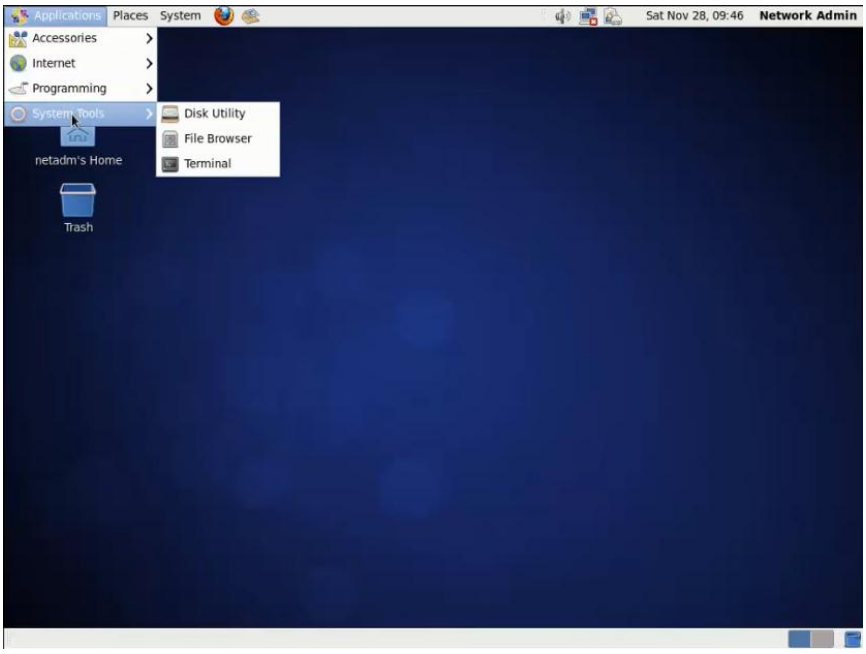

Figura 29 Escritorio de CentOS

Una vez ya instalado se debe configurar el fichero /etc/inittab, este archivo le indica al sistema en qué nivel de ejecución debe iniciarse. El nivel de ejecución 1 es

el mono-usuario, los niveles 2 y 3 son los niveles multi-usuario en modo consola, el nivel 5 es el que arranca las X, y es el que por defecto arranca el sistema. Los niveles de ejecución 0 y 6 son especiales por que el sistema no puede permanecer en ellos uno lo cierra y el otro lo reinicia.

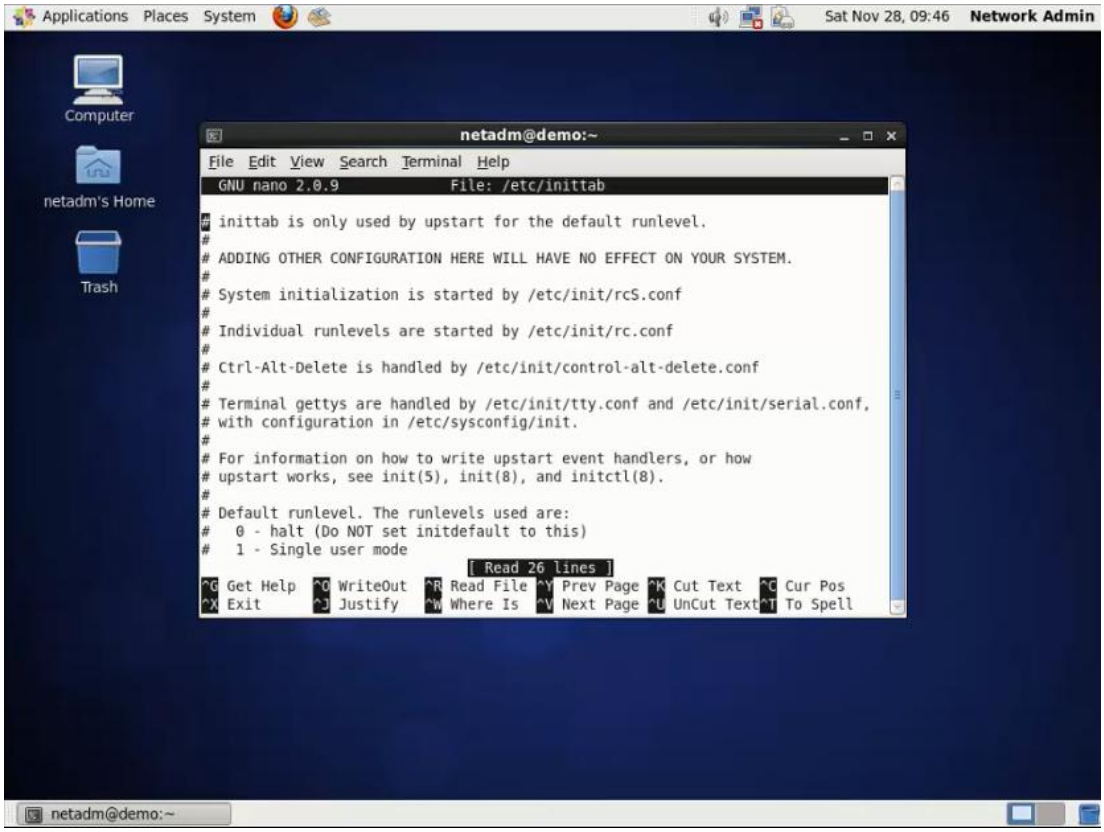

Figura 30 Modificación archivo /etc/inittab

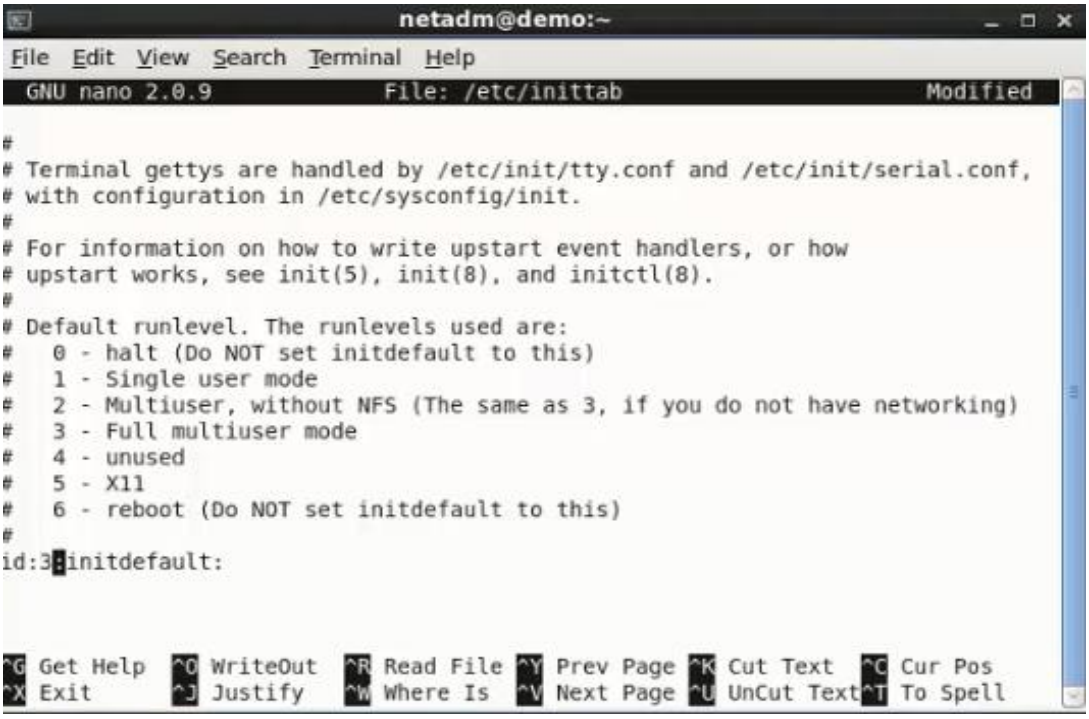

Figura 31 Cambio a nivel multi-usuario

Figura 32 Levantamiento de servicios

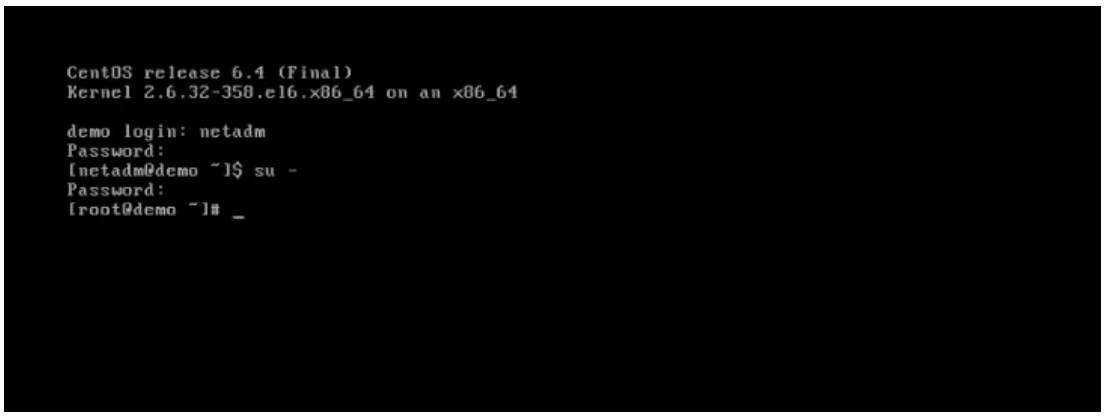

Figura 33 Acceso modo consola

4.1.3. Instalación de Mysql-5.6.21

Una vez instalado y configurado el servidor se procede a instalar MySQL que es un DBMS (DataBase Management System) o sistema de gestión de base de datos SQL multiusuario y multihilo con licencia GNU/GPL.

