

Universidad de Holguín “Oscar Lucero Moya”

Facultad de Informática y Matemática



**SISTEMA PARA LA CENTRALIZACIÓN DE LAS CUENTAS DE  
USUARIOS DE LOS SERVICIOS QUE BRINDA EL NODO  
CENTRAL DE LA UNIVERSIDAD DE HOLGUÍN “OSCAR  
LUCERO MOYA”**

**Trabajo de Diploma para optar por el título de Ingeniero Informático.**

Autor: Yanier Sánchez Ávila

Tutores: MSc. Sergio Cleger Tamayo

Ing. Rafael Torres Zaldívar

Consultante: Ing. Dayami Proenza Pupo

Holguín, 2010.

## **Dedicatoria.**

Dedico este Trabajo de Diploma:

A mis padres que con su ejemplo y dedicación me encaminaron en el largo trayecto a seguir para lograr este sueño.

A mis amigos que me brindaron su apoyo y toleraron mis inquietudes.

A mis hermanos que forman parte día a día.

## **Agradecimientos.**

A todos mis amigos, no los menciono ahora porque no quiero que se me olvide ninguno, muchas gracias.

A mis compañeros de la Universidad, en especial a los de mi grupo, por haber pasado tanto tiempo compartiendo buenos y malos momentos. Aunque quizá no nos reunamos de nuevo, siempre los tendré presentes.

A mis tutores Rafael y Sergio por haberme guiado en el transcurso de esta investigación.

Al colectivo del Nodo Central UHo por haberme apoyado en la realización de este trabajo.

A todo el que de una forma u otra contribuyó con la concepción y elaboración de este trabajo de diploma, muchas gracias.

## Resumen

El presente trabajo se titula: “Sistema para la centralización de las cuentas de usuarios de los servicios que brinda el Nodo Central de la Universidad de Holguín Oscar Lucero Moya”, y se desarrolla debido a la imperiosa necesidad de favorecer la administración más eficiente de los servicios que actualmente se prestan en el mencionado local. De esta manera surge la tarea de implantar un sistema informático que permita solucionar la problemática existente, el cual se encargará de centralizar las cuentas de usuarios.

En el transcurso de esta investigación, se explica el estudio realizado en el campo de la integración de cuentas de usuarios y sobre las tecnologías actuales, con especial atención a las de software libre. Se analizan en general los elementos teóricos que conllevan a la selección y adaptación del sistema propuesto, el cual permite la administración de forma intuitiva y eficiente de los servicios que se brindan.

Durante el proceso investigativo se tiene en cuenta además la valoración de sostenibilidad de la propuesta desde distintas dimensiones, de acuerdo con su influencia en cada una de ellas, así como el cumplimiento de la política trazada por el Estado cubano respecto a las tecnologías de la información y las comunicaciones.

## **Abstract.**

The present work is entitled: "System for the integration of the user accounts of the services provided by the Holguín University Central Node", and it is developed due to the urgent need to promote more efficient management of the services currently provided at the mentioned place. In consequence, the task of implementing a system for solving the existing problematic begins, one which will centralize the user accounts.

In the course of investigation, the study of user accounts' integration and existing technologies is explained, with special attention in free software's field. Generally, the theoretical elements leading to the selection and adaptation of the system proposed are discussed, and this one allows the administration of the services provided in an intuitive and efficient way.

During the research process, the sustainability's evaluation of the proposal from different dimensions is taken into account, according to its influence in each one of them, as well as compliance with the policy laid down by the Cuban government relative to information and communication technologies.

# Índice

<b>Introducción.....</b>	<b>1</b>
<b>1. Fundamentación teórica para el desarrollo de Mecanismos de Centralización de las Cuentas de Usuarios .....</b>	<b>7</b>
1.1 Software Libre.....	8
1.1.1 <i>Libertades del Software Libre .....</i>	<i>9</i>
1.2 Principales Servicios que presta el Nodo de la UHo.....	9
1.2.1 <i>Servicio de Correo Electrónico.....</i>	<i>9</i>
1.2.2 <i>Servicio Proxy Internet.....</i>	<i>11</i>
1.2.3 <i>Mensajería Instantánea .....</i>	<i>12</i>
1.3 Estudio del Arte de las tecnologías de la Información y las Comunicaciones..	14
1.3.1 <i>Integración de Servicios Telemáticos .....</i>	<i>14</i>
1.3.1.1 <i>LDAP, principales características, ventajas y situaciones en las que es conveniente utilizarlo .....</i>	<i>14</i>
1.3.1.2 <i>Comparación entre Software existentes para la creación de servidores LDAP</i>	<i>18</i>
1.3.2 <i>Sistemas Operativos.....</i>	<i>24</i>
1.3.2.1 <i>Distribuciones GNU/Linux .....</i>	<i>24</i>
1.4 Conclusiones del Capítulo .....	27
<b>2. Descripción y Resultados de la Propuesta. ....</b>	<b>28</b>
2.1 OpenLdap ¿Cómo obtenerlo?.....	28
2.1.1 <i>Instalación del sistema.....</i>	<i>29</i>
2.2 Descripción del Sistema.....	29
2.2.1 <i>Componentes y su Configuración .....</i>	<i>30</i>
2.2.1.1 <i>Slapd. ....</i>	<i>31</i>
2.2.2 <i>Autenticación basada en Ldap.....</i>	<i>37</i>
2.2.2.1 <i>Librerías de autenticación pam-ldap y nss-ldap. ....</i>	<i>38</i>
2.2.2.2 <i>Instalación y configuración de libnss-ldap. ....</i>	<i>39</i>
2.2.2.3 <i>Configuración del NSS .....</i>	<i>40</i>

2.2.2.4	<i>Configurar servicios PAM</i> .....	41
2.3	Administración del Servidor Ldap .....	45
2.3.1	<i>Jxplorer</i> .....	45
2.3.2	<i>PhpLDAPAdmin</i> .....	47
2.3.3	<i>Gosa</i> .....	48
2.4	Configuración de los Servicios .....	50
2.4.1	<i>Proxy</i> .....	50
2.4.2	<i>Correo Electrónico</i> .....	56
2.4.2.1	<i>Postfix</i> .....	57
2.4.2.2	<i>Dovecot</i> .....	63
2.4.3	<i>Mensajería Instantánea</i> .....	66
2.4.3.1	<i>Openfire</i> .....	66
2.5	Valoración de sostenibilidad de la propuesta de solución.....	68
2.5.1	<i>Dimensión Administrativa</i> .....	68
2.5.2	<i>Dimensión Socio-Humanista</i> .....	69
2.5.3	<i>Dimensión Ambiental</i> .....	69
2.5.4	<i>Dimensión Tecnológica</i> .....	70
2.5.5	<i>Conclusiones de la valoración de sostenibilidad</i> .....	70
2.6	Valoración de resultados con la implantación de los Mecanismos para la Centralización de Cuentas de Usuarios. ....	70
2.7	Conclusiones del capítulo. ....	71
<b>Conclusiones</b> .....		<b>72</b>
<b>Recomendaciones</b> .....		<b>73</b>
<b>Referencias Bibliográficas</b> .....		<b>74</b>
<b>Anexos</b> .....		<b>76</b>

## **Introducción**

Nadie está ajeno a la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. El comercio, las comunicaciones, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

El desarrollo de la computación y su integración con las telecomunicaciones en la telemática han propiciado el surgimiento de nuevas formas de comunicación, que son aceptadas cada vez por más personas. El desarrollo de las redes informáticas posibilitó su conexión mutua y, finalmente, la existencia de Internet, una red de redes gracias a la cual una computadora puede intercambiar fácilmente información con otras situadas en regiones lejanas del planeta.

El uso creciente de la tecnología de la información en la actividad diaria ha dado lugar a un incremento sustancial en el número de puestos de trabajo informatizados, con una relación de terminales por empleado que aumenta constantemente en todos los sectores industriales[24].

Para responder a ésta problemática han sido creadas las Redes de Área Local (LAN), el crecimiento de éstas a mediados de los años ochenta hizo que cambiase la forma de comunicarse con los ordenadores y la forma en que los ordenadores se comunicaban entre sí. Las redes LAN se han convertido en el entorno natural donde muchas pequeñas y medianas empresas basan o desarrollan su trabajo, con el fin de intercambiar y compartir información entre los distintos usuarios, y con ello aumentar la productividad del negocio, o en el caso de las instituciones académicas, la labor docente-educativa y la investigación científica. En un breve espacio de tiempo, se ha ido pasando de tener un reducido número de equipos independientes entre sí, a configurar redes LAN de cierta complejidad.

El elevado crecimiento de las redes de datos desde la segunda mitad del siglo pasado tiene como consecuencia negativa la aparición de problemas de congestión y de



dificultades para lidiar con la elevada demanda que se produce en los servicios de red, de esta manera surgen grandes centros que facilitan los mismos, llamados Nodos de Red. Los administradores de estos nodos tienen ante sí diferentes retos, sobre todo los que se asocian con la seguridad y estabilidad de los servicios brindados.[20]

El Nodo Central de la Universidad de Holguín “Oscar Lucero Moya” (UHo) tiene entre sus particularidades la tarea de prestar a los usuarios del centro los principales servicios de red, de ahí que sus principales objetivos sean[11]:

- Garantizar el intercambio ininterrumpido de información científico-técnica actualizada entre profesionales y estudiantes pertenecientes al sistema de Educación Superior.
- Elevar la calidad en la educación de pregrado y postgrado, así como en la investigación mediante el acceso a un sustancialmente mayor volumen de información científica y técnica, el intercambio operativo de información entre profesores, investigadores y estudiantes de distintos Centros de Educación Superior del país y con especialistas en el extranjero.
- Potenciar la colaboración entre instituciones académicas nacionales y extranjeras, facilitando el intercambio principalmente con universidades latinoamericanas.
- Permitir el acceso a bancos de datos y otros medios y(o) formas de organización y almacenamiento de la información (que posea el grado de actualización requerido), que resulte vital para los profesionales y estudiantes vinculados a la educación superior.
- Estimular la producción de información electrónica entre el claustro y colectivos estudiantiles, así como facilitar su publicación.
- Potenciar el desarrollo de la programación abierta y la solución de problemas.
- Mejorar la eficiencia en la explotación del equipamiento, así como extender y facilitar la utilización de nuevos servicios, herramientas y aplicaciones.

- Asumir con fuerza y rapidez el desarrollo de la educación a distancia como vía de superación, lo mismo en la formación de profesionales, como en la actividad de postgrado.

En la Universidad de Holguín (UHo), centro educacional donde se desarrolla esta investigación, existe una LAN privada, mediante la cual se comunican entre sí más de 800 ordenadores, divididos entre siete facultades y los distintos departamentos, oficinas, etc., posibilitando el intercambio rápido y necesario de la información que se requiere para la realización de muchas labores diarias.

De ello se deriva que deba realizarse un conjunto de acciones, tales como diseño, planificación, configuración, puesta a punto, mantenimiento y seguimiento (control) de los servicios de la red. Para esto se requiere de un conjunto de administradores de red calificados y otros en proceso de entrenamiento; los que cuenta, además, con un equipamiento específico para este tipo de actividades: servidores profesionales, estaciones de trabajo, equipos y medios de transmisión.

Entre los principales servicios dentro de la actividad informática en la UHo se encuentran los servicios de la Red de Datos, Correo Electrónico e Internet, mensajería instantánea dirigidos fundamentalmente por el grupo técnico del Nodo Central, perteneciente al Grupo de Informatización de la entidad.

En el Nodo Central de la UHo actualmente se encuentran implementadas herramientas que ayudan al proceso de administración de las cuentas de usuario de los servicios antes mencionados, llevando a cabo este proceso de forma individual para cada uno de éstos, creando una Base de datos de usuario para cada servicio con sus especificidades trayendo como consecuencia que los usuarios tengan varias cuentas con diferentes tipos de informaciones como contraseña, nombre de usuario, lo que trae consigo que se genere un gran volumen de información de usuarios por lo que se torna difícil a la hora de actualizar los datos de los clientes por estar todos los servicios montados con una base de datos individual,

A esta situación se le añade el aumento de los usuarios de la red, así como los equipos conectados a esta y por ende de la información y datos en las aplicaciones que están

configuradas en el Nodo Central, donde se maneja una gran cantidad de información, las cuales la gran mayoría son de acceso limitado.

Es de destacar que todos los servicios y tecnologías presentes en el Nodo Central de la Universidad de Holguín “Oscar Lucero Moya” están de una forma u otra afectados por la problemática anterior. El análisis de esta, en momentos críticos, da el punto de partida para la toma de decisiones y la solución de diferentes contratiempos que se presentan en el trabajo diario.

Tras un estudio de la situación se identificó el siguiente **Problema**:

¿Cómo integrar las cuentas de usuarios de los servicios que brinda el Nodo Central de la UHo?

Así se identifica como **Objeto de Estudio** de la investigación: La gestión de la información de las cuentas de usuarios de los servicios telemáticos que brinda el Nodo Central de la UHo.

Atendiendo a estos antecedentes se propone como **Objetivo**: Configurar e implantar un sistema para la integración de los servicios telemáticos que brinda el Nodo Central de la UHo.

El Objetivo deja delimitado el **Campo de acción**: El proceso de integración de las cuentas de usuarios de los servicios telemáticos que brinda el Nodo Central de la Uho.

La investigación ha seguido su curso guiada por la **hipótesis**:

El diseño e implantación de un sistema que sea fácil de utilizar, que posea una interfaz intuitiva, un tiempo rápido de respuesta, que centralice la información de las cuentas de usuarios, favorecerá la integración, control y funcionamiento de los servicios telemáticos que brinda el Nodo Central de la Uho.

Con el propósito de desarrollar la investigación con la mayor calidad posible, la investigación se está llevando a cabo a través de las siguientes **tareas**:

1. Establecer los referentes teóricos y metodológicos de la integración de servicios telemáticos.
2. Realizar la valoración de sostenibilidad del sistema según su impacto social,

económico, ambiental, administrativo y tecnológico.

3. Configurar un sistema de integración de servicios telemáticos.
4. Implantación del sistema de integración de servicios telemáticos.
5. Valorar el grado de aceptación del sistema de integración de servicios telemáticos.

Para el cumplimiento de éstas tareas se emplearon **métodos de investigación científica** teóricos y empíricos dentro de los cuales se encuentran:

De nivel teórico:

- ❖ Análisis y síntesis: permitió descomponer el proceso investigativo del sistema informático y a la vez sintetizar la información analizada para llegar a conclusiones parciales o generales.
- ❖ Hipotético-deductivo: debido a que la investigación se basa en una hipótesis, que se deriva del conocimiento de leyes y principios más generales, y la misma será verificada como cierta o falsa en el transcurso de la investigación.

De nivel empírico:

- ❖ Entrevista: principal vía de identificación y revisión de los requerimientos del sistema, así como la opinión de los usuarios que van a utilizar el mismo.
- ❖ Revisión de documentos: muy importante para revisar elementos teóricos acerca del problema en toda su extensión, y analizar la bibliografía necesaria para la fundamentación e implantación del sistema propuesto.
- ❖ Encuesta: su uso permitió la valoración del sistema mediante criterio de expertos y contribuyó a encontrar mejoras que se pueden aplicar próximamente.

La presente Tesis esta estructurada en 2 capítulos de acuerdo a los siguientes contenidos:

### **Capítulo 1, Fundamentación teórica del tema desarrollado:**

Aborda la fundamentación del tema que se trata, donde se expone claramente la situación actual de los servicios que se brindan en el Nodo Central Red UHo.

Igualmente, con vista a escoger la mejor solución se ha realizado un estudio de las últimas tendencias en el campo de la Integración de los Servicios los que se han resumido en este capítulo y donde se exponen las características de las herramientas, además de proponer una solución eficaz atendiendo al problema científico.

## **Capítulo 2, Descripción, Implantación y resultados de la propuesta**

En este capítulo se describe todo el proceso que se lleva a cabo para la puesta en marcha del Sistema Propuesto, así como se evalúan los resultados obtenidos una vez implantados. Además se recoge en este capítulo el estudio de la factibilidad y de sostenibilidad de los Mecanismos de Seguridad.

# Capítulo

# 1

## **1. Fundamentación teórica para el desarrollo de Mecanismos de Centralización de las Cuentas de Usuarios**

Se presenta a continuación la descripción del Nodo RED UHo, los diferentes servicios que se brindan, fundamentando el objeto de estudio y el campo de acción donde se realiza la investigación. Para la realización de la propuesta de solución se hace necesario detallar conceptos relacionados con la fundamentación del tema e investigar las últimas tendencias en el campo de los Mecanismos de Seguridad de red, haciendo énfasis en los de Código Abierto.

En la actualidad, el continuo desarrollo de la ciencia y la tecnología, y particularmente de la Informática, ha provocado que el volumen de información (datos, programas, etc.) haya aumentado considerablemente. Los ordenadores, ya sean de escritorio, personales o servidores, constituyen una poderosa herramienta que se encuentra presente en casi todos los sectores de la vida- de todo país. A nivel mundial son usados en cualquier clase de trabajo que implique manipulación de grandes volúmenes de información, o realización de cálculos complejos para cualquier proyecto científico o

investigativo. En Cuba la sociedad se encuentra inmersa en un proceso de informatización que se ramifica hacia varias direcciones. Entre ellas se encuentra la migración hacia el software libre.

## 1.1 Software Libre

El software libre es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente. Según la Fundación del Software Libre, el software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software; de modo más preciso, se refiere a cuatro libertades de los usuarios del software: la libertad de usar el programa, con cualquier propósito; de estudiar el funcionamiento del programa, y adaptarlo a las necesidades; de distribuir copias, con lo cual se puede ayudar a otros y de mejorar el programa y hacer públicas las mejoras, de modo que toda la comunidad se beneficie.

El software libre suele estar disponible gratuitamente, o al precio de costo de la distribución a través de otros medios; sin embargo no es obligatorio que sea así, por lo tanto no hay que asociar software libre a "software gratuito" (denominado usualmente freeware), ya que, conservando su carácter de libre, puede ser distribuido comercialmente ("software comercial"). Análogamente, el "software gratis" o "gratuito" incluye en ocasiones el código fuente; no obstante, este tipo de software no es libre en el mismo sentido que el software libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.

Tampoco debe confundirse software libre con "software de dominio público". Éste último es aquel software que no requiere de licencia, pues sus derechos de explotación son para toda la humanidad, porque pertenece a todos por igual. Cualquiera puede hacer uso de él, siempre con fines legales y consignando su autoría original. Este software sería aquel cuyo autor lo dona a la humanidad o cuyos derechos de autor han expirado, tras un plazo contado desde la muerte de este, habitualmente 70 años. Si un autor condiciona su uso bajo una licencia, por muy débil que sea, ya no es del dominio público.

### **1.1.1 Libertades del Software Libre**

De acuerdo con tal definición, el software es "libre" si garantiza las siguientes libertades:

1. libertad 0, ejecutar el programa con cualquier propósito (privado, educativo, público, comercial, etc.)
2. libertad 1, estudiar y modificar el programa (para lo cuál es necesario poder acceder al código fuente)
3. libertad 2, copiar el programa de manera que se pueda ayudar al vecino o a cualquiera.
4. libertad 3, mejorar el programa, y hacer públicas las mejoras, de forma que se beneficie toda la comunidad.

Es importante señalar que las "libertades 1 y 3" obligan a que se tenga acceso al código fuente. La "libertad 2" hace referencia a la libertad de modificar y redistribuir el software libremente licenciado bajo algún tipo de licencia de software libre que beneficie a la comunidad. [8]

## **1.2 Principales Servicios que presta el Nodo de la UHo**

El Nodo Central de la RED UHo es el encargado de las comunicaciones de la Universidad de Holguín, y prestar todos los servicios de red a los usuarios. Entre los numerosos servicios que ofrece se encuentran los relacionados con el correo electrónico, Internet, acceso remoto, transferencia de ficheros, resolución de nombres de dominio, publicación de páginas Web, entre otros.

Además es el centro de la topología existente en la RED UHo. Consta de los principales routers, switches, módems y servidores necesarios para establecer la comunicación de la Universidad de Holguín con el resto del mundo[28].

### **1.2.1 Servicio de Correo Electrónico**

Uno de los usos más comunes de las redes informáticas desde sus orígenes ha sido el correo electrónico. El servicio de correo electrónico consta de dos partes bien diferenciadas: aquella con la que trata el usuario, y la que se encarga de transportar los



mensajes del origen al destino. A menudo hay un componente adicional encargado de distribuir el correo que llega a la máquina destino a una ubicación especial dentro de ésta, propia de cada usuario[22]. Los nombres de estos componentes son:

- ❖ Cliente de Correo (MUA – *Mail User Agent*).
- ❖ Agente Transporte Correo (MTA. *Mail Transport Agent*)
- ❖ Utilidades.

Dentro de la arquitectura del soporte informático para la gestión de correo electrónico de la Universidad, se dispone de un sistema que gestiona todo el tráfico entrante y saliente. Este sistema es lo que se denomina una estafeta de primer nivel. En un segundo nivel, se encuentran 8 subnodos que han sido considerados necesarios para las mejores prestaciones del servicio en la universidad, a través de los cuales los usuarios acceden al servicio de correo electrónico[16].

