ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN TECNOLÓGICA

DISEÑO E IMPLEMENTACIÓN DE UN SERVIDOR DE CORREO ELECTRÓNICO SEGURO, WEBMAIL, Y GESTOR DE USUARIOS OPENLDAP PARA LA CARRERA DE TECNOLOGÍA EN ANÁLISIS DE SISTEMAS INFORMÁTICOS.

PROYECTO PREVIA A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS.

EDISON MAURICIO AYO SIMBAÑA

DIRECTOR: ING. CESAR GALLARDO

Quito: enero 2007

DECLARACIÓN

Yo EDISON MAURICIO AYO SIMBAÑA, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Ayo Simbaña Edison Mauricio

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por AYO SIMBAÑA EDISON MAURICIO, bajo mi supervisión.

Ing. Cesar Gallardo

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Mi mas sincero agradecimiento a Dios, por ofrecerme la gracia divina

de cada día poder levantarme y ver la luz, por haberme encontrado guías que marcaron diferentes etapas en mi vida, por haberme otorgado fuerza, valor y sabiduría para enfrentar mis metas, cumplirlas y seguir adelante.

Edison Mauricio Ayo Simbaña

DEDICATORIA

A mis padres, José María Ayo Chuquimarca y Rosa María de Lourdes Simbaña Iza; que con su enseñanza diaria, compresión y amor marcaron de mejor manera el camino por el que tengo que seguir.

A mis hermanos, Angelica, Carlos, Maribel y Daniel; por ser ellos quienes me impulsan cada día a seguir superándome.

A mis amigos, los que gracias a Dios están todavía presentes y los que se adelantaron al encuentro de nuestro creador; por dejar marcas profundas, y sabias enseñanzas que las llevare conmigo hasta el fin de los días.

Y a todos quienes sin mencionarlos me brindaron el apoyo directa o indirectamente.

Edison Mauricio Ayo Simbaña

CONTENIDO

CAPITULO I

CAPITULO II

CAPITULO III

INTRODUCCIÓN.

Actualmente la carrera de Tecnología en Análisis y Diseño de Sistemas Informáticos, no tiene en funcionamiento ningún sistema de correo electrónico que provea de este servicio a los usuarios (docentes y comunidad estudiantil) de la carrera. Es por tal motivo que este proyecto prevé el diseño e implementación de un servidor de correo electrónico seguro, acorde a las necesidades y/o políticas que requiera la organización estableciendo normas de seguridad, confiabilidad e integridad en la entrega y recepción de mensajes (e-mail) entre los usuarios.

Este servidor de correo electrónico esta en la capacidad de ofrecer el servicio a los estudiantes, docentes y personal administrativo de la carrera, que requieran el servicio, además el servidor esta configurado para poder ser administrado de forma fácil y segura.

Los usuarios tendrán soporte en sus respectivas cuentas de correo electrónico por medio de certificados digitales en las conexiones, autentificación de usuarios, soporte para el control de virus, spam y fraudes electrónicos.

CAPITULO 1

1.1 PLANTEAMIENTO DEL PROBLEMA.

Actualmente existe un aumento creciente de la necesidad de transmitir información confidencial y sensitiva vía Correo Electrónico, entre las instituciones educativas y la comunidad estudiantil; con la finalidad de reducir el uso de papel y agilizar los procesos en la toma de decisiones.

Es así que en la mayoría de centros de educación superior, el correo electrónico se ha convertido en el medio de transmisión de información, prácticamente estándar a diferentes niveles de dicha organización; sin embargo existen una serie falencias de configuración y mantenimiento que están provocando que el correo electrónico pasé de ser una herramienta de intercambio de información basada en el respeto de los usuarios a las normas de buena conducta; a ser cada vez más, el medio que se utiliza para acciones no deseadas: envíos masivos de mensajes no solicitados "Spam"[1], envío de mensajes con código malicioso "Virus Informáticos"[2], vehículo de mensajes anónimos o con el remitente falsificado, etc. Estas acciones degradan el servicio y afectan negativamente a la imagen de la organización de la que parten dichos mensajes.

No esta por demás, que los usuarios de correo electrónico demanden un servicio de calidad en el que esas acciones no deseadas se reduzcan al mínimo posible. Por ello han surgido servidores de "Listas Negras" que señalan aquellos servidores de correo cuya

1 Información detallada en el Capitulo: 2.1.8.3 Spam.
2 Información detallada en el Capitulo: 2.1.8.1 Virus Informáticos.

configuración no cumplen determinadas normas. Cada vez se emplean más estas listas como medio de rechazar mensajes provenientes de lugares sospechosos[3]. Además de estas opciones se han desarrollado nuevas tecnologías de seguridades informáticas como el "Smtp Secure"[4] que ofrecen servicios adicionales para minimizar el uso abusivo de este servicio de comunicación.

Actualmente el Laboratorio de Tecnologías Informáticas "LTI" tiene implementado este servicio de comunicación, pero esta fuera de servicio. Sin embargo luego de haber escaneado los registros del sistema de correo "maillog"[5] y de proceder con las respectivas pruebas de funcionamiento; estas presentaron falencias de configuración, autenticación y seguridad en el sistema instalado. Los mas importantes recaen en los siguientes puntos:

- Falta de un sistema para el control de Spam actualizado.
- Falta de un sistema para el control de Virus actualizado.
- Problemas para administrar usuarios de correo (crear, actualizar, borrar).
- Interfaz web no actualizada para manipulación de correos (enviar, recibir).
- Falta de actualización, mantenimiento y soporte del sistema.

1.2 FORMULACIÓN Y SISTEMATIZACIÓN DEL PROBLEMA.

1.2.1 FORMULACIÓN.

¿Como se pueden aprovechar las nuevas tecnologías que los servidores de correo electrónico "MailServer", ofrecen y promueven de cara a identificar a las personas y/o empresas que generan dichos mensajes de correo electrónico masivo conocido como spam y ofrecer un servicio mas seguro, óptimo y controlado para los estudiantes de la

3 Concepto basado del Informe: Autenticación de clientes SMTP, B. Pérez y Pascual Pérez.
4 Correo Seguro: http://www.unizar.es/sicuz/correo/mail_pgp.html?menu=correo
5 Registro de sucesos y funcionamiento del sistema de correo electrónico en sistemas GNU/Linux.

carrera de Tecnología en Diseño de Sistemas Informáticos?.

1.2.2 **SISTEMATIZACIÓN.**

¿Cual sera el servidor de correo "MTA"[6]?

¿Como autenticar y certificar las conexiones de los usuarios de correo?

¿Como controlar el correo basura "Spam", manteniendo estándares óptimos y seguros que no afecten a los usuarios finales?

¿Como controlar que los usuarios finales de correo estén libres de virus informáticos y mantengan informados a los remitentes de dichos mensajes?

¿Cual sera el servidor de correo "POP3 – IMAP[7]"?

¿Que sistema se utilizara para manipular los correos?

¿Como administrar el sistema en lo que se refiere a: usuarios y actualizaciones?

1.3 **OBJETIVOS.**

1.3.1 **OBJETIVO GENERAL.**

Diseñar e Implementar un sistema de correo electrónico seguro para la carrera de Análisis de Sistemas Informáticos; que garantice tres conceptos básicos; Confidencialidad, Autenticación e Integridad. Y que además permita establecer políticas de control, seguridad y mantenimiento del sistema.

1.3.2 **OBJETIVOS ESPECÍFICOS.**

- Instalar y configurar el servidor de correo MTA "Postfix"[8], que se encargará de la entrega y recepción de correos.

---

6 Información detallada en el Capitulo: 2.1.7.4 MTA.
7 Información detallada en el Capitulo: 2.1.7.2 Protocolos
8 Postfix MTA http://www.postfix.org

- Controlar las conexiones por medio de certificados digitales y el abuso del sistema mediante un excelente gestor de usuarios como lo es “OpenLDAP”[9] que en conjunto con el uso de librerías “SASL”[10]; verificaran si el usuario existe al momento de enviar o recibir los correos.
- Entregar los correos del servidor por medio del software “Dovecot”[11] y el uso de protocolos POP3 o IMAP acordes a la conexión del usuario.
- Instalar y configurar “MailScanner”[12], que identificará si éste mensaje tiene algún código malicioso o si alguno de sus archivos adjuntos pueden dañar el sistema.
- Configurar a la medida el software “SpamAssassin”[13], que en conjunto a otras aplicaciones enlazadas directamente a Internet mantendrán controlado el Spam que pretenda ingresar y pueda ser marcado antes del ingreso al buzón del usuario.
- Manipular los correos mediante el sistema “SquirrelMail”[14] que está diseñado de la forma más amigable posible, y como su código está orientado a la WEB no existe ningún problema para el uso de éste; sea en sistemas propietarios (Windows o Mac) o sistemas de libre distribución (GNU con Linux)[15].
- Administrar el sistema en lo referente a usuarios, mediante aplicativos Web “phpLDAPadmin”[16] con interfaces gráficas amigables que permitan que el sistema sea operativo por el administrador.

9 Protocolo de Acceso Liviano a Directorios http://www.openldap.org
10 Librerías de autenticación SASL http://asg.web.cmu.edu./sasl/
11 Courier POP/IMAP http://www.dovecot.org
12 Control de Virus http://www.mailscaner.info
13 Control de Spam http://www.spamassassin.org
14 Gestor de correo Webmail http://www.squirremail.org
15 Información detallada en el Capitulo: 2.1.1 (GNU con Linux).
16 Administrador Web de usuarios openLDAP http://phpldapadmin.sorceforge.net

1.4 JUSTIFICACIÓN DEL PROYECTO.

1.4.1 JUSTIFICACIÓN TEÓRICA.

Conseguir un sistema de correo electrónico totalmente funcional y de alto rendimiento que use un completo abanico de modernas tecnologías como son: OpenLDAP, MailScanner, Postfix, etc y técnicas como: autenticación y certificación; que mejoren su eficiencia, robustez, flexibilidad y seguridad. De igual forma proporcionar en lo posible aplicaciones para el fácil uso y mantenimiento del sistema.

1.4.2 JUSTIFICACIÓN METODOLÓGICA.

El aporte principal de este proyecto es mantener un sistema de comunicación y transmisión segura de información entre "estudiante - docente – estudiante", y con el sistema ya implantado dar a conocer el funcionamiento de nuevas tecnologías acerca de servidores de correo electrónico, los mismos que quedan a expensas del conocimiento de los estudiantes de la carrera y por ende proponer nuevos tópicos de estudio.

1.4.3 JUSTIFICACIÓN PRACTICA.

Asegurar que los mensajes de correos electrónicos lleguen a los buzones correspondientes de cada usuario, con la certeza de que estos correos fueron previamente clasificados, revisados y limpiados, estableciendo políticas de fiabilidad, autenticidad e integridad.

CAPITULO 2

2.1 GENERALIDADES.

El proyecto como tal prevé orientar a los estudiantes de la carrera y futuros administradores de redes en tópicos sobre nuevas técnicas y herramientas de Seguridades Informáticas para el diseño, implementación y correcta administración de clusters[17] GNU con Linux que operasen como servidores de Correo Electrónico; además, establecer pautas para contrarrestar de la forma más eficaz y eficientemente posible, problemas crecientes para este servicio, conocidos como: “Virus y Spam”.

Además, dado el caso que el proyecto en su totalidad ha sido diseñado, desarrollado, implementado, probado y documentado en sistemas GNU con Linux con sus referentes en: CentOS[18] (por ser una distribución que forma parte de la familia de RedHat y su uso esta mas orientada a servidores en producción) y Ubuntu[19] (por incorporar interfaces mas amigables con el usuario final y estar orientado a estaciones de trabajo, para la documentación); el proyecto prevé orientar a los usuarios el uso diario del Software Libre y los beneficios que este trae consigo.

2.1.1 SOFTWARE LIBRE[20].

“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:

17 http://es.wikipedia.org/wiki/Cluster_(inform%c3%A1tica)
18 Sistema Operativo CentOS http://www.centos.org
19 Ubuntu Linux http://www.ubuntu-es.org
20 Información obtenida del sitio Web: http://www.gnu.org/philosophy/free-sw.es.html

- La libertad de usar el programa, con cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.
- La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).
- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. (libertad 3). El acceso al código fuente es un requisito previo para esto.

Un programa es software libre si los usuarios tienen todas estas libertades. Así pues, deberías tener la libertad de distribuir copias, sea con o sin modificaciones, sea gratis o cobrando una cantidad por la distribución, a cualquiera y a cualquier lugar. El ser libre de hacer esto significa (entre otras cosas) que no tienes que pedir o pagar permisos.
También tener la libertad de hacer modificaciones y utilizarlas de manera privada en tu trabajo u ocio, sin ni siquiera tener que anunciar que dichas modificaciones existen.

La libertad para usar un programa significa la libertad para cualquier persona u organización de usarlo en cualquier tipo de sistema informático, para cualquier clase de trabajo, y sin tener obligación de comunicárselo al desarrollador o a alguna otra entidad específica.

La libertad de distribuir copias debe incluir tanto las formas binarias o ejecutables del programa como su código fuente, sean versiones modificadas o sin modificar (distribuir programas de modo ejecutable es necesario para que los sistemas operativos libres sean fáciles de instalar). Está bien si no hay manera de producir un binario o ejecutable de un programa concreto (ya que algunos lenguajes no tienen esta capacidad), pero debe tener la libertad de distribuir estos formatos, si encontrara o desarrollara la manera de crearlos.

Para que las libertades de hacer modificaciones y de publicar versiones mejoradas tengan sentido, debe tener acceso al código fuente del programa. Por lo tanto, la posibilidad de acceder al código fuente es una condición necesaria para el software libre.

Para que estas libertades sean reales, deben ser irrevocables mientras no hagas nada incorrecto; si el desarrollador del software tiene el poder de revocar la licencia aunque no le hayas dado motivos, el software no es libre.

Así pues, quizás hayas pagado para obtener copias de software GNU, o tal vez las hayas obtenido sin ningún coste. Pero independientemente de cómo hayas conseguido tus copias, siempre tienes la libertad de copiar y modificar el software, e incluso de vender copias.

“Software Libre” no significa “no comercial”. Un programa libre debe estar disponible para uso comercial y distribución comercial. El desarrollo comercial del software libre ha dejado de ser inusual; el software comercial libre es muy importante. Es aceptable que haya reglas acerca de cómo empaquetar una versión modificada, siempre que no bloqueen a consecuencia de ello la libertad de publicar versiones modificadas.

Los desarrolladores de software no tienen el poder de eliminar o sobrepasar estas restricciones, pero lo que pueden y deben hacer es rehusar el imponerlas como condiciones de uso del programa. De esta manera, las restricciones no afectarán a actividades y gente fuera de las jurisdicciones de estos gobiernos.

Para decidir si una licencia de software concreta es una licencia de software libre, lo juzgamos basándonos en estos criterios para determinar si tanto su espíritu como su letra en particular los cumplen. Si una licencia incluye restricciones contrarias a nuestra ética,

la rechazamos, aun cuando no hubiéramos previsto el problema en estos criterios. A veces un requisito de una licencia plantea una situación que necesita de una reflexión minuciosa, e incluso conversaciones con un abogado, antes de que podamos decidir si la exigencia es aceptable. Cuando llegamos a una conclusión, a veces actualizamos estos criterios para que sea más fácil ver por qué ciertas licencias se pueden calificar o no como de software libre.

No debe confundirse software libre con software de dominio público. Este último es aquel por el que no es necesario solicitar ninguna licencia y cuyos 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. El software sería aquél cuyo autor lo dona a la humanidad o cuyos derechos de autor han expirado. Si un autor condiciona su uso bajo una licencia, por muy débil que sea, ya no es de dominio público.

2.1.2 **GNU CON LINUX.**

2.1.2.1 **Gnu's Not Unix (GNU).**

El proyecto GNU fue lanzado en 1984 para desarrollar un completo sistema operativo tipo UNIX, bajo la filosofía del software libre el sistema GNU. Las variantes del sistema GNU que utilizan el núcleo llamado Linux, son utilizadas ampliamente en la actualidad; aunque a menudo estos sistemas se refieren como “Linux”, deben ser llamados sistemas GNU con Linux.[21]

2.1.2.2 **Linux.**

Es la denominación de un sistema operativo, pero su nombre esta mas orientado al núcleo (kernel) de sistemas GNU con Linux. Es uno de los paradigmas del desarrollo de

21 Información obtenida del sitio Web: http://www.gnu.org/home.es.html

software libre (y de código abierto), donde el código fuente está disponible públicamente y cualquier persona, con los conocimientos informáticos adecuados, puede libremente estudiarlo, usarlo, modificarlo y redistribuirlo.[22]

2.1.3 **DISTRIBUCIONES GNU CON LINUX[23].**

Una distribución GNU con Linux (abreviada con frecuencia distro) es un conjunto de aplicaciones reunidas que permiten brindar mejoras para instalar fácilmente un sistema GNU con Linux. Son "sabores" de GNU con Linux que, en general, se destacan por las herramientas para configuración y sistemas de paquetes de software a instalar.

Existen numerosas distribuciones Linux. Cada una de ellas puede incluir cualquier número de software adicional (Libre o no), como algunos que facilitan la instalación del sistema y una enorme variedad de aplicaciones, entre ellos, entornos gráficos, suites ofimáticas, servidores web, servidores de correo, servidores FTP, etcétera.

La base de cada distribución incluye el núcleo Linux, con las bibliotecas y herramientas del proyecto GNU y de muchos otros proyectos/grupos de software, como BSD.

Usualmente se utiliza la plataforma Xfree86 o la X.ORG para sostener interfaces gráficas.

Ahora las grandes distribuciones: RedHat, SuSE, Caldera, Mandrake, Corel Linux, TurboLinux; son potentes empresas que compiten entre sí por incluir el último software, a veces también software propietario, con instalaciones gráficas capaces de auto detectar el hardware que instalan un sistema entero en unos cuantos minutos sin apenas varias preguntas.

Entre las distribuciones de GNU con Linux, destaca el proyecto Debian/GNU[24]. Debian nace como una iniciativa no comercial de la FSF[25], aunque luego se independiza de ésta

22 Concepto obtenido del sitio Web: http://es.wikipedia.org/wiki/Linux
23 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/Distribuci%C3%B3n_Linux
24 Debian GNU/Linux http://www.debian.org
25 Free Software Foundation http://www.fsf.org

y va más allá del propio sistema GNU con Linux. Es la única de las grandes distribuciones que no tiene intereses comerciales ni empresariales. Son sus propios usuarios, muy activos, quienes mantienen la distribución de modo comunitario, incluidas todas sus estructuras de decisión y funcionamiento. Su objetivo es recopilar, difundir y promover el uso del software libre. Reúne el mayor catálogo de software libre, todos ellos probados, mantenidos y documentados por algún desarrollador voluntario.[26]

En una distribución hay todo el software necesario para instalar en un ordenador personal; servidor, correo, ofimática, fax, navegación de red, seguridad, etc.

2.1.3.1 **Distribuciones no comerciales.**

- Aurox (basada en Red Hat Linux).
- Debian (x86/PPC).
- CentOS (basada en Red Hat Enterprise Linux).
- Fedora Core (x86/PPC) (basada en Red Hat Linux).
- Gentoo Linux (x86/PPC).
- Knoppix (basada en Debian, de tipo CD autónomo).
- Kubuntu (x86/PPC/x86-64) (Ubuntu con KDE).
- Mandriva Linux (x86/PPC/x86-64) (antes Mandrake Linux).
- Slackware.
- Slax (Live basada en Slackware)
- OpenSuSE.
- Ubuntu (x86/PPC/x86-64) (basada en Debian)
- White Box (basada en Red Hat Enterprise Linux)
- Ututo XS (distribución 100% libre creada en Argentina por el Proyecto UTUTO con repositorios compilados para diversos procesadores Intel y AMD)
- Y cientos de distribuciones mas...

26 Información obtenida del sitio Web: http://gugs.sindominio.net/faqs/faqlinux.html

2.1.4 **UBUNTU**[27]**.**

Linux for human beings, es una distribución de Linux que ofrece un sistema operativo predominante enfocado a ordenadores de escritorio. Basada en Debían GNU con Linux . El proyecto Ubuntu está construido sobre las ideas expresadas en el Manifiesto Ubuntu: que el software debe estar disponible de forma gratuita, que las herramientas de software deben poder ser utilizadas por la gente en su idioma local, y que la gente debe tener la libertad de personalizar y alterar su software de la manera que necesiten. Por esos motivos:

- Ubuntu siempre será gratuito, y no habrá un coste adicional para la edición empresarial; hacemos que lo mejor de nuestro trabajo esté disponible para todos bajo los mismos términos de libertad.
- Ubuntu viene con un completo soporte profesional en términos comerciales de cientos de compañías de todo el mundo, en caso de que necesite de dichos servicios. Cada nueva versión de Ubuntu recibe actualizaciones gratuitas de seguridad durante 18 meses después de su publicación; algunas versiones incluso están soportadas durante más tiempo.
- Ubuntu usa lo mejor en infraestructura de traducciones y accesibilidad que la comunidad del Software Libre es capaz de ofrecer, para hacer que Ubuntu sea utilizable por el mayor número de personas posible.
- Ubuntu se publica regular y predeciblemente; se publica una nueva versión cada seis meses. Puede usar la versión estable actual o ayudar a mejorar la versión de desarrollo actual.
- La comunidad Ubuntu sigue enteramente los principios del desarrollo de software libre; invitamos a la gente a que use software de fuentes abiertas, lo mejore y lo

27 Conceptos tomados de la ayuda del Sistema Ubuntu/Linux F1.

difunda.[28]

2.1.4.1 **Características de Ubuntu[29].**

- Basada en la distribución Debian.
- Disponible en 4 arquitecturas: intel x86, AMD64, PowerPC, SPARC.
- Los desarrolladores de Ubuntu se basan en gran medida en el trabajo de la comunidades de Debian y Gnome.[30]
- Las versiones estables se liberan cada 6 meses y se mantienen actualizadas en materia de seguridad hasta 18 meses después de su lanzamiento.
- La nomenclatura de las versiones no obedece principalmente a un orden de desarrollo, se compone del dígito del año de emisión y del mes en que esto ocurre. La versión 4.10 es de octubre de 2004, la 5.04 es de abril de 2005, la 5.10 de octubre de 2005, la 6.06 es de junio de 2006 y la 6.10 es de octubre de 2006.
- El escritorio oficial es Gnome y se sincronizan con sus liberaciones.
- De forma sincronizada a la versión 6.06 de Ubuntu, apareció por primera vez las distribuciones Kubuntu y Xubuntu, basados en los entornos de escritorios KDE[31] y Xfce.
- El navegador web oficial es Mozilla Firefox.
- El sistema incluye funciones avanzadas de seguridad y entre sus políticas se encuentra el no activar, de forma predeterminada, procesos latentes al momento de instalarse. Por eso mismo no hay un firewall[32] predeterminado, ya que no existen servicios que puedan atentar a la seguridad del sistema.
- Para labores/tareas administrativas incluye una herramienta llamada sudo (similar

28 Conceptos tomados de la ayuda del Sistema Ubuntu/Linux F1.
29 Información obtenida del sitio Web: http://www.ubuntu-es.org/ubuntu/introduccion
30 Entorno gráfico para escritorio con sistemas GNU/Linux http://www.gnome.org
31 Entorno gráfico para escritorio con sistemas GNU/Linux http://www.kde.org
32 Firewall Pared de fuego, programa especializado para permitir o negar el acceso al Internet.

al Mac OS X[33]), con la que se evita el uso del usuario root[34].

- Mejorar la accesibilidad y la internacionalización, de modo que el software esté disponible para tanta gente como sea posible.
- Todos los lanzamientos de Ubuntu se proporcionan sin costo alguno. Los Cds de la distribución se envían de forma gratuita a cualquier persona. También es posible descargar las imágenes ISO de los discos por transferencia directa o bajo la tecnología Bittorrent.

2.1.5 **CENTOS.**

CentOS (acrónimo de **C**ommunity **ENT**erprise **O**perating **S**ystem) es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de Red Hat Enterprise Linux.

2.1.6 **CORREO ELECTRÓNICO.**

2.1.6.1 **Introducción.**

Fue creado por Ray Tomlinson en 1971, aunque no lo consideró un invento importante. Su gran difusión promueve servicios para chequear una cuenta POP desde cualquier navegador. El texto del primer mensaje enviado por e-mail fue algo así como "QWERTYUIOP" (teclas pulsadas al azar en el teclado por razones de pruebas) según su inventor y fue enviado a través de un programa llamado SNDMSG que él escribió. El invento se estaba terminando en 1971 cuando Tomlinson, un ingeniero de la firma Bolt Beranek y Newman, contratada por el gobierno de los Estados Unidos para construir la red Arpanet (la precursora de Internet), tuvo la idea de crear un sistema para enviar y recibir mensajes por la red.

---

33 Mac OS X: es el actual sistema operativo de la familia de ordenadores Macintosh.
34 Usuario en sistemas GNU/Linux con privilegios de Administración.

Tomlinson había escrito un programa para que los desarrolladores de la Arpanet se dejaran mensajes en las computadoras que compartían (15 en toda la red nacional). Jugando con otro protocolo para transferir archivos entre las máquinas diseminadas por la red, notó que juntos podían usarse para acceder a todas las casillas de correo.[35]

El Correo electrónico, o en ingles e-mail, (electronic mail) es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos (normalmente por Internet). Esto lo hace muy útil comparado con el correo ordinario, pues es más barato y rápido. Junto con los mensajes también pueden ser enviados ficheros como paquetes adjuntos.[36]

A diferencia del correo postal que se reparte a domicilio por un servicio postal (cartero), el correo electrónico se envía, a través de una red de ordenadores (estafetas), hasta el ordenador donde reside el buzón de la persona a quien va dirigido.[37]

2.1.6.2 **Correo Web.**

Webmail permite enviar y recibir correos mediante una página WEB diseñada para ello, y por tanto usando sólo un programa navegador WEB. La alternativa es usar un programa de correo especializado. El correo web es cómodo para mucha gente, porque permite ver y almacenar los mensajes siempre en el mismo sitio (en un servidor remoto, accesible por la página web) en vez de en un ordenador personal concreto.

Como desventaja, es difícil de ampliar con otras funcionalidades, porque la página ofrece unos servicios concretos y no podemos cambiarlos. Además, suele ser más lento que un programa de correo, ya que hay que estar continuamente conectado a páginas web

35 Información obtenida del sitio Web: http://www.maestrosdelweb.com/editorial/emailhis/
36 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/Correo_electr%C3%nico_
37 Información obtenida del sitio Web: http://www.unizar.es/sicuz/correo/mail_pgp.html?menu=correo

(Internet) y leer los correos de uno en uno.

2.1.6.3 **Clientes de correo.**

También están los clientes de correo electrónico que son programas para gestionar los mensajes recibidos y poder escribir nuevos.

Por el contrario, necesitan que el proveedor de correo ofrezca este servicio, ya que no todos permiten usar un programa especializado (algunos sólo dan correo web). En caso de que sí lo permita, el proveedor tiene que explicar detalladamente cómo hay que configurar el programa de correo. Esta información siempre está en su página web, ya que es imprescindible para poder hacer funcionar el programa, y es distinta en cada proveedor. Entre los datos necesarios están: tipo de conexión (POP o IMAP), dirección del servidor de correo, nombre de usuario y contraseña. Con estos datos, el programa ya es capaz de obtener y descargar nuestro correo.

El funcionamiento de un programa de correo es muy diferente al de un correo web, ya que un programa de correo descarga de golpe todos los mensajes que tenemos disponibles, y luego pueden ser leídos sin estar conectados a Internet (además, se quedan grabados en el ordenador). En cambio, en una página web se leen de uno en uno, y hay que estar conectado a la red (Internet) todo el tiempo.