MySQL es actualmente el servidor de base de datos más popular para los desarrollos a través de la red mundial, principalmente sitios de Internet ya que se considera rápido y sólido.

MySQL es una base de datos muy rápida en la lectura cuando utiliza el motor no transaccional, pero puede provocar problemas de integridad en entornos de alta concurrencia en la modificación. En aplicaciones web hay baja concurrencia en la modificación de datos y en cambio el entorno es intensivo en lectura de datos, lo que hace a MySQL ideal para este tipo de aplicaciones. Sea cual sea el entorno en el que va a utilizar MySQL, es importante monitorizar de antemano el rendimiento para detectar y corregir errores tanto de SQL como de programación.

Una vez descargado de la página oficial se continúa con la instalación, se deberá ubicar en la carpeta raíz de mysql por medio del comando cd mysql-5.6.21

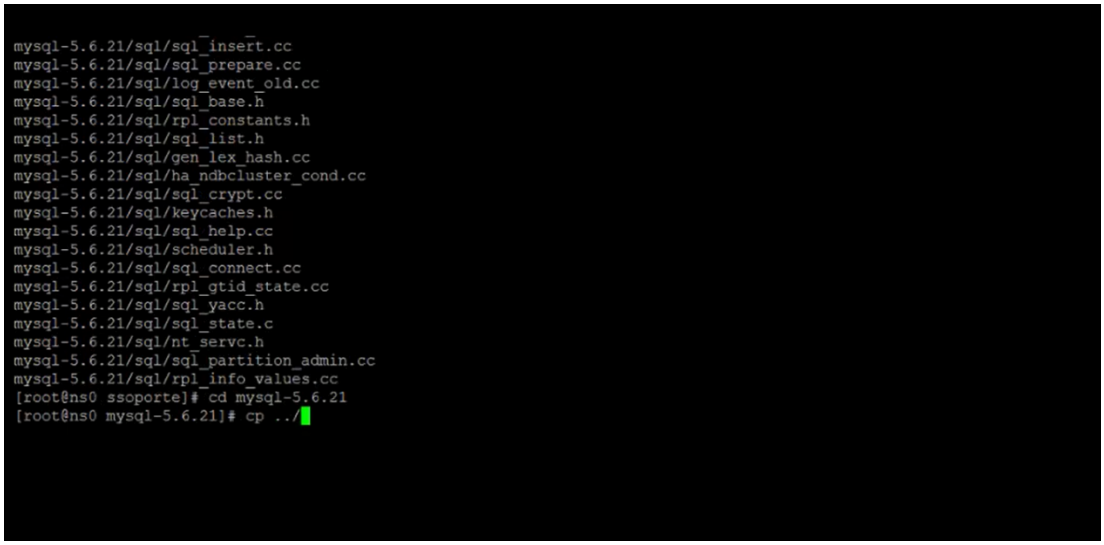

Figura 34 Ubicación raíz de mysql

De ahí se debe posicionar en el archivo de configuración de mysql

cp ../mysql.cfg.

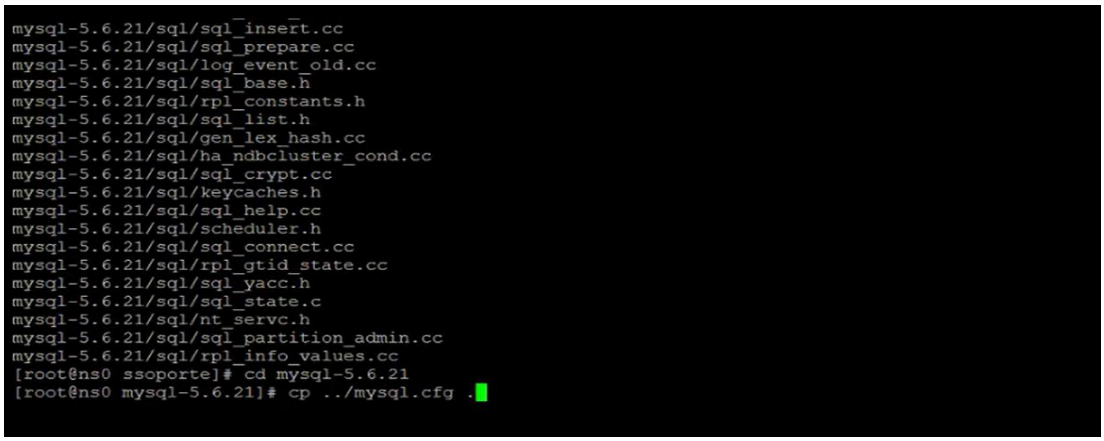

Figura 35 Archivo de configuración Mysql

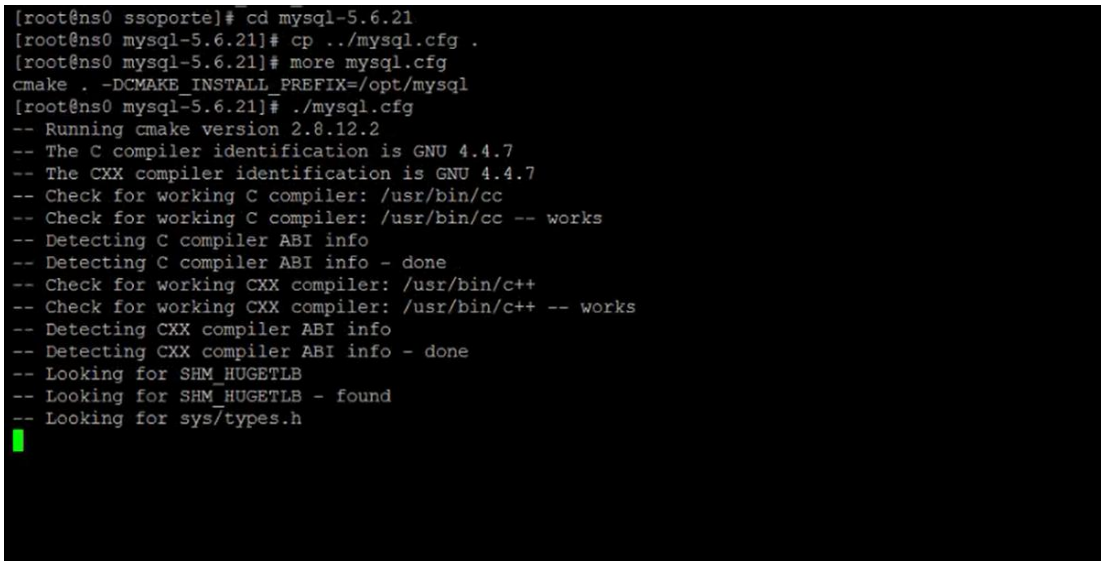

Figura 36 Configuración de Mysql

Para la configuración de mysql se recomienda los parámetros por omisión, solo se debe modificar la ubicación del software:

cmake . -DCMAKE_INSTALL_PREFIX=/opt/mysql

/home/downloads/ssoporte/mysql-5.6.21

Figura 37 Paquetes de configuración mysql

Ahora el paso siguiente es el de compilar con el comando make que ayuda a compilar los programas. Presenta muchas ventajas para programas grandes, en los que hay muchos ficheros fuente tales como mysql, estos están repartidos por varios directorios. Una ventaja del comando make es de que guarda los comandos de compilación con todos sus parámetros para encontrar librerías, no se tendrá que escribir largas líneas de compilación.

