



**FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS
CARRERA TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES**



TEMA:

IMPLEMENTACIÓN DE UN SERVIDOR DE CORREO ELECTRÓNICO SEGURO, CON FILTRO ANTISPAM Y ANTIVIRUS, BASADO EN OPEN SOURCE, ORIENTADO A FINES ACADÉMICOS PARA LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.

Trabajo de Graduación presentado por:

García Molina, Fredy Antonio

Leonor Orellana, Alejandro Omar

Ramos Pineda, María Elena

Para optar el grado de:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Marzo del 2008

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

PAGINA DE AUTORIDADES

LIC. JOSÉ MAURICIO LOUCÉL
RECTOR

ING. NELSON ZÁRATE SÁNCHEZ
VICERRECTOR ACADEMICO

ING. LORENA DUQUE DE RODRÍGUEZ
DECANO

JURADO EXAMINADOR

ING. DAVID JONATHAN RIVAS
PRESIDENTE

ING. SIGIFREDO PORTILLO
PRIMER VOCAL

ING. PEDRO PEÑATE
SEGUNDO VOCAL

Marzo del 2008

San Salvador, El Salvador, Centroamérica

DEDICATORIA

Hoy en esta fecha tan especial, quiero agradecerle a Dios en primer lugar, por ser el quien me dio la vida, la sabiduría y la fuerza para poder lograr hacer realidad mi sueño de coronar mi carrera académica, por haberme dado la paciencia y el conocimiento para lograr dar un paso adelante en el ámbito académico lo cual conllevara a promociones laborales. Y a todos los docentes de La Universidad Tecnológica de El Salvador quienes hicieron posible que todos los conocimientos que ellos poseen, lograran entrar en mi cabeza y poder lograr desarrollar en base a su experiencia nuestro Proyecto de Tesis.

Agradecer a mis padres quienes con sacrificio me ayudaron incansablemente tanto económicamente como moralmente, apoyándome y dándome fuerzas para que continuara con mi carrera en los momentos que veía que todo se venia abajo, agradecerles por sus consejos y la motivación recibida por parte de ellos.

A mi esposa Beatriz, la mujer que tantas noches deje durmiendo sola por estar haciendo la instalación del prototipo que tanto nos costo, por ese apoyo incondicional y motivación que me dio diciéndome en los momentos que me veía afligido que no dejara a medias la carrera y que siguiera haciendo el esfuerzo, diciéndome “Vos sos inteligente y tenes el potencial para lograrlo! no lo dejes así.”

Y finalmente a todos los alumnos que puedan llegar a tener el interés de leer este documento, decirles que no desmayen ni se estanquen en sus carreras, déjenme decirles que no saben que satisfacción mas grande es saber que todo el tiempo invertido se concreta en llegar a obtener ese titulo preciado, el cual nos ayudara enormemente en nuevas o futuras propuestas laborales y ante la felicidad de haber cumplido la meta fijada.

Fredy Antonio Garcia Molina.

DEDICATORIA

Este día tan especial quiero agradecerle al todopoderoso por haber permitido ver hecho realidad mi sueño de graduarme en la universidad, agradecerle por darme la sabiduría y la paciencia en el transcurso de mi carrera profesional para que todos esos conocimientos adquiridos sean aplicados en mi record laboral.

También quiero agradecer a mi madre Juana Antonia Orellana por financiar y apoyar mis decisiones que ahora han dado como fruto mi título quien además de su esfuerzo y empeño se ha estado conmigo en cada clase, en cada actividad, en cada parcial.

También quiero dar un agradecimiento especial al Lic. Walter Navarrete quien mostro una conducta altruista muy notable en nuestro grupo pues gracias a su apoyo y a su alto grado de ética profesional logramos un prototipo exitoso de provecho para los estudiantes de la universidad.

Por otra parte agradecer a los estudiantes que se toman el tiempo de leer esta dedicatoria que sin duda alguna expresa lo que en realidad siento en este momento en el cual culmino mis estudios del Técnico en Ingeniería de Redes Computacionales, muchas gracias.

Alejandro Omar Leonor Orellana

DEDICATORIA

Hoy en este día quiero especialmente primero agradecerle a Dios todopoderoso por haberme permitido culminar mis estudios, habiéndome proporcionado el entendimiento y la sabiduría para comprender y aplicar lo que se me enseñó y darle gracias por terminar el proceso de nuestra tesis con éxitos, llevándonos el primer lugar a nivel de prototipo y ser premiados por dicho evento; también agradecerle especialmente al Lic. Walter Navarrete por la ayuda y la asesoría incondicional a nuestro grupo y a Javier Arenas por su asesoría.

También quiero agradecer y dedicar este Título a mi hija Pamela Idalia Torres Ramos por comprender todo el tiempo que no pude estar con ella para apoyarla en todos los ámbitos y que solamente estuve en pocos momentos, pero quiero decirle que la Amo y gracias por su valioso apoyo y por que siempre me decía “Mami tu puedes hacerlo y saldrás bien”.

Por otra parte a los compañeros de la Universidad que lean esta dedicatoria decirles que sigan adelante que no se den por vencidos, que Dios todopoderoso les dará la sabiduría para cumplir sus objetivos y metas, pero que le echen ganas y saldrán victoriosos.

María Elena Ramos Pineda

ÍNDICE

CAPÍTULO I

GENERALIDADES DEL PROYECTO

INTRODUCCIÓN.....	1
1.1 Situación Problemática.....	2
1.2 Enunciado del Problema.....	3
1.3 Justificación del Proyecto.....	3
1.4 Objetivos.....	4
1.5 Alcances.....	5
1.6 Delimitaciones.....	5
1.7 Estudio de Factibilidad.....	6

CAPÍTULO II

MARCO TEÓRICO DE REFERENCIA

2.1 MTA.....	10
2.2 TLS (Transportation Layer Security)	11
2.3 Cyrus IMAP.....	12
2.4 Cyrus SASL.....	13
2.5 SMTP.....	14
2.6 SIEVE.....	15
2.7 AMAVISD-NEW.....	16
2.8 SPAMASSASIN.....	17

2.9 CLAM ANTIVIRUS.....	17
2.10 SQUIRRELMAIL.....	18
2.11 QMAIL.....	18
2.12 FECHMAIL.....	19
2.13 EXIM.....	19
2.14 SENDMAIL.....	20
2.15 OPENWEBMAIL.....	20
CAPÍTULO III	
PROYECTO TEMÁTICO	
3.1 Planteamiento del Proyecto Temático.....	21
3.2 Cronograma del Proyecto.....	23
3.3 Documentación Técnica.....	25
3.4 Evaluación Técnica y Económica.....	28
3.5 Tecnología y Recursos seleccionados.....	29
3.6 Presupuesto Proyectado	30
3.7 Oferta Técnica y Oferta Económica.....	31
CAPITULO IV	
DISEÑO Y ELABORACIÓN DEL PROTOTIPO	
4.1 Artículo del Prototipo (Texto).....	34
4.2 Presentación del Prototipo.....	37
4.3 Evidencias del Avance del Proyecto.....	56
Conclusiones.....	65
Recomendaciones.....	66
Bibliografía.....	67
Anexos.....	

CAPITULO I

GENERALIDADES DEL PROYECTO

INTRODUCCIÓN

Hoy en día es muy común que cada alumno de la Universidad Tecnológica de El Salvador tenga una cuenta de correo electrónica, crear una cuenta es sumamente sencillo, el correo electrónico ha venido a solventar muchos problemas de comunicación que hasta hace unos años atrás eran muy difíciles de resolver, pero esto aparte de un beneficio conlleva a una serie de problemas que muchas veces no se esperan, refiriéndose a los famosos y problemáticos “Virus” y “Spam” que causan un daño tremendo a la red, saturándola y volviéndola lenta, bien parecen ser lo mismo por el hecho que se les facilita la entrada por medio del correo electrónico pero actúan de forma diferente. En este documento se demostrara como prototipo como implementar y configurar un servidor de correo electrónico seguro y confiable, que aparte de ser uno de los laboratorios que ya se imparten en dos de las materias del Técnico en Ingeniería de Redes de La Universidad Tecnológica de El Salvador se debe de incluir en estas prácticas en otros Sistemas Operativos o Distribuciones como lo son los Open Source. Estas prácticas harán que los alumnos de carreras afines del área de informática podrán recibir y desarrollar “Nuevas Tecnologías” implementando además soluciones como Antivirus y Antispam, todo esto guiado a los estudiantes de la carrera de Técnico en Redes, quienes en las cátedras como Sistemas Operativos de Redes y Administración de Redes podrán incluirles esta práctica con manuales o guías paso a paso para que el estudiante pueda ver la implementación creada en prototipo del servidor de correo electrónico.

1.1 SITUACIÓN PROBLEMÁTICA

El problema consiste que los alumnos de la carrera de Técnico en Ingeniería de Redes Computacionales han encontrado que durante los ciclos de estudio no hay dentro de las asignaturas que se cursan información, contenido o manuales que contemple el aplicar dentro de la carrera el poder configurar un prototipo de servidor de correo electrónico basado en OpenSource de GNU/Linux, y que a la vez la Universidad Tecnológica de El Salvador (UTEC) no cuenta con la infraestructura ni manuales de dicho prototipo que permita realizar pruebas de implementación y configuración de cómo funciona el servidor de correo electrónico.

También los alumnos se encuentran con la dificultad en el ámbito laboral que el porcentaje de Servidores GNU/Linux en las empresas es grande y no tienen los conocimientos adecuados sobre dichos servidores, de esta manera hay ausencia de información en los temarios de las asignaturas de Sistemas Operativos de Redes y Administración de Redes sobre la implementación y configuración de servidores de GNU/Linux en Open Source.

1.2 ENUNCIADO DEL PROBLEMA

¿Cómo podrán los alumnos del Técnico en Ingeniería de Redes Computacionales implementar un prototipo de servidor de correo electrónico seguro con filtro antispam y antivirus basado en una distribución Open Source de GNU/Linux?

1.3 JUSTIFICACIÓN DEL PROYECTO

- Se creará un prototipo de un servidor de correo electrónico para que en este, los alumnos puedan realizar pruebas de cómo funciona dicho servidor.
- Con la creación de manuales y guías de implementación y configuración del servidor de correo electrónico se pretende que los alumnos puedan tener prácticas para tener un sólido conocimiento en configurar un servidor de correo electrónico seguro que posea filtros AntiSpam y AntiVirus, y así resolver problemas que a este se le presenten a futuro en esta rama.
- Será de gran importancia contar con las prácticas de implementación y configuración de un servidor correo electrónico basado en open source, para así posteriormente los alumnos de la carrera del Técnico en Ingeniería de Redes Computacionales puedan realizar las pruebas en el prototipo y de esta manera poder manipularlo.

1.4 OBJETIVOS

OBJETIVO GENERAL

Facilitarles a los estudiantes de la carrera de Técnico en Redes de la UTEC, una herramienta para que logren el aprendizaje sobre la implementación y la configuración de un servidor de correo electrónico seguro basado en Open Source.

OBJETIVOS ESPECIFICOS

- Realizar la implementación del prototipo del servidor de correo electrónico seguro, con filtro Antispam y Antivirus basado en Open Source a través del paso a paso de las guías.
- Crear los manuales o guías de implementación y configuración del servidor de correo electrónico orientado a las asignaturas de Sistemas Operativos de Redes y Administración de Redes de la carrera de Técnico en Ingeniería de Redes Computacionales.
- Probar y verificar si las guías de implementación y configuración del servidor de correo electrónico, cumple con el filtrado Antispam y Antivirus razones por las cuales ha sido creado.

1.5 ALCANCES

- Llegar a implementar el prototipo del servidor de Correo Electrónico Seguro, con filtro Antispam y Antivirus basado en Open Source, orientados a fines académicos para la Universidad Tecnológica de El Salvador.
- Al realizar las guías y manuales orientadas a la implementación del prototipo del correo electrónico el alumno podrá familiarizarse a manera que podrá probar, manipular y trabajar en un servidor de correo electrónico en OpenSource.

1.6 Delimitaciones

GEOGRÁFICA

Este proyecto se implementará en las instalaciones del Laboratorio de Redes de la Universidad Tecnológica de El Salvador, ubicada el edificio Francisco Morazán en Calle Arce # 1026 S.S

TEMPORAL

El desarrollo de este proyecto tendrá una duración de 5 meses a partir del 8 de Agosto de 2007 al 7 de Diciembre de 2007.

ORGANIZACIONAL

Este proyecto esta destinado a brindar una alternativa de implementación y configuración de un servidor de correo electrónico con fines académicos para la Facultad de Informática de la Universidad Tecnológica de el Salvador.

ESPECÍFICO

Este proyecto esta específicamente diseñado para los alumnos de la carrera del Técnico en Ingeniería de Redes de la UTEC, quienes dentro de su plan de estudio podrán obtener un nuevo método de configuración de correo electrónico en las asignaturas de Sistemas Operativos de Redes y Administración de Redes ya que en estas es en la que mejor se acoplarían estas guías de configuración por el hecho que es en estas que se ve mucho la configuración de servidores.

