Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

SISTEMA ÚNICO DE AUTENTICACIÓN DE USUARIOS, FACULTAD DE INGENIERÍA, USAC

Jairo Alberto Cifuentes Fuentes
Marvin Alexander Valenzuela Palacios
Asesorado por el Ing. Pedro Luis Domingo Vásquez

Guatemala, mayo de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

SISTEMA ÚNICO DE AUTENTICACIÓN DE USUARIOS, FACULTAD DE INGENIERÍA, USAC

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JAIRO ALBERTO CIFUENTES FUENTES
MARVIN ALEXANDER VALENZUELA PALACIOS
ASESORADO POR EL ING. PEDRO LUIS DOMINGO VÁSQUEZ

AL CONFERÍRSELES EL TÍTULO DE

INGENIEROS EN CIENCIAS Y SISTEMAS

GUATEMALA, MAYO DE 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Marlon Antonio Pérez Türk
EXAMINADORA	Inga. Sonia Yolanda Castañeda Ramírez
EXAMINADORA	Inga. Floriza Ávila Pesquera de Medinilla
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presentamos a su consideración nuestro trabajo de graduación titulado:

SISTEMA ÚNICO DE AUTENTICACIÓN DE USUARIOS,
FACULTAD DE INGENIERÍA, USAC

Tema que nos fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 28 de febrero 2012.

Jairo Alberto Cifuentes Fuentes

Marvin Alexander Valenzuela Palacios

Guatemala, 3 de septiembre de 2012

Inga. Sigrid Alitza Calderón De León de De León
Directora EPS
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimada Ingeniera Sigrid Calderón:

Por este medio atentamente le informó que como Asesor de la Practica del Ejercicio Profesional Supervisado (E.P.S.) de los estudiantes universitarios **Jairo Alberto Cifuentes Fuentes *carné No. 200614994* y *Marvin Alexander Valenzuela Palacios carné No. 200714427*** de la Carrera de Ingeniería en Ciencias y Sistemas, procedí a revisar el proyecto final, cuyo título es **"SISTEMA UNICO DE AUTENTICACION DE USUARIOS, FACULTAD DE INGENIERIA, USAC".**

En tal virtud, **LO DOY POR APROBADO,** solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Ing. Pedro Domingo
Colegiado 10,899

Ing. Pedro Luis Domingo Vásquez
Asesor de proyecto

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

UNIDAD DE EPS

Guatemala, 25 de enero de 2013.
REF.EPS.D.40.01.2013.

Ing. Marlon Antonio Pérez Turk
Director Escuela de Ingeniería Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ingeniero Perez Turk.

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **"SISTEMA ÚNICO DE AUTENTICACIÓN DE USUARIOS, FACULTAD DE INGENIERÍA, USAC",** que fue desarrollado por los estudiantes universitarios **Jairo Alberto Cifuentes Fuentes carné No. 200614994 y Marvin Alexander Valenzuela Palacios carné No. 200714427** quienes fueron debidamente asesorados por el Ing. Pedro Luis Domingo Vásquez y supervisados por la Inga. Floriza Felipa Ávila Pesquera de Medinilla.

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación del mismo por parte del Asesor y la Supervisora de EPS, en mi calidad de Directora apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,
"Id y Enseñad a Todos"

Inga. Sigrid Alitza Calderón de León
Directora Unidad de EPS

Universidad de San Carlos de Guatemala
DIRECCIÓN
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

SACdL/ra

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 6 de Febrero de 2013

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS de los estudiantes **JAIRO ALBERTO CIFUENTES FUENTES** carné **200614994,** y **MARVIN ALEXANDER VALENZUELA PALACIOS** carné **200714427** titulado: **"SISTEMA ÚNICO DE AUTENTICACIÓN DE USUARIOS, FACULTAD DE INGENIERÍA, USAC"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"SISTEMA ÚNICO DE AUTENTICACIÓN DE USUARIOS, FACULTAD DE INGENIERÍA, USAC"****, realizado por los estudiantes JAIRO ALBERTO CIFUENTES FUENTES Y MARVIN ALEXANDER VALENZUELA PALACIOS, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Turk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 21 de mayo 2013

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.340.2013

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **SISTEMA ÚNICO DE AUTENTICACIÓN DE USUARIOS, FACULTAD DE INGENIERÍA, USAC,** presentado por los estudiantes universitarios: **Jairo Alberto Cifuentes Fuentes y Marvin Alexander Valenzuela Palacios,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, mayo de 2013

/cc

ACTO QUE DEDICO A:

Dios Por su infinita gracia, su iluminación y guía para siempre seguir hacia adelante.

Mis padres Alberto Cifuentes y Brenda Fuentes, este trabajo es la muestra que tengo para decirles que lo he logrado, el triunfo no es solo mío si no de ustedes.

Abuela Carmen García, por sus guías y consejos han sido mi inspiración.

Hermanos Wilmer Cifuentes, Irene Cifuentes, Palty Cifuentes y Crosbin Cifuentes por haberme apoyado en lograr esta meta.

Amigos Bitzel Cortez, Marvin Valenzuela, Jerry Osorio y a todos en general, porque sin el trabajo en equipo no se logran los proyectos más grandes y ambiciosos.

Jairo Alberto Cifuentes Fuentes

ACTO QUE DEDICO A:

Dios Por la sabiduría y la fuerza para poder alcanzar la meta deseada.

Mis padres Saúl Valenzuela y Maritza Palacios por ser la base fundamental de mis logros. Han sido el soporte fundamental en mi vida, esto es para ustedes.

Mis hermanos Saúl Valenzuela y William Valenzuela por estar junto a mí en toda mi vida y brindarme su apoyo para lograr esta meta.

Mi tía Miriam Palacios por brindarme su apoyo a lo largo de toda mi carrera y brindarme un cariño tan especial.

Mi novia Miriam Morales por estar a mi lado en todo momento y brindarme la fuerza para terminar este recorrido.

Amigos José Arturo, Pablo Tum, Jairo Cifuentes, Julio Ayapan, Oswaldo López, Nathan Soto, Deiby Gómez, Jerry Osorio, Susana Fuentes por estar conmigo en el transcurso de esta meta.

Marvin Alexander Valenzuela Palacios

AGRADECIMIENTOS A:

Dios Por ser el que ha hecho posible todo, y el que me ha iluminado, guiado y ayudado durante cada día de mi vida.

Mis padres Alberto Cifuentes y Brenda Fuentes por su apoyo moral y económico incondicional. Por sus consejos, sabiduría y porque siempre marcaron mi forma de vivir.

USAC Mi alma mater, por ser una institución fuente de sabiduría y progreso para Guatemala y que me ha dado la oportunidad de pertenecer al cambio.

CCIE Por brindarme la oportunidad de ejercer mis conocimientos en uno de sus proyectos en especial a la Inga. Susan Verónica.

Asesor Ing. Pedro Domingo por sus guías y consejos a lo largo de nuestro trabajo de graduación.

Jairo Alberto Cifuentes Fuentes

AGRADECIMIENTOS A:

Dios El que me ha dado luz en los momentos difíciles.

Mis padres Saúl Valenzuela y Maritza Palacios por creer en mí en todo momento, desde el momento que me tuvieron en sus brazos.

USAC Por abrirme la puerta a esta grandiosa casa de estudios.

CCIE Por brindarme la oportunidad de demostrar mis conocimientos en forma especial a la Inga. Susan Verónica.

Asesor Ing. Pedro Domingo por estar ahí para darnos guía en este trabajo de graduación.

Marvin Alexander Valenzuela Palacios

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
&&	*AND,* Operador lógico Y
@	Arroba, utilizado en informática como un separador de dominios
>=	Mayor o igual que
<=	Menor o igual que
*****	Multiplicación
||	*Or,* operador lógico
root@nombre#	Prompt, símbolo del sistema en Linux

GLOSARIO

Api	*Application programming interface*, se refiere a un conjunto específico de reglas, que comunican a un sistema con otro.
Árbol jerárquico	Esquema lógico de datos, que sirve para el almacenamiento de información referente a un sistema, de tal forma que toda la información está contenida en nodos, este tipo de esquemas se utiliza en LDAP
cn	*Common Name* describe un nodo en el árbol jerárquico.
dn	Describe el contenido de los atributos en el árbol jerárquico
Replicación	Consiste en el transporte de datos entre dos o más servidores, permitiendo que ciertos datos de la base de datos estén almacenados en más de un sitio
uid	Se refiere a un identificador único en el árbol jerárquico, convirtiéndolo en un nodo hoja en dicho árbol

RESUMEN

La institución, Centro de Cálculo e Investigación Educativa, es la encargada del análisis, desarrollo e implantación de sistemas en general dentro de la Facultad de Ingeniería de la Universidad San Carlos de Guatemala, además de brindar soporte a los usuarios finales de las soluciones creadas.

La institución tiene varios sistemas a los cuales se les realiza mantenimiento de sus catálogos y niveles de acceso a distintos sistemas, ya sea software o acceso a computadoras físicas. Todos estos mantenimientos se realizan de una forma manual y distribuida.

Con el diseño e implementación del Sistema Único de Autenticación se logra una mejora de procesos, una centralización y estandarización en la información, además de una actualización y modernización en los sistemas de la facultad, que benefician a los usuarios de los sistemas que tiene a su cargo la institución.

El Sistema Único de Autenticación, es un sistema basado en el protocolo LDAP que es el protocolo que las grandes empresas de software y ámbito internacional están adquiriendo como un estándar en el manejo de información de autenticación. Por lo que se eligió este protocolo para que los sistemas de la institución sean compatibles con los sistemas externos ya sea actual o futuro; además de que al utilizar dicho protocolo se generaliza los tipos de información que se puedan almacenar, ya sea información de autenticación de acceso a computadoras, correo electrónico, servidores, base de datos, etc.

La compatibilidad y el traslado de información de un sistema a otro es el reto a superar en la implementación de todo sistema en la actualidad, en lo que tener un tipo de sistema no debe limitar la implementación de otro tipo de sistema. El Sistema Único de Autenticación, reúne la información de distintos sistemas y las almacena en una base de datos jerárquica, por lo que la extracción, transformación y carga de los sistemas actuales hacia el nuevo sistema es una prioridad. Para este fin se utilizan herramientas de ETL para realizar dicha tarea.

OBJETIVOS

General

Desarrollar e implementar un sistema centralizado de autenticación a usuarios que utiliza la Facultad de Ingeniería de la Universidad San Carlos de Guatemala de tal manera que todas las credenciales sean controladas por un sistema central, utilizando un servidor con el protocolo LDAP ofreciendo alta disponibilidad

Específicos

1. Desarrollar el sistema completamente con herramientas bajo licencias de código abierto para lograr un ahorro a la institución en cuanto a licencias.

2. Automatizar la administración de acceso a usuarios hacia los distintos sistemas.

3. Diseñar configurar e implementar un sistema con políticas de alta disponibilidad que más se adapten al tipo de uso que se le dará al sistema único de autenticación.

4. Integrar la información actual al nuevo sistema de forma íntegra, de tal manera que los datos actuales sean un reflejo de los actuales.

5. Documentar la implementación del sistema, detallando la utilización y configuración de la tecnología implementada.

INTRODUCCIÓN

El presente trabajo consta de la necesidad de tener un sistema único de autenticación en Centro de Cálculo e Investigación Educativa de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, que sea capaz de tener el control de todos los usuarios de los sistemas que dicha institución administra.

La característica principal de este nuevo sistema, es la capacidad de integrar usuarios de múltiples sistemas en un sistema único y centralizado, proveyendo la capacidad de administrarlos de una forma más eficiente y sencilla, además de garantizar alta disponibilidad.

Otra característica es el diseño del nuevo sistema de tal manera que el cambio a este tipo de autenticación no conlleve cambios drásticos en los sistemas actuales, permitiendo un mínimo impacto y menor coste en el traslado de los sistemas actuales a un tipo de autenticación centralizado e íntegro con respecto a la información de los sistemas existentes.

Con el paso de los años la tecnología se ha convertido en parte de la vida diaria cambiando poco a poco la forma en que se administra, se gestiona y se ven las cosas rutinarias en la vida. De esta forma sucede en las instituciones que gradualmente trasladan distintas actividades manuales a automáticas con el uso de un nuevo sistema informático. Pero a medida que se cambian más actividades y se crean sistemas aparentemente independientes, se acumulan la cantidad de sistemas a administrar, por lo que se hace necesario el diseñar e implementar una forma de centralizar los múltiples sistemas que permita un

mejor control, una mayor fiabilidad y además, permitir la integración y control de nuevos sistemas informáticos que se puedan implementar en el futuro.

Durante el desarrollo del sistema con las tecnologías utilizadas, se comprueba que este tipo de tecnología es la que se ha comenzado a utilizar en grandes empresas de software como un estándar en el uso de información de usuarios. En este punto se modernizan los sistemas en la facultad teniendo grandes beneficios, no solo para la institución si no que para todo los usuarios que se autentiquen con algún sistema perteneciente a la Facultad de Ingeniería USAC.

Una de las limitaciones de este trabajo es que por ser un sistema gigantesco y de afectar a todos los sistemas relativos a la facultad, se ha convenido la realización en varias fases una de análisis, diseño e implementación del nuevo sistema, otra de crear el cambio de todos los sistemas actuales a autenticarse al sistema ya implementado y una última de puesta en marcha de todos los sistemas y de realizar los cambios necesarios en cada computadora que tenga a cargo centro de cálculo. En este trabajo se cubre extensivamente la primera fase.

1. FASE DE INVESTIGACIÓN

Se pone en manifiesto los aspectos de la institución, la descripción de las necesidades del proyecto y su priorización.

1.1. Antecedentes de la institución

Como la institución de Centro de Cálculo e Investigación Educativa nació en la Facultad de Ingeniería, su misión, visión y los servicios que brinda divididos en distintas áreas.

1.1.1. Reseña histórica

En 1965 se puso en funcionamiento el Centro de Cálculo Electrónico, dotado de computadoras y del equipo periférico necesario.

Se comenzó con tecnología IBM de la época, tal como la IBM 1620 y luego se evolucionó a sistemas más actuales, tales como el sistema 32, 34 y 36 de IBM.

A finales de los años 80's y principios de los 90's también se trabajó con la tecnología Texas Instruments con sistemas operativos Xenix.

Luego se migró al uso de tecnología SUN comenzando con la SPARC 1 y posteriormente a SPARC 2.

En los últimos años de la década de los 90's se adquirieron servidores IBM Netfinity (3000 y 5000). Las primeras asignaciones de cursos en línea se llevaron a cabo en el año 1987.

El primer laboratorio con servicio de internet de la facultad de Ingeniería, se instaló en el Centro de Cálculo a mediados de los años 90.

A mediados del 2001 comenzó el proyecto de asignación de cursos vía Internet y el primer semestre del 2002, se llevaron a cabo las asignaciones a través de este medio.

1.1.2. Misión

Crear las mejores soluciones informáticas para el manejo de la información académica y administrativa generada en la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, tomando en cuenta las necesidades de los usuarios, tanto estudiantes como personal administrativo y docente, aprovechando al máximo los recursos asignados por medio de la utilización de herramientas adecuadas para su desarrollo.

1.1.3. Visión

Administrar toda la información de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala de manera eficiente, segura y accesible a todas las personas que la soliciten, cumpliendo con los reglamentos y normas establecidas, mejorar día a día las aplicaciones desarrolladas, además de mantener el equipo de cómputo de la facultad en las mejores condiciones posibles.

1.1.4. Servicios que realiza

La institución presta múltiples servicios, a la comunidad académica y estudiantil en la universidad San Carlos de Guatemala como se lista a continuación.

1.1.4.1. Desarrollo

Se encarga del análisis, desarrollo e implementación de sistemas en general; además de brindar soporte a los usuarios finales de las soluciones creadas.

También se encarga de la administración de los servidores de internet y de bases de datos de las distintas soluciones web creadas por el Centro de Cálculo.

1.1.4.2. Área de redes

Se encarga de la administración de la red de cómputo principal de la Facultad de Ingeniería.

Brinda servicio de soporte técnico a las distintas dependencias de la facultad, adicionalmente, se encarga del procesamiento de datos tal como horarios, notas de cursos, etc. y de la administración de los servidores y soluciones en sus versiones anteriores.

1.1.4.3. Investigación educativa

Principalmente, es la encargada de la generación de informes y estadísticas solicitadas al Centro de Cálculo por cualquier entidad, tanto de la Facultad de Ingeniería así como de entidades externas a esta.

1.2. Descripción de las necesidades

La institución tiene varios sistemas a los cuales se les realiza mantenimiento de sus catálogos y niveles de acceso, ya sea software o acceso a computadoras físicas.

Todos estos mantenimientos se realizan de una forma manual y distribuida, dando el caso de que al momento de crear un nuevo registro, grupo, usuario que tiene acceso a más de uno de los sistemas al cargo de la institución, el técnico designado debe ir a cada sistema a realizar los cambios solicitados. Añadiendo complejidad y tiempo a dicho proceso lo que convierte en una necesidad el poder realizar dichos cambios en una forma centralizada.