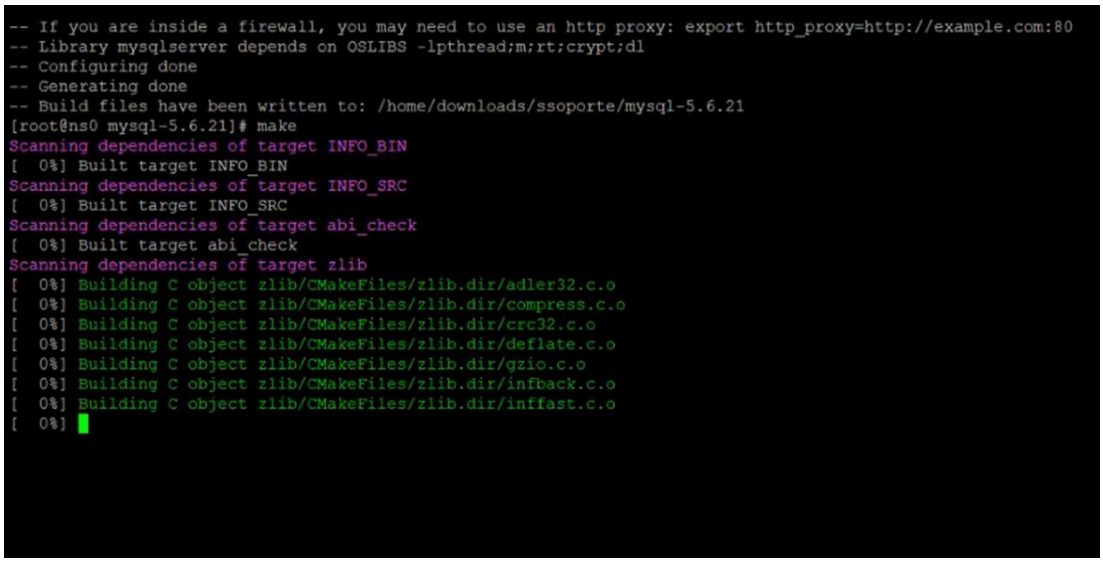

Figura 38 Compilación de mysql

Una vez compiladas todas las librerías y componentes de mysql se debe proceder a ver si la instalación fue correcta y si están los archivos que se necesitan para una correcta funcionalidad de mysql.

ls –al /opt/mysql/

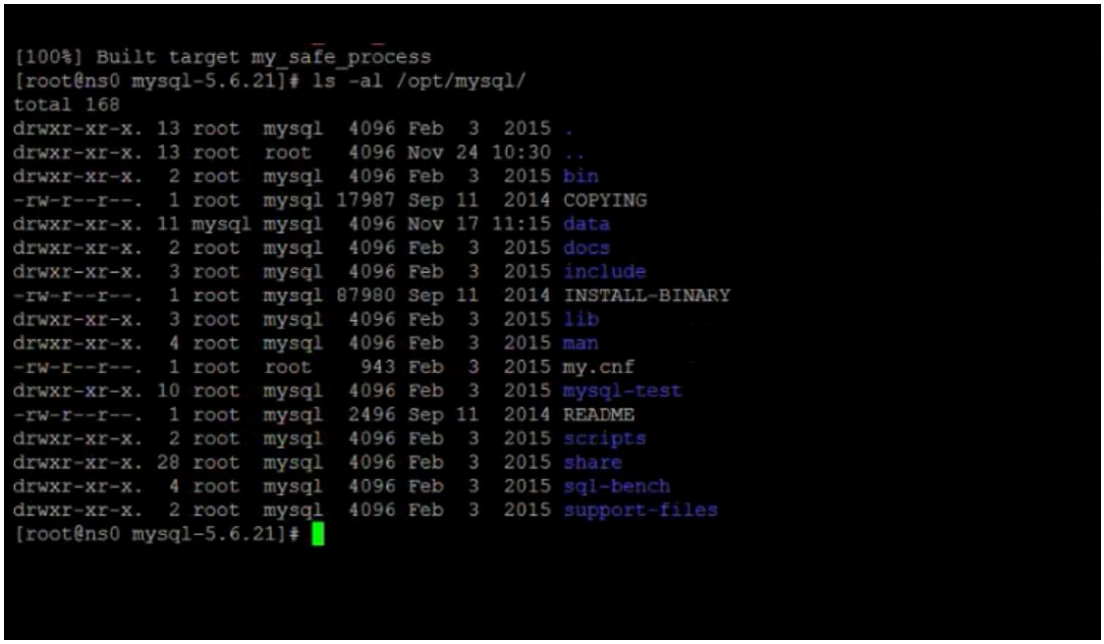

Figura 39 Verificación de archivos mysql

4.1.4. Instalación de Php

Para la instalación de php-5.4.33 primeramente al igual que las otras tecnologías es de código abierto, la cual se debe descargar y descomprimirla para poder instalarla.

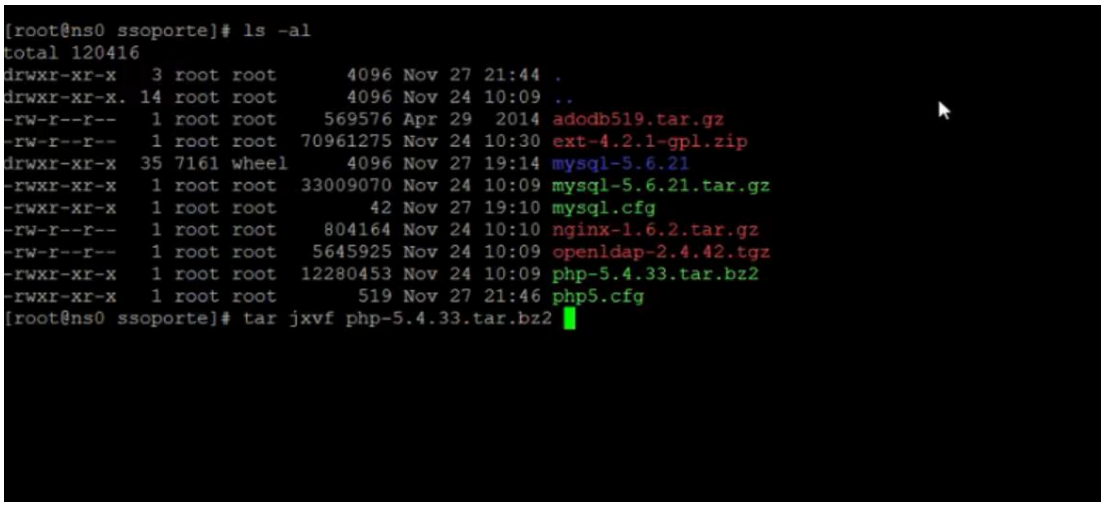

Figura 40 Descomprimir el paquete de instalación de Php

Se utiliza mismo procedimiento para la configuración de Php, la ubicación debe de ser en la carpeta donde se descomprimió, y se corre el archivo de configuración