1.7 ESTUDIO DE FACTIBILIDAD

FACTIBILIDAD TÉCNICA

Dentro de los recursos Técnicos necesarios para lograr la implementación de un sistema de correo electrónico, se requieren los siguientes elementos:

- Que la Universidad Tecnologica de El Salvador capacite a los docentes y a los encargados de los laboratorios en las distribuciones de GNU/Linux.
- A los alumnos que recibirán estas prácticas, los docentes deberán brindarles conocimientos básicos y generales sobre GNU/Linux antes de desarrollar las guías.
- Como grupo crearemos un manual y guías dirigidas a los docentes, para su desarrollo en las cual detallaremos la implementación del servidor de correo electrónico.
- Dentro del manual de la implementación del correo electrónico que le brindaremos a los docentes se incluirá un listado de los comandos a utilizar.
- Para desarrollar las prácticas, los laboratorios deberán poseer equipos que contengan la distribución de GNU/Linux a utilizar, así como además equipos activos y pasivos de conexión de red.

Software:

- La distribución de GNU/Linux que mejor se aplique entre ellas tenemos Suse, Ubuntu y Debian, y los complementos o paquetes para hacerlo seguro y funcional como podrían ser:
- Cyrus SASL ,Cyrus IMAP **(Protocolos de acceso de mensajes por internet y soporte de autenticación de seguridad)**
- Postfix , Sendmail, Qmail, Exim **(Agentes de transporte de correo MTA)**
- SpamAssassin, Cyrus-IMAP, Procmal, MailFilter **(Filtros de identificación de Spam)**
- Clam-AV , OpenAntivirus, RAV Antivirus **(Filtros e identificadores de Virus)**
- Amavisd-new, **(Interfaz entre el MTA y uno o mas filtros Antispam y Antivirus)**
- Squirrelmail, FetchMail, OpenWebMail **(Paquetes de correo electrónico con funcionalidades como libreta de direcciones, agenda, calendario.)**

Hardware:

- Para poder montar el prototipo de servidor de correo electrónico se necesitaran las siguientes características:
 - o Procesador de: 250Mhz (como mínimo)
 - o Memoria: 256 MB (como mínimo)
 - o Capacidad en disco duro: 8.0 GB (como mínimo)
 - o Tarjeta de Red (Conexión a internet)

ECONÓMICA

En lo referente a la parte económica de este proyecto, al trabajar en una distribución de OpenSource no será necesario incurrir en gastos demasiado altos, a diferencia que si lo trabajáramos en un Sistema Operativo como lo es Windows Server 2003 en el cual solo el costo de la licencia sobrepasa los \$2000.00. Así de esta manera en las distribuciones de GNU/Linux solamente se gastara en la capacitación del recurso humano docente, equipos de hardware activos/pasivos y el soporte técnico.

OPERATIVA

Orientar a los docentes a la inducción de la implementación de un servidor de correo electrónico basado en OpenSource, el cual ayudará en gran manera a los alumnos de redes, ya que al incluir 8 horas de práctica en la materia el cual puede ser Sistemas Operativos de Redes ó Administración de Redes dentro del ciclo cursado les ayudará a incrementar sus conocimientos Técnicos y podrán desenvolverse en futuras propuestas, basadas en servidores de correo electrónico en Open Source.

La práctica deberá cubrir los siguientes puntos:

- Introducción a las tecnologías open source.
- Manual de códigos a utilizar para poder configurar el servidor de correo electrónico.
- Se le brindará al docente una copia de la distribución de GNU/Linux a utilizar para que los alumnos puedan obtenerlo.
- El número de prácticas a cumplir dependerá de las que la asignatura permita dentro del ciclo.
- Los laboratorios ya cuentan con los requerimientos mínimos para estas prácticas los cuales son: Procesador de mas de 250Mhz, memoria de 256MB, capacidad de disco duro de 8GB y una tarjeta de red para conexión a Internet.
- Configuración del prototipo del servidor de correo electrónico.

CAPITULO II

MARCO TEORICO DE REFERENCIA

DISTRIBUCIÓN DEBIAN 4.0 (ETCH) STABLE GNU/LINUX.

[Debian](#) es un sistema operativo (SO) [libre](#) para ordenadores. El sistema operativo es el conjunto de programas básicos y utilidades que hacen que funcione el ordenador. Debian utiliza el núcleo GNU/Linux (el corazón del sistema operativo), pero la mayor parte de las herramientas básicas vienen del [Proyecto GNU](#); de ahí el nombre GNU/Linux.

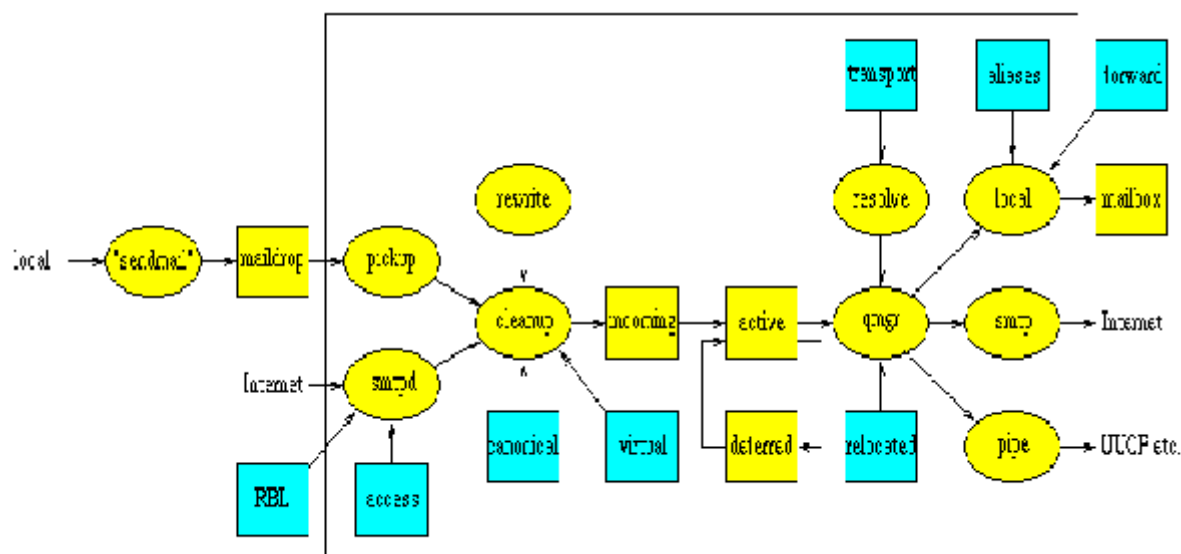
Debian GNU/Linux ofrece más que un SO puro; viene con miles de [paquetes](#), programas precompilados distribuidos en un formato que hace más fácil la instalación en su ordenador. En este proyecto se utilizará la rama Sarge de Debian.

2.1 MTA (Mail Transport Agent).

El MTA, es un agente de transporte de correo de software libre/código abierto, un programa informático para el enrutamiento y envío de correo electrónico; dentro de ellos se encuentra [Postfix](#) que pretende ser rápido, fácil de administrar y seguro, a la vez que suficientemente compatible con [Sendmail](#) como para que los usuarios existentes no se asusten.

Por lo tanto, externamente mantiene el estilo de Sendmail, mientras que internamente es completamente diferente.

A diferencia de Sendmail, Postfix no es un programa monolítico, sino una combinación de pequeños programas, cada uno de los cuales lleva a cabo una función especializada. En este documento, el lector encontrará la información necesaria para tener el sistema funcionando junto a otros componentes que completan la instalación de un sistema de correo electrónico. (Ver figura #1)



Puede encontrarse más información sobre Postfix en la [documentación online](#) de su website.

FIGURA #1

2.2 TLS (Transportation Layer Security).

Por defecto, toda comunicación en Internet se hace sin ningún tipo de cifrado y sin una autenticación fiable. Esto significa que cualquiera con acceso físico a la línea de datos por la que viaja un paquete puede espiar dicha comunicación. Aún peor, es posible redirigir o alterar esa comunicación para que la información que se desea mandar se pierda y nadie se dé cuenta.

De cara a solventar estos problemas de seguridad, [Netscape Inc.](#) introdujo el protocolo [SSL](#) (Secure Sockets Layer), que ha ido evolucionando en el protocolo estandarizado [TLS](#) (Transportation Layer Security). Ofrece tanto cifrado de la comunicación (frenando las escuchas) como autenticación fuerte (asegurando que ambas partes de una comunicación son correctamente identificadas y que la comunicación no puede ser alterada).

Postfix/TLS no implementa el protocolo TLS por sí mismo, sino que usa el paquete [OpenSSL](#) para esta tarea. En el website de OpenSSL pueden encontrarse enlaces a documentación que profundiza en el protocolo y sus características.

2.3 CYRUS IMAP.

Cyrus IMAP (Internet Message Access Protocol) es desarrollado y mantenido por el [Andrew Systems Group](#) de la [Carnegie Mellon University](#).

A diferencia de otros servidores IMAP, Cyrus usa su propio método para almacenar el correo de los usuarios. Cada mensaje es almacenado en su propio fichero. El beneficio de usar ficheros separados es una mayor fiabilidad ya que sólo un mensaje se pierde en caso de error del sistema de ficheros.

Los metadatos, tales como el estado de un mensaje (leído, etc.) se almacenan en una base de datos.

Además, los mensajes son indexados para mejorar el rendimiento de Cyrus, especialmente con muchos usuarios e ingentes cantidades de mensajes. No hay nada tan rápido como el servidor IMAP Cyrus.

Otra característica muy importante es que no son necesarias cuentas locales de GNU/Linux para cada usuario.

Todos los usuarios son autenticados por el servidor IMAP. Esto lo convierte en una magnífica solución cuando se tiene una gran cantidad de usuarios.

La administración es llevada a cabo mediante comandos especiales de IMAP. Esto le permite usar tanto la interfaz de línea de comandos como los interfaces web. Este método es mucho más seguro que un interfaz web para `/etc/passwd`.

Desde la versión 2.1 de Cyrus, se usa la versión 2 de la librería SASL para la autenticación. En la configuración descrita en este artículo se implementa una autenticación de tres capas. Cyrus se autentica con `saslauthd`, quien redirige la petición al mecanismo que le hayamos definido, por ejemplo `sasldb`, que buscará la información del usuario en una base de datos [Berkeley DB](#).

2.4 CYRUS SASL.

SASL son las siglas de *Simple Authentication and Security Layer*, un método para añadir soporte para la autenticación a protocolos basados en la conexión que ha sido estandarizado por la [IETF](#) (Internet Engineering Task Force). Se usa en servidores (en este caso Cyrus IMAP) para manejar las peticiones de autenticación de los clientes.

Para ello, el protocolo incluye un comando para identificar y autenticar un usuario contra un servidor y para, opcionalmente, negociar la protección de las subsiguientes interacciones del protocolo. Si se

negocia su uso, una capa de seguridad es añadida entre el protocolo y la conexión.

La [librería SASL de Cyrus](#) también usa la librería OpenSSL para cifrar los datos. Se puede encontrar más información en la página web de [Cyrus SASL](#).

2.5 SMTP.

SMTP (Simple Mail Transfer Protocol) y sus extensiones ESMTP (SMTP Service Extensions) proporcionan un mecanismo para transferir correo fiable y eficientemente. El diseño del protocolo SMTP requiere que el servidor maneje colas de envío de correo.

En ciertas circunstancias, fuera del área que engloba el intercambio entre hosts independientes en Redes públicas, es deseable implementar un sistema donde el receptor del correo no maneje colas, como es el caso de un MDA (Mail Delivery Agent). Esto es precisamente lo que hace el protocolo [LMTP](#) (Local Mail Transfer Protocol).

Aunque LMTP es una alternativa al protocolo ESMTP, usa (con algunos pequeños cambios) la sintaxis y la semántica de ESMTP. Este diseño permite al LMTP utilizar las extensiones definidas para el ESMTP. LMTP no debería ser nunca usado en el puerto 25.

2.6 SIEVE.

[Sieve](#) es un lenguaje que puede usarse para crear filtros de correo electrónico en el momento de la entrega final del correo (en el lado del servidor). No está ligado a ningún sistema operativo o servidor de correo en particular. Requiere el uso de la especificación de mensajes del RFC 822. El lenguaje es suficientemente potente para ser útil, pero está limitado de modo que permita la creación de sistemas de filtrados seguros en el lado del servidor.

El objetivo es no permitir a los usuarios hacer nada más complejo (y peligroso) que escribir sencillos filtros de correo, además de facilitar editores basados en interfaces gráficas de usuario. El lenguaje no permite definir bucles o funciones, ni tampoco proporciona variables.

Se supone que el uso del lenguaje tiene lugar al final de la entrega, cuando el mensaje se mueve a una cuenta accesible por el usuario. En aquellos sistemas donde el MTA (Mail Transport Agent) realiza la entrega final (como es tradicional en los sistemas UNIX), es razonable clasificar cuando el MTA deposita el correo en la cuenta del usuario. Sin embargo, los filtros Sieve pueden ser usados por varios "puntos finales de entrega" del sistema de correo: por el servidor SMTP, por un servidor IMAP o

POP que archive una o más cuentas de usuario, o por un cliente de correo (MUA, Mail User Agent) que actúe como gestor de las entregas (por ejemplo, un cliente POP o IMAP sin conexión).

2.7 AMAVISD-NEW.

Amavisd-new es un interfaz de alto rendimiento y fiabilidad entre el MTA y uno o más filtros de contenidos: antivirus o el módulo Mail SpamAssassin de Perl.

Está escrito en Perl, asegurando alta fiabilidad, portabilidad y facilidad de mantenimiento. Se comunica con el MTA vía (E) SMTP o LMTP, o mediante el uso de otros programas. No existen problemas de sincronización en su diseño que pudieran causar pérdidas de correos.