Con este planteamiento, la estafeta de primer nivel se encarga de recibir y encaminar el tráfico de correo electrónico hacia el exterior de la Universidad o hacia las estafetas de segundo nivel, que no son más que los servidores locales de cada facultad, que son quienes realmente proporcionan el servicio a los usuarios.

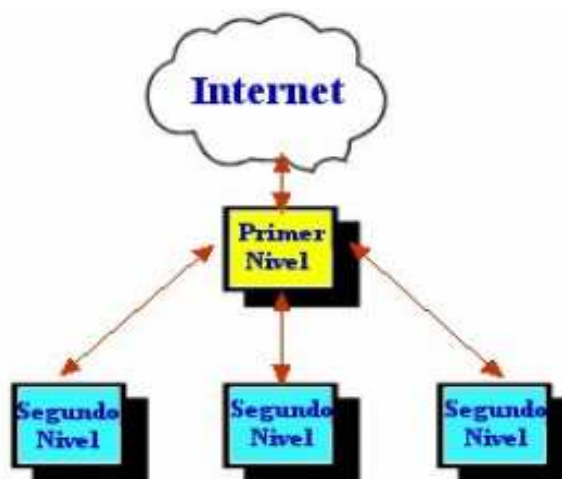
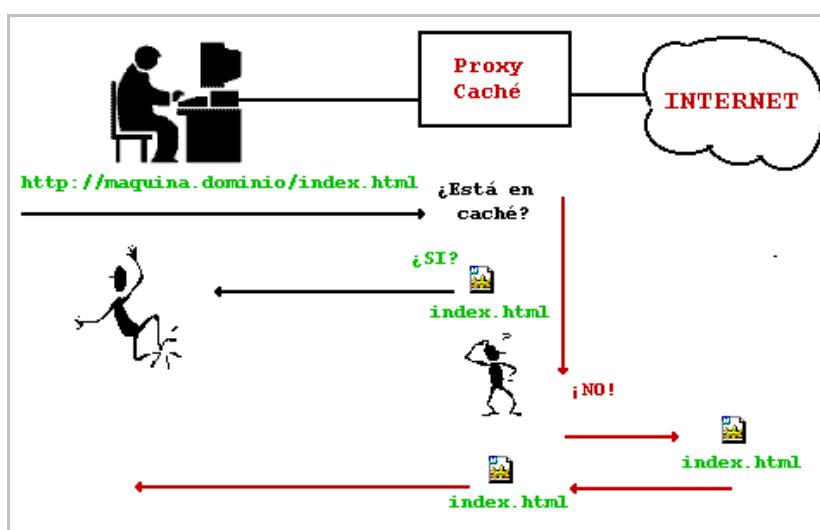


Figura 1 Relación entre las estafetas en el servicio de correo

### 1.2.2 Servicio Proxy Internet

El Servicio Proxy permite a los usuarios de una organización el acceso a Internet, actuando como intermediario entre el programa Cliente y el Servidor de Información al que se desea acceder, incrementando así de forma local, las páginas mas consultadas por los usuarios, de forma que ante otra petición por parte de algún otro usuario, el Proxy puede servirlo evitando las conexiones directas con los accesos remotos a Internet.

Los usuarios configuran su navegador Web para acceder al servicio Proxy en vez de ir directamente a Internet. El servicio Proxy se encarga de proporcionarles la pagina pedida obteniéndola de la caché o accediendo a la pagina original en Internet; al brindar este servicio a muchos usuarios la caché contendrá muchos documentos beneficiándose toda la organización de ello.



**Figura 2 Funcionamiento del Servicio Proxy Internet.**

Para evitar que todos los usuarios puedan acceder a Internet a través del servidor Proxy en vez de los previamente autorizados se implementa un proceso de autenticación en el servidor Proxy donde se procede a la creación de una serie de cuentas y horarios en los que van a acceder estos usuarios para la utilización de este servicio.

Actualmente este servicio se encuentra implementado en la Universidad en el servidor Proxy y brinda el servicio de acceso a Internet a los usuarios autorizados entre los

cuales se encuentran profesores, investigadores, estudiantes y demás funcionarios de la Universidad. Todos los usuarios autorizados poseen una cuenta que les permite autenticarse en el servidor y de esta forma acceder a Internet según horarios establecidos.

El servidor proxy es el encargado de gestionar las peticiones de los usuarios en la red de redes y en parte de los sitios nacionales que no pertenecen a la red del MES. Este servicio está funcionando gracias a Squid (versión 2.7.stable3), el cual es un programa de software libre que implementa esta clase de acceso.

Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix. Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Aunque orientado principalmente a HTTP y FTP es compatible con otros protocolos como Internet Gopher. Implementa varias modalidades de cifrado como TLS, SSL, y HTTPS.[23]

### **1.2.3 Mensajería Instantánea**

La mensajería instantánea requiere el uso de un cliente de mensajería instantánea que realiza el servicio y se diferencia del correo electrónico en que las conversaciones se realizan en tiempo real. La mayoría de los servicios ofrecen el "aviso de presencia", indicando cuando el cliente de una persona en la lista de contactos se conecta o en que estado se encuentra, si está disponible para tener una conversación. En los primeros programas de mensajería instantánea, cada letra era enviada según se escribía y así, las correcciones de las erratas también se veían en tiempo real. Esto daba a las conversaciones más la sensación de una conversación telefónica que un intercambio de texto. En los programas actuales, habitualmente, se envía cada frase de texto al terminarse de escribir. Además, en algunos, también se permite dejar mensajes aunque la otra parte no esté conectada al estilo de un contestador automático. Otra función que tienen muchos servicios es el envío de ficheros.

La mayoría usan redes propietarias de los diferentes softwares que ofrecen este servicio. Adicionalmente, hay programas de mensajería instantánea que utilizan el protocolo abierto Jabber, con un conjunto descentralizado de servidores.[9]

Las aplicaciones de mensajería instantánea permiten gestionar una lista de personas con las que uno desea mantenerse en contacto intercambiando mensajes. Convierte la comunicación asíncrona proporcionada por el correo electrónico en una comunicación síncrona en la que los participantes pueden comunicarse en tiempo real.

- ❖ Además de la conversación básica permite otras prestaciones como:
- ❖ Salas de conversación.
- ❖ Transferencia de ficheros.
- ❖ Actualizaciones de estado (por ejemplo: ocupado, al teléfono, ausente).
- ❖ Pizarra compartida que permite ver y mostrar dibujos a los contactos.
- ❖ Conexión simultánea desde distintos dispositivos con prioridades (por ejemplo: desde el móvil y el ordenador dando preferencia a uno de ellos para la recepción de mensajes).

En la actualidad existen multitud de protocolos de mensajería instantánea como ICQ, AIM, MSN o Yahoo! Messenger cuyo funcionamiento es básicamente centralizado y propietario.

Sin embargo, también existe Jabber/XMPP que es un conjunto de protocolos y tecnologías que permiten el desarrollo de sistemas de mensajería distribuidos. Estos protocolos son públicos, abiertos, flexibles, extensibles, distribuidos y seguros.[5]

En el Nodo Central de la Uho se encuentra configurado un servidor Openfire para gestionar las cuentas de mensajería instantánea de los profesores, directivos y estudiantes de la Universidad.

### **1.3 Estudio del Arte de las tecnologías de la Información y las Comunicaciones.**

Para la realización de la propuesta de solución se hace necesario investigar las últimas tendencias en los servicios de administración de una red y en el desarrollo de Sistemas de Centralización de cuentas de usuario, resultados que se muestran en los siguientes epígrafes.

#### **1.3.1 Integración de Servicios Telemáticos**

La integración de servicios es la pieza angular que debe afrontar un administrador de sistemas. Cuando en una organización deben convivir diferentes sistemas operativos, el administrador debe facilitar a los usuarios la forma de acceder a los recursos independientemente de la plataforma que estos decidan utilizar.

Unas credenciales únicas facilitarán al usuario el acceso a la red e implicará una mayor seguridad y control del funcionamiento de la misma. Esto conlleva la creación de un repositorio único donde se almacena la información de cada elemento de la red. Máquinas, usuarios y servicios podrán ser fácilmente creados, modificados y eliminados si disponemos de un único punto de administración. En los últimos años con el auge de la centralización de servicios se desarrollo un nuevo protocolo Ldap que combinado con otros software logra de forma mas eficiente y rápida la implementación de dominios y administración de los servicios.[13]

##### **1.3.1.1 LDAP, principales características, ventajas y situaciones en las que es conveniente utilizarlo**

###### **¿Qué es LDAP?**

El Protocolo de Acceso Ligero a Directorio, mejor conocido como **LDAP** (por sus siglas en inglés, Lightweight Directory Access Protocol), está basado en el estándar X.500, pero significativamente más simple y más realmente adaptado para satisfacer las necesidades del usuario. A diferencia de X.500 **LDAP** soporta TCP/IP (Transport Control Protocol and Internet Protocol), que es necesario para el acceso a Internet.

###### **¿Qué es un directorio?**

Un directorio es como una base de datos, pero en general contiene información más descriptiva y más basada en atributos. La información contenida en un directorio normalmente se lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos. Las actualizaciones en un directorio son usualmente cambios sencillos de todo o nada, si es que permiten algo. Los directorios están para proporcionar una respuesta rápida a operaciones de búsqueda o consulta. Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta. Cuando se duplica la información de un directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización. Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados. Algunos servicios de directorios son locales, proporcionando servicios a un contexto restringido. Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

### **¿Un directorio LDAP es una base de datos?**

El sistema gestor de una base de datos (Database Management System ó DBMS) de Sybase, Oracle, Informix ó Microsoft es usado para procesar peticiones (queries) ó actualizaciones a una base de datos relacional. Estas bases de datos pueden recibir cientos o miles de órdenes de inserción, modificación o borrado por segundo. Un servidor LDAP es usado para procesar peticiones (queries) a un directorio LDAP. Pero LDAP procesa las órdenes de borrado y actualización de un modo muy lento. En otras palabras, LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente. Funcionamiento de 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 de 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 donde puede el cliente hallar más información. No importa con que servidor LDAP se conecte el cliente ya que 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.

### **Ventajas en el uso de LDAP**

Un directorio LDAP destaca sobre los demás tipos de bases de datos por las siguientes características:

1. Es muy rápido en la lectura de registros
2. Permite replicar el servidor de forma muy sencilla y económica
3. Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente
4. Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas
5. Usa un sistema jerárquico de almacenamiento de información.
6. Permite múltiples directorios independientes
7. Funciona sobre TCP/IP y SSL
8. La mayoría de aplicaciones disponen de soporte para LDAP
9. La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

Dadas las características de LDAP sus usos más comunes son:

1. Directorios de información. Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) ó cualquier tipo de páginas amarillas.
2. Sistemas de autenticación/autorización centralizada.

Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos.

- ❖ Active Directory Server de Microsoft, para gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.
  - ❖ Sistemas de autenticación para páginas Web, algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.
  - ❖ Sistemas de control de entradas a edificios, oficinas.
3. Sistemas de correo electrónico. Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
  4. Sistemas de alojamiento de páginas web y FTP, con el repositorio de datos de usuario compartido.
  5. Grandes sistemas de autenticación basados en RADIUS, para el control de accesos de los usuarios a una red de conexión o ISP.
  6. Servidores de certificados públicos y llaves de seguridad
  7. Autenticación única ó “single sign-on” para la personalización de aplicaciones.
  8. Perfiles de usuarios centralizados, para permitir itinerancia ó “Roaming”.
  9. Libretas de direcciones compartidas.

### **¿Cuándo resulta interesante usar LDAP?**

Como se ha visto LDAP es una base de datos optimizada para entornos donde se realizan muchas lecturas de datos y pocas modificaciones o borrados. Por lo tanto es muy importante saber elegir dónde es conveniente usarlo. No será conveniente como base de datos para sitios que realicen constantes modificaciones de datos (por ejemplo en entornos de e-commerce) Normalmente el tipo de preguntas que se deben hacer para saber si LDAP es conveniente para las aplicaciones son:

1. ¿Gustaría que los datos fueran disponibles desde distintos tipos de plataforma?



2. ¿Se acceso a estos datos desde un número muy elevado de servidores y/o aplicaciones?
3. Los datos que se almacenan ¿son actualizados muchas veces?, o por el contrario ¿son sólo actualizados unas pocas veces?
4. ¿Tiene sentido almacenar este tipo de datos en una base de datos relacional? Si no tiene sentido, ¿Se pueden almacenar todos los datos necesarios en un solo registro?[26]

### **1.3.1.2 Comparación entre Software existentes para la creación de servidores LDAP**

#### **OpenDS**

Es un software es libre, escrito en Java que se desarrolló como parte del proyecto OpenDS. OpenDS software implementa una amplia gama de Lightweight Directory Access Protocol (LDAP, por sus siglas en ingles) y normas conexas, incluido el pleno cumplimiento de LDAPv3, sino también de apoyo para servicios de directorio (Lenguaje de marcado DSMLv2). También ofrece varios maestros de replicación, control de acceso, y muchas extensiones.

OpenDS software es liberado bajo Sun Microsystems Común del Desarrollo y Distribución (CDDL) de licencia. LDAP y DSML dependen de la plataforma protocolos independientes. El software se desarrolla y funciona en cualquier sistema de apoyo con el lenguaje de programación Java, incluyendo Linux y las distribuciones comunes de UNIX, Microsoft Windows, Mac OS X.[10]

#### **Directory Server Enterprise Edition**

El componente de servidor de directorio Directory Server Enterprise Edition (DSEE) proporciona la más escalable y de alto rendimiento de datos LDAP para almacenar información de identidad en el sector y sirve como base para la nueva generación de aplicaciones e-business y servicios Web.

Servicio de administración: el servidor de Directorio ofrece un conjunto completo de herramientas de gestión para administrar el servidor, así como el servicio.

El servidor de Directorio ofrece siempre disponibles consistentes los datos de identidad y ofrece un punto central de control para la gestión del servicio. Una GUI basada en Web centralizada y basada en la consola de administración se puede utilizar para configurar y administrar varios servidores de directorio. La interfaz incluye todas las herramientas necesarias para la eficacia de la administración del servidor de día y servicio de configuración de control. Flexibilidad de gestión hace que sea mucho más sencillo de implementar el servicio de directorio en muchos entornos diferentes. Si los centros de datos se subcontratan a terceras empresas o que funcionan de "Lights Out" base que requiere la administración remota, las utilidades de línea de comandos que sea lo más fácil de gestionar el servicio como si estuviera en un centro de datos local.

Disponibilidad: El servidor de directorios de forma nativa soporta una amplia variedad de protocolos de acceso y ofrece un muy flexible y escalable entorno de replicación para asegurar la disponibilidad en entornos distribuidos. El servidor de directorio LDAP soporta la v2 y v3 los protocolos y el directorio de marcado de Servicio de Idiomas (DSML) v2 nativa basada en estándares para el acceso. LDAP y DSML a través de HTTP / Simple Object Access Protocol (SOAP), los protocolos permiten a los clientes en cualquier parte de una red de forma segura la búsqueda y actualización de los objetos del directorio de datos, recibir los cambios realizados por otras aplicaciones, y autenticar usuarios o aplicaciones - incluso a través de firewalls. Para asegurar que no hay ningún punto único de fallo para aplicaciones que utilizan los protocolos antes mencionados para acceder a los datos de identidad, Directory Server soporta un número ilimitado de servidores de sólo lectura.

Seguridad: El servidor de Directorio ofrece muchas características de seguridad avanzadas para lograr el cumplimiento con las políticas de seguridad de la información y para garantizar que sólo aquellos con la debida autorización tengan acceso a la información. Macro-nivel y la dinámica de control de acceso de Instrucciones (AIC), que el acceso definibles en el nivel más bajo de los datos. Hacen posible la definición de políticas de control de acceso una vez y luego volver a utilizarlos en todo el árbol de directorios. Macro AIC se puede utilizar para optimizar el número de AIC en el directorio y así reducir la complejidad del marco de seguridad. Junto con la AIC, acceso basado

en roles proporciona una manera más sencilla para proporcionar acceso basado en la información en la entrada de un usuario. Los roles están definidos y administrados como los grupos, pero dan más eficientes los mecanismos de agrupación de aplicaciones. Funciones se pueden utilizar en los AIC para controlar el acceso a los datos. También puede ser utilizado por la Clase de Servicio (CoS) para definir "virtual" de los atributos de una entrada, reduciendo los requerimientos de almacenamiento en las entradas y permitir un solo cambio para actualizar un número ilimitado de entradas relacionadas. Directory Server soporta un medio para determinar qué acceso tiene un usuario en un conjunto de información. Al utilizar el control de los derechos Get eficaz, los administradores que mantengan políticas de acceso para el servicio de directorio puede reforzar la seguridad de "auditoría" de los permisos de los usuarios del directorio y aplicaciones. Esta capacidad también puede ser usada para construir aplicaciones con interfaces de adaptación, basada en los derechos del usuario. Directorio Server es compatible con los mecanismos de encriptación para proteger los datos en el disco y durante la transferencia a través de canales de comunicación. Combinado con soporte para la replicación fraccionaria y de ocultación de datos basados en el acceso, esto puede ser utilizado para cumplir con la Unión Europea y otras regulaciones de privacidad internacional. Para evitar el acceso no autorizado a cuentas de usuario que pueden utilizarse para obtener información de identidad, Directory Server admite varias directivas de contraseñas que pueden ser definidas en función de cada usuario o dirigidos a determinados grupos.

Escalabilidad: el servidor de Directorio ofrece para el crecimiento vertical y horizontal sin un rediseño importante despliegue. Este nivel de escalabilidad es cada vez más importante como el despliegue crece. El servidor de directorio es el más alto rendimiento de servidor de directorio LDAP en el mercado hoy en día, con la capacidad para proporcionar un rendimiento de búsqueda sostenida de más de 10.000 entradas por segundo en una sola máquina y escalabilidad horizontal a decenas de miles de búsquedas por segundo. La exigencia de conservar y actualizar la información constantemente está aumentando con la expansión del uso de toda la organización. [1]

## **FreeIPA**

Es patrocinado por Red Hat proyecto de código abierto que pretende ofrecer una suite fácil de gestionar la identidad, la política y Auditoría (IPA), dirigido principalmente hacia las redes de ordenadores Linux y Unix. FreeIPA se puede comparar a la Identidad de Novell o el Administrador de Active Directory de Microsoft en que los objetivos y los mecanismos utilizados son similares.

FreeIPA utiliza en la actualidad 389 Directory Server para su aplicación LDAP y Kerberos 5 del MIT para la autenticación y single sign-on. Este año FreeRADIUS y Samba, son también para ser incluidos en la solución de FreeIPA. Aunque cada uno de los principales componentes de FreeIPA es un pre-existentes proyecto de código abierto es la agrupación de estos componentes en un conjunto manejable único que hacen FreeIPA más comparable al de sus primos de software propietario, Identity Manager y Active Directory.[6]

## **Apple Open Directory**

Es el servicio de directorio LDAP modelo de aplicación de Apple Inc. Un servicio de directorio es un programa que almacena y organiza la información sobre los usuarios de una red informática y los recursos de la red y que permite a los administradores de red para gestionar el acceso de los usuarios a los recursos. En el contexto de Mac OS X Server, Open Directory describe un dominio compartido directorio LDAPv3 basado en OpenLDAP y un modelo de autenticación correspondiente compuesto de Apple y la contraseña del servidor de Kerberos 5 atados juntos con un sistema modular de servicios de directorio.

El término Open Directory también se puede utilizar para describir la totalidad de los servicios de directorio marco utilizado por Mac OS X y Mac OS X Server. En este contexto, se describe el papel de un Mac OS X o Mac OS X Server cuando el sistema está conectado a un dominio de directorio existente. [19]

## **OpenLDAP**

Es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP. Está liberada bajo su

propia licencia OpenLDAP Public License. LDAP es un protocolo de comunicación independiente de la plataforma. Muchas distribuciones GNU/Linux incluyen el software OpenLDAP para el soporte LDAP.

### **Componentes**

Básicamente, OpenLDAP posee tres componentes principales:

- ❖ Slapd - Dominio de servidor y herramientas
- ❖ Bibliotecas que implementan el protocolo LDAP
- ❖ Programas cliente: ldapsearch, ldapadd, ldapdelete, entre otros

Históricamente la arquitectura del servidor OpenLDAP (slapd, Standalone LDAP Daemon) fue dividida entre una sección frontal que maneja las conexiones de redes y el procesamiento del protocolo, y una base de datos dorsal o de segundo plano (backend) que trata únicamente con el almacenamiento de datos. La arquitectura es modular y una variedad de backends está disponible para interactuar con otras tecnologías, no sólo bases de datos tradicionales.