Algunos ejemplos de programas de correo son Mozilla Thunderbird, Evolution, Outlook Express y Eudora.[38]

38 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/Correo_electr%C3%nico

2.1.7 **SERVIDORES DE CORREO ELECTRÓNICO.**

2.1.7.1 **Introducción.**

Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando. Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta.[39]

2.1.7.2 **Protocolos.**

2.1.7.2.1 **Simple Mail Transfer Protocol (SMTP).**

Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc).
Una de las limitaciones del SMTP original es que no facilita métodos de autenticación a los emisores, así que se definió la extensión SMTP – AUTH.

2.1.7.2.2 **Post Office Protocol (POP).**

POP ha sido diseñado para poder trabajar en modo "offline", sin necesidad de mantener una conexión permanente con el servidor. El buzón de correo se consulta a intervalos regulares. Para ello se hace una conexión con el servidor, se recoge cualquier nuevo mensaje llegado y se cierra la conexión.
El cliente, una vez recibidos los mensajes, los archiva en el ordenador local (MAC o PC) para que el usuario pueda leerlos, contestarlos, borrarlos o clasificarlos.
Esta filosofía de trabajo hace que el protocolo POP sea muy aconsejable en entornos en los que no es posible una conexión permanente a la red (acceso remoto vía telefónica,

39 Definición tomada del sitio Web: http://es.wikipedia.org/wiki/Servidor_de_correo

por ejemplo).

2.1.7.2.3 **Internet Message Access Protocol (IMAP).**

IMAP es un protocolo de acceso interactivo ("online") al buzón de correo. Los mensajes residentes en el buzón no son trasladados automáticamente al ordenador donde reside el cliente.

El cliente IMAP establece una conexión con el servidor, abre el buzón del usuario y da libertad para trabajar con cada uno de los mensajes allí almacenados. Se actúa directamente sobre el buzón en el servidor. Cualquier cambio quedara reflejado directamente en el buzón y no solamente en el ordenador personal del cliente. Esto facilita la gestión del correo a usuarios con mucha movilidad geográfica, pero obliga a estar permanentemente conectados a la red.[40]

2.1.7.3 **Funcionamiento[41].**

Un servidor de correo consta en realidad de dos servidores (programas informáticos) instalados en una sola estación o Cluster: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario (como el caso de Mozilla Mail, Evolution, Microsoft Outlook). Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario; es el caso de los clientes vía web, como: Gmail, Hotmail, SquirrelMail, OpenWebmail o Terra. En ellos la arquitectura del servicio es más compleja.

---

40 Información obtenida del sitio Web: http://www.unizar.es/sicuz/correo/mail_pgp.html?menu=correo

41 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/Servidor_de_correo

2.1.7.4 **Mail Transport Agent (MTA).**

Es una sigla en inglés que significa Mail Transport Agent (Agente de Transporte de Correos), y también Message Transport Agent (Agente de Transporte de Mensajes).

En otras palabras, es el servicio de correo (SMTP) en sí y no la parte que usa el usuario para recuperar los mensajes que este recibió.

Algunos de los más conocidos son Sendmail, Postfix, Qmail, Exim y Microsoft Exchange Server.

2.1.7.4.1 **Postfix.**

Postfix es un Agente de Transporte de Correos (MTA) de código abierto, un programa informático para el enrutamiento y envío de correo electrónico.

2.1.7.5 **Servidores POP3/IMAP.**

Son servidores encargados de la entrega de correos a los clientes finales; sean estos mediante los protocolos POP3 (clientes de correo) o IMAP (Webmail), entre los mas destacados encontramos los siguientes: Courier, Dovecot, IMAP, POP3.

2.1.7.5.1 **Dovecot.**

Dovecot es un servidor de código abierto IMAP y POP3 para los sistemas de GNU con Linux/UNIX. Aunque está escrito en C, utiliza varias técnicas de codificación para evitar agujeros de seguridad.

2.1.8 **PROBLEMAS DEL CORREO ELECTRÓNICO.**

El principal problema actual es el Spam, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades.

Además del Spam, existen otros problemas que afectan a la seguridad y veracidad de

este medio de comunicación:

- Los virus informáticos, que se propagan mediante ficheros adjuntos infectando el ordenador de quien los abre.
- El phishing, que son correos fraudulentos que intentan conseguir información bancaria.
- Los engaños, que difunden noticias falsas masivamente.
- Las cadenas de correo electrónico, que consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye al Spam.[42]

2.1.8.1 **Virus informáticos[43].**

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus habitualmente reemplazan archivos ejecutables por otros infectados con el código de éste. Los virus pueden intencionalmente destruir datos en la computadora, aunque también existen otros más benignos, que sólo se caracterizan por ser molestosos.

Los virus informáticos tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple: ejecutando un programa infectado en la mayoría de las veces por desconocimiento del usuario, el código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma

42 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/Correo_electr%C3%nico
43 Información tomada del sitio Web: http://es.wikipedia.org/wiki/Virus_inform%c3%A1tico

entonces el control de los servicios básicos del sistema operativo, infectando los posteriores archivos ejecutables que sean llamados para su ejecución, añadiendo su propio código al del programa siendo este infectado y grabándolo en disco, con lo cual el proceso de replicado se completa.

2.1.8.2 **Clasificación de los virus.**

2.1.8.2.1 **Según lo infectado.**

Según algunos autores, fundamentalmente existen dos tipos de virus:

- Aquellos que infectan archivos. A su vez, éstos se clasifican en:
- Virus de acción directa. En el momento en el que se ejecutan, infectan a otros programas.
- Virus residentes. Al ser ejecutados, se instalan en la memoria de la computadora. Infectan a los demás programas a medida que se accede a ellos. Por ejemplo, al ser ejecutados.
- Los que infectan el sector de arranque (virus de boot).Recordemos que el sector de arranque es lo primero que lee el ordenador cuando es encendido. Estos virus residen en la memoria.

Existe una tercera categoría llamada multipartite, pero corresponde a los virus que infectan archivos y al sector de arranque, por lo que se puede decir que es la suma de las dos categorías anteriores.

Para otros autores, la clasificación de los virus también se divide en dos categorías, pero el método de clasificación utilizado es diferente:

- Virus de archivos, que modifican archivos o entradas de las tablas que indican el lugar donde se guardan los directorios o los archivos.
- Virus de sistema operativo, cuyo objetivo consiste en infectar aquellos archivos que gobiernan la computadora.

Existe una tercera clasificación, promovida por CARO[44], para unificar la forma de nombrar a los virus. En esta clasificación se atiende a la plataforma en la que actúa el virus y a algunas de sus características más importantes.

2.1.8.2.2 **Según su comportamiento.**

Los grupos principales (y más simples) de virus informáticos son:

- Kluggers: Aquellos virus que al entrar en los sistemas de otro ordenador y se reproducen o bien se encriptan de manera que tan sólo se les puede detectar con algún tipo de patrones.
- Viddbers: Aquellos virus que lo que hacen es modificar los programas del sistema del ordenador en el cual entran.

Además hay otros subgrupos de los anteriores grupos:

- Virus uniformes, que producen una replicación idéntica a sí mismos.
- Virus encriptados, que cifran parte de su código para que sea más complicado su análisis. A su vez pueden emplear:
- Encriptación fija, empleando la misma clave.
- Encriptación variable, haciendo que cada copia de sí mismo esté encriptada con una clave distinta. De esta forma reducen el tamaño del código fijo empleable para su detección.
- Virus oligomórficos, que poseen un conjunto reducido de funciones de encriptación y eligen una de ellas aleatoriamente. Requieren distintos patrones para su detección.
- Virus polimórficos, que en su replicación producen una rutina de encriptación completamente variable, tanto en la fórmula como en la forma del algoritmo. Con polimorfismos fuertes se requiere de emulación, patrones múltiples y otras técnicas antivirus avanzadas.

44 CARO http://es.wikipedia.org/wiki/CARO

- Virus metamórficos, que reconstruyen todo su cuerpo en cada generación, haciendo que varíe por completo. De esta forma se llevan las técnicas avanzadas de detección al límite. Por fortuna, esta categoría es muy rara y sólo se encuentran en laboratorio.
- Sobrescritura, cuando el virus sobrescribe a los programas infectados con su propio cuerpo.
- Stealth o silencioso, cuando el virus oculta síntomas de la infección.

2.1.8.3 **Spam**[45].

Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de spam incluyen grupos de noticias usenet, motores de búsqueda, wikis, foros y blogs. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

El spam mediante el servicio de correo electrónico nació el 5 de marzo de 1994. Este día, una firma de abogados de Canter and Siegel, publica en Usenet un mensaje de anuncio de su firma legal, el cual en el primer día después de la publicación, facturó cerca de 10.000 dólares por casos de sus amigos y lectores de la red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

El spam por medio del fax (spam-fax), es otra de las categorías de esta técnica de marketing directo, y consiste en enviar faxes masivos y no solicitados a través de sistemas electrónicos automatizados hacia miles de personas o empresas cuya información ha sido cargada en bases de datos segmentadas según diferentes variables.

45 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/Spam

2.1.8.4 **Spam por correo electrónico.**

El correo electrónico es, con diferencia, el medio más común de spamming en Internet. Involucra enviar mensajes idénticos o casi idénticos a un gran número de direcciones. A diferencia de los correos electrónicos comerciales legítimos, el spam generalmente es enviado sin el permiso explícito de los receptores, y frecuentemente contiene varios trucos para sortear los filtros de spam. Las computadoras modernas generalmente vienen con cierta capacidad para enviar spam. El único ingrediente necesario es la lista de direcciones objetivo.

2.1.8.5 **Técnicas de Spam.**

2.1.8.5.1 **Obtención de direcciones de correo.**

Los spammers (individuos o empresas que envían spam) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren Internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el spam son:

- Las propias páginas web, que con frecuencia contienen la dirección de su creador, o de sus visitantes (en foros, weblogs, etc.).
- Los grupos de noticias de usenet, cuyos mensajes suelen incluir la dirección del remitente.
- Listas de correo: les basta con apuntarse e ir anotando las direcciones de sus usuarios.
- Correos electrónicos con chistes, cadenas, etc. que los usuarios de Internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular

docenas de direcciones en el cuerpo del mensaje, pudiendo ser capturadas por un troyano o, más raramente, por un usuario malicioso.

- Páginas en las que se solicita tu dirección de correo (o la de "tus amigos" para enviarles la página en un correo) para acceder a un determinado servicio o descarga.
- Compra de bases de datos de direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).
- Entrada ilegal en servidores.
- Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales.

2.1.8.5.2 **Envío de los mensajes.**

Una vez que tienen una gran cantidad de direcciones de correo válidas (en el sentido de que existen), los spammers utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) y en general a Internet, por consumirse gran parte del ancho de banda en mensajes basura.

2.1.8.5.3 **Verificación de la recepción.**

Además, es frecuente que el spammer controle qué direcciones funcionan y cuáles no por medio de web bugs o pequeñas imágenes o similares contenidas en el código HTML del mensaje. De esta forma, cada vez que alguien lee el mensaje, su ordenador solicita la imagen al servidor del spammer, que registra automáticamente el hecho. Son una forma más de spyware. Otro sistema es el de prometer en los mensajes que enviando un mail a una dirección se dejará de recibirlos: cuando alguien contesta, significa no sólo que lo ha

abierto, sino que lo ha leído. Si recibe un correo no solicitado debe borrarlo sin leerlo.

2.1.8.5.4 **Troyanos y ordenadores zombis.**

Recientemente, han empezado a utilizar una técnica mucho más perniciosa: la creación de virus troyanos que se expanden masivamente por ordenadores no protegidos (sin cortafuegos). Así, los ordenadores infectados son utilizados por el spammer como "ordenadores zombis", que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros o correos nuevos en busca de más direcciones. Esto puede causar perjuicios al usuario que ignora haber sido infectado (que no tiene por qué notar nada extraño), al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que no se le deje acceder a determinadas páginas o servicios.

2.1.8.5.5 **Servidores de correo mal configurados.**

Los servidores de correo mal configurados son aprovechados también por los spammer. En concreto los que están configurados como Open Relay. Estos no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos. Existen diferentes bases de datos públicas que almacenan los ordenadores que conectados directamente a Internet permiten su utilización por los spammers. El más conocido es la Open Relay DataBase.

2.1.9 **Multipurpose Internet Mail Extensions (MIME).**

(Extensiones de Correo Internet Multipropósito) son una serie de convenciones o especificaciones, utilizado en Internet con dos finalidades: de un lado, normalizar el intercambio de todo tipo de archivos (texto, audio, vídeo, etc.) En la Red; de forma transparente para el usuario y la otra, acabar con el problema de las transferencias de

texto internacional por e-mail.[46]

2.1.9.1 **MIME y E – MAIL.**

Como se ha señalado al tratar de los protocolos de transmisión utilizados en el correo electrónico, la porción de mensaje que vemos está completada con una cabecera en la que el sistema incluye información adicional algunas de estas "etiquetas" incluidas en cualquier mensaje.

- MIME-Version: 1.0 indica al programa de correo que se trata de un mensaje en dicho formato (es decir, que se ajusta a lo señalado en la RFC 1521.
- Content-Type: Indica que tipo de datos contiene el mensaje. Pueden encontrarse los siguientes:
- text/plain = solo texto.
- image = imágenes estáticas.
- video = imágenes dinámicas, puede incluir audio.
- audio = sonido.
- message. Significa que el contenido está configurado según el estándar RFC 822; esto puede ser usado para reexpedir mensajes.
- application se emplea para señalar que el contenido es para ser enviado a un programa externo, por ejemplo texto para una impresora PostScript.

Un mensaje también puede tener varias partes (multipart) con varios contenidos separados, incluso de tipos diferentes (texto, audio e imágenes). Incluso cada parte puede tener subpartes (ser a su vez multiparte), puesto que el formato MIME puede ser recursivo.

Content-type puede tener un subtipo, ambos separados por una barra inclinada /. Por ejemplo, image/gif es una imagen en formato GIF; el tipo es image y el subtipo gif. Finalmente, puede tener parámetros opcionales empezando por un punto y coma**;** Por

46 Información obtenida del sitio web: http://es.wikipedia.org/wiki/Multipurpose_Internet_Mail_Extensions

ejemplo, el parámetro charset= en Content-type: text/plain; charset=iso-8859-1, indica que el cuerpo del mensaje utiliza el juego de caracteres ISO-8859-1 (El juego de caracteres por defecto es US-ASCII).

- Content-transfer-encoding: Señala como ha sido codificado el mensaje para su transmisión por e-mail, de forma que pueda viajar sin problemas de que sea corrompido desde el destinatario al receptor a través de los agentes de correo (**MUA**s). Los tipos que pueden darse para esta etiqueta son los anteriormente definidos es decir: 7bit, quoted-printable, base64, 8bit y binary.[47]

2.1.10 **AUTENTICACIÓN Y CERTIFICACIÓN.**

2.1.10.1 **Simple Authentication Secure Layer (SASL)[48].**

SASL es un entorno de trabajo para autenticación y autorización en protocolos de Internet.

2.1.10.2 **Los mecanismos de SASL.**

Un mecanismo SASL se modela como una sucesión de retos y respuestas. Los mecanismos definidos por SASL incluyen:

- "EXTERNAL", aquí la autenticación está implícita en el contexto (para protocolos que ya usan IPsec (Internet Protocol Security) o TLS).
- "ANONYMOUS", para el acceso de invitados sin autentificar.
- "PLAIN", un mecanismo de contraseña simple en texto claro.
- Se prevé soportar los mecanismos GSSAPI en una familia de nomenclatura de mecanismos.

47 Información obtenida del sitio Web: http://www.zator.com/Internet/N_16.htm
48 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/SASL

2.1.10.3 **Los protocolos de uso SASL – enterados.**

Los protocolos definen su representación de intercambios SASL con un perfil. Un protocolo tiene un nombre de servicio como "LDAP" en un registro compartido con GSSAPI y Kerberos.

Entre los protocolos que ahora mismo usan SASL se incluyen IMAP, LDAP, POP3, SMTP y XMPP.

2.1.10.4 **Certificados digitales.**

Un certificado de clave pública es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada.

Los certificados de clave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado. La entidad identificada se denomina sujeto del certificado o subscriptor (si es una entidad legal como, por ejemplo, una persona).

Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora (Certification Authority o CA) que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca.

Es importante ser capaz de verificar que una autoridad certificadora ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la entidad certificadora después de autentificar la identidad de un sujeto, firma el certificado digitalmente.

Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes.[49]

---

49 Información obtenida del sitio Web: http://www.infocentre.gva.es/

2.1.10.5 **Certificados x.509.**

El formato de certificados X.509 es un estándar del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization / International Electrotechnical Commission) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios.

Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996.

Los elementos del formato de un certificado X.509 v3 son:

- Versión.- El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- Número de serie del certificado.- Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- Identificador del algoritmo de firmado.- Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- Nombre del emisor. Este campo identifica la CA que ha firmado y emitido el certificado.
- Periodo de validez. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- Nombre del sujeto. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el

mismo nombre si es para la misma entidad.

- Información de clave pública del sujeto. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- Identificador único del emisor. Este es un campo opcional que permite reutilizar nombres de emisor.
- Identificador único del sujeto. Este es un campo opcional que permite reutilizar nombres de sujeto.
- Extensiones.- Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:
- Tipo de extensión. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
- Valor de la extensión. Este sub-campo contiene el valor actual del campo.
- Indicador de importancia. Es un flag que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3:

- Limitaciones básicas. Este campo indica si el sujeto del certificado es una CA y el máximo nivel de profundidad de un camino de certificación a través de esa CA.
- Política de certificación. Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.
- Uso de la clave. Este campo restringe el propósito de la clave pública certificada, indicando, por ejemplo, que la clave sólo se debe usar para firmar, para la encriptación de claves, para la encriptación de datos, etc. Este campo suele

marcarse como importante, ya que la clave sólo está certificada para un propósito y usarla para otro no estaría validado en el certificado.

- El formato de certificados X.509 se especifica en un sistema de notación denominado sintaxis abstracta uno (Abstract Sintax One o ASN-1). Para la transmisión de los datos se aplica el DER (Distinguished Encoding Rules o reglas de codificación distinguible), que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales.

2.1.10.6 **Listas de anulación de certificados (CRLS).**

Los certificados tienen un periodo de validez que va de unos meses a unos pocos años. Durante el tiempo que el certificado es válido la entidad certificadora que lo generó mantiene información sobre el estado de ese certificado.

La información más importante que guarda es el estado de anulación, que indica que el periodo de validez del certificado ha terminado antes de tiempo y el sistema que lo emplee no debe confiar en él. Las razones de anulación de un certificado son varias: la clave privada del sujeto se ha visto comprometida, la clave privada de la CA se ha visto comprometida o se ha producido un cambio en la afiliación del sujeto (por ejemplo cuando un empleado abandona una empresa).

Las listas de anulación de certificados (Certification Revocation Lists o CRL) son un mecanismo mediante el cual la CA publica y distribuye información a cerca de los certificados anulados a las aplicaciones que los emplean. Una CRL es una estructura de datos firmada por la CA que contiene su fecha y hora de publicación, el nombre de la entidad certificadora y los números de serie de los certificados anulados que aun no han expirado.

Cuando una aplicación trabaja con certificados debe obtener la última CRL de la entidad que firma el certificado que está empleando y comprobar que su número de serie no está incluido en él.

Existen varios métodos para la actualización de CRLs:

- Muestreo de CRLs. Las aplicaciones acceden a la CA o a almacenes de archivos y copian el último CRL a intervalos regulares. La pega de este esquema es que durante el periodo entre actualizaciones del CRL podemos aceptar un certificado ya anulado, por lo que el periodo debe ser corto.
- Anuncio de CRLs. La entidad certificadora anuncia que ha habido un cambio en el CRL a las aplicaciones. El problema de este enfoque es el anuncio puede ser muy costoso y no sabemos que aplicaciones deben ser informadas.
- Verificación en línea. Una aplicación hace una consulta en línea a la CA para determinar el estado de revocación de un certificado. Es el mejor método para las aplicaciones, pero es muy costoso para la CA.

2.1.10.7 **Listas de anulación de certificados x.509.**

El formato de listas de anulación de certificados X.509 es un estándar del ITU-T y la ISO/IEC que se publicó por primera vez en 1988 como versión 1. El formato fue modificado para incluir campos de extensión, dando origen al formato X.509 v2 CRL.

Los campos básicos de un formato X.509 CRL (válidos para las versiones 1 y 2) son:

- Versión. Debe especificar la versión 2 si hay algún campo de extensión.
- Firma. El campo contiene identificador del algoritmo empleado para firmar la CRL.
- Nombre del generador. Este campo contiene el nombre de la entidad que ha generado y firmado la CRL.
- Esta actualización. Fecha y hora de la generación de la CRL.
- Próxima actualización. Indica la fecha y hora de la próxima actualización. El siguiente CRL puede ser generado antes de la fecha indicada pero no después de ella.
- Certificado del usuario. Contiene el número de serie de un certificado anulado.
- Fecha de anulación. Indica la fecha efectiva de la anulación.

Existe también un conjunto de campos de entrada de extensión en las CRLs X.509 v2, como el código de razón, que identifica la causa de la anulación: sin especificar, compromiso de clave, compromiso de la CA, cambio de afiliación, superado (el certificado ha sido reemplazado), cese de operación (el certificado ya no sirve para su propósito original), certificado en espera (el certificado está suspendido temporalmente) y elimina de la CRL (un certificado que aparecía en una CRL previa debe ser eliminado).

Adicionalmente también se ha añadido un conjunto de extensiones para las X.509v2 CRL con los mismos subcampos que en los certificados X.509v3. Estas extensiones permiten que una comunidad o entidad se defina sus propios campos de extensión privados.

2.1.10.8 **Autoridades certificadoras.**

Una autoridad certificadora es una organización fiable que acepta solicitudes de certificados de entidades, las valida, genera certificados y mantiene la información de su estado.

Una CA debe proporcionar una Declaración de Prácticas de Certificación (Certification Practice Statement o CPS) que indique claramente sus políticas y prácticas relativas a la seguridad y mantenimiento de los certificados, la responsabilidad de la CA respecto a los sistemas que emplean sus certificados y las obligaciones de los subscriptores respecto de la misma.

Las labores de un CA son:

- Admisión de solicitudes. Un usuario rellena un formulario y lo envía a la CA solicitando un certificado. La generación de las claves pública y privada son responsabilidad del usuario o de un sistema asociado a la CA.
- Autentificación del sujeto. Antes de firmar la información proporcionada por el sujeto la CA debe verificar su identidad. Dependiendo del nivel de seguridad deseado y el tipo de certificado se deberán tomar las medidas oportunas para la validación.

- Generación de certificados. Después de recibir una solicitud y validar los datos la CA genera el certificado correspondiente y lo firma con su clave privada. Posteriormente lo manda al subscriptor y, opcionalmente, lo envía a un almacén de certificados para su distribución.
- Distribución de certificados. La entidad certificadora puede proporcionar un servicio de distribución de certificados para que las aplicaciones tengan acceso y puedan obtener los certificados de sus subscriptores. Los métodos de distribución pueden ser: correo electrónico, servicios de directorio como el X.500 o el LDAP, etc.
- Almacenes de datos. Hoy en día existe una noción formal de almacén donde se guardan los certificados y la información de las anulaciones. La designación oficial de una base de datos como almacén tiene por objeto señalar que el trabajo con los certificados es fiable y de confianza.[50]

2.1.11 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

2.1.11.1 Descripción de LDAP.

LDAP ("Lightweight Directory Acces Protocol", en español Protocolo Ligero de Acceso a Directorios) es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

Se usó inicialmente como un Front-end o interfaz final para x.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

50 Información captada del documento en el sitio Web: http://people.debian.org/~sto/articulos_bei/BEI-2003-11/certificados_digitales.pdf

CAPITULO 3.

3.1 ASPECTOS METODOLÓGICOS.

La metodología a utilizarse en la "Implementación de un servidor de Correo Electrónico Seguro, Webmail y gestor de usuarios OpenLDAP", empleando autenticación de usuarios y certificados digitales en las conexiones, para proveer el servicio de correo electrónico a los estudiantes de la carrera de Tecnología en Diseño de Sistemas Informáticos de la Escuela Politécnica Nacional se lo dividió de la siguiente manera:

3.1.1 ANÁLISIS.

3.1.1.1 Correo seguro.

No hay nada más fácil que leer los correos de otras personas, ya que viajan desnudos por la Red. Valga la siguiente analogía. Un correo electrónico normal es como una tarjeta postal sin sobre, que puede leer todo el que tenga interés. Por consiguiente, la mejor manera de preservar la intimidad en los mensajes de correo electrónico es recurrir a la criptografía. Esto se lo realiza por medio de potentes técnicas criptográficas, el contenido del mensaje pude ser enviado cifrado, permitiendo así que sólo el destinatario legítimo del correo sea capaz de leerlo. Con este mecanismo se garantiza la confidencialidad del correo. Sin embargo, los modernos sistemas de seguridad del correo, no se limitan a cifrar el contenido de los mensajes intercambiados, sino que también añaden otros servicios, como la integridad, que garantiza que el contenido del mensaje no ha sido alterado por el camino; la autenticación de usuarios, que asegura la identidad del

remitente del correo; la certificación de conexiones, que autorizan el uso del servicio, de manera que podemos estar seguros de que fue escrito por quien lo envió y no ha sido falsificado.[51]

3.1.1.2 **Funciones del correo seguro.**

Las funciones básicas para un sistema de correo electrónico seguro denotan en los siguientes normas de seguridad:

- Autentificación de usuarios, que permite a un usuario sea identificado en la organización antes de enviarlo.
- Certificación de las conexiones, así como de los clientes antes de realizar cualquier solicitud en el servicio de correo.
- Firma digital, permite que sólo el remitente lea el mensaje. (No contemplado en el proyecto).

3.1.1.3 **Tecnologías.**

En tecnologías de servidores de correo, se hace referencia al número de combinaciones (software para MailServer) existentes en el mercado para proveer el servicio de correo electrónico.

Dichas combinaciones son el resultado de la fusión de diferentes tecnologías de software desarrolladas en base al sistema operativo, la plataforma de operación, el tipo de infraestructura de la red o las necesidades del o las empresas.

Las opciones más frecuentes de software libre para MailServer son:

- Servidores MTA; Postfix, Sendmail, Exim, Qmail.
- Servidores POP/IMAP; Courier, Dovecot, Imap,
- Antivirus; Amavisd, Clamav, MailScanner.
- Antispam; SpamAssassin.

51 Concepto basado en el sitio Web: http://www.iec.csic.es/criptonomicon/correo/

- Gestor de usuarios; OpenLDAP, phpLDAPadmin .
- Webmail; SquirrelMail.
- Autenticación y certificación; Librerías cyrusSASL /TLS

Como se puede ver el número de aplicaciones de software libre para servidores de correo es notablemente amplio. De ahí que las combinaciones posibles a obtenerse para satisfacer las necesidades del cliente son varias.

En el caso de los sistemas de correo electrónico con software privativo que ofrecen las empresas (Microsoft, IBM, Kaspersky, Nod32). No todas permiten realizar dichas combinaciones o modificaciones con los sistemas, incluso algunas de estas firmas venden soluciones completas, pero los costos varían notablemente.

En el mercado existen empresas como (Axigen)[52] que desarrollan e implementan sistemas que operan como MailServer, haciendo uso de aplicativos software libre la ventaja que se obtiene está en los costos (Cuadro comparativo de costos para MailServer).

3.1.1.4 **Costos.**

Los costos en los sistemas de correo electrónico varían dependiendo del número de usuarios, el tipo de plataforma, servicios adicionales como (Antivirus, Antispam, Autenticación, Certificación, Soporte, Mantenimiento y Actualización) y en el caso de sistemas no libres el precio es mayor debido al pago de las licencias.

El siguiente cuadro muestra una pauta del costo para implementar el servicio de correo electrónico.

52 AXIGEN Servidor de correo electrónico para Linux http://www.axigen.com

Cuadro comparativo de costos para MailServer.