Normalmente se posiciona dentro o cerca del gestor de correo principal, no necesariamente donde se ubiquen las cuentas de correo de los usuarios (donde tiene lugar el envío final).

Si se está buscando una solución que soporte configuración por usuario y de mensajes pequeñas que se ubique al final del proceso de envío (p.e. llamado desde procmail o en sustitución de un agente local de envío), posiblemente puedan encontrarse otras soluciones más apropiadas.

Cuando está habilitado el uso de Mail SpamAssassin (SA), se llama a SA una sola vez por mensaje (independientemente del número de destinatarios). Amavisd-new se beneficia del uso del módulo de Perl Net Server, el cuál ofrece un rápido entorno multi-hilo. Amavisd-new ofrece un servidor SMTP que cumple con el RFC 2821, un servidor LMTP que cumple con el RFC 2033, un cliente SMTP y genera notificaciones de estado de envío (o no) que cumplen los RFC 1892 y 1894. Esto lo hace adecuado para múltiples analizadores de virus y de correo publicitario en plataformas de correo donde la fiabilidad y el cumplimiento de los estándares son importantes.

2.8 SPAMASSASSIN.

SpamAssassin es un filtro de correo que trata de identificar el *spam* mediante el análisis del texto y el uso en tiempo real de algunas listas negras a través de Internet.

A partir de su base de datos de reglas, utiliza un amplio abanico de pruebas heurísticas en las cabeceras y el cuerpo de los correos para identificar el *spam*, también conocido como correo electrónico comercial no solicitado.

Una vez identificado, el correo puede ser opcionalmente marcado como *spam* o más tarde filtrado usando el cliente de correo del usuario.

SpamAssassin normalmente identifica acertadamente entre un 95 y un 99% del *spam*, dependiendo

del tipo de correo que se reciba. También incluye soporte para informar de mensajes de *spam*, automática o manualmente, a bases de datos como [Vipul's Razor](#).

2.9 CLAM ANTIVIRUS.

[ClamAV](#) es una herramienta antivirus GPL para UNIX. El propósito principal de este software es la integración con los servidores de correo (escaneo de datos adjuntos). El paquete proporciona un servicio multi-hilo flexible y escalable, un analizador de línea de comandos y una utilidad para la actualización automática vía Internet. Los programas están basados en una librería distribuida con el paquete Clam Antivirus, la cual puede ser usada por su propio software. Y lo más importante, la base de datos se mantiene actualizada constantemente.

Otras características destacables son el soporte de firmas digitales en la actualización de la base de datos, el análisis durante el acceso bajo [Linux](#) y [FreeBSD](#), la detección de más de 20000 virus, gusanos y troyanos, el soporte integrado para archivos comprimidos con [Rar](#), Zip, [Gzip](#) y [Bzip2](#) y formatos de correo [Mbox](#), [Maildir](#) y ficheros crudos de correo.

2.10 SQUIRRELMAIL.

[SquirrelMail](#) es un paquete de correo por web basado en estándares y escrito en [PHP](#) 4. Incorpora soporte PHP para los protocolos IMAP y SMTP, y todas sus páginas se crean en puro [HTML 4.0](#) (sin requerir el uso de JavaScript), de modo que se garantice la máxima compatibilidad entre navegadores. Tiene muy pocos requerimientos y es muy fácil de instalar y configurar.

SquirrelMail tiene toda la funcionalidad que se espera de un cliente de correo electrónico, incluyendo soporte de MIME, agendas de contactos y gestión de carpetas.

[Avelsieve](#) (SIEVE Mail Filters Plugin for SquirrelMail) es un [plugin para SquirrelMail](#) que permite crear scripts hechos con Sieve en un servidor Cyrus IMAP que tenga habilitado el soporte para dicho lenguaje _ (Tim's SIEVE daemon). Avelsieve es parte de [Cyrusmaster](#), una herramienta de administración de Cyrus basada en web.

2.11 QMAIL.

Es un MTA que proporciona el servicio de correo electrónico en sistemas Linux y Unix, esta pensado

como un reemplazo mas seguro para el clásico SendMail.

2.12 FETCHMAIL

Permite acceder a un servidor externo de correo electrónico en un proveedor de servicio de Internet y bajar mensajes de usuarios con cuentas en este servidor externo, no requiere configuración y cualquier usuario puede tener un archivo en su directorio propio con la configuración de su cuenta de correo en el proveedor de servicio de Internet.

Puede centralizarse la recolección de correo externo creando un archivo con información de las cuentas de los usuario en diversos servidores externos; en una conexión periódica a Internet se traen y envían los mensajes de todos.

2.13 EXIM (Experimental Internet Mailer)

Es un agente de transporte de correo (MTA) y puede ser utilizado en la mayoría de los sistemas Unix (entre ellos GNU/Linux). Si bien puede compilarse en sistemas operativos Windows, se recomienda que sea utilizado en producción sobre sistemas operativos de la familia Linux. Se distribuye sin costo por lo que es un software libre.

Tiene una gran flexibilidad en los caminos que pueden seguir los mensajes según su origen y por presentar funcionalidades para control de Spam, listas de bloqueos basados en DNS, Virus, control de Relay, usuario y dominios virtuales y otros, que se configuran y mantienen en forma mas o menos sencilla.

Exim es el MTA por defecto en las distribuciones Debian GNU/LINUX

2.14 SENDMAIL

Permite configurar aspectos que normalmente yacen ocultos en el código compilado de otros programas similares. Sendmail es calificado de inseguro y con justa razón; tiene una gran larga historia de “vulnerabilidades” que han conminado a algunos administradores a optar por soluciones supuestamente mas seguras como Postfix y QMail, en ultimo adjetivo para sendmail puede ser legendario en el sentido que es una de las utilidades mas antiguas dentro de los sistemas Unix, y también en Linux es el servidor de e-mail mas utilizado e nivel mundial y sorprendentemente es a la vez una de las utilidades menos denominadas por los administradores debido a lo antes mencionado así como a una muy deficiente documentación.

2.15 OPENWEBMAIL

Es uno de los WebMails libres mas utilizados, de uso muy simple, esta dotado de una serie de herramientas muy potentes dentro de las que se encuentran:

- Libreta de Direcciones: con la posibilidad de mantener direcciones y grupos personales (por usuario) y globales (compartidas por todos los usuarios)
- Agenda y Calendario: para agendar eventos, compromisos, citas, etc.
- Disco Web: permite acceder a los archivos ubicados en le servidor a través de un interfaz web, con la posibilidad de almacenar en el mismo los archivos adjuntos de los mensajes recibidos y de adjuntarlos en mensajes salientes.

CAPITULO II

PROYECTO TEMÁTICO

3.1 PLANTEAMIENTO DEL PROYECTO TEMATICO

El proyecto a desarrollar consiste en la implementación de un servidor de correo electrónico seguro, con filtro antispam y antivirus, basado en open source, orientados para fines académicos para la Universidad Tecnológica de El Salvador, este se desarrolla en la distribución de DEBIAN 4.0; el proyecto se desarrolla en las siguientes etapas:

- 1.** Instalación de la distribución y configuración del sistema operativo DEBIAN 4.0
- 2.** Instalación y configuración de productos:
 - o POSTFIX MTA (Mail Transport Agent)
 - o TLS (Transportation Layer Security)
 - o CYRUS IMAP (Internet Message Access Protocol)
 - o CYRUS SASL (Simple Authentication and Security Layer)
 - o SMTP (Simple Mail Transfer Protocol)
 - o AMAVISD-NEW (Interfaz para filtros antivirus y antispam)
 - o SPAMASSASSIN (Filtro de identificación de Spam)
 - o CLAM ANTIVIRUS (Herramienta Antivirus)
 - o SQUIRRELMAIL (Paquete de correo electrónico)
 - o DNS (Servidor de dominio).
- 3.** Configuración del servidor de Correo Electrónico
- 4.** Elaboración detallada de Guías de Implementación del Correo Electrónico seguro, con filtro Antispam y Antivirus basado en Open Source.
- 5.** Realización de pruebas del prototipo de servidor de correo electrónico
- 6.** Entrega de Implementación Servidor de Correo Electrónico Seguro, con filtro Antispam y Antivirus basado en Open source, orientados a fines Académicos para la Universidad Tecnológica de El Salvador.

Este proyecto se esta desarrollando en un equipo tipo notebook modelo Intel celerón con un

procesador de 1.4Ghz con una memoria RAM de 756 Mb y un espacio particionado de 10 Gb en disco duro, la instalación de la distribución DEBIAN 4.0 ETCH es bastante sencilla pero se debe de tener mucho cuidado es en el tipo de ficheros que necesitamos que sea montado nuestro DEBIAN para ello seleccionamos ficheros raíz con extencion3 (ext3) y luego de ello nuestro DEBIAN continua su instalación, por otra parte después de instalado DEBIAN debemos instalar los productos que nos sirven para la implementación de correo electrónico por ejemplo, Cyrus IMAP ayuda a almacenar correos electrónicos de diferentes usuarios en el mismo fichero, Cyrus SASL este por su parte añade soporte de autenticación a protocolos basados en conexiones estandarizadas, sieve este crea un lenguaje que crea filtros de correo electrónico en el momento de la entrega final, Amavisd-New crea una interfaz de rendimiento y fiabilidad entre uno o mas contenidos antivirus y spam, Spamassasin es un filtro que identifica el spam mediante el análisis del texto usando listas negras a través de internet, clam es una herramienta de antivirus cuya función principal es integrar servidores de correo electrónico por medio del escaneo de datos adjuntos.

Squirrelmail este es un paquete de correo web que incorpora soporte PHP para los protocolos IMAP y SMTP.

3.

CRONOGRAMA DEL PROYECTO

No	DESCRIPCION	DIAS	INICIO	FIN	RECURSOS
1	Selección, Aprobación y Desarrollo de Proyecto	47 días	22/08/2007	22/10/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
2	Presentación de Proyecto a desarrollador para aprobación	2 días	22/08/2007	23/08/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
3	Desarrollo de Generalidades y Marco Teórico del proyecto	21 días	24/08/2007	21/09/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
4	Revisión y Aprobación de Generalidades y Marco Teórico	3 días	22/09/2007	25/09/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
5	Estructuración de Proyecto temático (segundo avance)	14 días	25/09/2007	12/10/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
6	Revisión de Proyecto Temático	1 día	13/10/2007	13/10/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
7	Desarrollo del Análisis de Prototipo	4 días	16/10/2007	19/10/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
8	Presentación de Análisis de Prototipo y Revisión de capítulos 2do, 3er	1 día	20/10/2007	20/10/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García
9	Instalación y configuración de Sistema Operativo y los paquetes a utilizar	1 día	22/10/2007	22/10/2007	Mania Elena Ramos, Alejandro Orellana, Freddy García

2 CRONOGRAMA

DEL PROYECTO.

DISEÑO Y ESTRUCTURA DEL PROYECTO					
No	DESCRIPCION	DIAS	INICIO	FIN	RECURSOS
1	Revisión y comparación de sistema operativo a utilizar en prototipo de servidor de correo electrónico	4 días	04/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
2	Instalación de SO DEBIAN 4.0 (ETC)	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
3	Selección de paquetes a utilizar en el proyecto	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
4	Instalación de paquetes seleccionados	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
5	Instalación de Cyrus IMAP	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
6	Instalación de Cyrus SASL	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
7	Instalación de POSTFIX	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
8	Instalación de SpamAssassin	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
9	Instalación de Amavis-New	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
10	Instalación de Cam-4V	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
11	Instalación de SquirrelMail	1 día	07/10/07	07/10/07	Elena Ramos, Fredy García, Alejandro Leonor
12	Configuración del servidor de correo electrónico	9 días	21/10/07	29/10/07	Elena Ramos, Fredy García, Alejandro Leonor
13	Configuración de Cyrus IMAP	1 día	22/10/07	22/10/07	Elena Ramos, Fredy García, Alejandro Leonor
14	Configuración de Cyrus SASL	1 día	23/10/07	23/10/07	Elena Ramos, Fredy García, Alejandro Leonor
15	Configuración de POSTFIX	1 día	24/10/07	24/10/07	Elena Ramos, Fredy García, Alejandro Leonor
16	Configuración SpamAssassin	1 día	25/10/07	25/10/07	Elena Ramos, Fredy García, Alejandro Leonor
17	Configuración de Amavis-New	1 día	26/10/07	26/10/07	Elena Ramos, Fredy García, Alejandro Leonor
18	Configuración de Cam-4V	1 día	27/10/07	28/10/07	Elena Ramos, Fredy García, Alejandro Leonor
19	Configuración de SquirrelMail	1 día	29/10/07	29/10/07	Elena Ramos, Fredy García, Alejandro Leonor
NOTA: EN EL CUADRO ANTERIOR SE ESTABLECE LA ESTRUCTURA DE LOS DÍAS Y LOS RECURSOS UTILIZADOS PARA LA IMPLEMENTACIÓN Y CONFIGURACIÓN DEL SERVIDOR DE CORREO ELECTRÓNICO.					

3.3 DOCUMENTACION TÉCNICA

*Documentos sobre comparaciones de productos y tecnologías sobre los aspectos técnicos de los

recursos a emplear en el prototipo.