Los sistemas que mantiene la institución manejan datos y mantienen servicios críticos para la facultad de tal manera que la disponibilidad del sistema se convierte en una necesidad prioritaria.

También se tiene la necesidad de que la institución optimice los costos de operación, por lo que se hace necesario utilizar herramientas de software que sean distribuidas con licencias de código abierto.

1.3. Priorización de las necesidades

La implementación de una solución a la necesidad de la institución se convierte en un sistema complejo y se hace necesaria la inversión de tiempo y recurso humano, por lo que para llevar a cabo el sistema completo se divide la implementación del sistema en varias fases, enfocándose este informe únicamente en las fases mencionadas a continuación:

- Documento de análisis y diseño del sistema
- Implementación del servidor LDAP
- Replicación del servidor LDAP
- Migración de datos

Las siguientes fases del sistema están definidas en su totalidad por la institución y estas estarán a cargo de otro grupo de epesistas, los cuales se encargarán de implementar las nuevas fases del sistema.

2. MARCO TEÓRICO

Los elementos conceptuales que sirven de base para la solución del proyecto se abarcan en este espacio, el desarrollo del servidor de centralización de usuarios, la replicación del servidor, la migración y almacenaje de la información.

2.1. LDAP

Sus siglas en inglés Lightweight Directory Access Protocol, conocido en español como protocolo compacto de acceso a directorios basado en el estándar X.500 de ISO.

Este servicio se implementa en base a un directorio jerárquico para acceder a la información que este almacenada, regularmente utilizado para la gestión de autenticación de usuarios y contraseñas de distintos sistemas.

En sí es un protocolo que unifica la información que existe sobre un entorno de red o cualquier información que se pueda tratar de esta forma.

Este protocolo se encuentra en estos momentos en su versión 3, por lo cual por cada versión existe un RFC (documentos de referencia de su utilización) para las versiones de LDAP podemos encontrar los siguientes:

- LDAP V.1 RFC 1487
- LDAP V.2 RFC 1777
- LDAP V.3 RCF 2251

La diferencia marcada entre V.2 y la V.3 es la seguridad pudiendo implementar en la nueva versión una autenticación SSL (Seguridad en las transacciones que se realizan).

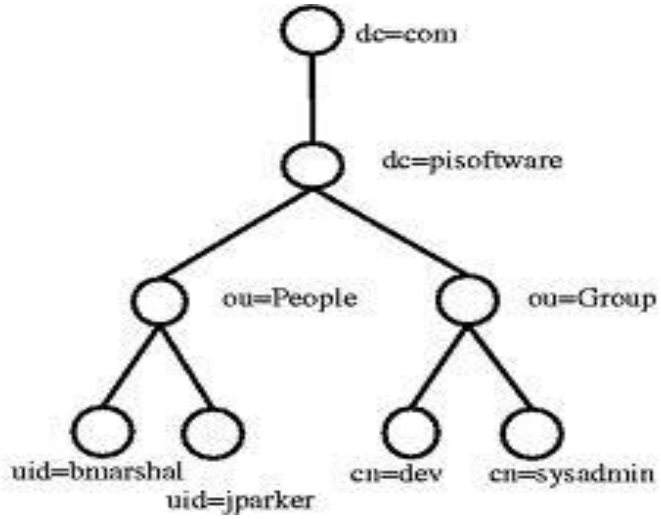
Se puede mencionar que un LDAP 3 es compatible con LDAP 2.

2.2. Directorio

Es una forma organizada para el almacenaje de información, un directorio maneja su estructura de forma jerárquica, un ejemplo claro es cómo maneja los sistemas Unix su sistema de directorios.

En si el directorio es como un árbol que se va extendiendo con sus ramas, de esta manera se trabaja la jerarquización. Así un directorio tiene una raíz o un inicio, donde todo se desprende. Esta forma de representar un directorio se le llama DIT (Árbol de información de directorio) ver figura 1.

Figura 1. **Ejemplo árbol jerárquico**



Fuente: elaboración propia.

Donde se puede observar como desde *dc=com*, la raíz, podemos ir descendiendo, atreves de sus hojas, hasta *cn=sysadmin.* De esta manera el en el árbol de jerarquización, podemos desarrollar el siguiente camino:

Dc=com,dc=pisoftware,ou=People,uid=bmarshal,uid=jparker

2.3. OpenLdap

OpenLdap es una implementación bajo licencia libre y de código abierta del protocolo LDAP, que maneja una gama de librerías bajo los estándares de LDAP, utilidades, herramientas y ejemplos de implementación.

Este software corre bajo distribuciones *G*NU/Linux, BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows y z/OS.

Está compuesto por tres elementos importantes:

- SLAP: Demonio del servidor
- Librerías bajo el protocolo LDAP
- Programas Clientes*: ldapsearch, ldapadd*, etc

OpenLdap puede soportar las siguientes características:

- Soporta LDAP V3, por consiguiente soporta SASL, TSL y SSL
- Soporte IPV6
- LDAP sobre IPC
- Soporte LDIF V1

2.3.1. Atributos LDAP

Al hablar de los atributos LDAP se quiere tocar los conceptos de directorios. Un directorio puede contener una cantidad de elementos, donde cada elemento representa algo específico, estos pueden crearse según la necesidad de cada sistema, pero de manera general existen elementos default.

- CN = *Common Name,* es el que identifica el nombre de un elemento
- DN = *DistingueshName*, es el atributo más importante, la base, la raíz. Este es por el cual se conoce la raíz del directorio, en este va incluido el usuario y la base general.

- OU = *Organizational unit*, contenedor regularmente para almacenar cuentas.

- DC = *Domain Component*
- Uid =*user id*
- *Givenname* = Nombre de la persona
- Sn = apellido de la persona

2.4. LDAPADMIN

Herramienta con la cual se conecta remotamente al servidor, es una implementación de distribución libre para la administración de un servidor LDAP*.*

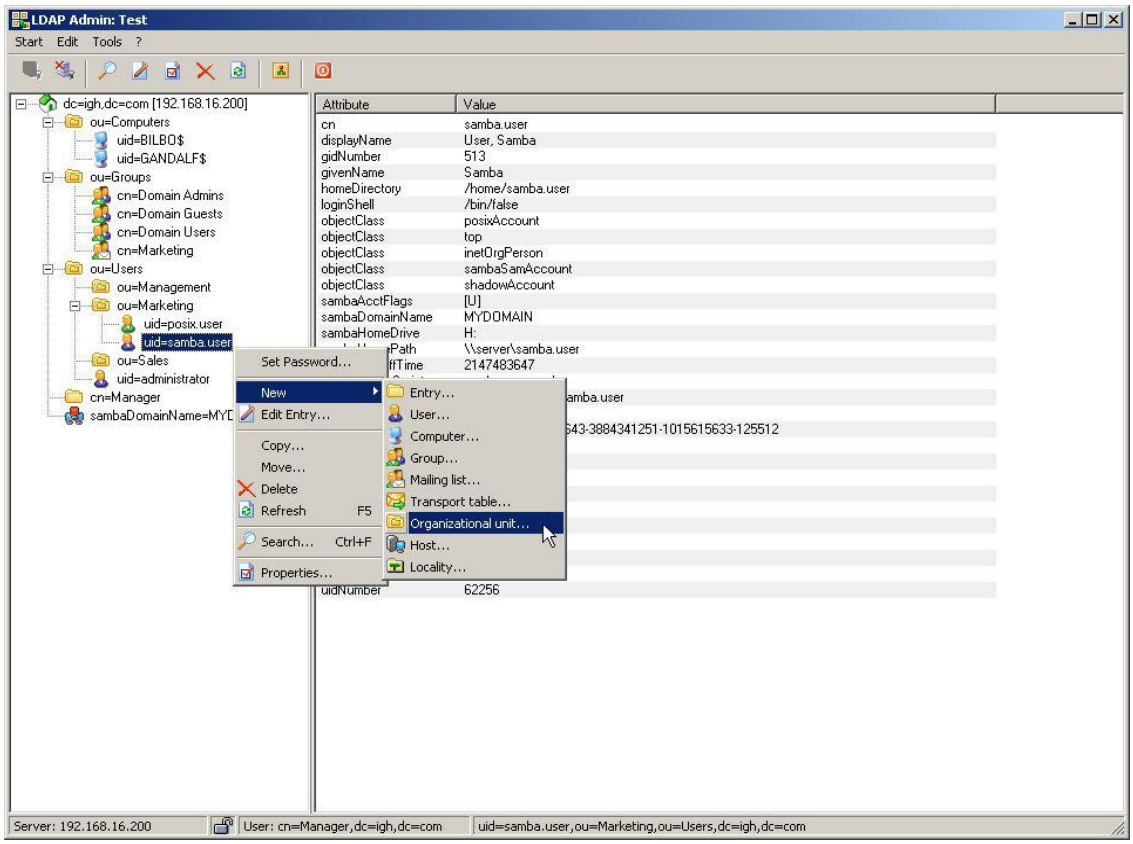
Es un administrador de LDAP que sirve para la gestión de directorios LDAP, de una forma visual e intuitiva. Permitiendo no solo la consulta de los datos sino que también la modificación y eliminación de información de los

arboles jerárquicos. En la figura 2 se muestra el entorno grafico de la herramienta.

Permite las siguientes acciones:

- Navegación y edición del directorio LDAP
- Ediciones de ABC
- Puede exportar e importar LDIF
- Gestión de contraseña, varios protocolos de encriptación

Figura 2. **Imagen de LDAPADMIN**



Fuente: elaboración propia con el programa Ldapadmin.

2.5. Replicación OpenLdap

Replicación en LDAP es la acción de reflejar todos los cambios en los datos de un servidor a otro. De tal forma que uno refleje la información del otro.

Existen 2 tipos de replicación, replicación maestro esclavo y multimaestro.

2.5.1. Maestro esclavo

Esta es la replicación más sencilla y es en la cual se manifiesta que solo en un servidor se puede realizar aspectos de escritura. Es decir el servidor maestro al hacer una escritura copia el DIT (Directoy Information Tree) hacia el servidor esclavo, manteniendo de esta forma una replicación de una sola vía. El servidor esclavo es siempre de lectura.

2.5.2. Multimaestro

Es la replicación por excelencia, en esta tanto servidor maestro, como esclavo pueden recibir escritura, por lo cual si se hace una escritura en cualquier de los servidores se crea un copia del DIT en el servidor contrario, por lo cual existe una replicación de ambas vías.

2.5.3. Diferencias

En la forma esclavo – maestro la configuración es configurado el módulo *syncrepl*, que es el encargado de realizar la replicación, con la diferencia que solamente en el esclavo es cargado el consumo que es referido hacia el servidor maestro.

En el modo multimaestros todos los servidores son referenciados como consumidores.

2.5.4. Módulo Syncrepl

Este módulo es el encargado de la sincronización y replicación dentro de los servidores LDAP. Es capaz de copiar una parte del árbol del directorio hacia el otro servidor, a la hora de que se realice un cambio, por lo cual el servidor consumidor puede fácilmente en base a este módulo saber que se modificó y tener una sincronización eficaz. Para controlar los cambios efectuados maneja un *Time Stamp* en cada servidor y uno en forma global ante un determinado evento.

2.5.5. Elementos de configuración de la réplica

El archivo que se debe configurar es el slapd.conf en el cual se tiene que agregar lo siguiente:

Primero se debe identificar a cada servidor con un índice único que lo identifique:

En este caso es *serverID 001*

Luego se debe configurar los aspectos esenciales de replicación:

Proveedor: de donde previenen los datos o el servidor que manda los datos.

Provider = ldap:/192.168.1.1:389

El tipo de replicación:

Type: RefreshAndPersit

Existen dos tipos *refreshAndPersist* y *RefreshOnly* la diferencia radica que en la primera abre un *socket* en el cual está verificando constantemente cambios y haciendo copias, en la segunda el servidor hace los cambios y posteriormente se desconecta.

Luego también se debe colocar lo siguiente:

Searchbase="dc=base,dc=ejemplo,dc=com"
Attrs=",+"*
Binddn="cn=admin,dc=base,dc=ejemplo,dc=com"
Credentials= pass

En sí estos serían los elementos a configurar:

2.5.5.1. *Provider*

Se indica la dirección IP hacia cual se hará la replicación, también se puede definir el nombre DNS del servidor.

2.5.5.2. *Type*

RefreshAndPersit que en si es forzar a replicar en el momento en el que se hace los cambios en un servidor.

2.5.5.3. *Retry*

Este parámetro indica cuantas veces el servidor intentará conectarse al otro servidor, si este se encuentra abajo. Existen 3 parámetros, el primero indica el tiempo entre cada intento de conexión, el segundo, cuantas veces se hará el intento de conexión, el tercero el tiempo que debe de pasar para volver a hacer otro intento luego de que se ha realizado lo configurado en los parámetros 1 y 2.

2.5.5.4. *SearchBase*

Es la base del servidor que tiene que buscar al conectarse al servidor. Siempre se define con los valores dc. Como en el ejemplo siguiente.

Dc=ejemplo,dc=com,dc=gt

2.5.5.5. *Attrs*

Es la forma en que se hará la búsqueda, que puede ser *scope*, *filter*, etc, al colocar *attrs*=”*,+” se define que se debe de recuperar todos los objetos y todos los atributos.

2.5.5.6. *Binddn*

Es el dn del usuario administrador. Es la dirección completa en el árbol jerárquico hacia el usuario administrador.

Cn=admin,dc=ejemplo,dc=com,dc=gt

2.5.5.7. *Credentiales*

Es la contraseña del usuario administrador definido en *Binddn*.

2.5.5.8. *Overlay Syncprov*

Con este parámetro cargamos el *Syncrov* para poder replicar.

2.5.5.9. *Syncprov-creckpoint*

Se refiere a la frecuencia con la que se realizara la validación de la integridad de datos entre los servidores.

2.5.5.10. *Syncrrov-sessionlog:*

Define la frecuencia de escritura del log por parte del servidor al momento de realizar las sincronizaciones con los otros servidores

2.6. Autenticación de Linux

Para poder realizar la autenticación de Linux por medio del protocolo LDAP son necesarios las siguientes 3 librerías*, libnss-ldap, libpam-ldap* y *nscd*.

2.6.1. *Libnss-ldap*

Esta librería es la encargá de decirle al sistema Linux, que la autenticación por medio del protocolo LDAP es posible, esta permite modificar el archivo */etc/nsswitch.conf*, donde se le indica que la autenticación es posible por medio de LDAP.

2.6.2. *Lib-pam*

Esta librería es la encargada de permitir usar PAM, que es una interfaz que permite que otros medios de autenticación sean posibles, en este caso el protocolo LDAP.

2.6.3. *NSCD*

Este es un demonio que guarda en cache los elementos de los usuarios que se autentican, haciendo más cómodo la forma de autenticación, por lo cual, cuando un usuario se autentica por primera vez, este guarda el nombre del usuario.

2.7. Log dentro de LDAP

El protocolo LDAP maneja varios tipos de log, según lo que se requiera, desde el concepto de tener una bitácora de cualquier proceso que se realice, solo configuraciones, autenticaciones o en su defecto no tener log.

El log de LDAP se realiza configurando el archivo *slap.conf* donde se le indica el nivel de detalle que se desea, este se escribe en el archivo */var/log/syslog,* el cual se puede modificar hacia otro archivo, media vez se configure el demonio *syslog*, indicándole otra ruta.

2.8. Autenticación en windows.

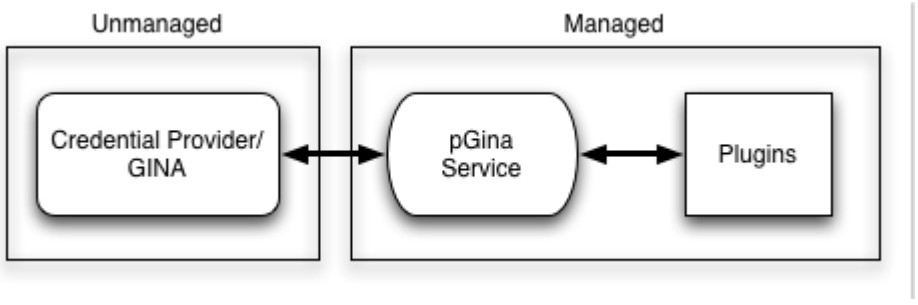
La autenticación de windows la realiza el componente denominado *Winlogon and credential provider* y se encarga de realizar las autenticaciones necesarias, además permite que otros proveedores rescriban sus componentes.

2.8.1. PGINA

Es un reemplazo para la autenticación de windows que viene por defecto. El reemplazo permite a PGINA cambiar la forma en que se autentican los usuarios en el sistema Windows permitiendo hacer la validación por medio de varios *plugins* incluyendo a un servidor LDAP.

El componente PGINA funciona añadiendo un servicio que extrae el control del componente GINA propio de Windows y luego le añade las nuevas formas de autenticación tal y como se muestra en la figura 3.

Figura 3. **Funcionamiento de PGINA**



Fuente: Pgina *Team, User's Guide*, www.pgina.org.