Nombre del producto y casa comercial.	**Sistema operativo.**	**Precio para 100 cuentas de correo.**
MailServer Edition (AVG)	GNU/Linux, FreBSD, Win.	1,144.00 USD
Kerio MailServer 5.	GNU/Linux, Win. MAC.	1,875.00 USD
Lotus Domino MailServer. (IBM)	Win 2000, 2003	N/A
Ability MailServer.	Win 2000, XP, 2003	345.00 USD
Avira MailServer + AntiVirus + AntiSpam.	GNU/Linux.	1,770.00 USD
Axigen MailServer.	GNU/Linux.	490.00 USD

Los costos por soporte del sistema no están tomados en cuenta.
Axigen MailServer es el único sistema en este cuadro que esta diseñado con Software Libre.

3.1.1.5 **Análisis de la red interna LTI.**

Las instalaciones del Laboratorio de Tecnologías de la Información LTI están ubicadas en el quinto piso del edificio de administración de la EPN; cuentan con los equipos básicos para brindar servicios elementales de Intranet a sus usuarios.

Actualmente está provisto de tres laboratorios para estudiantes. Los tres laboratorios están conectados en red por medio de un cableado estructurado en base de un cable UTP categoría 5 el que converge en la sala de auxiliares donde se mantienen equipos de conectividad tales como: hubs y un switch capa dos. Además se cuenta con una sala dedicada exclusivamente para el uso de tecnologías sobre redes informáticas, que proveen de equipos tales como: Patch Panel independiente de la sala de auxiliares,

Routers Cisco, switch, equipos de conexión inalámbrica y Voice Over IP.

En cuanto a la conexión a Internet esta se mantiene mediante el servicio que provee la Red de la Escuela Politécnica Nacional “PoliRed”. El enlace que se mantiene para la salida a Internet es por medio de cable UTP con conector RJ – 45, el que es conectado directamente a un puerto del switch capa dos. Por políticas establecidas por los administradores de la PoliRed, la conexión al Internet se la realiza mediante un servidor DHCP; quien provee de una dirección IP privada automáticamente cuando la computadora inicia el sistema, lo que permite que el usuario final tenga acceso al Internet.

3.1.1.6 **Análisis del sistema de correo (anterior).**

3.1.1.6.1 **Software.**

Actualmente se cuenta con un total de cuatro servidores, de los cuales uno esta designado a ofrecer el servicio de correo electrónico, que en la actualidad esta fuera de funcionamiento, este servidor luego de haber realizado las respectivas revisiones en los registros del sistema “Logs”, presenta la siguiente información:

- Sistema Operativo Red Hat 7.2.
- Sendmail, Sendmail – cf, m4, make, xinet, e imap.
- Sistema de Usuarios PAM.
- MailScanner, SquirrelMail.

3.1.1.6.2 **Hardware.**

En el caso del hardware, se realizaron las respectivas revisiones físicas del sistema dando como resultado los siguientes componentes:

Cuadro de características del hardware para realizar la Implementación.

Componente	Característica
Procesador	Intel Pentium III 750 Mhz
Tarjeta Principal	Intel Server
Memoria RAM	256 Mb Server
Disco Duro SCSI	Quantum 36 GB
Tarjetas de Red	3Com 10/100 Mbps
	Cnet 10/100 Mbps
CD – Rom	LG 52X
Monitor	LG Super VGA 15 pulgadas
Teclado y mouse	

3.1.1.7 **Conclusiones del análisis.**

Luego de haber recopilado la información necesaria en la etapa de análisis se establecen las siguientes conclusiones:

- La implementación de un servidor de correo electrónico seguro cubre las necesidades de los estudiantes y establece nuevos tópicos de estudio para la carrera.
- La implementación del proyecto se realizará con sistemas GNU con Linux (distribución CentOS).
- El hardware disponible no presenta inconveniente alguno para realizar las debidas instalaciones y configuraciones.

3.1.2 **DISEÑO DE LA SOLUCIÓN PROPUESTA.**

Debido a que el sistema engloba varios tópicos como; seguridades informáticas, calidad del servicio, soporte y actualización del sistema; esta etapa está dividida en tres partes:

- Diseño básico. Pautas de un modelo de correo electrónico seguro.
- Diseño complementario. Control de virus y spam.
- Diseño final. Funcionalidad, administración y mantenimiento.

La finalidad de realizar el diseño de la implementación en partes; es cubrir de mejor manera con las siguientes etapas del proyecto (implementación y pruebas), lo que permitirá establecer puntos de control al momento de realizar las configuraciones, instalaciones y pruebas de los respectivos paquetes requeridos para el proyecto.

Cabe recalcar que el diseño en su totalidad está relacionado con la topología física de la organización (red interna del LTI) que, luego de haber realizado los respectivos estudios y revisiones de software y hardware en la etapa de análisis, estas no presentaron inconveniente alguno para el diseño de la solución propuesta.

El diseño de implementación de la solución propuesta esta basado en lo siguiente.
Diseñar un servidor de correo electrónico seguro, que permita autenticar usuarios y certificar conexiones; que esté en la capacidad de controlar virus y spam; y que además esté complementado con herramientas de administración y actualización.

3.1.2.1 **Diseño básico.**

El diseño del proyecto en su etapa inicial estará en la capacidad de enviar y recibir

correos por medio del servidor SMTP (Postfix), dichos correos pasarán por un sistema de autenticación que incluyen: el uso de librerías SASL, el servidor de usuarios OpenLDAP y módulos de autenticación propios del sistema.

Para realizar la entrega de correos a los usuarios finales se procederá con el servidor POP/IMAP Dovecot.

La (Figura Diseño Básico 3.1.2.1), presenta un bosquejo inicial del diseño del proyecto en su etapa inicial.

Figura Diseño Básico 3.1.2.1

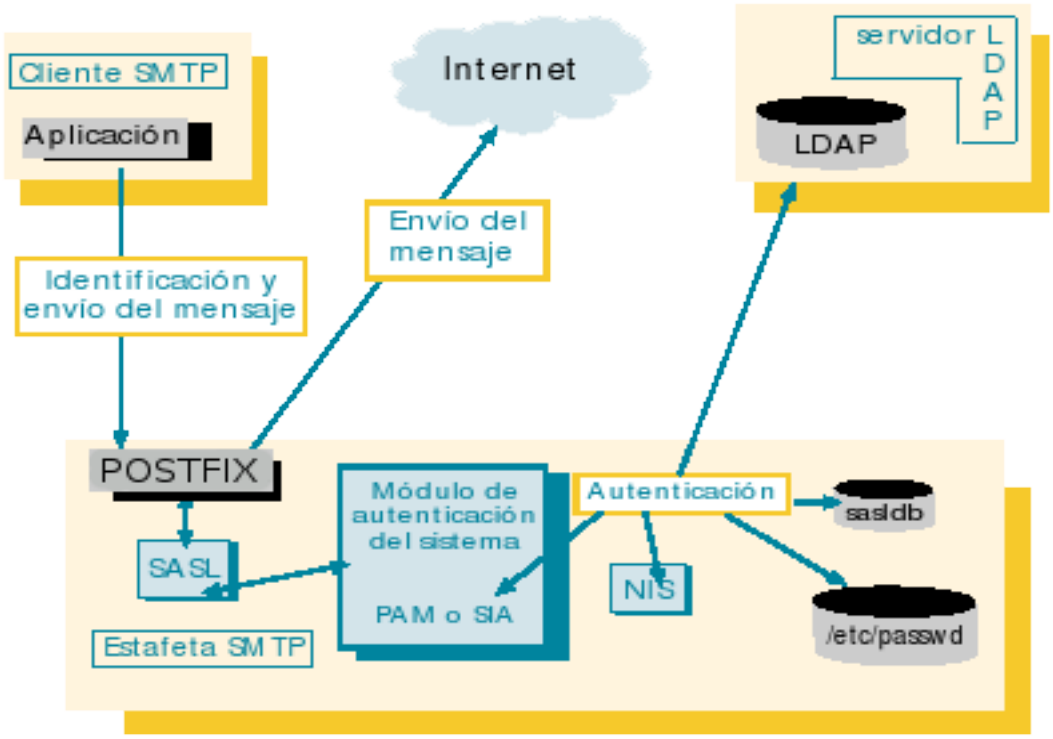


Imagen tomada del Informe: Autenticación de clientes SMTP, B. Pérez y Pascual Pérez.
El diagrama de la Figura 1, esta modificada acorde al proyecto con el editor de imágenes "The Gimp"[53].

3.1.2.2 **Diseño complementario.**

El diseño complementario implica el control de virus y spam. Para llevar a cabo esta tarea

53 The Gimp http://www.gimp.org

se utilizará el software MailScanner como interfaz entre el servidor de correo SMTP y las aplicaciones ClamAV (AntiVirus) y SpamAssassin (AntiSpam), las cuales analizarán el correo en busca de virus y Spam respectivamente.

La (Figura Diseño Complementario 3.1.2.2) muestra el diagrama del funcionamiento interno de esta herramienta y su integración con otros aplicativos.

Figura Diseño Complementario 3.1.2.2

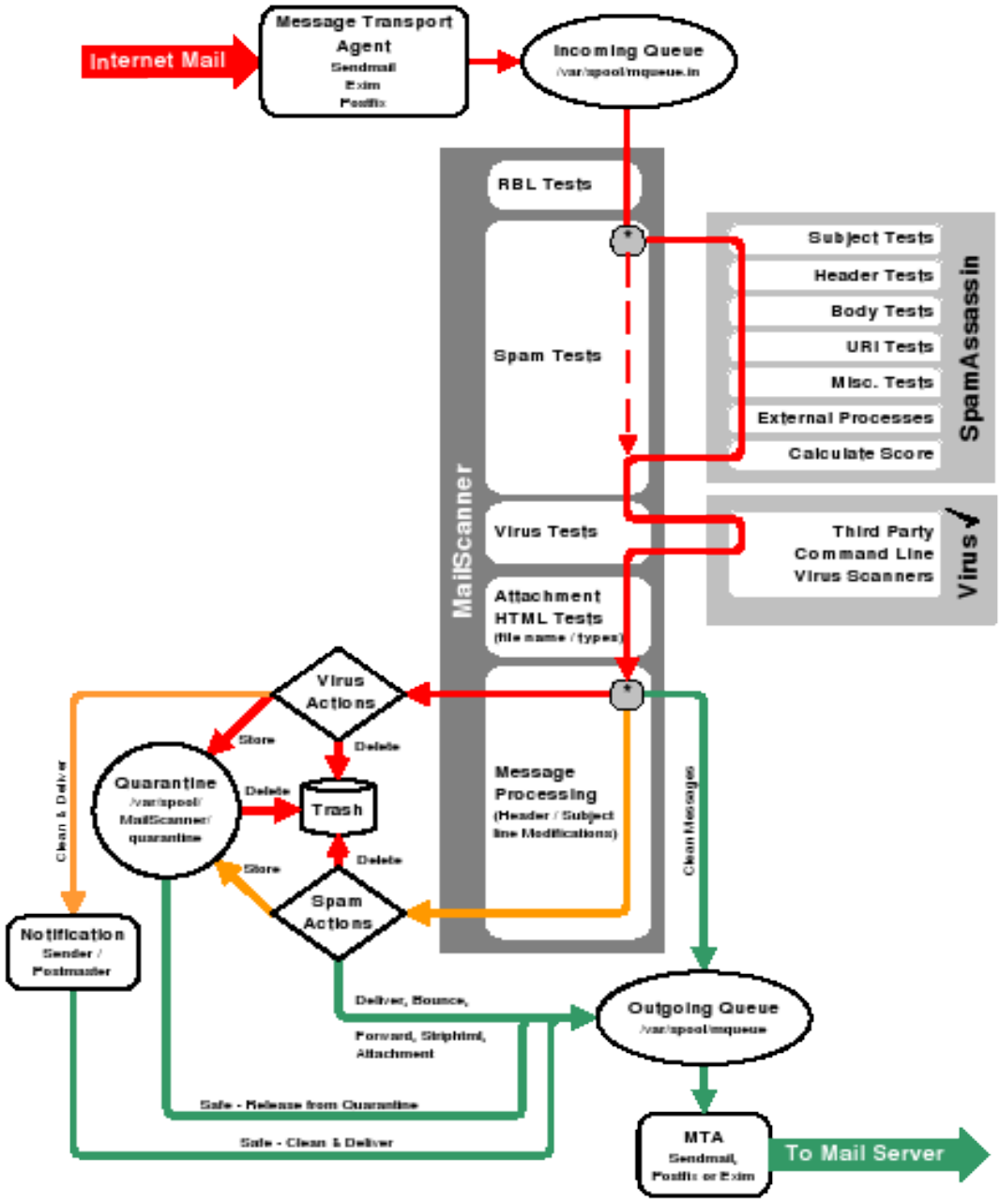
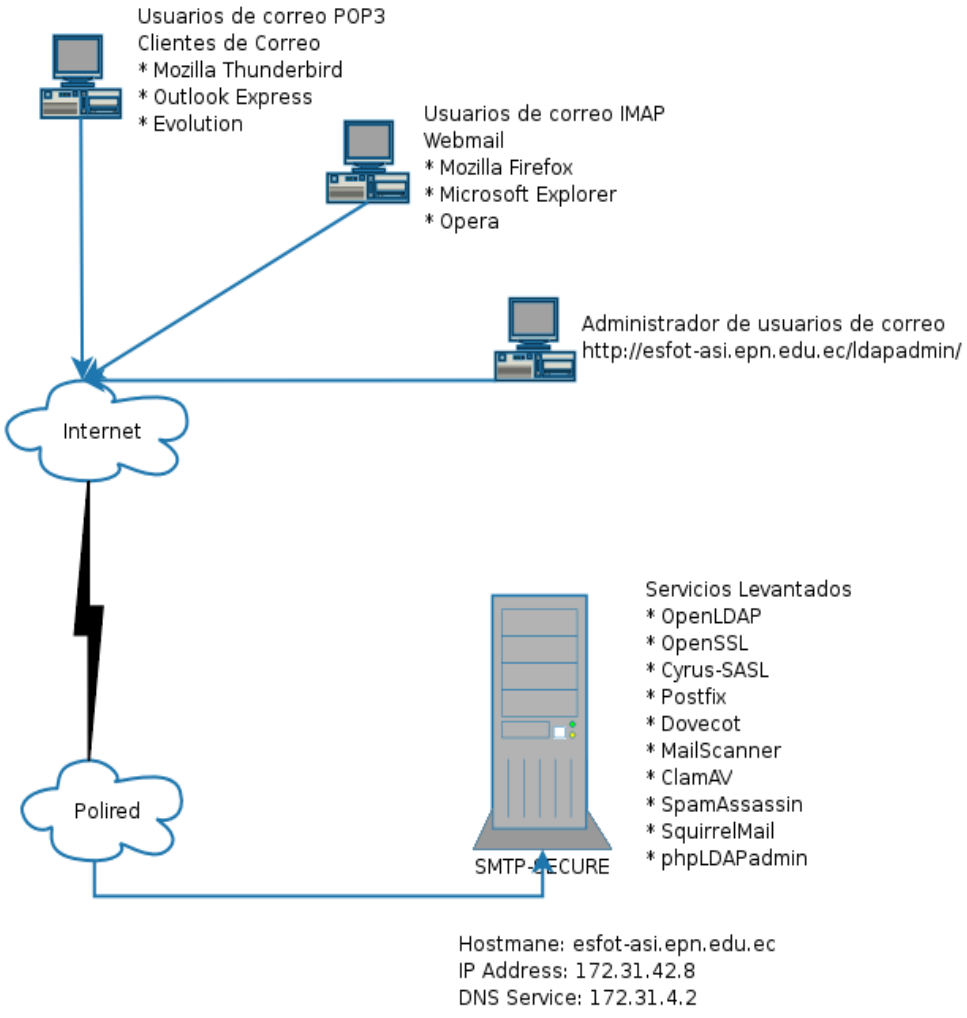


Imagen tomada del Documento: MailScanner Administrators Guide, Version 1.0.1

3.1.2.3 **Diseño final.**

El diseño final del proyecto tiene como objetivo el integrar la solución propuesta a la red interna de la organización con sus respectivas direcciones IP´s, los dominios correspondientes para el correcto funcionamiento en Internet y complementar el sistema con las herramientas faltantes de funcionalidad (SquirrelMail, necesario para la gestión de correos por medio de la Web), administración (phpLDAPadmin, encargado del mantenimiento de Usuarios de Correo) y actualización (Script Básicos para tareas automatización).

Figura Diseño Final 3.1.2.3



El diagrama de la Figura Diseño Final, esta diseñada acorde al proyecto con el editor de diagramas "Dia"[54].

3.1.3 **IMPLEMENTACIÓN.**

En la etapa de implementación se procederá a realizar las respectivas instalaciones y configuraciones del sistema operativo y los paquetes requeridos para el proyecto.
Aquí se establecen descripciones de cada uno de los paquetes así como la forma correcta de instalación, configuración, mantenimiento y recomendaciones de los mismos.

Todo lo referente a capturas de pantallas, ejecución de comandos, pruebas de funcionalidad y archivos de configuración están detallados en el Anexo Manual Técnico en forma paralela y secuencial al desarrollo de la etapa de implementación.

3.1.3.1 **Selección del sistema operativo.**

3.1.3.1.1 **CentOS[55].**

El sistema base seleccionado para realizar la implementación de un MailServer es CentOS (acrónimo de **C**ommunity **ENT**erprise **O**perating **S**ystem) que es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de Red Hat Enterprise Linux.

3.1.3.1.2 **Requerimientos del sistema.**

Hardware recomendado para operar:

- Memoria RAM: 64 MB (mínimo).
- Espacio en Disco Duro: 512 MB (mínimo) - 2 GB (recomendado).
- Procesador: ver Arquitecturas.

---

54 The Dia is a program for drawing structured diagrams. http://www.gnome.org/projects/dia
55 Información obtenida del sitio Web: http://es.wikipedia.org/wiki/CentOS

3.1.3.1.3 **Arquitecturas de CentOS.**

CentOS soporta casi todas las mismas arquitecturas que el original Red Hat Enterprise Linux.

- Intel x86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/I/II, AMD Duron, Athlon/XP/MP).
- Intel Itanium (64 bit).
- Advanced Micro Devices AMD64(Athlon 64, etc) e Intel EM64T (64 bit).
- PowerPC/32 (Apple Macintosh PowerMac corriendo sobre procesadores G3 o G4 PowerPC).
- IBM Mainframe (eServer zSeries y S/390).

Además tiene soporte para dos arquitecturas no soportadas por su original.

- Alpha procesador (DEC Alpha).
- SPARC.

3.1.3.1.4 **Recomendaciones.**

Para proceder con la instalación de CentOS como sistema base se deben tener en cuenta las siguientes recomendaciones:

- Realizar el proceso de instalación en modo texto, no se requiere el uso del servidor X en estaciones que operasen como MailServer.
- Instalar el sistema base mínimo.
- Seleccionar las herramientas de desarrollo (necesarias para compilar e instalar programas) y un editor de textos "VIM"[56] para realizar cambios en las configuraciones.
- Establecer los tamaños de cada partición.
- Solicitar las direcciones IP´s, asignadas para el servidor (Red, DNS).

56 Editor de textos VIM (Vi Mejorado): http://vi-editor.org

- Establecer los puertos necesarios para configurar el Firewall.
- Preferible instalar el sistema base en Ingles (Evita problemas para compilar programas en Perl[57]).
- Eliminar las herramientas de desarrollo de sistema base luego de terminar la implementación y pruebas.
- Realizar las debidas pruebas de funcionalidad del sistema base (Red, Sistema, Bugs) para luego continuar con la instalación de los otros paquetes.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación CentOS.

3.1.3.2 **Selección y descripción de paquetes necesarios para la implementación.**

Los paquetes necesarios para la implementación de un servidor de correo electrónico van a ser seleccionados siguiendo el orden preestablecido en la etapa de diseño del proyecto. Cada uno los paquetes seleccionados presentan una descripción detallada de las opciones que el paquete ofrece, así como recomendaciones de instalación, administración y soporte.

3.1.3.3 **OpenLDAP[58].**

3.1.3.3.1 **Descripción.**

Protocolo Liviano de Acceso a Directorio, es un protocolo que provee servicios de directorio, organizando la información de forma muy similar a como lo hace un sistema de archivos (/) o el servicio de nombres de dominio (DNS) en Internet ver (Figura Diagrama de un Árbol OpenLDAP).

57 Practical Extraction and Report Language (Perl): http://www.perl.org
58 Información obtenida del sitio Web: http://dns.bdat.net/documentos/ldap/

Diagrama de un Árbol OpenLDAP.

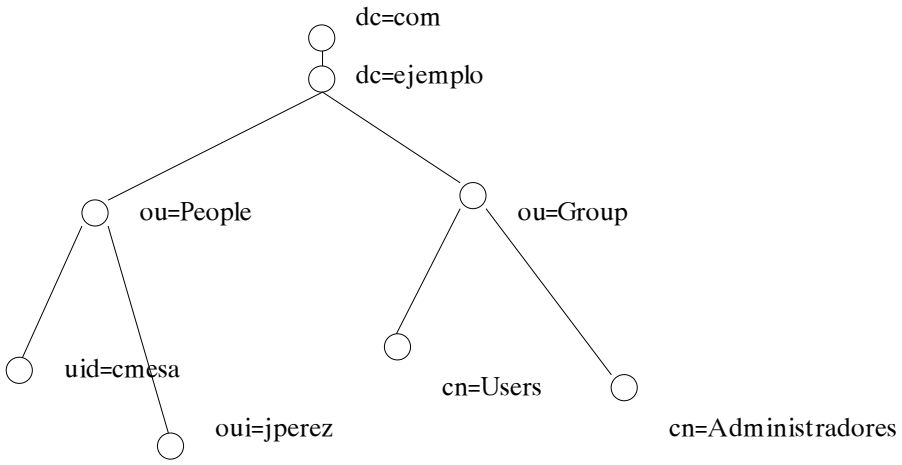


Imagen tomada del sitio Web: http://dns.bdat.net/documentos/ldap/
El diagrama de un Árbol OpenLDAP, muestra la Jerarquía de un directorio LDAP.

3.1.3.3.2 **Características.**

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

- Es muy rápido en la lectura de registros.
- Permite replicar el servidor de forma muy sencilla y económica.
- Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente.
- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.
- Usa un sistema jerárquico de almacenamiento de información.
- Permite múltiples directorios independientes.
- Funciona sobre TCP/IP y SSL.
- La mayoría de aplicaciones disponen de soporte para LDAP.

- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

3.1.3.3.3 **Usos prácticos.**

Dadas las características de LDAP sus usos más comunes son:

- 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.
- Sistemas de autenticación/autorización centralizada. Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos.

  Por ejemplo:

  - 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….
  - Sistemas de correo electrónico. Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
  - Sistemas de alojamiento de páginas web y FTP, con el repositorio de datos de usuario compartido.
  - Grandes sistemas de autenticación basados en RADIUS, para el control de accesos de los usuarios a una red de conexión o ISP.
  - Servidores de certificados públicos y llaves de seguridad.
  - Autenticación única ó “single sign-on” para la personalización de aplicaciones.

- Libretas de direcciones compartidas.

3.1.3.3.4 **Recomendaciones.**

La instalación y configuración de OpenLDAP, sera realizada de forma resumida y compacta debido a que no es el tema central del proyecto. Algunas recomendaciones para mejor desempeño de este aplicativo son las siguientes:

- OpenLDAP, viene por defecto en sistemas GNU con Linux pero el servidor LDAP no se instala automáticamente con el sistema base de CentOS.
- OpenLDAP soporta la Capa de autenticación y seguridad (SASL), la Seguridad de la capa de transporte (TLS) y la Capa de conexión segura (SSL).
- El tiempo de respuesta de conexiones o autenticaciones esta ligado con el servidor DNS, que debe estar previamente configurado.
- Pueden existir mas de un directorio en un servidor.
- Se pueden establecer listas de control de acceso (lectura o escritura), para diferentes tipos de usuarios del directorio.
- Tener un bosquejo del modelo de la organización en el servidor LDAP.
- La migración de datos al servidor LDAP, se la puede realizar de forma automática con herramientas OpenLDAP-migration.
- Existe un completo kit de administración del servidor por medio de consola, pero se pueden instalar aplicaciones de administración GUI o Web.
- Crear un usuario de prueba para realizar las pruebas de funcionalidad del servidor. Antes de orientarlo a usuarios de correo.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación OpenLDAP.

3.1.3.4 **SSL (Secure Sockets Layer) / TLS (Transport Layer Security).**

3.1.3.4.1 **Descripción.**

Desarrollado por Netscape[59], SSL versión 3.0 se publicó en 1996, que más tarde sirvió como base para desarrollar TLS versión 1.0, un estándar protocolo IETF[60] definido por primera vez en el RFC 2246[61]. Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves publicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping)[62], la falsificación de la identidad del remitente y mantener la integridad del mensaje.

TLS 1.1 es la última versión aprobada del protocolo TLS. TLS 1.1 clarifica algunas ambigüedades y añade cierto número de recomendaciones. TLS 1.1 es muy similar a TLS 1.0. La principal razón de esta nueva versión es un formato modificado para cifrado RSA anterior al uso de 'master secret', que es parte del mensaje de intercambio de claves del cliente (si se usa RSA), para usar PKCS#1[63] versión 2.1, en detrimento de PKCS#1 versión 1.5 en TLS 1.0. La razón de dicho cambio es para protegerse contra ataques descubiertos por Daniel Bleichenbacher que podían lanzarse contra servidores TLS 1.0, usando PKCS#1 versión 1.5, que podrían fallar de diferentes formas, dependiendo de si el formato descifrado fuera correcto o no.

---

59 Netscape http://www.netscape.com
60 IETF http://es.wikipedia.org/wiki/IETF
61 RFC 2246 http://www.ietf.org/rfc/rfc2246.txt
62 Eavesdropping http://es.wikipedia.org/wiki/Eavesdropping
63 PKCS http://es.wikipedia.org/wiki/PKCS

3.1.3.4.2 **Características.**

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves publicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, DSA (Digital Signature Algorithm) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);
- Con funciones hash: MD5 o de la familia SHA.[64]

3.1.3.4.3 **Usos prácticos.**

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

Aunque un número creciente de productos clientes y servidores pueden proporcionar SSL de forma nativa, muchos aún no lo permiten. En estos casos, un usuario podría querer

64 (RSA, DES, RC4, IDEA, DES, MD5, etc) Algoritmos criptográficos usados para poder encriptar conexiones o autenticaciones.

usar una aplicación SSL independiente como Stunnel[65] para proporcionar cifrado. No obstante, el Internet Engineering Task Force recomendó en 1997 que los protocolos de aplicación ofrecieran una forma de actualizar a TLS a partir de una conexión sin cifrado (plaintext), en vez de usar un puerto diferente para cifrar las comunicaciones; esto evitaría el uso de envolturas (wrappers) como Stunnel.

SSL también puede ser usado para tunelar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

3.1.3.4.4 **Recomendaciones.**

- Como SSL/TLS son aplicaciones que van a operar en conjunto con otros paquetes, se debe revisar que estén instaladas las herramientas de desarrollo de OpenSSL.
- Diseñar y crear las respectivos firmas, clave y autoridad certificadora; con los debidos comandos.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación SSL/TLS.

3.1.3.5 **Librerías SASL[66].**

3.1.3.5.1 **Descripción.**

Librerías desarrolladas en el proyecto Cyrus de la Universidad Carnegie Mellon.

Su función es independizar a la aplicación del proceso de autenticación. Permite usar distintos mecanismos de autenticación como los clásicos de login y password o más sofisticados como CRAM-MD5. Además puede buscar los datos de identificación en diferentes ubicaciones: /etc/passwd, NIS, LDAP, etc.