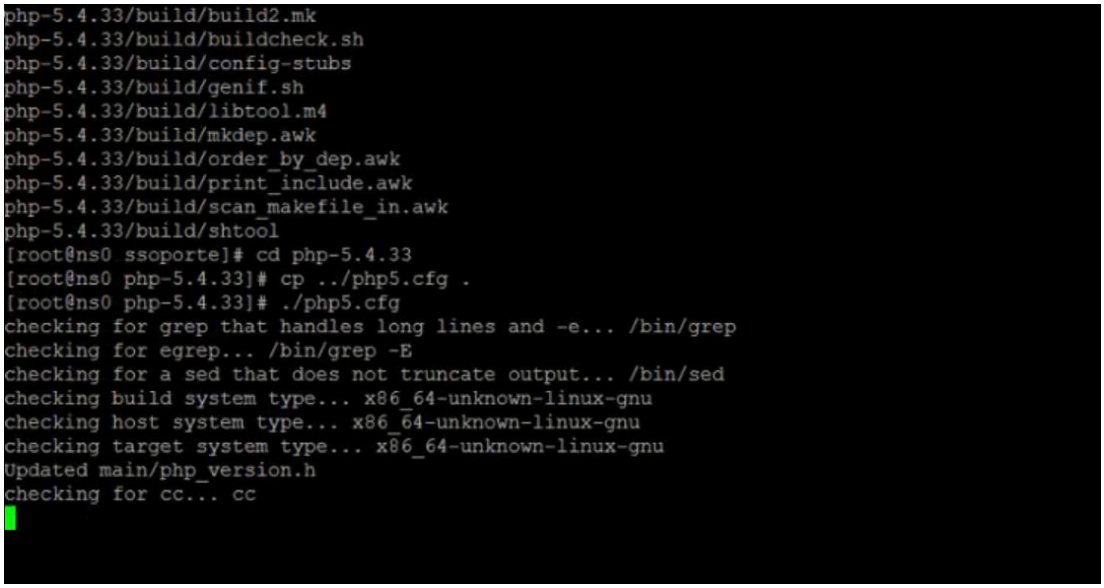

Figura 41 Configuración de Php

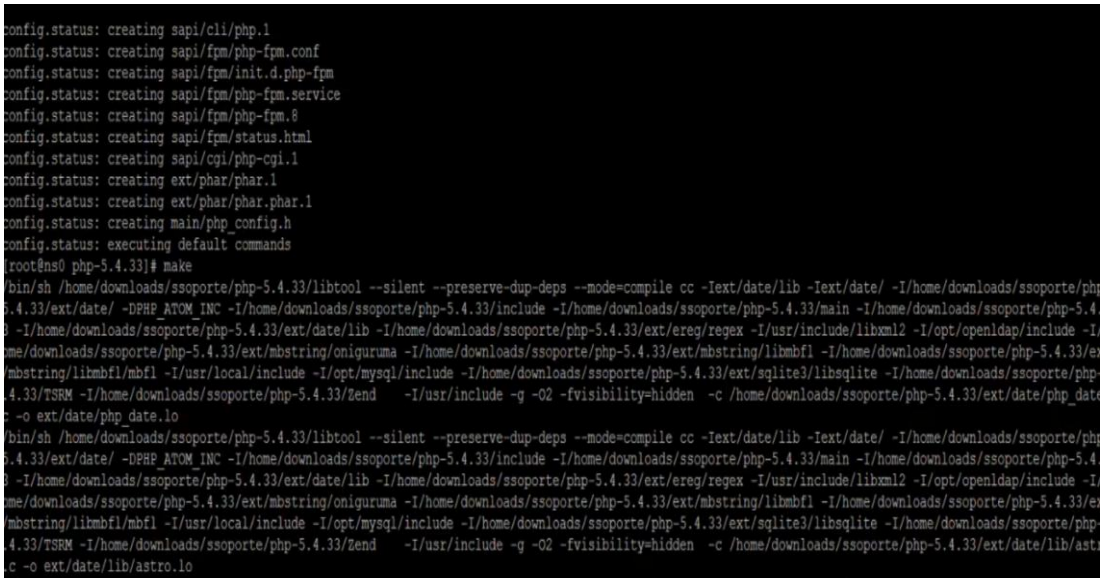

Figura 42 Paquetes de Configuración Php

Una vez compiladas todas las librerías y componentes php se debe proceder a ver si la instalación fue correcta y si están los archivos que se necesitan para una correcta funcionalidad de php.

```
Build complete.
Don't forget to run 'make test'.

[root@ns0 php-5.4.33]# ls -al /opt/php5
total 104
drwxr-xr-x. 10 root   root    4096 Mar 17  2015 .
drwxr-xr-x. 13 root   root    4096 Nov 24 10:30 ..
drwxr-xr-x.  2 root   root    4096 Nov 16 01:08 bin
drwxr-xr-x.  2 root   root    4096 Nov 16 01:08 etc
drwxr-xr-x.  3 root   root    4096 Feb  4  2015 include
drwxr-xr-x.  3 root   root    4096 Feb  4  2015 lib
drwxr-xr-x.  4 root   root    4096 Feb  4  2015 php
-rw-r--r--   1 netadm netadm 65520 Mar 17  2015 php.ini
drwxr-xr-x.  3 root   root    4096 Feb  4  2015 pools
drwxr-xr-x.  2 root   root    4096 Nov 16 01:08 sbin
drwxr-xr-x.  4 root   root    4096 Feb  4  2015 var
[root@ns0 php-5.4.33]#
```

Figura 43 Paquetes de Configuración Php

En el archivo de Configuración se deberá observar las librerías para la compilación de PHP y el para acceso LDAP y MySQL y en modo cgi.

```
[root@ns0 php-5.4.33]# more php5.cfg
./configure --prefix=/opt/php5 \
   --with-config-file-path=/opt/php5 \
   --with-fpm-user=www \
   --with-fpm-group=www \
   --enable-fpm \
   --enable-cli \
   --enable-cgi \
   --with-mysql=/opt/mysql \
   --with-pdo-mysql \
   --with-gd \
   --with-jpeg-dir=/usr/lib \
   --with-png-dir=/usr/lib \
   --with-mcrypt \
   --with-openssl \
   --enable-sigchild \
   --enable-sockets \
   --with-gettext \
   --with-zlib \
   --with-iconv \
   --enable-mbstring=all \
   --enable-mbregex \
   --with-ldap=/opt/openldap
[root@ns0 php-5.4.33]#
```

Figura 44 Líneas de archivo de configuración php

4.1.5. Instalación de OpenLDAP

Una vez descargado el openLDAP se lo descomprime para poder instalarlo y configurarlo.

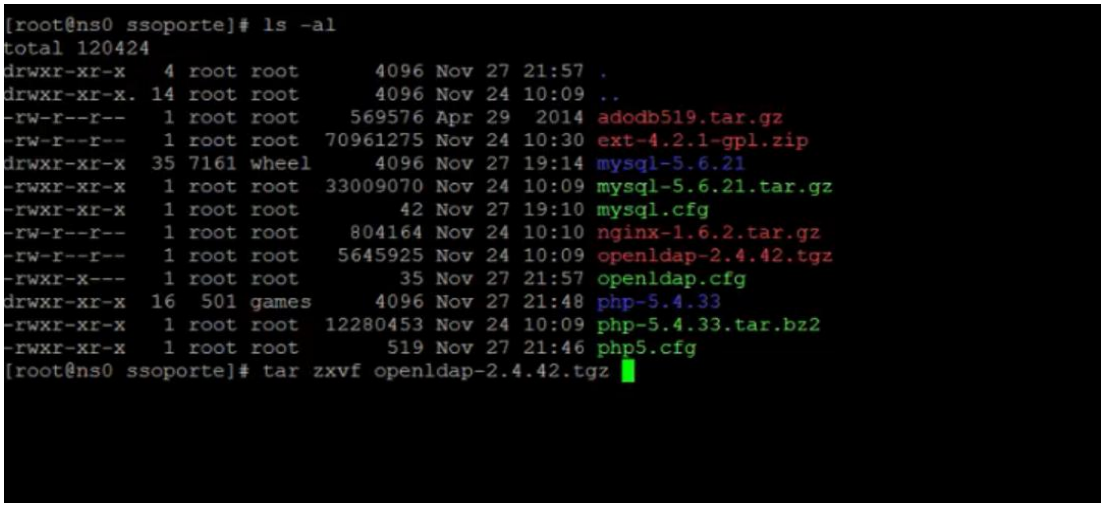

Figura 45 Descomprimiendo el paquete openLDAP

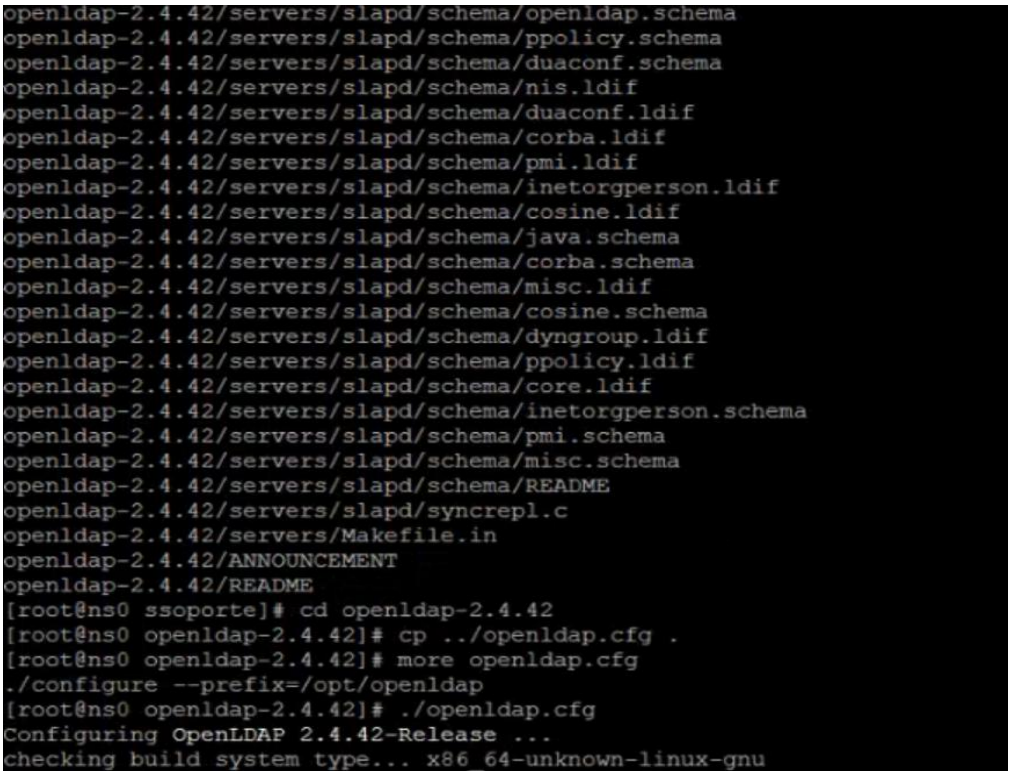

Figura 46 Configuración openLDAP

Una vez configurado los paquetes y librerías de openLDAP se deberá compilar de dos formas con el comando make, el uno compilara las dependencias de la otra forma se compilará todo el archivo de configuración.