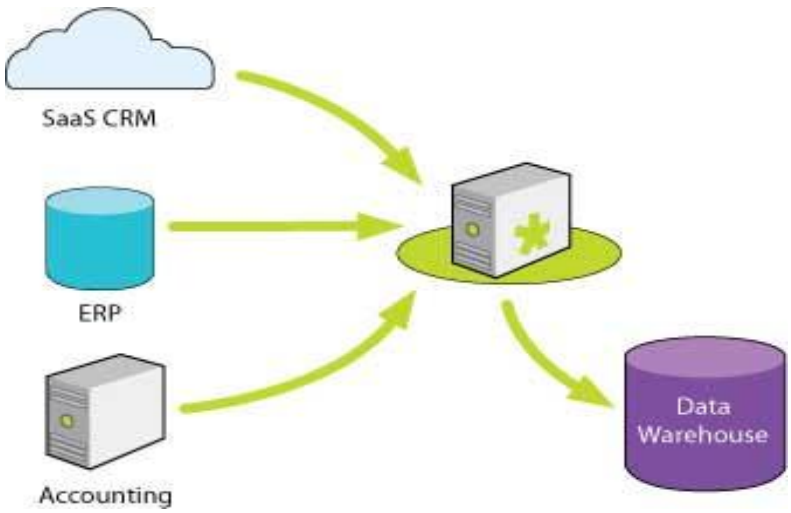
La forma de cómo configurarlo y administrarlo se encuentra en el apéndice A. al final de este trabajo.

2.9. ETL

Extracción, transformación y carga. Es un proceso que comprende múltiples pasos y tareas, enfocadas en transferir información de aplicaciones de producción hacia sistemas de inteligencia de negocios.

Una herramienta ETL siempre se encarga de conectarse a diferentes fuentes de información para cargarlas transformarlas unirlas y toda operación que se necesite para luego depositarla a otro conjunto variado de información de tal manera que la información o también hacia cubos de información de inteligencia de negocio. Dicha conexiones se ejemplifica en la figura 4.

Figura 4. **Proceso ETL**



Fuente: *Talend, Etl for analytics*, http://www.talend.com/solutions-data-integration/etl-for-analytics.php.

2.9.1. TALEND Open Studio *for data integration*

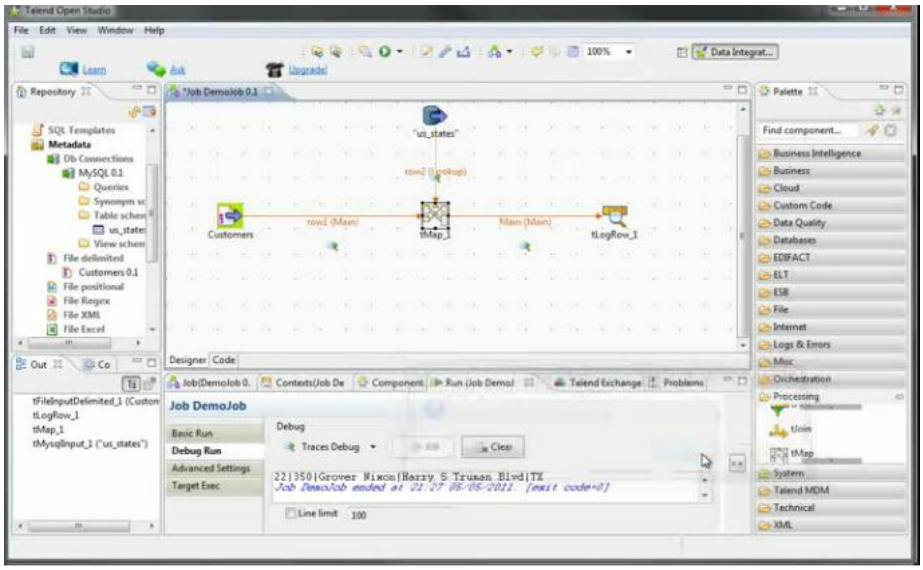
Es una herramienta ETL de código abierto, que permite la eficiencia de integración de datos a través de diseño de trabajos en un ambiente de desarrollo gráfico y fácil de utilizar. Para una referencia visual de Talend, véase figura 5.

Funciona bajo un servidor de aplicaciones en este caso un servidor Apache en el cual ejecuta todas las funciones en código java. La forma visual genera código en java que luego corre como una aplicación en el servidor.

Esto da la capacidad de poder correr los procesos de una forma desatendida y de una forma periódica según como lo configuremos en el servidor.

La herramienta es muy robusta ofreciendo un gran rango de tareas configurables, además de conexiones a base de datos archivos y múltiples formas de almacenar información lo convierten en una de las herramientas más completas cuando de ETL se trata.. Además de ser una aplicación que se puede utilizar en casi cualquier sistema operativo que soporte el servidor Apache

Figura 5**.** **Talend Studio**



Fuente: elaboración propia con programa Talend studio.

Talend Studio ofrece diferentes tareas, agrupadas en categorías, las cuales van desde condicionales hasta tareas complejas, tiene además la capacidad de simplificar tareas rutinarias tales como crear *logs* de las actividades que realiza.

3. FASE TÉCNICO PROFESIONAL

El proyecto a implementar en la institución tiene diferentes matices, en los cuales se definió el marco del proyecto delimitándolo y describiendo las tareas y pasos a seguir para llevar a cabo el proyecto.

3.1. Descripción del proyecto

El sistema a implementar en la institución, Centro de Cálculo e Investigación Educativa es un sistema que busca centralizar los usuarios de los distintos sistemas que la institución tiene a su cargo.

El sistema a implementar en esta fase del proyecto abarcará los siguientes sistemas:

- Autenticación de usuarios de sistemas internos
- Autenticación de usuarios de correo administrativo
- Autenticación de usuarios de correo de estudiantes
- Autenticación de usuarios de dominio
- Autenticación de usuarios de servidores

Dicha información de los sistemas se centralizarán en un único servidor LDAP, el cual contendrá políticas de alta disponibilidad, tales como sincronización con un servidor de respaldo.

3.2. Limitaciones

El proyecto denominado Sistema Único de Autenticación de Usuarios, Facultad de Ingeniería comprende varias fases de trabajo para poder ser completada.

En este proyecto únicamente se abarca las primeras 4 fases del proyecto las cuales son:

- Fase de análisis y diseño
- Construcción de árbol de LDAP
- Migración de cuentas
- Creación de redundancia

3.3. Fase de análisis y diseño

Todo proyecto necesita un análisis del problema y el respectivo diseño de su solución. Por lo que para iniciar este proyecto se realizará un documento que reúna los requerimientos que tenga la institución y también su solución a nivel de diseño, tomando en cuenta que dicha documentación será de vital importancia en las fases siguientes.

3.4. Construcción de árbol de LDAP

Para el almacenamiento de la información se utilizará un sistema basado en el protocolo LDAP, lo que hace necesario el diseño de un esquema de árbol jerárquico para almacenar la información de cada uno de los sistemas que se desean centralizar.

3.5. Migración de cuentas

Todos los sistemas a centralizar, claramente ya contienen cantidad considerables de información, además que están funcionando lo que hace necesario un plan de migración de datos, para mitigar los inconvenientes que puede dar la transición de los sistemas actuales al nuevo sistema centralizado.

3.6. Creación de redundancia

Para mitigar una de las desventajas más grandes de un sistema centralizado, se necesita de un sistema que tenga las características de alta disponibilidad, para poder tener un servidor de respaldo siempre en espera.

Además de una redundancia se espera que el sistema ofrezca el balanceo en el acceso a los servidores de tal forma de saturar lo menos posible al servidor, evitando sobrecargas y de baja de servicios por este medio.

La modificación de la información en el sistema se prevé que será escasa en cambio la lectura se espera que sea alta, por lo que el sistema debe de estar enfocado a la lectura sobre la escritura de registros.

3.7. Investigación preliminar para la solución del proyecto

El proyecto consiste en los siguientes aspectos:

- Diseño jerárquico en LDAP capaz de contener los diferentes tipos de usuario definidos en Centro de Cálculo e Investigación Educativa.

- Administrar los grupos de usuarios definidos en Centro de Cálculo e Investigación Educativa.

- Soporte de roles para los usuarios del sistema de software, basado en el modelo de base de datos actualmente utilizado.

- Administración de componentes de los sistemas de software y poder asignar permisos de accesos a dichos componentes.

- Permisos de acceso a los componentes de acuerdo al rol asignado al usuario.

- Poder alojar a los usuarios del tipo estudiante para realizar una autenticación de su cuenta de correo desde Google Aps. (Solamente definir la estructura).

- Poder manejar usuarios del sistema para los sistemas operativos GNU/Linux para autenticación vía LDAP y poder asignar a que usuario se autenticara.

- Poder tener una estructura capaz de autenticar a los usuarios del servidor de correo local Zimbra.

- Permitir autenticación para usuarios administrativos y docentes en sus computadoras personales y estaciones de trabajo.

3.8. Presentación de la solución del proyecto

Las herramientas a utilizar en su mayoría serán con licencias de código abierto. La elección de las herramientas se hizo en base a las necesidades de la institución y lo que se pretende optimizar con el nuevo sistema.

3.8.1. Herramientas a utilizar

Las herramientas a utilizar en su mayoría serán con licencias de código abierto. La elección de las herramientas se hizo en base a las necesidades de la institución y lo que se pretende optimizar con el nuevo sistema.

3.8.1.1. Sistema operativo

Se hará uso de un servidor con un sistema operativo Debían *6* squeeze. Por ser un servidor de altamente configurable, además que goza de una comunidad de soporte muy amplia.

El sistema operativo debían 6 es una de las implementaciones del kernel Linux, más reconocidas con una comunidad muy activa. Es muy estable, rápido y de poco consumo de recursos.

Debian es un sistema de código abierto y de muy buena documentación en la web, además sus repositorios están en constante actualización por los aportes de la comunidad, la seguridad en este sistema operativo es alta además que siempre hay actualizaciones de seguridad, que resuelven cualquier problema encontrado que ponga en peligro la seguridad del sistema.

3.8.1.2. Protocolo LDAP

Se hará uso del protocolo LDAP en su versión 3, porque ofrece mejores características de seguridad y replicación.

La versión 3 del protocolo ofrece extensiones al protocolo 2 en áreas como autenticación, referencia e implementación.

3.8.1.3. Servidor LDAP

Se utilizará el servidor SLAPD "*stand-alone LDAP daemon*" un servidor de OpenLDAP que es una implementación del protocolo LDAP, en su versión 2.4.25.

Este servidor tiene un muy buen rendimiento, ofreciendo la utilización de varias versiones del protocolo, es muy configurable y estable. Ofrece capacidades de replicación muy potentes.

3.8.1.4. Cliente LDAP

Para la autenticación de los equipos con el servicio de LDAP es diferente en los sistemas operativos.

En los sistemas operativos basados en Linux, no es necesario utilizar algún otro tipo de cliente o herramienta de terceros porque el mismo sistema operativo ofrece capacidades de autenticación con servidores LDAP

En el caso de computadoras con sistema operativos windows, es necesario la utilización de una herramienta de terceros, en este caso se hará

uso de PGINA que es una herramienta de código abierto, que forza al sistema operativo a autenticarse por medio del servicio de LDAP.

PGINA es una herramienta fácil de configurar, y que tiene una comunidad activa. Además funciona con múltiples versiones de windows.

3.8.2. Herramienta de administración

Para la administración del servidor SLDAP de una forma visual se hará uso de la herramienta LDAPADMIN.

LDAPADMIN es una herramienta visual que permite crear, editar y borrar esquemas, registros y directorios de un servidor LDAP. Se eligió esta herramienta por ser intuitiva, de una licencia de libre distribución.

3.8.2.1. Herramienta ETL

Para la extracción transformación y carga de información, de los sistemas actuales al nuevo servidor se utilizó la herramienta TALEND STUDIO

TALEND STUDIO es un software de código abierto, que permite la extracción y manipulación de información así como la carga a distintas base de datos y archivos. Permitiendo de esta forma realizar cargas automatizadas de un sistema a otro. También permite la capacidad de alojar dichas tareas en un servidor y ser ejecutadas periódicamente de una forma automática.

3.8.3. Tipo de replicación

Se decidió utilizar el tipo de replicación maestro maestro, porque ofrece una recuperación más rápida y cómoda que su contraparte, maestro esclavo.

El uso del modo de replicación maestro maestro, ofrece la posibilidad de poder consultar ambos servidores al mismo tiempo o de escribir en los 2 manteniendo una integridad de datos en ambos servidores. Esto nos da la capacidad de balancear el acceso a cada uno de los servidores a nivel de infraestructura y diseño.

Las ventajas que ofrece este tipo de replicación en esta implementación sobrepasan a sus desventajas.

La forma de instalación está en el apéndice.

3.8.4. Diseño de esquemas

Los esquemas en LDAP son la estructura de cómo se almacenaran los datos, y el diseño de los mismos es completamente fundamental porque un buen diseño permite que el almacenamiento y utilización de la información se haga de una forma fluida y rápida.

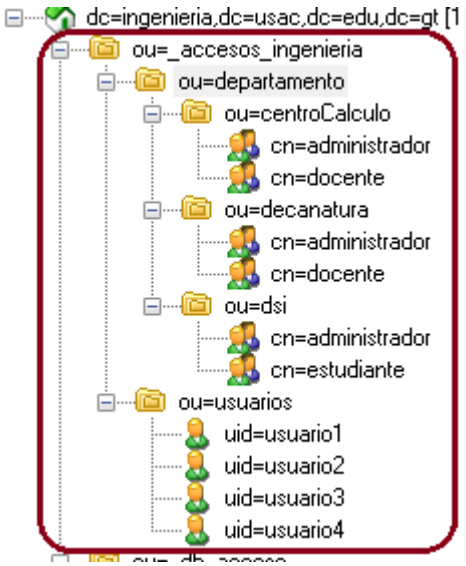
3.8.4.1. Esquema usuarios y dominios

La estructura de migración de *active directory* tuvo la creación de un directorio más complejo el cual se puede describir:

- Departamento
    - Nombre_Departamento
        - Rol
- Usuarios

Donde departamento, nombre_Departamento y usuarios son unidades organizacionales y rol un grupo.

Figura 6. **Esquema usuarios dominios**



Fuente: elaboración propia con el programa Ldapadmin

En la unidad organizacional denominada usuarios se tiene almacenado todos los usuarios de Active Directory sin excepción.

En la unidad organizacional, denominada departamento es el contenedor de todos los departamentos que pueda tener el sistema a cargo, este

departamento tiene asignado varios roles entre los cuales estarán asignados los usuarios que se encuentra dentro de la ou usuarios.

De esta manera se tendrá el control de los usuarios, los cuales estarán asignados hacia un rol específico dentro de un departamento específico.

3.8.4.2. Esquema correo administrativo

El correo administrativo se guardara de tal forma que el servidor Zimbra pueda utilizar los datos del servidor LDAP fácilmente, permitiendo la lectura y escritura.

El esquema del árbol jerárquico quedará de la siguiente forma:

- Usuarios_zimbra
  - People
    - uid=correo
      - ✓ firmas

Los correos administrativos son los correos internos manejados dentro del dominio de la página de ingeniería. “ingeniería.edu.gt”

3.8.4.3. Esquema autenticación servidores

En la institución se encuentran una cantidad considerable de servidores que se utilizan para diversas operaciones, y las cuales también se autenticarán con el servidor LDAP.

Para este sistema se utilizará el siguiente árbol jerárquico:

- Servidor
  - Cn=*servidor*
- Usuarios_servidores
  - Usuarios
    - Uid=usuario

Donde Usuarios_servidores es una unidad organizacional que tiene a los usuarios de los servidores que tiene a su cargo la institución de centro de cálculo e investigación educativa. Y servidor se refiere a un servidor específico.

3.8.4.4. Esquema autenticación correo estudiantes

Este esquema es para almacenar la información de los estudiantes de tal forma que el servicio prestado por Gmail pueda leer las autenticaciones en el servidor LDAP.

El esquema a realizar quedará de la siguiente forma:

- Correos_estudiante
  - Uid=estudiante

Donde correos_estudiante es una unidad organizacional que contiene a todos los usuarios que se tienen de alta en las base de datos de ingeniería. Específicamente la de los estudiantes.

3.8.5. Migración de datos

Para que se realice un cambio de un esquema y forma a otro de una forma correcta y con poco impacto, se realizó una migración de todos los datos actuales hacia el nuevo servidor implementado.

Esto se logró utilizando distintos procesos para cada uno de los sistemas a autenticar, en cada uno de ellos se utilizó una forma para poder migrar los datos de una forma correcta.

3.8.5.1. Traslado de la información de los sistemas

La información de la base de datos actual, se realizará su migración por medio de un proceso que se ejecutará automáticamente cada cierto periodo de tiempo.

Actualmente se tiene previsto que la ejecución de dicho proceso se realice diariamente. Y su función será de transmitir toda la información y sus modificaciones del servidor de base de datos actual hacia un árbol jerárquico en el servidor de openLDAP.