---

65 Stunnel http://www.stunnel.org/

66 Concepto basado del Informe: Autenticación de clientes SMTP, B. Pérez y Pascual Pérez.

3.1.3.5.2 **Características.**

- La librería SASL dispone también de un sistema propio para gestionar los datos de usuario, incluso admite la posibilidad de crear aplicaciones específicas para validar la identificación del usuario.
- Cada aplicación que utilice SASL debe tener un fichero de configuración dónde se indica el modelo de autenticación que se utilizará.
- Separa los mecanismos de autenticación de los protocolos de la aplicación permitiendo, en teoría, a cualquier protocolo de aplicación que use SASL; usar cualquier mecanismo de autenticación soportado por SASL.
- A pesar de que mediante SASL sólo se maneja la autenticación (y se requieren otros mecanismos como por ejemplo TLS para cifrar el contenido que se transfiere).
- SASL proporciona medios para un uso negociado del mecanismo elegido.

3.1.3.5.3 **Usos prácticos.**

Por estar acoplado a una de las herramientas potencialmente atractivas para la gestión de usuarios como es OpenLDAP, estas librerías son pretendidas para proveer autenticación de usuarios en servicios tales como: MailServer, Servidores ISP, Usuarios Samba, etc.

3.1.3.5.4 **Recomendaciones.**

- SASL de la misma manera que SSL/TLS, operan en conjunto con otros programas, y son necesarios los paquetes de desarrollo de cyrus-SASL para realizar las debidas integraciones con otros paquetes.
- Las versiones de CentOS actuales tienen dos versiones distintas de SASL, esto

no afecta al sistema pero si hay que tener en cuenta los comandos que se digita en la consola de administración. Ej: `saslpaswd` (version 1); `saslpaswd2` (version 2).

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación SASL.

3.1.3.6 **Postfix[67].**

3.1.3.6.1 **Descripción.**

Postfix es un agente de transporte de correo electrónico (MTA) bastante reciente que se suma a la lista de alternativas al legendario Sendmail[68]. En su diseño han primado factores como la seguridad, la eficiencia y la facilidad de configuración y administración, junto con la compatibilidad con Sendmail y con otros sistemas de correo. Siendo el correo electrónico hoy día una herramienta de trabajo vital en multitud de entornos de trabajo, sustituir los sistemas actuales por otro nuevo es una decisión muy delicada. Se debe garantizar que la migración se va a producir sin inconvenientes para los usuarios y con el mínimo tiempo de parada del servicio.

Desarrollado por Wietse Venema[69] un programador respetado como pocos. Autor de programas tan conocidos como los TCP Wrappers, SATAN, The Coroner Toolkit, sus versiones de portmap y rpcbind. Es un experto en seguridad informática, lo cual, como poco, tranquiliza a los usuarios de Postfix cuando pensamos en los múltiples agujeros que ha tenido Sendmail a lo largo de su historia.

Algunos de las cualidades y virtudes de postfix son:

---

67 Información obtenida del sitio Web de la UCO sobre Postfix. http://www.uco.es/ccc/sistemas/postfix/intro.html

68 Agente de Transporte de Correo (MTA) http://www.sendmail.org

69 Desarrollador de Postfix Wietse Venema http://www.porcupine.org/wietse

- Diseño modular (no es un único programa monolítico).
- La seguridad ha sido un condicionante desde el comienzo de su diseño.
- Lo mismo cabe decir del rendimiento (seguramente Sendmail no se diseñó pensando que algún día habría sitios que necesitarán procesar cientos de miles o millones de mensajes al día).
- Soporte para las tecnologías más usadas hoy día: LDAP, Bases de datos (MySQL), autentificación mediante SASL, LMTP, etc.
- Soporte muy bueno para dominios virtuales.
- Facilidad de configuración.
- Compatibilidad hacia/desde fuera con Sendmail (.forward, aliases, suplanta `mailq`, `newaliases`, `/usr/lib/sendmail` con versiones equivalentes).
- Abundante documentación, y de calidad.
- Fácil integración con AntiVirus.
- Uso sencillo de listas negras.
- Soporta de forma nativa el formato de buzones Maildir[70] original de qmail.
- Tiene múltiples formas de obtener información de 'lo que está pasando' para resolver problemas o simplemente, para aprender.
- Se pueden lanzar varias instancias de Postfix en la misma máquina con distintas configuraciones, usando cada una distintas direcciones IP, distintos puertos, etc.
- Filtrado de cabeceras y cuerpos de mensajes por expresiones regulares.
- Utilidades para varias cosas, como gestionar las colas de mensajes.

Por último, pero no menos importante, hay que decir que el código fuente de Postfix (por supuesto de dominio público) es un ejemplo de diseño, claridad y documentación, lo cual facilita su mantenimiento (por su autor o, en el futuro, por otros) así como la incorporación de nuevas capacidades, corrección de errores, etc.

---

70 Maildir, es un formato para guardar correos electrónicos de forma independiente y separada (para cada correo).

3.1.3.6.2 **Características.**

3.1.3.6.2.1 **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 (en el caso de 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, etc.
- 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 AntiVirus, filtrados, etc.
- Es posible, por ejemplo, lanzar un servidor SMTPD adicional en otro puerto o sobre otra IP, con distintas opciones de configuración de acceso.

También se puede correr varias instancias de Postfix, con las únicas limitaciones de que ambas no compartan el directorio de colas y que usen distintos valores para `myhostname`.

3.1.3.6.2.2 **Seguridad.**

Seguridad frente a ataques contra el servidor y también contra el uso inadecuado (spam,

etc). En cuanto a la primera acepción, no es conocido ningún problema serio de seguridad que se haya detectado aún en Postfix. Respecto al tema de spam, relay, etc. Postfix soporta directamente el uso de listas negras y es relativamente difícil configurarlo como relay abierto. Cuando se tienen cuidado con las restricciones.

3.1.3.6.2.3 **Rendimiento.**

El rendimiento de Postfix es realmente muy bueno. Por ejemplo, cuando se produce algún atasco de correo, tras resolverse los mensajes salen a una velocidad mucho mayor de la velocidad de respuesta de Sendmail.

3.1.3.6.2.4 **Configuración.**

La facilidad de configuración de Postfix es quizá el factor que más atrae a muchos administradores. Con Sendmail mucha gente usa 'recetas' para generar los ficheros de configuración, pero luego no son capaces de entenderlos, lo cual hace difícil su modificación y la resolución de problemas. En Postfix no es necesario esto. Cuando se conoce un poco, no sólo es sencillo escribir un fichero de configuración para casi cualquier situación (máquinas 'dial-up', servidores centrales, relays, etc.) sino que a la vista de una configuración que se nos presente es igual de fácil entender el funcionamiento que se pretende con ella. Existen multitud de parámetros que se pueden alterar (todos ellos con nombres coherentes con su función), pero la inmensa mayoría sólo hay que modificarlos en casos excepcionales.

3.1.3.6.3 **Recomendaciones.**

Postfix es uno de los pilares del proyecto, es por tal motivo, que se debe tener en cuenta las restricciones y servicios que van ha ser complementados (LDAP, SSL/TLS, SASL) de ahí que las recomendaciones para proceder con el proceso de instalación y configuración

de postfix son presentados en la siguiente lista:

- Revisar que no esté instalado Sendmail, en el caso de estarlo eliminar del sistema.
- Al igual que el servidor LDAP, postfix esta ligado con el MX[71] del servidor DNS y debe estar configurado y funcionando.
- Realizar un borrador de las reglas de restricciones y perfeccionarlos realizando las pruebas necesarias.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación Postfix.

3.1.3.7 **Dovecot.**

3.1.3.7.1 **Descripción.**

Dovecot es un Agente de Entrega de Correo, escrito con la mirada puesta en la seguridad. Puede trabajar con los formatos estándar de correo “mbox y Maildir” es totalmente compatible con diferentes servidores de correo, así como los clientes del correo que tienen acceso a las cajas directamente. Es fácil migrar de éstos a Dovecot. Dovecot también pronto tendrá su propio dbox.[72]

3.1.3.7.2 **Características.**

- Maildir Y mailbox, Pueden coexistir cada usuario puede tener uno de los dos formatos, lo que permite hacer una migración progresiva de los buzones.
- Usuarios Virtuales, El soporte para usuarios es excelente. Se pueden usar multiples bases de datos (LDAP, PostgreSQL, MySQL, ficheros), además de

71 Registro de Mail eXchange, el cual indica dónde debería de ir el correo enviado a un espacio de nombres particular controlado por esta zona.

72 Información obtenida del sitio Web: http://dovecot.org

forma simultanea, en secuencia y combinadas con usuarios del sistema.

- Indices, genera diversos indices que reducen el tiempo de localización de mensajes.
- Usuarios maestros, se pueden establecer una o varias, base de datos de claves donde se incluyen usuarios que pueden acceder al sistema como cualquier otro.
- Configurabilidad, casi cualquier parte del sistema se puede configurar de forma específica para cada usuario, especialmente la ubicación del buzón, las carpetas y los indices.
- Depuración, posibilidad de hacer logs en formato crudo (orientado al tipo de servicio que se opere).[73]

3.1.3.7.3 **Usos prácticos.**

Dovecot esta orientado a servidores de correo electrónico (en especial a servidores que deseen migrar el tipo de formato del buzón de correo).

3.1.3.7.4 **Recomendaciones.**

- Revisar la compatibilidad y funcionalidad de Dovecot (de las fuentes de CentOS), con el directorio OpenLDAP.
- Para configurar las conexiones SSL, establecer un path único para los certificados.
- En el caso de operar con OpenLDAP, crear y configurar el archivo de enlace con el directorio de usuarios.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación Dovecot.

---

73 Conceptos tomados del Documento: Visión general de Dovecot Luís Meléndez, Javier Álvarez Uriarte, Victoriano Giralt

En este punto del proyecto, luego de realizar las instalaciones correspondientes de los paquetes mencionados en Capitulo 3.1.2.1 Diseño básico, se realizaran las respectivas pruebas de funcionalidad; ver el Anexo Manual Técnico: Pruebas de Funcionalidad I.

3.1.3.8 **MailScanner[74].**

3.1.3.8.1 **Descripción.**

MailScanner es un robusto servicio que examina el correo electrónico e identifica y etiqueta correo masivo no solicitado (Spam) y fraudes electrónicos (Phishing). Combinado con ClamAV, un funcional anti-virus para GNU/Linux y otros sabores de Unix, resultan una de las soluciones más robustas para la protección contra virus, gusanos y troyanos desde el servidor de correo electrónico.

3.1.3.8.2 **Características.**

- Distribuido bajo los términos de la Licencia Pública General GNU versión 2.
- Revisa el correo electrónico en busca de virus utilizando cualquier combinación de entre más de una docena de distintos programas anti-virus.
- Automáticamente actualiza todo los anti-virus instalados cada hora.
- Identifica alrededor del 95% del correo masivo no solicitado (Spam) utilizando diferentes técnicas, incluyendo altamente avanzadas técnicas de heurística (capacidad de un sistema para realizar de forma inmediata innovaciones positivas para sus fines).
- El correo identificado como peligroso puede ser etiquetado, rechazado, descartado, archivado o reenviado hacia otras direcciones para su inspección por los administradores.
- Puede eliminar el contenido gráfico de correo masivo no solicitado (Spam) de tipo

74 Información obtenida del sitio Web: http://www.mailscanner.info/

pornográfico protegiendo a los usuarios de contenido obsceno.

- Verifica el coreo electrónico en busca de conocidas vulnerabilidades para las más populares aplicaciones de correo electrónico y corrige automáticamente los mensajes durante el proceso cuando sea posible poniendo en cuarentena las secciones peligrosas de contenidas en los mensajes.
- Es altamente escalable. Un servidor puede procesar más de millón y medio de mensajes de correo por día.
- Es robusto. Se protege a si mismo contra ataques de Denegación de Servicio (DoS) y fuga de recursos del sistema operativo.
- Es fácil de instalar y configurar puesto que sus opciones predefinidas permiten trabajar al servicio de correo sin complicaciones.

3.1.3.8.3 **Usos prácticos.**

Es altamente configurable, y por lo tanto esta orientado a los Proveedores de Servicios de Internet (**ISP** o **I**nternet **S**ervice **P**rovider y Proveedores de Servicios de Aplicaciones (**ASP** o **A**pplication **S**ervice **P**rovider) debido a la posibilidad de utilizar miles de diferentes reglas y configuraciones para cualquier combinación de usuarios y dominios.

3.1.3.8.4 **Recomendaciones.**

- MailScanner ésta basado en código Perl, lo que implica que el sistema base debe tener instalado el paquete de idioma Ingles o estar instalado en Ingles nativo (opcional). Esto es necesario para evitar fallas al compilar los fuentes de MailScanner.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación MailScanner.

3.1.3.9 **SpamAssassin.**

3.1.3.9.1 **Descripción.**

SpamAssassin es una herramienta para inspeccionar correos electrónicos que permite determinar si se trata de un mensaje chatarra, mejor conocido como SPAM.

Es una programática que utiliza un sistema de puntuación basado sobre algoritmos de tipo genético para identificar mensajes que pudieran ser sospechosos de ser correo masivo no solicitado, añadiendo entonces cabeceras a los mensajes de modo que pueda ser filtrados por el cliente de correo electrónico o MUA (**M**ail **U**ser **A**gent).

En este sentido SpamAssassin es considerado un pre-procesador de correos, ya que la inspección es llevada acabo en el servidor de correos previo a que el usuario descargue su correo, así permitiendo una pre-clasificación de mensajes antes de utilizar una herramienta en PC (Outlook, Eudora, Evolution o Mozilla).[75]

3.1.3.9.2 **Características.**

- Inspección de "Headers": Los "Headers" o cabeceras de mensaje contienen información importante acerca del mensaje, como lo son procedencia y rutas de servidor, SpamAssassin inspecciona esta información para fines de detección.
- Análisis del Mensaje: El cuerpo y titulo del mensaje también son leídos por SpamAssassin, realizando búsquedas por palabras claves o estructuras que conforman un correo chatarra.
- Listas Negras: Actualmente, existen listas que enumeran servidores de correo conocidos como generadores de SPAM ("Open-Relays"), SpamAssassin consulta estas listas negras entre las que se encuentran: http://www.mail-abuse.com/,

75 Información obtenida del sitio Web: http://spamassassin.apache.org/

http://www.ordb.org/ y http://www.surbl.org/ .

- Análisis probabilístico / bayesiano: Una vez definidas las reglas iniciales para detección, SpamAssassin utiliza análisis probabilístico para determinar similitudes entre mensajes entrantes y aquellos ya detectados como SPAM.
- Listas "Hash" / Firmas de Correo: Debido a que un correo SPAM suele ser enviado a miles de personas a la vez, la estructura de cada mensaje es idéntica en todas sus instancias, así produciendo un "Hash" inequívoco. SpamAssassin consulta listas de "Hashes" sobre mensajes conocidos, como lo serian: Razor[76], Pyzor[77] y DCC[78] [79].

3.1.3.9.3 **Usos prácticos.**

Su uso mas práctico está orientado a proveedores ISP, que permiten la personalización de reglas de control y controlar las posibilidades de sobrecarga en los servidores por las peticiones de correo basura.

3.1.3.9.4 **Recomendaciones.**

Revisar las configuraciones para integrar este servicio con Postfix, varían dependiendo de la version o el sistema.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación SpamAssassin.

3.1.3.10 **ClamAV.**

76 Vipul's Razor: http://razor.sourceforge.net/
77 Pyzor: http://pyzor.sourceforge.net/
78 DCC: http://www.rhyolite.com/anti-spam/dcc/
79 Información obtenida del sitio Web: http://www.digitalvalley.com/comunicados/comunicado-1-agosto.html

3.1.3.10.1 **Descripción.**

ClamAV es un proyecto abierto a colaboraciones de todo tipo (y, de hecho, tiene una buena lista de "contributors" individuales y empresas que han proporcionado recursos económicos o de otro tipo para la buena marcha de su desarrollo) cuyo objetivo es el de programar un motor AntiVirus y las correspondientes bases de datos de firmas actualizadas con un escáner en línea de comandos, interfaz para Sendmail, postfix y soporte para escanear ficheros comprimidos (RAR, ZIP, CHM -Microsoft-,...) entre otras facilidades.

Pese a que nació inicialmente como AntiVirus para sistemas Linux y BSD con misiones de servidor, podemos encontrar ports para entornos Windows, Mac OS X, Solaris e incluso BeOS.

Si alguien se pregunta sobre su efectividad, baste decir que durante la expansión de diversas variantes del virus Bagle a finales de 2004, ClamAV fue el tercer AntiVirus de una larga lista de estos programas en incorporar las firmas necesarias para detectarlas.

Gracias a su gratuidad y disponibilidad del código fuente, junto a su integración a nivel de servidor, ClamAV es una buena opción para los desarrolladores e integradores de cortafuegos por hardware, para poner un ejemplo. Además, a su alrededor se han desarrollado una serie de herramientas proporcionadas por terceras partes como interfaces gráficas de usuario que facilitan su empleo en computadoras de usuario final.

Pese a todo esto ClamAV no se considera en muchas ocasiones en las comparativas de AntiVirus, centradas en productos comerciales, lo cual redunda en un lastre que este producto arrastra ante muchos usuarios finales, que confían en estos estudios para seleccionar una herramienta AntiVirus.[80]

3.1.3.10.2 **Características.**

80 Información obtenida del sitio Web: http://www.noticias.com/articulo/30-06-2005/guillem-alsina/clamav-antivirus-libre-4j59.html

- Cumple con las especificaciones de familia de estándares **POSIX** (**P**ortable **O**perating **S**ystem **I**nterface for UNI**X** o interfaz portable de sistema operativo para Unix).
- Exploración rápida.
- Detecta más de 44 mil virus, gusanos y troyanos, incluyendo virus para MS Office.
- Capacidad para examinar contenido de ficheros ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Soporte para explorar ficheros comprimidos con UPX, FSG y Petite.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.[81]

3.1.3.10.3 **Usos prácticos.**

- ClamAV AntiVirus, se usos mas comunes están en servidores de correo electrónico integrados con MailScanner y además como fuente de regencia para empresas desarrolladoras de software.

3.1.3.10.4 **Recomendaciones.**

- Mantener conexión directa a Internet para permitir que el proceso de actualización de las bases de datos (virus informáticos), no presente falencias.
- Revisar los archivos de instalación README o INSTALL, dependiendo de la versión se debe crear o no el usuario "clamav[82]"

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación ClamAV.

81 Información obtenida del sitio Web: http://www.clamav.net/

82 clamav: Usuario requerido para compilar e instalar el AntiVirus ClamAV.

En este punto del proyecto, luego de realizar las instalaciones correspondientes de los paquetes mencionados en Capitulo 3.1.2.2 Diseño complementario, se realizaran las respectivas pruebas de funcionalidad; ver el Anexo Manual Técnico: Pruebas de Funcionalidad II.

3.1.3.11 **SquirrelMail[83].**

3.1.3.11.1 **Descripción.**

SquirrelMail es un Webmail muy interesante por su facilidad de instalación, simpleza y por la gran cantidad de características que ofrece gracias a su arquitectura de plug-ins[84]. Algunas de las ventajas mas interesantes que presenta son las siguientes:

- No tiene nada que envidiar a muchos clientes de correo. Además está escrito en PHP4[85] y es GPL[86], por lo que es posible ampliarlo, modificarlo fácilmente y es totalmente gratis.
- Gracias a la arquitectura de plug-ins se puede añadir otros plug-ins para incluir nuevas funciones.
- Es muchísimo más estable que bastantes clientes de correo.
- Acceso al correo personal desde cualquier sitio, basta cualquier ordenador con conexión a Internet y un navegador.
- Se puede acceder al correo personal de forma segura (a través de SSL).

3.1.3.11.2 **Características.**

83 Información obtenida del sitio Web: http://bulma.net/body.phtml?nIdNoticia=634

84 Aplicaciones software que se pueden instalar en el mismo software de edición no lineal para proporcionar al sistema funciones y características adicionales.

85 Lenguaje de programación tipo script para entornos Web utilizado, sobre todo, en servidores Linux

86 La GNU General Public License (GPL) es una licencia creada por la Free Software Foundation y orientada principalmente a los términos de distribución, modificación y uso de software.

- Gestión de carpetas.
- Internacionalización.
- Libro de direcciones personal y acceso a otros servicios de LDAP (muy útil si se tiene LDAP montado en una organización). Permite hacer búsquedas de direcciones.
- Gestión de attachments (archivos adjuntos).
- Servicio de búsqueda en emails.
- No necesita ninguna base de datos para funcionar (al contrario que muchos otros Webmail que necesitan MySQL o PostgreSQL).
- Interfaz de usuario fácil y potente.
- Arquitectura de plug-ins.
- Múltiples temas (interfaces de color, formato de texto, idioma, etc).
- Configuración de las vistas de mensajes: número de mensajes visibles en pantalla, campos visibles, orden, cada cuanto tiempo comprueba si hay nuevos mensajes, etc.

3.1.3.11.3 **Usos Prácticos.**

- Servidores de correo electrónico que operen como Webmail.
- Proveedores ISP con servicios de Webmail.

3.1.3.11.4 **Recomendaciones.**

- Instalar los plug-ins necesarios para opciones adicionales que se requieran.
- Configurar apache para el soporte de SquirrelMail con SSL.
- (Opcional), como SquirrelMail es GPL, se puede editar los archivos de configuración dependiendo de los requerimientos del clientes o el sistema.

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación SquirrelMail.

3.1.3.12 **phpLDAPadmin**[87]**.**

3.1.3.12.1 **Descripción.**

PhpLDAPadmin, es un cliente Web – LDAP (OpenLDAP). Proporciona un fácil acceso desde cualquier lugar accesible al Internet, la interfaz de administración es configurable al tipo de idioma en el que se encuentre y mantiene un árbol jerárquico y funcional que permite realizar búsquedas de forma mas rápida e instintiva.

Puesto que su uso esta orientado a la Web, trabaja en muchas plataformas haciendo el servidor OpenLDAP fácilmente manejable para administradores con poca experiencia en este tema.

3.1.3.12.2 **Características.**

- Plantilla basada en las entradas editadas.
- Copia uniforme entre diversos servidores.
- Copia recurrente de arboles completos hacia otros servidores OpenLDAP.
- Elimina de manera recurrente arboles completos.
- Ve y corrige cualidades de la imagen (como jpeg-Photo).
- Permite la creación y exportación de platillas LDIF[88] para formatos de salto de pagina (Windows, GNU con Linux, MAC).
- Renombra entradas de usuarios en el servidor.
- Administra los atributos user password (soporta algoritmos: sha, crypt, md5, blowfish, md5crypt).

87 Información obtenida del sitio Web: http://phpldapadmin.sourceforge.net/

88 El *LDAP Data Interchange Format* (LDIF) es un formato que se utiliza para la importación y exportación de datos independientemente del servidor LDAP que se esté utilizando.

- Incrementa automáticamente el atributo UID[89].
- Evaluado en 10 idiomas.

3.1.3.12.3 **Usos Prácticos.**

Administración del servidor OpenLDAP por medio del entorna gráfico orientado a la Web.

3.1.3.12.4 **Recomendaciones.**

- Revisar que version del paquete PHP esta instalado en el sistema base y dependiendo de esto descargar en phpLDAPadmin correspondiente

El proceso de Instalación, configuración y pantallas capturadas; ver el Anexo Manual Técnico: Instalación phpLDAPadmin.

3.1.4 **PRUEBAS.**

Dado el numero de paquetes a instalarse y con el fin de evitarse errores mas complejos a resolver; las pruebas de funcionalidad se las debe realizar con la culminación de cada etapa de diseño, mencionadas anteriormente en el capitulo 3.1.2 DISEÑO DE LA SOLUCIÓN PROPUESTA.

Las pruebas de funcionalidad del sistema en su totalidad que incluyen control de Spam, Virus, envío y recepción de mensajes (Webmail), descarga de correos (POP3); están detalladas en el Anexo Manual Técnico: Pruebas de Funcionalidad Finales. Esta sección también incluye la respectiva configuración para los clientes de correo (Webmail y POP3).

89 Identificador de usuarios en sistemas tipo UNIX.

CAPITULO 4

4.1 CONCLUSIONES.

- La documentación del proyecto, está detallada de la forma más clara y coherente para establecer pautas en el uso de nuevas tecnologías en servidores de correo electrónico seguro.
- El desarrollo del proyecto fue diseñado para ir avanzando de manera paulatina y ordenada.
- El diseño e implementación del proyecto está divido en etapas (básico, intermedio y final) para que el administrador del sistema, al terminar la implementación no tenga que revisar los diferentes paquetes (software) instalados para corregir posibles errores.

4.2 RECOMENDACIONES.

- Debido a que el proyecto se lo desarrolló para sistemas GNU con Linux, es recomendable tener conocimientos básicos de dichos sistemas.
- Para evitar confusiones, el proyecto establece recomendaciones con cada aplicativo instalado.
- Tener conocimientos básicos-avanzados de Inglés.
- Antes de realizar cualquier cambio, actualización o mantenimiento al sistema se deben realizar los debidos respaldos de los archivos de configuración.
- El Manual Técnico está estructurado de tal manera que si esté es seguido al pie de la letra no se tendrán mayor problema para poner en marcha un servidor de correo.

4.3 BIBLIOGRAFÍA.

Fuentes Primarias:

Laboratorio de Tecnologías en Sistemas Informáticos ASI – EPN

Fuentes Secundarias:

Documentación:

- [Configuración de un completo servidor de correo seguro con Postfix y Cyrus] [Tutorial versión 1.0] (http://www.linuxsilo.net), Jaume Sabater, 23 de mayo de 2005.
- [Sistema de Correo Electrónico] [Tutorial] (http://www.ipb.pt), Sergio González González, 3 de junio de 2004.
- [Postfix + TLS + SASL on FreeBSD] [Tutorial version 1.3] (http://yocum.org), Tim Yocum, 22 de febrero de 2005.
- [Como configurar OpenLDAP como servidor de autenticación] [Tutorial] (http://www.linuxparatodos.net), Joel Barrios Dueñas, 2005.
- [Red Hat Enterprise Linux 4] [Manual de seguridad] (http://www.redhat.com/docs/), Comunidad RedHat, Thomas Rude.

Web:

- http://www.gnu.org Web oficial de la Fundación GNU.
- http://www.centos.org Web oficial de CentOS Linux.
- http://www.ubuntu.com Web oficial de la comunidad Ubuntu.
- http://www.postfix.org Web oficial de Postfix.
- http://spamassassin.apache.org/ Pagina oficial de SpamAssassin.
- http://www.mailscanner.info/ Pagina oficial de MailScanner.
- http://www.clamav.net/ Pagina oficial de ClamAV AntiVirus.

- http://www.openldap.org/ Pagina oficial de OpenLDAP.
- http://www.squirrelmail.org/ Pagina oficial de SquirrelMail.
- http://phpldapadmin.sourceforge.net/ Pagina oficial de phpldapadmin.
- http://www.openssl.org/ Pagina oficial de SSL/TLS.
- http://asg.web.cmu.edu/sasl/ Pagina oficial de cyrusSASL.
- http://www.linuxparatodos.net Documentos y afiches para iniciar con GNU/Linux.

ÍNDICE DE FIGURAS

CAPITULO II

MANUAL TÉCNICO

MANUAL DE ADMINISTRACIÓN

MANUAL TÉCNICO

2 INTRODUCCIÓN.

Este documento es parte del proyecto de titulación “Diseño e Implementación de un Servidor de Correo Electrónico Seguro, Webmail, y gestor de usuarios OpenLDAP para la carrera de ASI.

En tal sentido, el Manual Técnico contiene informes detallados de las instalaciones y configuraciones realizadas para poner en funcionamiento un MailServer.

3 OBJETIVO.

El objetivo principal de este Manual Técnico, es informar y controlar el cumplimiento de las rutinas de instalación y configuración requeridas para el funcionamiento de un servidor de correo electrónico.