Actualmente 16 diferentes backends son proporcionados en la distribución de OpenLDAP, y varios proporcionados por terceros son conocidos para mantener otros backends de manera independiente. Los backends estándar están organizados de manera imprecisa en tres categorías:

- ❖ Backends de almacenamiento de datos (Data Storage backends) - estos realmente almacenan información
  1. back-bdb: el primer backend transaccional para OpenLDAP, construido en base a BerkeleyDB
  2. back-hdb: una variante de back-bdb que es totalmente jerárquica y soporta renombrado de sub-árboles
  3. back-ldif: construido en archivos LDIF de texto plano
  4. back-ndb: un backend transaccional construido en base al motor de cluster NDB de MySQL

- ❖ Proxy backends - actúan como puertas de enlace a otros sistemas de almacenamiento de datos
  1. back-ldap: proxy simple a otros servidores LDAP
  2. back-meta: proxy con características de meta-directorio
  3. back-passwd: usa un sistema basado en Unix de datos passwd y group
  4. back-relay: internamente redirige a otros backends de servidores slapd
  5. back-sql: establece conexiones a bases de datos SQL
- ❖ Backends dinámicos - estos generan datos sobre la marcha
  1. back-config: configuración del servidor slapd vía LDAP
  2. back-dnssrv: localiza servidores LDAP vía DNS
  3. back-monitor: estadísticas de slapd vía LDAP
  4. back-null: un backend nulo, análogo a /dev/null en Unix
  5. back-perl: invoca arbitrariamente módulos de perl en respuesta a peticiones LDAP
  6. back-shell: invoca scripts de shell para peticiones LDAP

Generalmente una petición LDAP es recibida por el frontend, decodificada y luego transferida a un backend para procesamiento. Cuando el backend completa la petición, devuelve un resultado al frontend, quien luego envía el resultado al cliente LDAP. Un overlay es una pieza de código que puede ser insertada entre el frontend y el backend. Es entonces capaz de interceptar peticiones y lanzar otras acciones en ellas antes de que el backend las reciba, y puede también actuar sobre los resultados del backend antes de que éstos alcancen el frontend. Overlays tiene acceso completo a las interfaces de programación (APIs) internas del servidor slapd, y por tanto pueden invocar cualquier llamada que podrían realizar el frontend u otros backends. [29]

### 1.3.2 Sistemas Operativos

Como parte de los esfuerzos que lleva a cabo Cuba para la promoción y el uso de software libre, en el Nodo Central están siendo utilizados sistemas operativos y aplicaciones de esta clase.

**Linux** es un término genérico para referirse a sistemas operativos similares a Unix basados en el núcleo de Linux. Su desarrollo es uno de los ejemplos más prominentes de software libre; normalmente todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la Licencia Pública General de GNU (GNU GPL) y otras licencias libres.

El nombre Linux viene del núcleo Linux, inicialmente escrito por Linus Torvalds en 1991. El software de sistema viene, normalmente, del sistema operativo GNU, iniciado por Richard Stallman en 1983 y mantenido por la Free Software Foundation (FSF, por sus siglas en inglés). La contribución de GNU es la razón por la que algunos prefieren llamar **GNU/Linux** al sistema operativo formado por las herramientas de GNU y el núcleo Linux en su conjunto.[18]

#### 1.3.2.1 Distribuciones GNU/Linux

Una distribución contiene el Kernel Linux (núcleo), bibliotecas y paquetes de software. Es un conjunto de aplicaciones Linux preparadas para que el usuario las pueda instalar (o ejecutar) de forma sencilla. La mayor parte de las distribuciones son fáciles de manejar. El usuario acostumbrado a utilizar Windows no tendrá grandes problemas para adaptarse.

Algunas distribuciones Linux se pueden utilizar sin instalar nada en la computadora. Se les llama LiveCD, pues se graban en un CD y este se inserta en el ordenador, es por ello que suelen ejecutarse más lentamente, ya que funcionan desde el CD y no se pueden guardar los datos. Suelen incluir la opción de instalar la distribución. Es una forma de probar Linux en el ordenador y si gusta, instalar el sistema completo. [27]

Entre ellas se pueden mencionar, a modo de ejemplo: Debian, Ubuntu, Red Hat, Suse, Knoppix, y muchas más. Cada distribución contiene todo lo necesario para instalar un sistema Linux completo: el núcleo, utilidades básicas, bibliotecas, ficheros de soporte y

aplicaciones. Las distribuciones de GNU/Linux pueden obtenerse a través de diferentes fuentes en línea, como internet. Cada una de ellas suele tener su vía de distribución por FTP y un sitio web. Los programas que no se instalan por defecto en cada distribución, es decir, la mayoría de ellos, se obtienen mediante repositorios.

## **Ubuntu**

Ubuntu Linux, es una distribución GNU/Linux basada en Debian GNU/Linux, cuyo nombre proviene de la ideología sudafricana Ubuntu ("humanidad hacia otros").

Proporciona un sistema operativo actualizado y estable para el usuario promedio, con un fuerte enfoque en la facilidad de uso y de instalación del sistema. Al igual que otras distribuciones se compone de múltiples paquetes de software normalmente distribuidos bajo una licencia libre o de código abierto.

Ubuntu está patrocinado por Canonical Ltd., una compañía británica propiedad del empresario sudafricano Mark Shuttleworth que en vez de vender la distribución con fines lucrativos, se financia por medio de servicios vinculados al sistema operativo y vendiendo soporte técnico. Además, al mantenerlo libre y gratuito, la empresa es capaz de aprovechar el talento de los desarrolladores de la comunidad en mejorar los componentes de su sistema operativo. Canonical también apoya y proporciona soporte para cuatro derivaciones de Ubuntu: Kubuntu, Xubuntu Edubuntu y la versión de Ubuntu orientada a servidores ("Ubuntu Server Edition").

Cada seis meses se publica una nueva versión de Ubuntu la cual recibe soporte por parte de Canonical, durante dieciocho meses, por medio de actualizaciones de seguridad, parches para bugs críticos y actualizaciones menores de programas. Las versiones LTS (Long Term Support), que se liberan cada dos años, reciben soporte durante tres años en los sistemas de escritorio y cinco para la edición orientada a servidores. [14]

## **Red Hat**

Red Hat Software Inc. fue fundada en 1994 por Bob Young y Marc Ewing. En agosto de 1999, Red Hat salió a bolsa y sus acciones obtuvieron la octava ganancia de primer día más grande en toda la historia de Wall Street. Cuatro años más tarde, el valor de las



acciones de Red Hat es en torno a una centésima parte del máximo valor que llegara a alcanzar antes de la crisis de las puntocom. Aun así, sus comienzos exitosos en el mercado de valores sirvieron para que Red Hat fuera portada en periódicos y revistas no directamente relacionadas con temas informáticos. En cualquier caso, parece ser que Red Hat ha sabido superar los problemas de otras compañías del mundo de los negocios en torno al software libre y anunció números negros por primera vez en su historia en el último cuarto del año 2002.

Otro de los hechos históricos más importantes de Red Hat fue la adquisición en noviembre de 1999 de Cygnus Solutions, una empresa fundada una década antes y que ya había demostrado cómo con una estrategia integral basada en software libre se puede ganar dinero.

En septiembre de 2003, Red Hat ha decidido concentrar sus esfuerzos de desarrollo en la versión corporativa de su distribución, Red Hat Enterprise Linux.[25]

## **Debian**

El proyecto Debian fue fundado en el año 1993 por Ian Murdock, después de cursar estudios en la Universidad de Purdue. Él escribió el manifiesto de Debian que utilizó como base para la creación de la distribución Debian Linux. Dentro de este texto los puntos destacables son: tenencia de la distribución de manera abierta, coherente al espíritu de Linux (núcleo) y de GNU. El proyecto creció lentamente al principio y lanzó sus primeras versiones 0.9x en 1994 y 1995. Las primeras portabilidades a otras arquitecturas fueron a comienzos de este último año, siendo la primera versión 1.x de Debian lanzada en 1996. Ha habido hasta hoy diez versiones estables, siendo la actual la 5.0 lenny, la de pruebas se denomina testing y para el desarrollo diario se trabaja sobre la llamada inestable (unstable). Está disponible en varias arquitecturas, la versión estable incluye doce plataformas.[21]

En el Nodo Central de la Uho todos los servicios, tanto principales como secundarios, se encuentran trabajando con esta distribución precisamente, pues es una opción excelente para servidores, por su velocidad de procesamiento, confiabilidad, seguridad y sobre todo, porque es parte importante en el cumplimiento de la política de migración gradual a software libre que se lleva a cabo en el país

## **1.4 Conclusiones del Capítulo**

Tras un análisis de los diferentes servicios prestados en el Nodo Central de la RED UHo y las necesidades que el mismo tiene, se llega a la conclusión que es importante la implantación de un sistema de integración de las cuentas de usuarios, que influye en el buen funcionamiento del Nodo; por lo que se decidió utilizar para resolver la problemática existente el sistema de código abierto OpenLdap, ya que constituye una alternativa eficiente y sostenible.

# Capítulo

# 2

## **2. Descripción y Resultados de la Propuesta.**

En el presente capítulo se explica todo lo relacionado con la configuración y adaptación de la propuesta para solucionar la problemática existente, teniendo en cuenta el Reglamento de Seguridad Informática vigente. Para ello se describe cada paso aplicado en el proceso, además se valora la sostenibilidad del sistema en cuanto a su impacto administrativo, socio-humanista, ambiental y tecnológico. Al finalizar el capítulo se muestra la evaluación de la aplicación luego de su puesta en marcha mediante los resultados del criterio de expertos.

### **2.1 OpenLdap ¿Cómo obtenerlo?**

Existen varias vías de adquirir OpenLdap, ya sea en binario (fichero ejecutable o instalador en Microsoft Windows, paquete para el caso de GNU/Linux) o el código fuente, en caso de que se desee contribuir como desarrollador del proyecto.

### 2.1.1 Instalación del sistema

Primeramente y de acuerdo al sistema operativo que se esté usando, obtener los paquetes del software. En el Nodo Central de la UHo el servidor de Ldap se monta sobre Debian 5.0 lenny, los clientes en este caso corren sobre Debian 4.0 etch, Debian 5.0 lenny.

Seguir alguna de las siguientes variantes:

- ❖ Entrar al sistema (login de usuario).
- ❖ Abrir la consola o terminal.
- ❖ Usar el comando su para entrar como root (administrador en los sistemas operativos basados en Unix, como GNU/Linux).
- ❖ Luego: aptitude search Ldap. Aquí aparece una lista de los paquetes que se encuentran en el repositorio y que contienen la palabra clave “Ldap”.
- ❖ Seleccionar los paquetes requeridos, en este trabajo de diploma se utilizan los siguientes: slapd (Servidor Ldap), y sus respectivas dependencias.
- ❖ Instalar mediante el comando: apt-get install los paquetes previamente seleccionados.
- ❖ Los paquetes se instalan automáticamente, luego queda listo el sistema para iniciar su personalización y adaptación al contexto actual.

## 2.2 Descripción del Sistema

A manera de recordatorio, OpenLdap está conformado por un conjunto de herramientas basadas en la arquitectura cliente/servidor que interactúan entre sí para la realización de los trabajos. Como fue citado en el capítulo anterior, sus componentes son los siguientes:

- ❖ slapd - Dominio de servidor y herramientas
- ❖ Bibliotecas que implementan el protocolo LDAP
- ❖ Programas cliente: ldapsearch, ldapadd, ldapdelete, entre otros

En los epígrafes siguientes se describe con mayor detenimiento el proceso de personalización del sistema, entiéndase configuración de cada uno de los ficheros de OpenLdap, los recursos que contienen los mismos y la correcta interrelación entre los distintos componentes para realizar los trabajos necesarios.

### 2.2.1 Componentes y su Configuración

A partir del presente epígrafe se definen los recursos y directivas que poseen los distintos ficheros de configuración del sistema, destacando los más importantes.

Como la inmensa mayoría de los programas que corren sobre distribuciones de GNU/Linux, OpenLdap posee un directorio propio (situado en /etc/ldap), en el que se encuentran los archivos de configuración, así como algunos scripts que se usan para su correcto funcionamiento. Los ficheros principales son: ldap, slapd, todos con extensión .conf, característica de este tipo de archivos en la familia de sistemas operativos GNU/Linux.

Fragmento del fichero ldap.conf

```
#  
# LDAP Defaults  
#  
# See ldap.conf(5) for details  
# This file should be world readable but not world writable.  
  
#BASE      dc=example,dc=com  
#URI ldap://ldap.example.com ldap://ldap-master.example.com:666  
#SIZELIMIT 12  
#TIMELIMIT 15
```

#DEREF                never

BASE dc=facinf,dc=uho,dc=edu,dc=cu

URI    <ldap://10.26.0.248>

### 2.2.1.1 Slapd.

Es el programa central que controla los demás servicios o demonios. Planifica y monitorea todos los trabajos. Normalmente el fichero de configuración se denomina slapd.conf. Es el más complicado de los ficheros necesarios para hacer funcionar el sistema.

La configuración del servidor LDAP se almacena en el archivo /etc/ldap/slapd.conf. Podemos editar manualmente dicho archivo, pero es mejor lanzar el asistente de configuración de slapd. Para ello debemos ejecutar el siguiente comando:

//Lanzar el asistente de configuración de slapd

```
# dpkg-reconfigure slapd
```

Lo primero que pregunta el asistente es si se desea omitir la configuración del servidor LDAP. Obviamente se responde que no, ya que precisamente lo que se quiere es configurar el servidor LDAP (**ver anexo # 1**).

El directorio LDAP debe tener una base, a partir de la cual cuelgan el resto de elementos. Como nombre de la base, habitualmente se utiliza el nombre del dominio. Ejemplo, el dominio de la universidad es uho.edu.cu, lo normal es que la base para dicho directorio LDAP sea: dc=uho,dc=edu,dc=cu (**ver anexo # 2**).

La siguiente pregunta que hace el asistente es el nombre del dominio. Éste nombre lo utilizará para crear el nombre distinguido (DN) o dicho más claramente, nombre identificativo de la base del directorio LDAP (**ver anexo # 3**). Después preguntará por la contraseña que se desea poner al usuario admin (administrador) del servidor LDAP.

Dicha contraseña se pedirá dos veces para evitar errores de tecleo. Se puede poner cualquier contraseña (**ver anexo # 4**).

Acto seguido se muestra una lista con los posibles gestores de datos para almacenar el directorio y en la siguiente ventana se le pone qué sistema utilizar. Lo recomendable es utilizar el sistema HDB (**ver anexo # 5**).

Una vez que se concluyen estos pasos queda configurado el servidor Ldap y listo para comenzar a agregar los usuarios y grupos.

Breve representación con los principales componentes del fichero de configuración del servidor Ldap.

```
# This is the main slapd configuration file. See slapd.conf(5) for more
```

```
# info on the configuration options.
```

```
#####
```

```
#
```

```
# Global Directives:
```

```
# Features to permit
```

```
#allow bind_v2
```

```
# Schema and objectClass definitions
```

```
include /etc/ldap/schema/core.schema
```

```
include /etc/ldap/schema/cosine.schema
```

```
include /etc/ldap/schema/inetorgperson.schema
```

```
include /etc/ldap/schema/openldap.schema
```

```
include /etc/ldap/schema/nis.schema
```

```
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/samba3.schema
include /etc/ldap/schema/gosystem.schema
include /etc/ldap/schema/gofon.schema
include /etc/ldap/schema/goto.schema
include /etc/ldap/schema/gofax.schema
include /etc/ldap/schema/goserver.schema
include /etc/ldap/schema/gosa+samba3.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile      /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile     /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel     none

# Where the dynamically loaded modules are stored
modulepath   /usr/lib/ldap
moduleload   back_hdb
```



# The maximum number of entries that is returned for a search operation

sizelimit 500

# The tool-threads parameter sets the actual amount of CPU's that is used

# for indexing.

tool-threads 1

#####

#

# Specific Backend Directives for hdb:

# Backend specific directives apply to this backend until another

# 'backend' directive occurs

backend            hdb

#####

#

# Specific Backend Directives for 'other':

# Backend specific directives apply to this backend until another

# 'backend' directive occurs

#backend            <other>

#####

#

# Specific Directives for database #1, of type hdb:

```
# Database specific directives apply to this databasse until another
# 'database' directive occurs

database      hdb

# The base of your directory in database #1
suffix        "dc=facinf,dc=uho,dc=edu,dc=cu"

# rootdn directive for specifying a superuser on the database. This is needed
# for syncrepl.
# rootdn      "cn=admin,dc=facinf,dc=uho,dc=edu,dc=cu"

# Where the database file are physically stored for database #1
directory     "/var/lib/ldap"

# The dbconfig settings are used to generate a DB_CONFIG file the first
# time slapd starts. They do NOT override existing an existing DB_CONFIG
# file. You should therefore change these settings in DB_CONFIG directly
# or remove DB_CONFIG and restart slapd for changes to take effect.

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0
```

# Number of objects that can be locked at the same time.

dbconfig set\_lk\_max\_objects 1500

# Number of locks (both requested and granted)

dbconfig set\_lk\_max\_locks 1500

# Number of lockers

dbconfig set\_lk\_max\_lockers 1500

# Indexing options for database #1

index        objectClass eq

# Save the time that the entry gets modified, for database #1

lastmod    on

# Checkpoint the BerkeleyDB database periodically in case of system

# failure and to speed slapd shutdown.

checkpoint    512 30

# Where to store the replica logs for database #1

# relogfile    /var/lib/ldap/relog

# The userPassword by default can be changed

# by the entry owning it if they are authenticated.

# Others should not be able to see it, except the

```
# admin entry below

# These access lines apply to database #1 only

access to attrs=userPassword,shadowLastChange

    by dn="cn=admin,dc=facinf,dc=uho,dc=edu,dc=cu" write

    by anonymous auth

    by self write

    by * none


# happily.

access to dn.base="" by * read


# The admin dn has full write access, everyone else

# can read everything.

access to *

    by dn="cn=admin,dc=facinf,dc=uho,dc=edu,dc=cu" write

    by * read
```

Una vez que se concluye el proceso de configuración del servidor Se procede a configurar la parte cliente para poder comenzar a utilizar el servidor de autenticación.

### 2.2.2 Autenticación basada en Ldap

Como se ha comentado anteriormente, una de las utilidades más importantes de un servidor LDAP es como servidor de autenticación. Autenticarse es necesario para entrar en un sistema Linux. También para acceder a algunos servicios como un servidor FTP o a páginas privadas en un servidor web. Aquí veremos las modificaciones que hay que

realizar en un sistema Linux para que autentique a los usuarios en un servidor LDAP en lugar de utilizar los clásicos archivos `/etc/passwd`, `/etc/group` y `/etc/shadow`. Para ello es necesario instalar y configurar los paquetes `libpam-ldap` y `libnss-ldap`.

#### 2.2.2.1 Librerías de autenticación `pam-ldap` y `nss-ldap`.

La librería **`pam-ldap`** permite que las aplicaciones que utilizan PAM para autenticarse, puedan hacerlo mediante un servidor LDAP. Para que el sistema linux se autentique mediante un servidor LDAP es necesario instalar esta librería ya que utiliza PAM. El archivo de configuración de ésta librería es **`/etc/pam_ldap.conf`**. Hay otras aplicaciones o servicios que utilizan PAM para la autenticación y por tanto podrían, gracias a la librería `pam-ldap`, autenticarse ante un servidor LDAP.

Para especificar el modo de autenticación de cada servicio es necesario configurar los archivos que se encuentran en la carpeta **`/etc/pam.d/`**.

La librería **`nss-ldap`** permite que un servidor LDAP suplante a los archivos **`/etc/passwd`**, **`/etc/group`** y **`/etc/shadow`** como bases de datos del sistema. Su archivo de configuración se encuentra en **`/etc/libnss-ldap.conf`**. Posteriormente deberemos configurar el archivo **`/etc/nsswitch.conf`** para que se utilice LDAP como base de datos del sistema en lugar de los archivos `passwd`, `group` y `shadow`.

#### ***Instalación y configuración de `libpam-ldap`.***

```
# apt-get install libpam-ldap
```

El archivo de configuración de la librería es el archivo **`/etc/pam_ldap.conf`**. Únicamente hay que configurar los siguientes parámetros:

- ❖ Quién es el servidor LDAP (nombre o IP)
- ❖ Cuál es la base de nuestro directorio LDAP (base DN)
- ❖ Cuál es la versión de LDAP a utilizar
- ❖ Quién es el administrador del directorio

- ❖ En qué unidad organizativa se encuentran los usuarios (sustituto de **/etc/passwd**)
- ❖ En qué unidad organizativa se encuentran las contraseñas (sustituto de **/etc/shadow**)
- ❖ En qué unidad organizativa se encuentran los grupos (sustituto de **/etc/group**)

Para ello las líneas que hay que modificar en el archivo de configuración son las siguientes.

```
host 10.26.0.248
```

```
# The distinguished name of the search base.
```

```
base dc=facinf,dc=uho,dc=edu,dc=cu
```

```
# Another way to specify your LDAP server is to provide an
```

```
uri ldap://10.26.0.248/
```

```
ldap_version 3
```

```
rootbinddn cn=admin,dc=facinf,dc=uho,dc=edu,dc=cu
```

```
nss_base_passwd      ou=people,dc=facinf,dc=uho,dc=edu,dc=cu?one
```

```
nss_base_shadow      ou=people,dc=facinf,dc=uho,dc=edu,dc=cu?one
```

```
nss_base_group       ou=groups,dc=facinf,dc=uho,dc=edu,dc=cu?one
```

### **2.2.2.2 Instalación y configuración de libnss-ldap.**

```
# apt-get install libnss-ldap
```

Acto seguido se inicia el asistente de configuración de dicha librería. Se puede lanzar dicho asistente más adelante mediante el comando:

```
# dpkg-reconfigure libnss-ldap
```

Este asistente modificará el archivo `/etc/libnss-ldap.conf` que es donde se almacena la configuración de la librería. Posteriormente se edita dicho archivo manualmente para introducir algún cambio que no realice el asistente.