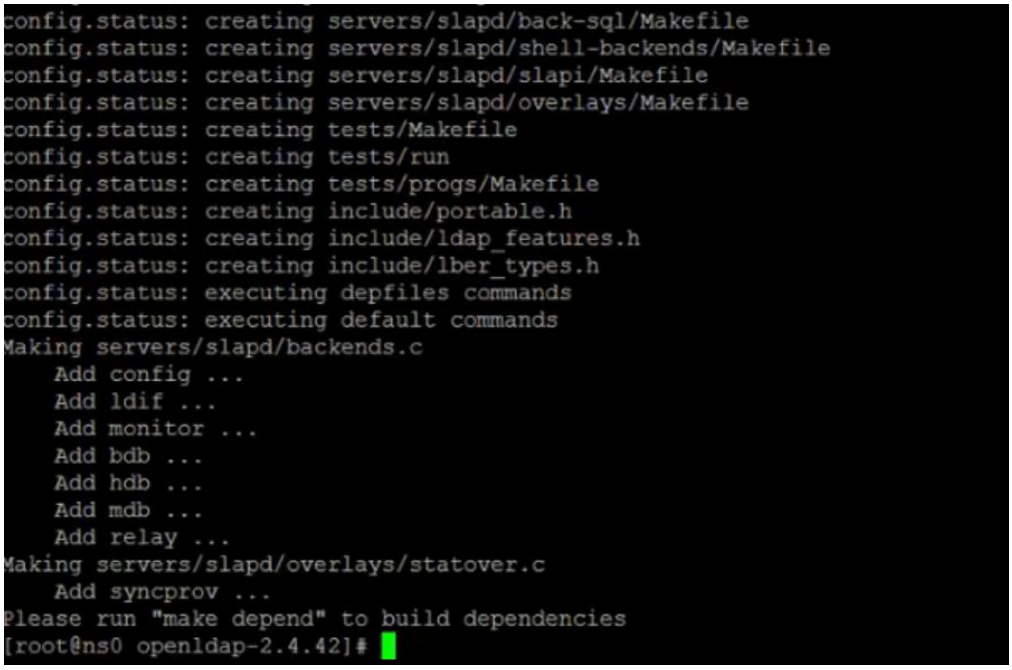

Figura 47 Paquetes de configuración openLDAP

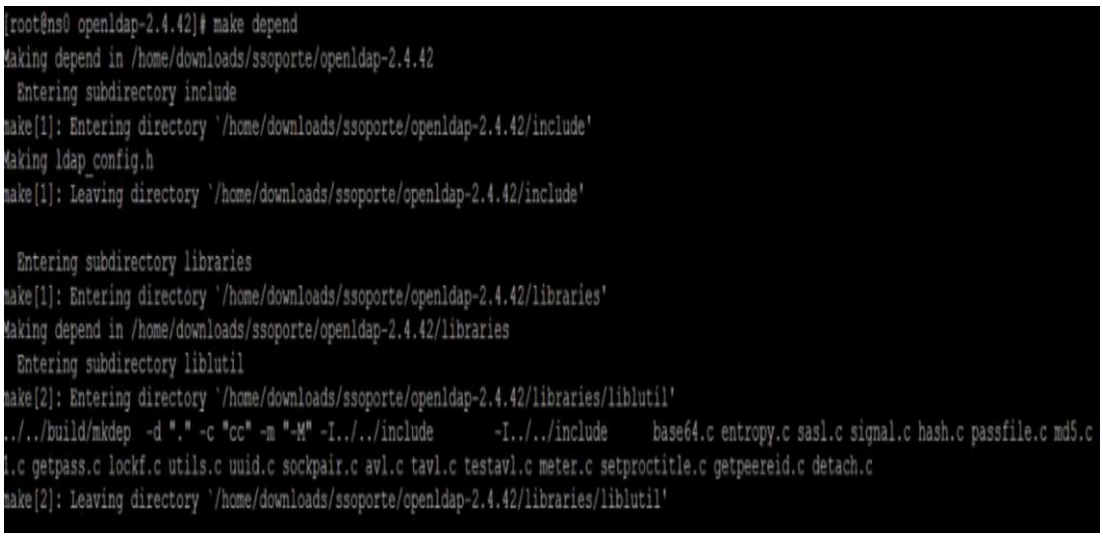

Figura 48 Compilación make depend de openLDAP

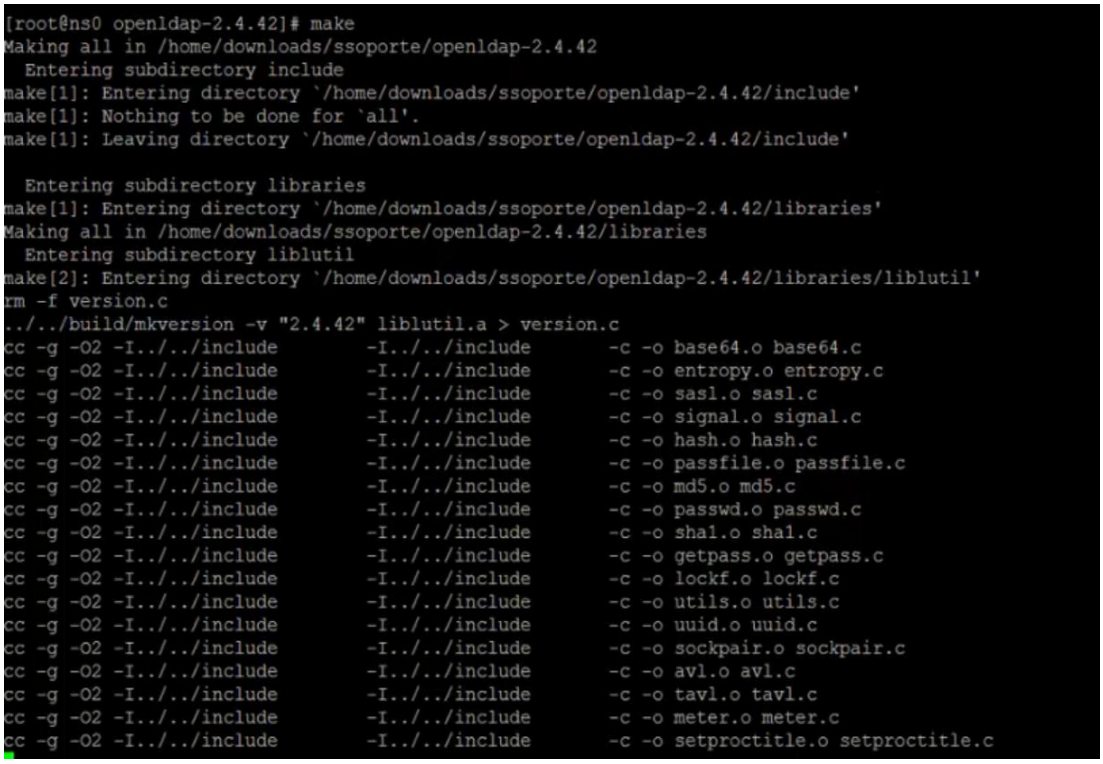

Figura 49 Compilación make de openLDAP

Después de configurarlo y compilarlo ya se encuentra instalado el openLDAP, igual se deberá comprobar los archivos que se instalaron, mismos que modificaremos para el añadir o eliminar entradas en el servidor LDAP.

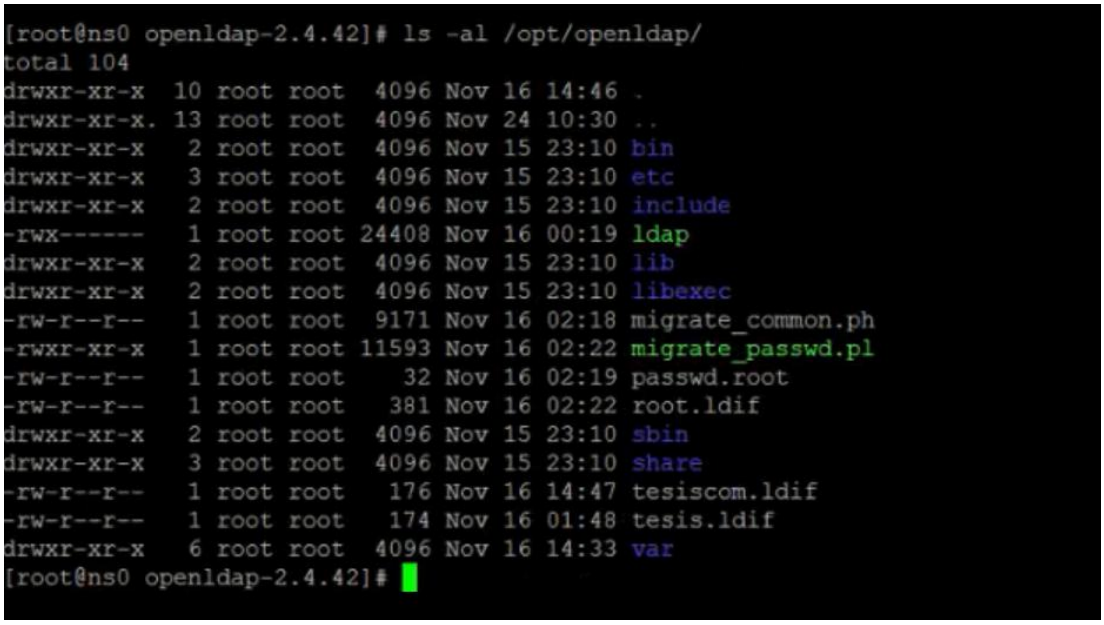

Figura 50 Verificación de archivos de openLDAP

También es posible manipular si se requiere las diferentes herramientas que posee el servidor openLDAP, estos se pueden utilizar mediante línea de comandos.

