Análisis, Diseño e Implementación de un sistema de autenticación normalizado para la unificación de una red de servicios informáticos, aplicado a la Universidad Tecnológica de Bolívar.

YURANIS HENRIQUEZ NUÑEZ
JAIRO ENRIQUE SERRANO CASTAÑEDA
GILBERTO OROZCO LINERO

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR
PROGRAMA DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA

CARTAGENA DE INDIAS D.T y C

2006

Análisis, Diseño e Implementación de un sistema de autenticación normalizado para la unificación de una red de servicios informáticos, aplicado a la Universidad Tecnológica de Bolívar.

YURANIS HENRIQUEZ NUÑEZ
JAIRO ENRIQUE SERRANO CASTAÑEDA
GILBERTO OROZCO LINERO

TRABAJO DE GRADO

Director:
JUAN CARLOS MANTILLA GÓMEZ
Ingeniero de sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR
PROGRAMA DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA

CARTAGENA DE INDIAS D.T y C

2006

En este momento traigo a corazón a todas las personas que me han apoyado durante mi larga jornada de estudio.

Mi agradecimiento va en primer lugar a Dios que es mi fuente y fortaleza.

En segundo lugar a mis padres quienes me dieron uno de los mejores regalos, la educación y que siempre han permanecido firmes dando alegría y ánimos a mi vida.
También a mis hermanos, gracias por todos sus consejos, este en especial que comparto con ustedes:

"En la universidad no te rindas cuando vengan dificultades,
ten puesta tu mirada en Dios.
¿De donde vendrá tu socorro?
Tu socorro viene de Dios que hizo los cielos y la tierra.
Salmo 121,1-2"

Por ultimo al personal docente de sistemas de la UTB, quienes contribuyeron en la evolución de mi carrera e hicieron que cada día amara más mi profesión.
Y finalmente le doy gracias a mis compañeros con quienes compartí mis estudio.

A ti Jairo, gracias por luchar juntos, nos propusimos cumplir esta meta y lo logramos.

Yuranis Henriquez Nuñez

Gracias a DIOS por ser la fuerza que nos impulsa a cumplir nuestras metas.

Todo mi trabajo y esfuerzo se lo dedico a mis padres, hermanos y familiares que con su ayuda, cariño y comprensión siempre me apoyan en mi vida y proyectos.

Gracias a los profesores, amigos y compañeros con quienes compartí estos buenos años en la universidad.

Yury gracias por ser un significado más grande que la palabra amor en mi vida.

Jairo Enrique Serrano Castañeda

Este trabajo no se habría terminado, de no ser por el apoyo permanente que recibí de mis padres y hermanos; a mis amigos, quienes creyeron en mí y en lo posible que era terminar esta etapa de mi vida.

A mi novia, Wendy Solano, quien estuvo todo el tiempo susurrando a mi oído todo el apoyo, la fuerza y la motivación que necesitaba para alcanzar este objetivo y quien se ha convertido en mi sueño y logro más grande.

A Yury, Jairo y su familia, quienes como compañeros de trabajo tuvieron la paciencia, el entusiasmo y el amor para terminar este proyecto en nuestras vidas, me acogieron y me brindaron posada y estadía para lograr este fin.

Gracias por todo su amor y cariño.

Agradecimientos

Los autores de este trabajo expresan sus profundos agradecimientos por la colaboración y apoyo recibido de:

Docentes de la Universidad Tecnológica de Bolívar por compartir desinteresadamente sus conocimientos y enseñanzas, por ser guías en nuestro camino.

Los jurados del trabajo por sus valiosos comentarios y sugerencias, por su tiempo y preocupación en el desarrollo de esta tesis.

A nuestro director de tesis, Ingeniero Juan Carlos Mantilla Gómez, por su gran dedicación y excelentes consejos, los cuales nos permitieron concluir satisfactoriamente este proyecto.

Indice

Índice de Figuras

Índice de Tablas

1 DESCRIPCIÓN DEL PROYECTO

1.1 ANTECEDENTES

En la actualidad las computadoras están ineludiblemente presentes en la vida diaria de las personas, ya que controlan sistemas complejos tales como redes financieras, el transporte de personas, sistemas telefónicos, plantas eléctricas, entre otros.

Esta evolución de la tecnología, así como la búsqueda de nuevos y mejores métodos para prestar servicios, ha llegado al punto en que la participación humana es mínima, dejando así una gran cantidad de datos a disposición de las máquinas. Ejemplo de ello y el más utilizado es el Internet. Miles de millones de personas lo utilizan para acceder a información, comprar, recrearse, comunicarse, realizar negocios, etcétera.

Por todo esto actualmente es una necesidad básica que los servicios que la gente utiliza a través de Internet, y de las redes locales en las organizaciones empresariales, posean una serie de características como son la confidencialidad, la autenticación segura de la identidad, la integridad de los datos, el control de acceso y disponibilidad, que garanticen al usuario un buen nivel de administración de sus datos. Esto significa además, que el usuario pueda tener plena confianza en que sus datos confidenciales están completamente seguros, y solo pueden ser consultados o modificados por el. Y además que el servicio utilizado sea de fácil uso. Estas características se constituyen entonces en una prioridad dentro de las

consideraciones de diseño utilizadas por los desarrolladores.

De lo anterior se desprende entonces la necesidad de discutir temas como la usabilidad, la seguridad en la transferencia de datos, además de los métodos de identificación y autenticación de usuarios, utilizados en la actualidad por los diferentes servicios que se prestan a través de las redes, que resultan de utilidad para efectos de una implementación óptima tanto en lo relativo a la definición y requerimientos del sistema.

El propósito es entonces alcanzar la integración total de los datos entre los diferentes servicios informáticos de la Universidad. Implementando así un mejor sistema que facilite la identificación y autenticación de usuarios dentro de este.

1.2 EL PROBLEMA QUE CUBRE LA INVESTIGACIÓN

El diseño de todo sistema debe poseer una serie de características como son la claridad, la consistencia, la verificabilidad y la completitud, que en conjunto permiten conocer una visión general de lo que hace, de lo que los usuarios necesitan y del grado en que, como sistema, es una solución que facilita algún aspecto de la vida humana.

En el trabajo aquí propuesto se remplazará el sistema existente que posee muchas carencias; presenta problemas en sus servicios tales como la incoherencia o la multiplicidad en los nombres de los usuarios dependiendo si usa SAVIO, RAS (Remote Access Service) o el Correo electrónico y el no poder tener una clave de acceso unificada, a causa de que la bases de datos de sus usuarios no están integradas entre si, y/o no han sido desarrolladas de manera integrada, es decir con un diseño claro, estable y normalizado para el intercambio de información entre ellas.

Se carece de un sistema estándar de identificación y autenticación de usuarios para los servicios que se ofrecen, es decir, no existe un método estándar para el control y manejo de identificadores de usuario y contraseñas, razón por la cual cada uno de los sistemas de información efectúa la autenticación por separado. Lo que implica que el usuario debe aprender diferentes nombres de usuario y sus correspondientes contraseñas para poder acceder a cualquiera de los servicios.

No existe un método apropiado de configuración personalizada de los datos del usuario, es decir que para la edición de datos o corrección de los mismos, el usuario debe recurrir al administrador del servicio para hacer esos cambios, cuando lo correcto es que el administrador sea consultado por el usuario únicamente en casos excepcionales o de soporte.

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo General

Diseñar e implementar un modelo de sistema de autenticación que permita simplificar y unificar la administración de los datos de identidad (nombres de usuarios y claves), tanto para los usuarios finales como para administradores en algunos sistemas y servicios de red que presta la Universidad.

1.3.2 Objetivos Específicos

1. Formular un nuevo esquema de autenticación de los datos de identidad de los usuarios de los servicios de SAVIO, Mensajería Instantánea y Correo Electrónico en la Universidad Tecnológica de Bolívar.
2. Instalar y configurar un servidor de directorio para implementar el nuevo esquema de autenticación.
3. Desarrollar una interfaz de fácil uso para los usuarios.
4. Implementar una interfaz robusta y bien documentada para administradores del servidor de directorio.
5. Generar la documentación y manuales especificados en los productos a entregar.

1.4 RESULTADOS ESPERADOS

Al terminar el proyecto se disponen de los siguientes productos:

1. Servidor de Directorio LDAP, configurado y funcionando.

2. Integración de los servicios:

    - Correo entrante
    - Correo saliente
    - Servicio de mensajería Instantánea
    - SAVIO - Sistema de Aprendizaje Virtual Interactivo

3. Manual de integración de los servicios.

4. Manual de instalación y uso de LDAP

5. Manual de instalación y uso de la aplicación de cambio de contraseñas.

6. Manual de uso del directorio de correos, para usarse desde un cliente de escritorio cualquiera.

2 MARCO TEÓRICO

A continuación se exponen los conceptos claves para el buen entendimiento de los resultados de esta tesis y sus implicaciones con los servicios que la Universidad ofrece a su comunidad.

2.1 AUTENTICACIÓN

La acción o procedimiento de verificar la identidad de una persona es lo que se denomina autenticación; la cual tiene como objetivo permitirle a esa persona autorizada el acceso a un recurso físico, telemático o informático.
Los métodos de autenticación existentes hoy en día son muy variados. Una forma de clasificarlos es de acuerdo a su relación con el usuario. También están los métodos denominados biométricos. Aquellos se basan en datos conocidos por el usuario, es decir requieren que el usuario lleve la información de identificación y la confirme en un dispositivo destinado para el efecto. Estos se basan en rasgos físicos o en patrones de comportamiento.

2.1.1 Servicios de Autorización

En la Wikipedia se define que “La autorización se da normalmente en un contexto de autenticación previa. Se trata de un mecanismo que permite que el usuario pueda acceder a servicios o realizar distintas actividades conforme a su identidad.” de eso de trata este trabajo: permitir que los servicios informáticos de La Universidad, solo puedan usarse por personal relacionado directamente con ella y que además estén caracterizados por un acceso fácil y homogéneo.

2.1.2 Datos conocidos por el usuario

En esta categoría están las contraseñas usadas para el acceso a recursos informáticos, generalmente con un nombre de usuario asociado, y los PINs o NIPs (Número de Identificación Personal).

El principal problema de estos métodos de autenticación es que las claves, para ser seguras, deben ser complejas, y si son complejas, son difíciles de recordar para el usuario, quien fácilmente termina escribiendo las claves de acceso en post-it pegados en la CPU o en la pantalla del PC.
Para obviar estos problemas, se han creado sistemas de claves desechables, donde se le entrega al usuario una lista de claves, que se van usando una sola vez y de manera consecutiva. Obviamente, si otra persona obtiene dicha lista, puede lograr el acceso sin problema.

Por otra parte, una vez el usuario se autenticó en algún servicio, los datos que se transmiten por la red usualmente están desprotegidos a la merced de que cualquier cibernauta intercepte la comunicación y acceda sin autorización a ellos, que generalmente se consideran como de carácter personal y privados. En tal caso se requiere utilizar técnicas de Cifrado.

2.1.3 Políticas necesarias para el manejo de la información de usuarios

Plantear y establecer una política clara y efectiva para el tratamiento adecuado de la información personal es un derecho de todos y cada uno de las personas y usuarios de nuestra comunidad Universitaria, a quienes se les debe brindar medios y facilidades, para el manejo de sus cuentas de servicios y claves con el

fin de evitar la dificultad que supone llevar la cuenta de las diferentes claves que utiliza a diario. Por ello, con el cifrado, se pretende asegurar la confiabilidad de los datos mediante la designación y uso de una clave única por usuario para acceder a los servicios informáticos de la Institución.

2.1.4 Servicios de directorio LDAP (Lighweight Directory Access Protocol)

En el área del manejo de información ya se habla de distintas y variadas herramientas para la administración de volúmenes de datos. Archivos, manejadores de bases de datos y actualmente una herramienta que está siendo bastante implementada en empresas grandes y en diferentes tipos de aplicaciones, conocida como LDAP. (Lighweight Directory Access Protocol), que puede traducirse como Protocolo liviano (o ligero) de acceso a los Servicios de Directorio.

Una implementación LDAP en una empresa o una aplicación que necesite manejar volúmenes de datos es algo novedoso. Por que LDAP facilita el acceso de datos desde cualquier punto en el que se encuentre el servidor, además de ser una herramienta multiplataforma, es decir que soporta cualquier sistema operativo en el que se trabaje.

Los volúmenes de datos como direcciones de correo electrónico, datos de recursos humanos, claves públicas de seguridad, listas de contactos, y muchos más, son algunos rangos de datos que pueden ser trabajados por LDAP.

Un servidor LDAP provee de información a cualquier usuario que se encuentre en la misma empresa, en la misma ciudad, en el mismo país o en cualquier lugar que tenga acceso a este servidor sin tener que pasar a buscarla en otro lugar remoto.

Para las aplicaciones LDAP no se necesitan herramientas adicionales de base de datos ni programas de administración de datos, pues LDAP es una herramienta totalmente autónoma.

2.1.4.1 ¿Qué es LDAP?

Sus siglas en español se traducen como **Protocolo Ligero de Acceso a Directorio** y está basado en el estándar X.500 de ITU-T.

LDAP es una especie de un servidor de directorios, o de lo que se entiende por directorio, en donde se encuentran diferentes tipos de archivos o información ordenados de una manera jerárquica para facilitar el acceso a la misma.

Entonces puede surgir una pregunta: ¿es LDAP una base de datos? Así como una base de datos relacional, como las actualmente conocidas, MySQL, Oracle, DB2, Informix, entre otras, manejan inmensos volúmenes de información que pueden ser guardados, actualizados o eliminados, LDAP funciona como base de datos pero no es una base de datos relacional.

Para presentar un punto clave del uso de LDAP, se expondrán a continuación algunas de las ventajas que esta herramienta trae:

Una de las mejores ventajas de LDAP es que cualquier usuario de una empresa

puede acceder a ella desde cualquier plataforma, con cualquier número de programas, que actualmente se encuentran en crecimiento, que implementan el uso de LDAP o están disponibles con LDAP. Además en el uso de una implementación empresarial se puede personalizar LDAP para el uso de sus aplicaciones internas.

LDAP se ha hecho a un espacio muy importante en Internet gracias a que las aplicaciones y las diferentes plataformas que lo usan no necesitan preocuparse por el tipo de servidor en que se hospeda el directorio; esto le ha posibilitado ubicarse como una herramienta con un estatus estándar en Internet. Esto permite que los diseñadores de software no se preocupen por saber que tipo de servidor es aquel al que van a integrar la aplicación que se diseñe de manera remota, y además es aprovechable en distintas formas por que resulta de utilidad para cualquier cliente y no se requiere de un diseño individualizado por cada usuario, ya que para hacer la integración con una base de datos solo se necesita de la configuración del usuario con el servidor principal.