La primera pregunta que hace el asistente es quién es el servidor LDAP. Podemos poner la IP o el nombre (**ver anexo # 6**), acto seguido pide el nombre de la base (**ver anexo # 7**) y la versión de Ldap que se utilizará (**ver anexo # 8**).

Posteriormente preguntará si el archivo `/etc/libnss-ldap` debe solamente tener permisos de lectura y escritura para el usuario (root que es quién instala) o no (**ver anexo # 9**). Como en el paso anterior se indicó que no se necesita autenticación, no se almacenarán contraseñas en el archivo de configuración, por tanto se puede responder 'No' (**ver anexo # 10**).

Finalmente el asistente advierte que se debe modificar el archivo `/etc/nsswitch.conf` para que el sistema utilice el directorio LDAP como base de datos del sistema, al igual que hace con los archivos `passwd`, `group` y `shadow` (**ver anexo # 11**).

Una vez concluido el asistente se habrá configurado casi todo lo necesario aunque para que el sistema se autentifique por LDAP, aún hay que configurar dos parámetros más:

- ❖ En qué unidad organizativa se encuentran los usuarios (sustituto de `/etc/passwd`)
- ❖ En qué unidad organizativa se encuentran los grupos (sustituto de `/etc/group`)

Para ello se modifican dos líneas en el archivo de configuración.

```
nss_base_passwd      ou=people,dc=facinf,dc=uho,dc=edu,dc=cu?one
```

```
nss_base_group       ou=groups,dc=facinf,dc=uho,dc=edu,dc=cu?one
```

### 2.2.2.3 Configuración del NSS

Para que el servidor LDAP actúe como si se tratara de los archivos `passwd`, `group` y `shadow`, además de instalar las dos librerías anteriores, se debe indicar que utilice LDAP como alternativa para autenticar usuarios. Para ello se configura en las líneas que hacen referencia a `passwd`, `group` y `shadow` en el archivo `/etc/nsswitch.conf`.

Una vez que se configura queda de la siguiente forma.

```
# /etc/nsswitch.conf

# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:    files ldap
group:     files ldap
shadow:    files ldap
hosts:     files dns
networks:  files
protocols: db files
services:  db files
ethers:    db files
rpc:       db files
netgroup:  nis
```

#### 2.2.2.4 Configurar servicios PAM.

El sistema ya esta preparado para autenticarse por LDAP. Editando los archivos que hay en la carpeta **/etc/pam.d**, se puede configurar la forma en la que se autentifica cada uno de los servicios que requieren autenticación.

Para no tener que configurar de cada uno de los servicios, existen unos archivos comunes cuyo nombre empieza por **common** que afectan a la mayoría de ellos y sus archivos de configuración los referencian mediante una línea **@include** a los archivos comunes causando el mismo el efecto que si el contenido de los archivos comunes estuviera copiado en el lugar de la línea **@include**. Los archivos comunes son:

- ❖ **/etc/pam.d/common-auth** (para autenticarse)



- ❖ `/etc/pam.d/common-account` (para disponer de una cuenta)
- ❖ `/etc/pam.d/common-session` (para poder iniciar sesión)
- ❖ `/etc/pam.d/common-password` (para poder cambiar password)

Estos archivos contienen una línea que hace referencia a la librería `pam_unix.so` que corresponde a la autenticación contra los archivos UNIX. Para que los servicios del sistema utilicen primero las librerías `pam_ldap.so` para autenticar al usuario, se debe añadir la línea correspondiente a `pam_ldap.so` por encima de la línea correspondiente a la librería `pam_unix.so` en los archivos `common`. Así, autenticará primero contra el servidor LDAP, y si la autenticación falla, probará después con los archivos UNIX.

### **Configuración del archivo common-auth.**

Para que los servicios del sistema utilicen las librerías pam-ldap para autenticar al usuario, se debe editar el archivo `/etc/pam.d/common-auth` quedando de la siguiente forma.

```
# /etc/pam.d/common-auth - authentication settings common to all services

# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.

auth    sufficient    pam_ldap.so
auth    required      pam_unix.so nullok_secure
```

### **Configuración del archivo common-account.**

Para permitir que los servicios del sistema comprueben la cuenta del usuario mediante las librerías pam-ldap, se debe editar el archivo **`/etc/pam.d/common-account`**.

```
# /etc/pam.d/common-account - authorization settings common to all services

# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system. The default is to
# only deny service to users whose accounts are expired in /etc/shadow.

account sufficient    pam_ldap.so
account    required    pam_unix.so
```

### **Configuración del archivo *common-session*.**

Para permitir que los servicios del sistema obtengan los parámetros de la sesión de usuario mediante las librerías pam-ldap, se debe editar el archivo **/etc/pam.d/common-session**.

```
# /etc/pam.d/common-session - session-related modules common to all services
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive). The default is pam_unix.
session    sufficient    pam_ldap.so
session    required     pam_unix.so
```

### **Configuración del archivo *common-password*.**

Para permitir que los servicios del sistema puedan modificar la contraseña del usuario mediante las librerías pam-ldap, se debe editar el archivo **/etc/pam.d/common-password**.

```
# /etc/pam.d/common-password - password-related modules common to all Services
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
# The "nullok" option allows users to change an empty password, else
# empty passwords are treated as locked accounts.
```

```
# The "md5" option enables MD5 passwords. Without this option, the
# default is Unix crypt.
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
# You can also use the "min" option to enforce the length of the new
# password.
# See the pam_unix manpage for other options.
password sufficient pam_ldap.so
password required pam_unix.so nullok obscure md5
```

## 2.3 Administración del Servidor Ldap

Para lograr hacer mas asequible la administración del servidor Ldap se utilizaran tres herramientas las cuales tienen debilidades y fortalezas a la hora de administrar el servidor pero si se utilizan las tres entonces ya se logra hacer funcionar de forma impecable el servicio de autenticación.

Las herramientas utilizadas son:

1. Jxplorer.
2. PhpLDAPAdmin.
3. Gosa.

### 2.3.1 Jxplorer

JXplorer es un navegador de código abierto de LDAP, originalmente desarrollado por Computer Associates' eTrust. Es compatible con las versiones 2 y 3 de Ldap (**ver anexo # 12**).

Está disponible para descarga gratuita bajo licencia Open Source.

## Funcionalidades

JXplorer plenamente funcional ha sido probado y se ejecuta en Windows, Solaris, Linux y OS390, y debería funcionar en cualquier sistema operativo de apoyo java. Sus características incluyen:

- ❖ Operaciones LDAP normales: añadir / eliminar / copiar / modificar
- ❖ Operaciones complejas: árbol de copiar y borrar árbol
- ❖ Opcional GUI basado en la construcción de filtros de búsqueda
- ❖ Autenticación SASLy SSL
- ❖ conexión con editores / visores
- ❖ conexión con proveedores de seguridad
- ❖ Plantillas HTML / formas de visualización de datos
- ❖ Full i18n support
- ❖ Formato de archivo LDIF de apoyo
- ❖ altamente configurable por el usuario
- ❖ operación drag-and-drop en navegación.
- ❖ Apoyo DSML
- ❖ se ocupa de casos complejos ldap:
  - multi valorado rdns
  - atributos binarios
  - Certificados y contraseñas
  - Caracteres Unicode
  - Caracteres especiales / UTF8 en nombres.
- ❖ Arquitectura extensible basada en clase con objeto de Java plugins.[4]

### 2.3.2 PhpLDAPAdmin

PhpLDAPAdmin también conocido como PLA, es una herramienta para la administración de servidores LDAP escrito en PHP, basado en interfaz Web. Trabaja en varias plataformas, pudiendo acceder al servidor LDAP desde cualquier lugar en Internet usando un navegador Web. Se encuentra disponible bajo licencia GPL

Posee una vista jerárquica basada en árbol en donde se puede navegar por toda la estructura de directorio. Permite ver los esquemas LDAP, realizar búsquedas, crear, borrar, copiar y editar entradas LDAP, incluso copiar entradas entre servidores LDAP (ver anexo # 13).

#### Características

1. Árbol jerárquico de navegación LDAP.
2. Edición de entradas basadas en Plantillas.
3. Copia entradas LDAP (incluso entre servidores distintos).
4. Copia recursivamente un árbol entero.
5. Borra entradas LDAP.
6. Borra recursivamente un árbol.
7. Ver y editar atributos de imágenes.
8. Navegador avanzado de esquema LDAP.
9. Búsquedas LDAP (simple y avanzada).
10. Exporta LDIF y DSML.
11. importa LDIF.
12. Renombra entradas LDAP.
13. Administración de hash de password (sha, crypt, md5, blowfish, md5crypt).
14. Automáticamente determina el DN root Server.

15. Traducción de atributos en una forma más amigables (p.e muestra "Fax" en vez de "facsimileTelephoneNumber").
16. Soporta atributos Binarios.
17. Automáticamente incrementa los números de UID.
18. Disponible en 10 idiomas[17].

### 2.3.3 Gosa

GOsa<sup>2</sup> es un sistema web para la administración servicios de infraestructura en redes de computadoras, incluye la administración de usuarios, grupos y su acceso a los recursos. Se basa en un directorio LDAP y se encuentra escrito principalmente en PHP. GOsa<sup>2</sup> es software libre y se distribuye bajo la licencia GPL (**ver anexo # 14**).

#### Características.

GOsa<sup>2</sup> esta construido de forma modular, esto quiere decir que sus funcionalidades son provistas por los distintos módulos o plugins que se activen.

GOsa<sup>2</sup> integra la administración de:

- ❖ Computadoras de escritorio y clientes delgados
- ❖ Aplicaciones
- ❖ Clientes Linux usando FAI
- ❖ Administración de clientes Windows OPSI
- ❖ Administración de Samba
- ❖ Asterisk

#### Complementos.

GOsa esta compuesto por múltiples complementos o "Plugins" que agregan funcionalidades específicas como:

- |                |                 |
|----------------|-----------------|
| 1. addressbook | 3. connectivity |
| 2. apache2     | 4. dak          |

5. dfs	29.samba
6. dhcp	30.scalix
7. dns	31.squid
8. fai	32.ssh
9. glpi	33.sudo
10.gofax	34.systems
11.gofon	35.uw-imap
12.goto	36.webdav
13.heimdal	
14.kolab	
15.ldapmanager	
16.log	
17.mail	
18.mit-krb5	
19.nagios	
20.netatalk	
21.opengroupware	
22.openexchange	
23.opsi	
24.phpgw	
25.phpscheduleit	
26.pptp	
27.pureftpd	
28.roleManagement	



GOSA<sup>2</sup> proporciona un marco de gran alcance GPL para la gestión de cuentas y sistemas de bases de datos LDAP. GOSA <sup>2</sup> permite a los administradores del sistema para administrar las aplicaciones, los teléfonos y faxes, listas de distribución de correo y muchos otros parámetros. En relación con el FAI (Instalación completamente automática), GOSA <sup>2</sup> permite la instalación altamente automatizada de los sistemas preconfigurados. GOSA <sup>2</sup> por lo tanto proporciona un punto único, basado en LDAP de la administración para entornos de grandes y pequeños, con lo que la administración de usuarios y sistemas, y todos los parámetros relacionados manejable y fácil.[7]

## **2.4 Configuración de los Servicios**

En el Nodo Central de la Uho se prestan los servicios de Mensajería Instantánea, Correo Electrónico e Internet los que se encuentran corriendo sobre el Sistema Operativo debian 5 lenny distribución estable.

En este epígrafe se configuraran los servicios para que autentiquen contra el servidor Ldap anteriormente configurado para ellos se llevara a cabo la instalación y configuración de los antes mencionados.

### **2.4.1 Proxy**

Para montar este servicio se utilizó el Squid es un software libre bajo licencia GPL que implementa un conjunto de características que fueron claves para que se decidiera utilizarlo sobre los demás.

#### **Squid**

Es un popular programa de software libre que implementa un servidor proxy y un dominio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Aunque orientado a principalmente a HTTP y FTP es compatible con otros protocolos como Internet Gopher. Implementa varias modalidades de cifrado como TLS, SSL, y HTTPS.

### **Características.**

Squid posee las siguientes características:

#### ***Proxy y Caché de HTTP, FTP, y otras URL***

Squid proporciona un servicio de Proxy que soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentra fuera de la red interna.

#### ***Proxy para SSL***

Squid también es compatible con SSL (*Secure Socket Layer*) con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios.

#### ***Jerarquías de caché***

Squid puede formar parte de una jerarquía de caches. Diversos proxys trabajan conjuntamente sirviendo las peticiones de las páginas. Un navegador solicita siempre las páginas a un sólo proxy, si este no tiene la página en la caché hace peticiones a sus hermanos, que si tampoco las tienen las hacen a su/s padre/s... Estas peticiones se pueden hacer mediante dos protocolos: HTTP e ICMP.

#### ***ICP, HTCP, CARP, caché digests***

Squid sigue los protocolos ICP, HTCP, CARP y *caché digests* que tienen como objetivo permitir a un proxy "preguntarle" a otros proxys caché si poseen almacenado un recurso determinado.

### **Caché transparente**

Squid puede ser configurado para ser usado como proxy transparente de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

### **WCCP**

A partir de la versión 2.3 Squid implementa WCCP (*Web Cache Control Protocol*). Permite interceptar y redirigir el tráfico que recibe un router hacia uno o más proxys caché, haciendo control de la conectividad de los mismos. Además permite que uno de los proxys caché designado pueda determinar como distribuir el tráfico redirigido a lo largo de todo el array de proxys caché.

### **Control de acceso**

Ofrece la posibilidad de establecer reglas de control de acceso. Esto permite establecer políticas de acceso en forma centralizada, simplificando la administración de una red.

### **Aceleración de servidores HTTP**

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché, si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet. Esta función permite navegar rápidamente cuando los objetos ya están en el caché y además optimiza enormemente la utilización del ancho de banda.

### **SNMP**

Squid permite activar el protocolo SNMP, este proporciona un método simple de administración de red, que permite supervisar, analizar y comunicar información de estado entre una gran variedad de máquinas, pudiendo detectar problemas y proporcionar mensajes de estados.

### **Caché de resolución DNS**

Squid está compuesto también por el programa dnsserver, que se encarga de la búsqueda de nombres de dominio. Cuando Squid se ejecuta, produce un número configurable de procesos dnsserver, y cada uno de ellos realiza su propia búsqueda en DNS. De este modo, se reduce la cantidad de tiempo que la caché debe esperar a estas búsquedas DNS.

El proxy caché es una manera de guardar los objetos solicitados de Internet (por ejemplo, datos como páginas web) disponibles vía protocolos HTTP, FTP y Gopher en un sistema más cercano al lugar donde se piden. Los navegadores web pueden usar la caché local Squid como un servidor proxy HTTP, reduciendo el tiempo de acceso así como el consumo de ancho de banda. Esto es muchas veces útil para los proveedores de servicios de Internet para incrementar la velocidad de sus consumidores y para las redes de área local que comparten la conexión a Internet.

Debido a que también es un proxy (es decir, se comporta como un cliente en lugar del cliente real), puede proporcionar un cierto grado de anonimato y seguridad. Sin embargo, también puede introducir problemas significativos de privacidad ya que puede registrar mucha información, incluyendo las URL solicitadas junto con otra información adicional como la fecha de la petición, versión del navegador y del sistema operativo, etc.

Un programa cliente (por ejemplo, un navegador) o bien tiene que especificar explícitamente el servidor proxy que quiere utilizar (típico para consumidores de ISP) o bien podría estar usando un proxy sin ninguna configuración extra. A este hecho se le denomina caché transparente, en el cual todas las peticiones HTTP son interceptadas por squid y todas las respuestas guardadas en caché. Esto último es típico en redes corporativas dentro de una red de acceso local y normalmente incluye los problemas de privacidad mencionados previamente.

Squid tiene algunas características que pueden facilitar establecer conexiones anónimas. Características tales como eliminar o modificar campos determinados de la cabecera de peticiones HTTP de los clientes. Esta política de eliminación y alteración

de cabeceras se establece en la configuración de Squid. El usuario que solicita páginas a través de una red que utiliza Squid de forma transparente, normalmente no es consciente de este proceso o del registro de información relacionada con el proceso.[30]

### **Instalación y Configuración.**

Una vez que ya se realizó todo el análisis de cuál de todos los software existentes sería el que estaría más acorde con las necesidades del Nodo Central de la Uho se procede a la instalación y configuración del servicio.

```
# apt-get install Squid
```

Una vez que está instalado el servidor Proxy se procede a su configuración editando el fichero `squid.conf` que se encuentra en `/etc/squid/squid.conf`. A continuación se muestran los principales parámetros que se recomienda configurar para el squid.

`http_port`

`cache_mem`

`cache_dir`

`ACL`

`http_access`

`httpd_accel_host`

`httpd_accel_port`

`httpd_accel_with_proxy`

**`http_port:`**

Es el puerto que squid utilizará para funcionar, por defecto squid funciona en el puerto 3128.

`http_port 10.26.0.248:3128`

**`cache_mem:`**

Este parámetro limita la cantidad máxima de memoria que squid utilizará para almacenar objetos.

```
cache_mem 16
```

**cache\_dir:**

Determina el tamaño de la caché en el disco duro que utilizará squid para almacenar información. La cantidad se determina en función de lo que el usuario necesite

```
cache_dir ufs /var/spool/squid 4000 16 256
```

**Listas de control de accesos (ACL)**

```
acl password proxy_auth REQUIRED
```

#Recommended minimum configuration:

```
acl all src 0.0.0.0/0.0.0.0
```

```
acl EFTS src 10.27.2.0/255.255.255.240
```

```
acl manager proto cache_object
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl to_localhost dst 127.0.0.0/8
```

```
acl SSL_ports port 443 # https
```

```
acl SSL_ports port 563 # snews
```

```
acl SSL_ports port 873 # rsync
```

```
acl Safe_ports port 80 # http
```

```
acl Safe_ports port 21 # ftp
```

```
acl Safe_ports port 443 # https
```

```
acl Safe_ports port 70 # gopher
```

```
acl Safe_ports port 210 # wais
```

```
acl Safe_ports port 1025-65535 # unregistered ports
```

```
acl Safe_ports port 280 # http-mgmt
```

```
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 631 # cups
acl Safe_ports port 873 # rsync
acl Safe_ports port 901 # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
```

#### **http\_acces:**

Éste parámetro determina las reglas de control de acceso de nuestra red.

```
# Only allow cachemgr access from localhost
```

```
http_access allow manager localhost
```

```
http_access deny manager
```

```
# Only allow purge requests from localhost
```

```
http_access allow purge localhost
```

```
http_access deny purge
```

```
# Deny requests to unknown ports
```

```
http_access deny !Safe_ports
```

```
# Deny CONNECT to other than SSL ports
```

```
http_access deny CONNECT !SSL_ports
```

### **2.4.2 Correo Electrónico**

Para este servicio se utilizó Postfix y Dovecot por su fácil configuración como por el buen funcionamiento que tienen para el manejo de cuentas de correo.

### **2.4.2.1 Postfix**

Postfix es un Agente de Transporte de Correo (MTA) de software libre / código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail. Anteriormente conocido como VMailer e IBM Secure Mailer, fue originalmente escrito por Wietse Venema durante su estancia en el Thomas J. Watson Research Center de IBM, y continúa siendo desarrollado activamente.

Postfix es el agente de transporte por omisión en diversas distribuciones de Linux y en las últimas versiones del Mac OS X.[2]

#### **Características**

##### ***Diseño modular***

El sistema Postfix está compuesto de varios procesos que se comunican entre sí, aparte de varias utilidades que puede usar el administrador para influir en el sistema u obtener información de él. Este diseño, junto con el fichero master.cf que permite configurarlos tiene algunas ventajas:

- ❖ Cada proceso corre con los mínimos permisos necesarios para realizar su tarea.
- ❖ Es más sencillo localizar cuál está fallando (suponiendo que eso ocurriera :-)
- ❖ Se puede activar la emisión de más información de depuración de forma independiente para cada programa. Esto es realmente útil para resolver problemas.
- ❖ Se puede definir ciertos parámetros para cada uno de ellos, como el número máximo de procesos simultáneos de un tipo.
- ❖ Se pueden activar y desactivar algunos de ellos. Por ejemplo en una máquina dial-up que sólo envía correo podemos desactivar el proceso servidor SMTPD.
- ❖ Se puede insertar procesos externos entre ciertas partes del sistema lo cual es muy útil para anti-virus, filtrados, etc.

Otro aspecto en el que Postfix es modular es en el sistema de colas de mensajes. Se mantienen las siguientes colas:



### **maildrop**

Es donde van los mensajes enviados localmente, mediante la versión de Postfix de `/usr/lib/sendmail`

### **incoming**

Aquí van los mensajes recibidos por SMTP y los que han pasado por la cola maildrop.

### **active**

Los que se está intentando enviar en un momento dado.

### **deferred**

Los que se ha intentado y no se ha podido enviar.

Aunque parezca mucha sobrecarga tanta cola, en realidad Postfix las procesa de forma realmente eficiente.[15]

## **Instalación y configuración del Postfix-Ldap.**

Para comenzar a instalar se abre el Terminal de root y se ejecuta el siguiente comando.

```
# apt-get install Postfix
```

Una vez que ya se ha instalado el postfix solo queda editar el fichero de configuración que se encuentra en `/etc/postfix/main.cf`, y `/etc/postfix/master.cf` para lograr su correcto funcionamiento.