SUSE Linux es una de las más conocidas [distribuciones GNU/Linux](#) existentes a nivel mundial, se basó en sus orígenes en [Slackware](#). Entre las principales virtudes de esta distribución se encuentra el que sea una de las más sencillas de instalar y administrar, ya que cuenta con varios asistentes gráficos para completar diversas tareas en especial por su gran herramienta de instalación y configuración [Yast](#). Su nombre "**SuSE**" es el acrónimo, en [alemán](#) "*Software und Systementwicklung*", el cual formaba parte del nombre original de la compañía y que se podría traducir como "**desarrollo de software y sistemas**". El nombre actual de la compañía es *SuSE LINUX*, habiendo perdido el primer término su significado... **(VER ANEXOS)**

Debian Linux es un sistema operativo (SO) [libre](#) para ordenadores. El sistema operativo es el conjunto de programas básicos y utilidades que hacen que funcione el ordenador. Debian utiliza el núcleo [Linux](#) (el corazón del sistema operativo), pero la mayor parte de las herramientas básicas vienen del [Proyecto GNU](#); de ahí el nombre GNU/Linux. Debian GNU/Linux ofrece más que un SO puro; viene con miles de [paquetes](#), programas precompilados distribuidos en un formato que hace más fácil la instalación. **(VER ANEXOS)**

- Nombre del Sitio: WWW.SEGURIDAD.UNAM.MX/ (Ver anexo #1)

URL: file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/TESIS/Departamento%20de%20Seguridad%20en%20C%C3%B3mputo.html

AUTOR: Universidad Nacional Autónoma de México

ÚLTIMA FECHA DE ACTUALIZACIÓN: 24-03-2006

- Nombre del Sitio: WWW.ENTER.COM (Ver anexo #2)

URL: http://enter.com.co/enter2/ente2_actu/articulo-web-nota_interior_2-3331806.html

AUTOR: Casa Editorial el Tiempo

ÚLTIMA FECHA DE ACTUALIZACIÓN: 10-11-2006

- Nombre del Sitio: HTTP:// SINETGY.ORG (ANEXO #3)

URL: <http://sinetgy.org/~jgb/articulos/soft-libre-que-es/>

AUTOR: JESÚS M. GONZÁLEZ BARAHONA

ÚLTIMA FECHA DE ACTUALIZACIÓN: 06-04-2003

- Nombre del Sitio: KERNELSOURCE.ORG (ANEXO #4)

URL: <http://kernelsource.org/2005/09/24/programa-3-2292005-breve-historia-de-gnulinux/>

AUTOR: Editorial Kernel Source

ÚLTIMA FECHA DE ACTUALIZACIÓN: 22-09-2005

- Nombre del Sitio: WWW.LINUXRSP.COM (ANEXO #5)

URL: <http://www.linuxrsp.ru/win-lin-soft/index-spanish.html>

AUTOR: FIODOR SOREX

ÚLTIMA FECHA DE ACTUALIZACIÓN: 07-07-2007

3.4 EVALUACION TECNICA Y ECONOMICA

En la realización de la implementación del servidor de correo electrónico seguro, con filtro Antispam y Antivirus, basado en open source, se realiza la siguiente evaluación técnica y económica de diferentes los diferentes productos a instalar en GNU/Linux:

* EL VALOR PARA ELEGIR Y UTILIZAR LA DISTRIBUCION DE LINUX DEBERA DE SER MAYOR O IGUAL A 100%.

3.5 TECNOLOGÍA Y RECURSOS SELECCIONADOS

Para la realización de la implementación del servidor de correo electrónico seguro, con filtros Antispam y Antivirus, basado en open source se ha decidido trabajar bajo la distribución Estable de Debían 4.0 (etch) por ser la distribución que posee las cualidades idóneas para la implementación del servidor de correo electrónico con las características antes mencionadas y la tecnología seleccionada a utilizar es: Procesador de: 1.4 Ghz (como mínimo), Memoria: 512 MB (como mínimo), Capacidad en disco duro: 10 GB (como mínimo) y Tarjeta de Red (Conexión a internet).

3.6 PRESUPUESTO PROYECTADO

San Salvador, 08 de Agosto del 2007.

Ingeniero Perdomo

Presente.

A consideración:

Nosotros "Grupo # 3", le presentamos el siguiente PRESUPUESTO para la Implementación de un Servidor de Correo Electrónico seguro, con filtro Antispam y Antivirus, basado en Open Source, orientado a fines Académicos para La Universidad Tecnológica de El Salvador.

Distribución de Software a Utilizar (Debian 4.0 ETCH)	\$0.00
Instalación de Sistema Operativo y Configuración de Servidor de Correo Electrónico y entrega de manuales y guías.	\$1,500.00
Creación de cuentas de correo (50 cuentas)	\$200.00
CPU Pentium III, 256 Mb de RAM disco duro de 10 GB, tarjeta de red ETHERNET y lectora de DVD.	\$250.00
TOTAL	\$1,950.00



3.7 OFERTA TECNICA

San Salvador, 8 de agosto de 2007

Señores.

Universidad Tecnológica de El Salvador

Presente.

Atención Ing. Perdomo

De ante mano deseándole éxitos en sus labores cotidianas Project Linux Corp. Le presenta la siguiente Oferta Técnica de la configuración de un Servidor de correo electrónico con las características de filtros AntiSpam y Antivirus basado en Open Source y orientado a fines académicos.

SOFTWARE A UTILIZAR:

- Distribución Libre (Debían 4.0 etch)
- MTA (agente de transporte de correo)
 - Qmail
 - Exim
- Cyrus SASL (soporte de autenticación de protocolos)
- Cyrus IMAP (almacenamiento de correo de usuarios)
- SpamAssassin (filtro de control de spam)
- ClamAV (antivirus)
- Amavisd-new (interfaz de filtros spam y antivirus)
- Squirrelmail (paquete de soporte PHP para protocolos IMAP y SMTP)
 - Fetchmail
 - Openwebmail



HARDWARE REQUERIDO:

- Computador Pentium III o similares AMD
- Procesador de 250 Mhz (como mínimo)
- Memoria 256 Mb (como mínimo)
- Espacio en Disco duro de 10 Gb (como mínimo)
- 1 Tarjeta de Red Ethernet/FastEthernet
- 1 Lectora de CD
- Otros: Monitor, teclado y mouse.

CONECTIVIDAD:

- Conexión a Internet de 256 Kbps (como mínimo)
- 1 IP Publica
- 1 Dominio propio con Domain Name Server.



OFERTA ECONOMICA

San Salvador, 08 de Agosto del 2007.

Ingeniero Perdomo

Presente.

A consideración:

Nosotros Project Linux Corp. Conocido como "Grupo # 3", le presentamos la siguiente OFERTA ECONOMICA para la Implementación de un Servidor de Correo Electrónico seguro, con filtro Antispam y Antivirus, basado en Open Source, orientado a fines Académicos para La Universidad Tecnológica de El Salvador.

Distribución de Software a Utilizar (Debian 4.0 ETCH)	\$0.00
Instalación de Sistema Operativo y Configuración de Servidor de Correo Electrónico y entrega de manuales y guías.	\$1,500.00
Creación de cuentas de correo (50 cuentas)	\$200.00
TOTAL	\$1,700.00

Por su atención, gracias.

Project Linux Corp.

CAPITULO IV

DISEÑO Y ELABORACION DEL PROTOTIPO

4.1 ARTICULO.

La idea se concibió en el transcurso del estudio de la carrera, luego de haber cursado varios ciclos, donde se ve la necesidad de agregar a las unidades de algunas asignaturas del pensum como Sistemas Operativos de Redes o Administración de Redes la Implementación de un Servidor de Correo Electrónico Seguro, con filtro Antispam y Antivirus, basado en Open Source; de esta manera se investiga sobre las diferentes distribuciones de Linux que son de licencia gratis, haciendo un comparativo entre las distribuciones de Debian 4.0 ETCH, Ubuntu 7.10 y Suse 10.2, optando por Debian 4.0 ETCH para el desarrollo de la implementación del prototipo de correo electrónico.

Para dicha implementación se empezó con el requerimiento del hardware el cual es el siguiente:

- Computador Pentium III o similares AMD
- Procesador de 250 Mhz (como mínimo)
- Memoria 256 Mb (como mínimo)
- Espacio en Disco duro de 10 Gb (como mínimo)
- 1 Tarjeta de Red Ethernet/FastEthernet
- 1 Lectora de CD
- Otros: Monitor, teclado y mouse.

CONECTIVIDAD REQUERIDA:

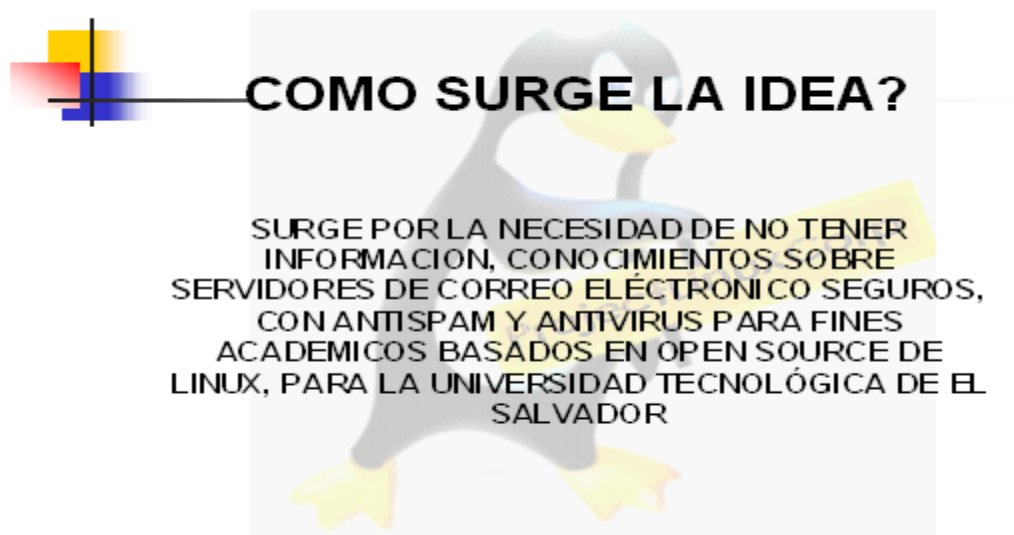
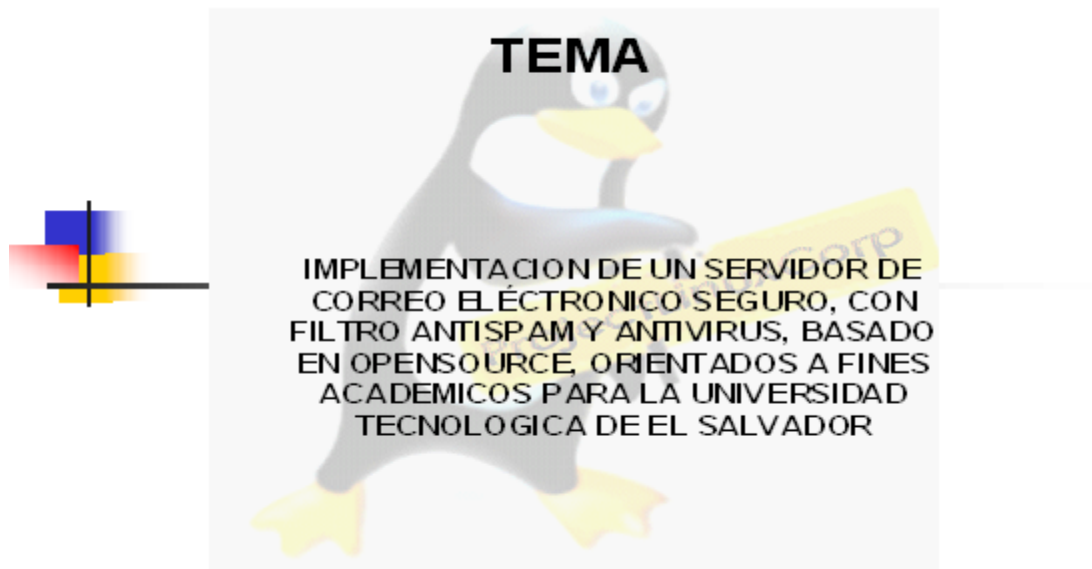
- Conexión a Internet de 256 Kbps (como mínimo)
- 1 IP Publica
- 1 Dominio propio con Domain Name Server.

Luego se Instaló el software a utilizar que es la Distribución de DEBIAN 4.0 ETCH de GNU/Linux de la versión estable, con sus respectivos paquetes; donde cada paquete tiene su propia función específica ejemplo de ello tenemos CYRUS IMAP que usa su propio método para almacenar el correo de los usuarios y cada mensaje es almacenado en su propio fichero, CYRUS SASL este añade soporte para la autenticación a protocolos e identificar y autenticar un usuario contra un servidor y para, opcionalmente, negociar la protección de las subsiguientes interacciones del protocolo, POSTFIX es una combinación de pequeños programas los cuales cada uno de ellos lleva a cabo una función específica, siendo así Postfix el agente de transporte de correo (MTA) mas rápido, fácil de administrar y a la vez seguro y podemos seguir mencionando otros paquetes que han sido instalados en dicha implementación del Correo electrónico para su desarrollo, todos los paquetes son instalados uno por uno, para luego integrarlos, logrando de esta manera el funcionamiento del prototipo del correo electrónico.