Existe además una ventaja en el aspecto económico, puesto que no se requiere de una licencia, ni pagar por cada conexión de software de manera individualizada. Esto es gracias a que LDAP es un programa de código abierto.

La mayoría de los servidores LDAP son relativamente simples de instalar, fácilmente mantenibles, y fáciles de optimizar.

Los servidores LDAP permiten replica de su información a través de métodos de envíos o recepción como lo hacen los manejadores de base de datos, lo que permite enviar datos a servidores remotos, o hacer réplicas de los mismos, incrementando la seguridad y personalización de las aplicaciones. Los métodos para hacer réplicas vienen incorporados con LDAP y su configuración es

relativamente fácil, a diferencia de los manejadores de base de datos en los que este trabajo puede ser mucho más complejo y costoso.

LDAP también integra una herramienta conocida como ACL (Access Control List) el cual se traduce como Lista de Control de Acceso, que permite delegar jerarquías o administrar el nivel de entrada de cada uno de los usuarios que tengan permiso en LDAP, lo que quiere decir que la autenticación o los permisos de los usuarios no es necesario administrarlos a través de la aplicación final, y por lo tanto el desarrollador ahorra muchas líneas de código y además puede definir para cada usuario cuáles son los datos a los que tiene acceso de lectura, cuales puede modificar y cuales no, a qué servidor tiene acceso y otros tipos de registros que desee modificar.

LDAP es particularmente utilizable cuando se va a almacenar información que va a ser leída muchas veces en el día y desde muchas localidades diferentes a las locales, pero que a la vez no sea actualizada muy frecuentemente.

Los servidores LDAP trabajan a un menor rendimiento que los manejadores de Bases de Datos relacionales cuando se hacen actualizaciones seguidas de la información que administran.

Por ejemplo, LDAP en una empresa permite manejar con una eficiencia relativamente alta, información como el directorio telefónico interno, las cuentas de correo de cada uno de los empleados o información estática de los clientes, pero LDAP no se puede contemplar como una base de datos para un sitio de comercio electrónico de alto volumen.

Para escoger entre LDAP y una base de datos relacional se deben tener en cuenta los siguientes puntos de vista:

- Disponer de los datos en cualquiera de las plataformas existentes.
- El número de aplicaciones o usuarios que accedan a esta información la consulten de manera regular y constante.
- El tiempo medio de actualización de los datos se realiza una vez al día o por lo menos una vez cada medio día.
- Tiene sentido almacenar todos los datos en una base de datos plana y no en una base de datos relacional, es decir, que los datos de un ítem se guarden en un solo registro.

A este último ítem se le debe poner más atención. El acceso de la información o la relación que exista entre todos los datos también ayudará a escoger la herramienta más eficaz para la aplicación en la que se está pensando, pero si se pueden ver esos datos ordenados y fáciles de consultar en una agenda personal entonces LDAP es la herramienta más adecuada.

2.1.4.2 Implementaciones

2.1.4.2.1 OpenLDAP

Lo ideal al tener un servidor de directorio es que al hacer una petición en él, la respuesta a esta se produzca en forma rápida y eficiente, independientemente de que se tenga un gran volumen de datos o información en el directorio.

OpenLDAP permite contener los datos de los usuarios y realizar la autenticación

en máquinas clientes de forma centralizada, soportando así múltiples esquemas (usuarios, claves) y de esta forma las peticiones que se han de resolver, respondan rápidamente y no tenga muchas actualizaciones.

Es por ello que a pesar de existir numerosas implementaciones de LDAP, OpenLDAP es una buena alternativa y es pieza esencial para la definición del diseño administrativo de los servicios de red unificados de la Universidad Tecnológica de Bolívar.

El servicio de directorio es totalmente libre y además provee una serie de librerías y utilidades que aportan una solución integral al manejo del directorio, facilitando así que se compartan información de manera más segura en la red y que se proteja la autenticación del usuario.

2.1.4.2.2 Novell eDirectory

Este tipo de directorio, a diferencia del anterior, básicamente tiende a tener una base de datos jerárquica y orientada a objeto; esto quiere decir que un único servidor (servidor padre) llama a otros servidores (servidores hijos) y de esta forma se sincronizan y acceden a los recursos en la red.

En otras palabras puede decirse que al utilizar este servicio de directorio, los servidores, sin importar cuantos estos sean (En cantidad), trabajan en herencia.

Así que para manejar los controles tanto de identidades como de acceso de los usuarios, estos primero deben conceder un permiso a una rama del árbol, y este permiso lo deben heredar de manera automática todos los usuarios y una vez identificados los usuarios cuando estos se conectan, se determinan dónde están,

qué necesitan, de forma que estos puedan acceder a la red en cualquier lugar y momento.

2.1.4.2.3 RedHat Directory Server

Otro de los servidores basado en LDAP es el RedHat, que centraliza configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas para la infraestructura de manejo de identidad, así como información de control de acceso dentro de un sistema operativo independiente de la plataforma y así simplifica el manejo de usuarios y elimina la redundancia de datos.

RedHat Directory Server está basado en la tecnología Netscape Security Solutions-Iplanet, y se le puede considerar como una buena alternativa para gestionar información de los usuarios, ya que es un servidor de directorio alternativo de bajo coste y estandarizado.

2.1.4.2.4 Active Directory

El directorio activo (Active Directory) almacena la información (Ya sea información tanto de usuarios, recursos de red, políticas de seguridad, configuración, asignación de permisos, etcétera) de manera centralizada, y actúa como una base de datos que permite que exista sincronización entre distintos servidores .

El trabajo del Directorio Activo consiste en proporcionar un directorio de objetos específicos para el sistema operativo de red. De esta forma puede así manejar no sólo los usuarios y sus propiedades, sino también otra gran cantidad de

prestaciones específicas (como pueden ser los volúmenes GPO - objetos de directiva de grupos, infraestructuras de claves públicas.)

Por las razones anteriores, el Directorio Activo se considera uno de los mas complejos en cuanto a administración y control de acceso a los recursos de la red.

Ejemplo clave de este directorio es el que implementa Windows, en especial en la versión 2003 que se sirve de este esquema para la autenticación de los usuarios cuando inician sesión en la red.

2.2 SERVICIOS DE CORREO

Es un sistema de envío y recepción de mensajes ampliamente utilizado actualmente, que ocasiona gran porcentaje del tráfico de Internet. Para hacer uso del correo electrónico es necesario disponga de algún proveedor de este servicio. Hay servidores gratuitos y pagos ampliamente conocidos por la comunidad de usuarios de Internet.

Uno de los servicios que La universidad presta a su comunidad es el de correo electrónico. Todo el personal que labora en ella puede disponer de una cuenta de correo en los servidores institucionales. Se manejan dos (2) convenciones para crear los nombres de usuarios: en el caso de los alumnos el identificador de usuario será la letra “c” seguida de los siete dígitos del código del estudiante y si es empleado, docente o administrativo su nombre de usuario será un subconjunto compuesto de las letras de su primer nombre y apellido. Dando como resultado, por ejemplo, para un estudiante “c0105001@unitecnologica.edu.co” ó administrativo “jperez@unitecnologica.edu.co”.

En el momento en que estos usuarios interactúan con el servicio, se debe tener en cuenta que intercambiaran información con 2 tipos de servidores diferentes, uno de correo saliente llamado (MTA1) y el otro, el servidor de correo entrante (MDA2). Teniendo en cuenta lo anterior, se configuraron 2 servicios diferentes:

1. MTA, siendo el servidor Postfix el encargado de hacer este trabajo.
2. MDA, Courier es el servidor instalado para tal fin.

Los usuarios de este servicio a su vez, también necesitan un cliente o programa para enviar o recibir correo, estos se clasifican en dos:

1. Programas de escritorio: Son aquellos programa de que se sirve el usuario descargar o enviar los correos del servidor de correo, desde su PC.
2. Webmail: No se necesita tener un programa de escritorio para interactuar con el servidor de correo de La Universidad gracias al uso de un portal web especializado en la interacción con este tipo de servicios, desde el que se pueden leer los mensajes , consultar los mensajes no descargados desde el cliente de escritorio o enviar mensajes a cualquier destinatario.

En los anexos se hace una explicación de estos servidores y clientes.

2.3 SERVICIO DE ACCESO TELEFONICO A REDES

1 MTA: Mail Transfer Agent, en español traduce: Agente de transporte de correo

2 MDA: Mail Delivery Agent, en español traduce: Agente de entrega de correo

El servicio denominado RAS “Remote Access Services” ó su significado en español “Servicio de Acceso Remoto”, es una combinación de Hardware (modems y lineas telefónicas) y software (base de datos de usuarios) que le permiten a determinados usuarios conectarse a Internet por las redes de La Universidad utilizando una línea telefónica conmutada. Este era uno de los servicios más usados en La Universidad, en el pasado reciente. Sin embargo, actualmente el acceso telefónico a Internet no se presta a los usuarios nuevos de la comunidad Universitaria, por la limitada capacidad técnica y costo de la infraestructura que se utiliza para prestarlo, y se prevé que entrara en desuso en un futuro relativamente cercano.

Aunque el servicio de RAS está incluido como uno de los servicios a integrar dentro de los objetivos del presente proyecto, considerando su presumiblemente corta vida futura, los autores tomaron la decisión, concertada con el Director de integrar un servicio institucional de mensajería instantánea en lugar de aquel.

2.4 SERVICIOS DE MENSAJERIA INSTANTÁNEA

Este servicio básicamente consiste en que 2 personas o más, usando una red, se puedan comunicar entre si con la ayuda de un software especializado y un protocolo definido, pudiendo así, conversar principalmente por medio del mensajes de texto escrito, aunque recientemente es creciente la tendencia de integrar este servicio con el de Voz sobre IP.

Este es un servicio nuevo que prestara La Universidad, con el fin de hacer posibles mayores niveles de integración de la comunidad gracias la posibilidad que sus miembros tienen de estar “en linea”. Ademas de que hace posible un

ahorro importante en el uso del ancho de banda institucional porque no necesita salir a Internet para lograr esta comunicación, a diferencia de lo que ocurre con con otros servicios de mensajería instantánea como gtalk, ICQ de Mirabilis, o MSN de Microsoft.

Para poner en marcha este servidor se requiere contar con un protocolo y servidores preferentemente basados en software libre.

Esto se hace posible con una facilidad relativamente alta, gracias a que la "Jabber Software Foundation"[3] desarrolló XMPP[4]., protocolo principal en el que está basada la tecnología Jabber. Actualmente está conformada por miles de servidores descentralizados que en teoría tienen millones de usuarios y gigantes como Google la usan para su cliente de mensajería. Esto se traduce en que, desde las cuentas de mensajería de La Universidad, se puede conversar tranquilamente con algún contacto que use alguna cuenta de Google o de cualquier otro servidor público. Esto refuerza la idea cada vez más popular de que el software libre y los estándares abiertos proveen nuevas posibilidades muy interesantes para los desarrolladores.

2.5 SERVICIOS DE AULAS VIRTUALES – SAVIO

SAVIO es el Sistema de Aprendizaje Virtual Interactivo de La Universidad

3 Jabber Software Foundation: Fundación encargada del desarrollo y mantemiento del protocolo jabber para mensajería instantanea, más informacion en http://www.jabber.org

4 XMPP: "Extensible Messaging and Presence Protocol" protocolo abierto y extensible basado en XML, desarrollado como evolución de jabber.

Tecnológica de Bolívar. Este servicio es el encargado de prestar soporte a las aulas presenciales y virtuales que se utilizan para apoyo de los procesos académicos.. Este servicio también esta completamente integrado al Sistema de Autenticación Normalizado.

La versión 5 de SAVIO estará preparada para identificar a los usuarios: alumnos, docentes y directivos directamente con el sistema de autenticación normalizado de La Universidad.

3 LA SOLUCIÓN

Actualmente cada uno de los servicios informáticos de la Universidad Tecnológica de Bolívar dispone de un sistema de autenticación diferente, el servidor de correo entrante utiliza un sistema de autenticación por la clave asignada a los usuarios del sistema, SAVIO, RAS y por lo general cualquier otro servicio generado en la Web, utiliza MySQL para almacenar los datos.

El Sistema de Autenticación Normalizado, de ahora en adelante llamado “SAN”, además de unificar la administración de los datos de identidad de los usuarios, facilitara la integración de nuevos servicios en la red institucional mejorando así la eficiencia y la calidad de los servicios.

3.1 ANÁLISIS DE REQUISITOS DEL SISTEMA ACTUAL

Para que el sistema cumpla con los objetivos planteados, es necesario saber por parte de los administradores de estos servicios como es el funcionamiento interno y mantenimiento del sistema actual, recopilando por medio de un par de entrevistas la información requerida, para así acordar los últimos detalles sobre el nuevo sistema.

3.1.1 ENTREVISTA ADMINISTRADOR DE HARDWARE Y TECNOLOGÍA

Administrador: ALFREDO FIGUEROA

Entrevistador - ¿Como es la administración de usuarios que acceden a los servicios del sistema?

Administrador - Los usuarios que acceden a nuestros servicios deben tener como primer requisito estar relacionado con la universidad de forma activa, es decir; estos usuarios deben ser estudiantes activos, docentes de cátedra o de tiempo completo, o personal administrativo de la universidad.

Para hacer uso de los servicios, estos deben asistir personalmente a las oficinas de sistemas y diligenciar un formulario, que en un lapso de 24 horas sera procesado por algún auxiliar de sistema que lo adicionara en cada una de las bases de datos de los servicios(Servidor de correo, Acceso telefónico).

Solo hay una restricción al momento de crear una cuenta de correo basándose en los 3 tipos de usuarios que manejan el servicio: si es un alumno se le ofrece 9 megabytes para almacenar los correos, si es un docente este tendrá 15 megabytes y si es un administrativo 25. Adicionalmente se maneja un tipo de usuarios especial , que tienen una cuenta sin límite de espacio..

Por otra parte, si el usuario necesita acceder a las aulas virtuales deberá también asistir personalmente a las oficinas de SAVIO para gestionar los datos que le permitan su acceso.

Entrevistador - ¿Como es el tratamiento de los datos privados de los usuarios? en especial el tratamiento y almacenamiento de las contraseñas de los usuarios en las bases de datos de los servidores?

Administrador - Después de que el usuario diligencia el formatos de solicitud para su creación, esta contraseña es leída por el auxiliar y digitada directamente en un campo de texto plano en el formulario de registro del servidor. El formulario original en papel es destruido.