Esta migración será una réplica porque mantendrá actualizada la información de la base de datos en el servidor LDAP.

Este proceso fue desarrollado como un *job* utilizando la herramienta TALEND STUDIO. La cual tiene la capacidad de conectarse a múltiples base de datos incluyendo a servidores que utilicen el protocolo LDAP.

El proceso parte de la consulta de los datos en el servidor actual, que es un servidor postgresql y luego transforma dichos datos a su equivalente de árbol jerárquico y lo carga al servidor LDAP que se implementó.

3.8.5.2. Migración de Zimbra

Zimbra es un servidor para el uso de correo electrónico, por lo cual se necesita migrar los usuarios existentes dentro de zimbra hacia el servidor LDAP.

La estructura como se almacena los elementos de Zimbra es muy similar o más bien se guardan en una estructura como la de un servidor ldap, por lo cual tiene dn, cn, sn, uid, userpassword, mail y otros elementos que son propios de Zimbra.

Por lo cual los pasos para poder migrar la información de Zimbra hacia el servidor LDAP fueron los siguientes:

Se crea un archivo LDIF donde está toda la información de los usuarios de zimbra.

Se debe de modificar ese archivo LDIF para que sea compatible con el servidor LDAP por lo cual se modifica el dn, el dn a utilizar seria ou=people,ou=usuarios_zimbra,dc=ingenieria,dc=usac,dc=edu,dc=gt, sería el lugar correspondiente donde los usuarios de Zimbra migrarían dentro del servidor LDAP.

Como Zimbra utiliza elementos propios de él, dentro del servidor LDAP no existen los *schemas* necesarios para poder migrar con éxito los datos que Zimbra maneja de forma propia, por lo cual se instala dentro del servidor dos schemas nuevos Zimbra.schema y LDAP.*schema*, los cuales se pueden descargar de la página de ayuda de Zimbra.

Luego de instalar los *schemas* de Zimbra es necesario reiniciar el servidor.

Al reiniciar el servidor todo se encuentra ya en orden, por lo cual lo único que se debe de realizar es introducir el archivo LDIF en el servidor LDAP y poder migrar exitosamente los usuarios de Zimbra.

3.8.5.2.1. Instalación de *schemas* de Zimbra en LDAP

Dentro del directorio */etc/ldap/schema* se necesita agregar los archivos zimbra*.schema* y LDAP.*schema.*

Luego en el archivo de configuración /usr/share/slapd/sladp.conf en la parte de *include* se necesita agregar la siguiente dos líneas:

- Include /lib/ldap/schema/zimbra.schema
- Include /lib/ldap/schema/LDAP.schema

Se reinicia el servidor LDAP, /etc/init.d/sladp restart, listo schemas instalados.

3.8.5.3. Migración de usuarios de *Active Directory*

Active Directory utiliza de igual manera la estructura de ldap para guardar la información de sus usuarios, claramente con estructuras propias, para hacer la migración de datos, es un proceso de alto cuidado.

La migración de Active Directory fue un proceso costoso, ya que utiliza una estructura general que no se encuentra dentro de un servidor LDAP, utiliza un *schema* propio, el problema radica en que este *schema* es de uso privativo por lo cual no se puede migrar hacia un servidor LDAP.

Al utilizar Active Directory un *schema* privativo la información que se tiene que migrar hacia un servidor LDAP se filtró, catalogando los aspectos importantes o información del usuario que realmente se necesita entre esos datos se mencionaron los siguientes:

- Dn
- Cn
- Sn
- DisplayName
- userPassword
- uid
- givenName

Por lo cual para poder migrar esos datos se tuvo que utilizar un *schema* del sistema y se hizo una migración a mano.

Dentro de la clase *PosixAccount* se puede observar que es la estructura perfecta para los datos que se requieren para los usuarios de Active Directory, acoplándose al 100% a lo que se necesita.

3.8.6. Autenticación de clientes LDAP

La autenticación se refiere a la capacidad de un sistema de poder pedir comparar la información de acceso proporcionada localmente con el servidor centralizado, esta petición se realiza de distinta forma entre los diferentes sistemas operativos.

3.8.6.1. Autenticación de servidores Linux

Como uno de los propósitos es que atreves del servidor LDAP se pueda autenticar los servidores existentes que están sobre sistemas operativos Linux, es necesario realizar ciertas modificaciones en estos servidores.

Se debe de instalar 3 librerías, siendo estas las siguientes:

- Libnss-ldap: la cual es necesaria para que el servidor LDAP pueda suplantar los archivos */etc/passwd, /etc/group* y */etc/shadow* como base de datos del sistema.

- Libpam-ldap: es la que permite hacer la autenticación por medio de LDAP, es el que proporciona el medio para lograr que la autenticación por medio de ldap sea posible sobre un sistema Linux.

- Nscd: si por medio de la librería nss podemos lograr suplantar los archivos */etc/passwd*, */etc/group* y */etc/shadow* esta librería es la encargada de indicar que la autenticación se hará por medio de LDAP.

  Se deben de modificar 3 archivos que son:

- */etc/nsswitch.conf*: autoriza autenticarse por medio de LDAP
- */etc/libnss-ldap.conf*: realiza el filtro de los usuarios permitidos en el cliente, que pueden autenticarse.

- */etc/pam.d/common-session*: permite configurar la creación del directorio home del usuario.

3.9. Costos del proyecto

El proyecto se realizó con recursos propios del Centro de Cálculo e Investigación Educativa los cuales son los siguientes:

- 2 servidores con sistema operativo *Debian*
- Infraestructura de red
- Energía eléctrica

Y un costo de desarrollo, distribuidos entre diferentes rubros de la siguiente forma:

Tabla I. **Tabla costo proyecto**

Recursos	Cantidad	Costo unitario	Subtotal
Consultora institución	1 persona 20 días	500 el día	10,000
Consultor Escuela	1 persona 20 días	500 el día	10,000
Configuración de los servidores	2 personas 100 días.	100 el día persona	20,000
Desarrollo TALEND	2 personas 10 días.	100 el día persona.	2,000
Impresiones	100 impresiones	0.25	25
Materiales oficina	400		400

Costo Total: Q 42,425

Fuente: elaboración propia.

3.10. Beneficios del proyecto

- Centralización de los distintos sistemas, para su fácil administración
- Aumento de la eficiencia y el tiempo de respuesta al cambio de permisos en un servidor o terminal.

- Actualización de los sistemas de autenticación actuales, trayendo consigo todas las ventajas de las nuevas tecnologías.

- Mitigación de resistencia al cambio de los sistemas. Al momento de actualizar el sistema se migraran los datos actuales para que los usuarios no tengan problemas al cambio.

- Seguridad en los usuarios y autenticaciones de los sistemas permitiendo el uso de las nuevas tecnologías en encriptación.

4. FASE ENSEÑANZA APRENDIZAJE

El sistema implementado será mantenido por el propio recurso humano de la institución por lo que se procedió a elaborar material de guía y capacitación a los técnicos encargados de darle soporte al nuevo sistema.

4.1. Capacitación realizada

La institución, Centro de Cálculo e Investigación Educativa, actualmente está dividida en varios departamentos organizaciones, donde cada departamento cumple una función específica para la organización.

En este caso el proyecto está bajo la supervisión del departamento de redes en el cual existe un coordinador y varios técnicos.

Para este proyecto se capacitó al técnico encargado del proyecto como se muestra en la siguiente ficha.

Tabla II. **Ficha de capacitación 1**

Nombre	Juan Fernando García Ochoa
Perfil	Técnico redes.
Horas de capacitación	40 horas
Capacitación	8 horas nivel funcional 32 horas nivel técnico.

Fuente: elaboración propia.

Además se capacitó e informó a la coordinadora del departamento sobre las funcionalidades del proyecto. La capacitación se realizó como se muestra en la siguiente ficha:

Tabla III. **Ficha de capacitación 2**

Nombre	Inga. Susan Gudiel
Perfil	Coordinadora departamento redes
Horas de capacitación	8 horas.
Capacitación	7 horas nivel funcional 1 nivel técnico

Fuente: elaboración propia.

4.2. Material elaborado

Se realizó un manual sobre las instalaciones de los componentes principales del servidor, además de una guía sobre los procesos críticos del sistema.

Este material se adjunta en el apéndice 1.

CONCLUSIONES

1. En la implementación del sistema, se logró la utilización total de software con licencia de código abierto en todos los servidores de administración en la institución, logrando el objetivo de hacer uso de solo software de licencia libre.

2. Al tener un sistema de centralización, la administración y control de los distintos usuarios que se autentican en múltiples sistemas se convierte en una tarea más rápida, segura y simple, ofreciendo la facilidad del ingreso de un único usuario a diversos sistemas y proveyendo respuesta más rápida a ellos, logrando una automatización en la administración y control de usuarios.

3. La replicación de tipo multimaestro ofrece una mejor respuesta ante caída del sistema, ofreciendo una recuperación total del sistema de una forma más simple y sin dejar de prestar todos los servicios.

4. La utilización de herramientas ETL permite el traslado de la información con menos esfuerzo y con un mayor control en un proceso de migración con información extensa y heterogénea.

5. La documentación sobre la tecnología del sistema aun es escasa por lo que la documentación elaborada en este proyecto cubre detalles técnicos que aún no son sencillos de encontrar.

RECOMENDACIONES

1. Al Centro de Cálculo e Investigación Educativa se les sugiere que al momento de analizar y diseñar un nuevo sistema, siempre tomen en consideración sistemas basados en tecnologías con licencia libre, de tal manera lograr una reducción en su costo en lo referente a licencias.

2. En el sistema implementado se utilizó una interfaz de usuario de terceros si bien es una implementación adecuada, ayudaría a la administración con una interfaz de usuario desarrollado a la medida permitiendo un mejor control visual del sistema.

3. El sistema por su diseño tipo multimaestro siempre mantiene un *Backup* del sistema, pero es prudente realizar un *backup* completo del sistema periódicamente para tener un respaldo como última instancia a los niveles de respuesta a fallos del sistema.

4. A la institución se les propone que al momento de realizar futuras migraciones utilicen herramientas de ETL para realizar la transición de una forma simple y a la vez integra.

5. Cualquier cambio o requerimiento nuevo que sea implementado, agregar a la guía creada de este proyecto la forma en que se realizó de una forma detallada y técnica, de tal manera de expandir la información disponible de la tecnología utilizada.

BIBLIOGRAFÍA

1. Blog Wordpress. *Replicación de servidores LDAP* [en línea]. [ref. 24 de julio de 2011]. Disponible en Web: <https://devsysadmin.wordpress.com/2011/07/24/openldap-2-4-mestro-maestro-en-debian-6-squeeze-phpadminldap/>.

2. Comunidad Arch Linux*. Autenticación de usuarios LDAP* [en línea]. [ref. 9 de junio de 2011]. Disponible en Web: <https://wiki.archlinux.org/index.php/LDAP_Authentication>.

3. Comunidad de software libre. *Autenticación de usuarios LDAP* [en línea]. [ref. 29 de enero de 2011]. Disponible en Web: <http://hpantaleev.wordpress.com/2011/07/24/openldap-2-4-mestro-maestro-en-debian-6-squeeze-phpadminldap/>.

4. Comunidad OpenLDAP. *Master to slave replication* [en línea]. [ref. septiembre de 2008]. Disponible en Web: <http://www.openldap.org/lists/openldap-software/200809/msg00157.html>.

5. Grupo de trabajo IFLICA. *Instalación física y lógica de una red cableada e inalámbrica en un aula* [en línea]. Almería, España: I.E.S Cura Valera, [ref. 19 de junio de 2006]. Disponible en Web: <http://informatica.iescuravalera.es/mod/resource/view.php?id=257>.

6. PGina Team. *PGina documentación oficial* [en línea]. <http://pgina.org/docs/v3.0/index.html>. [Consulta. agosto de 2012].

7. Red Had Red Satelital Red Hat, *Guia de despligue* [en línea]. USA, 1801 Varsity Drive, 2010 <https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Network_Satellite/5.3/html/Deployment_Guide/> [Consulta. agosto de 2012].

APÉNDICE

A.1. Instalación de OpenLDAP en Debian Squeeze

Para esta guía es necesario tener instalado correctamente Debian Squezee de una forma estándar, para luego instalarle los nuevos repositorios.

A.1.1. Actualizar Repositorios Debían Squeeze:

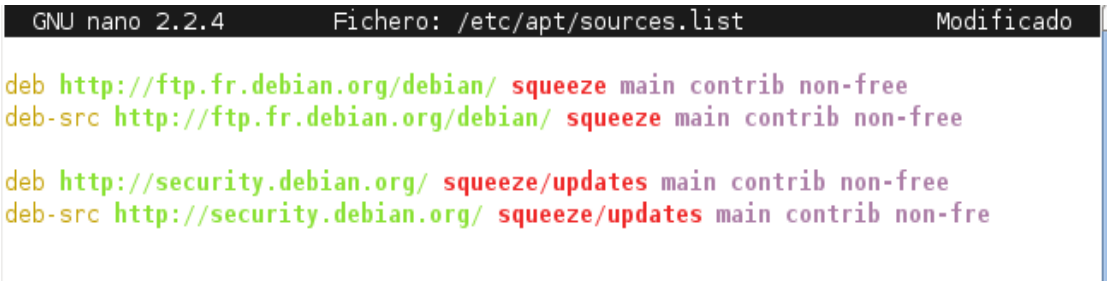
Lo primero que se tiene que hacer es actualizar los repositorios de *Debian Squeeze*, por lo que se tiene que modificar el archivo */etc/apt/sources.list*

Se agrega lo siguiente:

##OFICIALES
Deb http://ftp.fr.debian.org/debian/ squeeze main contrib non-free
Deb-src http://ftp.fr.debian.org/debian/ squeeze main contrib non-free

Existen muchos más como de seguridad, multimedia, etc., pero en este caso no son necesarios.

Figura A-1. **Repositorios Oficiales Debian Squeeze**



Fuente: elaboración propia. Consola de GNU nano 2.2.4.

Luego de esto se debe actualizar los paquetes en el servidor

Apt-get update

Lo primero que se tiene que realizar es instalar los siguientes paquetes en el servidor:

- Slapd
- Ldap-utils

Apt-get install slapd ldap-utils.

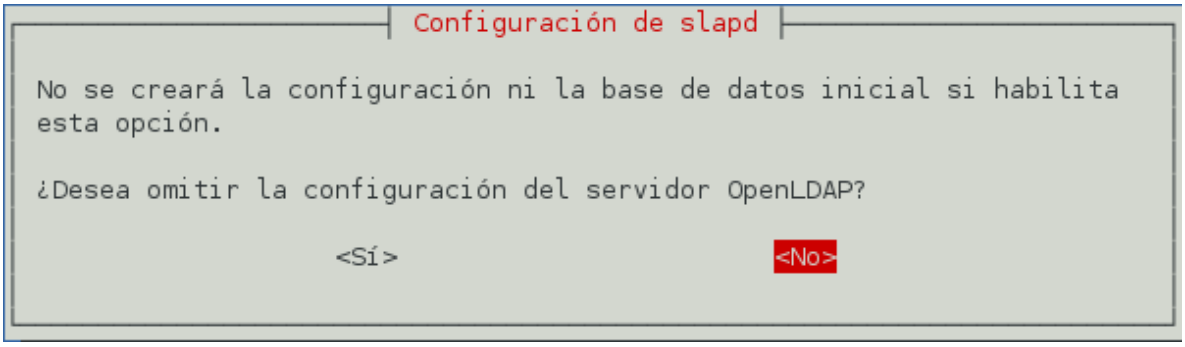
Luego de la instalación se debe reconfigurar el demonio de slapd con el siguiente comando:

Dpkg-Reconfigure slapd

El sistema pedirá los siguientes pasos:

a. Desea omitir la configuración del servidor OpenLDAP?: NO

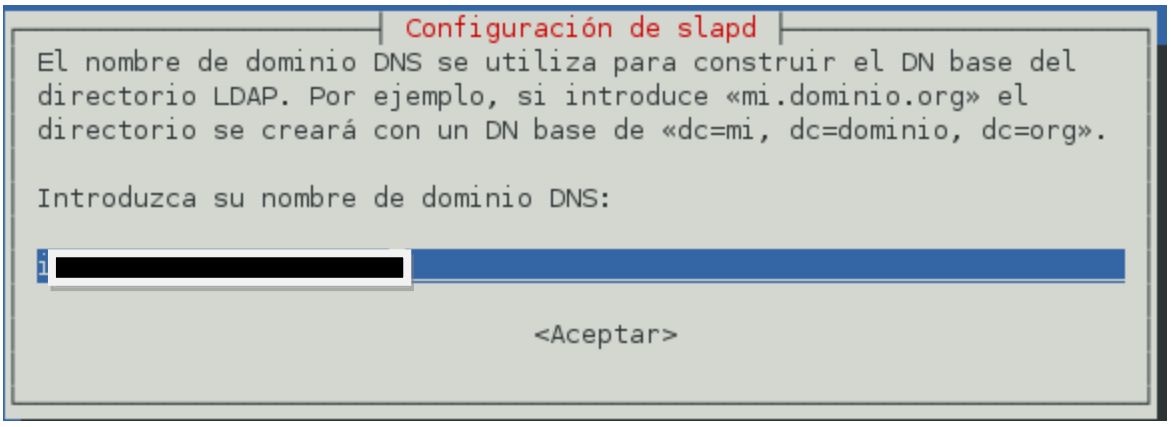
Figura A-2. **Configurar el Sistema OpenLDAP**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

b. Introduzca su nombre de dominio DNS: ingeniería.usac.edu.gt

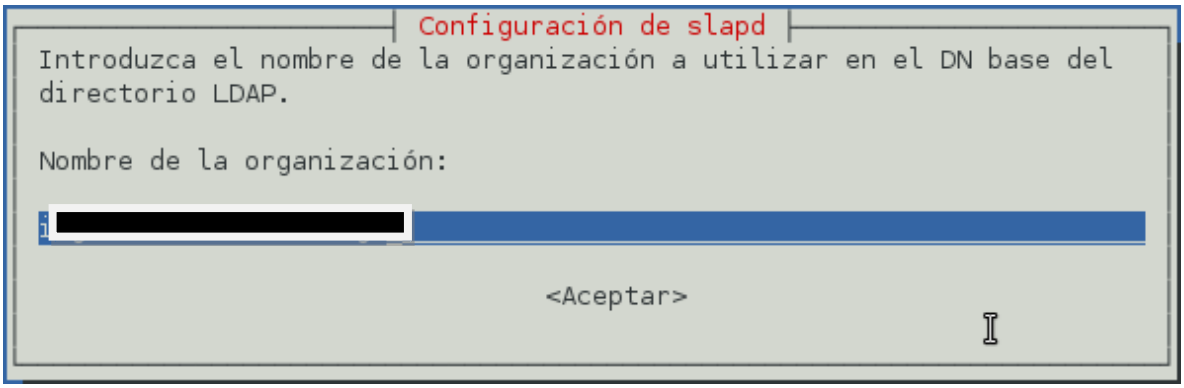
Figura A-3. **Ingreso de Dominio DNS**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

c. Nombre de la organización: ingeniería.usac.edu.gt

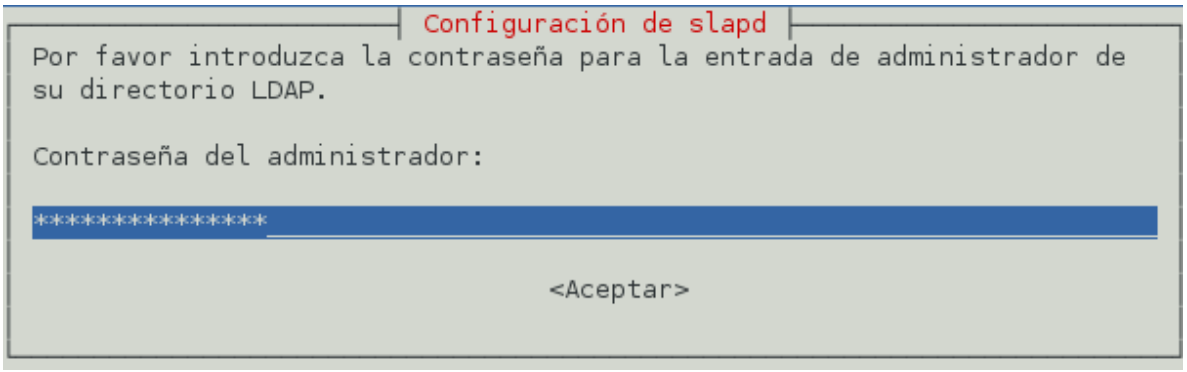
Figura A-4. **Ingreso DN Base de Directorio LDAP**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

d. Contraseña del administrador: *password*

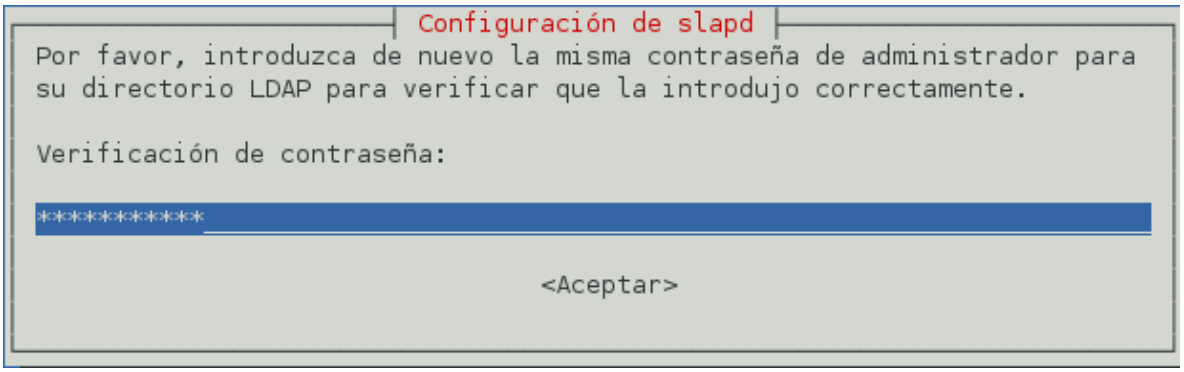
Figura A-5. **Ingreso de Contraseña**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

e. Verificación de la contraseña: *password*

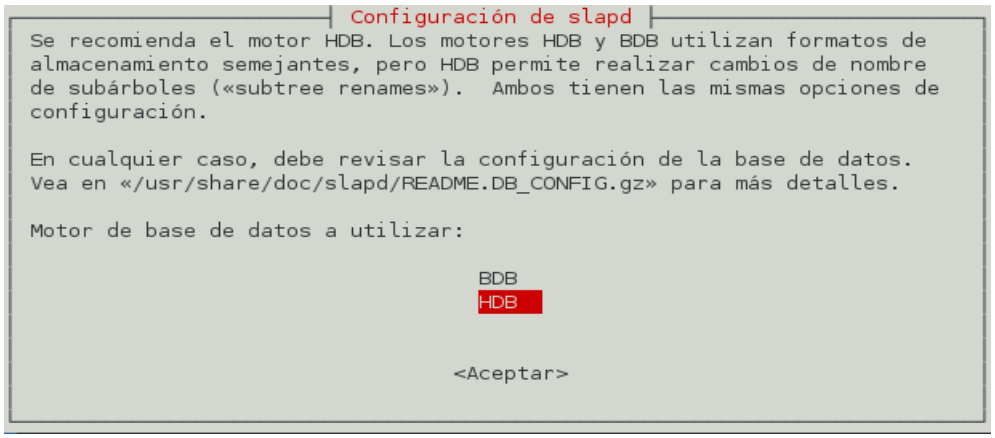
Figura A-6. **Verificación de Contraseña**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

f. Motor de base de datos a utilizar: HDB (recomendada)

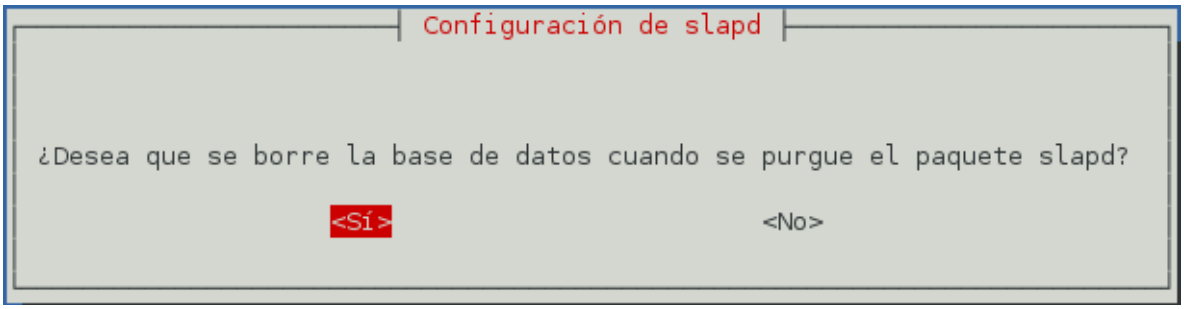
Figura A-7. **Seleccionar motor de base de datos**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

g. ¿Desea que se borre la base de datos cuando se purgue el paquete slapd?: SI

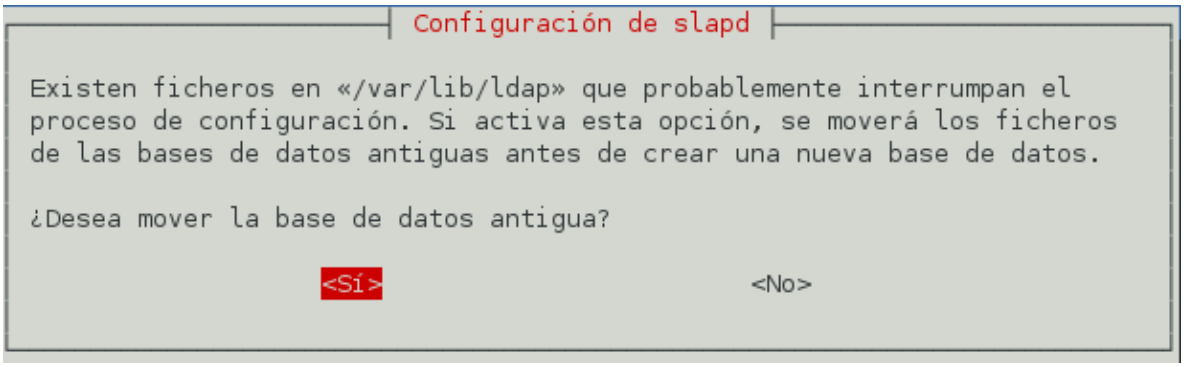
Figura A-8. **Purgar Base de Datos anterior**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

h. ¿Desea mover la base de datos antigua?: SI

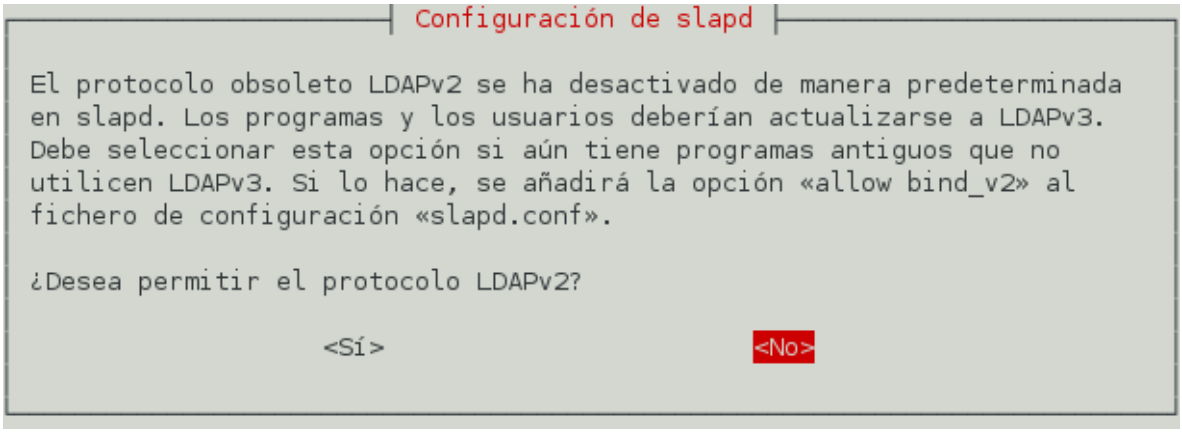
Figura A-10. **Mover la base de datos antigua**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

i. ¿Desea permitir el protocolo LDAPv2?: NO (usaremos V3)

Figura A-11. **Seleccionar protocolo de LDAP**



Fuente: elaboración propia. Programa de configuración OpenLDAP.

Por último se indica que utilizaremos el archivo *slapd.conf* como base para correr los servicios, agregamos lo siguiente:

En el archivo /etc/default/slapd se modifica la línea “LAPD_CONF =” agregando la ruta del archivo slapd.conf.

SLAPD_CONF="/usr/share/slapd/slapd.conf"

Figura A-12. **Seleccionar Archivo de Configuración slapd**

Fuente: elaboración propia. Consola de GNU nano 2.2.4

A.2. Log en el servidor LDAP

Openldap maneja los siguientes niveles de log, según el número que se le asigna, los distintos valores se muestran en la Tabla A-1:

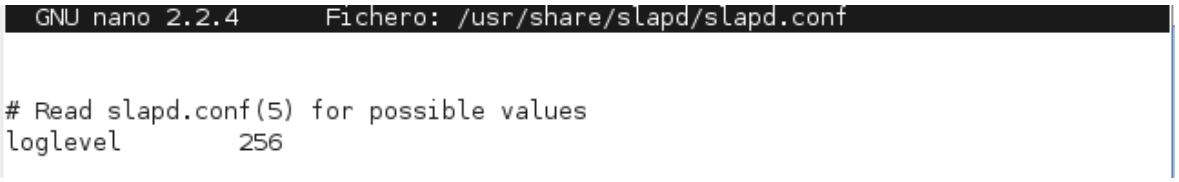
Tabla A-1. **Configuraciones posibles de Log**

-1	**enable all debugging**
0	*no debugging*
1	*trace function calls*
2	*debug packet handling*
4	*heavy trace debugging*
8	*connection management*
16	*print out packets sent and received*
32	*search filter processing*
64	*configuration file processing*
128	*access control list processing*
256	*Stats log connections/operations/results*
512	*stats log entries sent*
1024	*print communication with shell backends*
2048	*print entry parsing debugging*

Fuente: elaboración propia.

Para asignar el número de log que se desea, se modifica el archivo slapd.conf de la siguiente manera:

Figura A-12. **Configurar Nivel de Log**



Fuente: elaboración propia. Consola GNU nano 2.2.4

Por *default* los log de ldap se dirigen hacia el archivo */var/log/syslog*

Pero si deseamos que se dirija hacia otro archivo se tiene que modificar el archivo:

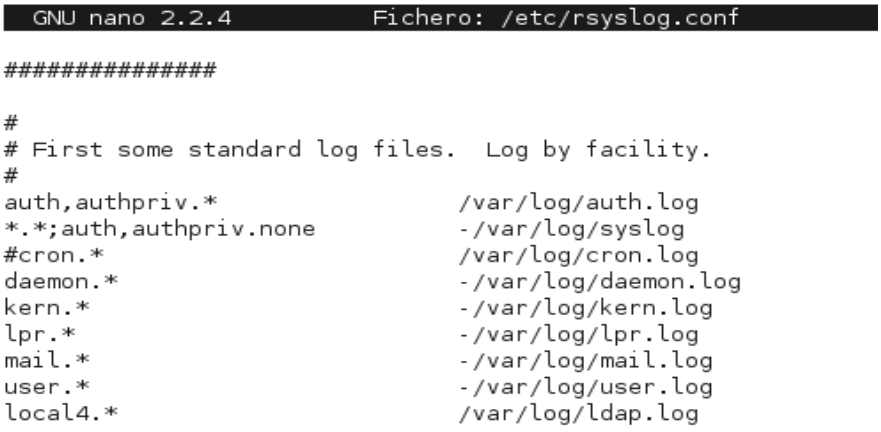
/etc/rsyslog.conf

Y agregar la siguiente línea:

local4. /var/log/ldap*

Al agregar dicha línea al archivo queda el archivo de la siguiente forma, mostrado en la figura A-13, que es una toma de pantalla del contenido del editor nano con el contenido del archivo *rsyslog*.

Figura A-13. **Modificación archivo rsyslog**



Fuente: elaboración propia. Consola GNU nano 2.2.4.

Donde eso hará que se redirige todo lo correspondiente a ldap hacia el archivo */var/log/ldap*

Figura A-14. **Verificación de Archivo Log**

Fuente: elaboración propia. Consola GNU nano 2.2.4.

A.3. Manual de Replicación LDAP

- Maestro – Esclavo: Cuando del servidor principal se replica hacia uno o más servidores secundarios, pero no viceversa.
- Maestro – Maestro: Cuando la replicación es ambas vías de los n servidores existentes. (regularmente 2).

En este caso la replicación que vamos a aplicar es una Maestro-Maestro en 2 servidores únicamente.

A.3.1. Modificar el archivo */etc/default/slapd*

En este archivo se indica al servidor Ldap que se va a trabajar con el archivo de configuración *slapd.conf*

Este archivo en la versión *Debian squeeze* se encuentra en */usr/share/slapd/slapd.conf*

Se edita el archivo /etc/default/slapd dejándolo de la siguiente manera en la parte que corresponde.

```
SLAPD_CONF=”/usr/share/slapd/slapd.conf”
```

Este paso, es importante, si no se realiza el servidor nunca trabajara sobre el slapd.conf.

Figura A-15. **Modificar Archivo SLAPD_CONF**

Fuente: elaboración propia. Consola GNU nano 2.2.4.