Además permitirá:

- Simplificar la responsabilidad por fallas o errores.
- Facilitar las labores de mantenimiento del sistema.
- Guiar a administradores del sistema en caso de que este falle.
- Permitir que tanto usuarios como administradores del sistema tengan un esquema del funcionamiento y mantenimiento del sistema.

4 NORMAS DE OPERACIÓN.

Los lineamientos de este documento están elaborados clara y concisamente, a fin de que sean comprendidos incluso por personas no familiarizadas con ciertos temas o con el procedimiento mismo de funcionamiento. Esto implica que el usuario debe realizar en lo posible las siguientes normas:

- Respetar estrictamente los comandos[90] que son ejecutados en la consola[91] para

90 Ordenes en un lenguaje especial, que permiten a GNU con Linux ejecutar las funciones definidas por los comandos que escribes.

91 La consola de Linux es aquella pantalla negra donde puedes escribir los comandos.

realizar los debidos cambios o instalaciones (En sistemas tipo Unix no es lo mismo el prompt[92] con el signo #[93], que con el signo $[94]).

- Seguir el orden pre-establecido por el autor.
- No olvidarse que se está operando con servidores GNU con Linux (Dichos sistemas son muy potentes y seguros, pero a la vez potencialmente inestables si no se conoce nociones básicas del funcionamiento).

El documento también establece guías de reconocimiento para: comandos, mensajes, path (ubicación) de los archivos y documentos o archivos de los paquetes. Ejemplo.

- Comandos o mensajes que el sistema muestre presentaran el siguiente formato.

```
kas@pianist:~$ vi /etc/resolv.conf
root@pianist:~# vi /etc/resolv.conf

kas@pianist:~$ echo "hola mundo"
hola mundo
```

- El path de los archivos tendrán el siguiente formato: `/etc/init.d/rc.local`
- Los archivos de configuración presentarán el siguiente formato:

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

passwd:         compat
group:          compat
shadow:         compat
```

5 IMPLEMENTACIÓN DISEÑO INICIAL.

5.1.1 SISTEMA OPERATIVO.

5.1.1.1 INSTALACIÓN CENTOS.

El proceso de instalación del sistema operativo CentOS como sistema base para un

92 prompt: símbolo inicial del sistema en la Consola.
93 # Consola de usuarios con privilegios de administración (En sistemas tipo Unix conocido como root)
94 $ Consola de usuarios sin privilegios de administración.

servidor de correo electrónico es el siguiente:

- En la pantalla de Bienvenida del programa de instalación de CentOS, digitar “linux text”, esto permitirá que el proceso de instalación se realice en modo texto (requerido para servidores).

```
boot: linux text
```

Figura Instalación CentOS 1

El programa de instalación procederá y mostrara las siguientes pantallas:

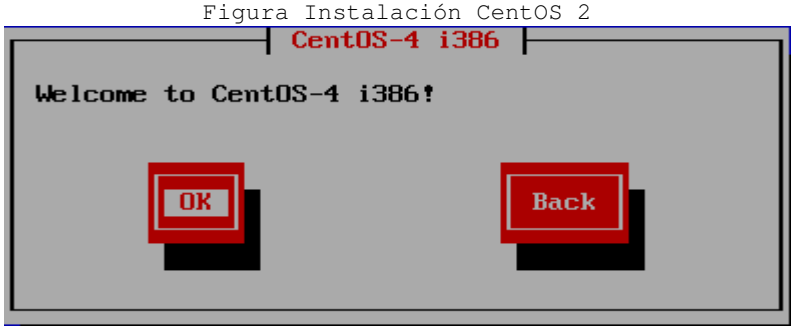
- Escaneo del CD de instalación; (Press OK, si los CD's de instalación son de fuentes no confiables o defectuosas).

Figura Instalación CentOS 2

- Bienvenida a la instalación de CentOS-4 i386; (Esta pantalla es mostrada luego

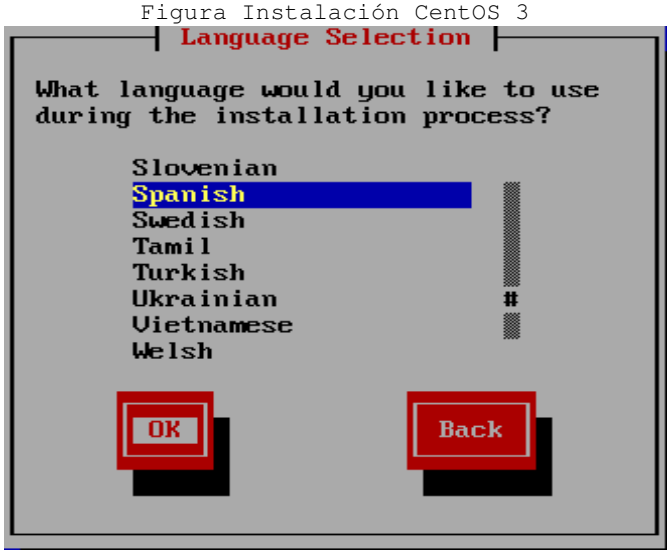
de que el programa de instalación verifica que el tipo de hardware sea compatible).

Figura Instalación CentOS 2



- Selección del idioma que se usará en la instalación; (Este idioma sólo es para el proceso de instalación).

Figura Instalación CentOS 3



- Selección del teclado; (Seleccionar “es”, común en teclados ecuatorianos).

Figura Instalación CentOS 4

- Tipo de Instalación; (Seleccionar Custom para personalizar los paquetes requeridos y eliminar los innecesarios).

Figura Instalación CentOS 5

- Configuración de la partición del disco duro; (Configurar con Disk Druid, para establecer tamaños personalizados).

Figura Instalación CentOS 6

- Esta pantalla muestra el proceso de partición del disco, en este caso se va a crear

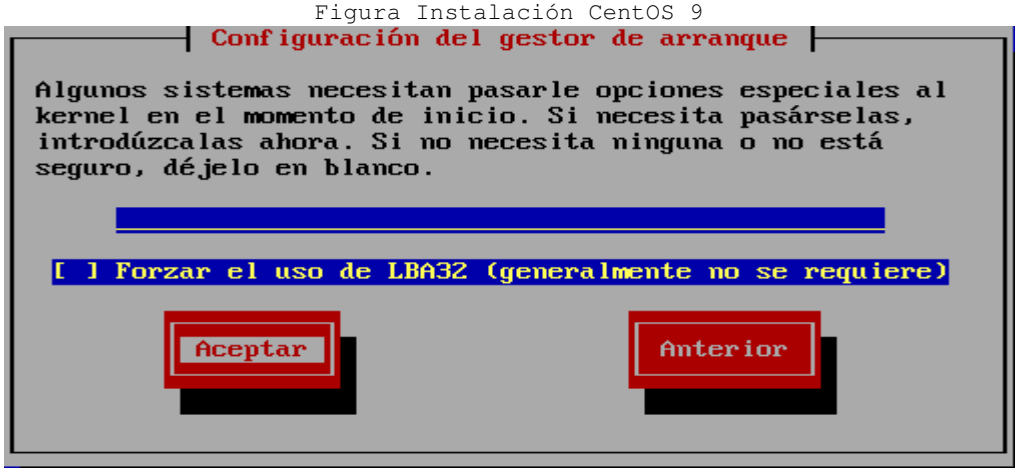
una partición para usuarios ”/home” con capacidad de 20 Gb. Este proceso se realizara para las otras particiones necesarias (“/”, “swap”, “/boot”, etc).

Figura Instalación CentOS 7

- Configuración del gestor de arranque; (Necesario para controlar el acceso al sistema por medio de la consola de administración del gestor de arranque Grub).

Figura Instalación CentOS 8

Figura Instalación CentOS 9



- La clave del gestor de arranque Grub es independiente de la contraseña del administrador del sistema (root).

Figura Instalación CentOS 10

Figura Instalación CentOS 11

Figura Instalación CentOS 12

- Configuración de la interfaz eth0; (Tarjeta de Red, estos datos deben ser proporcionados por el encargado de la Red en la organización).

Figura Instalación CentOS 13

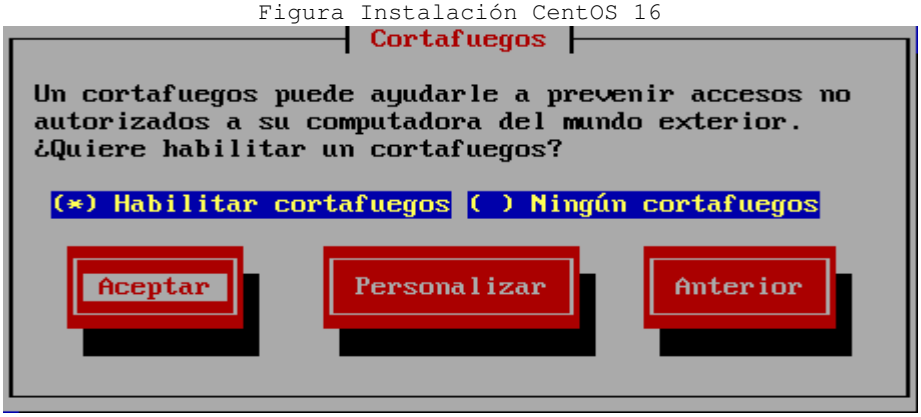
Figura Instalación CentOS 14

- Configuración del nombre del host.

Figura Instalación CentOS 15

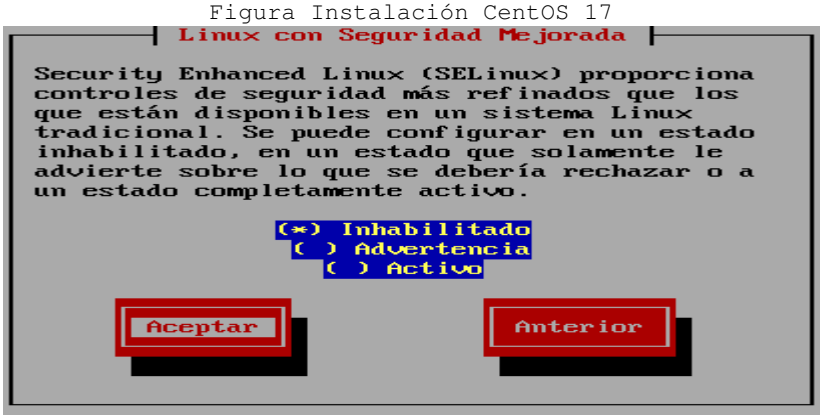
- Configuración Firewall; (Esta aplicación será configurada al finalizar el proyecto con reglas Iptables[95].)

Figura Instalación CentOS 16



- Seguridades extras de Linux.

Figura Instalación CentOS 17



95 Herramienta de administración de paquetes Ipv4 y filtros NAT.

- Soporte del idioma para el sistema; (Seleccionar English para compilar aplicaciones en lenguaje Perl).

Figura Instalación CentOS 18

- Selección zona horaria.

Figura Instalación CentOS 19

- Contraseña de root; (En lo posible escribir una contraseña con letras y números y mayor a 8 caracteres).

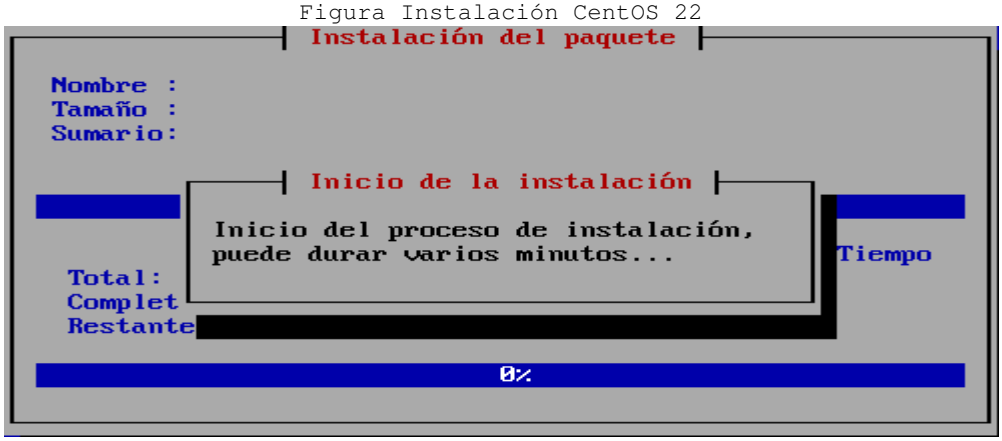
Figura Instalación CentOS 20

- Inicio de Instalación. (Este archivo tiene un registro completo del proceso de instalación que puede ser revisado si la instalación presentó algún error).

Figura Instalación CentOS 21

- Proceso de instalación; (Esta pantalla muestra en detalle los paquetes que se están instalando, el tiempo promedio de instalación y una descripción básica de cada uno.

Figura Instalación CentOS 22



Al terminar con el proceso de instalación, este reiniciara automáticamente. Luego que el sistema operativo reinicie proceder con la automatización del mismo.

Eliminar servicios del sistema (demonios) que no son requeridos:

MailScanner; acpid; cpuspped; crond; httpd; iptables; irqbalance; ldap; netfs; portmap; rawdevices; rpcgssd; saslauthd; smartd; sshd; syslog; xfs; xinetd

Configurar la variable de idioma:

```
[root@mailasi ~]# vi /etc/sysconfig/i18n
      LANG="en_US.UTF-8" a esto LANG="en_US"
```

```
[root@mailasi ~]# export LANG='en_US'
[root@mailasi ~]# reboot
```

5.1.2 **INSTALACIÓN OPENLDAP.**

Revisar paquetes instalados:

```
[root@mailasi ~]# rpm -q openldap
openldap-2.2.13-3
[root@mailasi ~]# rpm -q openldap-devel
openldap-devel-2.2.13-3
[root@mailasi ~]# rpm -q openldap-clients
package openldap-clients is not installed
                                        13
[root@mailasi ~]# rpm -q openldap-servers
package openldap-servers is not installed
[root@mailasi ~]# rpm -q authconfig
authconfig-4.6.10-rhel4.1
```

Instalar fuentes del CD #3 de CentOS:

```
[root@mailasi ~]# mount /media/cdrecorder/
mount: block device /dev/hda is write-protected, mounting read-only
[root@mailasi ~]# cd /media/cdrecorder/CentOS/RPMS/
[root@mailasi RPMS]# rpm -ivh openldap-clients-2.2.13-3.i386.rpm
warning: openldap-clients-2.2.13-3.i386.rpm: V3 DSA signature: NOKEY, key ID
443e1821
Preparing...                ###########################################
[100%]
      1:openldap-clients    ###########################################
[100%]
```

```
[root@mailasi RPMS]# rpm -ivh openldap-servers-2.2.13-3.i386.rpm
warning: openldap-servers-2.2.13-3.i386.rpm: V3 DSA signature: NOKEY, key ID
443e1821
Preparing...                          ########################################
[100%]
      1:openldap-servers              ########################################
[100%]
```

Generar la clave de administrador para el servidor openldap:

```
[root@mailasi openldap]# slappasswd -h {crypt}
New password: claveldap
Re-enter new password: claveldap
{CRYPT}ZhUpkAC5x3s8w
```

Configurar el servidor LDAP:

```
[root@mailasi ~]# cd /etc/openldap/
[root@mailasi openldap]# vi slapd.conf
       CACertificateFile /usr/share/ssl/asiCert/cacert.pem
       TLSCertificateFile /usr/share/ssl/asiCert/Cert.pem
       TLSCertificateKeyFile /usr/share/ssl/asiCert/PrivateKey.pem
       database           bdb
       suffix             "o=esfotasi"
       rootdn             "cn=administrador,dc=esfotasi,dc=o"
       rootpw                     {CRYPT}ZhUpkAC5x3s8w
```

Iniciar el servidor y cargar como servicio predeterminado:

```
[root@mailasi openldap]# /etc/init.d/ldap start
Checking configuration files for : config file testing succeeded
Starting slapd:                                            [ OK
[root@mailasi openldap]# chkconfig --level 35 ldap on
```

Crear y cargar en el directorio LDAP, la plantilla base.ldif con el diagrama básico de la organización:

```
[root@mailasi openldap]# vi base.ldif
       #Plantilla base.ldif
       #Autor: Edison Ayo

       dn: o=esfotasi
       o: esfotasi
       objectClass: top
       objectClass: organization

       dn: cn=administrador,o=esfotasi
       cn: administrador
```

```
objectClass: top
objectClass: organizationalRole

dn: ou=Correo,o=esfotasi
ou: Correo
objectClass: top
objectClass: organizationalUnit

dn: ou=Estudiantes,ou=Correo,o=esfotasi
ou: Estudiantes
objectClass: organizationalUnit
objectClass: top

dn: ou=Profesores,ou=Correo,o=esfotasi
ou: Profesores
objectClass: organizationalUnit
objectClass: top

dn: ou=Group,o=esfotasi
ou: Group
objectClass: top
objectClass: organizationalUnit
```

```
[root@mailasi openldap]# ldapadd -x -W -D 'cn=administrador, o=esfotasi' -h
127.0.0.1 -f base.ldif
Enter LDAP Password: claveldap
adding new entry "o=esfotasi"
adding new entry "cn=administrador,o=esfotasi"
adding new entry "ou=Estudiantes,ou=Correo,o=esfotasi"
adding new entry "ou=Profesores,ou=Correo,o=esfotasi"
adding new entry "ou=Otros,ou=Correo,o=esfotasi"
adding new entry "ou=Group,o=esfotasi"
```

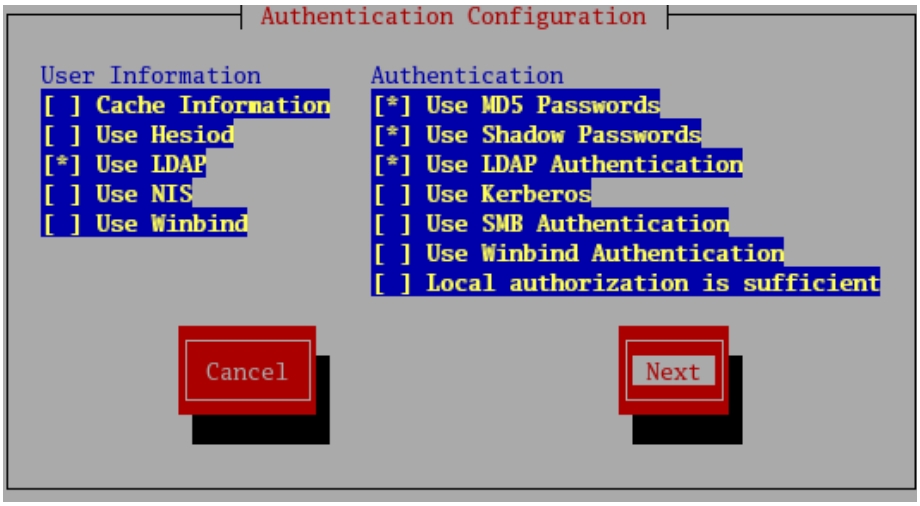
Configurar el cliente para el servidor LDAP:

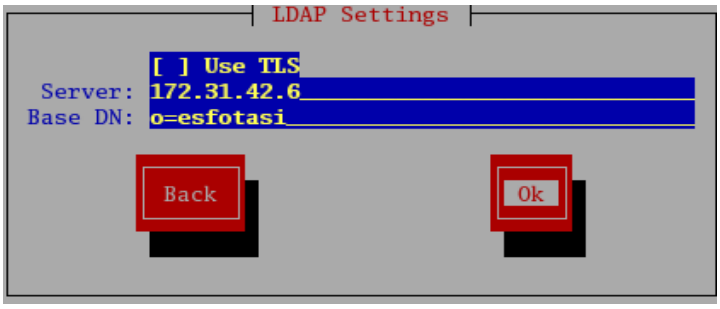
[root@mailasi openldap]# vi /etc/ldap.conf

host 172.31.42.8

base o=esfotasi

[root@mailasi openldap]# authconfig





Crear la plantilla tester-user.ldif y cargar un usuario en el directorio LDAP, para realizar pruebas de funcionamiento del servidor:

```
[root@mailasi openldap]# vi tester-user.ldif
       #Plantilla tester-user.ldif
       #Autor: Edison Ayo

        dn: uid=tester,ou=Correo,o=esfotasi
        uid: tester
        cn: Nombres
        sn: Apellidos
        userPassword: {CRYPT}PUg3kkHMYsjUI
        loginShell: /bin/bash
        uidNumber: 1003
        gidNumber: 5555500
        homeDirectory: /home/tester
        objectClass: top
        objectClass: person
        objectClass: posixAccount
        objectClass: shadowAccount


[root@mailasi openldap]# ldapadd -x -W -D 'cn=administrador, o=esfotasi' -h
```

```
127.0.0.1 -f tester-user.ldif
Enter LDAP Password: claveldap
adding new entry "uid=tester,ou=Correo,o=esfotasi"
```

Verificar que el usuario existe y esté dado de alta:

```
[root@mailasi ~]# getent passwd tester
tester:x:1003:5555500:Nombres:/home/tester:/bin/bash
[root@mailasi openldap]# su -l tester
su: warning: cannot change directory to /home/tester: No such file or
directory
-bash-3.00$
```

5.1.3 **INSTALACIÓN SSL/TLS.**

Revisar paquetes instalados:

```
[root@mailasi ~]# rpm -q openssl
openssl-0.9.7a-43.2
```

Crear los certificados y las llaves de acceso:

```
[root@mailasi ~]# openssl req -config /usr/share/ssl/openssl.cnf -new -x509
-nodes -out Cert.pem -keyout PrivateKey.pem -days 3650
Generating a 1024 bit RSA private key
..............++++++
....++++++
writing new private key to 'PrivateKey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:EC
State or Province Name (full name) [Berkshire]:Pichincha
Locality Name (eg, city) [Newbury]:Quito
Organization Name (eg, company) [My Company Ltd]:Escuela Politecnica Nacional
Organizational Unit Name (eg, section) []:Analisis de Sistemas Informaticos
Common Name (eg, your name or your server's hostname)
[]:http://esfot-asi.epn.edu.ec
Email Address []:admin@esfot-asi.epn.edu.ec
```

Mover los certificados generados a un único lugar seguro, para que puedan acceder los

servicios que requieran de certificados:

```
[root@mailasi ~]# mkdir /usr/share/ssl/asiCert/
[root@mailasi ~]# mv Cert.pem PrivateKey.pem /usr/share/ssl/asiCert/
[root@mailasi ~]# cd /usr/share/ssl/asiCert/
```

Copiar el archivo Cert.pem como cacert.pem, este ultimo es necesario cuando se tiene alguna empresa certificadora:

```
[root@mailasi   asiCert]# cp Cert.pem cacert.pem
[root@mailasi   asiCert]# ll
total 12
-rw-r--r-- 1    root root 1610 Jan 15 13:59 cacert.pem
-rw-r--r-- 1    root root 1610 Jan 15 13:59 Cert.pem
-rw-r--r-- 1    root root 887 Jan 15 13:59 PrivateKey.pem
```

5.1.4 **INSTALACIÓN SASL.**

Revisar paquetes instalados:

```
[root@mailasi ~]# rpm -q cyrus-sasl
cyrus-sasl-2.1.19-5.EL4
```

Iniciar el demonio saslauthd y cargar como servicio predeterminado:

```
[root@mailasi sasl2]# /etc/init.d/saslauthd start
Starting saslauthd:                                        [ OK ]
[root@mailasi ~]# chkconfig --level 35 saslauthd on
```

5.1.5 **INSTALACIÓN POSTFIX.**

Revisar paquetes instalados:

```
[root@mailasi ~]# rpm -q postfix
package postfix is not installed
```

Eliminar sendmail y las dependencias en el caso de que este instalado:

```
[root@mailasi ~]# rpm -q sendmail
sendmail-8.13.1-2
[root@mailasi ~]# rpm -e sendmail
error: Failed dependencies:
        /usr/sbin/sendmail is needed by (installed) redhat-lsb-3.0-8.EL.i386
        smtpdaemon is needed by (installed) mdadm-1.6.0-2.i386
[root@mailasi ~]# rpm -e redhat-lsb
[root@mailasi ~]# rpm -e mdadm
```

```
[root@mailasi ~]# rpm -e sendmail
warning: /etc/mail/submit.cf saved as /etc/mail/submit.cf.rpmsave
```

Instalar fuentes del CD #3 de CentOS:

```
[root@mailasi ~]# mount /media/cdrecorder/
mount: block device /dev/hda is write-protected, mounting read-only
[root@mailasi ~]# rpm -ivh /media/cdrecorder/CentOS/RPMS/postfix-2.1.5-
.2.RHEL4.i386.rpm
                                                                                18
warning: /media/cdrecorder/CentOS/RPMS/postfix-2.1.5-4.2.RHEL4.i386.rpm: V3
DSA signature: NOKEY, key ID 443e1821
Preparing...                ########################################### [100%]
   1:postfix                ########################################### [100%]
```

Configurar el servidor Postfix:

```
[root@mailasi postfix]# vi main.cf
       myhostname = esfot-asi.epn.edu.ec
       mydomain = epn.edu.ec
       inet_interfaces = all
       home_mailbox = Maildir/
       #
       # TLS/SSL (Encryption)
       #
       smtp_use_tls = yes
       smtpd_use_tls = yes
       smtp_tls_note_starttls_offer = yes
       smtpd_tls_key_file = /usr/share/ssl/asiCert/PrivateKey.pem
       smtpd_tls_cert_file = /usr/share/ssl/asiCert/Cert.pem
       smtpd_tls_CAfile = /usr/share/ssl/asiCert/cacert.pem
       smtpd_tls_loglevel = 1
       smtpd_tls_received_header = yes
       smtpd_tls_session_cache_timeout = 3600s
       tls_random_source = dev:/dev/urandom
       #
       # SASL (Authentication)
       #
       smtpd_sasl_auth_enable = yes
       smtpd_sasl_security_options = noanonymous
       smtpd_sasl_local_domain = $myhostname
       broken_sasl_auth_clients = yes
       smtpd_recipient_restrictions =
         permit_sasl_authenticated,
         permit_mynetworks,
         reject_unauth_destination
```

```
[root@mailasi postfix]# vi master.cf
       smtps     inet n       -       n       -       -       smtpd
         -o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
```

```
       587    inet    n       -       n       -       -       smtpd
         -o smtpd_enforce_tls=yes -o smtpd_sasl_auth_enable=yes
       tlsmgr    fifo -        -       n       300     1       tlsmgr
```

```
[root@mailasi ~]# mkdir /var/spool/postfix/Maildir
[root@mailasi ~]# chown postfix.postfix /var/spool/postfix/Maildir/
```

Iniciar el demonio postfix:

```
[root@mailasi ~]# /etc/init.d/postfix start
Starting postfix:                          [ OK ]
```

Integrar postfix con SASL:

```
[root@mailasi ~]# vi /usr/lib/sasl2/smtpd.conf
        pwcheck_method: saslauthd
```

Reiniciar los servicios saslauthd y postfix:

```
[root@mailasi ~]# /etc/init.d/saslauthd restart
Stopping saslauthd:                                [    OK   ]
Starting saslauthd:                                [    OK   ]
[root@mailasi ~]# /etc/init.d/postfix restart
Stopping postfix:                                 [   OK    ]
Starting postfix:                                 [   OK    ]
```

5.1.6 **INSTALACIÓN DOVECOT.**

Revisar paquetes instalados:

```
[root@mailasi ~]# rpm -q dovecot
squirrelmail-1.4.3a-12.EL4
```

Configurar dovecot:

```
[root@mailasi ~]# cd /etc/
[root@mailasi etc]# cp dovecot-example.conf dovecot.conf
[root@mailasi etc]# vi dovecot.conf
       protocols = imap imaps pop3 pop3s
       listen = *
       disable_plaintext_auth = no
       ssl_disable = no
       ssl_cert_file = /usr/share/ssl/asiCert/Cert.pem
       ssl_key_file = /usr/share/ssl/asiCert/PrivateKey.pem
       default_mail_env = maildir:/%h/Maildir
       first_valid_uid = 100
       last_valid_uid = 0
```