Entrevistador - ¿Como es el procedimiento para que un usuario cambie su clave?

Administrador - No existe un procedimiento para que el usuario cambie sus datos manualmente; este debe presentar una solicitud al departamento de sistema, en donde un auxiliar procesara la solicitud en un lapso de 24 horas.

El único servicio en donde el usuario puede cambiar su clave de forma manual , es en el servicio de webmail pero esta clave solo funcionara para el servicio de recibir correo.

Entrevistador - ¿Cual es el procedimiento para el retiro de usuarios del sistema?

Administrador - No existe ningún procedimiento definido donde se defina como se deben retirar los usuarios inactivos del sistema. Aunque cada cierto tiempo de hace una eliminación de usuarios de todos los servicios antes de iniciar el semestre, en caso de ser un docente o administrativo, por conocimiento del retiro de este usuario se elimina.

Entrevistador - ¿Como están conformadas las comunicaciones de la universidad?

Administrador - Comunicación dedicada entre las sedes a 1Mbit, Acceso dedicado a Internet por ADSL en la sede de Manga de 512kbs, Acceso dedicado a Internet por fibra óptica a 1,5Mbits en la sede de ternera., Acceso Telefónico RAS - rack de 32 módem configurados en PBX

Entrevistador - ¿Que nivel de seguridad tiene el acceso a los servidores?

Administrador - El acceso a los servicios es mediante el usuario y la clave que cada usuario tiene. Se restringe completamente el acceso a personal no autorizado al espacio físico de las salas de servidores, a las cuales sólo se puede ingresar acompañado del encargado de Hardware y Tecnología o del Jefe del Departamento.

Entrevistador - ¿Que documentación disponible existe sobre el montaje de los servicios ofrecidos?

Administrador - Disponemos de la documentación libre que se encuentra en los portales de las aplicaciones libres que usamos (Apache, MySQL, Postfix, imapd). no hay documentación generada sobre este tema de parte del departamento de sistemas.

Entrevistador - ¿Cuales son las características de las maquinas que cubren estos servicios?

Administrador - El servidor de WEB es un Compaq ML 350 con 2 discos duros de 18 GB, memoria ram de 512 MB, procesador: 933 Mhz y sistema operativo SuSE 9,3. El servidor de correo es un IBM Xseries 232, con 2 discos duros de 18.2 GB, memoria de 2048 MB, procesador de 2,6 GHz y sistema operativo SuSE

9.3. El servidor de acceso telefónico es un Compaq ML 330 con 1 disco duro de 9 GB, memoria de 128 MB, procesador: 1,1 Ghz y sistema operativo RedHat Linux 8.

Entrevistador - ¿Cual es la frecuencia con la que se realizan procedimientos de Backups de los datos de usuario en los servicios?

Administrador - No se realiza con frecuencia copias de seguridad de los correos, pero si, cada vez que hay una actualización importante de usuarios se hace un backup.

Entrevistador - ¿Que software de antivirus tiene la universidad para filtrar correos?

Administrador - Computer Asociates e-Trust. con licencia de por vida y actualizaciones constantes.

Entrevistador - ¿De que software dispone la universidad para filtrar correos indeseados o SPAM?

Administrador - La universidad no cuenta con ningún software anti-SPAM en sus servidores.

Entrevistador - ¿Para estos servicios se dispone de alguna licencia de software?

Administrador - Gracias a que existe una excelente calidad en el Software Libre usado en los servidores no necesitamos grandes inversiones de capital para el mantemiento de estos equipos. Usamos una gran variedad de servidores entre los cuales están: APACHE, MYSQL, POSTFIX, IMAPD, Ubuntu Linux, SuSE Linux.

Entrevistador - ¿Como administrador de los servicios de la Universidad Tecnología de Bolívar, esta consciente de que la integración de los servicios no es la mas óptima y ¿Esta dispuesto a colaborar en la integración de proyecto de tesis en la red institucional?

Administrador - Estoy de acuerdo con cualquier propuesta que mejore la red de servicios institucionales. Antes no se había puesto en marcha una iniciativa de este tipo por falta de recursos.

3.1.2 ENTREVISTA AL DESARROLLADOR DE SAVIO.

Administrador: JAIRO ENRIQUE SERRANO CASTAÑEDA

Entrevistador - ¿Como es la administración de usuarios que acceden a los servicios del sistema?

Administrador - El primero que se registra en SAVIO, es el docente al cual personalmente se le asigna un nombre de usuario correspondiente al mismo del correo institucional, la clave es generada automáticamente y es dada a conocer al docente, este al igual que los alumnos se le invita a cambiar su contraseña inmediatamente ingresa al aula virtual.

El proceso con los alumnos es más automatizado, se solicita un volcado (copia) de la tabla de usuarios y relaciones de curso en el departamento de sistemas, esta es procesada por unos scripts en el servidor y el llenado de la información de

usuarios se hace automáticamente. Generando una clave que es conocida por el estudiante en el momento de iniciar el curso. En caso de ser un usuario antiguo, esta clave se le respeta y no es mostrada por el sistema en caso de solicitarla, en cambio se le ofrece la posibilidad de cambiarla y generar otra.

Entrevistador - ¿Como es el tratamiento de los datos privados de los usuarios? en especial el tratamiento y almacenamiento de las contraseñas de los usuarios en las bases de datos de los servidores?

Administrador - Las contraseñas son generadas por el sistema, y después de ser entregadas al usuario por el auxiliar encargado, este no tiene más acceso a ellas.

Entrevistador - ¿Como es el procedimiento para que un usuario cambie su clave?

Administrador - El usuario en cualquier momento puede cambiar su clave de forma manual, accediendo a un formulario especifico en el aula virtual.

Entrevistador - ¿Cual es el procedimiento para el retiro de usuarios del sistema?

Administrador - Al final del semestre se desactivan todos los usuarios del sistema a la espera del inicio del semestre donde paulatinamente se activan los nuevos basándose en los listados de registro académico.

Entrevistador - ¿Que nivel de seguridad tiene el acceso a los servidores?

Administrador - Los servidores se encuentran en el mismo espacio fisico del departamento de sistemas.

Entrevistador - ¿Que documentación disponible existe sobre el montaje de los

servicios ofrecidos?

Administrador - Disponemos de la documentación libre que se encuentra en los portales de las aplicaciones libres que usamos (Apache, MySQL, Postfix, imapd). La documentación se encuentra en el portal http://trac.unitecnologica.edu.co sobre diferentes temas.

Entrevistador - ¿Cuales son las características de la maquina que cubre este servicio?

Administrador – Es un IBM 325 con 1 disco duro de 70 GB, memoria de 4GB, 2 procesadores de 64bits AMD OPTERON a 2,6 GHz y sistema operativo Ubuntu Linux Server 6.06.

Entrevistador - ¿Cual es la frecuencia con la que se realizan procedimientos de Backups de los datos de usuario en los servicios?

Administrador - Todos los viernes se realiza una copia general del sistema y día por medio de la base de datos.

Entrevistador - ¿Para estos servicios se dispone de alguna licencia de software?

Administrador - Gracias a que existe una excelente calidad en el Software Libre usado en los servidores no necesitamos grandes inversiones de capital para el mantemiento de estos equipos.

Usamos una gran variedad de servidores entre los cuales están: APACHE, MYSQL, PHP5, PRADO y Ubuntu Linux.

3.2 ESPECIFICACIÓN DE REQUISITOS DEL SISTEMA

Garantizar el desempeño y la calidad del sistema implica que este sea confiable, seguro, eficiente, eficaz.

El sistema debe estar en capacidad de dar respuesta al acceso de todos los usuarios con tiempos de respuestas, aceptables y uniforme dado cualquier período de alta, media y baja demanda de uso del sistema.

Especificando un poco mas los requerimiento obtenidos y necesarios para el correcto desarrollo del sistema tenemos los REQUERIMIENTOS NO FUNCIONALES como atributos de calidad del sistema y los REQUERIMIENTOS FUNCIONALES que debe cumplir el sistema.

3.2.1 REQUERIMIENTOS NO FUNCIONALES

[01]	Seguridad
Descripción	El sistema tiene que ser seguro, y la seguridad del sistema debe empezar por la integridad, la privacidad de los datos ya almacenados y en especial por la autenticación de los datos de identidad de los usuarios de los servicios de SAVIO, acceso telefónico (RAS) y Correo Electrónico en La Universidad Tecnológica de Bolívar. El acceso al sistema debe ser restringido, sólo pueden ingresar a este, aquellas personas que estén registradas por el uso de claves asignadas. Esto implica que cada usuario autorizado debe tener nombre de ingreso y contraseña única. Estos usuarios están clasificados según su rol, por tal motivo el control de acceso implementado debe permitir asignar los perfiles para cada uno de los roles identificados. Según su rol especifico puede hacer modificaciones o no a los datos almacenados.
Importancia	Vital.
Urgencia	Importante
Comentario	Ninguno

Tabla 1: Caso de uso "Seguridad"

[02]	Confidencialidad
Descripción	El sistema debe estar en capacidad de rechazar accesos de posibles ataques contra la privacidad de los datos para que así la información pueda ser solo conocida por aquellas personas autorizadas y de esta forma provea los servicios requeridos por los usuarios del sistema.
Importancia	Vital.

Urgencia	Importante
Comentario	Ninguno

Tabla 2: Caso de uso "Confidencialidad"

[03]	Operatividad
Descripción	El sistema debe ser fácil en sus operaciones, de esta forma demandara un bajo nivel de soporte de usuarios. En otras palabras la interfaz como tal del sistema debe ser de fácil uso para sus usuarios. El sistema debe también poder ser administrado remotamente por las personas encargadas o designadas de los servicios de SAVIO, acceso telefónico (RAS) y Correo Electrónico en La Universidad Tecnológica de Bolívar.
Importancia	Vital.
Urgencia	Importante
Comentario	Ninguno

Tabla 3: Caso de uso "Operatividad"

[04]	*Mantenibilidad*
Descripción	El sistema debe de permitir su fácil mantenimiento, ya que si en algún momento se presentara o produce algún error, un evento de falla, este sea fácil de restituir y conserve así su funcionamiento normal. Además debe ser fácil de actualizar, en caso de que se presenten nuevas necesidades.
Importancia	Vital.

Urgencia	Importante
Comentario	Ninguno

Tabla 4: Caso de uso "Mantenibilidad"

[05]	*Escalabilidad y Flexibilidad*
Descripción	El sistema seguirá siendo capaz de permitir el desarrollo de nuevas funcionalidades en un futuro, adaptándose así a nuevos requisitos conforme cambian sus necesidades y sin perder calidad en los servicios. De esta forma contara con mayor nivel de flexibilidad y rapidez de respuesta en estos.
Importancia	Vital.
Urgencia	Importante
Comentario	Ninguno

Tabla 5: Caso de uso "Escalabilidad y Flexibilidad"

[06]	*Validación de Información*
Descripción	El sistema debe validar la información contenida en los servicios de SAVIO, acceso telefónico (RAS) y Correo Electrónico en La Universidad Tecnológica de Bolívar.
Importancia	Vital.

Urgencia	Importante
Comentario	Ninguno

Tabla 6: Caso de uso "Validación de Información"

[07]	Instalación
Descripción	La instalación del servidor de directorio debe ejecutarse satisfactoriamente bajo el sistema operativo GNU/LINUX
Importancia	Vital.
Urgencia	Importante
Comentario	Ninguno

Tabla 7: Caso de uso "Instalación"

3.2.2 REQUERIMIENTOS FUNCIONALES

3.2.2.1 Definición de actores

SAN cuenta con 2 actores básicos, los administradores del sistema y los usuarios que pueden ser a su vez: Alumnos, Docentes, Empleados o Administrativos de La Universidad.

[01]	Administrador del Sistema
Descripción	Representa al encargado de manipular los servicios de SAVIO, mensajería instantánea y Correo Electrónico en La Universidad Tecnológica de Bolívar. Se encargará de confirmar que la base datos contenga la información verídica. Genera un informe de posibles errores en la información contenida en el directorio.
Comentario	Es el único con acceso total.

Tabla 8: Definición de actor "Administrador del Sistema"

[04]	Usuarios
Descripción	Representa a las personas cuya información personal se encuentra en la base de datos, estos son tanto estudiantes como docentes o administrativos de La Universidad Tecnológica de Bolívar. Solo pueden consultar el los campos de Nombres, Apellidos y Código. Cambia su clave personal.
Comentario	Los usuarios no acceden directamente al servidor de directorio, lo hace a

	través de las aplicaciones de gestión.

Tabla 9: Definición de actor "Usuarios"

3.2.2.2 Definición de los casos de uso básicos del sistema

[G1]	Iniciar sesión	
Actores	Administrador y Usuarios	
Descripción	Valida el usuario para iniciar el sistema	
Precondición	Se debe disponer de nombre de usuario y clave	
Secuencia normal	Paso	Acción
	1	El administrador o usuario digita su nombre de usuario y clave
	2	El sistema valida el usuario
	3	Conexión al servidor LDAP
	4	El sistema verifica el usuario y clave.
	5	El servidor LDAP retorna verdadero o falso.
	6	El sistema cede al usuario el control de la aplicación.
Post condición	El usuario ha iniciado sesión.	
Excepciones	2	Si los datos son inválidos, el sistema pide confirmación de estos
	3	No hay conexión, se presenta un mensaje de error.
	4	Si retorna falso se pide al usuario nuevamente nombre y clave para su validación.
Rendimiento	Paso	Tiempo
	2	5 seg.
Frecuencia esperada	Siempre	
Importancia	Vital	
Urgencia	Inmediata	
Comentarios	Este proceso se realiza para cualquier tipo de acción	

Tabla 10: Caso de uso básico del sistema "Iniciar sesión"

[G2]	Cambiar contraseña.	
Actores	Administrador y Usuario	
Descripción	Cualquier usuario del sistema tiene la facultad de cambiar su propia contraseña para acceder al sistema.	
Precondición	Iniciar sesión	
Secuencia normal	Paso	Acción
	1	El sistema presenta un formulario con 3 campos a llenar, contraseña actual y confirmar 2 veces la nueva contraseña.
	2	El usuario confirma los datos escritos en el formulario y su contraseña es cambiada.
Post condición	Los datos han sido actualizados	
Excepciones	1	Si la contraseña actual no coincide con la almacenada en el servidor LDAP, se presenta un error y se pide llenar de nuevo los campos del paso 1.
	1	Si las 2 repeticiones de la contraseña nueva no coinciden, se presenta un error y se pide llenar de nuevo los campos del paso 1.
	2	Si el usuario no confirma el cambio de la contraseña, se retorna al formulario 1.
Rendimiento	Paso	Tiempo
	1	no determinado.
	2	no determinado.
Frecuencia esperada	no determinada	
Importancia	Vital	
Urgencia	Importante	
Comentarios	Si el usuario pierde su contraseña, este deberá reportarse ante el administrador del sistema con un documento que confirme su identidad y así, solicitar un cambio de contraseña manual.	