A.3.2. Datos de los servidores

- El servidor 1 tendrá la siguiente IP 192.168.1.7 mascara 255.255.255.0
- El servidor 2 tendrá la siguiente IP 192.168.1.8 mascara 255.255.255.0
- El dn de ambos servidores será = dc=ingenieria,dc=usac,dc=edu,dc=gt
- El nombre del administrador = *admin*

A.3.4. Editar el archivo /usr/share/slapd/slapd.conf

Este archivo ya tendrá una base para poder trabajarlo únicamente se debe de ir modificando poco a poco lo que necesitamos.

Se colocara todo el archivo para poder entenderlo de mejor manera y dar puntos claves:

- *ServerId*: Es el nombre que identifica al servidor, este se utiliza en el caso de replicación. Cada ServerId es distinto en cada sistema de LDAP, en el servidor 01 el ServerId es 001 y en el servidor 02 el ServerId es el 002.

- *Syncrepl*: Lo que realiza este elemento es que cuando se realiza una modificación crea un *TimeStamp* (Información que guarda hora y fecha de

un evento especifico) al momento en que se realizó, guardándose en la base de datos y existe un *timestamp* global que contiene el valor para la última modificación existente. Por lo cual para la replicación el *timeStamp* se conecta al *TimeStamp* global, se compara entre ellos y se replica lo que se ha realizado entre estos dos timeStamp. En esta línea se le indica el RID o ServerID hacia cual tendrá que estar en conexión.

- *provider*: Indicamos la dirección IP hacia cual se hará la replicación
- *Type: RefreshAndPersit* que en si es forzar a replicar en el momento en el que se hace los cambios en un servidor.

- *Retry*: Este parámetro indica cuantas veces el servidor intentara conectarse al otro servidor, si este se encuentra abajo. En este caso sería el primer 5, el tiempo en el cual hará la prueba de conectarse, el otro 5 las veces que realizara o intentara conectarse y el 300 el tiempo en segundos en el que volverá a tratar de conectarse luego de hacer 5 intentos cada 5 segundos.

- *SearchBase*: es la base del servidor que tiene que buscar al conectarse al servidor.

- *Attrs*= Es la forma en que se hará la búsqueda, que puede ser scope, filter, etc, al colocar attrs="*,+" definimos que se debe de recuperar todos los objetos y todos los atributos.

- *Binddn*= Es el usuario administrador
- *Credentiales = Password*
- *Overlay Syncprov*: Cargamos el *Syncrov* para poder replicar
- *Syncprov-creckpoint*: La frecuencia de escritura en la base de datos

- *Syncrrov-sessionlog*: La frecuencia de escritura del log

Figura A-16. **Modificación archivo slapd.conf**

Fuente: elaboración propia. Consola GNU nano 2.2.4.

A.4. Manual de personalización de esquemas

A.4.1. Archivo .schema

Los archivos de esquemas de LDAP se encuentran en /etc/ldap/schema/, si se desea agregar un nuevo esquema se agrega el archivo en esa dirección y luego se agrega la línea de con la dirección a ese archivo, en el archivo de configuración de slapd.conf que se encuentra en /usr/share/slapd/slapd.conf

La estructura de los archivos de esquema es completamente sencilla.

Primero se tiene que definir el id a utilizar por nuestro, esquema una vez elegido nos enfocamos a los atributos y luego a las clases.

A.4.2. Oid:

Es el número identificador de un atributo, clase, sintaxis esquema. Es una de las primeras definiciones a realizar al momento de crear un archivo de esquema.

Primero definimos el root de nuestro esquema

objectIdentifier EJEMPLOroot x.x.x.x.x.x.xxx

Luego definimos el root del esquema

objectIdentifier EJEMPLOLDAP CCIEroot:3

Luego definimos el root de los atributos

objectIdentifier EJEMPLOAttrType CCIELDAP:1

Y el root de las clases.

ObjectIdentifier EJEMPLOObjectClass CCIELDAP:2

Después el valor oid único para cada atributo, tomar en cuenta que en este caso se agrega el oid a la frase atributo de esta manera al ser mencionado en en la definición de un atributo este tomara el número oid que se defina en esta parte del archivo.

objectIdentifier atributo EJEMPLOAttrType:5

También el valor oid único para cada clase

objectIdentifier nombreClase EJEMPLOObjectClass:10

A.4.3. Definición de un atributo

attributeType(oid <número oid>
NAME <nombre del atributo>
DESC <descripción del atributo>
EQUALITY <como se comparara al momento de realizar búsqueda>
SBSTR <si es string si buscara substring o no>
SYNTAX <la sintaxis a utilizar>
SINGLE-VALUE <si solo se permitirá un valor en la clase o varios>)

Ejemplo:

attributetype (atributo
NAME 'atributo'
DESC 'tipo string'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{500}
SINGLE-VALUE)

A.4.4. Herencia

Un atributo o clase puede heredar todas las definiciones a otras únicamente utilizando al final la definición SUP

Ejemplo:

attributetype (url
NAME 'url'
DESC 'define la url de un componente'
SUP atributo)

A.4.5. Definición Clase:

Se definen, los valores oid, nombre, superior o herencia el tipo de clase y los atributos que debe de llevar, y los que podría llevar

Los tipos de clase que existen son *AUXILIARY* y *STRUCTURAL*. La diferencia es que la primera no puede crear un componente por si sola si no que necesita ser combinada con una del tipo *STRUCTURAL*.

La de tipo STRUCTURAL define por si sola un componente LDAP se puede combinar con una o varias clases AUXILIARY pero nunca con otra tipo STRUCTURAL.

objectclass (<numero oid>
NAME ‘<nombre de la clase>’
SUP top <STRUCTURAL/AUXILIARY>
DESC '<descripcion de la clase>'
MUST(<lista de atributos que debe contener>)
MAY(<lista de atributos que puede conetener o no>)
)

A.4.6. Ejemplo definición clase

```
objectclass ( unidadClase
 NAME 'unidadClase'
 SUP top STRUCTURAL
 DESC 'unidad administrativa'
 MUST(unidadid $ unidad $ nombre )
 MAY( descripcion )
 )
```

A.5. Manual Autenticar un servidor Linux

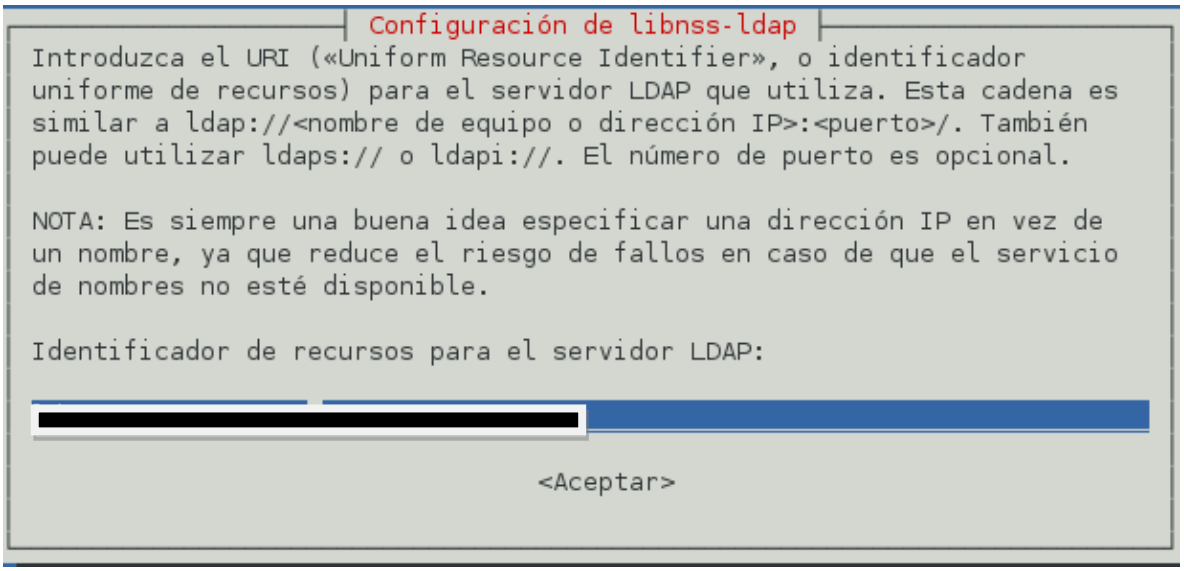
La autenticación de los servidores se hara por medio de las librerías pam, las cuales se tienen que configurar como se enumera a continuación.

A.5.1. Pasos de Instalación

Instalar las 3 librerías requeridas anteriormente libnss-ldap, libpam-ldap, nscd.

Dpkg-reconfigure libnss-ldap
Dirección del servidor LDAP (IP)

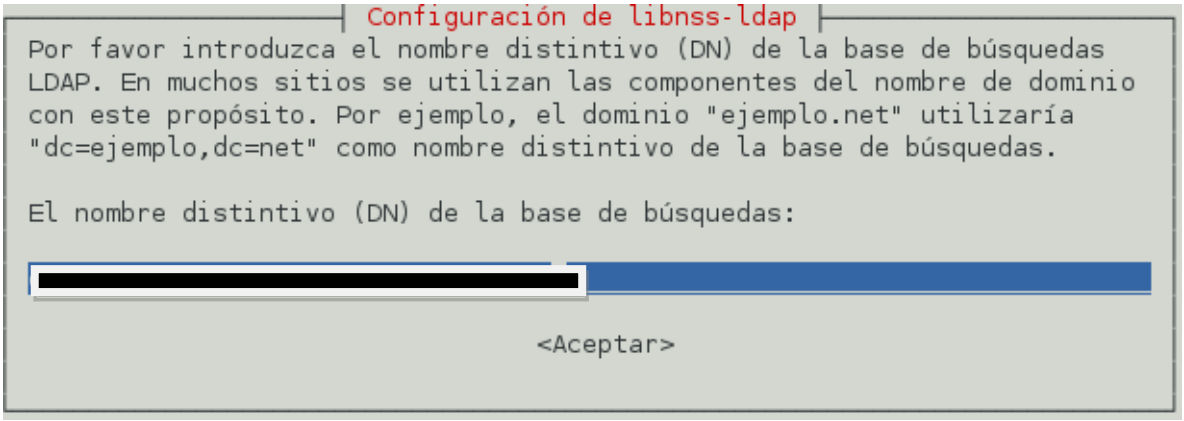
Figura A-17. **Configurar IP del servidor LDAP**



Fuente: elaboración propia. Programa de configuración librería libnss-ldap.

DN que se utiliza en el servidor LDAP.

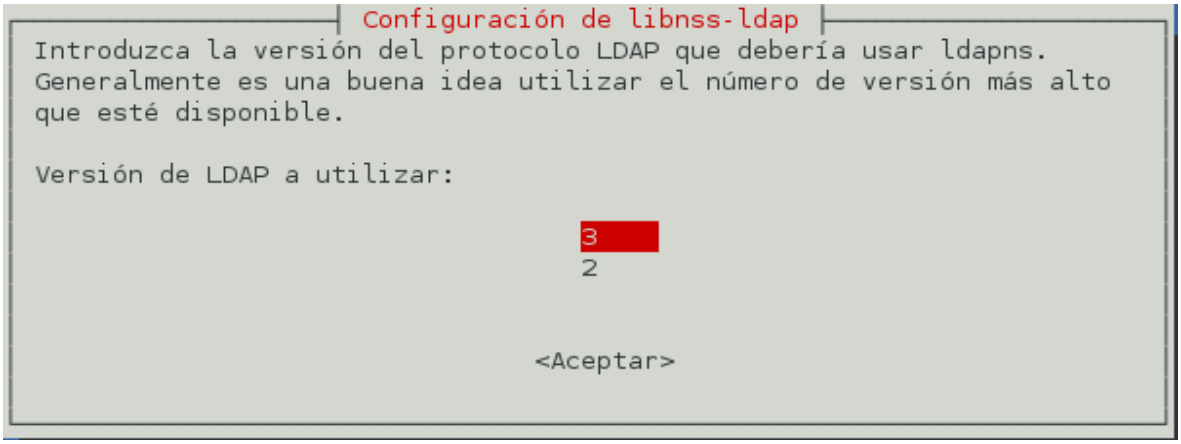
Figura A-18. **Introducir DN de LDAP**



Fuente: elaboración propia. Programa de configuración librería libnss-ldap.

La versión de LDAP que se utiliza.

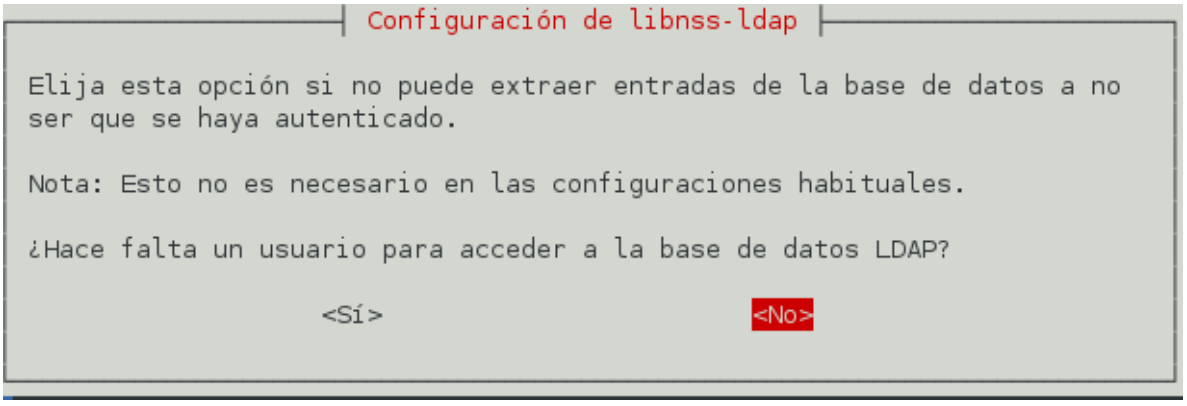
Figura A-19. **Versión de LDAP utilizado**



Fuente: elaboración propia. Programa de configuración librería libnss-ldap.

Luego si es necesario autenticarse en el servidor LDAP o no, en este caso la respuesta es no, dado que solo consultaremos.

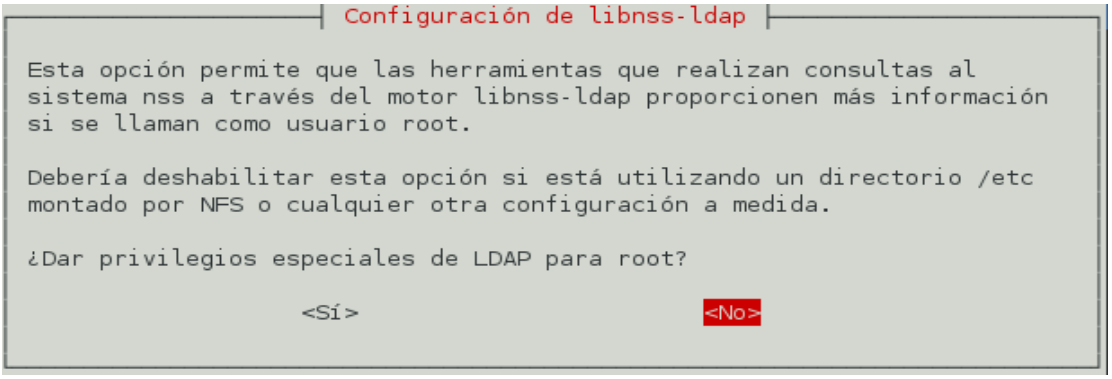
Figura A-20. **Configuración Autenticación por usuario**



Fuente: elaboración propia. Programa de configuración librería libnss-ldap.

Luego se cunsulta si el archivo */etc/libnss-ldap* puede ser configurable solo por el *root* del sistema, se responde que no, dado que en el paso anterior indicamos que no es necesario la autenticación, no se guardaran contraseñas en este archivo.

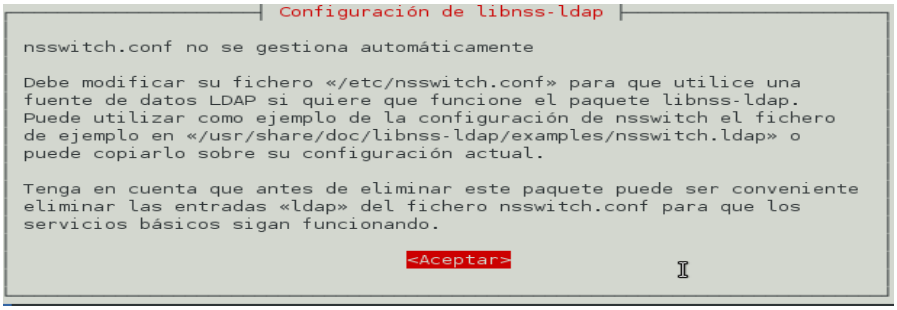
Figura A-21. **Dar privilegios al usuario *Root***



Fuente: elaboración propia. Utilizando programa de configuración librería libnss-ldap.

Advierte de que en la instalación es necesario modificar el archivo */etc/nsswitch.conf* para poder autenticarse por medio de ldap.