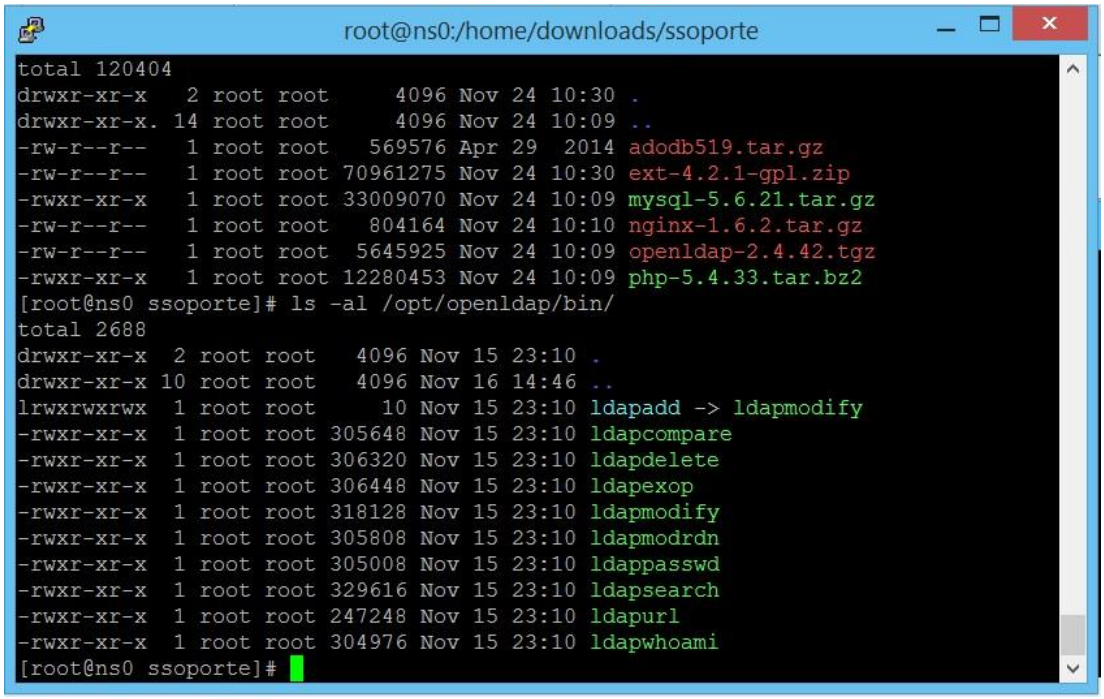

Figura 51 Herramientas de openLDAP

Una vez instalado el servidor openLDAP, queda ingresar las entradas las cuales serán ingresadas mediante una interfaz web, el acceso tendrá el administrador de claves de la cooperativa.

Como ya se lo menciono anteriormente, el administrador puede crear usuarios y de asignarles permisos de acceso, como se indica en la Figura 52.

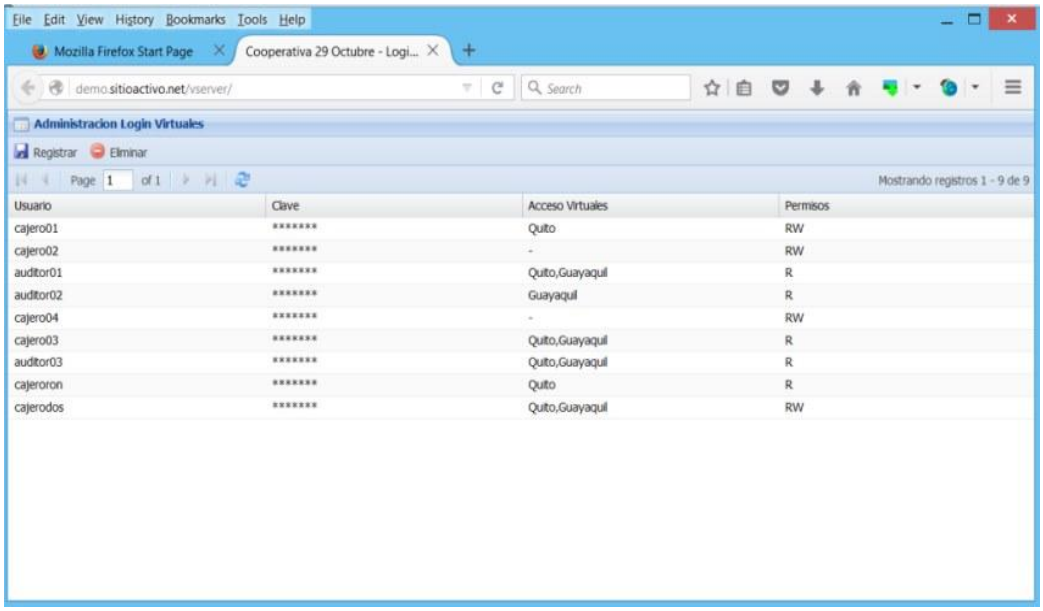

Figura 52 Interfaz de Administrador

Por otro lado se tiene otra interfaz web la cual es para uso de los usuarios, en la cual tendrán el control de acceso de usuario con su contraseña a los servidores virtuales que llamamos oficinas virtuales, como se indica en la Figura 53, si su contraseña no es la correcta o no tiene permiso a ese acceso virtual se le dirigirá a una pantalla donde se le hace ver el error en clave o permiso, tal como se indica en la Figura 54.

Dependiendo del permiso asignando podrá ingresar a una u más oficinas, si el permiso es de lectura solo podrá acceder a leer sin la opción de ingresar o eliminar algún dato dentro de la oficina, si al contrario el permiso es de lectura y escritura si podrá ingresar y eliminar usuarios dentro del acceso virtual al que hayan ingresado.

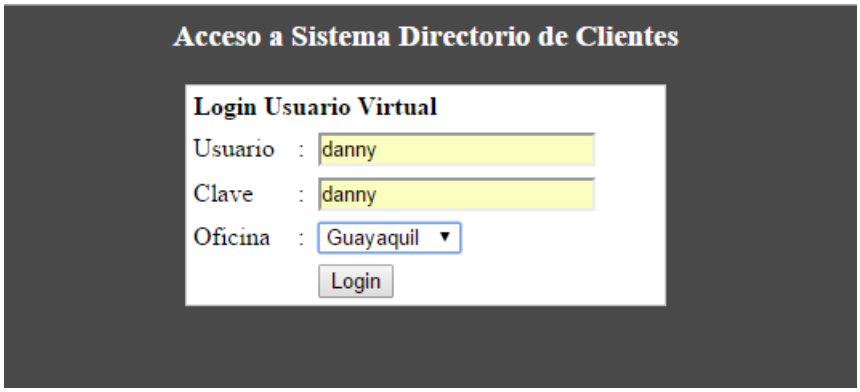

Figura 53 Interfaz de Usuario

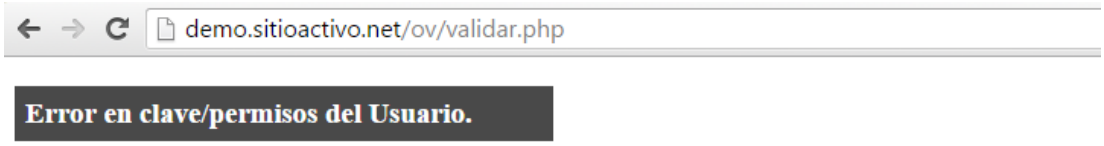

Figura 54 Mensaje de Error de acceso

4.2. Pruebas

4.2.1. Prueba de Aplicación

Conforme a la información de la cooperativa la administración del servidor será responsabilidad del administrador de red, este tendrá acceso al servidor openLDAP para agregar, eliminar y consultar entradas por medio de la interfaz web, dicha información puede ser consultada por línea de comandos del servidor para poder ver los datos, como se indica en la Figura 55.

Figura 55 Consulta de usuarios por línea de comandos

4.2.2. Prueba de Interfaz

Se ha tomado en cuenta los siguientes criterios:

Enlaces: Cada uno de los enlaces de la interfaz se enlace al objeto deseado.

Formato: El servidor openLDAP recibe toda la información y no existe pérdida de datos en la ejecución de administración de las claves.

Ventanas Dinámicas: En la interfaz web la navegación de cada una de las ventanas se maneja memoria dinámica para construir y destruir los objetos que tiene cada una de estas con los scripts de programación.