Tabla 11: Caso de uso básico del sistema "Cambiar contraseña"

3.2.2.3 Definición de los casos de uso del administrador

[A1]	Generador de Reportes	
Actores	Administrador	
Descripción	Describe el proceso de generación de los reportes	
Precondición	Iniciar sesión	
Secuencia normal	Paso	Acción
	1	Selecciona el tipo de reporte a generarse.
	2	El sistema hace la búsqueda de acuerdo a los parámetros
	3	Se genera el reporte en PDF (vista previa).
	4	El sistema pregunta si se va a imprimir el reporte
	5	Se imprime el reporte.
Post condición	El reporte se ha generado e impreso	
Excepciones	2	Si los parámetros de búsqueda son incorrectos, pide al administrador nuevos datos de búsqueda.
Rendimiento	Paso	Tiempo
	3	1 seg.
	5	5 min.
Frecuencia esperada	De acuerdo a las políticas establecidas para generar reportes del departamento de sistemas	
Importancia	Vital	
Urgencia	Importante	
Comentarios		

Tabla 12: Caso de uso administrador "Generador de Reportes"

[A2]	Buscar Usuario	
Actores	Administrador	
Descripción	Se puede realizar una búsqueda de usuarios en el servidor LDAP, para seleccionarlo y realizar alguna acción con el.	
Precondición	Haber iniciado sesión	
Secuencia normal	Paso	Acción
	1	Se presenta un formulario con los posibles campos para buscar al usuario.
	2	Se llena los campos necesarios para la búsqueda.
	3	Según los datos dados por el administrador se construye la consulta.
	4	Se envía la consulta al servidor LDAP
	5	Se captura los resultados y se presentan al administrador.
	6	Visualizar los datos del usuario
	7	Selecciona una acción a realizar
Post condición	Los datos han sido actualizados	
Excepciones	3	Si algún tipo de dato introducido por el administrador es incorrecto se pide a él que lo escriba de nuevo.
	5	Si la consulta no retorna nada se presenta de nuevo el formulario de búsqueda.
Rendimiento	Paso	Tiempo
	1	5 seg.
	4	10 seg.
Frecuencia esperada	no determinada	
Importancia	Vital	
Urgencia	Importante	
Comentarios		

Tabla 13: Caso de uso administrador "Buscar usuario"

[A3]	Actualizar de datos de usuarios	
Actores	Administrador	
Descripción	Si existe la posibilidad de haber cometidos errores o equivocaciones al ingresar algunos de los datos de un usuario. Con este proceso hay la posibilidad de que estos sean modificables. De igual forma si el usuario cambie datos como por ejemplo la dirección y números telefónicos.	
Precondición	tener un usuario seleccionado desde el caso de uso “Buscar Usuario”	
Secuencia normal	Paso	Acción
	1	Se presenta un formulario con los datos del usuario seleccionado.
	2	El Administrador introduce los datos nuevos.
	3	Se pulsa el botón de guardar.
	4	Se pide confirmación de la acción
	5	Se aplican los cambios en el servidor LDAP
Post condición	Los datos han sido actualizados	
Excepciones	2	El dato nuevo no es valido, mostrar advertencia.
	4	Si no se confirma, no se actualizan los datos
Rendimiento	Paso	Tiempo
	5	10 seg.
Frecuencia esperada	no determinada	
Importancia	Vital	
Urgencia	Importante	

Comentarios	

Tabla 14: Caso de uso administrador "Actualizar de datos de usuarios"

[A4]	Eliminar un Usuario	
Actores	Administrador	
Descripción	Los usuarios se puede eliminar en caso de que ya no pertenezcan a la Institución.	
Precondición	tener un usuario seleccionado desde el caso de uso “Buscar Usuario”	
Secuencia normal	Paso	Acción
	1	Se presenta un formulario con los datos del usuario seleccionado.
	2	Se pulsa el botón de eliminar.
	3	Se pide confirmación de la acción
	4	Se aplican los cambios en el servidor LDAP
Post condición	Los datos han sido actualizados	
Excepciones	3	Si no se confirma, no se elimina el usuario.
Rendimiento	Paso	Tiempo
	4	10 seg.
Frecuencia esperada	no determinada	
Importancia	Vital	
Urgencia	Importante	
Comentarios		

Tabla 15: Caso de uso administrador "Eliminar un Usuario"

[A5]	Cargar listados de alumnos	
Actores	Administrador	
Descripción	Los alumnos son los únicos usuarios del sistema que se pueden crear en bloque, por ello se cargan unos listados provenientes de registro académico con la información relevante de los alumnos que estén activos en el periodo actual.	
Precondición	Disponer del listado de usuarios valido para realizar el proceso.	
Secuencia normal	Paso	Acción
	1	Se presenta un formulario donde se le permite al administrador del sistema seleccionar un archivo en modo texto de su disco duro.
	2	Se pulsa el botón “subir y procesar archivo”
	3	El archivo es validado según una estructura definida que debe tener. Se genera listado nuevo.
	4	Se compara con un listado (listado viejo) de este mismo tipo que se encuentre en el servidor.
	4,1	Generar 2 listados de códigos de usuario según los archivos.
	4,2	Se genera un listado de usuarios que estén en el archivo viejo pero no el archivo nuevo para proceder a su eliminación.
	4,3	Se genera un listado de usuarios que estén en el archivo nuevo y no el archivo viejo para proceder a su adición.
	5	Se procesa el listado de usuarios a eliminar.
	6	Se procesa el listado de usuarios para adicionar.
	7	Se aplican los cambios en el servidor LDAP
Post condición	Los datos han sido actualizados	
Excepciones	3	La estructura del archivo no corresponde a la especificada. Se presenta un mensaje de error y se pide subir nuevamente el archivo.
	4	Si no existe un listado viejo, se procede a registrar todos los alumnos como nuevos.
Rendimiento	Paso	Tiempo
	2	30 seg.
	3	1 minuto

	4	1 minuto
	5	20 segundos por registro para no saturar el servidor.
	6	20 segundos por registro para no saturar el servidor.
Frecuencia esperada	Al iniciar y finalizar el semestre se produce la mayor carga del sistema al adicionar o borrar usuarios.	
Importancia	Vital	
Urgencia	Importante	

Tabla 16: Caso de uso administrador "Cargar listados de alumnos"

[A6]	Adicionar usuarios en forma manual	
Actores	Administrador	
Descripción	Se ingresan los datos del usuario a la base de datos	
Precondición	El administrador debe haber iniciado sesión.	
Secuencia normal	Paso	Acción
	1	Se presenta un formulario para llenar los datos requeridos.
	2	Se validan los datos suministrados.
	3	El sistema verifica si el usuario existe.
	4	Se aplican los cambios en el servidor LDAP.
Post condición	El usuario ha sido agregado satisfactoriamente.	
Excepciones	2	Si algún dato es invalido se pide llenar de nuevo los campos en el formulario.
	3	Los datos suministrados coinciden con unos ya existentes. se presenta un mensaje de error y se pide llenar de nuevo el formulario.
Rendimiento	Paso	Tiempo
	3	1 seg.
Frecuencia esperada	No determinada.	
Importancia	Vital	

Urgencia	Inmediata
Comentarios	Este proceso solo se realiza para usuarios que no se encuentren drectamente relacionados con el sistema académico de la Universidad Tecnológica de Bolívar. por ejemplo, como empleados de la sección administrativa.

Tabla 17: Caso de uso administrador "Adicionar usuarios en forma manual"

3.3 ARQUITECTURA PROPUESTA

3.3.1 ESQUEMA GENERAL

Hasta ahora se ha descrito ampliamente el sistema actual , principalmente con el fin de identificar las debilidades y restricciones que lo caracterizan.

A continuación se describirá la arquitectura completa del sistema de autenticación normalizado que ofrece la solución, y seguido la estructura del sistema en detalle.

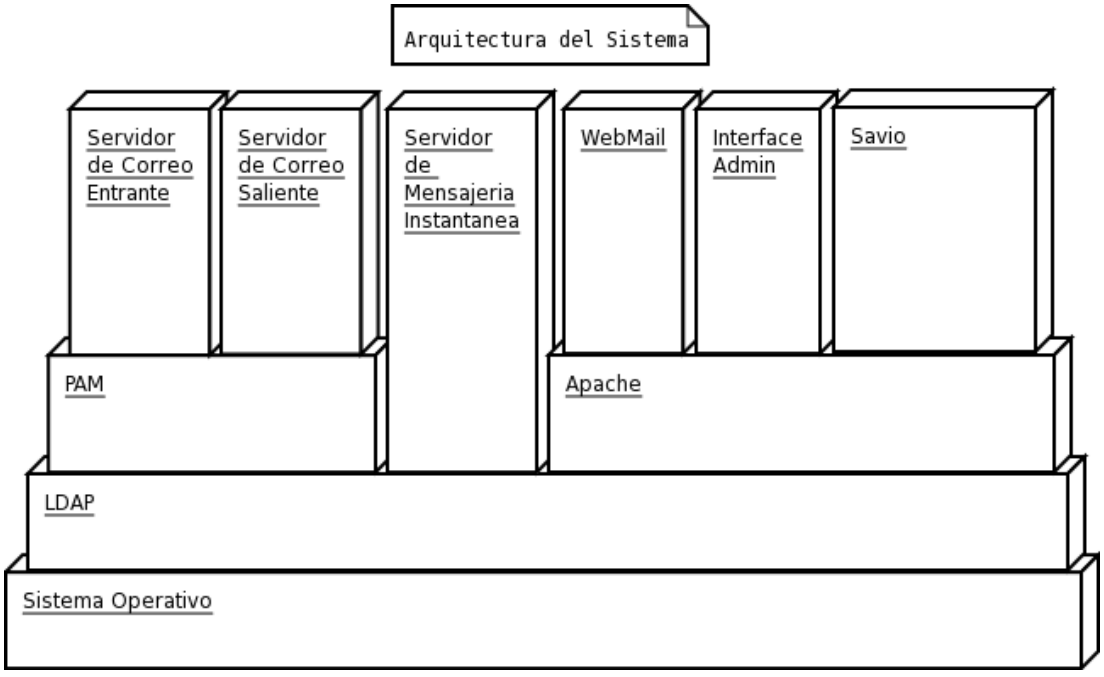


Figura 1: Arquitectura del sistema

Linux es la plataforma que soporta estos servicios gracias a su excelente

documentación, gran variedad de herramientas y bajo costo de mantenimiento.

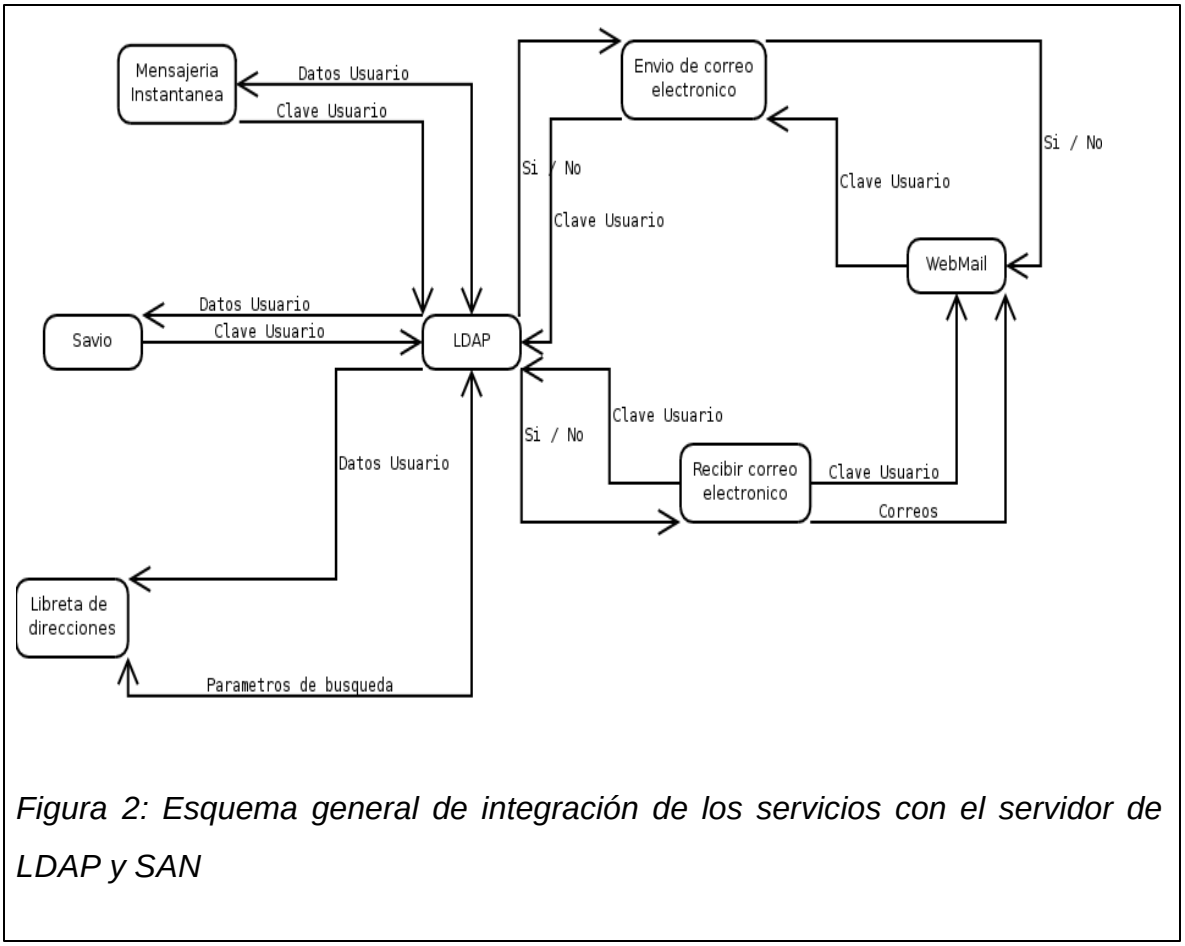


Figura 2: Esquema general de integración de los servicios con el servidor de LDAP y SAN

3.3.2 SERVIDORES

Para la prestación de los servicios LDAP(encargado de mantener la base de datos de usuarios), correo entrante(ya sea IMAP o POP3), envío de correo y mensajería instantánea se usan servidores que se instalaran desde el administrador de software de la distribución de Ubuntu Linux Server, estos pueden ser:

Servidor	Software
Envío de correo electrónico	SENDMAIL http://www.sendmail.org/
	POSTFIX (parte de la solución) http://www.postfix.org/
	QMAIL http://www.qmail.org/
	EXIM http://www.exim.org/
Recepción de correo electrónico IMAP o POP3	DOVECOT http://www.dovecot.org/
	COURIER (parte de la solución) http://www.courier-mta.org/
LDAP	OpenLDAP (parte de la solución) http://www.openldap.org/
	Fedora Directory Server http://directory.fedora.redhat.com/
Mensajería instantánea	Jabberd http://www.jabber.org/
	eJabberd http://ejabberd.jabber.ru/
	Wildfire (parte de la solución) http://www.jivesoftware.org/wildfire/

Tabla 18: Características de los servicios

El servicio de aulas virtuales se presta gracias al desarrollo de una plataforma propia el cual se integrará con los demás servicios para la autenticación de sus usuarios.