A-22. **Advertencia de modificación de nsswitch.conf**

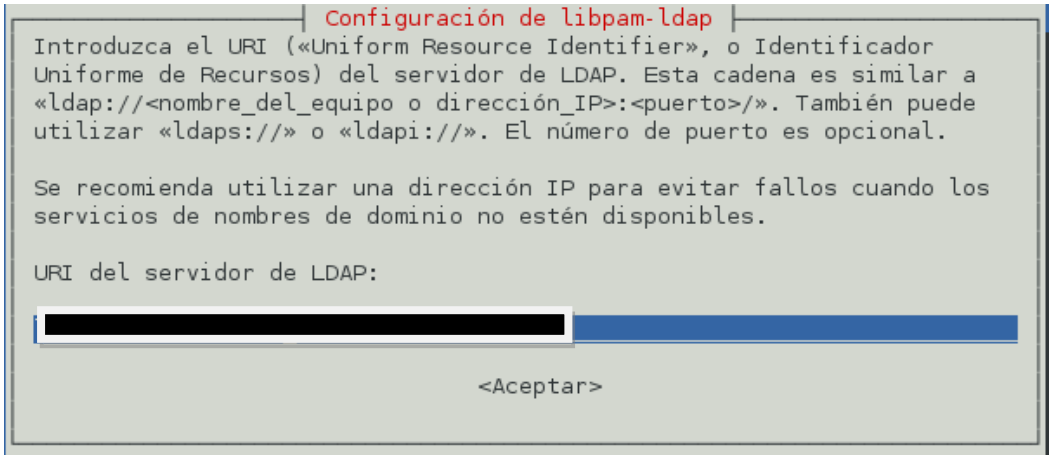


Fuente: elaboración propia. Programa de configuración librería libnss-ldap.

Dpkg-reconfigure libpam-ldap

Luego pregunta el URI del servidor LDAP

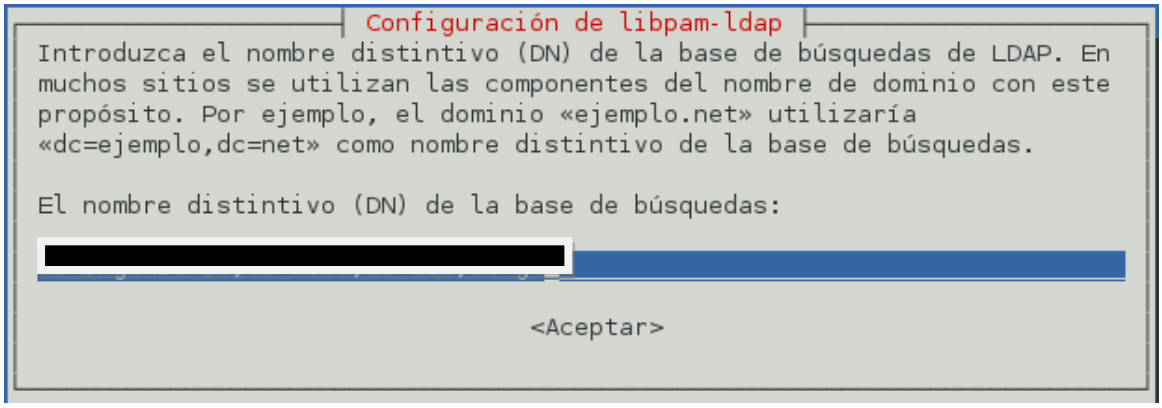
A-23. **URL del Servidor LDAP**



Fuente: elaboración propia. Programa de configuración librería libpam-ldap.

DN del servidor

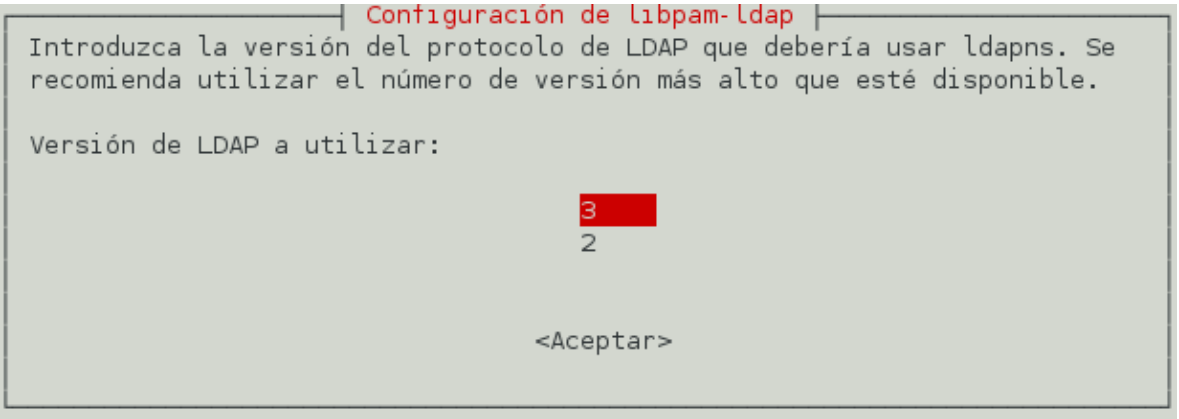
A-24**.** **DN del servidor LDAP**



Fuente: elaboración propia. Programa de configuración librería libpam-ldap.

Versión de LDAP que se está utilizando

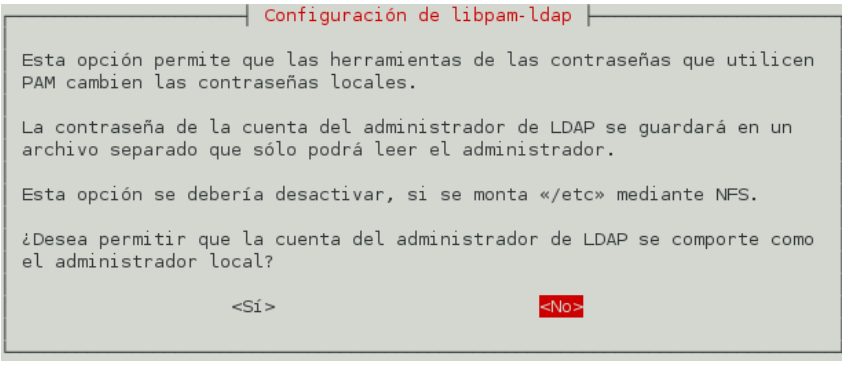
A-25. **Versión de LDAP**



Fuente: elaboración propia. Programa de configuración librería libpam-ldap.

Se pregunta si los usuarios que se conecten a través de ldap se comporten como administrador local, en este caso decimos no, solo queremos que sean invitados.

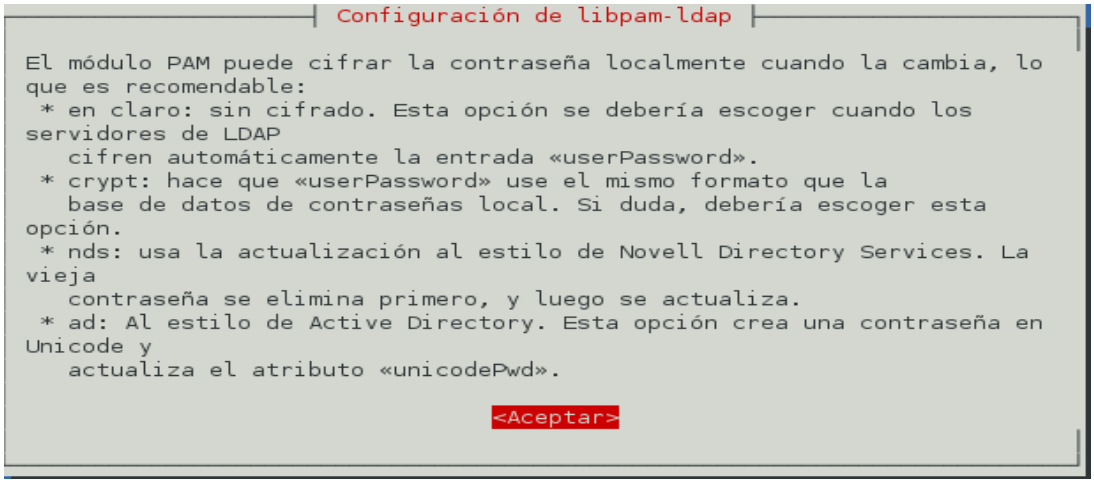
A-26. **Permitir a PAM privilegios**



Fuente: elaboración propia. Programa de configuración librería libpam-ldap.

Nos da una recomendación del cifrado de contraseñas:

A-27. **Recomendación de cifrado de contraseñas**



Fuente: elaboración propia. Utilizando Programa de configuración librería libpam-ldap.

Escogemos lo que nos recomienda:

A-28. **Selección de cifrado de contraseña**

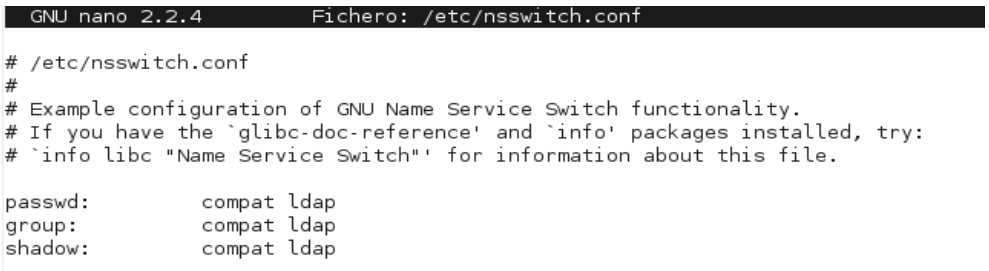
Fuente: elaboración propia. Programa de configuración librería libpam-ldap.

Luego se necesita editar el archivo */etc/nsswitch.conf*, donde debemos modificar lo siguiente dentro del archivo existirá la siguiente parte:

```
Passwd:     files
Group:      files
Shadow:     files
```

El cual debe de quedar de la siguiente manera:

A-29. **Archivo de configuración nsswitch.conf**

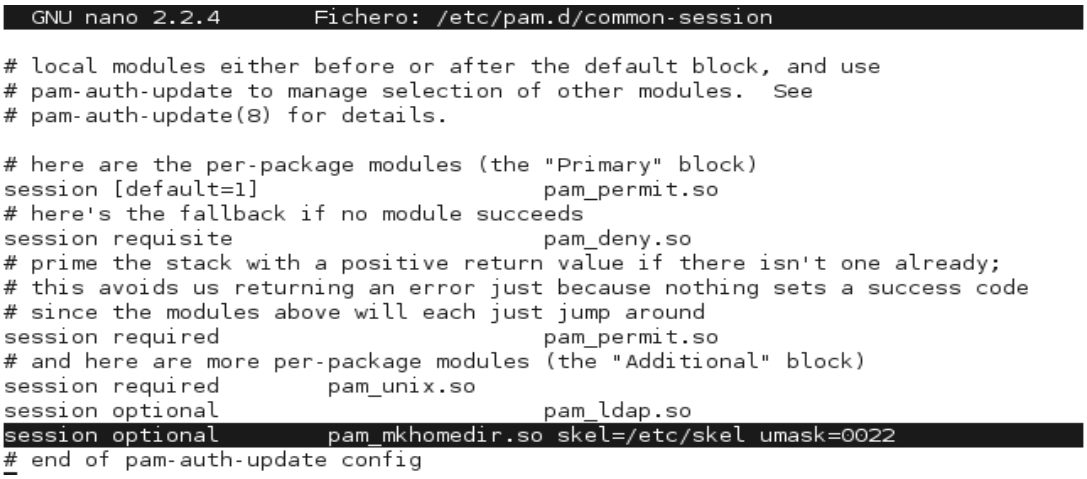


Fuente: elaboración propia. Consola GNU nano 2.2.4.

Esto para indicar que una autenticación es posible por medio de ldap.

Se debe de modificar el archivo /etc/pam.d/common-session y agregar la siguiente línea ession optional pam_mkhomedir.so skel=/etc/skel umask=0022, esto hará que a la hora de autenticar un usuario automáticamente se crea su carpeta /home/usuario y no haya un tipo de problema en la autenticación.

A-30. **Configuración de carpeta Home del usuario**



Fuente: elaboración propia. Consola GNU nano 2.2.4.

Por último se tiene que modificar el archivo en las cuales se debe de colocar esencialmente estas líneas en el archivo para que la autenticación por medio de un servidor LDAP sea exitosa.

/etc/libnss-ldap.conf

base dc=base,dc=ejemplo

uri ldaps://192.168.1.5

ldap_version 3

binddn cn=usuario,dc=base,dc=ejemplo

bindpw CLAVE

scope one

nss_base_passwd ou=user, dc=base,dc=ejemplo

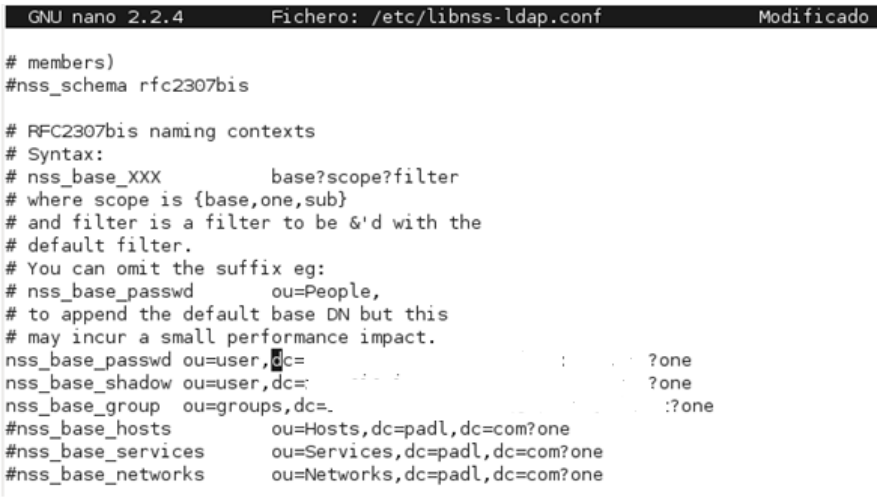
nss_base_shadow ou=user, dc=base,dc=ejemplo

nss_base_group ou=gruop, dc=base,dc=ejemplo

Esta configuración es la base, claramente las opción de base, *uri, ldap_version, binddn* al abrir el archivo estarán con la información que anteriormente se configuro en el asistente, pero lo importante de esto son *nss_base_passwd, nss_base_shadow, nss_base_group* en estas líneas se coloca la dirección de la unidad organizacional de la cual se hará la autenticación en el servidor ldap.

Estas tres líneas son los filtros para decir los usuarios que son capaces de autenticarse al servidor. Únicamente los resultados que devuelvan estos filtros, serán los únicos que pueden autenticarse en el servidor.

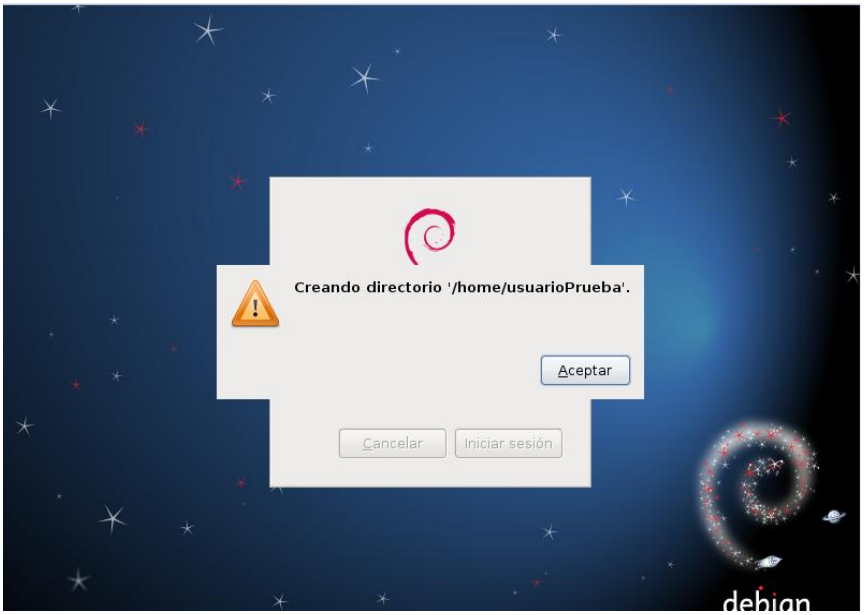
A-31. **Filtro de autenticación de usuarios**



Fuente: elaboración propia. Consola GNU nano 2.2.4.

Aquí cuando un usuario hace *log in* por primera vez, creando su directorio.

A-32 **Primera autenticación de usuario en el sistema**



Fuente: elaboración propia. Sistema Operativo Debian 6.

A.6. Instalación y configuración Pgina

Pgina es un *plugin* GINA y reemplazo de proveedor de credenciales es totalmente *open source*. Permite alternar entre métodos de autenticación y acceso pudiendo manejar a computadoras que corren con sistemas operativos Windows. En resumen permite a tus usuarios *windows* realizar *log in* usando el sistema de autenticación de tu preferencia. El resultado final es que tú el administrador, puede elegir como los usuarios son autenticados autorizados y manejados.