Ya instalado el prototipo de correo electronico se empieza a realizar los manuales y guias que seran los que utilizaran los alumnos de la carrera de Técnico en Ingeniería en Redes para realizar las prácticas en las asignaturas de Sistemas Operativos de Redes y Administración de Redes para la implementacion y configuración del correo electrónico seguro, con antispam y antivirus basado en Open Source orientado a fines académicos.

De esta manera esperamos a futuro poder actualizar la versión utilizada en la Implementación del Correo Electrónico y a la vez poder venderlo a las empresas donde laboramos ó a las que podamos ofrecer nuestro producto.

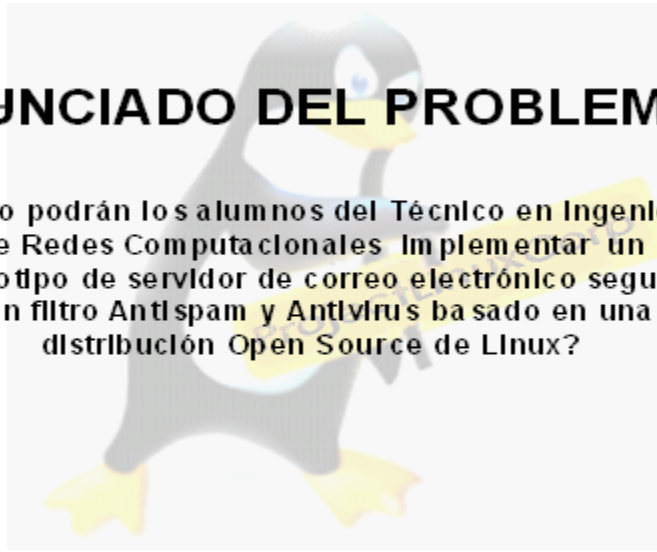
4.2 PRESENTACION DEL PROTOTIPO





ENUNCIADO DEL PROBLEMA

¿Como podrán los alumnos del Técnico en Ingeniería de Redes Computacionales Implementar un prototipo de servidor de correo electrónico seguro con filtro Antispam y Antivirus basado en una distribución Open Source de Linux?



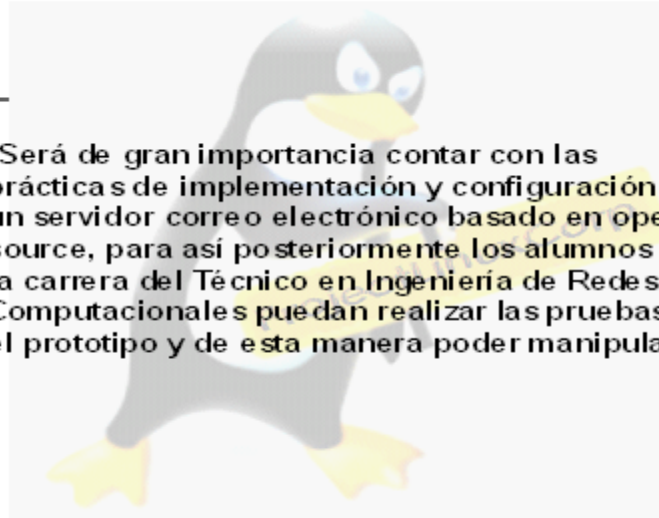
JUSTIFICACIÓN DEL PROYECTO

•Se creará un prototipo de un servidor de correo electrónico para que en este, los alumnos puedan realizar pruebas de cómo funciona dicho servidor.

•Con la creación de manuales y guías de implementación y configuración del servidor de correo electrónico se pretende que los alumnos puedan tener prácticas para tener un sólido conocimiento en configurar un servidor de correo electrónico seguro que posea filtros AntiSpam y AntiVirus, y así resolver problemas que a este se le presenten a futuro en esta rama.

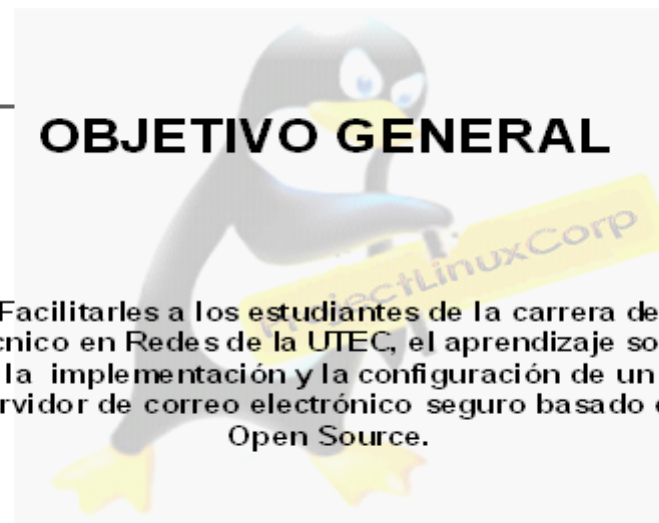


•Será de gran importancia contar con las prácticas de implementación y configuración de un servidor correo electrónico basado en open source, para así posteriormente los alumnos de la carrera del Técnico en Ingeniería de Redes Computacionales puedan realizar las pruebas en el prototipo y de esta manera poder manipularlo.



OBJETIVO GENERAL

Facilitarles a los estudiantes de la carrera de Técnico en Redes de la UTEC, el aprendizaje sobre la implementación y la configuración de un servidor de correo electrónico seguro basado en Open Source.



- Realizar la implementación del prototipo del servidor de correo electrónico seguro, con filtro Antispam y Antivirus basado en Open Source a través del paso a paso de las guías.

- ELABORACION DE TABLA COMPARATIVA DE DISTRIBUCIONES EN LINUX DE LICENCIA G

CARACTERISTICA	VALOR REQUERIDO	PESO O PORCENTAJE	DEBIAN 4.6		UBUNTU 7.10		SUSE 16.2	
			PONDERRACION	CALIFICACION	PONDERRACION	CALIFICACION	PONDERRACION	CALIFICACION
DOCUMENTACION	Disponibilidad y variedad de manuales.	30%	2	60%	2	60%	2	60%
REQUIREMIENTO DE HARDWARE	Compatible con especificaciones mínimas.	25%	2	50%	2	20%	1	25%
PAQUETES ANTISPAM	Que trabaje con Spamassassin	20%	2	40%	2	40%	2	40%
PAQUETES ANTI VIRUS	Que trabaje con ClamAV	20%	2	40%	1	20%	1	20%
SERVIDOR	Facile configurar	5%	2	10%	1	5%	1	5%
			TOTALES	200%		150%		80%
				100%		75%		75%
FUNDAMENTOS								
# NO CUMPLE LAS ESPECIFICACIONES								
# CUMPLE LAS ESPECIFICACIONES FACILMENTE								
# CUMPLE LAS ESPECIFICACIONES								

* EL VALOR PARA ELEGER Y UTILIZAR LA DISTRIBUCION DE LINUX DEBERA DE SER MAYOR O IGUAL A 100%

CARACTERISTICA	VALOR REQUERIDO	PESO O PORCENTAJE	DEBIAN 4.6		UBUNTU 7.10		SUSE 10.2	
			PONDERRACION	CALIFICACION	PONDERRACION	CALIFICACION	PONDERRACION	CALIFICACION
DOCUMENTACION	Disponibilidad y variedad de manuales.	30%	2	60%	2	60%	2	60%
REQUIREMIENTO DE HARDWARE	Compatible con especificaciones mínimas.	25%	2	50%	2	20%	1	25%
PAQUETES ANTISPAM	Que trabaje con Spamassassin	20%	2	40%	2	40%	2	40%
PAQUETES ANTI VIRUS	Que trabaje con ClamAV	20%	2	40%	1	20%	1	20%
SERVICIOR	Facile configurar	5%	2	10%	1	5%	1	5%
			TOTALES	200%		150%		80%
				100%		75%		75%
FUNDAMENTOS								
* EL VALOR PARA ELEGER Y UTILIZAR LA DISTRIBUCION DE LINUX DEBERA DE SER MAYOR O IGUAL A 100%								

0 = NO CUMPLE LAS ESPECIFICACIONES

1 = CUMPLE A MEDIDAS PERDIDAS FACT
--

2 = COMPLETE EXPECTATIONS

* EL VALOR PARA ELEGIR Y UTILIZAR LA DISTRIBUCION DE LINUX DEBERA DE SER MAYOR O IGUAL A 1000



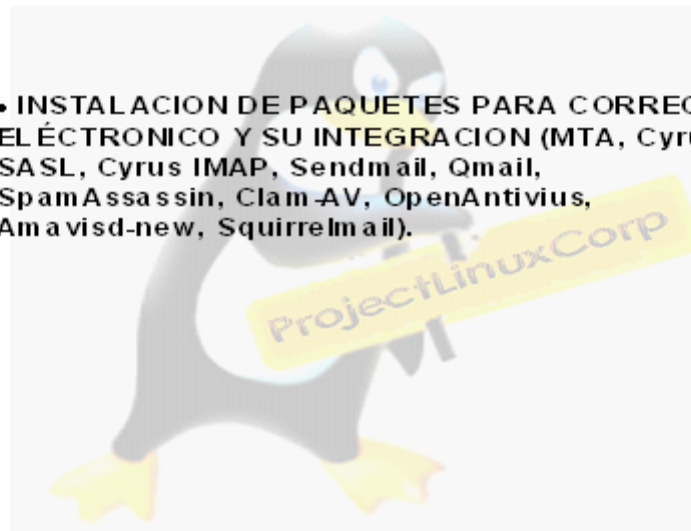
• **SELECCIÓN DE HARDWARE REQUERIDO:**
Computador Pentium III o similares AMD
Procesador de 250 Mhz (como mínimo)
Memoria 256 Mb (como mínimo)
Espacio en Disco duro de 10 Gb (como mínimo)
1 Tarjeta de Red Ethernet/FastEthernet
1 Lectora de CD
Otros: Monitor, teclado y mouse.

CONECTIVIDAD:
Conexión a Internet de 256 Kbps (como mínimo)
1 IP Publica
1 Dominio propio con Domain Name Server.

• **SELECCIÓN DE DISTRIBUCION A UTILIZAR**
(SE OPTA POR DEBIAN 4.0 ETCH)



• **INSTALACION DE PAQUETES PARA CORREO ELÉCTRONICO Y SU INTEGRACION (MTA, Cyrus SASL, Cyrus IMAP, Sendmail, Qmail, SpamAssassin, Clam-AV, OpenAntivirus, Amavisd-new, Squirrelmail).**



DISEÑO Y ESTRUCTURA DEL PROYECTO

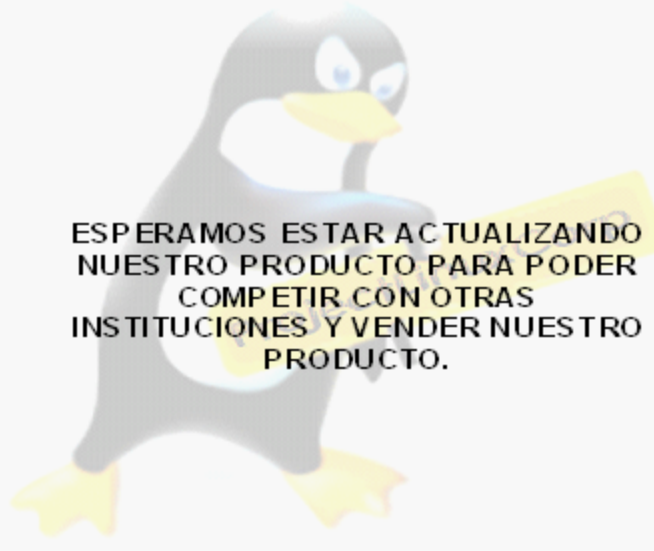
DISEÑO Y ESTRUCTURA DEL PROYECTO					
NO.	DESCRIPCION	DIAS	INICIO	FIN	RECURSOS
1	Revisión y comparación de sistema operativo a utilizar en prototipo de servidor de correo electrónico	4 días	04/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
2	Instalación de S.O. DEB EN 4.0 (ETCH)	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
3	Selección de paquetes a utilizar en el proyecto	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
4	Instalación de paquetes seleccionados	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
5	Instalación de Cyrus IMAP	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
6	Instalación de Cyrus SASL	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
7	Instalación de POSTFIX	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
8	Instalación de SpamAssassin	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
9	Instalación de Amavis-New	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
10	Instalación de Clam-AV	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
11	Instalación de Squirrel Mail	1 día	07/10/07	07/10/07	Bena Ramos, Fredy García, Alejandro Leonor
12	Configuración del servidor de correo electrónico	9 días	21/10/07	29/10/07	Bena Ramos, Fredy García, Alejandro Leonor
13	Configuración de Cyrus IMAP	1 día	22/10/07	22/10/07	Bena Ramos, Fredy García, Alejandro Leonor
14	Configuración de Cyrus SASL	1 día	23/10/07	23/10/07	Bena Ramos, Fredy García, Alejandro Leonor
15	Configuración de POSTFIX	1 día	24/10/07	24/10/07	Bena Ramos, Fredy García, Alejandro Leonor
16	Configuración SpamAssassin	1 día	25/10/07	25/10/07	Bena Ramos, Fredy García, Alejandro Leonor
17	Configuración de Amavis-New	1 día	26/10/07	26/10/07	Bena Ramos, Fredy García, Alejandro Leonor
18	Configuración de Clam-AV	1 día	27/10/07	28/10/07	Bena Ramos, Fredy García, Alejandro Leonor
19	Configuración de Squirrel Mail	1 día	28/10/07	29/10/07	Bena Ramos, Fredy García, Alejandro Leonor

NOTA: EN EL CUADRO ANTERIOR SE ESTABLECE LA ESTRUCTURA DE LOS DIAS Y LOS RECURSOS UTILIZADOS PARA LA IMPLEMENTACIÓN Y CONFIGURACIÓN DEL SERVIDOR DE CORREO ELECTRÓNICO.