3.3.3 INFORMACIÓN ALMACENADA EN EL DIRECTORIO

En el servidor de directorio se almacenan 8 campos clave:

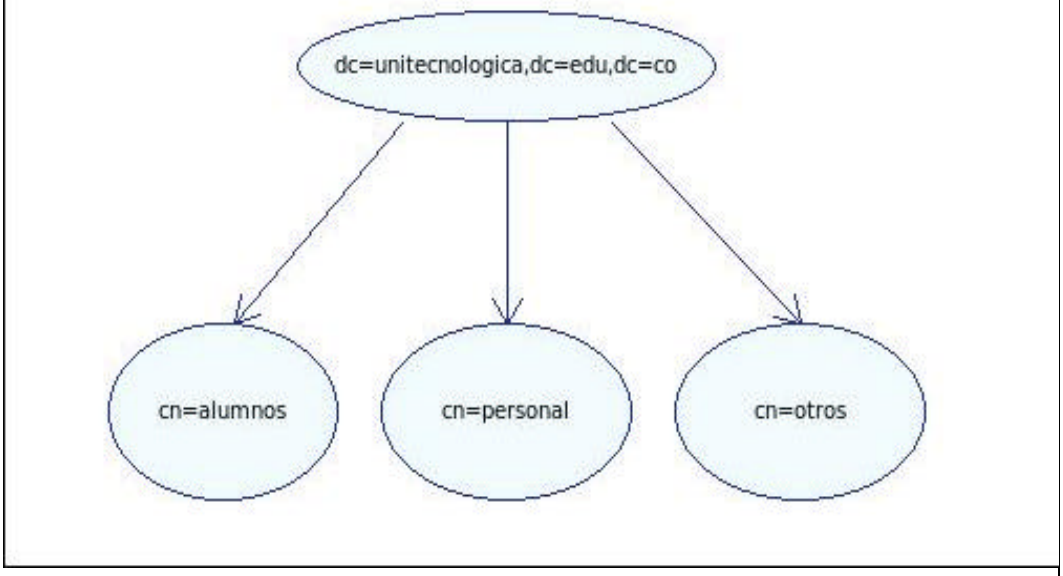
Campo	**Significado**
First name	Nombres
Last name	Apellidos
Common Name	Identificador de usuario. Siguiendo la nomeclatura de la Universidad.
User ID	Se usara igual que el “Common Name”
Password	Contraseña del usuario.
UID Number	Identificador de usuario en el sistema, este campo se genera automáticamente.
GID Number	Identificador del grupo al que pertenece el usuario.
Home directory	Directorio donde se almacenarán los datos, correos o configuraciones del propio usuario.

Table 19: Datos de usuarios almacenados en OpenLDAP

La creación de usuarios se hace de 2 maneras.

1. Creación de usuarios por lote, utilizada para el caso de los usuarios que son alumnos. En esta modalidad, la información se toma de las listas de alumnos del sistema de registro académico.
2. Creación de usuarios individuales, orientada a usuarios de otro tipo, categoría que incluye a docentes, admnistrativos y cuentas institucionales.

Al crearse estos usuarios con sus respectivos grupos, crean un árbol de directorio con la siguiente estructura:



Este modelo de árbol puede extenderse con nodos hijos de alumnos, como nodos

por profesión, personal con nodos hijos como “empleados, docentes, directivos” y en definitiva cualquier disección que se precise con el árbol de directorio.

3.3.4 DESEMPEÑO DE OpenLDAP

El desempeño de OpenLdap ha sido evaluado antes, y los resultados de esa evaluación, hecha por Thornton, Mundy y Chadwick, al compararlo con otras seis soluciones LDAP permite asegurar que OpenLDAP es una solución de buen rendimiento, en las tareas básicas relativas a esta clase de servicio: carga, búsqueda, adición, borrado y modificación de datos.

Los resultados de la evaluación, publicados en el documento “A comparative Perfomance Análisis of 7 Lightweight Directory Access Protocol”, permiten concluir que :

- OpenLDAP es relativamente fácil de administrar.
- OpenLDAP es la solución de mayor rendimiento en las búsquedas de información.
- Cuando se hace necesaria la modificación en el funcionamiento del servidor, el proceso con OpenLDAP no es amigable pues no se cuenta con una herramienta de configuración incluida. No obstante, el administrador del software de Linux puede ayudar bastante haciendo que esta limitante no sea crítica.
- El desempeño de OpenLDAP para atender transacciones es excelente cuando la base de datos no cambia con una frecuencia

muy alta, como en el caso de los servicios que la universidad presta. En este caso el mayor índice de movimientos se presenta en los inicios de cada período académico, y una vez registrados los usuarios, a lo largo del semestre la inscripción baja y modificación de datos de usuarios es de menor orden, pues la mayoría de los usuarios está conformada por la comunidad de estudiantes ya activos.

3.4 IMPLEMENTACIÓN DE LA SOLUCIÓN

3.4.1 INSTALACIÓN DEL SISTEMA OPERATIVO

La instalación del sistema operativo es uno de los puntos más fáciles al momento de la configuración del sistema base de SAN, se uso para tal fin la distribución Ubuntu Linux Server, por ser un producto de optima calidad, siguiendo los principios del software libre y una excelente comunidad de usuarios a su alrededor.

La configuración del servidor asignado para la puesta en marcha del proyecto se logra mediante un procedimiento relativamente sencillo. En los anexos se hace referencia a ellos con más detalle. Solo se hablará de las actualizaciones en este punto, ya que de ellas depende la estabilidad del sistema en producción.

```
$ sudo apt-get update
$ sudo apt-get upgrade
```

y para acceder al servidor desde un punto de red, se recomienda usar el servidor de shell[5] segura como openssh[6]

```
$ sudo apt-get openssh-server
```

5 Shell: Interprete de comandos, en este caso bash en Linux.

6 OpenSSH: servicio de shell por red que cuenta con la característica de estar cifrado.

3.4.2 INSTALACIÓN DEL SERVIDOR OPENLDAP

Se procede a instalar el servidor de directorio, el punto base del sistema de autenticación de la Universidad.

```
$ sudo apt-get install slapd
```

Se procede a ajustar el servidor de directorio para acoplarlo complemente a los requerimientos del sistema.

```
$ sudo dpkg-reconfigure slapd
```

El servidor esta completamente configurado y no se necesita reiniciar el equipo.

Es necesario ajustar el acceso directo al servidor de directorio desde la red exterior por medio de un firewall, para limitar el acceso a información que no corresponde necesariamente a un publico exterior a los intereses de la universidad.

3.4.3 CONFIGURACIÓN DE NSS y PAM

Teniendo el sistema base en línea se procede con la instalación y configuración del servicio que enlazará la base de datos de usuarios virtuales creados en LDAP con los usuarios que el sistema tomará como propios.

```
$ sudo apt-get install libpam-ldap libnss-ldap
```

Al descargarse los paquetes del repositorio de fuentes, se auto configuran preguntando los detalles de la instalación del sistema LDAP

1. Dirección del servidor LDAP, en este caso porque el servidor LDAP esta en la misma maquina es: 127.0.0.1 para acelerar el proceso de conexión.
2. El nombre distintivo “distinguished name” de la base de usuarios, “dc=unitecnologica,dc=edu,dc=co”
3. La versión LDAP que se usará, se selecciona la versión 3
4. Nos muestra una advertencia de que el archivo nsswitch.conf lo tendremos que modificar manualmente, se pulsa “ok”
5. Se configura el acceso como administrador a LDAP, “cn=admin,dc=unitecnologica,dc=edu,dc=co”

```
$ sudo vi /etc/nsswitch.conf
```

Con el editor “vi” se edita el archivo y se procede a reemplazar “compat” por “ldap files”

Desde el vi:

```
:%s/compat/ldap files/g
```

Más adelante se podrá probar si los usuarios y grupos creados en LDAP como “posixAccount” y “posixGroup” respectivamente, los toma el sistema.

```
$ getent passwd admin
$ getent group alumnos
```

Modificar los siguientes archivos dejándolos como a continuación se presenta:

Se modifica también el archivo common-account:

```
$ sudo vi /etc/pam.d/common-account
account sufficient      pam_ldap.so #adicionado
account required        pam_unix.so
```

Se modifica el archivo common-auth:

```
$ sudo vi /etc/pam.d/common-auth
auth    sufficient      pam_ldap.so #adicionado
auth  required pam_unix.so nullok_secure use_first_pass
```

Se modifica el archivo common-password:

```
$ sudo vi /etc/pam.d/common-password
password   sufficient  pam_ldap.so #adicionado
password  required pam_unix.so nullok obscure min=4 max=8 md5
```

Y finalmente se modifica el archivo common-session:

```
$ sudo vi /etc/pam.d/common-session
session required        pam_unix.so
#adicionando la siguiente linea los directorios de usuarios se crean
al momento de iniciar la sesión el usuario en el sistema o al momento
de recibir un correo.
session required        pam_mkhomedir.so skel=/etc/skel/
session optional        pam_ldap.so #adicionado
session optional        pam_foreground.so
```

3.4.4 CONFIGURACIÓN DEL SERVIDOR DE CORREO ENTRANTE

Desde el shell:

```
$ sudo apt-get install courier-imap courier-imap-ssl  courier-pop3
courier-pop-ssl
```

Al momento de crearse un usuario en el sistema, hay un directorio llamado “skel” donde están los archivos por defecto que contendrá el “home” de este. Como se acordó el formato de almacenamiento de los correos en el servidor fuera “Maildir”, se adiciona al “skel” con el comando “maildirmake” la configuración por defecto.

```
$ sudo maildirmake /etc/skel/Maildir
$ sudo maildirmake /etc/skel/Maildir/.Drafts
$ sudo maildirmake /etc/skel/Maildir/.Sent
$ sudo maildirmake /etc/skel/Maildir/.Trash
$ sudo maildirmake /etc/skel/Maildir/.Templates
```

Ahora se crean las carpetas donde se almacenarán los mensajes de los usuarios.

Se tienen en cuenta 3 grupos principales:

- Alumnos
- Personal (Docentes, Administrativos y empleados)
- Otros

Ahora desde el shell se crean las carpetas del usuario nuevo:

```
$ sudo mkdir -p /home/users/alumnos
$ sudo mkdir -p /home/users/personal
$ sudo mkdir -p /home/users/otros
$ sudo chown -R root:alumnos /home/users/alumnos
$ sudo chown -R root:personal /home/users/personal
$ sudo chown -R root:otros /home/users/otros
$ sudo chmod -R ug+rwx /home/users/
```

3.4.5 CONFIGURACIÓN DEL SERVIDOR DE CORREO SALIENTE

Desde el shell:

```
$ sudo apt-get install postfix
$ sudo postconf -e 'home_mailbox = Maildir/'
$ sudo postconf -e 'mailbox_command ='
$ sudo /etc/init.d/postfix restart
```

3.4.6 CONFIGURACIÓN DEL SERVIDOR MENSAJERÍA INSTANTÁNEA

Teniendo el instalador del servidor Wilfire, se puede descargar la última versión de http://www.jivesoftware.org/wildfire. Se descomprimen y ubican los archivos en "/usr/lib" del sistema desde un shell:

```
$ tar xvzf wildfire_3_0_1.tar.gz
$ mv wildfire /usr/lib
$ cd /usr/lib/wildfire/
$ chown -R root:root ../wildfire/
```

Ahora se necesita crear el servicio de inicio, para que el servidor arranque con el sistema, cada vez que este se reinicie o encienda. Pra esto dentro del directorio /etc/init.d existe un archivo llamado "skeleton" que no es más sino una plantilla para crear servicios.

```
$ cd /etc/init.d/
$ cp skeleton wildfire
$ vi wildfire
```

Solo se necesita editar un par de detalles en este archivo, procurando dejar el archivo como a continuación se detalla:

```
#! /bin/sh
```

```
### BEGIN INIT INFO
# Provides:          Wildfire
# Required-Start:    $local_fs $remote_fs
# Required-Stop:     $local_fs $remote_fs
# Default-Start:     2 3 4 5
# Default-Stop:      S 0 1 6
# Short-Description: Wildfire Jabber Server
# Description:       Servidor Jabber integrado en SAN

### END INIT INFO

set -e

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
DESC="Wildfire Jabber Server "
NAME=wildfire
DAEMON=/usr/lib/wildfire/bin/wildfire
SCRIPTNAME=/etc/init.d/$NAME
# Gracefully exit if the package has been removed.
test -x $DAEMON || exit 0

d_start() {
         $DAEMON start
}

d_stop() {
        $DAEMON stop
}
d_reload() {
        $DAEMON start;$DAEMON stop; \
                --name $NAME --signal 1
}

case "$1" in
  start)
        echo -n "Starting $DESC: $NAME"
        d_start
       echo "."
        ;;
  stop)
        echo -n "Stopping $DESC: $NAME"
        d_stop
        echo "."
        ;;
  restart|force-reload)
        echo -n "Restarting $DESC: $NAME"
        d_stop
        sleep 1
```

```
        d_start
        echo "."
        ;;
  *)
        echo "Usage: $SCRIPTNAME {start|stop|restart|force-reload}"
>&2
        exit 3
        ;;
esac
exit 0
```

Se guarda los cambios con “:wq” en el vi.