### **Fichero de configuración**

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
```

```
# Debian specific: Specifying a file name will cause the first
```

```
# line of that file to be used as the name. The Debian default
```

```
# is /etc/mailname.
```

```
#myorigin = /etc/mailname
```

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
```

biff = no

# appending .domain is the MUA's job.

append\_dot\_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings

#delay\_warning\_time = 4h

# TLS parameters

### usar TLS siempre que se pueda

smtp\_use\_tls = no

### situación de la clave pública

smtp\_tls\_cert\_file = /etc/postfix/ssl/postfix.pem

### situación de la clave privada (en los ficheros .pem, ambas están juntas)

smtp\_tls\_key\_file = \$smtp\_tls\_cert\_file

### nivel de log. Poner 2 hasta que todo funcione bien

smtp\_tls\_loglevel = 2

### tiempo de validez de las claves

smtp\_tls\_session\_cache\_timeout = 3600s

smtp\_tls\_note\_starttls\_offer = yes

##tiempo mimo del intercambio de claves

smtp\_starttls\_timeout = 300s

##fuente de entropía (hay sistemas que no tienen /dev/urandom)

```
tls_random_source = dev:/dev/urandom
```

```
#smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
```

```
#smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

```
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
```

```
smtp_tls_session_cache_database = btree:$ /smtp_scache
```

```
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for  
# information on enabling SSL in the smtp client.
```

```
smtpd_sasl_auth_enable = yes
```

```
#myhostname = localhost
```

```
myhostname = facinf.uho.edu.cu
```

```
mydomain = uho.edu.cu
```

```
#relay = 192.168.224.1
```

```
relay = 10.26.0.6
```

```
#relay = mail.uho.edu.cu
```

```
myorigin = /etc/mailname
```

```
transport_maps = hash:/etc/postfix/transport
```

```
relayhost = [$relay]
```

```
#mynetworks = 127.0.0.0/8, 10.26.0.0/16, 10.27.2.0/28, 192.168.224.0/24, 10.27.2.0/24,  
10.71.43.0/24
```

```
mynetworks = 127.0.0.0/8, 10.27.2.0/24, 10.71.43.0/24, 10.26.6.1/32, 10.26.8.1/32,  
10.26.14.1/32, 10.26.12.1/32, 10.26.16.1/32, 10.26.4.1/32
```

```
#mynetworks = 127.0.0.0/8, 10.26.6.1/32, 10.26.8.1/32, 10.26.14.1/32, 10.26.12.1/32,
10.26.16.1/32, 10.26.4.1/32
```

```
mailbox_command = procmail -a "$EXTENSION"
```

```
mydestination = facinf.uho.edu.cu, facinf.facinf.uho.edu.cu, localhost.uho.edu.cu,
uho.edu.cu, localhost, vru.uho.edu.cu
```

```
relay_domains = $mydestination
```

```
#alias_maps = hash:/etc/aliases
```

```
alias_maps = hash:/etc/aliases
```

```
#hash:/var/lib/mailman/data/aliases
```

```
#alias_database = hash:/etc/aliases
```

```
##### LIMITAR ENVIO DE CORREOS
```

```
smtpd_recipient_limit = 7
```

```
#####
#####
```

```
#### restricciones de acceso por usuarios ...
```

```
#nacout: usuarios que solo pueden enviar correo a cuba
```

```
#inter: usuarios con cuentas internacionales
```

```
#nacin: usuarios que solo pueden recibir correo de cuba
```

```
#smtpd_restriction_classes = inter,nacout,nacin
```

```
smtpd_restriction_classes = internacional,nacional,auth
```

```
#smtpd_restriction_classes = internacional,nacional
```

```
smtpd_sender_restrictions =
```

```
    permit_mynetworks,
```

```
    check_recipient_access mysql:/etc/postfix/access.cf,
```

```
    permit_auth_destination,
```

```
    reject_unauth_destination,
```

```
#        reject
```

```
smtpd_recipient_restrictions =
```

```
    permit_mynetworks,
```

```
    check_sender_access mysql:/etc/postfix/access.cf,
```

```
    permit_auth_destination,
```

```
    reject_unauth_destination,
```

```
    reject
```

```
auth = permit_sasl_authenticated, reject
```

```
#internacional = permit
```

```
internacional = auth
```

```
nacional = check_recipient_access regexp:/etc/postfix/filtro_nac,
```

```
    reject
```

```
header_checks =regexp:/etc/postfix/header_checks
```

```
body_checks =regexp:/etc/postfix/body_checks
```

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

#### **2.4.2.2 Dovecot**

Dovecot es un servidor de IMAP y POP3 de código abierto para sistemas GNU/Linux / UNIX-like, escrito fundamentalmente pensando en seguridad. Desarrollado por Timo Sirainen, Dovecot fue liberado por primera vez en julio del año 2002. Dovecot apunta fundamentalmente a ser un servidor de correo de código abierto ligero, rápido, fácil de instalar y por sobre todo seguro.

#### **Características**

Dovecot puede trabajar con el estándar mbox, Maildir y sus propios formatos nativos mbox de alto desempeño. Es completamente compatible con implementaciones de servidores UW IMAP y Courier IMAP, así como con clientes que acceden directamente a los buzones de correo.

Dovecot incluye un Agente de Entrega de Correo con un filtro de apoyo Sieve opcional.

1. Soporta POP3/IMAP bajo los estándares pertinentes (incluyendo las conexiones cifradas).
2. Es compatible tanto con mbox como con Maildir.
3. Es RÁPIDO en las consultas IMAP. En parte porque genera unos ficheros de caché en los que indexa los datos que se necesitan.
4. Tiene su propio sistema de autenticación SASL
5. Soporta plugins externos, entre los que se encuentran funcionalidades esenciales como cuota y ACLs o dspam.[3]

#### **Instalación y configuración.**

```
# apt-get install dovecot dovecot-ldap
```

### **Fichero Dovecot-ldap.conf.**

# This file is opened as root, so it should be owned by root and mode 0600.

#

# <http://wiki.dovecot.org/AuthDatabase/LDAP>

hosts =10.26.0.248

dn = cn=admin,dc=facinf,dc=uho,dc=edu,dc=cu

dnpass = a

ldap\_version = 3

base = ou=people,dc=facinf,dc=uho,dc=edu,dc=cu

deref = never

scope = subtree

user\_attrs = homeDirectory=home,uidNumber=uid,gidNumber=gid

user\_filter = (&(objectClass=posixAccount)(uid=%u))

pass\_attrs = uid=user,userPassword=password

pass\_filter = (&(objectClass=posixAccount)(uid=%u))

default\_pass\_scheme = md5

### **Fichero dovecot.conf**

#protocols = imap imaps

protocols = imap imaps pop3 pop3s

#disable\_plaintext\_auth = yes

disable\_plaintext\_auth = yes

#log\_timestamp = "%b %d %H:%M:%S "

log\_timestamp = "%Y-%m-%d %H:%M:%S "

```
mail_privileged_group = mail
```

```
protocol pop3 {
```

```
# Login executable location.
```

```
#login_executable = /usr/lib/dovecot/pop3-login
```

```
# POP3 executable location. See IMAP's mail_executable above for examples
```

```
# how this could be changed.
```

```
#mail_executable = /usr/lib/dovecot/pop3
```

```
#
```

```
# Note that Outlook 2003 seems to have problems with %v.%u format which was
```

```
# Dovecot's default, so if you're building a new server it would be a good
```

```
# idea to change this. %08Xu%08Xv should be pretty fail-safe.
```

```
#
```

```
# NOTE: Nowadays this is required to be set explicitly, since the old
```

```
# default was bad but it couldn't be changed without breaking existing
```

```
# installations. %08Xu%08Xv will be the new default, so use it for new
```

```
# installations.
```

```
#
```

```
pop3_uidl_format = %08Xu%08Xv
```

```
}
```

```
# LDAP database <doc/wiki/AuthDatabase.LDAP.txt>
```

```
passdb ldap {
```



```
# Path for LDAP configuration file

args = /etc/dovecot/dovecot-ldap.conf

}

LDAP database <doc/wiki/AuthDatabase.LDAP.txt>

userdb ldap {

    # Path for LDAP configuration file

    args = /etc/dovecot/dovecot-ldap.conf

}
```

### 2.4.3 Mensajería Instantánea

Para montar este servicio se probaron distintos software para servidores de mensajería pero por su sencillez, su administración desde una pagina web, su multiplicidad de funciones se instaló Openfire, con Openfire instalado se tiene un servidor de mensajes instantáneos sin tener que acudir a servicios de terceros. Esto implica una red de mensajería instantánea segura, sin posibilidad de ser interceptada, gracias al uso del protocolo TLS.

#### 2.4.3.1 Openfire

Es un sistema de mensajería instantánea GPL y hecho en java y utiliza el protocolo XMPP con el podrás tener tu propio servidor de mensajería puedes administrar a tus usuarios, compartir archivos, auditar mensajes, mensajes offline, mensajes broadcast, grupos y además contiene plugins gratuitos con diferentes funciones extras. La administración del servidor se hace a través de una interfaz web, que corre por defecto en el puerto 9090 (HTTP) y 9091 (HTTPS). Los administradores pueden conectarse desde cualquier lugar y editar la configuración del servidor, agregar y borrar usuarios, crear cuartos de conferencia permanentes.

Características

- ❖ Panel de administración web
- ❖ Interfaz para agregar plugins

- ❖ SSL/TLS
- ❖ Amigable
- ❖ Adaptable según las necesidades
- ❖ Conferencias
- ❖ Interacción con MSN, Google Talk, Yahoo messenger, AIM, ICQ
- ❖ Estadísticas del Servidor, mensajes, paquetes, etc.
- ❖ Cluster con múltiples servidores
- ❖ Transferencia de Archivos
- ❖ Compresión de datos
- ❖ Tarjetas personales con Avatar
- ❖ Mensajes offline
- ❖ Favoritos
- ❖ Autenticación vía Certificados, Kerberos, LDAP, PAM y Radius
- ❖ Almacenamiento en Active Directory, LDAP, MS SQL, MySQL, Oracle y PostgreSQL.[12]

### Instalación y configuración.