REALIZACIÓN DE MANUALES Y GUÍAS PARA LA IMPLEMENTACIÓN Y CONFIGURACIÓN DEL CORREO ELECTRÓNICO SEGURO, FILTRO ANTISPAM Y ANTIVIRUS, BASADOS EN OPEN SOURCE PARA FINES ACADÉMICOS.



**ESPERAMOS ESTAR ACTUALIZANDO
NUESTRO PRODUCTO PARA PODER
COMPETIR CON OTRAS
INSTITUCIONES Y VENDER NUESTRO
PRODUCTO.**



INSTALACION Y CONFIGURACION DE PAQUETES

CONFIGURACION DE CYRUS IMAP, en ruta de archivo: redes: /etc# cat -n cyrus.conf

```
# Debian Cyrus imapd.conf
apt-get install libsasl2 sasl2-bin libsasl2-modules
```

```
# Configuration directory
configdirectory: /var/lib/cyrus
START=yes
MECHANISMS="sasl2"
/etc/init.d/saslauthd start
```

```
# Which partition to use for default mailboxes
defaultpartition: default
partition-default: /var/spool/cyrus/mail
```

```
START {
recover    cmd="/usr/sbin/ctl_cyrusdb -r"
delprune   cmd="/usr/sbin/ctl_deliver -E 3"
tlsprune   cmd="/usr/sbin/tls_prune"
}
SERVICES {
imap       cmd="imapd -U 30" listen="imap" prefork=0 maxchild=100
lmtpunix    cmd="lmtpd" listen="/var/run/cyrus/socket/lmtp" prefork=0 maxchild=20
sieve      cmd="timsieved" listen="localhost:sieve" prefork=0 maxchild=100
notify     cmd="notified" listen="/var/run/cyrus/socket/notify" proto="udp" prefork=1
}
EVENTS {
checkpoint cmd="/usr/sbin/ctl_cyrusdb -c" period=30
delprune   cmd="/usr/sbin/ctl_deliver -E 3" at=0401
tlsprune   cmd="/usr/sbin/tls_prune" at=0401
}
```

```
# News setup
partition-news: /var/spool/cyrus/news
newsspool: /var/spool/news
```

```
# Alternate namespace
# If enabled, activate the alternate namespace as documented in
# /usr/share/doc/cyrus21-doc/html/altnamespace.html, where an user's
# subfolders are in the same level as the INBOX
# See also userprefix and sharedprefix on imapd.conf(5)
altnamespace: no
```

```
# UNIX Hierarchy Convention
# Set to yes, and cyrus will accept dots in names, and use the forward
# slash "/" to delimit levels of the hierarchy. This is done by converting
# internally all dots to "^", and all "/" to dots. So the "rabbit.holes"
# mailbox of user "helmer.fudd" is stored in "user.elmer^fud.rabbit^holes"
unixhierarchysep: no
```

```
# Munging illegal characters in headers
```

```
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including most
# spamware. Disable this if you want Cyrus to leave the crappage untouched
# and you don't care that IMAP SEARCH won't work right anymore.
#munge8bit: no

# Forcing recipient user to lowercase
# Cyrus 2.1 is case-sensitive. If all your mail users are in lowercase, it is
# probably a very good idea to set lmtp_downcase_rcpt to true. The default is
# to assume the user knows what he is doing, and not downcase anything.
#lmtp_downcase_rcpt: yes

# Uncomment the following and add the space-separated users who
# have admin rights for all services.
#admins: cyrus

# Space-separated list of users that have lmtp "admin" status (i.e. that
# can deliver email through TCP/IP lmtp) in addition to those in the
# admins: entry above
#lmtp_admins: postman

# Space-separated list of users that have mupdate "admin" status, in
# addition to those in the admins: entry above. Note that mupdate slaves and
# backends in a Murder cluster need to authenticate against the mupdate master
# as admin users.
#mupdate_admins: mupdateman

# Space-separated list of users that have imapd "admin" status, in
# addition to those in the admins: entry above
#imap_admins: cyrus

# Space-separated list of users that have sieve "admin" status, in
# addition to those in the admins: entry above

#sieve_admins: cyrus
configdirectory: /var/lib/cyrus
defaultpartition: default
partition-default: /var/spool/cyrus/mail
partition-news: /var/spool/cyrus/news
newsspool: /var/spool/news
altnamespace: no
unixhierarchysep: no
lmtp_downcase_rcpt: yes
admins: cyrus
allowanonymouslogin: no
popminpoll: 1
autocreatequota: 0
umask: 027
sieveusehomedir: false
sievedir: /var/spool/sieve
hashimapspool: true
allowplaintext: yes
```

```
sasl_mech_list: PLAIN
sasl_minimum_layer: 0
sasl_pwcheck_method: saslauthd
sasl_auxprop_plugin: sasldb
sasl_auto_transition: no
tls_ca_path: /etc/ssl/certs
tls_session_timeout: 1440
tls_cipher_list: TLSv1:SSLv3:SSLv2:!NULL:!EXPORT:!DES:!LOW:@STRENGTH
lmtpsocket: /var/run/cyrus/socket/lmtp
idlesocket: /var/run/cyrus/socket/idle
notifysocket: /var/run/cyrus/socket/notify
```

```
# List of users and groups that are allowed to proxy for other users,
# seperated by spaces. Any user listed in this will be allowed to login
# for any other user. Like "admins:" above, you can have imap_proxyserver
# and sieve_proxyserver.
#proxyserver: cyrus
```

```
# No anonymous logins
allowanonymouslogin: no
```

```
# Minimum time between POP mail fetches in minutes
popminpoll: 1
```

```
# Sendmail binary location
# DUE TO A BUG, Cyrus sends CRLF EOLs to this program. This breaks Exim 3.
# For now, to work around the bug, set this to a wrapper that calls
# /usr/sbin/sendmail -dropcr instead if you use Exim 3.
#sendmail: /usr/sbin/sendmail
```

```
# The maximum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires some
# amount of encryption.
#sasl_maximum_layer: 256
```

```
# List of remote realms whose users may log in using cross-realm
# authentications. Separate each realm name by a space. A cross-realm
```

```
# identity is considered any identity returned by SASL with an "@" in it.
#loginrealms:

#
# SASL library options (these are handled directly by the SASL libraries,
# refer to SASL documentation for an up-to-date list of these)
#

# The mechanism(s) used by the server to verify plaintext passwords. Possible
# values are "saslauthd", "auxprop", "pwcheck" and "alwaystrue". They
# are tried in order, you can specify more than one, separated by spaces.
#
# Do note that, since sasl will be run as user cyrus, you may have a lot of
# trouble to set this up right.
sasl_pwcheck_method: auxprop

# What auxpropd plugins to load, if using sasl_pwcheck_method: auxprop
# by default, all plugins are tried (which is probably NOT what you want).
#sasl_auxprop_plugin: sasldb

# If enabled, the SASL library will automatically create authentication secrets
# when given a plaintext password. Refer to SASL documentation
sasl_auto_transition: no

#
# SSL/TLS Options
#
# Remember that Cyrus needs to access these as user cyrus, not as root,
# you will need to take care of file permissions according to your system's
# policy.
#

# File containing the global certificate used for ALL services (imap, pop3,
# lmtp, sieve)
#tls_cert_file: /etc/ssl/certs/cyrus-global.pem

# File containing the private key belonging to the global server certificate.
#tls_key_file: /etc/ssl/private-cyrus/cyrus-global.key

# File containing the certificate used for imap. If not specified, the global
# certificate is used. A value of "disabled" will disable SSL/TLS for imap.
#tls_imap_cert_file: /etc/ssl/certs/cyrus-imap.pem

# File containing the private key belonging to the imap-specific server
# certificate. If not specified, the global private key is used. A value of
# "disabled" will disable SSL/TLS for imap.
#tls_imap_key_file: /etc/ssl/private-cyrus/cyrus-imap.key

# File containing the certificate used for pop3. If not specified, the global
# certificate is used. A value of "disabled" will disable SSL/TLS for pop3.
#tls_pop3_cert_file: /etc/ssl/certs/cyrus-pop3.pem

# File containing the private key belonging to the pop3-specific server
# certificate. If not specified, the global private key is used. A value of
# "disabled" will disable SSL/TLS for pop3.
#tls_pop3_key_file: /etc/ssl/private-cyrus/cyrus-pop3.key

# File containing the certificate used for lmtp. If not specified, the global
```

```
# certificate is used. A value of "disabled" will disable SSL/TLS for Imtp.
#tls_lmtp_cert_file: /etc/ssl/certs/cyrus-lmtp.pem

# File containing the private key belonging to the Imtp-specific server
# certificate. If not specified, the global private key is used. A value of
# "disabled" will disable SSL/TLS for Imtp.
#tls_lmtp_key_file: /etc/ssl/private-cyrus/cyrus-lmtp.key

# File containing the certificate used for sieve. If not specified, the global
# certificate is used. A value of "disabled" will disable SSL/TLS for sieve.
#tls_sieve_cert_file: /etc/ssl/certs/cyrus-sieve.pem

# File containing the private key belonging to the sieve-specific server
# certificate. If not specified, the global private key is used. A value of
# "disabled" will disable SSL/TLS for sieve.
#tls_sieve_key_file: /etc/ssl/private-cyrus/cyrus-sieve.key

# File containing one or more Certificate Authority (CA) certificates.
#tls_ca_file: /etc/ssl/certs/cyrus-imapd-ca.pem

# Path to directory with certificates of CAs.
tls_ca_path: /etc/ssl/certs

# The length of time (in minutes) that a TLS session will be cached for later
# reuse. The maximum value is 1440 (24 hours), the default. A value of 0 will
# disable session caching.
tls_session_timeout: 1440

# The list of SSL/TLS ciphers to allow. The format of the string is described
# in ciphers(1). THIS DISABLES THE WEAK 'FOR EXPORT' CRAP!
tls_cipher_list: TLSv1:SSLv3:SSLv2:!NULL:!EXPORT:!DES:!LOW:@STRENGTH

# Require a client certificate for ALL services (imap, pop3, Imtp, sieve).
#tls_require_cert: false

# Require a client certificate for imap ONLY.
#tls_imap_require_cert: false

# Require a client certificate for pop3 ONLY.
#tls_pop3_require_cert: false

# Require a client certificate for Imtp ONLY.
#tls_lmtp_require_cert: false
```

CONFIGURACION DE POSTFIX en ruta de archivo: redes: /etc/postfix# cat -n master.cf

apt-get install postfix postfix-tls postfix-doc postfix-pcre mime-codecs

redes:/etc/postfix# cat -n master.cf

```
1 #
2 # Postfix master process configuration file. For details on the format
3 # of the file, see the master(5) manual page (command: "man 5 master").
4 #
5 # =====
6 # service type private unpriv chroot wakeup maxproc command + args
7 #          (yes) (yes) (yes) (never) (100)
8 # =====
```

```

9 smtp    inet n    -    -    -    -    smtpd
10 #submission inet n    -    -    -    -    smtpd
11 # -o smtpd_enforce_tls=yes
12 # -o smtpd_sasl_auth_enable=yes
13 # -o smtpd_client_restrictions=permit_sasl_authenticated,reject
14 #smtps   inet n    -    -    -    -    smtpd
15 # -o smtpd_tls_wrappermode=yes
16 # -o smtpd_sasl_auth_enable=yes
17 # -o smtpd_client_restrictions=permit_sasl_authenticated,reject
18 #628     inet n    -    -    -    -    qmqpd
19 pickup  fifo n    -    -    60    1    pickup
20 cleanup unix n    -    -    -    0    cleanup
21 qmgr     fifo n    -    n    300    1    qmgr
22 #qmgr     fifo n    -    -    300    1    oqmgr
23 tlsmgr    unix -    -    -    1000?  1    tlsmgr
24 rewrite  unix -    -    -    -    -    trivial-rewrite
25 bounce   unix -    -    -    -    0    bounce
26 defer    unix -    -    -    -    0    bounce
27 trace    unix -    -    -    -    0    bounce
28 verify   unix -    -    -    -    1    verify
29 flush    unix n    -    -    1000?  0    flush
30 proxymap unix -    -    n    -    -    proxymap
31 smtp     unix -    -    -    -    -    smtp
32 # When relaying mail as backup MX, disable fallback_relay to avoid MX loops
33 relay    unix -    -    -    -    -    smtp
34     -o fallback_relay=
35 #     -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
36 showq    unix n    -    -    -    -    showq
37 error    unix -    -    -    -    -    error
38 discard  unix -    -    -    -    -    discard
39 local    unix -    n    n    -    -    local
40 virtual  unix -    n    n    -    -    virtual
41 lmtp     unix -    -    -    -    -    lmtp
42 anvil    unix -    -    -    -    1    anvil
43 scache   unix -    -    -    -    1    s cache
44 #
45 # =====
46 # Interfaces to non-Postfix software. Be sure to examine the manual
47 # pages of the non-Postfix software to find out what options it wants.
48 #
49 # Many of the following services use the Postfix pipe(8) delivery
50 # agent. See the pipe(8) man page for information about ${recipient}
51 # and other message envelope options.
52 # =====
53 #
54 # maildrop. See the Postfix MAILDROP_README file for details.
55 # Also specify in main.cf: maildrop_destination_recipient_limit=1
56 #
57 maildrop  unix -    n    n    -    -    pipe
58 flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
59 #
60 # See the Postfix UUCP_README file for configuration details.
61 #
62 uucp      unix -    n    n    -    -    pipe
63 flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
64 #
65 # Other external delivery methods.
66 #