```
first_valid_gid = 1
last_valid_gid = 0
 passdb ldap {
      # Path for LDAP configuration file, see doc/dovecot-ldap.conf for
example
     args = /usr/local/etc/dovecot-ldap.conf
  }
 userdb ldap {
      # Path for LDAP configuration file, see doc/dovecot-ldap.conf for
example
     args = /usr/local/etc/dovecot-ldap.conf
  }
```

Integrar dovecot con el directorio LDAP:

Crear el archivo dovecot-ldap.conf y configurar las siguientes lineas:

```
[root@mailasi etc]# vi dovecot-ldap.conf
hosts = localhost
dn = cn=administrador,o=esfotasi
dnpass = claveldap
ldap_version = 3
base = o=esfotasi
deref = never
scope = subtree
user_attrs = uid,homeDirectory,,uid,,
user_filter = (&(objectClass=posixAccount)(uid=%u))
pass_attrs = uid,userPassword
default_pass_scheme = CRYPT
user_global_uid = 101
user_global_gid = 101
```

Iniciar el servicio dovecot:

```
[root@mailasi ~]# /etc/init.d/ dovecot  restart
Stopping dovecot:                                  [ OK ]
Starting dovecot:                                  [ OK ]
```

Crear el grupo vmail en el sistema:

```
[root@mailasi ~]# groupadd -r -g 200 vmail
```

Crear la plantilla del grupo vmail.ldif en el directorio LDAP:

```
[root@mailasi openldap]# vi vmail.ldif
 dn: cn=vmail,ou=Group,o=esfotasi
 cn: vmail
 gidNumber: 200
 objectClass: top
```

```
        objectClass: posixGroup
```

```
[root@mailasi openldap]# ldapadd -x -W -D 'cn=administrador, o=esfotasi' -h
127.0.0.1 -f vmail.ldif
Enter LDAP Password: claveldap
adding new entry "cn=vmail,ou=Group,o=esfotasi"
```

Crear el home de los usuarios de correo:

```
[root@mailasi correo]# mkdir -vp -m 2755 mail-asi
mkdir: created directory `mail-asi'
[root@mailasi correo]# chown -v root.vmail mail-asi/
changed ownership of `mail-asi/' to root:vmail
```

5.1.7 **PRUEBAS DE FUNCIONALIDAD I.**

Crear un usuario de correo:

```
[root@mailasi openldap]# vi mail-user.ldif
       #Plantilla mail-user.ldif
       #Autor: Edison Ayo

       dn: uid=edison,ou=Estudiantes,ou=Correo,o=esfotasi
        uid: edison
        cn: Edison
        sn: Ayo
        userPassword: {CRYPT}PUg3kkHMYsjUI
        loginShell: /bin/bash
        uidNumber: 1000
        gidNumber: 200
        objectClass: top
        objectClass: person
        objectClass: posixAccount
        objectClass: shadowAccount
        homeDirectory: /correo/mail-asi/edison
```

```
[root@mailasi openldap]# ldapadd -x -W -D 'cn=administrador, o=esfotasi' -h
127.0.0.1 -f mail-user.ldif
Enter LDAP Password: claveldap
adding new entry "uid=edison,ou=Estudiantes,ou=Correo,o=esfotasi"
```

Pruebas del servidor MTA postfix con el comando telnet:

- Integración con TLS y SASL:

```
kas@pianist:~$ telnet 172.31.42.6 25
Trying 172.31.42.6...
```

```
Connected to 172.31.42.6.
Escape character is '^]'.
220 esfot-asi.epn.edu.ec ESMTP Postfix
ehlo esfot-asi
250-esfot-asi.epn.edu.ec
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN CRAM-MD5 LOGIN DIGEST-MD5
250-AUTH=PLAIN CRAM-MD5 LOGIN DIGEST-MD5
250 8BITMIME
```

- Envío de mensajes:

```
kas@pianist:~$ telnet 172.31.42.6 25
Trying 172.31.42.6...
Connected to 172.31.42.6.
Escape character is '^]'.
220 esfot-asi.epn.edu.ec ESMTP Postfix
mail from: <tester@esfot-asi.epn.edu.ec>
250 Ok
rcpt to: <edison@esfot-asi.epn.edu.ec>
250 Ok
data
                                    22
354 End data with <CR><LF>.<CR><LF>
hola, este es un mensaje de prueba.
.
250 Ok: queued as 3E988287FC
quit
221 Bye
Connection closed by foreign host.
```

Pruebas del servidor dovecot:

- Recepción de correos (POP3):

```
kas@pianist:~$ telnet 172.31.42.6 110
Trying 172.31.42.6...
Connected to 172.31.42.6.
Escape character is '^]'.
+OK Dovecot ready.
user edison
+OK
pass secret
+OK Logged in.
list
+OK 6 messages:
```

```
1 1903
2 2038
3 3843
4 1390
5 2015
6 526
.
retr 6
+OK 526 octets
Return-Path: <tester@esfot-asi.epn.edu.ec>
X-Original-To: edison@esfot-asi.epn.edu.ec
Delivered-To: edison@esfot-asi.epn.edu.ec
Received: from unknown (unknown [172.31.42.55])
        by esfot-asi.epn.edu.ec (Postfix) with SMTP id 3E988287FC
        for <edison@esfot-asi.epn.edu.ec>; Tue, 16 Jan 2007 11:51:35 -0500 (ECT)
Message-Id: <20070116165135.3E988287FC@esfot-asi.epn.edu.ec>
Date: Tue, 16 Jan 2007 11:51:35 -0500 (ECT)
From: tester@esfot-asi.epn.edu.ec
To: undisclosed-recipients:;
hola, este es un mensaje de prueba.
.
quit
```

- Recepción de correos (IMAP):

```
kas@pianist:~$ telnet 172.31.42.6 143
Trying 172.31.42.6...
Connected to 172.31.42.6.
Escape character is '^]'.
                                                                        23
* OK Dovecot ready.
x login edison secret
x OK Logged in.
x select inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen    \Draft \*)] Flags
permitted.
* 6 EXISTS
* 0 RECENT
* OK [UNSEEN 1] First unseen.
* OK [UIDVALIDITY 1168954065] UIDs valid
* OK [UIDNEXT 7] Predicted next UID
x OK [READ-WRITE] Select completed.
x fetch 6 (flags body[header.fields (subject)])
* 6 FETCH (FLAGS (\Seen) BODY[HEADER.FIELDS (SUBJECT)] {2}
)
x OK Fetch completed.
x fetch 6 (body[text])
* 6 FETCH (BODY[TEXT] {37}
hola, este es un mensaje de prueba.
)
```

```
x OK Fetch completed.
x logout
* BYE Logging out
x OK Logout completed.
```

6 IMPLEMENTACIÓN DISEÑO COMPLEMENTARIO.

6.1.1 INSTALACIÓN MAILSCANNER.

Compilar e Instalar MailScanner:

```
[root@mailasi ~]# tar -xzvf MailScanner-4.57.6-1.rpm.tar.gz
[root@mailasi ~]# cd MailScanner-4.57.6-1
[root@mailasi MailScanner-4.57.6-1]# ./install.sh
Good. You have the patch command.
Good, you have /usr/src/redhat in place.
Writing a .rpmmacros file in your home directory to stop
unpackaged files breaking the build process.
You can delete it once MailScanner is installed if you want to.
.
.
NOTE: If you get lots of errors here, run the install.sh script
NOTE: again with the command "./install.sh nodeps"
Preparing...                ########################################### [100%]
   1:mailscanner            ########################################### [100%]
                                                                    24
Good, SpamAssassin site rules found in /etc/mail/spamassassin
[root@mailasi MailScanner-4.57.6-1]# service postfix stop
Shutting down postfix:                                     [ OK ]
[root@mailasi MailScanner-4.57.6-1]# chkconfig postfix off
```

Integrar MailScanner con postfix:

```
[root@mailasi MailScanner-4.57.6-1]# cd /etc/MailScanner/
[root@mailasi MailScanner]# vi MailScanner.conf
       %org-name% = Escuela Politecnica Nacional
       %org-long-name% = Tecnología en Analísis de Sistemas Informáticos
       %web-site% = http://esfot-asi.epn.edu.ec
       Run As User = postfix
       Run As Group = postfix
       Incoming Queue Dir = /var/spool/postfix/hold
       Outgoing Queue Dir = /var/spool/postfix/incoming
       MTA = postfix
```

Cambiar permisos:

```
[root@mailasi MailScanner]# chown postfix.root /var/spool/postfix/
[root@mailasi MailScanner]# chown postfix.postfix
/var/spool/MailScanner/incoming/
```

```
[root@mailasi MailScanner]# chown postfix.postfix
/var/spool/MailScanner/quarantine/
```

Iniciar el servicio MailScanner:

```
[root@mailasi MailScanner]# /etc/init.d/MailScanner start
Starting MailScanner daemons:
            incoming postfix:                              [ OK ]
            outgoing postfix:                              [ OK ]
            MailScanner:                                   [ OK ]
[root@mailasi MailScanner]# chkconfig --level 2345 MailScanner on
```

6.1.2 **INSTALACIÓN SPAMASSASSIN.**

Revisar paquetes instalados:

```
[root@mailasi ~]# rpm -q spamassassin
spamassassin-3.0.4-1.el4
```

Integrar SpamAssassin con MailScanner:

```
[root@mailasi ~]# vi /etc/MailScanner/MailScanner.conf
        Use SpamAssassin = yes
        Required SpamAssassin Score = 4
        High SpamAssassin Score = 6.5
        SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
```

```
[root@mailasi ~]# mkdir /var/spool/MailScanner/spamassassin
[root@mailasi ~]# chown postfix.postfix /var/spool/MailScanner/spamassassin/
```

6.1.3 **INSTALACIÓN CLAMAV.**

Compilar e Instalar ClamAV:

```
[root@mailasi ~]# tar xzvf install-Clam-0.88.7-SA-3.1.7
[root@mailasi ~]# cd install-Clam-0.88.7-SA-3.1.7
[root@mailasi install-Clam-0.88.7-SA-3.1.7]# ./install.sh
Good, you appear to only have 1 copy of Perl installed: /usr/bin/perl
Found gcc.
cc is really gcc.
Good, I have found GNU tar in /bin/tar.
.
.
Good, SpamAssassin site rules found in "/etc/mail/spamassassin"
Good, the link was created to /etc/MailScanner
Make sure your MailScanner.conf says "Use SpamAssassin = yes"
```

Actualizar ClamAV:

```
[root@mailasi install-Clam-0.88.7-SA-3.1.7]# clamd
[root@mailasi install-Clam-0.88.7-SA-3.1.7]# freshclam
ClamAV update process started at Tue Jan 16 14:31:32 2007
main.cvd is up to date (version: 42, sigs: 83951, f-level: 10, builder: tkojm)
daily.cvd is up to date (version: 2457, sigs: 3100, f-level: 9, builder: arnaud)
```

Reiniciar el servicio de MailScanner:

```
[root@mailasi ~]# /etc/init.d/MailScanner restart
Shutting down MailScanner daemons:
         MailScanner:         [ OK ]
         incoming postfix:    [ OK ]
         outgoing postfix:    [ OK ]
Starting MailScanner daemons:
         incoming postfix:    [ OK ]
         outgoing postfix:    [ OK ]
         MailScanner:         [ OK ]
```

6.1.4 **PRUEBAS DE FUNCIONALIDAD II.**

Pruebas de envío con el comando telnet :

```
kas@pianist:~$ telnet 172.31.42.6 25
Trying 172.31.42.6...
Connected to 172.31.42.6.
Escape character is '^]'.
220 esfot-asi.epn.edu.ec ESMTP Postfix
mail from: <edison@esfot-asi.epn.edu.ec>
250 Ok
rcpt to: <edison@esfot-asi.epn.edu.ec>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
HOla, este es un mensaje de prueba de MailScanner, SpamAssassin, ClamAV
.
250 Ok: queued as 857662887A
quit
221 Bye
Connection closed by foreign host.
```

Pruebas de recepción por medio del comando telnet al puerto 110 (POP3):

```
kas@pianist:~$ telnet 172.31.42.6 110
Trying 172.31.42.6...
Connected to 172.31.42.6.
Escape character is '^]'.
+OK Dovecot ready.
```

```
user edison
+OK
pass secret
+OK Logged in.
list
+OK 8 messages:
1 1903
2 2038
7 1253
8 1023
.
retr 8
+OK 1023 octets
Return-Path: <edison@esfot-asi.epn.edu.ec>
X-Original-To: edison@esfot-asi.epn.edu.ec
Delivered-To: edison@esfot-asi.epn.edu.ec
Received: from esfot-asi (unknown [172.31.42.55])
        by esfot-asi.epn.edu.ec (Postfix) with ESMTP id 857662887A
        for <edison@esfot-asi.epn.edu.ec>; Tue, 16 Jan 2007 15:53:37 -0500 (ECT)
Message-Id: <20070116205337.857662887A@esfot-asi.epn.edu.ec>
Date: Tue, 16 Jan 2007 15:53:37 -0500 (ECT)
From: edison@esfot-asi.epn.edu.ec
To: undisclosed-recipients:;
MIME-Version: 1.0
X-Escuela Politecnica Nacional-MailScanner-Information: Please contact the ISP fo
r more information
X-Escuela Politecnica Nacional-MailScanner: Found to be clean
X-Escuela Politecnica Nacional-MailScanner-SpamScore: s
X-Escuela Politecnica Nacional-MailScanner-From: edison@esfot-asi.epn.edu.ec
X-Spam-Status: No
HOla, este es un mensaje de prueba de MailScanner, SpamAssassin, ClamAV
--
This message has been scanned for viruses and
dangerous content by MailScanner, and is
believed to be clean.
quit
+OK Logging out.
Connection closed by foreign host.
```

7 IMPLEMENTACIÓN DISEÑO FINAL.

7.1.1 INSTALACIÓN SQUIRRELMAIL.

Revisar paquetes instalados:

```
[root@mailasi ~]# rpm -q squirrelmail
package squirrelmail is not installed
```

Instalar fuentes del CD #3 de CentOS:

```
[root@mailasi ~]# mount /media/cdrecorder/
mount: block device /dev/hda is write-protected, mounting read-only
```

```
[root@mailasi ~]# rpm -ivh /media/cdrecorder/CentOS/RPMS/squirrelmail-1.4.3a-
12.EL4.centos4.noarch.rpm
warning: /media/cdrecorder/CentOS/RPMS/squirrelmail-1.4.3a-
12.EL4.centos4.noarch.rpm: V3 DSA signature: NOKEY, key ID 443e1821
Preparing...                ########################################### [100%]
   1:squirrelmail           ########################################### [100%]
```

Configurar SquirrelMail:

```
[root@mailasi config]# ./conf.pl
              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 (LDAP)
7. Message of the Day (MOTD)
8. Plugins
9. Database
D.  Set pre-defined settings for specific IMAP servers
C.  Turn color off
S   Save data
Q   Quit
Command >>1
SquirrelMail Configuration : Read: config.php (1.4.0)
--------------------------------------------------------
Organization Preferences
1. Organization Name       : ESFOT-ASI
2. Organization Logo       : ../images/sm_logo.png
3. Org. Logo Width/Height : (308/111)
4. Organization Title      : Bienvenido al Webmail de ASI
5. Signout Page            :
6. Default Language        : es_ES
7. Top Frame               : _top
8. Provider link           : http://esfot-asi.epn.edu.ec
9. Provider name           : ASI
R   Return to Main Menu
C.  Turn color off
S   Save data
Q   Quit
Command >> r

SquirrelMail Configuration : Read: config.php (1.4.0)
--------------------------------------------------------
Server Settings
General
```



```
-------
```

```
1. Domain                  : esfot-asi.epn.edu.ec
2. Invert Time             : false
3. Sendmail or SMTP        : Sendmail
A.  Update IMAP Settings   : localhost:143 (uw)
B.  Change Sendmail Config : /usr/sbin/sendmail
R   Return to Main Menu
C.  Turn color off
S   Save data
Q   Quit
Command >> r
```

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Folder Defaults
1. Default Folder Prefix          : mail/
2. Show Folder Prefix Option      : true
3. Trash Folder                   : Papelera
4. Sent Folder                    : Enviados
5. Drafts Folder                  : Borradores
6. By default, move to trash      : true
7. By default, move to sent       : true
8. By default, save as draft      : true
9. List Special Folders First     : true
10. Show Special Folders Color    : true
11. Auto Expunge                  : true
12. Default Sub. of INBOX         : false
13. Show 'Contain Sub.' Option    : true
14. Default Unseen Notify         :2
15. Default Unseen Type           :1
16. Auto Create Special Folders   : true
17. Folder Delete Bypasses Trash : false
18. Enable /NoSelect folder fix   : false
R   Return to Main Menu
C.  Turn color off
S   Save data
Q   Quit
Command >> s
Data saved in config.php
Press enter to continue...
Command >> q
```

Habilitar SSL para Webmail:

```
[root@mailasi ~]# cd /etc/httpd/conf.d/
[root@mailasi conf.d]# vi ssl.conf
       Listen 0.0.0.0:443
       SSLCertificateFile /usr/share/ssl/asiCert/Cert.pem
       SSLCertificateKeyFile /usr/share/ssl/asiCert/PrivateKey.pem
```

```
[root@mailasi conf.d]# vi squirrelmail.conf
       <Location /webmail>
```

```
                SSLRequire SSL
        </Location>
[root@mailasi conf.d]# /etc/init.d/httpd restart
```

Al terminar la configuración de SquirrelMail con conexión segura mediante certificados digitales este el link debe ser escrito de la siguientes forma:

https://nombre-del-servidor-de-correo/webmail

Al iniciar la conexión el servidor emitirá el debido certificado que autorice o no el uso del servicio.

7.1.2 **INSTALACIÓN PHPLDAPADMIN.**

Instalar phpldapadmin:

```
[root@mailasi ~]# cp phpldapadmin /var/www/html/
[root@mailasi ~]# cd /var/www/html/
[root@mailasi html]# tar xzvf phpldapadmin-0.9.8.2.tar.gz
```

Configurar phpldapadmin:

```
[root@mailasi html]# mv phpldapadmin-0.9.8.2 ldapadmin
[root@mailasi html]# cd ldapadmin/config/
[root@mailasi config]# cp config.php.example config.php
```

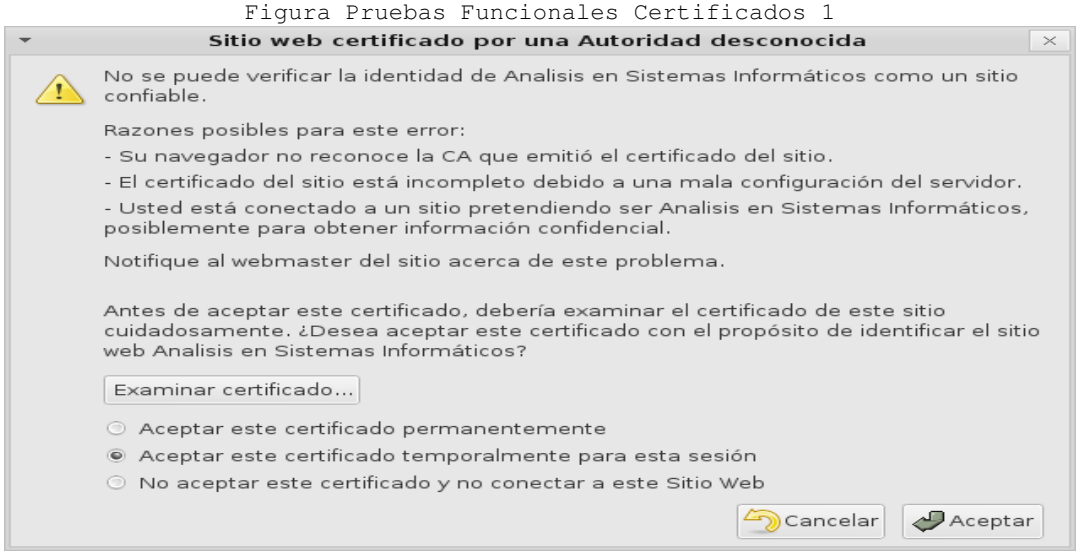
PhpLDAPadmin, es una aplicativo web para administrar el directorio LDAP; por lo tanto su uso y administración esta detallado en el Anexo Manual de Administración:

8 PRUEBAS DE FUNCIONALIDAD FINALES.

Envío de correo por medio del servicio Webmail:

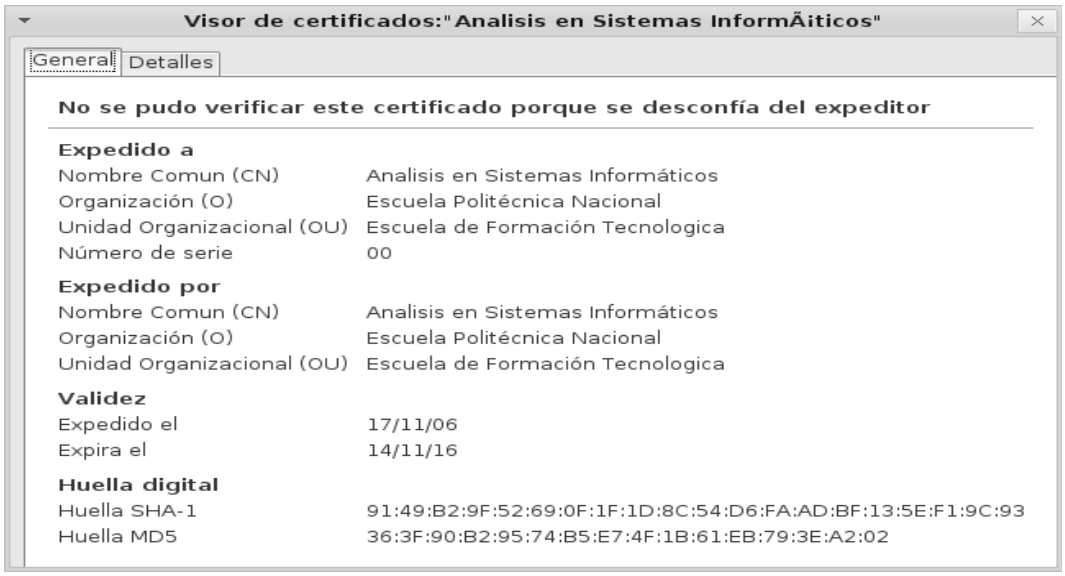
- Teclear en el navegador la dirección del servidor: https://esfotasi.epn.edu.ec/webmail como el servidor está configurado para operar realizando conexión segura SSL/TLS, mostrará los respectivos certificados para establecer la conexión con el servidor de correo Webmail.
- Este es el certificado que el servidor envía para autorizar la conexión:

Figura Pruebas Funcionales Certificados 1



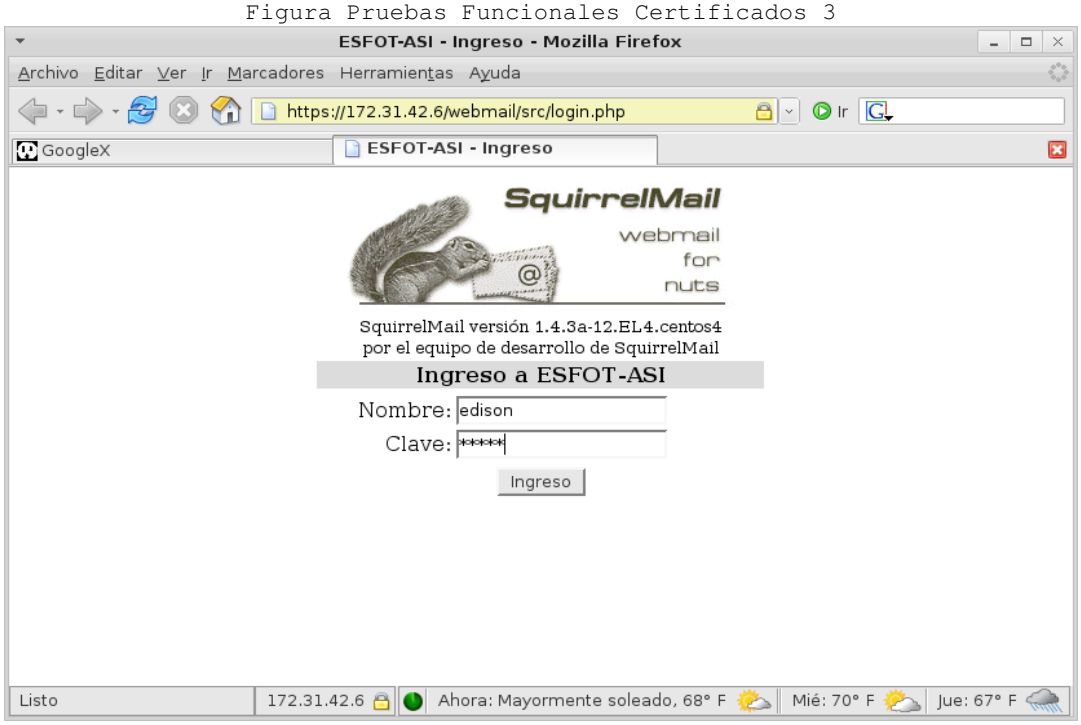
- Se puede examinar el certificado presionando el botón" Examinar certificado":

Figura Pruebas Funcionales Certificados 2



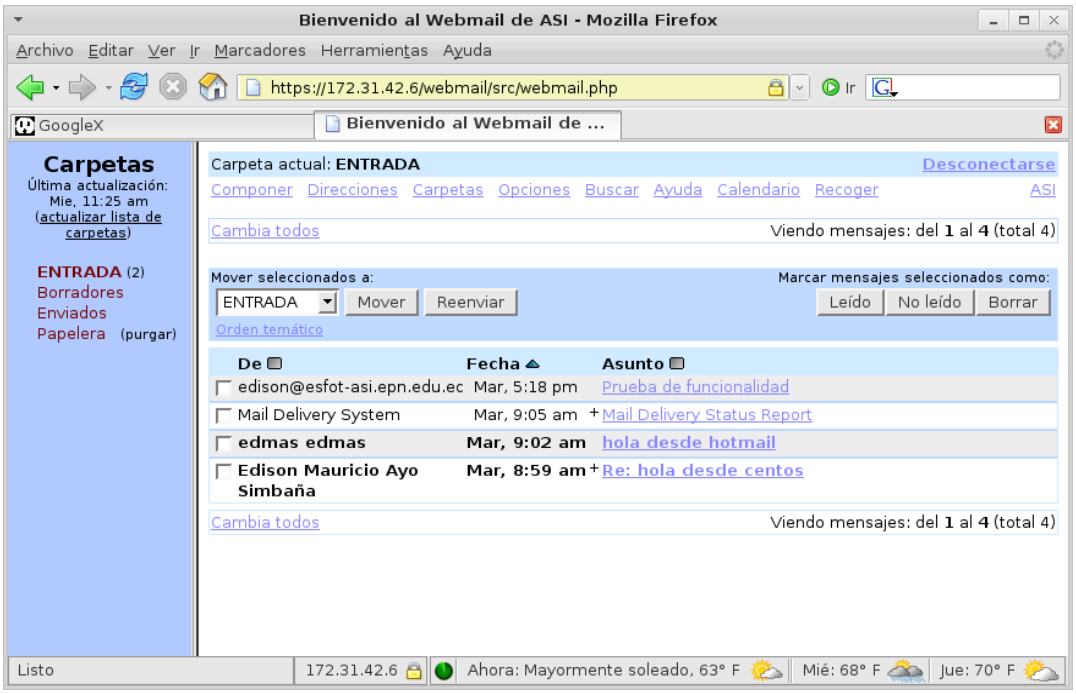
- Al presionar “Aceptar” se establecerá la conexión con el servidor.