En este caso se usara para autenticar a los usuarios que tiene la misma máquina y a los usuarios que se encuentren en el servidor LDAP.

A.6.1. Requisitos de Instalación.

- Sistema operativo Windows 2000 o superior
- *Framework* .NET 4.0
- Microsoft Visual c++ 2010 *redistributable*
- Instalador PGina 3.0.1.2.1

A.6.2. Instalación

Se instala correctamente los prerrequisitos, en este caso el *framework* .NET y el paquete de *visual c++.* Luego se ejecuta el archivo de instalación de PGINA y se siguen los simples pasos que pide.

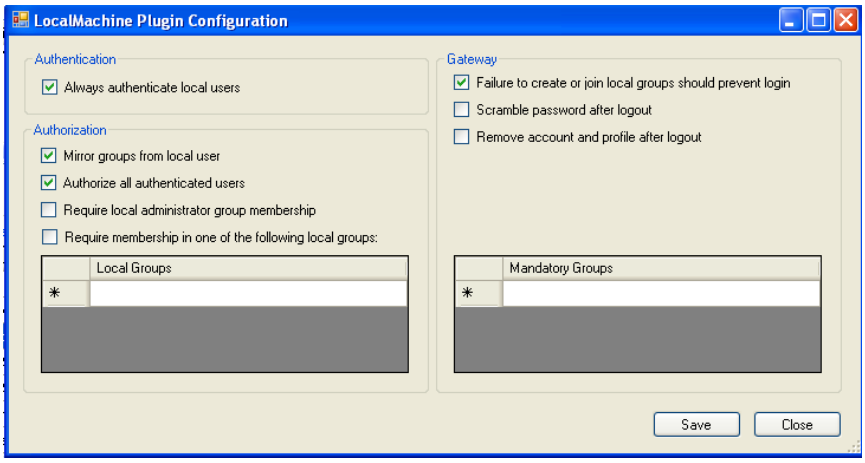
En el momento de la instalación, por defecto toma el *plugin* de “Local machine” que son los usuarios propios de la máquina.

A.6.3. Configuración de PGINA.

A.6.3.1. Usuarios Local machine.

Debe de elegir que los usuarios propios de la maquina sean usuarios administradores, este paso es muy importante porque si no se elige de esta forma la computadora no tendrá usuarios administradores y ya no permitirá la configuración de pGina mas adelante ni de cualquier otra aplicación que necesite privilegios.

A-33. **Filtro de Usuarios**

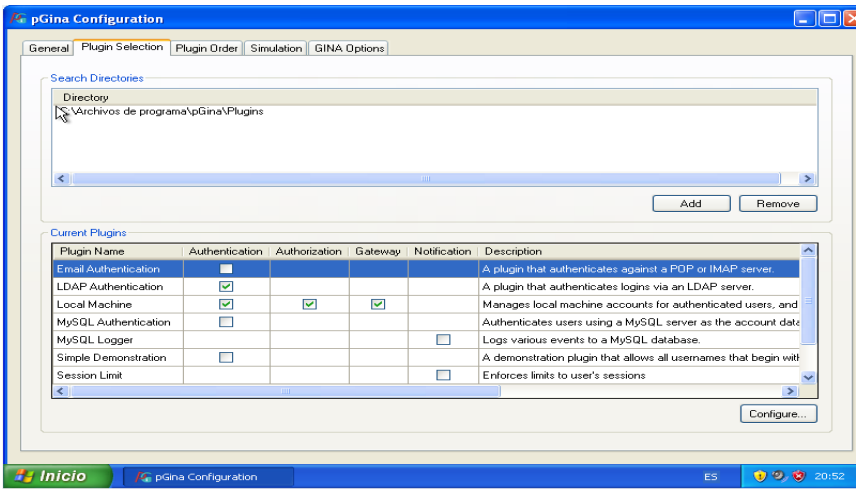


Fuente: elaboración propia. Programa Pgina.

A.6.3.2. Usuarios LDAP

Se activa esta opción entre los *plugins*.

A-34. **Activar opción de LDAP**



Fuente: elaboración propia. Programa Pgina.

Se escribe la dirección ip o el nombre DNS del servidor, donde se encuentra ldap. Los datos de acceso al servidor LDAP. Algo importante en este paso es el filtro o dirección DN donde se encontraran los usuarios a autenticar dentro del árbol jerárquico.

En las búsquedas que se realicen con los *plugins*, una parte importante es la forma en que se representa el usuario y la *password*. El usuario se representa por %u y la contraseña ingresada al momento de autenticar, la compara con la del registro que devuelva la búsqueda, y el usuario ingresado en tiempo de ejecución se reemplaza por el %u.

A.6.4. La opción de hacerlo por filtro

Con esta opción autenticara cualquier usuario que devuelva la consulta del filtro. Ejemplo:

(&(usuario=%u)(ou=usuarios)(ou=usuarios_sistemas))

Autenticara con los valores que devuelva dicho filtro.

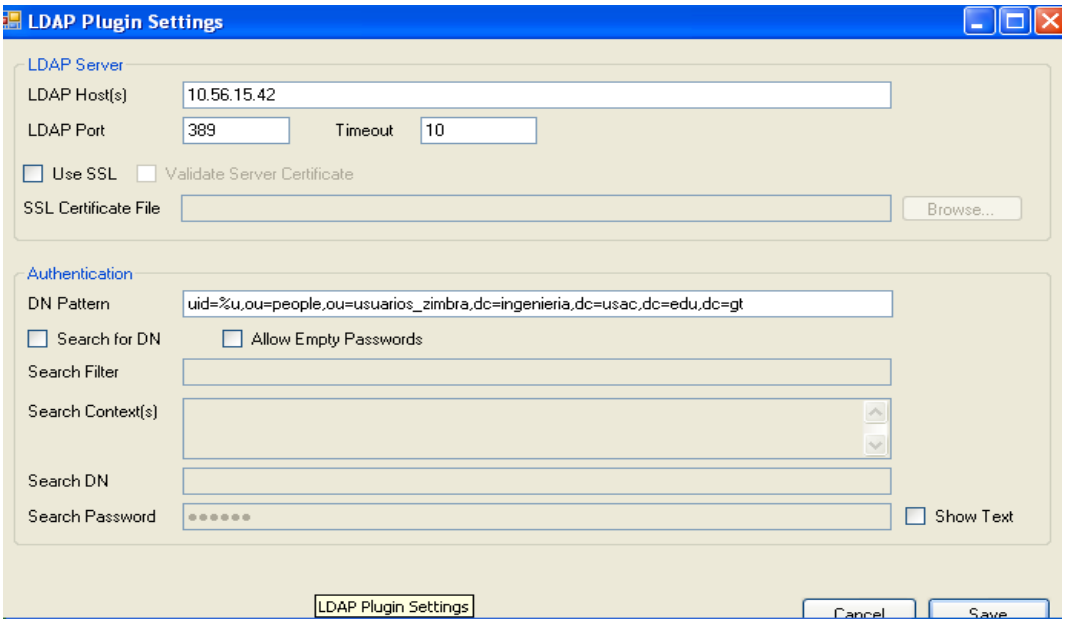
A.6.5. La opción de autenticar por RDN

Con esta función se busca los usuarios que se encuentre directamente en una rama del árbol, y no se puede salir de esa rama. Ejemplo:

Usuario=%u, ou=usuarios,ou=usuarios_sistemas,dc=ingeniería

Esta búsqueda buscara en la rama ou=usuarios y únicamente dentro de ella.

A-35 **Autenticación por RDN**



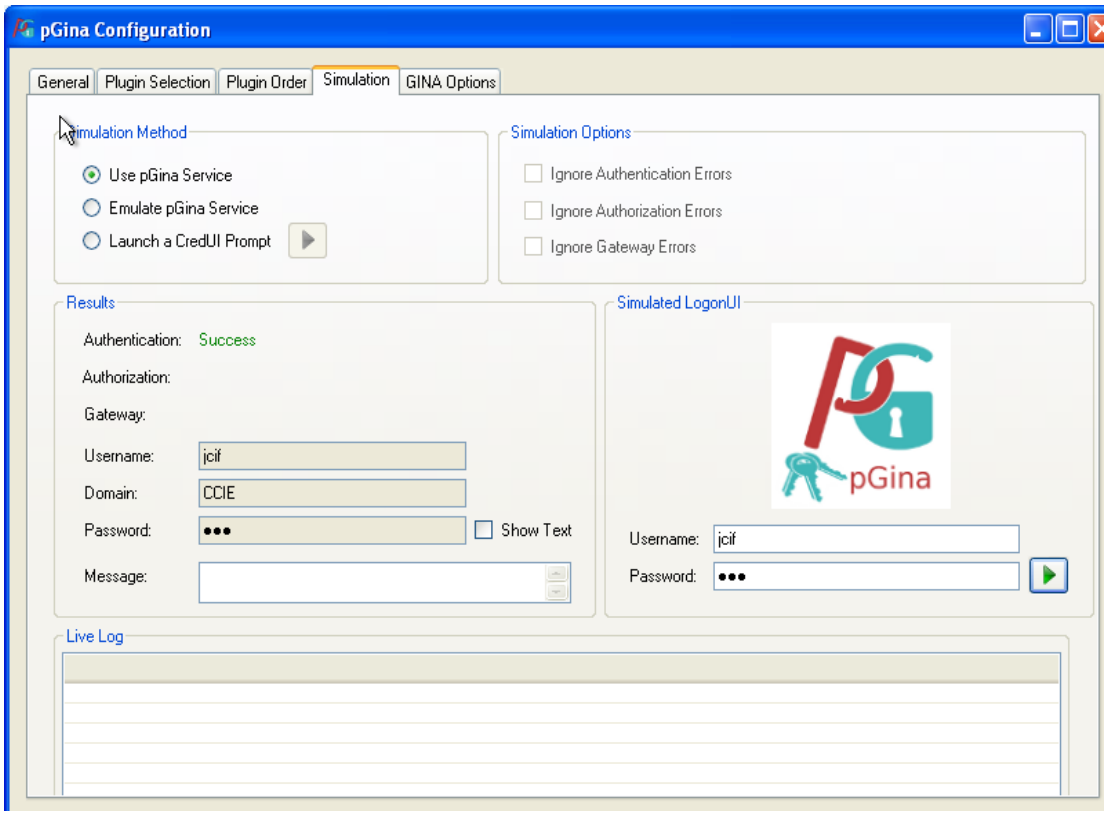
Fuente: elaboración propia. Programa Pgina.

A.6.7. Simulación:

Antes de reiniciar nuestro sistema operativo, vamos a realizar una simulación para comprobar si nuestras configuraciones son correctas.

Se elige la función **"*Use pGina service*",** y luego ingresamos los valores que nos piden en usuario y contraseña luego presionamos en autenticar. Si todo está bien se reinicia.

A-36. **Simulación de autenticación**

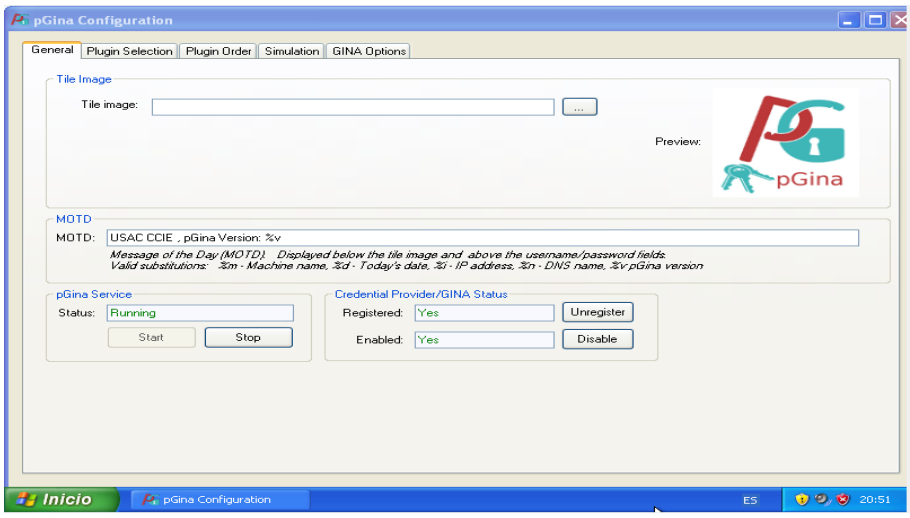


Fuente: elaboración propia. Programa Pgina.

A.6.8. Personalización.

Para personalizar el inicio de sesión de PGINA es completamente fácil, se ingresan los valores reemplazando a los por defecto, incluyendo imagen, botón de reinicio o de apagado, además el texto de bienvenida.Para personalizar la pantalla de *login*.

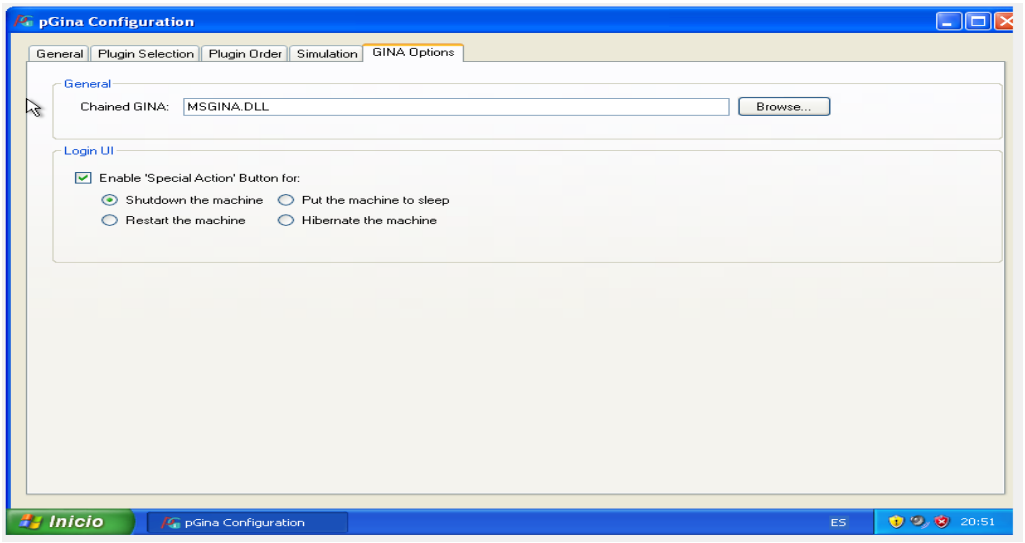
A-37. **Personalización *login***



Fuente: elaboración propia. Programa Pgina.

Para activar los botones en la pantalla l*ogin*.

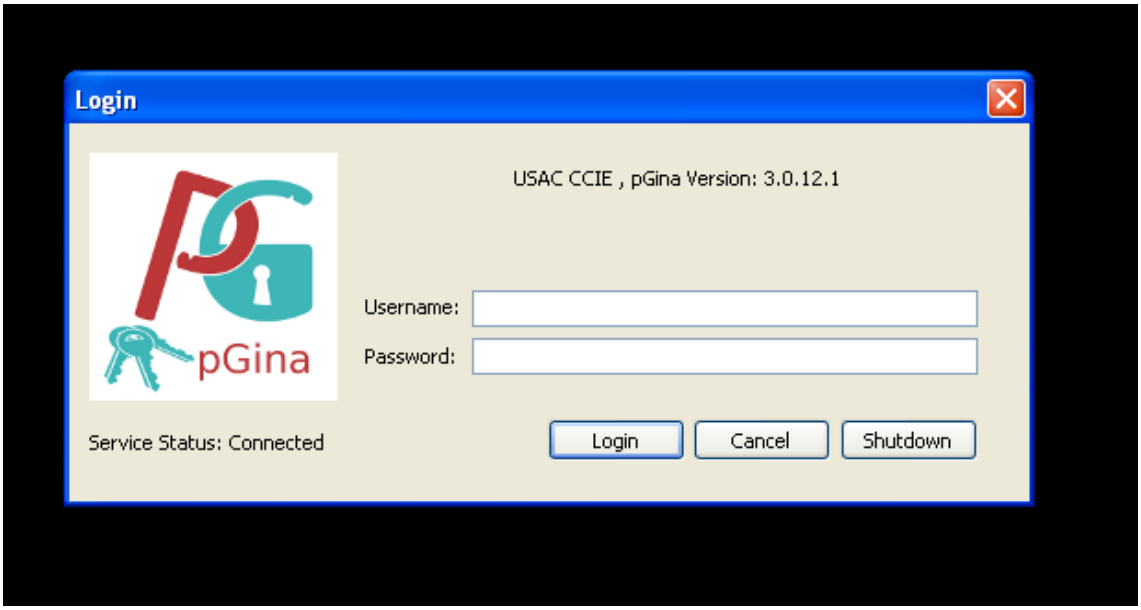
A-38. **Activar botones de *login***



Fuente: elaboración propia. Programa Pgina.

Vista final del login de pGina.

A-39. **Vista final pGina**



Fuente: elaboración propia. Programa Pgina.