Y se asignan derechos de ejecución sobre ese archivo

```
$ chmod ug+x wildfire
```

Se da una orden a Linux que ejecute ese servicio en los niveles de inicio predefinidos.

```
$ update-rc.d wildfire defaults
```

Para ejecutar el servidor, se necesita tener java, por lo que se procede a instalar desde un shell:

```
$ apt-get -d install sun-java5-bin sun-java5-jre
```

Ahora bien se procede a configurar el servidor de mensajería instantánea para su integración con SAN.

```
$ vi /usr/lib/wildfire/conf/wildfire.xml
```

Buscando la sección de LDAP, se procura dejar el archivo de configuración como se describe a continuación:

```
  <ldap>
    <host>127.0.0.1</host>
    <port>389</port>
    <usernameField>uid</usernameField>
    <nameField>cn</nameField>
    <emailField/>
    <baseDN>dc=unitecnologica;dc=edu;dc=co</baseDN>
    <adminDN/>
    <adminPassword/>
    <debugEnable>true</debugEnable>
  </ldap>
  <provider>
    <user>

<className>org.jivesoftware.wildfire.ldap.LdapUserProvider</className>
    </user>
    <auth>

<className>org.jivesoftware.wildfire.ldap.LdapAuthProvider</className>
    </auth>
  </provider>
  <connectionProvider>

<className>org.jivesoftware.database.EmbeddedConnectionProvider</class
Name>
  </connectionProvider>
  <setup>true</setup>
  <log>
    <debug>
      <enabled>true</enabled>
    </debug>
```

```
  </log>
```

Con esto se puede iniciar el servidor de mensajería instantánea y se procede a su configuración:

```
$ /etc/init.d/wildfire start
```

Desde un navegador se accede a la siguiente dirección:

- http://unitecnologica.edu.co:9090

Se accede con el usuario “admin” y con la clave asignada desde el servidor LDAP.

3.4.7 INSTALACIÓN DEL ADMINISTRADOR DE DIRECTORIO

Desde el shell:

```
$ sudo apt-get install apache2 php5-session php5-gettext php5-ldap
```

se descarga la última versión de phpLDAPadmin de http://phpldapadmin.sourceforge.net y desde el shell se descomprime y copia al directorio raiz del servidor web:

```
$ tar xvzf phpldapadmin-1.0.1.tar.gz
$ mv phpldapadmin-1.0.1 /var/www/phpldapadmin
```

Se configura phpldapadmin editando los archivos contenidos en la carpeta “conf”

```
$ cd /var/www/phpldapadmin/conf
$ mv config.php.example config.php
$ vi config.php
```

Se descomenta la linea 74

```
$ldapservers->SetValue($i,'server','host','127.0.0.1')
```

Se guarda con “:wq” desde “vi” y desde un navegador se accede a la dirección:

- http://unitecnologica.edu.co/phpldapadmin

Se pulsa “login” y en el campo “Login DN” se escribe “cn=admin,dc=unitecnologica,dc=edu,dc=co” y en “Password” se pone temporalmente “12345”

Inmediatamente se procede a la creación de los grupos del sistema:

1. Se pulsa sobre el dominio “dc=unitecnologica,dc=edu,dc=co”
2. Seleccionandose “Create a child entry”

3. Se selecciona “Posix Group”
4. El campo necesario para esto es “Group” donde se adiciona: “alumnos”
5. Se realiza el mismo procedimiento 2, 3 y 4 pero con el “Group” “personal” e “institucional”

Para adicionar usuarios:

1. Se pulsa sobre el dominio “dc=unitecnologica,dc=edu,dc=co”
2. Se pulsa sobre “cn=alumnos”, “cn=empleados” o “cn=otros”
3. Seleccionandose “Create a child entry”
4. Se selecciona “User Account” y se completan los siguientes datos:

    - “First name”: Primer nombre del usario
    - “Last name”: Apellidos
    - “Common Name” y “User ID”: el Identificador del usuario, por ejemplo si es alumno: “c0105001”
    - “Password:” y “Verify Password:” la contraseña que se asignara al usuario.
    - “GID Number:” Se selecciona el grupo a que corresponde entre “alumnos”, “personal” u “otros”.
    - “Home directory:” se asigna una combinación del path automatico para el directorio raiz del usuario y el CN o UID del mismo, por ejemplo: “/home/users/alumnos/c0105001/”
5. Se pulsa proceder y el usuario a sido creado.

3.4.8 INSTALACIÓN DEL CLIENTE DE CORREO WEB SQUIRRELMAIL

Solo queda configurar el servicio webmail, para esto de instala desde el shell:

```
$ sudo apt-get install squirrelmail
```

Se necesita editar el archivo de configuración del servidor web apache, creando un alias para acceder directamente al servicio:

```
$ vi /etc/apache2/sites-available/default
```

Solamente se necesita adicionar “Alias /webmail '/usr/share/squirrelmail'“ entre los tags “VirtualHost” predefinidos:

```
# se busca esta parte y se adicionado un alias
<VirtualHost ... >
...
        ServerAdmin san@san
      #adicionar la siguiente linea...
        Alias /webmail "/usr/share/squirrelmail"
      #...
        DocumentRoot /var/www
...
```

```
</VirtualHost>
```

Se accede al webmail desde un navegador en la siguiente dirección:

- http://unitecnologica.edu.co/webmail

Se puede configurar con mejor eficiencia squirrelmail con la utilidad que se instala en el sistema para tal fin:

```
$ squirrelmail-configure
```

En especial en la opción 2 “Server Settings” donde se configurarán los datos de conexión al servidor.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> 2
```

Se edita los parámetros del servidor IMAP:

```
Server Settings

General
-------
1.  Domain                : unitecnologica.edu.co
2.  Invert Time           : false
3.  Sendmail or SMTP      : SMTP

A.  Update IMAP Settings  : localhost:143 (other)
B.  Update SMTP Settings  : localhost:25

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> S
```

Se guarda “S” y se sale de la configuración “Q”.

Existe una serie de accesorios (plugins) recomendados para instalar:

Corrector ortográfico:

```
$ apt-get install ispell wspanish
```

Ahora se procede a la configuración de estos:

```
$ squirrelmail-configure
SquirrelMail Configuration : Read: config.php (1.4.0)
```

```
-------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> 8
```

Se procede a activar todos los accesorios:

```
Plugins
  Installed Plugins
    1. message_details
    2. squirrelspell
    3. newmail
    4. calendar
    5. bug_report

  Available Plugins:
    8. abook_take
    9. delete_move_next
    10. administrator
    11. listcommands
    12. filters
    13. fortune
    15. mail_fetch
    16. sent_subfolders
    17. spamcop
```

```
R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> S
```

La configuración se lleva a cabo escribiendo el identificador que acompaña el accesorio que se necesita, por ejemplo se desea eliminar “bug_report” de los activos solo se escribe “5” y se pulsa “enter”, por defecto no hay ningún accesorio activo, se aconseja activar: squirrelspell, newmail, calendar, bug_report y message_details.

Para lograr una mayor integración con el gestor de contenidos de la universidad, se puede adicionar la ruta del webmail en un contenido nuevo ayudado por un iframe xhtml.

3.4.9 INTEGRACIÓN CON EL PORTAL DE LA UNIVERSIDAD

La universidad cuenta con infraestructura web desarrollada con el sistema de gestión de contenidos Drupal[7], en la cual los usuarios pueden identificarse usando el usuario y contraseña del servidor de directorio. Gracias a esta ventaja, los propios usuarios pueden cambiar su contraseña fácilmente.

7 Drupal: Sistema de gestión de contenidos, puede acceder a su portal en ingles (http://www.drupal.org) ó en español (http://www.drupal.org.es) administrado por uno de los realizadores de esta tesis.

Se resalta que esta integración no viene por defecto en el sistema, tiene que instalarse de la siguiente forma:

```
$ wget
http://ftp.osuosl.org/pub/drupal/files/projects/ldap_integration-
4.7.0.tar.gz
$ tar xvzf ldap_integration-4.7.0.tar.gz
$ mv ldap_integration /var/www/modules/
```

Se procede a activar el módulo en drupal desde un navegador y con la contraseña de administrador se ingresa a:

- http://www.unitecnologica.edu.co/user

Se ingresa a la “zona administrativa”, “módulos” y se selecciona “ldapauth” y “ldapdata”, se pulsa el botón para guardar la configuración.

Ahora se ingresa a “opciones”, “ldapauth” y el “Login procedure” se selecciona “LDAP directory only”, en “Base dn” se escribe “dc=unitecnologica,dc=edu,dc=co”, por ultimo “UserName attribute:” se asigna “uid”. Con esto se configura el servidor para ingresar únicamente con los datos almacenados en el servidor LDAP.

Se procede a la configuración para activar el cambio de la contraseña desde la interfaz del usuario en el portal. Se ingresa a “ldapdata” se selecciona “Changes in account fields will be mapped to LDAP attributes and back“, el campo que se le permitirá cambiar al usuario es la contraseña, entonces “pass” se asigna

“userPassword” el cual es el campo de la contraseña en el servidor LDAP, con esto ser termina la configuración y el usuario desde ese momento puede cambiar su clave universal fácilmente, con solo cambiar sus datos personales en la pagina web de la universidad.

3.4.10 COPIAS DE SEGURIDAD

Parte importante de un servidor en producción es el mantenimiento siempre al día de una copia reciente de los datos vitales y configuraciones almacenadas.

Es necesario crear un archivo de script para tal fin.

```
#!/bin/sh
echo "Generando Copia..."
FECHA=`date +%d-%m-%Y`
echo "Deteniendo el servidor OpenLDAP"
/etc/init.d/slapd stop
echo "Deteniendo el servidor Wildfire"
/etc/init.d/wildfire stop
echo "Deteniendo el servidor Postfix"
/etc/init.d/postfix stop
echo "Deteniendo el servidor IMAP"
/etc/init.d/courier-imap stop
echo "Deteniendo el servidor POP"
/etc/init.d/courier-pop stop
echo "Deteniendo el servidor AUTH"
/etc/init.d/courier-authdaemon stop


echo "Comprimiendo la base de datos de OpenLDAP"
tar -cjvf /home/backups/var_ldap-SAN-$FECHA.tar.bz2 /var/lib/ldap
echo "Comprimiendo configuraciones"
tar -cjvf /home/backups/etc-SAN-$FECHA.tar.bz2 /etc/ldap
echo "Comprimiendo Wildfire"
tar -cjvf /home/backups/wildfire-SAN-$FECHA.tar.bz2 /usr/lib/wildfire
echo "Comprimiendo Datos de usuarios"
```

```
tar -cjvf /home/backups/users-SAN-$FECHA.tar.bz2 /home/users


echo "Iniciando Servicio OpenLDAP"
/etc/init.d/slapd start
echo "Iniciando el servidor Wildfire"
/etc/init.d/wildfire start
echo "Iniciando  el servidor Postfix"
/etc/init.d/postfix start
echo "Iniciando  el servidor IMAP"
/etc/init.d/courier-imap start
echo "Iniciando  el servidor POP"
/etc/init.d/courier-pop start
echo "Iniciando  el servidor AUTH"
/etc/init.d/courier-authdaemon start
```

Se guarda el archivo como copia.sh, se crea una carpeta en “/home” llamada backups:

```
$ sudo mkdir /home/backups
```

Para crear un backup:

```
$ sh copia.sh
```

Generándose así los archivos comprimidos de los datos y configuraciones. Este procedimiento se recomienda realizar a la media noche automáticamente, con la ayuda del programador de tareas.

En cuanto se presente una falla en el sistema, las copias se pueden usar selectivamente y restaurar los datos o servicios afectados.

4 ALCANCES Y LIMITACIONES

Este proyecto logró la instalación y puesta en marcha del servidor de directorio LDAP para la implantación del sistema de autenticación normalizado que unificará la red de servicios informáticos de la Universidad Tecnológica de Bolívar, integrándolo con los servicios propuestos.

Durante el desarrollo del trabajo, se efectuó un ajuste a los objetivos propuestos inicialmente en el anteproyecto, consistente en la sustitución del servicio de RAS por el de Mensajería Interna, como parte del servidor de directorio LDAP. La principales razón para implementar este cambio son dos:

En primer lugar, se hizo una evaluación cualitativa del futuro previsible del servicio RAS en la red de la Universidad, encontrándose que presumiblemente dicho servicio tienden a desaparecer, dada la imposibilidad de escalar la tecnología de hardware que lo soporta para garantizar una eficiencia mínima, a un costo razonable. Adicionalmente, el desarrollo de diferentes ofertas de acceso a Internet, al alcance de los miembros de la comunidad universitaria, en modalidades de acceso telefónico, ADSL, vía cable o fibra óptica, de costos bajos, sustituyen el principal objetivo que el servicio RAS tuvo en su momento: garantizar que los usuarios tuvieran una vía de acceso a Internet.

En segundo lugar, la integración de un servicio de mensajería instantánea interno, resulta más útil y beneficiosa para la comunidad de usuarios, al proporcionar un servicio que no se tiene en la actualidad, pero sobre todo al posibilitar un mejor aprovechamiento del ancho de banda en el canal de salida a Internet, pues un servicio de mensajería interna no requiere salir a Internet para funcionar y ofrece

mayores niveles de privacidad y mejores posibilidades de control que los mensajeros disponibles en Internet, sean comerciales o gratuitos.

Este trabajo se realizó bajo la supervisión de la dirección General de Tecnologías de la Información de la Universidad Tecnológica de Bolívar con quien se realizaron reuniones periódicas para el seguimiento y puesta en marcha del proyecto.

5 RECOMENDACIONES

Para lograr una mejor implementación, que asegure en mayor proporción la estabilidad en el funcionamiento de la solución implementada en este trabajo, sería recomendable tener en cuenta las siguientes propuestas:

1. Es conveniente instalar el servicio en un hardware (servidor) con más prestaciones, más potente, que posibilite integrar los servicios con mayores niveles de respuesta y confiabilidad. Para ello se podría tomar como referencia el servidor que presta el servicio de SAVIO.

2. Convendría, para un mejor aprovechamiento del trabajo planteado en el presente proyecto, adquirir un segundo servidor para que sea configurado y actué como espejo (redundante) de manera que se garantice un adecuado nivel de respaldo y se eviten interrupciones en el servicio en casos de falla del servidor LDAP. Esta recomendación obedece a que una falla en el servicio de autenticación resulta crítica para el funcionamiento de todos los demás servicios involucrados.

3. Los autores consideran importante recomendar que la Universidad fortalezca en su comunidad interna la conciencia de la importancia que tiene el uso del software libre disponible, para los desarrollos actuales, en la medida en que ello contribuye a disminuir las necesidades de inversión para desarrollar nuevas funcionalidades de mucha utilidad para la comunidad de usuarios. El uso de software libre, en la práctica, ahorra dinero, que puede ser invertido en capacitación para el personal que trabaja en el área de sistemas.

4. Una etapa siguiente del presente proyecto, podría ser la relacionada con la implementación del cifrado de datos para las transacciones de comunicación entre servicios, con lo que se ganarían niveles más altos de privacidad y seguridad de la información.

6 CONCLUSIONES

La experiencia obtenida luego del desarrollo de este trabajo, abre un horizonte de reflexiones en el que se pueden apreciar diversas posibilidades para el mejoramiento de los servicios prestados a toda la comunidad universitaria a través de la infraestructura computacional y de redes.

La existencia de los servicios de directorio dista mucho de ser algo nuevo en el ámbito empresarial o académico. Sin embargo, en nuestro medio, las organizaciones que poseen una red de computadoras que apoya la gestión, no los utilizan, o los utilizan en forma relativamente leve o superficial.

Lo anterior obedece a razones como el desconocimiento de dichos servicios, en algunos casos, o a un facilismo mal entendido en otros, en virtud del cual el administrador de la red genera soluciones rápidas a los distintos problemas de identidad, pero que a mediano o largo plazo se convierten en soluciones ineficaces, que generalmente involucran el uso indiscriminado de bases de datos heterogéneas para autenticar la identidad de los usuarios en cada uno de los servicios que la requieren.