```
# apt-get install Openfire
```

Después de esto se procede a su configuración.

Ejecute un navegador, en la dirección digite `http://localhost:9090`, luego de esto, seleccione el idioma, español y presione el botón de continuar (**ver anexo # 15**), en la próxima ventana se pone el nombre del dominio y el puerto de la consola de administración y se presiona el botón continuar (**ver anexo # 16**), acto seguido se escoge el tipo de conexión que se tendrá con la base de datos la cual será base de datos interna (**ver anexo # 17**).y se pasa al siguiente paso en la configuración que es seleccionar el sistema de usuarios y grupos a utilizar en openfire en este paso escogemos Servidor de Directorio Ldap (**ver anexo # 18**).

En la pagina **Seteos de perfil: Seteos de Conexión Paso 1 de 3: Seteos de Conexión Servidor LDAP** configure su conexión a servidor LDAP, **Tipo de Servidor: OpenLDAP**, **Servidor: localhost**, **DN Base: dc=facinf,dc=uho,dc=edu,dc=cu**, en **Autenticación**, **DN del Administrador: cn=admin, dc=facinf,dc=uho,dc=edu,dc=cu** y **Clave:** la clave del administrador, para comprobar que todo ha sido ingresado correctamente presione el botón **Testear seteos** (recomendado) o continúe presionando el botón Salvar y continuar (**ver anexo # 19**),, Ahora se pasa al **Paso 2 de 3: Mapeos de Usuarios** donde se le dice a openfire la forma en la que encontrara y cargara los usuarios del servidor Ldap (**ver anexo # 20**), y en el tercer paso que es el mapeo de grupos se le configura la forma en que accederá a los grupos del servidor Ldap (**ver anexo # 21**) una vez que se concluyen todos estos pasos se procede a agregar el usuario o los usuarios del servidor Ldap que serán administradores del Openfire (**ver anexo # 22**) se presiona el botón continuar y se concluye la instalación (**ver anexo # 23**) se presiona en conectarse a la consola de administración (**ver anexo # 24**) para adaptar el servidor a las características del dominio.

## 2.5 Valoración de sostenibilidad de la propuesta de solución

A continuación se describe la valoración del sistema propuesto según el impacto que el mismo puede ocasionar en el medio donde se planea implantar, desde distintas dimensiones: administrativa, socio-humanista, ambiental y tecnológica. Es importante determinar si la aplicación propuesta se adapta satisfactoriamente al entorno para el que fue decidida su utilización, haciendo énfasis en la protección del medio ambiente como la medida esencial de todo proceso relativo a la elaboración, configuración y explotación de los sistemas informáticos.

### 2.5.1 Dimensión Administrativa

La implantación del producto informático constituirá el resultado de un trabajo de diploma y por consiguiente no requerirá inversión alguna. El ahorro de recursos será efectivo, pues la información estará en formato digital. Influirá de manera favorable en la calidad de los servicios que se prestan, porque aumentará la capacidad de respuesta ante los desastres que puedan ocurrir. Minimizará el tiempo de trabajo en la gestión de los usuarios de los sistemas del Nodo Central de la Universidad de Holguín. No

generará monetariamente ningún ingreso directo ni indirecto. El sistema no requerirá pago de licencias ni permisos especiales, pues la plataforma es libre.

### **2.5.2 Dimensión Socio-Humanista**

El producto informático resolverá la ausencia de un sistema informático que centralice la administración de las cuentas de usuarios de los servicios que presta el Nodo Central. Se implantará en el Nodo Central UHo, se podrá extender a los demás nodos de otras facultades y la red del MES. El sistema mejorará notablemente el trabajo de los administradores del Nodo Central, principalmente con el ahorro de tiempo y el aumento de la confiabilidad de los datos, con su uso no se disminuirán empleos, ni se generarán nuevas plazas, ya que el personal existente resulta suficiente para su correcta utilización. Ayudará en la formación de valores en el personal que lo implanta, por ejemplo, solidaridad y preocupación por los intereses colectivos. Debido a los problemas que resolverá, será acogido con aceptación por los usuarios finales, no existirá rechazo por parte de estos. Con la puesta en marcha del sistema existirá un aporte a la ciencia, pues formará parte de un proceso de investigación que resolverá la problemática planteada mediante el uso de tecnologías de software libre.

### **2.5.3 Dimensión Ambiental**

Influirá indirectamente en el ahorro de recursos dañinos al entorno, pues disminuirá la cantidad de materiales utilizados en el proceso laboral; no impactará directamente al medio ambiente, aunque lo favorecerá en cierta medida. Los colores usados en la interfaz gráfica resultan adecuados, lo más agradable posible al usuario y no genera ruidos. Con el uso de la interfaz intuitiva del sistema disminuirá el riesgo de estrés psicológico que puedan padecer los usuarios. Podrá ser reutilizado el código fuente de esta aplicación, además es permisible su mejora y su uso para otros proyectos siempre que cumpla lo planteado en la Licencia Pública General (GNU/GPL). Para manejar este sistema informático, se deberá hacer uso de la computadora, lo que podrá traer consigo enfermedades vinculadas a ello. Para mitigar los daños, el sistema posee un tamaño de fuente adecuado, además de accesibilidad por teclado y ratón, sin embargo, para cuidar mejor la visión se recomienda disminuir el brillo de los monitores o colocar protectores de pantalla.

#### **2.5.4 Dimensión Tecnológica**

Los usuarios finales que administrarán el sistema poseen competencias laborales adecuadas, sólo necesitan una mínima capacitación para adaptarse al mismo, la organización cuenta con la infraestructura necesaria para la implantación y utilización de este producto informático. El nivel de independencia de la organización usuaria para sostener el sistema se puede catalogar de alto, siempre que existan uno o varios trabajadores aptos para mantener la aplicación con la tecnología actual y los recursos que se poseen. Sus vulnerabilidades se circunscriben a los diversos problemas que acechan a todo sistema informático. La aplicación podrá adaptarse sin complicaciones a futuros cambios, como quitarle o añadirle funcionalidades. Su evolución estará en dependencia de cómo se adapte al entorno en donde se implanta.

#### **2.5.5 Conclusiones de la valoración de sostenibilidad.**

Se puede afirmar que el sistema informático propuesto es sostenible porque se podrá mantener en la misma medida de su utilización por los trabajadores (administradores) y perdurará en el tiempo como la solución del problema que genera su explotación. El código fuente del mismo podrá ser reutilizado o mejorado si se requiere, y su calidad en general se cataloga de satisfactoria.

### ***2.6 Valoración de resultados con la implantación de los Mecanismos para la Centralización de Cuentas de Usuarios.***

Luego de la implantación del sistema se alcanzaron varios beneficios, primeramente se debe mencionar la centralización de las cuentas de usuarios esencial para la administración de los servicios. Además de contar con este servicio, se poseen también otras herramientas con las que antes no se contaba por lo que de forma general el sistema de integración de cuentas de usuarios agiliza y le facilita de forma considerable la administración a los administradores del Nodo Central de la Uho.

Para obtener un estimado de la utilidad e importancia de haber implantado este sistema, se desarrolló el método científico de criterio de expertos, conocido también como Método Delphi.

La encuesta realizada, así como los resultados de la aplicación de este método, se adjuntan en los **anexos 25 y 26**.

## **2.7 Conclusiones del capítulo.**

Luego de la concepción e implantación de los Mecanismos para la Centralización de Cuentas de Usuarios se puede concluir:

- Los Mecanismos para la Centralización de Cuentas de Usuarios para el apoyo a la administración y monitoreo de los servicios que brinda el Nodo Central de la UHo, basado en principios de problemas de satisfacción y desarrollo con herramientas y tecnologías libres como OpenLdap, permite una mayor organización y control en los Nodos con este tipo de tecnología que lo implementen y apoya a la toma de decisiones de sus administradores.
- El sistema informático desarrollado, según las dimensiones administrativa, socio – humanista, ambiental y tecnológica es sostenible.

---

## Conclusiones

Al término de la presente investigación, se arribaron a las siguientes conclusiones:

- La implantación de Mecanismos para la Centralización de Cuentas de Usuarios es un problema altamente complejo y muy investigado, que requiere de un estudio minucioso de todos los factores que están implicados y su tratamiento, lo que permitió la realización de un buen proceso de informatización.
- Para solucionar el problema científico planteado se asumieron las bases teóricas de ésta investigación resultando esencial para la concepción general de los mecanismos unidos con el estudio de los procedimientos tradicionales.
- Los Mecanismos para la Centralización de Cuentas de Usuarios han de permitir desarrollar una administración y monitoreo más completa de las cuentas de los Servicios a los Administradores del Nodo Central de la Red UHo.
- Fue realizada la valoración de sostenibilidad de los Mecanismos para la Centralización de Cuentas de Usuarios, dentro de la cual se valoró la utilización de herramientas y tecnologías de software libre como una solución viable y superior a las de software comercial, se puede afirmar que los mismos son sostenible.
- Los argumentos obtenidos permiten afirmar que se cumple la hipótesis y se logró el objetivo para resolver el problema que dio lugar a esta investigación.

---

## Recomendaciones

Los Mecanismos de Centralización de Cuentas de Usuarios que se han desarrollado e implantado son un eslabón de la cadena de transformaciones en que se encuentra inmerso el Nodo Central de la UHo. Muchas son las expectativas de mejoras de los diferentes servicios de red que se brindan. El estudio de la situación problemática arrojó otras dificultades que por diferentes aspectos no fueron posibles culminar, y las que se reflejan a continuación como parte de las recomendaciones de este trabajo de diploma:

- Valorar la extensión de estos Mecanismos de Centralización de Cuentas de Usuarios a todos los Nodos de la Red Uho que usen este tipo de tecnología.
- Valorar la extensión de estos Mecanismos de Centralización de Cuentas de Usuarios a todos los Nodos de la Red Mes.