```

```

67 ifmail  unix -   n   n   -   -   pipe
68  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nex thop ($recipient)
69 bsmtp  unix -   n   n   -   -   pipe
70  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$ne xthop -f$sender $recipient
71 scalemail-backend unix -   n   n   -   p ipe
72  flags=R user=scaemail argv=/usr/lib/scaemail/bin/s caemail-store ${nexthop} ${user} ${extension}
73 mailman unix -   n   n   -   -   pipe
74  flags=FR user=list argv=/usr/lib/mailman/bin/postfix -to-mailman.py
75  ${nexthop} ${user}
76
77
78 #configuracion lmtip para amavis
79 amavisfeed unix -   -   n   -   2   lmtip
80  -o lmtip_data_done_timeout=1200
81  -o lmtip_send_xforward_command=yes
82  -o disable_dns_lookups=yes
83  -o max_use=20
84
85 #configuracion smtp para amavis
86 #amavisfeed unix -   -   n   -   2   smtp
87  -o smtp_data_done_timeout=1200
88  -o smtp_send_xforward_command=yes
89  -o disable_dns_lookups=yes
90  -o max_use=20
91
92 #servidor smtp que recibe todo lo calificado por amavi s
93 #
94 127.0.0.1:10025 inet n   -   n   -   -   smtpd
95  -o content_filter
96  -o smtpd_delay_reject=no
97  -o smtpd_client_restrictions=permit_myn etworks,reject
98  -o smtpd_helo_restrictions=
99  -o smtpd_sender_restrictions=
100  -o smtpd_recipient_restr ictions=permit_mynetworks,reject
101  -o smtpd_data_restr ictions=reject_unauth_pipelining
102  -o smtpd_end_o f_data_restrictions=
103  -o smtpd_restriction_classes=
104  -o m ynetworks=127.0.0.0/8
105 -o smtpd_error_sleep_time=0
106  -o smtpd_soft_error_limit=1001
107  -o smtpd_hard_error_limit=1000
108  -o smtpd_client_connection_count_limit =0
109  -o smtpd_client_connection_rate_limit=0
110  -o receive_override_options=no_header_ body_checks,no_unknown_recipient_checks,no_milters
111  -o local_header_rewrite_clients=
112 ##

```

redes:/etc/postfix# cat -n main.cf

```

1 # See /usr/share/postfix/main.cf.dist for a commented, more complete version
2
3
4 # Debian specific: Specifying a file name will cause the first
5 # line of that file to be used as the name. The Debian default
6 # is /etc/mailname.
7 #myorigin = /etc/mailname
8
9 smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)

```

```

10 biff = no
11
12 # appending .domain is the MUA's job.
13 append_dot_mydomain = no
14
15 # Uncomment the next line to generate "delayed mail" warnings
16 #delay_warning_time = 4h
17
18 # TLS parameters
19 smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
20 smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
21 smtpd_use_tls=yes
22 smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
23 smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache
24
25 # See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
26 # information on enabling SSL in the smtp client.
27
28 myhostname = redes.utec.edu.sv
29 alias_maps = hash:/etc/aliases
30 alias_database = hash:/etc/aliases
31 myorigin = /etc/mailname
32 mydestination = redes.utec.edu.sv, localhost.utec.edu.sv, localhost
33 relayhost =
34 mynetworks = 127.0.0.0/8
35 #mailbox_command = procmail -a "$EXTENSION"
36 mailbox_size_limit = 0
37 home_mailbox = Maildir/
38 recipient_delimiter = +
39 inet_interfaces = all
40 unknown_local_recipient_reject_code = 450
41 content_filter=amavisfeed:[127.0.0.1]:10024

```

CONFIGURACION DE SPAMASSASSIN en ruta de archivo: redes: /etc / spamassasin# cat -n local.cf

```

# This is the right place to customize your installation of SpamAssassin.
#
# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be
# tweaked.
#
# Only a small subset of options are listed below
#
#####
# Add *****SPAM***** to the Subject header of spam e-mails
#
# rewrite_header Subject *****SPAM*****
# Save spam messages as a message/rfc822 MIME attachment instead of
# modifying the original message (0: off, 2: use text/plain instead)
#
# report_safe 1
# Set which networks or hosts are considered 'trusted' by your mail

```

```
# server (i.e. not spammers)
#
# trusted_networks 212.17.35.
# Set file-locking method (flock is not safe over NFS, but is faster)
#
# lock_method flock
# Set the threshold at which a message is considered spam (default: 5.0)
#
# required_score 5.0
# Use Bayesian classifier (default: 1)
#
# use_bayes 1
# Bayesian classifier auto-learning (default: 1)
#
# bayes_auto_learn 1
# Set headers which may provide inappropriate cues to the Bayesian
# classifier
#
# bayes_ignore_header X-Bogosity
# bayes_ignore_header X-Spam-Flag
# bayes_ignore_header X-Spam-Status
```

CONFIGURACIÓN DE CLAM-AV. en ruta de archivo: `redes: /etc / clamav# cat -n clamd.conf`

```
#Automatically Generated by clamav-base postinst
#To reconfigure clamd run #dpkg-reconfigure clamav-base
#Please read /usr/share/doc/clamav-base/README.Debian.gz for details
LocalSocket /var/run/clamav/clamdctl
FixStaleSocket true
User clamav
AllowSupplementaryGroups true
ScanMail true
ScanArchive true
ArchiveMaxRecursion 5
ArchiveMaxFiles 1000
ArchiveMaxFileSize 10M
ArchiveMaxCompressionRatio 250
ArchiveLimitMemoryUsage false
ArchiveBlockEncrypted false
MaxDirectoryRecursion 15
FollowDirectorySymlinks false
FollowFileSymlinks false
ReadTimeout 180
MaxThreads 12
MaxConnectionQueueLength 15
StreamMaxLength 10M
LogSyslog false
LogFacility LOG_LOCAL6
LogClean false
LogVerbose false
PidFile /var/run/clamav/clamd.pid
DatabaseDirectory /var/lib/clamav
```

```

TemporaryDirectory /tmp
SelfCheck 3600
Foreground false
Debug false
ScanPE true
ScanOLE2 true
ScanHTML true
DetectBrokenExecutables false
MailFollowURLs false
ArchiveBlockMax false
ExitOnOOM false
LeaveTemporaryFiles false
AlgorithmicDetection true
ScanELF true
NodalCoreAcceleration false
IdleTimeout 30
MailMaxRecursion 64
PhishingSignatures true
LogFile /var/log/clamav/clamav.log
LogTime true
LogFileUnlock false
LogFileMaxSize 0

```

**CONFIGURACION DE SQUIRREMAIL, en ruta de archivo: redes: /etc / squirrelmail# cat -n
apache.conf**

```

</IfModule>
<IfModule mod_php5.c>
    php_flag register_globals off
</IfModule>
<IfModule mod_dir.c>
    DirectoryIndex index.php
</IfModule>

# access to configtest is limited by default to prevent information leak
<Files configtest.php>
    order deny,allow
    deny from all
    allow from 127.0.0.1
</Files>
</Directory>

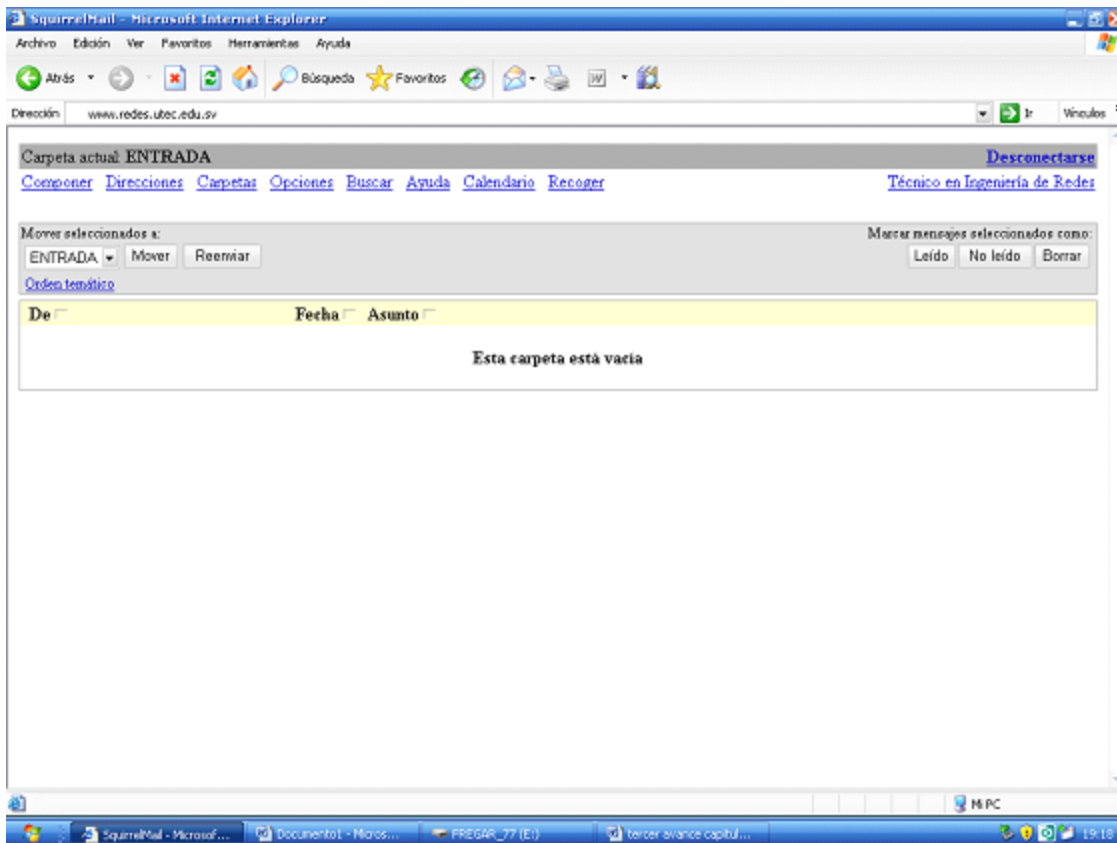
# users will prefer a simple URL like http://webmail.example.com
#<VirtualHost 1.2.3.4>
# DocumentRoot /usr/share/squirrelmail
# ServerName webmail.example.com
#</VirtualHost>

# redirect to https when available (thanks omen@descolada.dartmouth.edu)
#
# Note: There are multiple ways to do this, and which one is suitable for
# your site's configuration depends. Consult the apache documentation if
# you're unsure, as this example might not work everywhere.
#
#<IfModule mod_rewrite.c>
# <IfModule mod_ssl.c>

```

```
# <Location /squirrelmail>
# RewriteEngine on
# RewriteCond %{HTTPS} !on$ [NC]
# RewriteRule . https://%{HTTP_HOST}%{REQUEST_URI} [L]
# </Location>
# </IfModule>
#</IfModule>
```

4.3 EVIDENCIAS DEL AVANCE DEL PROYECTO



En esta pantalla se muestra la bandeja de entrada del prototipo de correo electrónico, el cual ha sido configurado con WebMail.