Figura Pruebas Funcionales Certificados 3



- Teclear “Nombre de usuario y Clave”
- Si los datos ingresados son correctos, se accede al servicio Webmail:

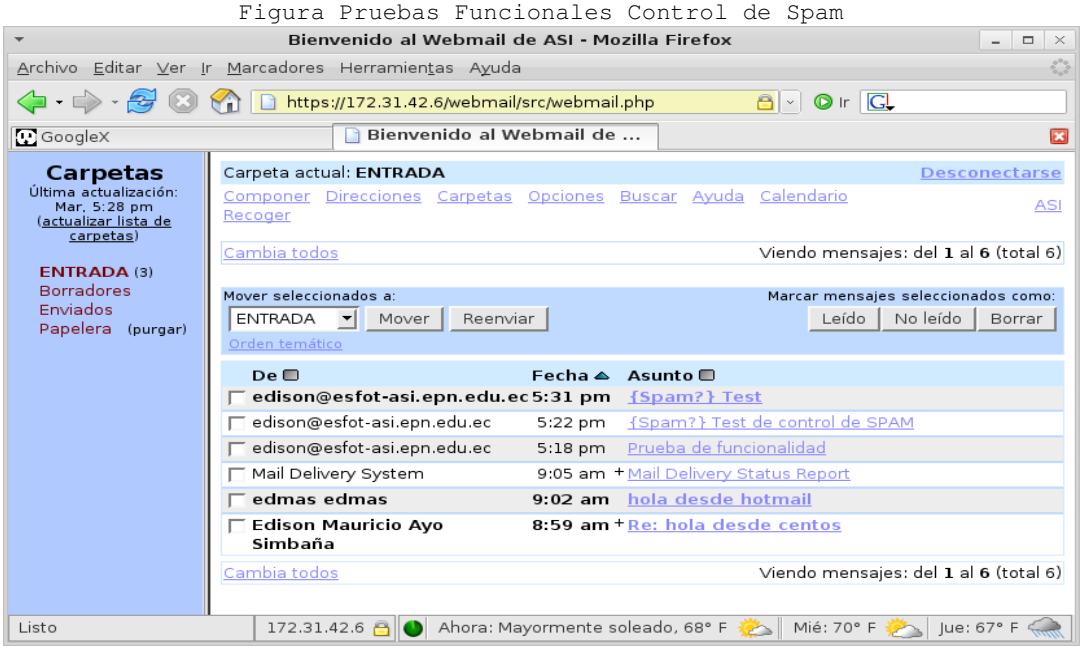
Figura Pruebas Funcionales Webmail



Pruebas de control de Spam:

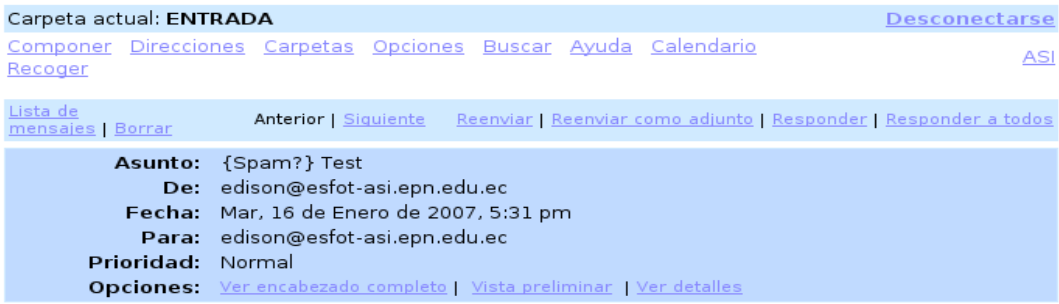
- Para realizar la prueba de control de Spam, se utilizarán ejemplos de correos con Spam que se pueden obtener del Internet.
- En el caso que el correo se Spam, este sera marcado automáticamente por MailScanner.

Figura Pruebas Funcionales Control de Spam



- La pantalla muestra que el correo enviado fue marcado como {Spam?}, dichos correos no son borrados, pero si superan el limite establecido de envíos MailScanner automáticamente bloqueara el usuario o en algunos caso borrará los correos del o las personas que envíen correo masivo.
- Para entender mejor el funcionamiento de MailScanner se puede presionar “Ver encabezado completo” y mostrara un detalle completo del correo.

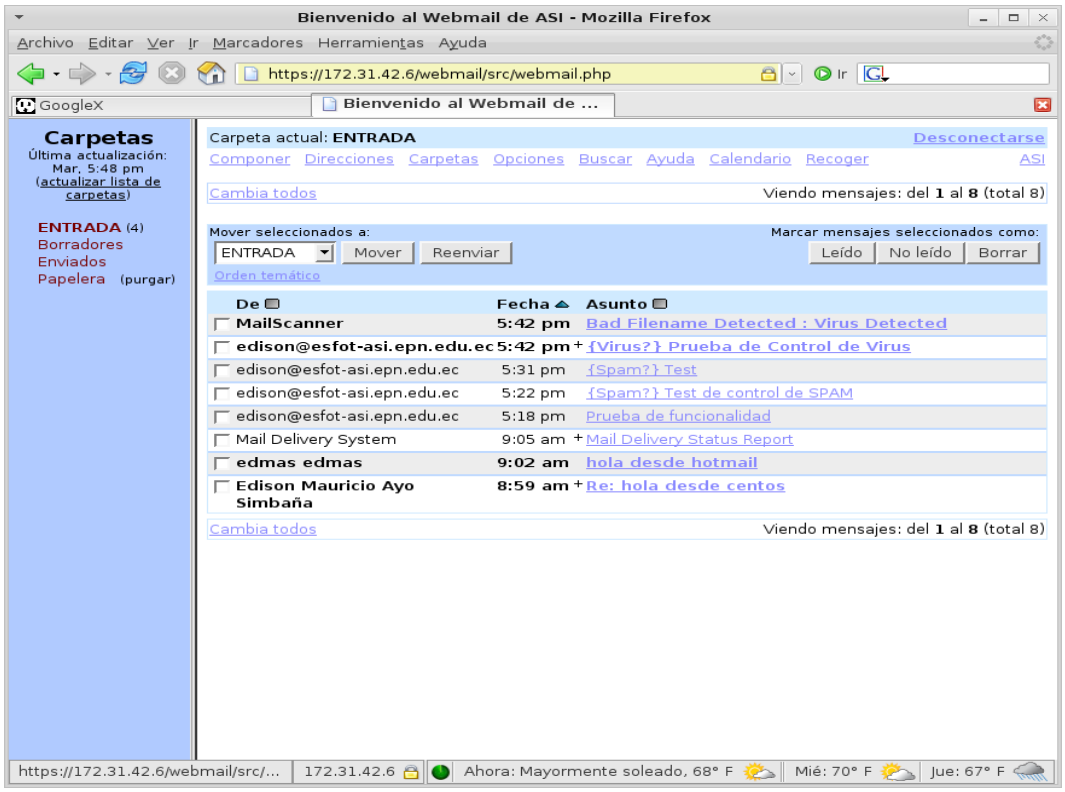
Figura Pruebas Funcionales Control de Spam



Pruebas de control de Virus:

- Estas pruebas se la realiza con el virus de prueba eicar.com, eicar.zip, eicar2.zip; que se los obtiene del Internet.
- Se procederá con el envío de un correo electrónico adjuntando el archivo eicar (virus); si MailScanner esta funcionando correctamente y controla virus este sera marcado.

Figura Pruebas Funcionales Control de Virus



- La pantalla muestra que efectivamente MailScanner opera correctamente y notifica el correo infectado en el asunto del mensaje {Virus?}.
- Se debe tener en cuenta que un correo electrónico que este infectado MailScanner solo eliminara el archivo infectado y el correo llegara a su destinatario pero con el reporte correspondiente.
- En el caso que el usuario requiera de dicho archivo debe contactar con el administrador del sistema y solicitar la debida copia del archivo que guarda MailScanner en el directorio de cuarentena.

MANUAL DE ADMINISTRACIÓN

1 **ÍNDICE.**

2 INTRODUCCIÓN.

Este documento es parte del proyecto de titulación “Diseño e Implementación de un Servidor de Correo Electrónico Seguro, Webmail, y gestor de usuarios OpenLDAP para la carrera de ASI.

En tal sentido este Manual de administración contiene el soporte necesarios para administrar el sistema operativo en general y la gestión de usuarios de correo electrónico con el aplicativo phpldapadmin.

3 OBJETIVO.

El objetivo principal de este Manual de Administración, es informar y controlar el cumplimiento de las rutinas de administración requeridas para el funcionamiento de un servidor de correo electrónico.

4 NORMAS DE OPERACIÓN.

Los lineamientos de este documento están elaborados clara y concisamente, a fin de que sean comprendidos incluso por personas no familiarizadas con ciertos temas o con el procedimiento mismo de funcionamiento. Esto implica que el usuario debe realizar en lo posible las siguientes normas:

- Respetar estrictamente los comandos[96] que son ejecutados en la consola[97] para realizar los debidos cambios o instalaciones (En sistemas tipo Unix no es lo mismo el prompt[98] con el signo #[99], que con el signo $[100]).

96 Ordenes en un lenguaje especial, que permiten a GNU con Linux ejecutar las funciones definidas por los comandos que escribes.
97 La consola de Linux es aquella pantalla negra donde puedes escribir los comandos.
98 prompt: símbolo inicial del sistema en la Consola.
99 # Consola de usuarios con privilegios de administración (En sistemas tipo Unix conocido como root)
100 $ Consola de usuarios sin privilegios de administración.

- Seguir el orden pre-establecido por el autor.
- No olvidarse que se está operando con servidores GNU con Linux (Dichos sistemas son muy potentes y seguros, pero a la vez potencialmente inestables si no se conoce nociones básicas del funcionamiento).

El documento también establece guías de reconocimiento para: comandos, mensajes, path (ubicación) de los archivos y documentos o archivos de los paquetes. Ejemplo.

- Comandos o mensajes que el sistema muestre presentaran el siguiente formato.

```
kas@pianist:~$ vi /etc/resolv.conf
root@pianist:~# vi /etc/resolv.conf

kas@pianist:~$ echo "hola mundo"
hola mundo
```

- El path de los archivos tendrán el siguiente formato: `/etc/init.d/rc.local`
- Los archivos de configuración presentaran el siguiente formato:

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

passwd:         compat
group:          compat
shadow:         compat
```

4.1.1 **ADMINISTRACIÓN DEL SISTEMA OPERATIVO CENTOS.**

El sistema operativos CentOS, está personalizado para proveer el servicio de correo electrónico, esto implica que se deben revisar periódicamente los logs del sistema.
Algunos de los comandos mas comunes requeridos para la administración son los siguientes:

Revision de logs del sistema. Este comando debe ser ejecutado periódicamente para ver los mensajes de error, actualización, conexiones, configuraciones, etc. Que el sistema

muestra con el fin de administrar el sistema de correo.

```
[root@mailasi ~]# tail -f /var/log/maillog
Jan 17 11:44:35 mailasi postfix/smtpd[11779]: connect from
smtprelay.uio.telconet.net[200.93.216.6]
Jan 17 11:44:49 mailasi postfix/smtpd[11779]: setting up TLS connection from
smtprelay.uio.telconet.net[200.93.216.6]
Jan 17 11:44:50 mailasi postfix/smtpd[11779]: TLS connection established from
smtprelay.uio.telconet.net[200.93.216.6]: TLSv1 with cipher DHE-RSA-AES256-SHA
(256/256 bits)
Jan 17 11:45:02 mailasi postfix/smtpd[11779]: NOQUEUE: reject: RCPT from
smtprelay.uio.telconet.net[200.93.216.6]: 554 <mtirira@esfotasi.epn.edu.ec>:
Relay access denied; from=<Rodrigues@billwaldack.com>
to=<mtirira@esfotasi.epn.edu.ec> proto=ESMTP helo=<smtprelay.uio.telconet.net>
Jan 17 11:45:46 mailasi dovecot: imap-login: Login: user=<edison>, method=PLAIN,
rip=127.0.0.1, lip=127.0.0.1, secured
Jan 17 11:45:46 mailasi dovecot: IMAP(edison): Disconnected: Logged out
Jan 17 11:46:47 mailasi postfix/smtpd[11779]: disconnect from
smtprelay.uio.telconet.net[200.93.216.6]
Jan 17 11:50:47 mailasi dovecot: imap-login: Login: user=<edison>, method=PLAIN,
rip=127.0.0.1, lip=127.0.0.1, secured
Jan 17 11:50:47 mailasi dovecot: IMAP(edison): Disconnected: Logged out
Jan 17 11:55:47 mailasi dovecot: imap-login: Login: user=<edison>, method=PLAIN,
rip=127.0.0.1, lip=127.0.0.1, secured
Jan 17 11:55:47 mailasi dovecot: IMAP(edison): Disconnected: Logged out
Jan 17 12:00:47 mailasi dovecot: imap-login: Login: user=<edison>, method=PLAIN,
rip=127.0.0.1, lip=127.0.0.1, secured
Jan 17 12:00:47 mailasi dovecot: IMAP(edison): Disconnected: Logged out
Jan 17 12:01:01 mailasi update.virus.scanners: Delaying cron job up to 600
seconds
Jan 17 12:02:11 mailasi update.virus.scanners: Found clamav installed
Jan 17 12:02:11 mailasi update.virus.scanners: Running autoupdate for clamav
Jan 17 12:02:16 mailasi ClamAV-autoupdate[11852]: ClamAV did not need updating
Jan 17 12:02:16 mailasi update.virus.scanners: Found generic installed
Jan 17 12:02:16 mailasi update.virus.scanners: Running autoupdate for generic
Jan 17 12:05:48 mailasi dovecot: imap-login: Login: user=<edison>, method=PLAIN,
rip=127.0.0.1, lip=127.0.0.1, secured
Jan 17 12:05:48 mailasi dovecot: IMAP(edison): Disconnected: Logged out
```

Revisar periódicamente la cola de mensajes:

```
[root@mailasi ~]# tail -f /var/log/maillog
```

Eliminar periódicamente las colas (mqueue) de los correos acumulados:

```
[root@mailasi ~]# cd /var/spool/mqueue.in
```

Cambiar periódicamente las claves de los administradores (root, openldap, grub).

El sistema de correo esta implementado de tal manera que si se requiere de alguna actualización de algún paquete se lo puede realizar sin impedimento alguno.

El sistema incorpora generadores de directorios “HOME”, para los usuarios de correo, dicho archivo se encuentra en `/usr/sbin/mailhome`, que permite que solo el super user (root) pueda ejecutar el archivo, además esta automatizado para ejecutarse cada hora.

El gestor de usuarios puede ser administrado de forma local por medio de herramientas de administración que este ofrece pero se las utiliza en modo consola. Puedes revisar los comandos requeridos tecleando:

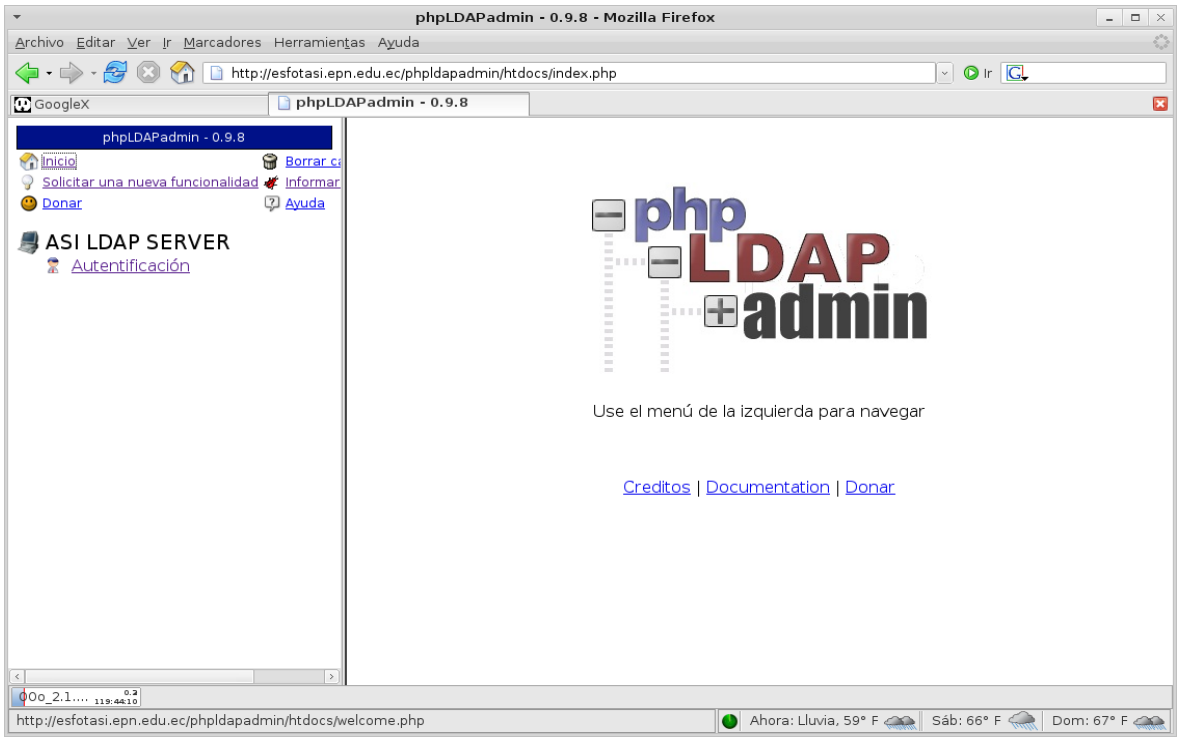
```
[root@mailasi ~]# man openldap
```

4.1.2 **ADMINISTRACIÓN DE PHPLDAPADMIN.**

Este aplicativo administra de forma local y remota por medio de la Web el servidor LDAP, por lo tanto para mostrar el uso se procederá con la creación de un usuario de correo y se creara un grupo de acceso en el directorio LDAP.

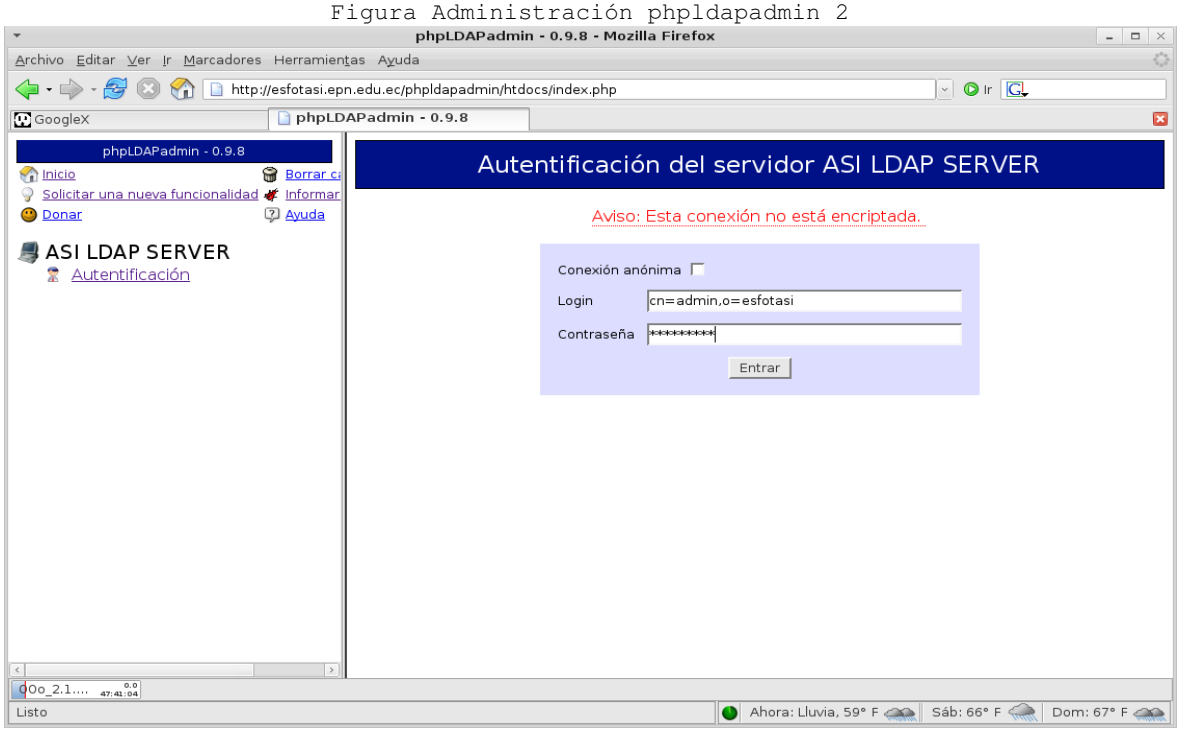
Para ingresar se debe ingresar al siguiente link: http://esfotasi.epn.edu.ec/phpldapadmin, esta dirección solicitara una clave de acceso que solo el administrador de poseer. Ejemplo:

Figura Administración phpldapadmin 1



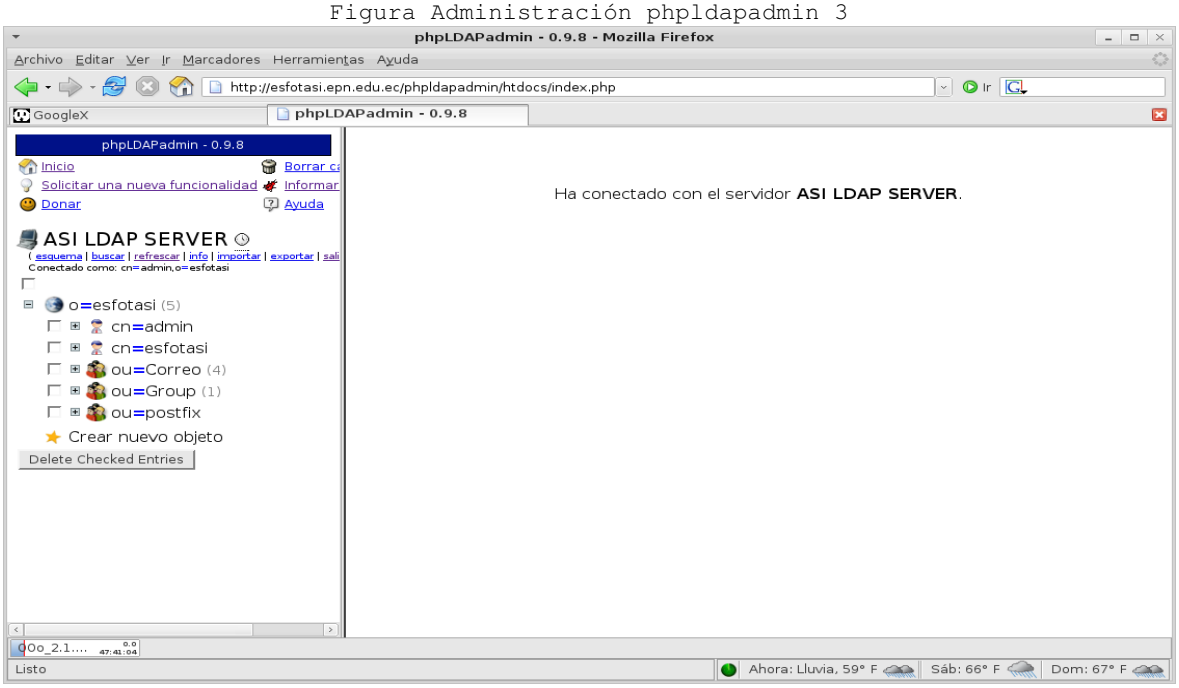
Al ingresar a esta pantalla presionar el link “Autenticación”, y el sistema solicitara el nombre del usuario que va administrar el sistema y la debida contraseña. Ejemplo:

Figura Administración phpldapadmin 2



Si los datos ingresados son los correctos mostrará esta pantalla con la estructura del directorio LDAP.

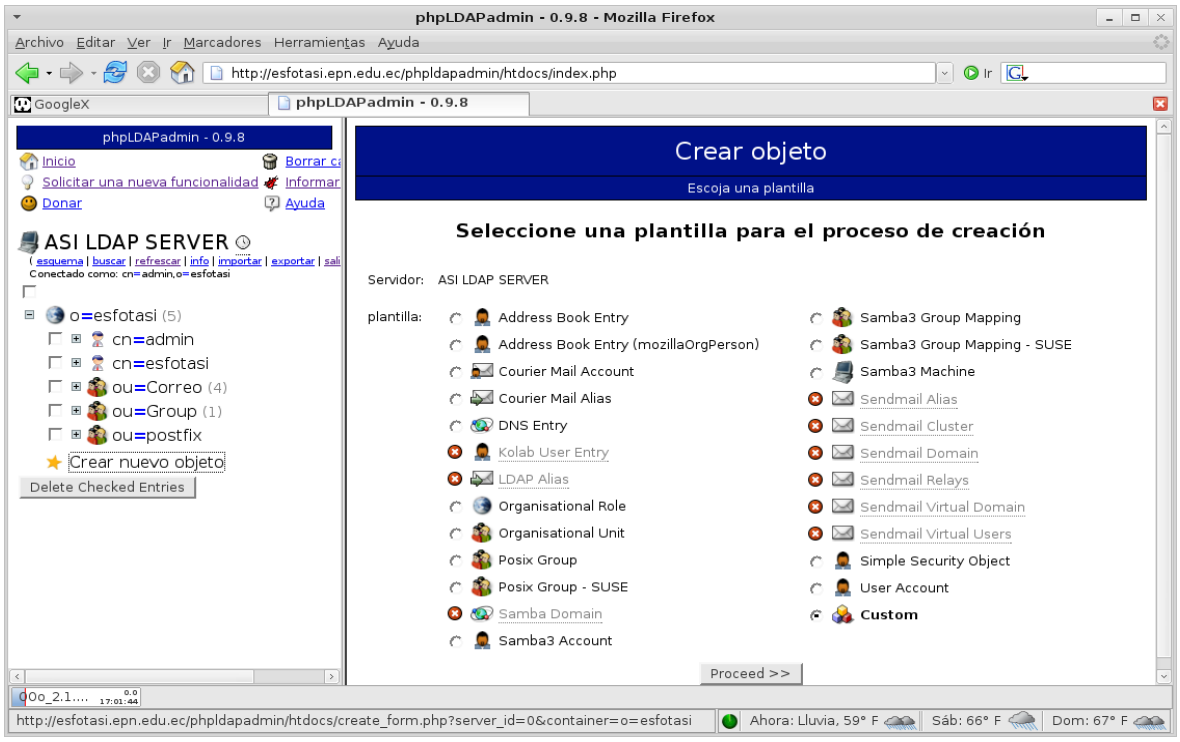
Figura Administración phpldapadmin 3



El procedimiento para crear un grupo usuarios que se va ha llamar “postfix” es el siguiente:

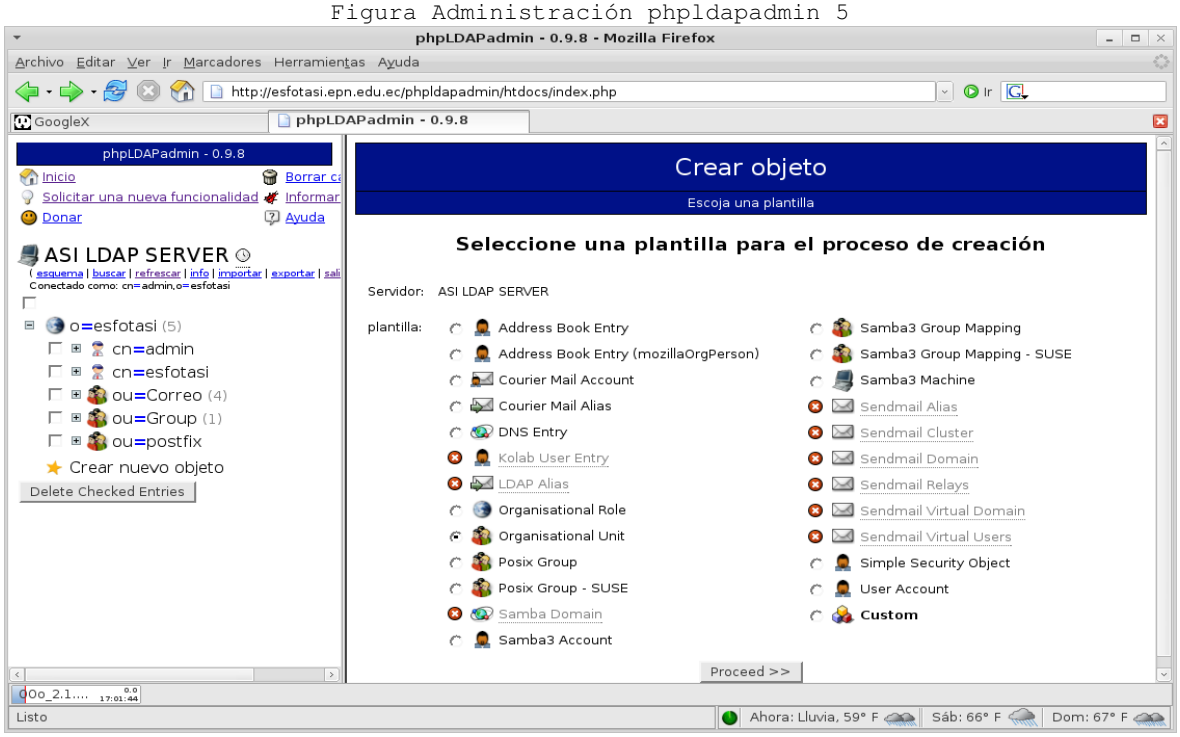
- Ubicarnos en la organización la raíz de la organización “o=esfotasi” y presionar el correspondiente link “Crear un objeto:

Figura Administración phpldapadmin 4



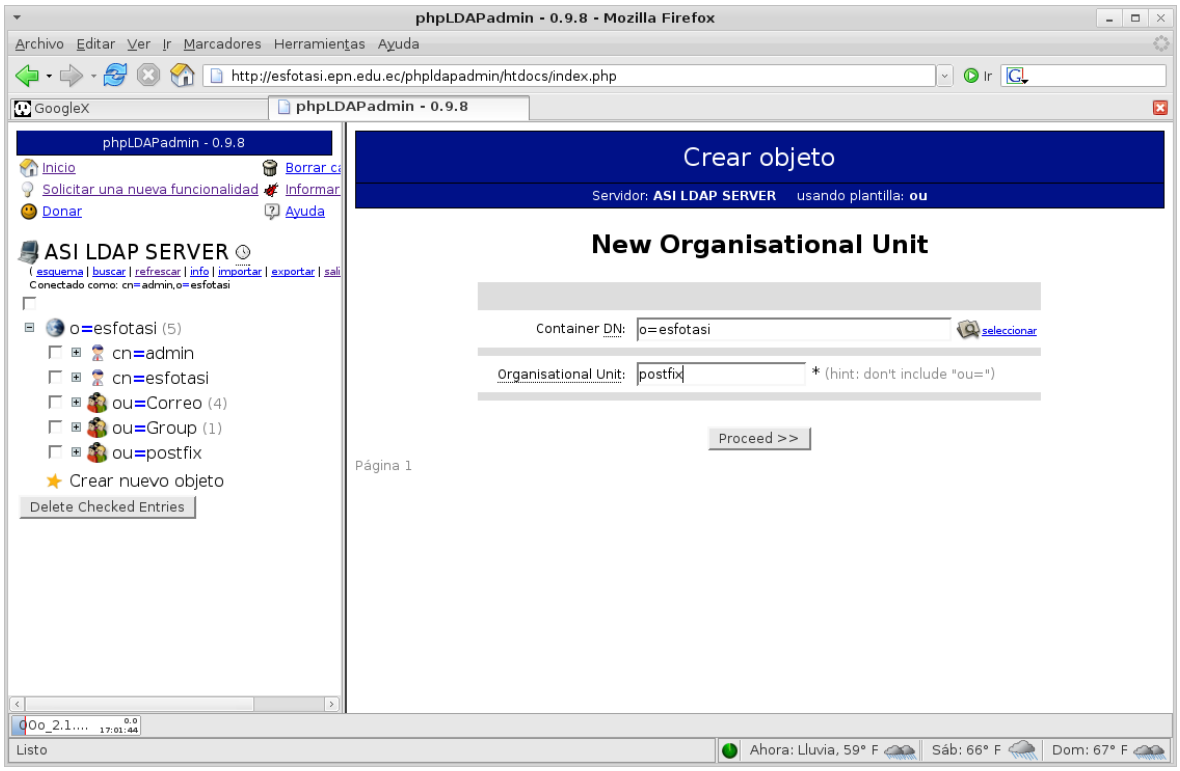
- Seleccionar “Organisational Unit” y presionar el botón Proceed >>

Figura Administración phpldapadmin 5



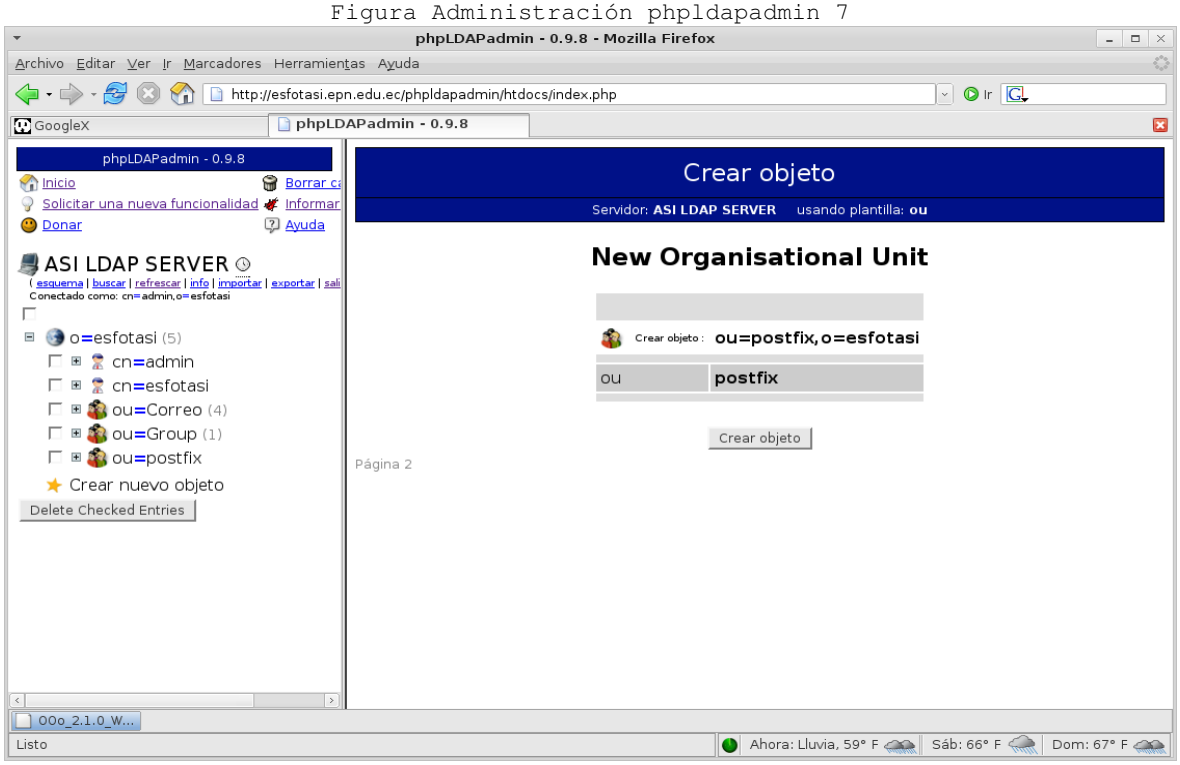
- En la pantalla siguiente digitar “postfix” y presionar el botón Proceed >>

Figura Administración phpldapadmin 6



- En esta pantalla presione el botón “Crear objeto”

Figura Administración phpldapadmin 7



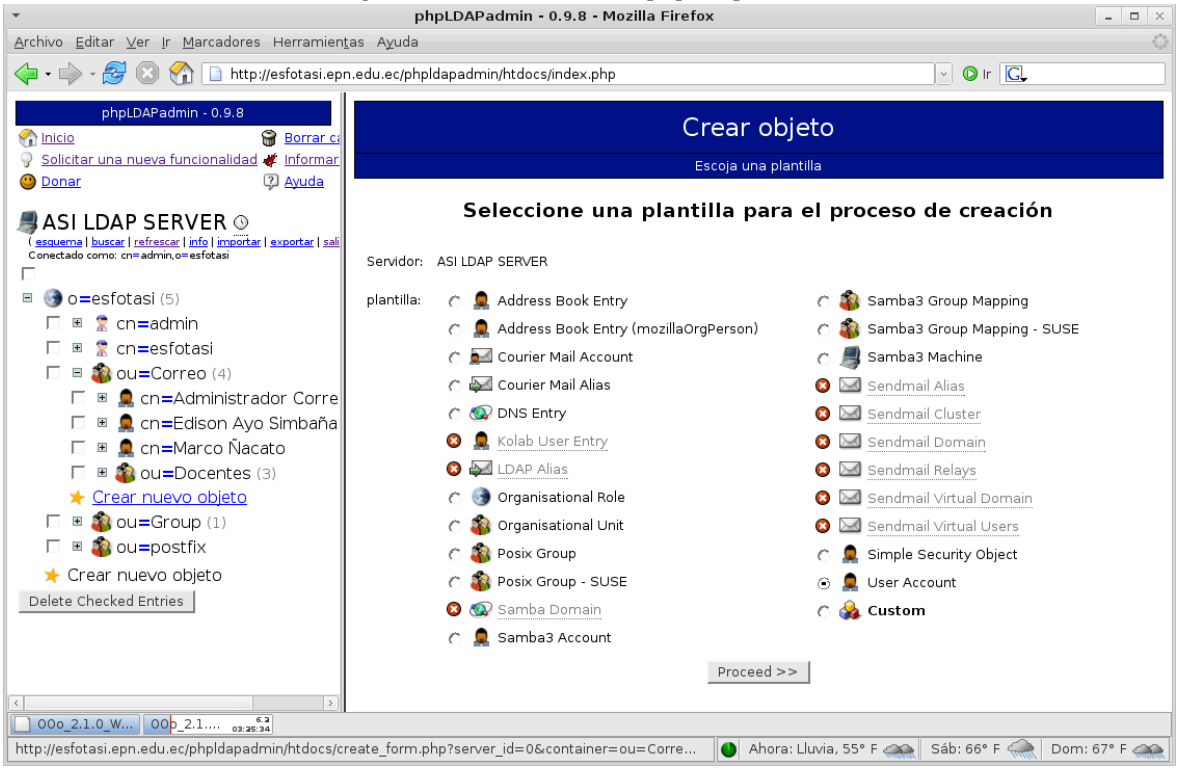
- Proceso terminado.

El procedimiento para crear un usuario de correo electrónico dentro de la organización

“o=esfotasi” es el siguiente:

- El usuario se va a crear dentro de la rama “ou=Correo, o=esfotasi”.
- Para acceder se debe seleccionar los links correspondientes en el árbol gráfico que el sistema phpldapadmin ofrece para mejorar la administración.
- Ubicarse en la rama correspondiente del grupo “ou=Correo”.
- Presionar “Crear un objeto hijo”.
- Presionar “User Account”.

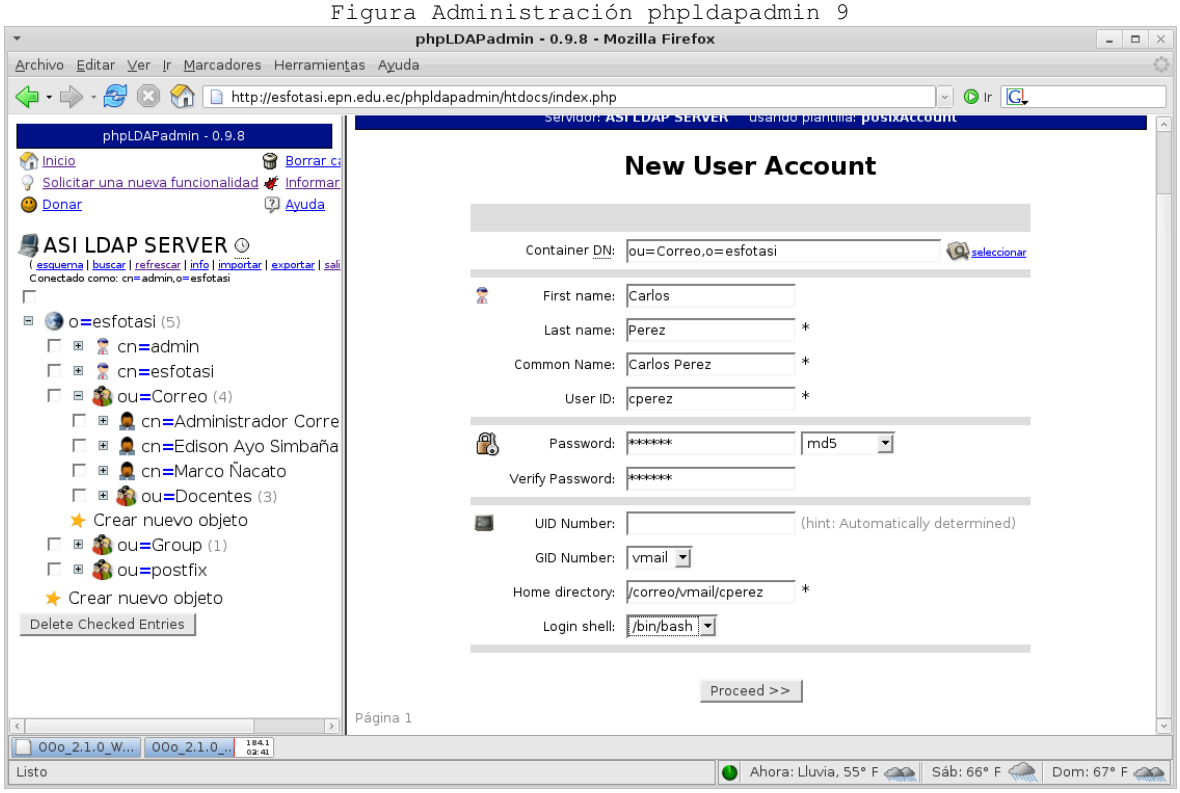
Figura Administración phpldapadmin 8



- En la siguiente pantalla digitar los datos correspondientes del usuario:
- First name: Carlos
- Last name: Perez
- Common name: Carlos Perez (Se genera automáticamente, pero puede ser modificado).

- User ID: cperez (Se genera automáticamente, pero puede ser modificado).
- Password: *****(Encriptado en md5).
- Verify Password: ***** (Si las claves son ingresadas son idénticas son aceptadas).
- UID Number: (Se genera automáticamente).
- GID Number: vmail (Se pueden seleccionar otros usuarios dependiendo del tipo de permisos que el administrador ofrece).
- Home directory: /correo/vmail/cperez (Escribir este path para el home de los correos “Obligatorio”).
- Login shell: /bin/bash (Eliminar esta opción terminada la creación del usuario por motivos de seguridad).
- Presionar el botón Proceed >>

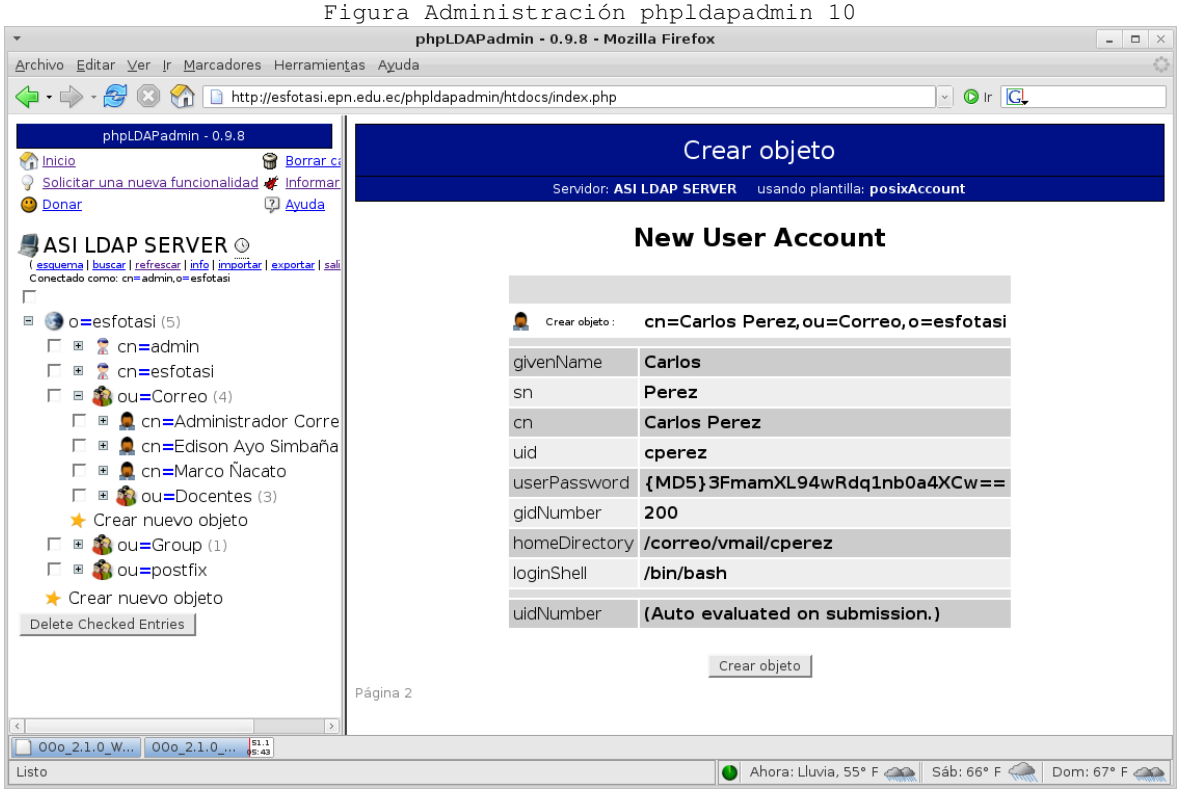
Figura Administración phpldapadmin 9



- Luego de presionar el botón proceed mostrara un resumen de que atributos con

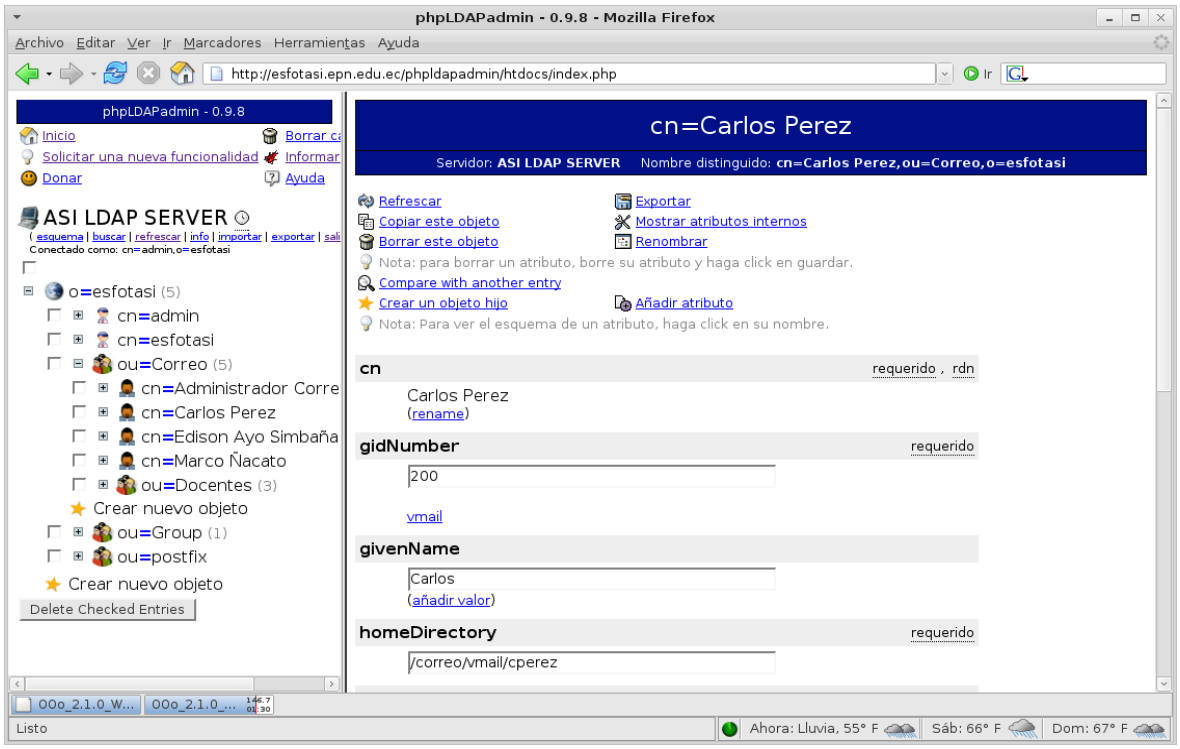
los que se va a crear el usuario en el sistema:

Figura Administración phpldapadmin 10



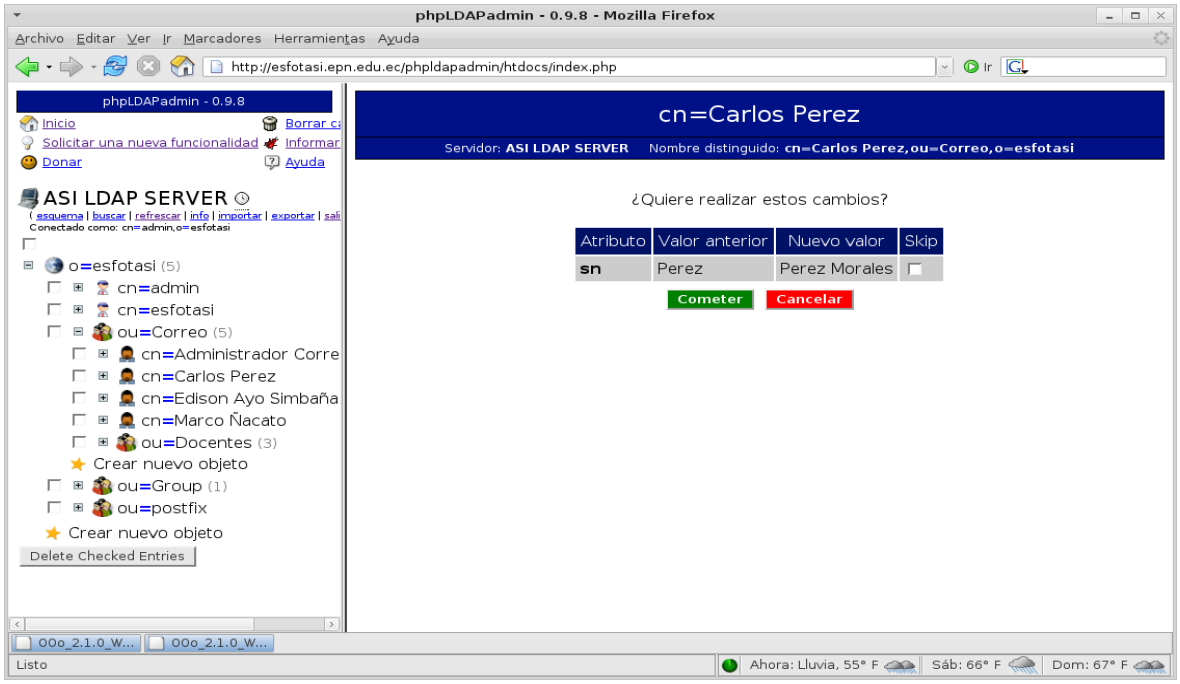
- Al presionar el botón “Crear objeto” mostrara el usuario creado y los atributos de este.

Figura Administración phpldapadmin 11



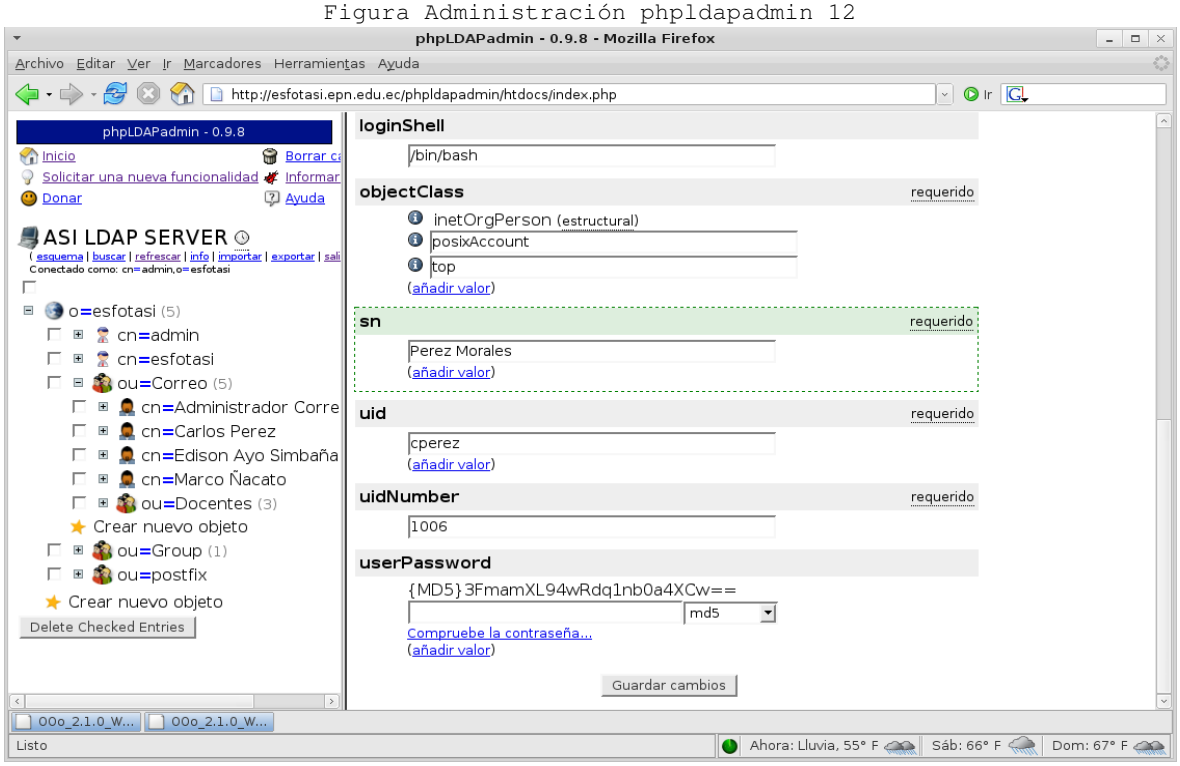
- Estos atributos pueden ser cambiados o modificados acorde solicitudes de los usuarios o requerimientos de los administradores.
- Para realizar las pruebas se va a cambiar el atributo apellido “sn”, en este caso se va adicionar el otro apellido del usuario. Ejemplo: digitar Morales y presionar el botón Guardar cambios.

Figura Administración phpldapadmin 12



- El sistema muestra una pantalla para confirmar cambios, presionar el botón Cometer.

Figura Administración phpldapadmin 12



- Se pueden adicionar mas usuarios de correo con el mismo proceso.
- El sistema además permite añadir otros valores, usuarios, actualizar, renombrar.

El sistema genera automáticamente el “HOME” y da de alta (Autoriza el uso del sistema de correo) de los usuarios, este proceso se realiza automáticamente cada hora en el servidor pero si por algún caso el administrador quiera dar de alta una cuenta debe digitar el comando:

```
[root@mailasi ~]# mailhome
```