Paulatinamente, a medida que los servicios, o las cantidades de usuarios se incrementan, el administrador debe enfrentarse a los problemas de confusión en las identidades de usuario, dificultad de administración de las mismas, redundancia en los datos y otros, que son completamente resueltos con la implementación de un servicio de directorio como el propuesto y desarrollado en el presente trabajo.

El costo de implementación de un servicio de esta naturaleza no resulta excesivo,

si se considera la cantidad de trabajo administrativo que se ahorra, además del incremento en la seguridad y confiabilidad que los usuarios sienten hacia la organización. Si bien la implementación de esta clase de servicios a gran escala, puede requerir la incorporación de hardware (servidores), cuyas características pueden estar relacionada con el tipo de servicios que se ofrecen y con la cantidad de usuarios atendidos, en el caso particular del presente trabajo, los requerimientos de hardware y software son relativamente muy bajos, para una población significativa de usuarios, que en general es superior a la de la mayoría de las organizaciones empresariales que operan en la región.

Por consiguiente, la solución descrita en este trabajo, resultaría de enorme utilidad para esa comunidad de empresas, cuyas exigencias de servicios de red son muy similares a las que ofrece la universidad, pero con un menor número de usuarios

Los servicios de autenticación de identidad, asociados a directorios, al igual que muchos otros de los recursos asociados al desarrollo de la tecnología de las redes y las comunicaciones, han sido objeto de una evolución permanente desde su aparición. Es presumible que sigan desarrollándose y evolucionando hacia nuevas formas dada el desarrollo permanente de las tecnologías que sustentan los servicios y que dan paso a nuevas posibilidades, mayores velocidades, coberturas más amplias y que por consiguiente obligan a nuevas y mejores concepciones de seguridad.

El administrador de los servicios debe entonces desarrollar la habilidad de auto-aprender al mismo ritmo, para garantizar que los recursos bajo su control, superan los mínimos de seguridad y confiabilidad necesarios. Curiosamente, es notable que habiendo mucha información disponible sobre estos temas, aparentemente falte capacitación alrededor de los servicios expuestos aquí. Este trabajo pretende servir de base para la investigación de nuevo conocimiento y el

desarrollo de nuevos ángulos del problema. Los autores esperan que sea aprovechado al máximo y mejorado constantemente, tanto a nivel de los administradores de los servicios como de toda la comunidad universitaria en general.

7 BIBLIOGRAFÍA

7.1 PÁGINAS CONSULTADAS

http://es.wikipedia.org/wiki/LDAP

Wikipedia La enciclopedia Libre. - LDAP

http://ldapman.org/articles/sp_intro.html

Una introducción a LDAP

https://help.ubuntu.com/community/Postfix

Ubuntu Postfix Configuration

https://help.ubuntu.com/community/LDAPClientAuthentication

Ubuntu PAM Configuration

http://www.openldap.org/doc/admin/

LDAP Quick Start Admin

http://es.tldp.org/COMO-INSFLUG/COMOs/LDAP-Linux-Como/

LDAP-LINUX-COMO

http://whitepapers.zdnet.co.uk/0,39025945,60112021p-39000720q,00.htm

A Comparative Performance Analysis of 7 Lightweight Directory Access Protocol Directories - University of Salford - 2003

7.2 TEXTOS CONSULTADOS

* SLOMAN Morris, Kramer Jeft. Distributed systems and computers networks. UK. Great Britain. Distributed data buses. 15p.

* TACKETT Jack. Linux edición especial. México: Prentice Hall. Como mejorar la seguridad del sistema: Seguridad de contraseñas. 623p.

* MEDIAVILLA Manuel. Seguridad en Linux. Colombia: Combutcc:Ra-Ma. Las contraseñas. 27p.

* GARFINKEL Simson y Spafford Gene. Seguridad practica en Unix e Internet. México: O'Reilly, 1999. Criptografía 118p.
------ Seguridad en WWW. 465p.

* FARLEY Marc, Stearns Tom, Hsu Jeffrey. Guia de seguridad e integridad de datos. España: McGraw Hill, 1996. Seguridad informática. 181p.
------ Seguridad en redes. 199p.
------ Identificación y confidencialidad en redes. 219p.

8 ANEXO

8.1 DIAGRAMA DE CASOS DE USO

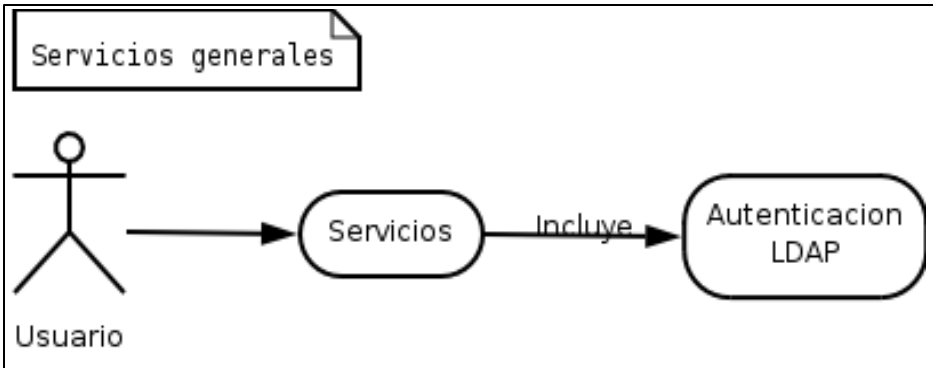


Figura 4: Servicios generales, todos se autentican contra un servidor LDAP

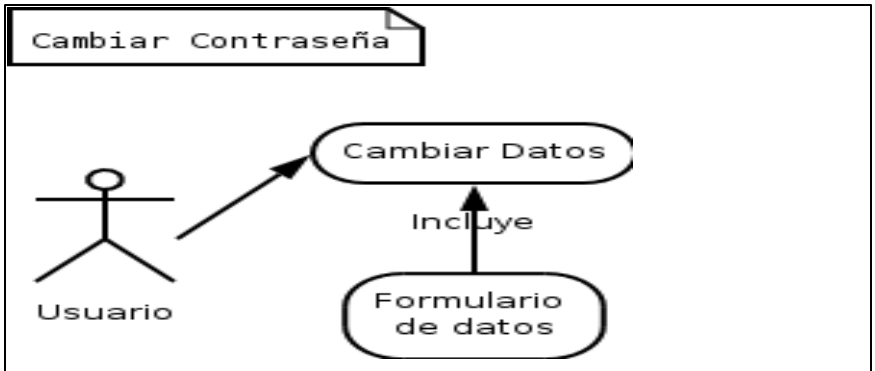


Figura 5: Cambiar contraseña

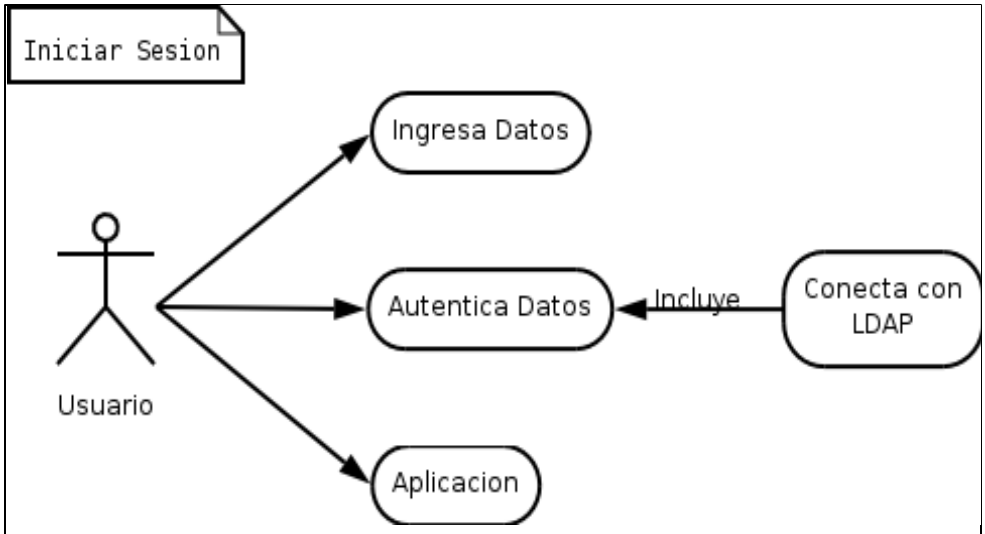


Figura 6: Inicio de sesión

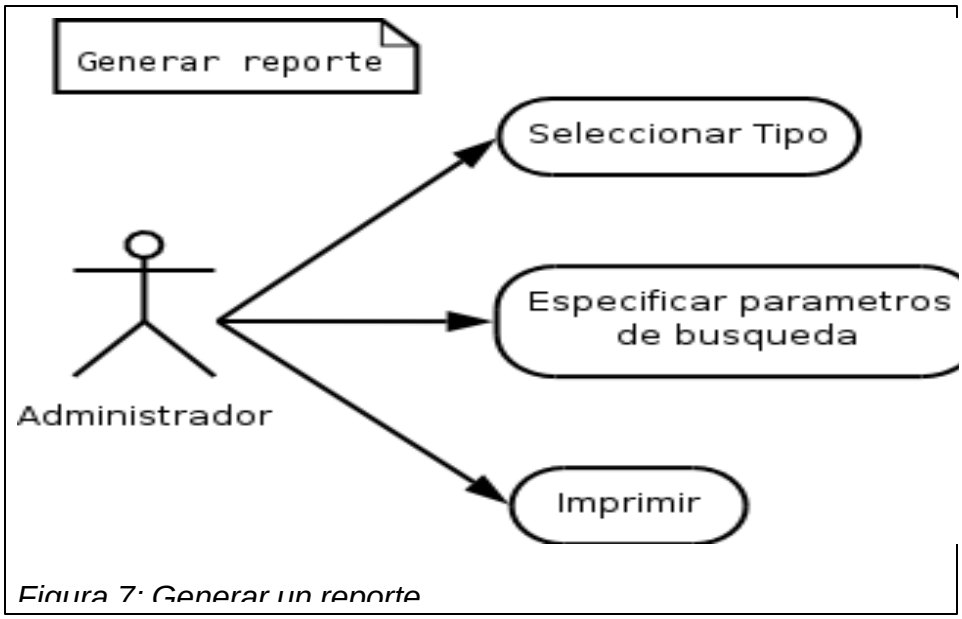


Figura 7: Generar un reporte

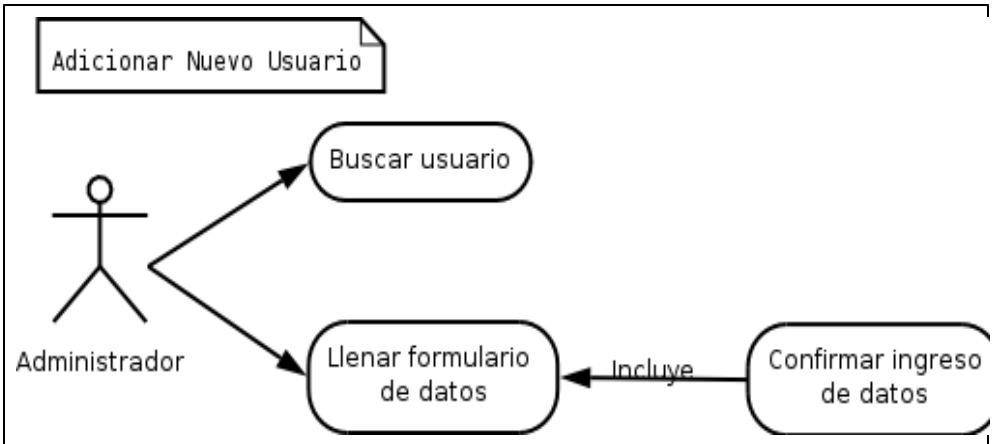


Figura 8: Adicionar un usuario al sistema manualmente

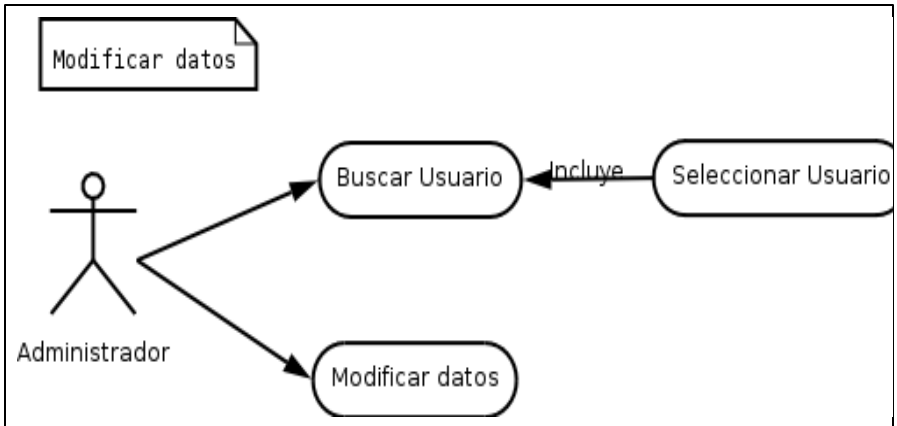


Figura 9: Modificar manualmente los datos de un usuario

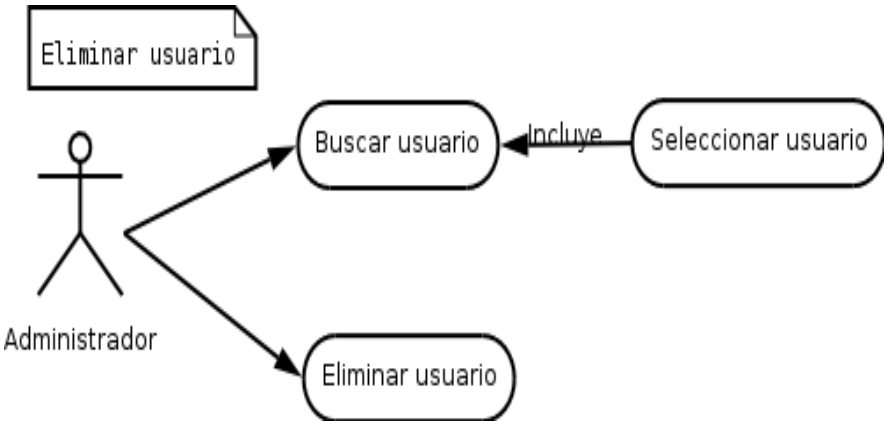


Figura 10: Eliminar un usuario manualmente

8.2 DIAGRAMA DE SECUENCIAS

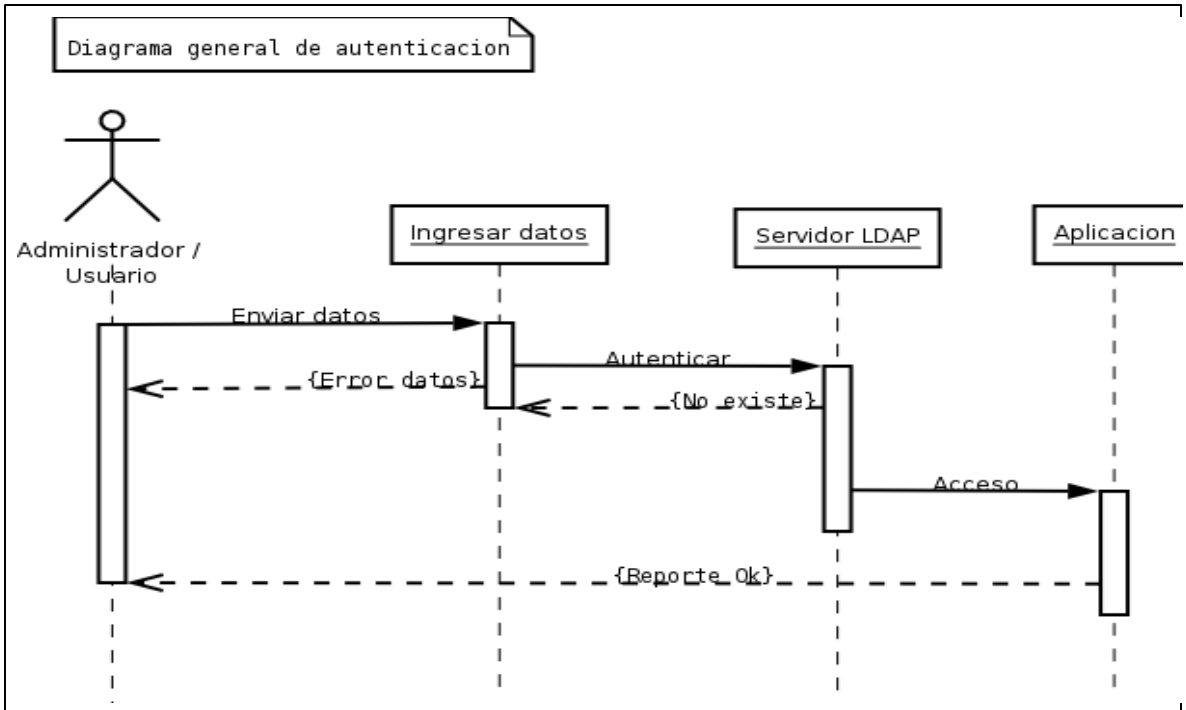


Figura 11: Secuencia general de autenticación incluido en iniciar sesión

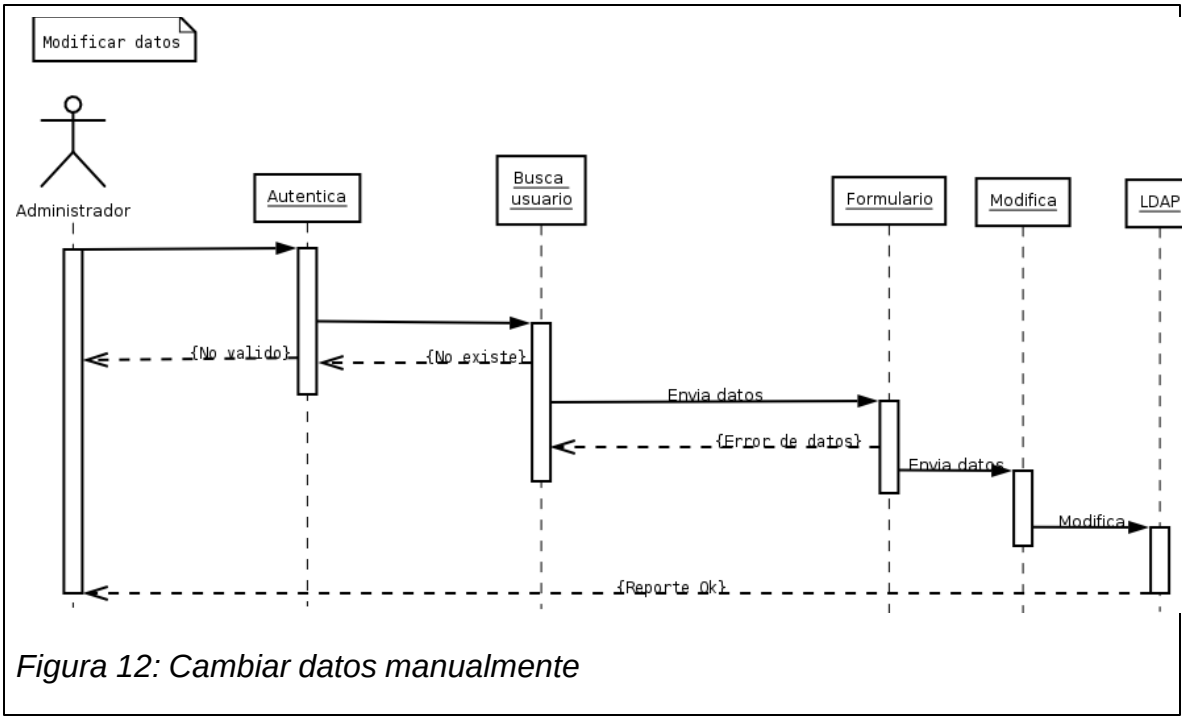


Figura 12: Cambiar datos manualmente

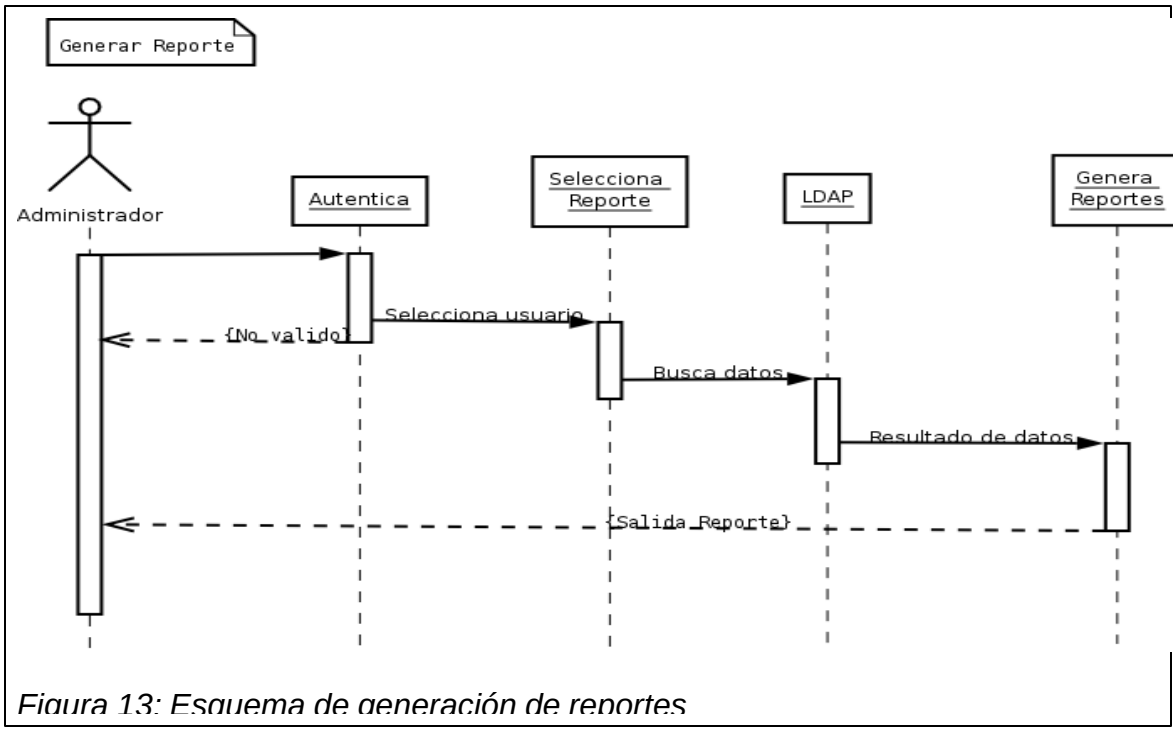


Figura 13: Esquema de generación de reportes

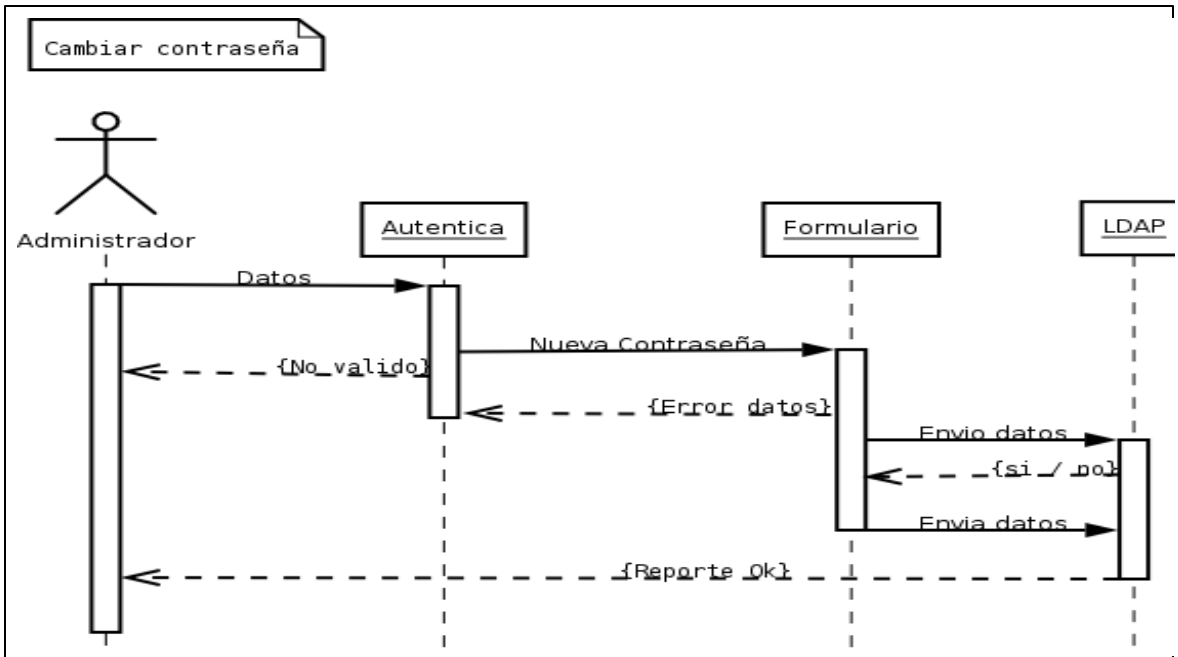


Figura 14: Esquema para el proceso de cambio de clave

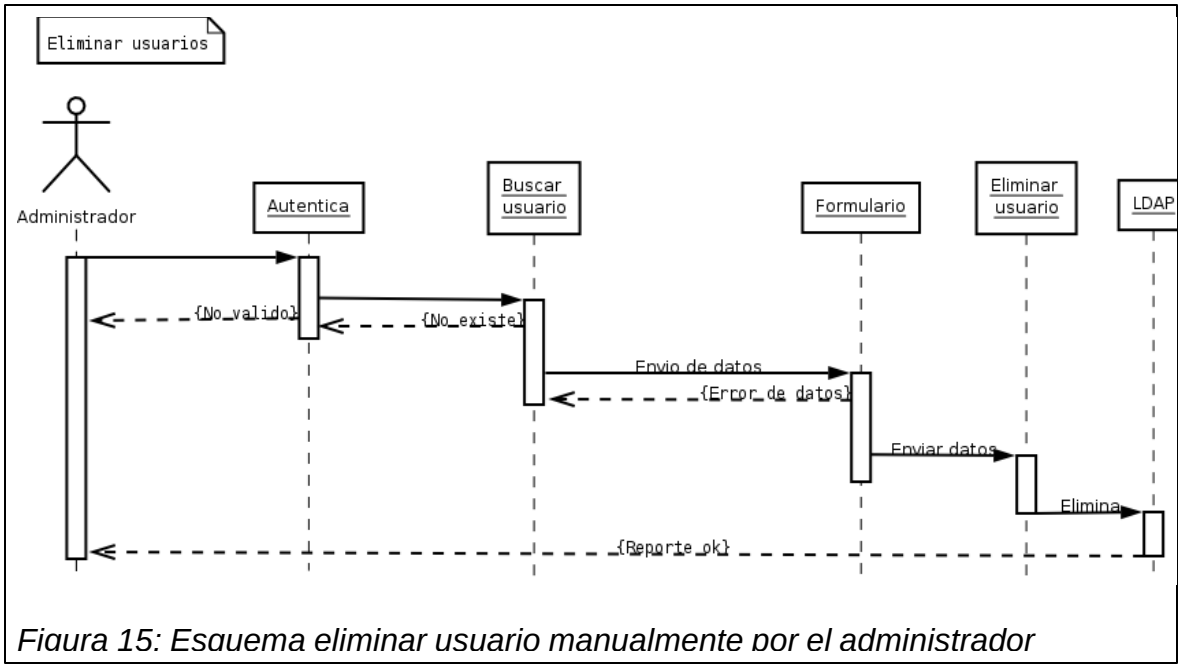


Figura 15: Esquema eliminar usuario manualmente por el administrador