- Valorar la implantación de un servidor de domino utilizando Ldap para la red Uho.



## Referencias Bibliográficas

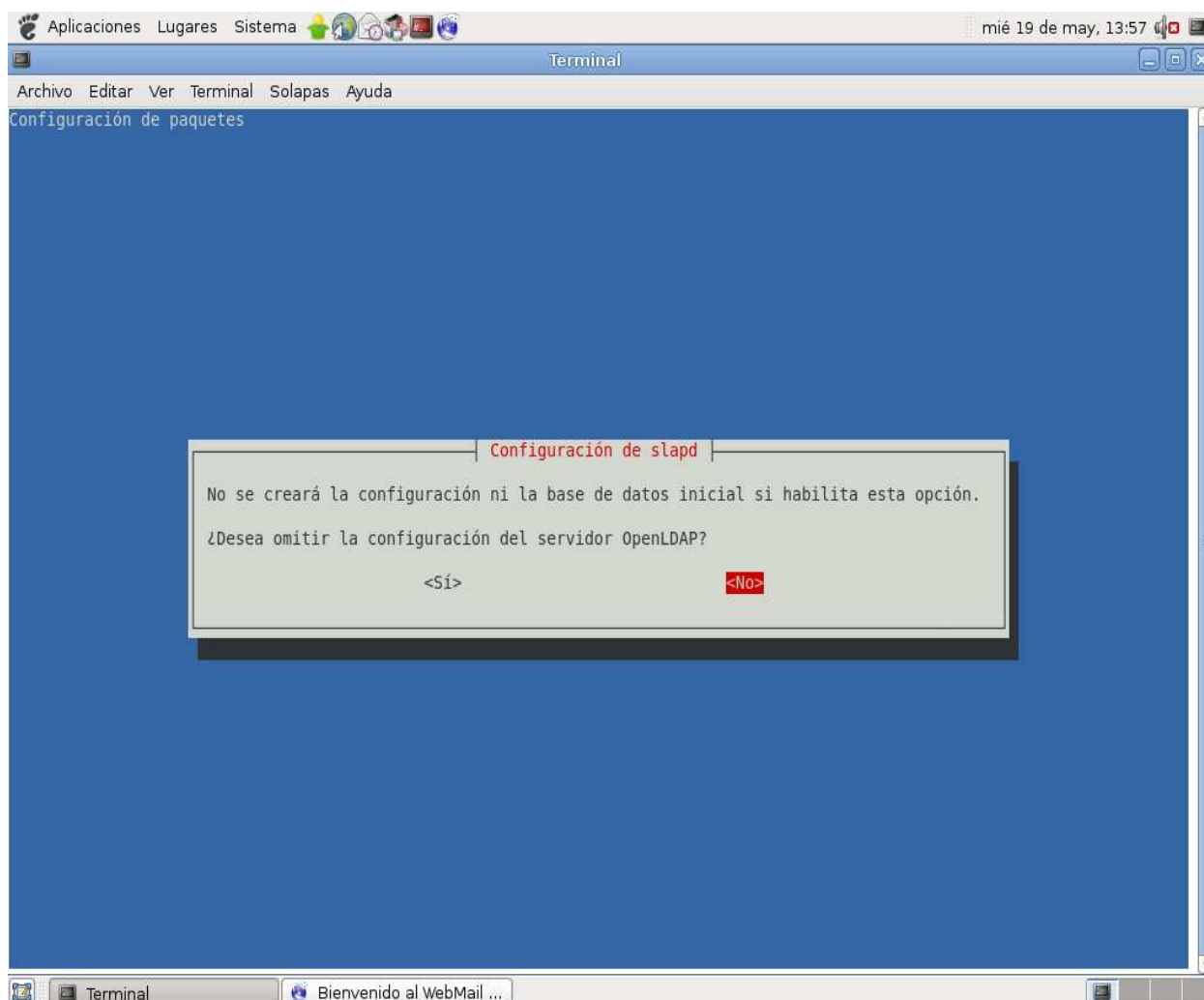
1. Directory Server. [Consultado: enero de 2010]; en [http://www.sun.com/software/products/directory\\_srvr\\_ee/dir\\_srvr/index.xml](http://www.sun.com/software/products/directory_srvr_ee/dir_srvr/index.xml).
2. ebox. [Consultado: octubre/2008]; en <http://es.wikipedia.org/wiki/EBox>.
3. Endian Firewall. [Consultado: enero/2009]; en <http://www.bicubik.net/2006/06/13/endian-firewall/>
4. Familia de protocolos de Internet. [Consultado: enero/2009]; en [http://es.wikipedia.org/wiki/TCP\\_IP](http://es.wikipedia.org/wiki/TCP_IP).
5. File Transfer Protocol. [Consultado: diciembre/2008]; en [http://es.wikipedia.org/wiki/File\\_Transfer\\_Protocol#Cliente\\_FTP](http://es.wikipedia.org/wiki/File_Transfer_Protocol#Cliente_FTP).
6. FreeIPA. [Consultado: enero de 2010]; en <http://en.wikipedia.org/wiki/FreeIPA>.
7. GOsa. [Consultado: abril 2010]; en <http://es.wikipedia.org/wiki/GOsa>.
8. La Definición de Software Libre. 2010 [Consultado: enero/2010]; en <http://www.gnu.org/philosophy/free-sw.es.html>.
9. Mensajería instantánea. [Consultado: enero de 2010]; en [http://es.wikipedia.org/wiki/Mensajería\\_instantánea](http://es.wikipedia.org/wiki/Mensajería_instantánea).
10. OpenDS. [Consultado: enero de 2010]; en <http://en.wikipedia.org/wiki/OpenDS>.
11. "Plan de seguridad informática y de contingencias y acceso Internet", Universidad de Holguín "Oscar Lucero Moya". 2007.
12. Servicio Proxy-Caché. [Consultado: diciembre/2008]; en <http://www.ujaen.es/sci/redes/proxy/>.
13. Sobre Linux. [Consultado: diciembre/2008]; en [http://www.linux-es.org/sobre\\_linux](http://www.linux-es.org/sobre_linux).
14. Ubuntu. [Consultado: marzo de 2010]; en <http://es.wikipedia.org/wiki/Ubuntu>.
15. Un cortafuego amigable. [Consultado: enero/2009]; en <http://www.mexicoextremo.com.mx/content/view/807/2/>
16. Almenares Iserns, Y., Beltrán Oro, M, "Sistema Web de Control de la información de los servicios que presta el Nodo Red UHo," Tesis para optar por el título de Ingeniería en Informática Facultad de Matemática-Matemática. Universidad de Holguín "Oscar Lucero Moya", . Holguín, 2005.
17. Altadill Izura, P.X., IPTABLES Manual practico.

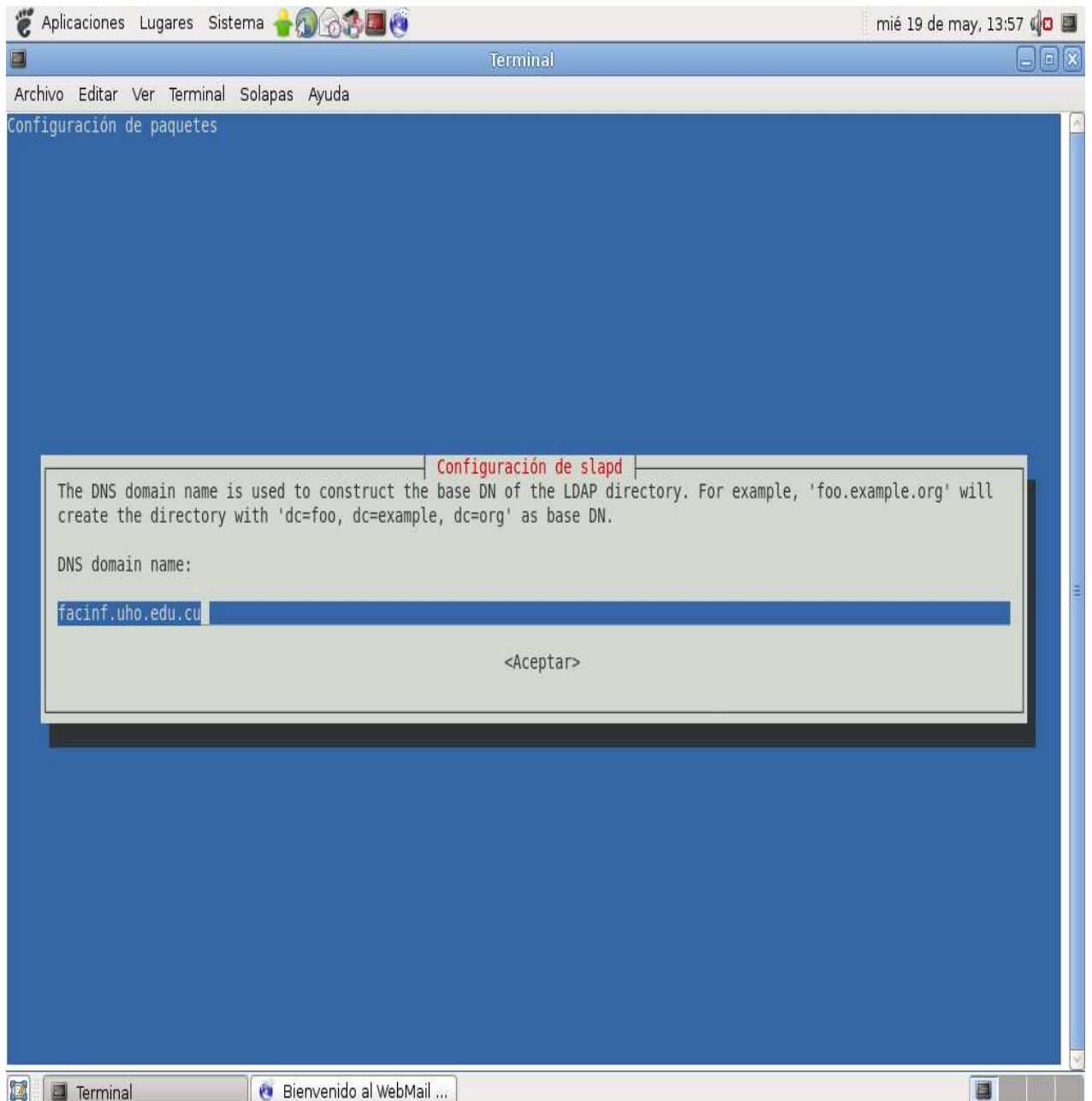
18. Argentina, R.T.A.P., Manual de Seguridad en Redes. 2001.
19. Bustillos Safe, A.A. Las Redes. 2004 [Consultado: diciembre/2008]; en <http://www.monografias.com/trabajos15/redes-clasif/redes-clasif.zip>.
20. Chang Peña, M.E., Sistema para la gestión de copias de seguridad de los servicios que presta el Nodo Central de la Universidad de Holguín "Oscar Lucero Moya". 2009.
21. Elorreaga Madrigal, D.R. Firewalls. 2003 [Consultado: diciembre/2008]; en <http://www.monografias.com/trabajos14/firewalls/firewalls.zip>.
22. Limon, F., "Tutorial de postfix," 2002, 43 p.
23. Limon Flimon, F., "Tutorial de postfix," 2003, 45 p.
24. Martínez Obregón, J.H. Diseño y administración de redes. [Consultado; en <http://www.monografias.com/trabajos62/disenio-administracion-redes/disenio-administracion-redes.zip>].
25. Shuth Hurtado, R., "Implementación de un Servidor/Firewall Gnu/Linux en un Entorno Escolar", Trabajo para optar al título de Bachiller Académico. Colegio Alemán de Medellín. Áreas de Informática y de Español. Itagüí, 2008.
26. Suárez, J.M., Curso OpenLDAP. 2004.
27. Tafur, M. Seguridad Informatica en las Pymes: Parte 2. [Consultado: enero/2009]; en [http://www.enterese.net/articulos/articulo\\_192.php](http://www.enterese.net/articulos/articulo_192.php).
28. Torrez Zaldívar, R., "Subsistemas de Apoyo para la Gestión de las Cuentas de Usuarios de los Servicios de Correo Electrónico, Internet y Acceso Remoto que brinda el Nodo Central de la Universidad de Holguín Oscar Lucero Moya" Tesis para optar por el título de Ingeniería en Informática Facultad de Matemática-Matemática. Universidad de Holguín "Oscar Lucero Moya",. Holguín, 2008.
29. Urueña León, E.E. Redes de Área Local. 2006 [Consultado: enero/2009]; en <http://www.monografias.com/trabajos30/redes-de-datos/redes-de-datos.zip>
30. Villalón Huerta, A., Seguridad en Unix y Redes. Julio, 2002.

## Anexos

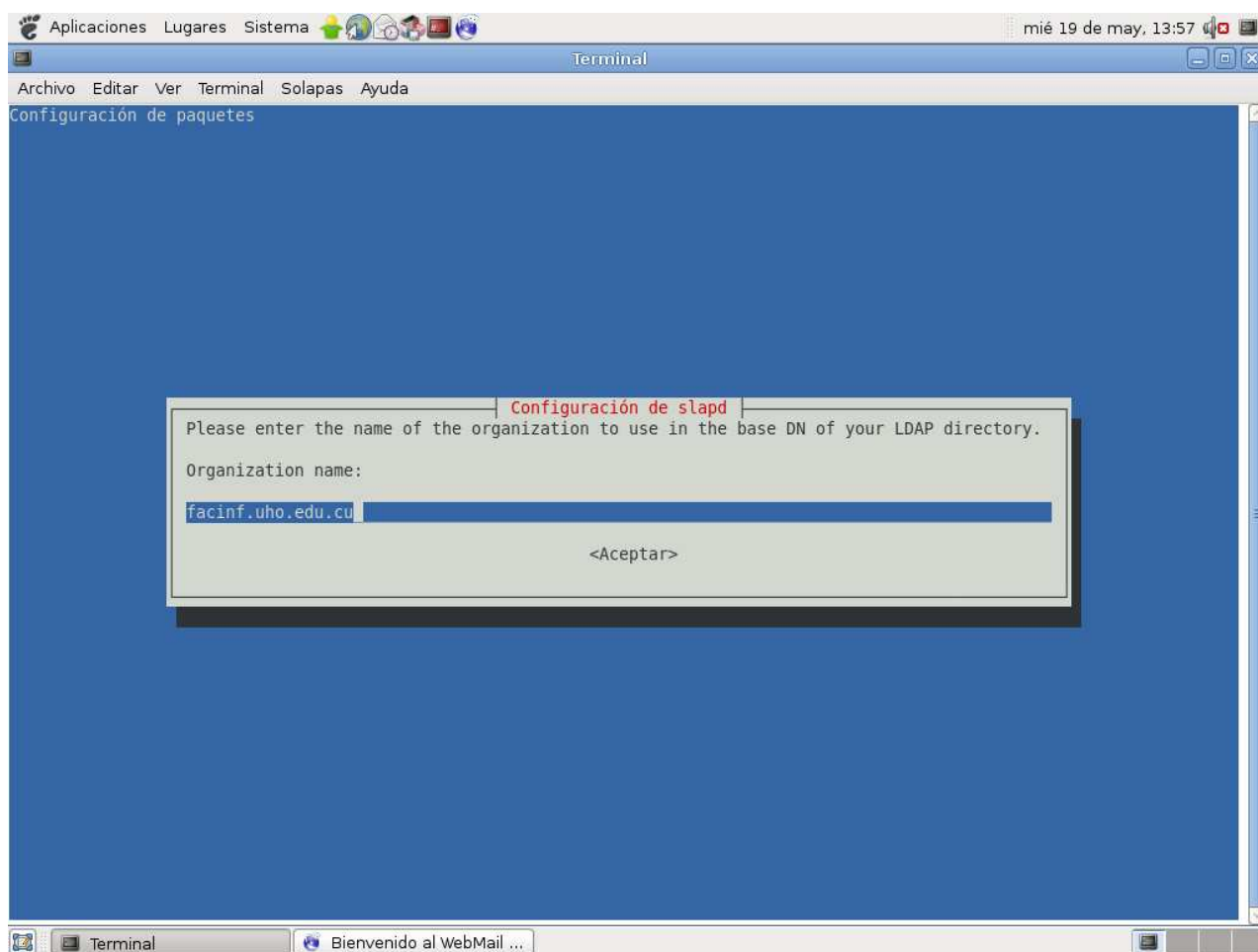
Anexo 1 Configuración por defecto del servidor.....	77
Anexo 2 Nombre del dominio.....	78
Anexo 3 Nombre de la organización. ....	79
Anexo 4 Contraseña de administración.....	80
Anexo 5 Gestores de datos a almacenar. ....	81
Anexo 6 Identificador de recursos para el servidor Ldap.....	82
Anexo 7 Nombre distintivo para la base de búsquedas.....	83
Anexo 8 Versión de Ldap a Utilizar. ....	84
Anexo 9 Permisos a lo usuarios a acceder a la base de datos ....	85
Anexo 10 Permisos especiales de Ldap para root. ....	86
Anexo 11 Fin de instalación de libnss-ldap. ....	87
Anexo 12 Interfaz administrativa de Jxplorer. ....	88
Anexo 13 Interfaz administrativa de PhpLdapAdmin.....	89
Anexo 14 Interfaz administrativa de Gosa.....	90
Anexo 15 Selección del lenguaje del Openfire.....	91
Anexo 16 Especificación del domino y puertos. ....	92
Anexo 17 Configuración de la fuente de datos.....	93
Anexo 18 Tipo de servidor a utilizar. ....	94
Anexo 19 Seteos de conexión. ....	95
Anexo 20 Mapeo de usuarios. ....	96
Anexo 21 Mapeo de grupos. ....	97
Anexo 22 Cuenta de administración de Openfire. ....	98
Anexo 23 Fin de la instalación. ....	99
Anexo 24 Consola de administración.....	100
Anexo 25 Encuesta aplicada a expertos. ....	101
Anexo 26 Resultados de la encuesta aplicada mediante el empleo del Método Delphi.....	103

## Anexo 1 Configuración por defecto del servidor.

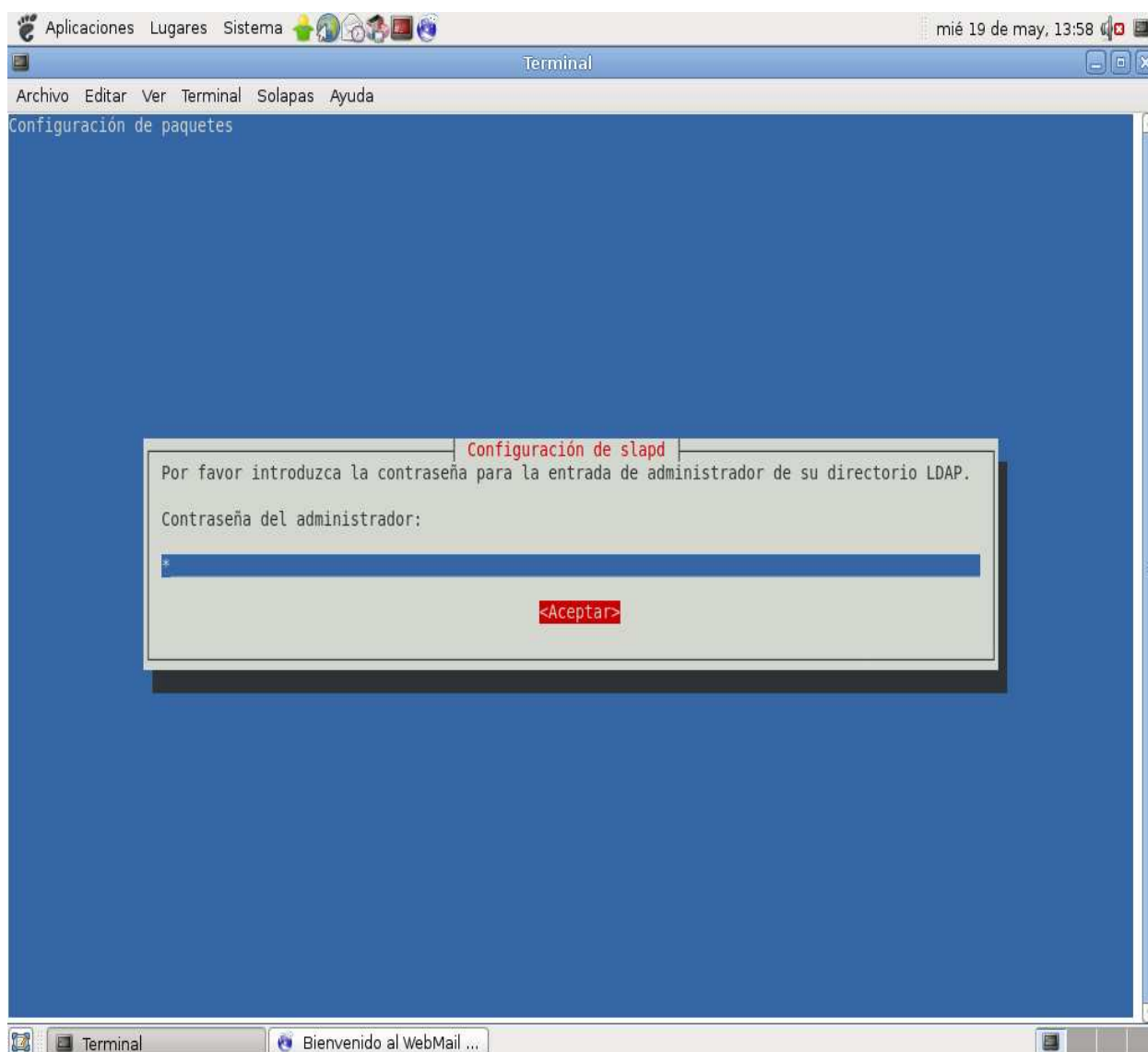


**Anexo 2 Nombre del dominio.**

### Anexo 3 Nombre de la organización.



## Anexo 4 Contraseña de administración.

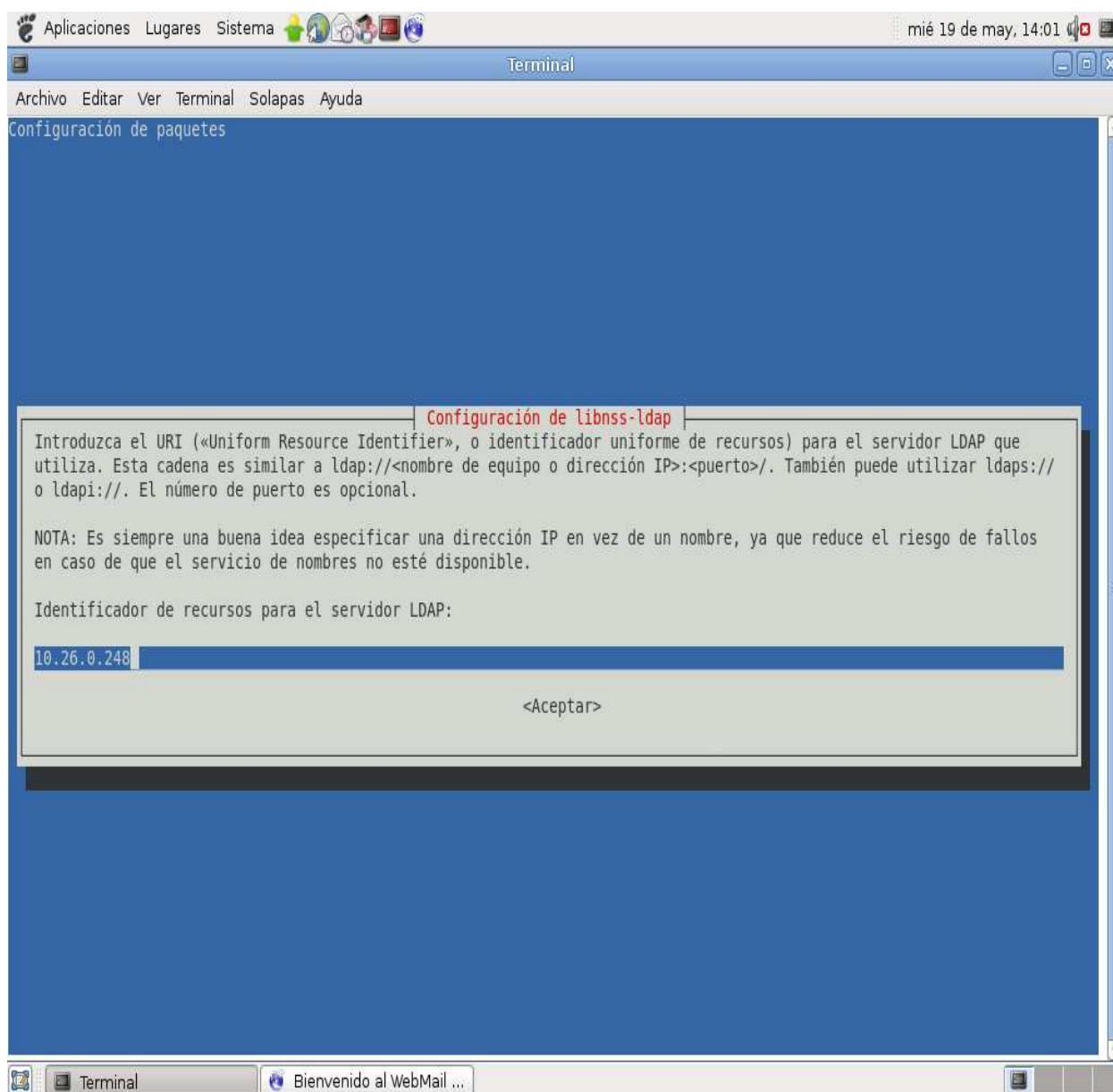


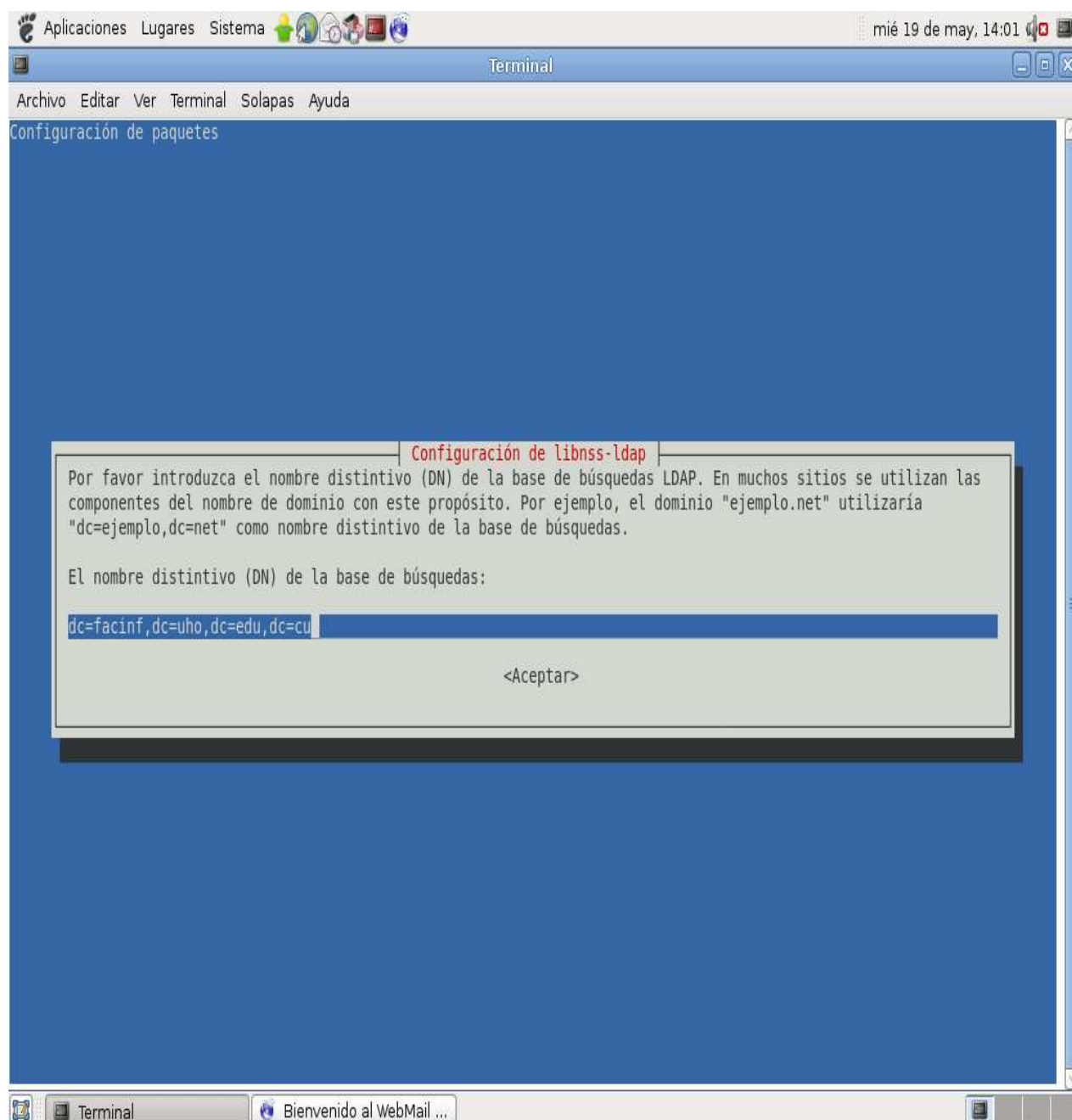
## Anexo 5 Gestores de datos a almacenar.



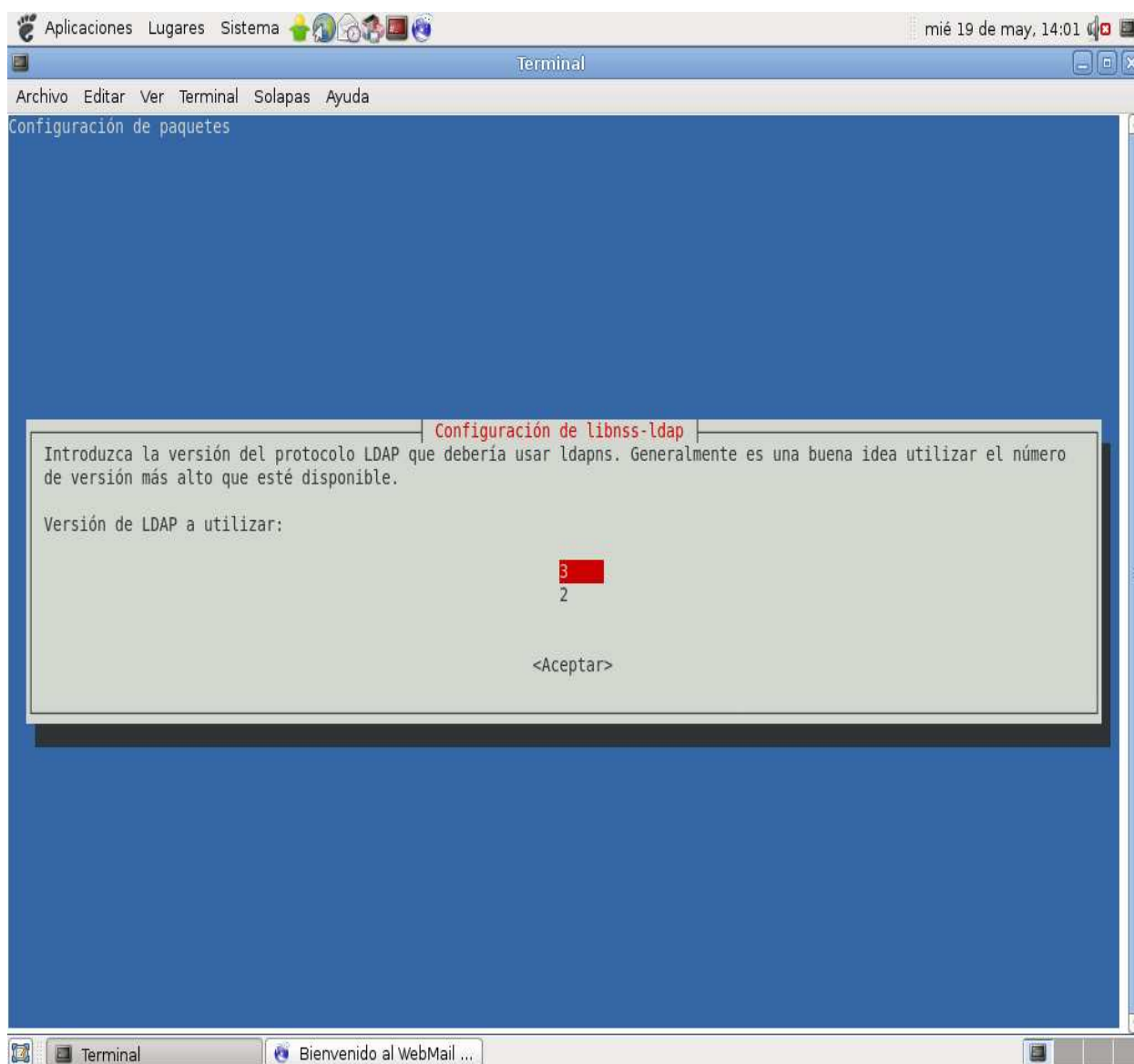


## Anexo 6 Identificador de recursos para el servidor Ldap

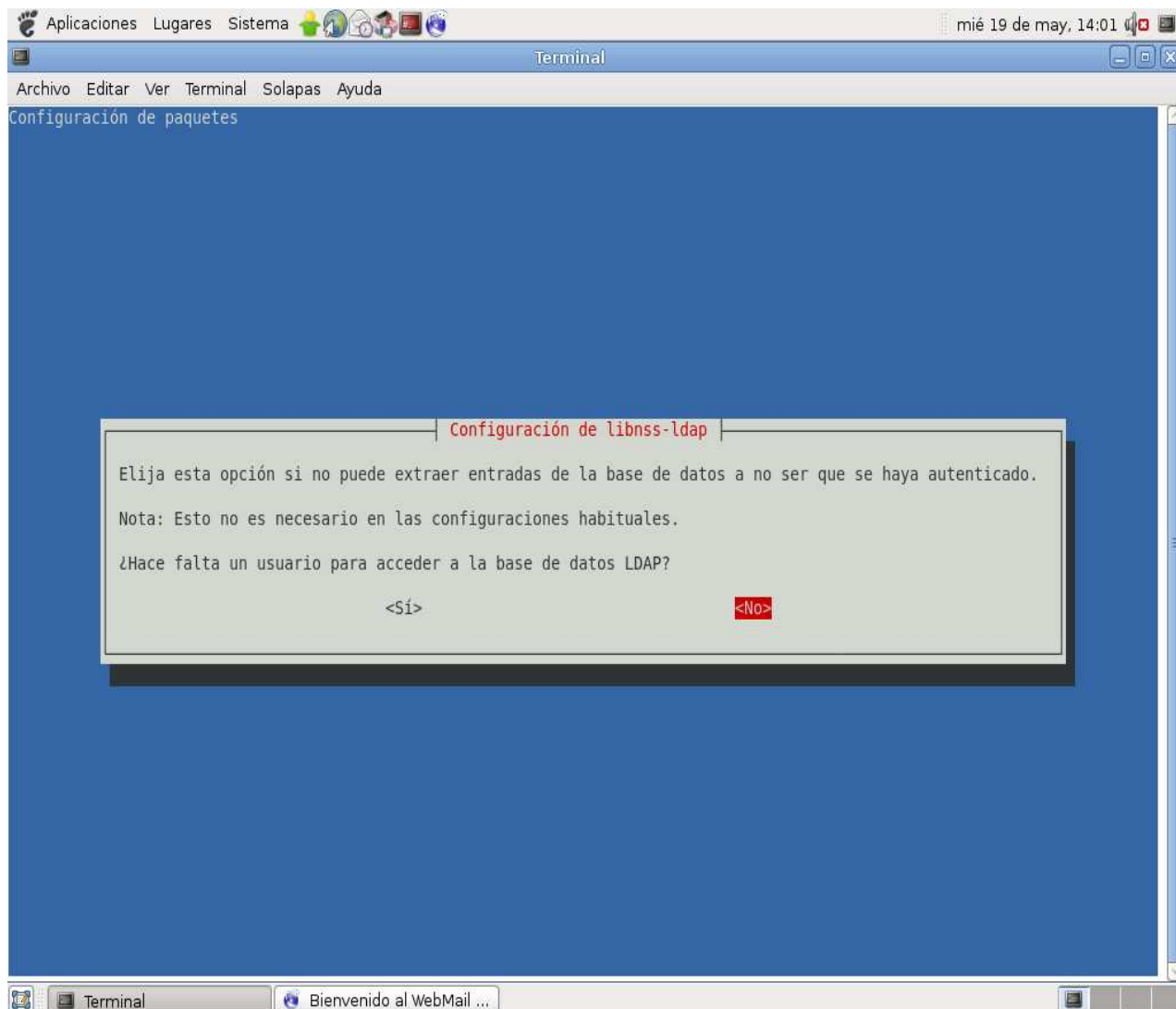


**Anexo 7 Nombre distintivo para la base de búsquedas.**

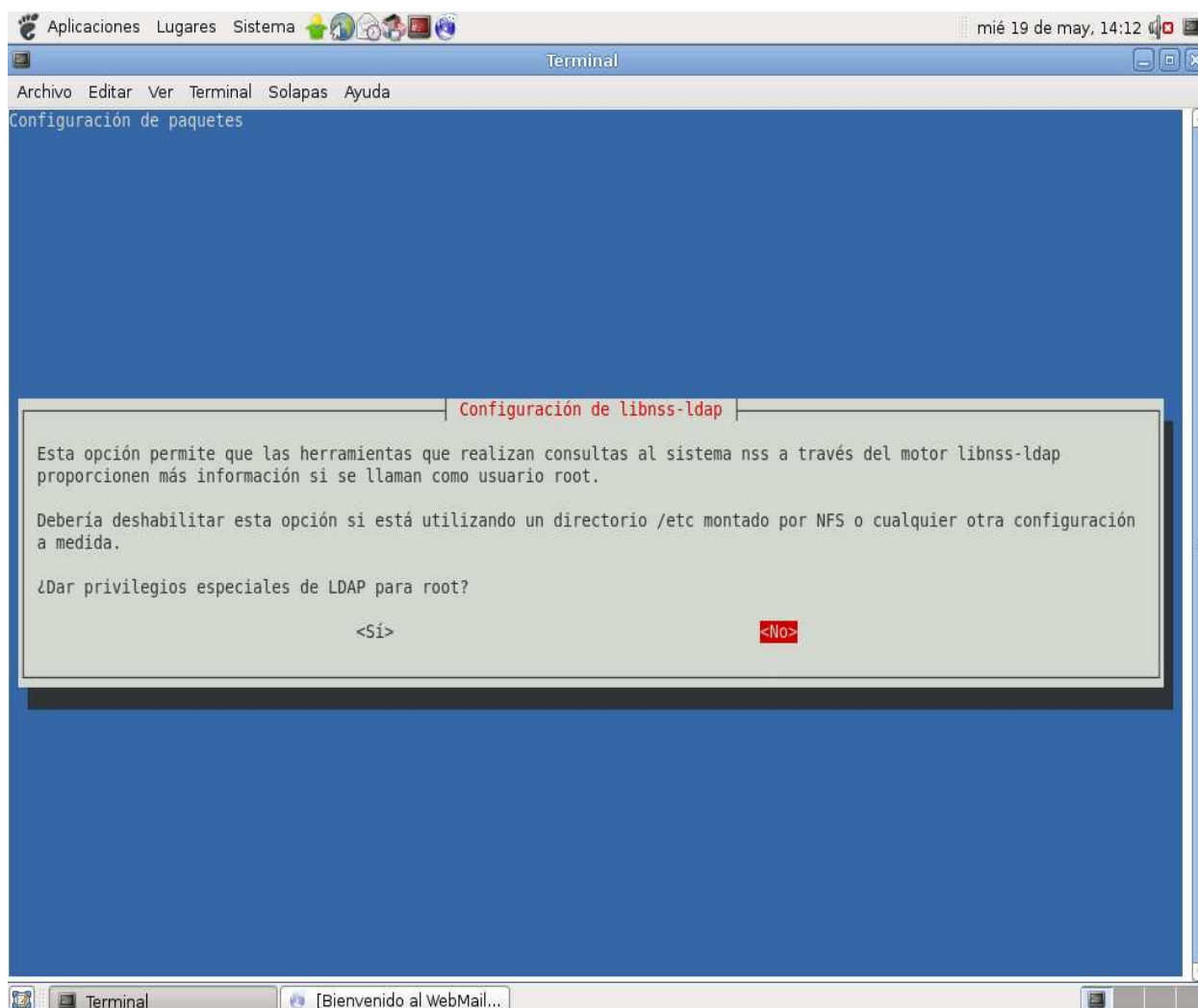
## Anexo 8 Versión de Ldap a Utilizar.



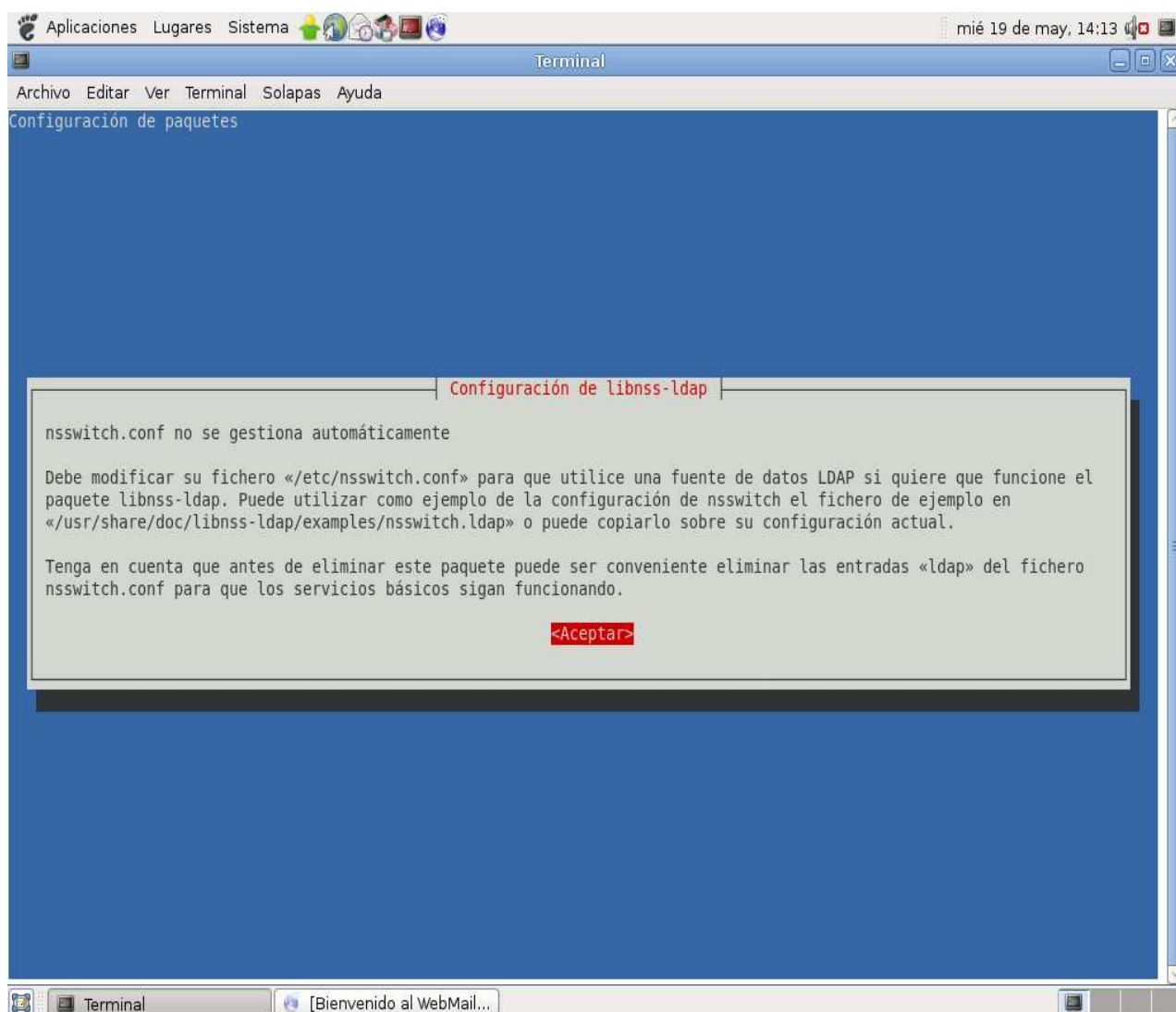
## Anexo 9 Permisos a lo usuarios a acceder a la base de datos



## Anexo 10 Permisos especiales de Ldap para root.



## Anexo 11 Fin de instalación de libnss-ldap.



## Anexo 12 Interfaz administrativa de Jxplorer.

The screenshot shows the Jxplorer application window. The left pane displays a tree view of the LDAP hierarchy, with the entry 'administrador Admini' selected under the 'people' group. The right pane shows the 'HTML View' of this entry, displaying a table of attributes and their values.

attribute type	value
cn	administrador Administrador
gosaProxyAcctFlags	
objectClass	gosaProxyAccount
objectClass	top
objectClass	person
objectClass	organizationalPerson
objectClass	inetOrgPerson
objectClass	gosaAccount
sn	Administrador
uid	administrador
givenName	administrador
gosaProxyQuota	5g
gosaProxyQuotaPeriod	m
gosaProxyWorkingStart	420
gosaProxyWorkingStop	1020
sambaBadPasswordCount	0
sambaBadPasswordTime	0
sambaLMPassword	758424888D2C9F9EAAD3B435B51404EE
sambaNTPassword	186CB09181E2C2ECAAC768C47C729904
sambaPwdLastSet	1271351843
userPassword	(non string data)
academicTitle	
audio	
businessCategory	
carLicense	
dateOfBirth	
departmentNumber	
description	
destinationIndicator	
displayName	
employeeNumber	
employeeType	
facsimileTelephoneNumber	
gender	
gosaDefaultLanguage	

At the bottom of the interface, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. The status bar at the bottom indicates 'Connected To 'ldap://10.26.0.248:389''.

## Anexo 13 Interfaz administrativa de PhpLdapAdmin.

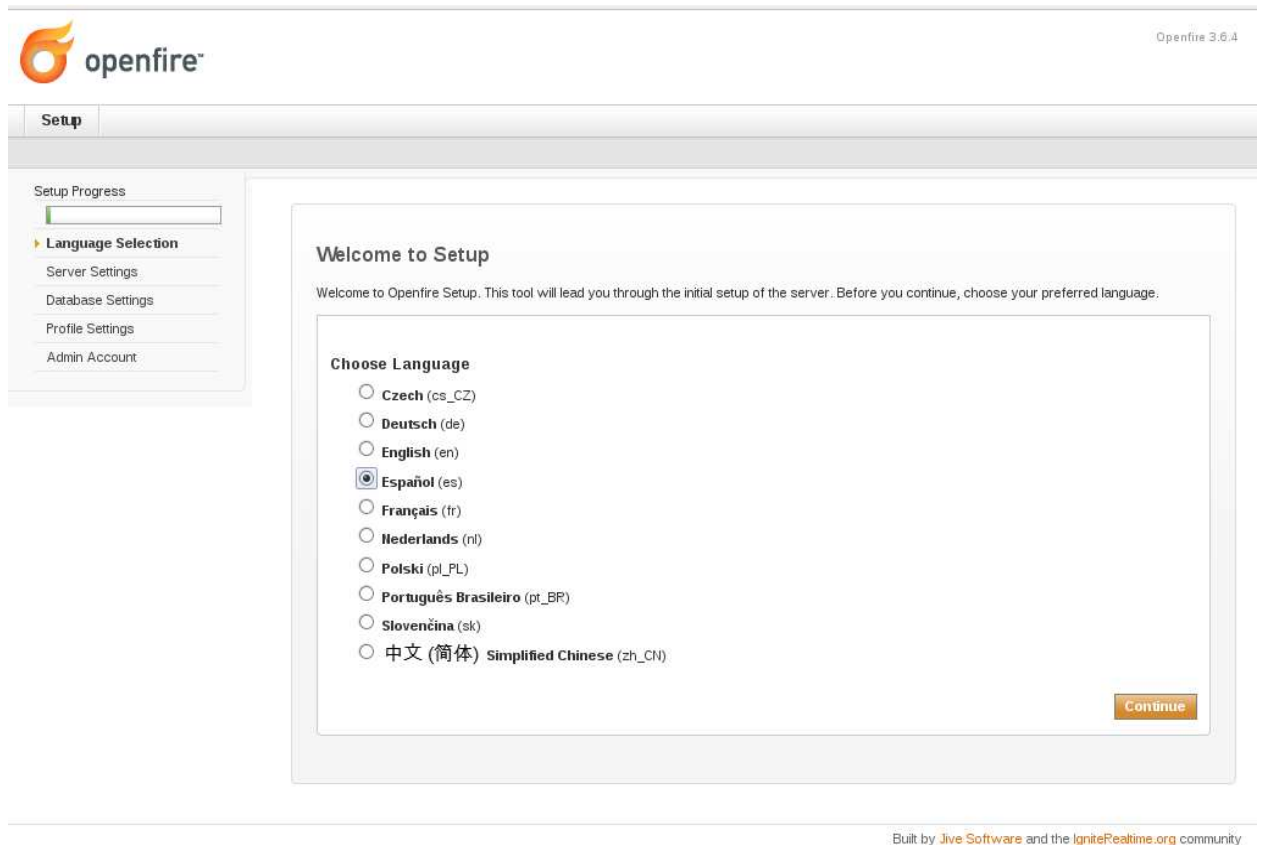




## Anexo 14 Interfaz administrativa de Gosa.



## Anexo 15 Selección del lenguaje del Openfire.



The screenshot shows the Openfire 3.6.4 Setup interface. On the left, a sidebar contains a 'Setup Progress' bar and a list of steps: 'Language Selection' (highlighted), 'Server Settings', 'Database Settings', 'Profile Settings', and 'Admin Account'. The main content area is titled 'Welcome to Setup' and includes a welcome message: 'Welcome to Openfire Setup. This tool will lead you through the initial setup of the server. Before you continue, choose your preferred language.' Below this, a 'Choose Language' section lists several options with radio buttons: Czech (cs\_CZ), Deutsch (de), English (en), Español (es) (selected), Français (fr), Nederlands (nl), Polski (pl\_PL), Português Brasileiro (pt\_BR), Slovenčina (sk), and 中文 (简体) Simplified Chinese (zh\_CN). A 'Continue' button is located at the bottom right of the language selection area. At the bottom of the page, a footer states: 'Built by [Jive Software](#) and the [IgniteRealtime.org](#) community.'

Openfire 3.6.4

Setup

Setup Progress

Language Selection

Server Settings

Database Settings

Profile Settings

Admin Account

### Welcome to Setup

Welcome to Openfire Setup. This tool will lead you through the initial setup of the server. Before you continue, choose your preferred language.

#### Choose Language

- ☐ Czech (cs\_CZ)
- ☐ Deutsch (de)
- ☐ English (en)
- ☒ Español (es)
- ☐ Français (fr)
- ☐ Nederlands (nl)
- ☐ Polski (pl\_PL)
- ☐ Português Brasileiro (pt\_BR)
- ☐ Slovenčina (sk)
- ☐ 中文 (简体) Simplified Chinese (zh\_CN)

Continue

Built by [Jive Software](#) and the [IgniteRealtime.org](#) community.

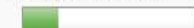
## Anexo 16 Especificación del domino y puertos.



Openfire 3.6.4

### Configuración

Progreso de la instalación



✓ Selección de idioma

✚ Configuración del servidor

Configuración de la fuente de datos

Configuración del Perfil

Cuenta de administrador

### Configuración del Servidor

A continuación se muestra la configuración del servidor. Nota: el valor sugerido para el dominio está basado en la configuración de la red en esta máquina.

Dominio:	<input type="text" value="idapservet"/>	?
Puerto de la Consola de Administración:	<input type="text" value="9090"/>	?
Puerto de la Consola de Administración Segura:	<input type="text" value="9091"/>	?

Continuar

Built by [Jive Software](#) and the [IgniteRealtime.org](#) community

## Anexo 17 Configuración de la fuente de datos.

Openfire<sup>™</sup>

Openfire 3.6.4

Configuración

Progreso de la Instalación

- ✓ Selección de idioma
- ✓ Configuración del servidor
- ✚ Configuración de la fuente de datos
- Configuración del Perfil
- Cuenta de administrador

### Configuración de la fuente de datos

Elja como quiere conectarse a la base da datos Openfire...