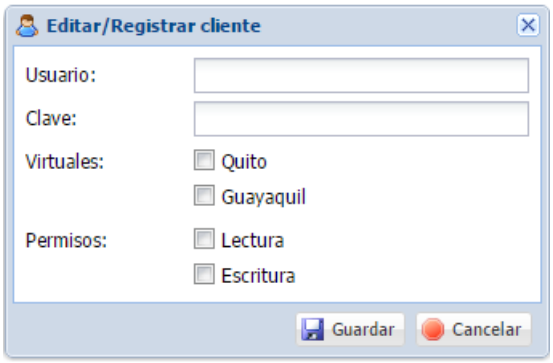

Figura 56 Ventana de Creación de Usuarios

4.2.3. Prueba de Facilidad de Uso

Para este tipo de pruebas se ha tomado en consideración aspectos como el grado de usabilidad interacción con el usuario y el despliegue de opciones.

4.2.4. Prueba de Navegación

Para la realización de esta prueba se ha establecido una verificación de todos los enlaces de la aplicación.

Se ha analizado en conjunto con el administrador y el usuario que los enlaces creados lleven hacia la funcionalidad adecuada y sobretodo que estos enlaces sean entendibles.

Con esta prueba se ha logrado ejercitar ampliamente la navegación de la aplicación por parte del administrador y de los usuarios finales.

4.2.5. Prueba de Configuración

El modelo y la administración web explica el concepto de LDAP el cual es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

4.2.6. Prueba de Seguridad

La administración del servidor OpenLDAP por ser un demo no implementa ninguna seguridad de acceso, por lo que puede cualquier usuario acceder a la misma. Además el acceso a la administración web tanto como para el administrador y para el usuario puede ser en cualquier momento y desde cualquier computador con internet ya que esta levantada sobre un dominio activo del demo.

4.2.7. Prueba de Desempeño

Con esta prueba se determinó que la administración web del servidor openLDAP trabaja bajo una arquitectura Cliente - Servidor es decir respondió a varias condiciones de carga y soportó adecuadamente las transacciones con varios usuario a la vez desde diferentes lugares.

4.2.8. Prueba de consultas

Una vez realizada la creación de usuarios y de concederle permisos de acceso a las oficinas virtuales procedemos a preguntar al servidor openLDAP si los usuarios y entradas creadas se están guardando y actualizando de manera correcta y en tiempo real.

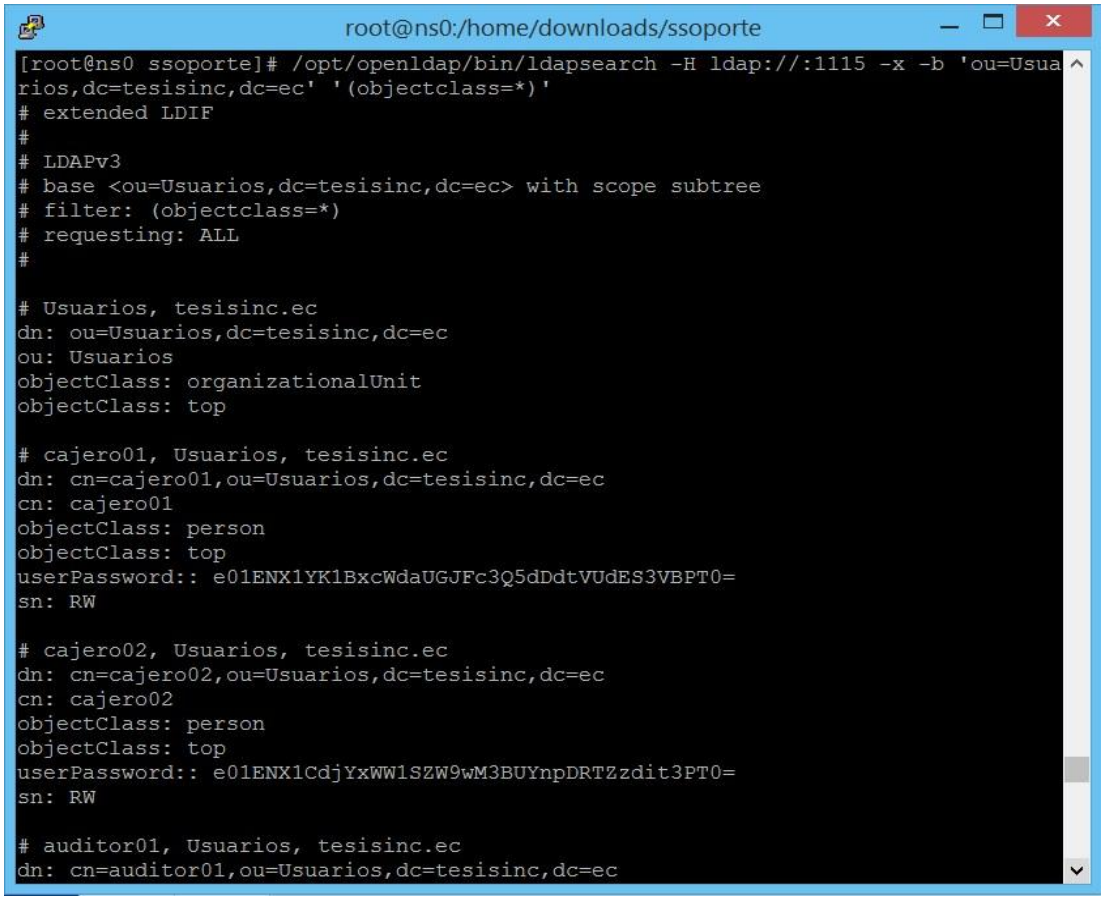

Figura 57 Consulta de Usuario por línea de comando

De igual manera se realizó las pruebas de consultar objetos de los nodos

Figura 58 Consulta de nodos

Como resultado nos arroja el nodo específico

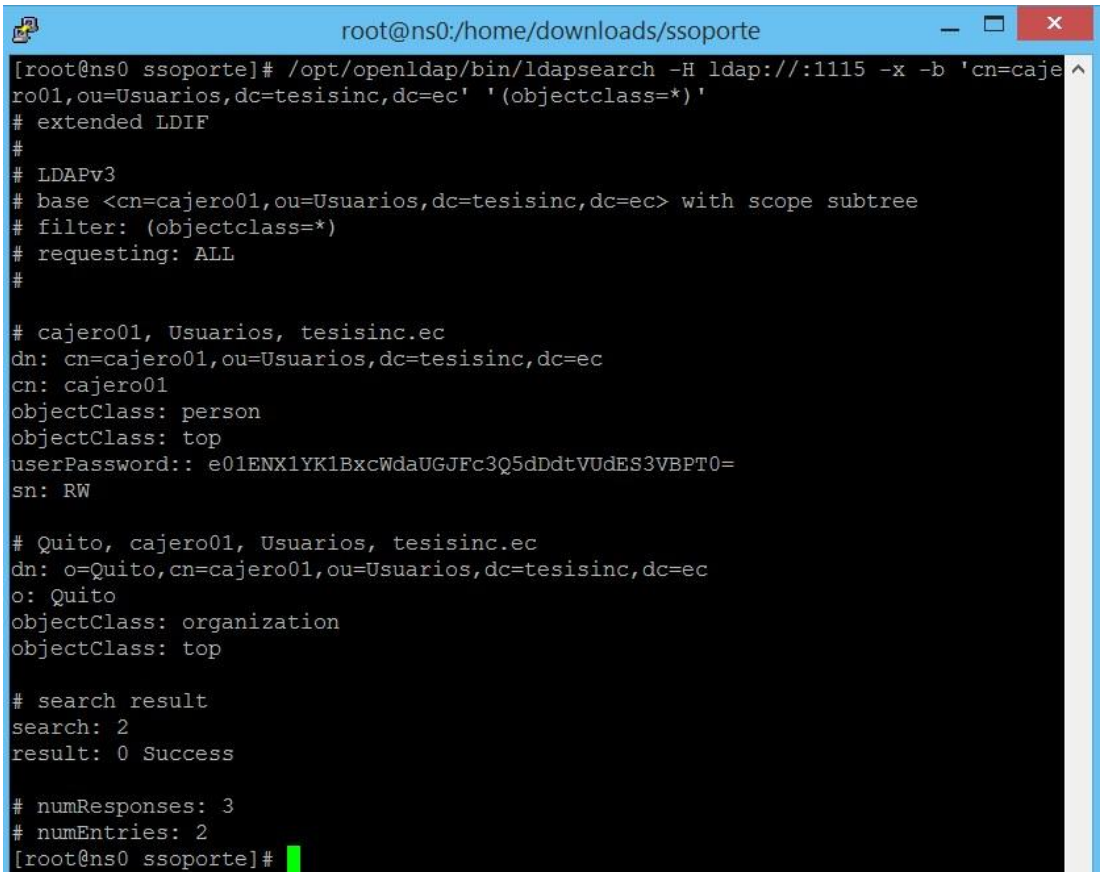

Figura 59 Resultado de Consulta de Nodo

Ahora se realiza la consulta del acceso a la oficina virtual, se consultará objetos de cualquier nodo, para ello se selecciona solo aquellos que sean del tipo organization.

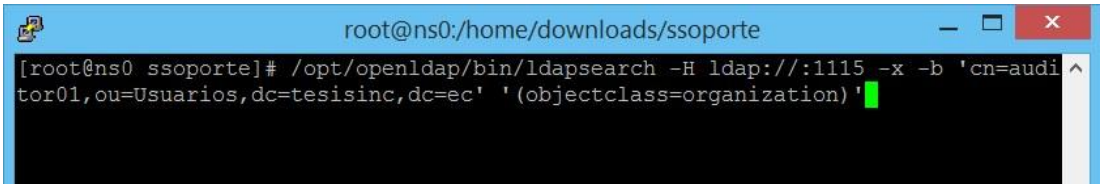

Figura 60 Consulta tipo organization

Como resultado se verifica la organización y el nodo

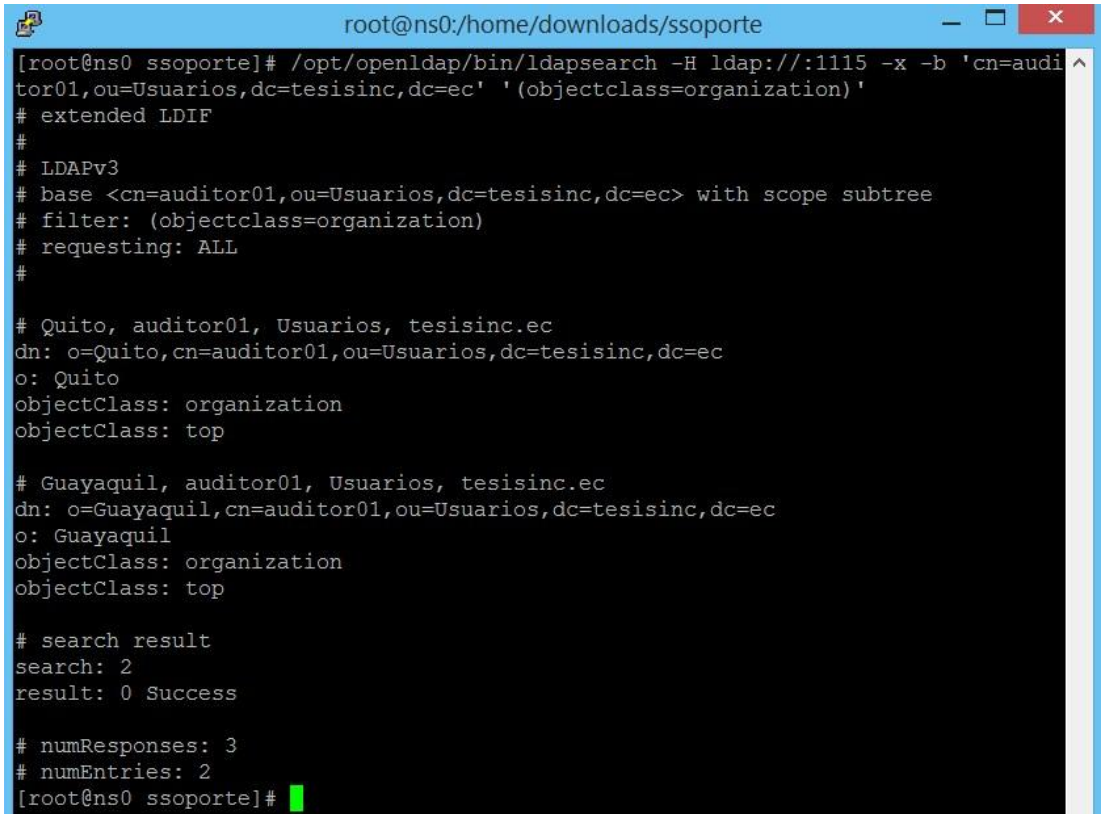

Figura 61 Resultado de consulta tipo organization

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones Generales

- En vista de que en la Cooperativa de Ahorro y Crédito “29 de Octubre” no existía un modelo de administración centralizado de claves, se realizó la revisión de documentación, y por medio de entrevistas con el administrador de cada servidor se logró identificar los roles y funciones de cada servidor virtualizado Linux para de esta manera obtener el punto de inicio para el diseño.

- Basado en el protocolo LDAP se diseñó el modelo que centraliza la autentificación de los usuarios en un servidor, es decir para poder ingresar a la información de un servidor virtual de la cooperativa, el usuario se autentificará en el servidor LDAP, si sus credenciales son correctas y posee permisos tendrá acceso a dicho servidor virtual caso contrario no se le permitirá el ingreso.

- LDAP permitió implementar el servidor de administración centralizado, de manera que para tener acceso de lectura, escritura o ambos a la información de algún servidor virtualizado de la Cooperativa, el usuario deben tener permisos sobre el servidor al cual se quiere ingresar, esta solución incrementa la seguridad de acceso a los servidores.

- En el presente proyecto, el servidor LDAP implementado permitió configurar los permisos que otorgan o restringen acceso de los usuarios, de igual manera se puede eliminar usuarios que no sean necesarios.

5.2. Recomendaciones

- Tomar en cuenta las políticas de seguridad de la institución para evitar manipular información de carácter privado, esto para prevenir daños no deseados.

- Realizar una adecuada configuración del servidor LDAP ya que existe una gran variedad de cambios dependiendo de la distribución de Linux utilizada, el mismo paquete de instalación de openLDAP posee configuraciones que no se inician.

- Es también recomendable organizar equipos para que el proceso de análisis, modelo e implementación sigan el mismo sentido, estos grupos deben ser capacitados y especializados en su rol.

- Para la adecuada selección las herramientas tecnológicas OpenSource a ser instalados en el servidor, se recomienda escoger las que tengan mayores comentarios positivos y con mayores votaciones, ya que serían los más calificados por su estabilidad y funcionalidad.

- En estos proyectos de implementaciones, se debe definir una fase de pruebas que podría ser integrada dentro del proyecto desde su inicio para controlar la calidad del proyecto

- Conformar organizadamente el grupo de trabajo con miembros de las áreas involucradas para que el proceso fluya de manera normal, esto acortará los tiempos de implementación del servidor. Además se recomienda que tengan conocimiento sobre las políticas de seguridad de la información que nos permita cumplir con los objetivos puestos, sin poner en riesgo de alguna manera a la institución.

Bibliografía

Alvarez, R. (2002). *Introducción a la programación en PHP*. Obtenido de Introducción a la programación en PHP: http://www.desarrolloweb.com/articulos/303.php

cursohacker.es. (2015). *Que es la Virtualizacion*. Obtenido de Que es la Virtualizacion: http://cursohacker.es/que-es-la-virtualizacion-ventajas

Flandes, S. R. (28 de Marzo de 2011). *Implementación de un Sistema de Directorios LDAP para la*. Obtenido de Implementación de un Sistema de Directorios LDAP para la: http://bosque.udec.cl/~sram/manuals/informe.pdf

Ghaffar, A. (Julio de 2000). *Introducción a LDAP sobre Linux*. Obtenido de Introducción a LDAP sobre Linux: http://www.linuxfocus.org/Castellano/July2000/article159.shtml

Kioskea. (Junio de 2014). *Protocolo LDAP*. Obtenido de Protocolo LDAP: http://es.ccm.net/contents/269-protocolo-ldap

Lara, J. (s.f.). *OPENLDAP*. Obtenido de OPENLDAP: http://blog.phenobarbital.info/openldap/

Linux, G. (2001-2015). *Gentoo Linux wiki*. Obtenido de Gentoo Linux wiki: https://wiki.gentoo.org/wiki/Centralized_authentication_using_OpenLDAP/es

Llaquet, F. P. (Marzo de 2011). *Hardening básico de linux Permisos y Configuraciones*. Obtenido de http://www.isecauditors.com/sites/default/files//files/iseclab13-hardening_basico_linux_permisos_y_configuraciones.pdf

Malere, L. E. (Febrero de 2000). *LDAP-Linux-Como*. Obtenido de LDAP-Linux-Como: http://es.tldp.org/COMO-INSFLUG/COMOs/LDAP-Linux-Como/LDAP-Linux-Como.html#toc1

Mizner, W. (2008-2015). *Investigación Empírica*. Obtenido de Investigación Empírica: https://explorable.com/es/investigacion-empirica

OpenLDAP. (s.f.). Obtenido de OpenLDAP: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/administracin_de_openldap.html

Pentima, L. D. (19 de Junio de 2007). *ldap*. Obtenido de ldap: http://www.bdat.net/documentos/ldap/

Red Hat, I. (2005). *Introducción a la administración de sistemas*. Obtenido de Introducción a la administración de sistemas: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/index.html