☐ **Conexión Estándard**  
Usa una base de datos externa con el pool de conexiones interno.

☒ **Base de datos interna**  
Usa una base de datos interna (HSQLDB). Esta opción no requiere la configuración de una base de datos externa y permite poner al servidor en producción rápidamente. Sin embargo dicha base de datos no se desempeña tan bien como una base de datos externa.

Continuar

Built by [Jive Software](#) and the [IgniteRealtime.org](#) community

## Anexo 18 Tipo de servidor a utilizar.

 Openfire 3.6.4

Configuración

Progreso de la Instalación

✓ Selección de idioma

✓ Configuración del servidor

✓ Configuración de la fuente de datos

✚ Configuración del Perfil

Cuenta de administrador

### Seteos de Perfil

Seleccione el sistema de usuarios y grupos a utilizar en Openfire.

☐ **Por defecto**  
Almacenar usuarios y grupos en la base de datos de Openfire. Esta es la mejor opción para instalaciones simples.


☒ **Servidor de Directorio (LDAP)**  
Integrar con un servidor de directorio como ser Active Directory o OpenLDAP utilizando el protocolo LDAP. Usuarios y grupos van a ser almacenados en el directorio y tratados como de sólo-lectura.

☐ **Integración con Clearspace**  
Integrar con una instalación existente de Clearspace. Usuarios y Grupos van a ser leídos directamente desde Clearspace. Clearspace sera utilizado para autenticar a los usuarios

Continuar

Built by [Jive Software](#) and the [IgniteRealttime.org](#) community

## Anexo 19 Seteos de conexión.

Openfire™

Openfire 3.6.4

Configuración

Progreso de la Instalación

✓ Selección de idioma

✓ Configuración del servidor

✓ Configuración de la fuente de datos

➤ Configuración del Perfil

Cuenta de administrador

### Seteos de Perfil: Seteos de Conexión

1. Seteos de Conexión

2. Mapeos de Usuarios

3. Mapeos de Grupos

#### Paso 1 de 3: Seteos de Conexión

Configurar seteos de conexión para su servidor LDAP. Todos los campos son requeridos; si desea información adicional sobre un campo lleve el ratón sobre el icono de ayuda correspondiente.

**Servidor LDAP**

Tipo de Servidor:

Servidor:  Puerto:

DN Base:

**Autenticación:**

DN del Administrador:

Clave:

[Seteos Avanzados](#)

Testear Seteos

Salvar & Continuar

## Anexo 20 Mapeo de usuarios.

Openfire 3.6.4

Configuración

Progreso de la Instalación

- ✓ Selección de idioma
- ✓ Configuración del servidor
- ✓ Configuración de la fuente de datos
- ✚ Configuración del Perfil
- Cuenta de administrador

### Seteos de Perfil: Mapeos de Usuarios

1. Seteos de Conexión   2. Mapeos de Usuarios   3. Mapeos de Grupos

#### Paso 2 de 3: Mapeos de Usuarios

Configurar la manera en que Openfire encuentra y carga usuarios del servidor LDAP. Si necesita mayor información sobre un campo, lleve el ratón al icono de ayuda correspondiente.

**Mapeos de Usuarios**

Campo de nombre de usuario:  ?

[Seteos Avanzados](#)


**Perfil de Usuario (vCard)**

Complete el siguiente formulario para indicar el mapeo entre los campos del servidor LDAP y el perfil de usuario. Campos no completados serán ignorados. Valores entre {} serán reemplazados por el contenido encontrado en el servidor LDAP.

☐ Almacenar avatar en la base de datos si no existe en LDAP

Campo del Perfil	Valor
Nombre	<input data-bbox="900 1176 1177 1205" type="text" value="{cn}"/>
Email	<input data-bbox="900 1216 1177 1245" type="text" value="{mail}"/>
Nombre Completo	<input data-bbox="900 1279 1177 1308" type="text" value="{displayName}"/>
Alias	<input data-bbox="900 1319 1177 1348" type="text" value="{uid}"/>
Fecha de Nacimiento	<input data-bbox="900 1359 1177 1388" type="text"/>
Foto/Avatar	<input data-bbox="900 1400 1177 1429" type="text" value="{jpegPhoto}"/>
Personal	<input data-bbox="900 1440 1177 1469" type="text"/>

## Anexo 21 Mapeo de grupos.

 Openfire 3.6.4

Configuración

Progreso de la Instalación

✓ Selección de idioma

✓ Configuración del servidor

✓ Configuración de la fuente de datos

✚ Configuración del Perfil

Cuenta de administrador

### Seteos de Perfil: Mapeos de Grupos

1. Seteos de Conexión

2. Mapeos de Usuarios

3. Mapeos de Grupos

#### Paso 3 de 3: Mapeos de Grupos

Configurar la manera que Openfire busca y carga grupos de su servidor LDAP. Si necesita mayor información sobre un campo, lleve el ratón al icono de ayuda correspondiente.

**Mapeos de Grupos**  
Campo del Grupo:  ?  
Campo del Miembro:  ?  
Campo de Descripción:  ?  
[▶ Seteos Avanzados](#)

Testear Seteos

Salvar & Continuar

Built by [Jive Software](#) and the [IgniteRealtime.org](#) community



## Anexo 22 Cuenta de administración de Openfire.

The screenshot displays the Openfire 3.6.4 administration web interface. The top left features the Openfire logo and version number. A navigation bar at the top contains the 'Configuración' (Configuration) tab. On the left side, a sidebar shows the 'Progreso de la Instalación' (Installation Progress) with a green progress bar and a list of steps: 'Selección de idioma' (Language Selection), 'Configuración del servidor' (Server Configuration), 'Configuración de la fuente de datos' (Data Source Configuration), 'Configuración del Perfil' (Profile Configuration), and 'Cuenta de administrador' (Administrator Account), which is currently selected and highlighted with an orange arrow. The main content area is titled 'Cuenta del Administrador' and includes the instruction: 'Seleccione uno o más usuarios de su directorio LDAP para ser administradores de Openfire ingresando sus nombres de usuarios.' (Select one or more users from your LDAP directory to be Openfire administrators by entering their usernames). Below this, there is a form with a label 'Agregar Administrador:' followed by a text input field and an 'Agregar' (Add) button. A table below the form lists the selected administrators. The table has columns for 'Administrador' (Administrator), 'Testear' (Test), and 'Eliminar' (Remove). One administrator, 'administrador', is listed. To the right of the name is a small icon and a checkbox. Below the checkbox is a 'Remove' button. At the bottom right of the table area is a 'Continuar' (Continue) button. The footer of the page states: 'Built by [Jive Software](#) and the [IgniteRealtime.org](#) community'.

Openfire 3.6.4

Configuración

Progreso de la Instalación

- ✓ Selección de idioma
- ✓ Configuración del servidor
- ✓ Configuración de la fuente de datos
- ✓ Configuración del Perfil
- ▶ Cuenta de administrador

### Cuenta del Administrador

Seleccione uno o más usuarios de su directorio LDAP para ser administradores de Openfire ingresando sus nombres de usuarios.

Agregar Administrador:

Administrador	Testear	Eliminar
administrador		<input type="checkbox"/>
		<input type="button" value="Remove"/>

Built by [Jive Software](#) and the [IgniteRealtime.org](#) community

## Anexo 23 Fin de la instalación.



## Anexo 24 Consola de administración.

---



## Anexo 25 Encuesta aplicada a expertos.

Estimado(a) compañero(a), con motivo de obtener su valoración del sistema informático encargado de la integración de las cuentas de usuarios en el Nodo Central UHo se realiza la presente encuesta. Si está de acuerdo en colaborar se le pide leer detenidamente las preguntas y responder con honestidad. Su opinión vale mucho para la conclusión de este trabajo, gracias de antemano por su ayuda.

Las categorías propuestas son las siguientes:

MA – Muy adecuado(a)

BA – Bastante adecuado(a)

A – Adecuado(a)

PA – Poco adecuado(a)

NA – No adecuado(a)

1. Marque con una X la categoría que considere adecuada a cada aspecto:

Aspectos a consultar	MA	BA	A	PA	NA
¿Cómo valora la interfaz gráfica del sistema?					
¿Cómo valora la forma en que el sistema integra las cuentas de usuarios?					
¿Cómo valora la velocidad y rendimiento del sistema?					
¿Cómo valora la utilidad de la implantación del sistema?					
¿Cómo valora en general el sistema?					

2. ¿Cuál es el mayor problema que usted observa en esta aplicación?

---

---

---

3. ¿Considera algún aspecto que debe mejorarse en el proceso de integración de cuentas de usuario?

---

---

---

4. Cite alguna idea que crea pertinente a esta investigación y que no haya sido abordada en la encuesta.

---

---

---

---

## Anexo 26 Resultados de la encuesta aplicada mediante el empleo del Método Delphi.

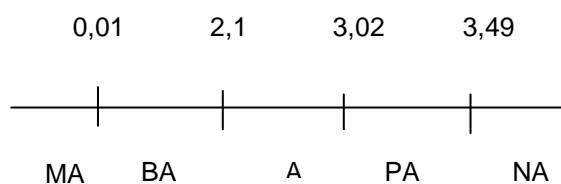
Sobre el modelo de actuación						
Tabla de frecuencia absoluta						
Aspectos a consultar	MA	BA	A	PA	NA	Total
¿Cómo valora la interfaz gráfica del sistema?	2	8	5	5	0	20
¿Cómo valora la forma en que el sistema integra las cuentas de usuarios?	10	8	2	0	0	20
¿Cómo valora la velocidad y rendimiento del sistema?	15	5	0	0	0	20
¿Cómo valora la utilidad de la implantación del sistema?	12	8	0	0	0	20
¿Cómo valora en general el sistema?	9	7	4	0	0	20

Tabla de frecuencia absoluta acumulada					
Aspectos a consultar	MA	BA	A	PA	NA
¿Cómo valora la interfaz gráfica del sistema?	2	10	15	20	20
¿Cómo valora la forma en que el sistema integra las cuentas de usuarios?	10	18	20	20	20
¿Cómo valora la velocidad y rendimiento del sistema?	15	20	20	20	20
¿Cómo valora la utilidad de la implantación del sistema?	12	20	20	20	20
¿Cómo valora en general el sistema?	9	16	20	20	20

Tabla del inverso de la frecuencia absoluta acumulada				
Aspectos a consultar	MA	BA	A	PA
¿Cómo valora la interfaz gráfica del sistema?	0.1	0.5	0.75	1
¿Cómo valora la forma en que el sistema integra las cuentas de usuarios?	0.5	0.9	1	1
¿Cómo valora la velocidad y rendimiento del sistema?	0.75	1	1	1
¿Cómo valora la utilidad de la implantación del sistema?	0.6	1	1	1
¿Cómo valora en general el sistema?	0.45	0.8	1	1



Tabla de determinación de los puntos de corte							
Aspectos a consultar	MA	BA	A	PA	Suma	Promedio	N - Prom.
¿Cómo valora la interfaz gráfica del sistema?	-1.28	0	0.67	3.49	2.88	0.72	1.43
¿Cómo valora la forma en que el sistema respalda los datos?	0	1.28	3.49	3.49	8.26	2.07	0.08
¿Cómo valora la velocidad y rendimiento del sistema?	0.67	3.49	3.49	3.49	11.14	2.79	-0.64
¿Cómo valora la utilidad de la implantación del sistema?	0.25	3.49	3.49	3.49	10.72	2.68	-0.53
¿Cómo valora en general el sistema?	-0.13	0.84	3.49	3.49	7.69	1.92	0.23
Suma	0.03	12.59	18.12	20.94	51.68		
Puntos de corte	0.01	2.1	3.02	3.49	8.61	2.15	= N (Prom. Gen.)



Conclusiones generales					
Fases y momentos	MA	BA	A	PA	NA
¿Cómo valora la interfaz gráfica del sistema?	-	Si	-	-	-
¿Cómo valora la forma en que el sistema integra las cuentas de usuario?	-	Si	-	-	-
¿Cómo valora la velocidad y rendimiento del sistema?	Si	-	-	-	-
¿Cómo valora la utilidad de la implantación del sistema?	Si	-	-	-	-
¿Cómo valora en general el sistema?	-	Si	-	-	-