SquirrelMail - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Abás Búsqueda Favoritos

Dirección: www.redes.utec.edu.sv

[Comenzar](#) [Direcciones](#) [Carpetas](#) [Opciones](#) [Buscar](#) [Ayuda](#) [Calendario](#) [Recoger](#) [Técnico en Ingeniería de Redes](#)

Para:

Cc:

Bcc:

Asunto:

Prioridad: Normal Confirmación: ☐ De lectura ☐ De entrega

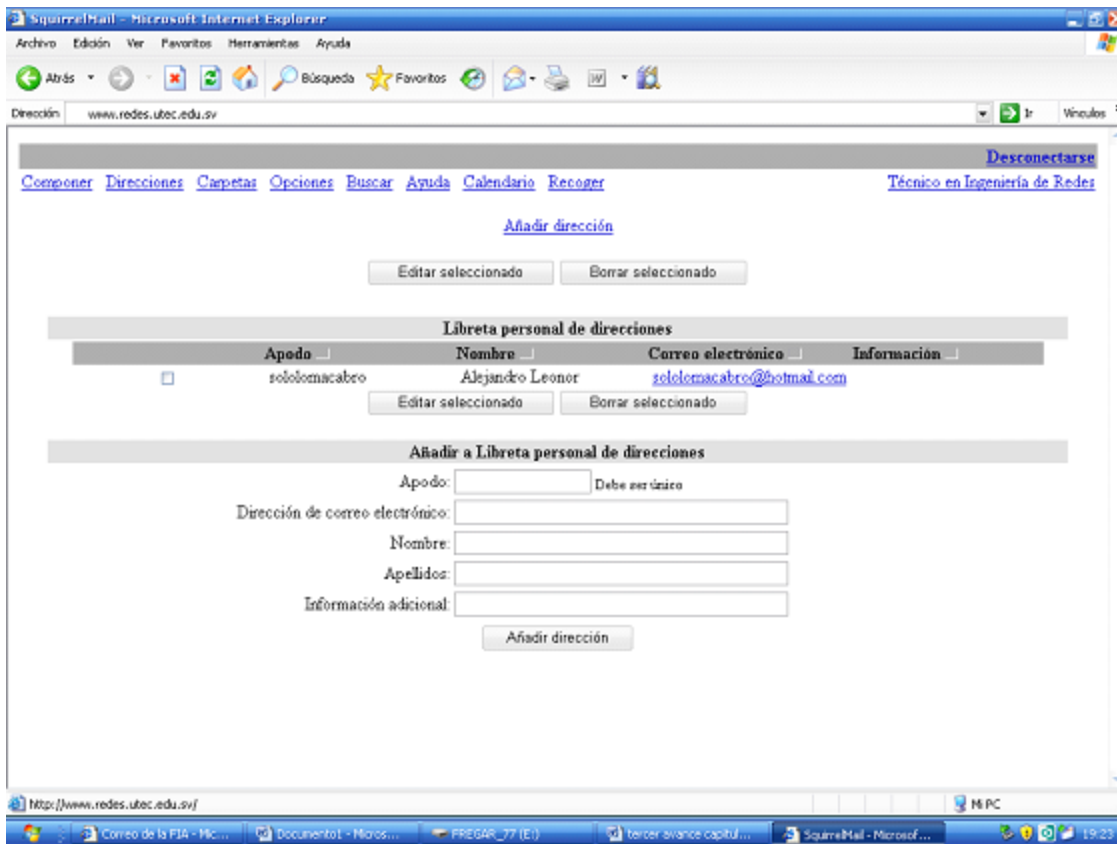
Firma Direcciones Guardar borrador Enviar Ortografía

Enviar

Adjunto: Examinar... Añadir (max: 2 M)

<http://www.redes.utec.edu.sv/> N PC 19:21

En esta pantalla se muestra como se creara o ingresara el correo a enviar.



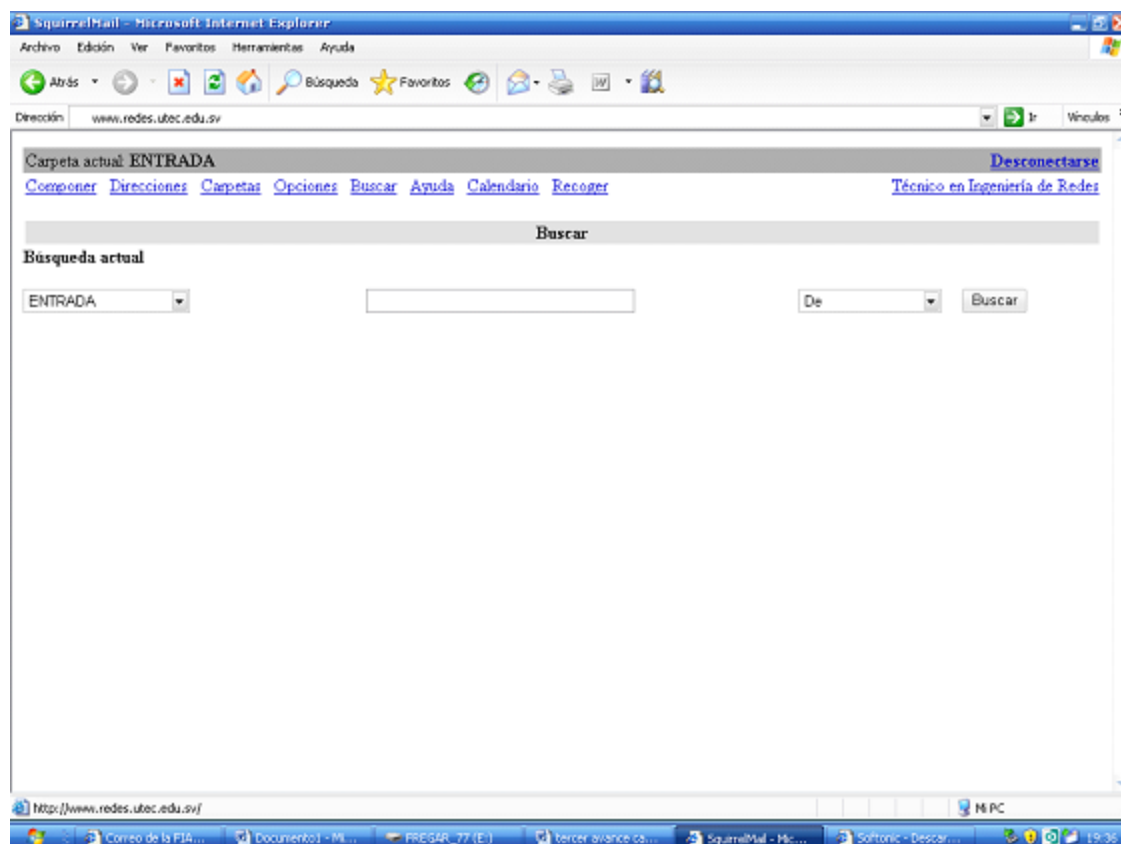
En esta pantalla es donde se encuentran las direcciones de todos los contactos o se pueden agregar nuevos.



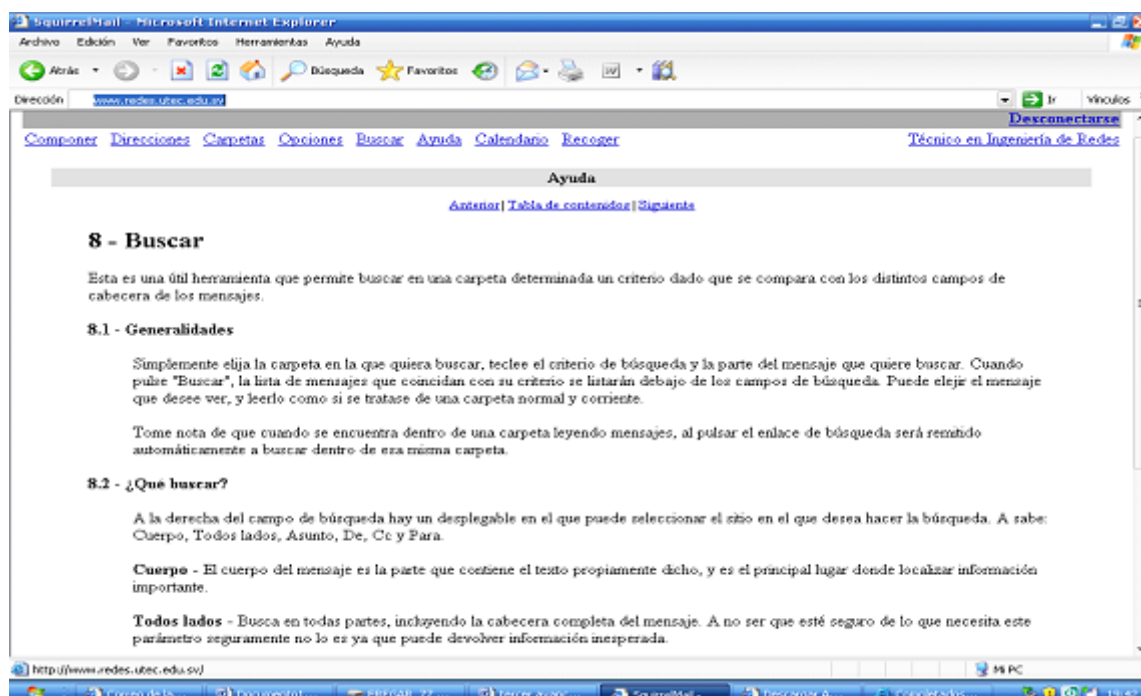
En esta pantalla se muestra en donde se pueden crear y guardar las carpetas que deseemos.

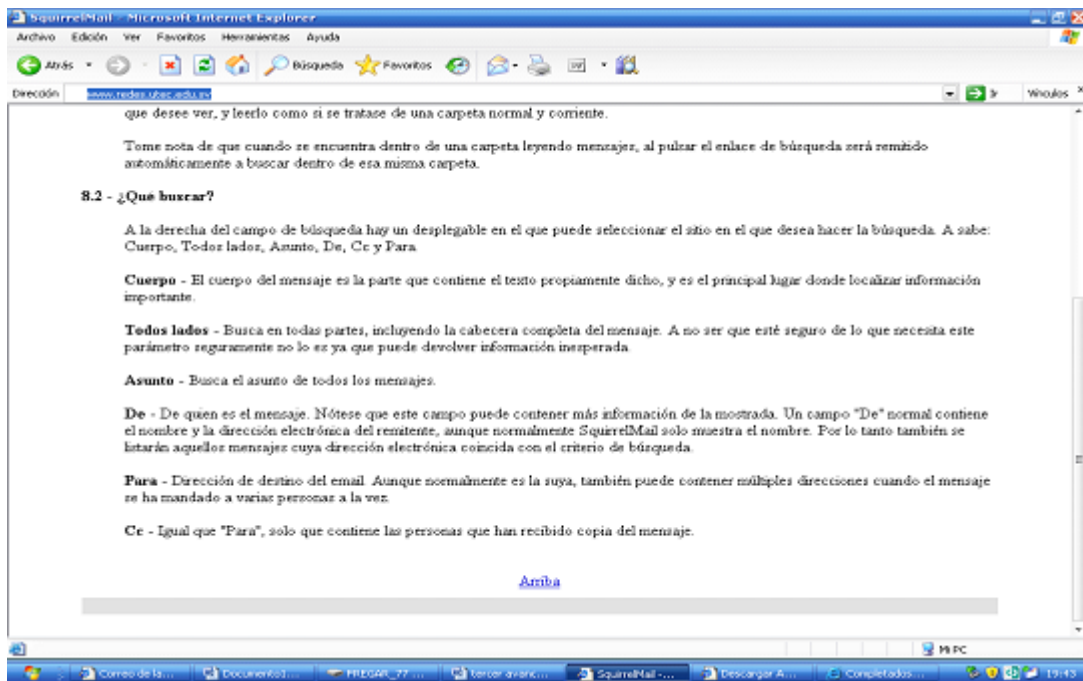


En esta pantalla se muestran las opciones para poder personalizar nuestro correo.

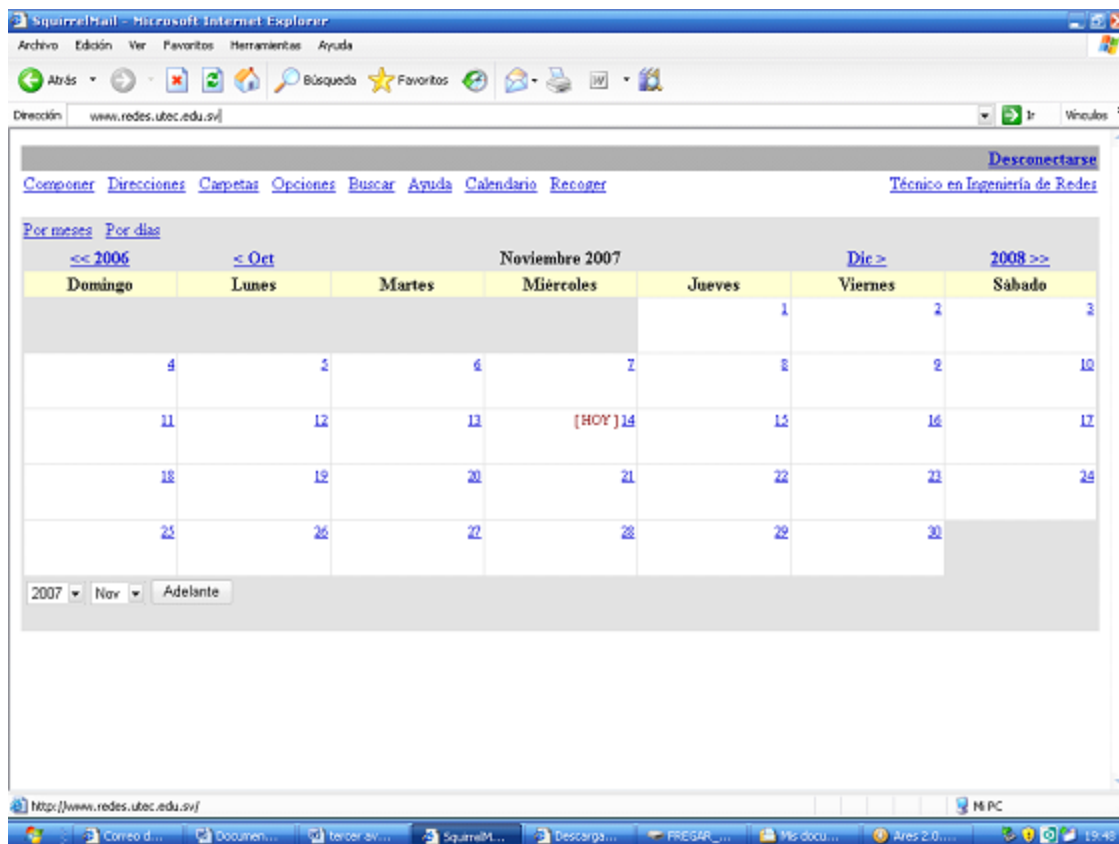


Esta pantalla muestra la Bandeja de Entrada que es donde llegan los correos electrónicos que se reciben.

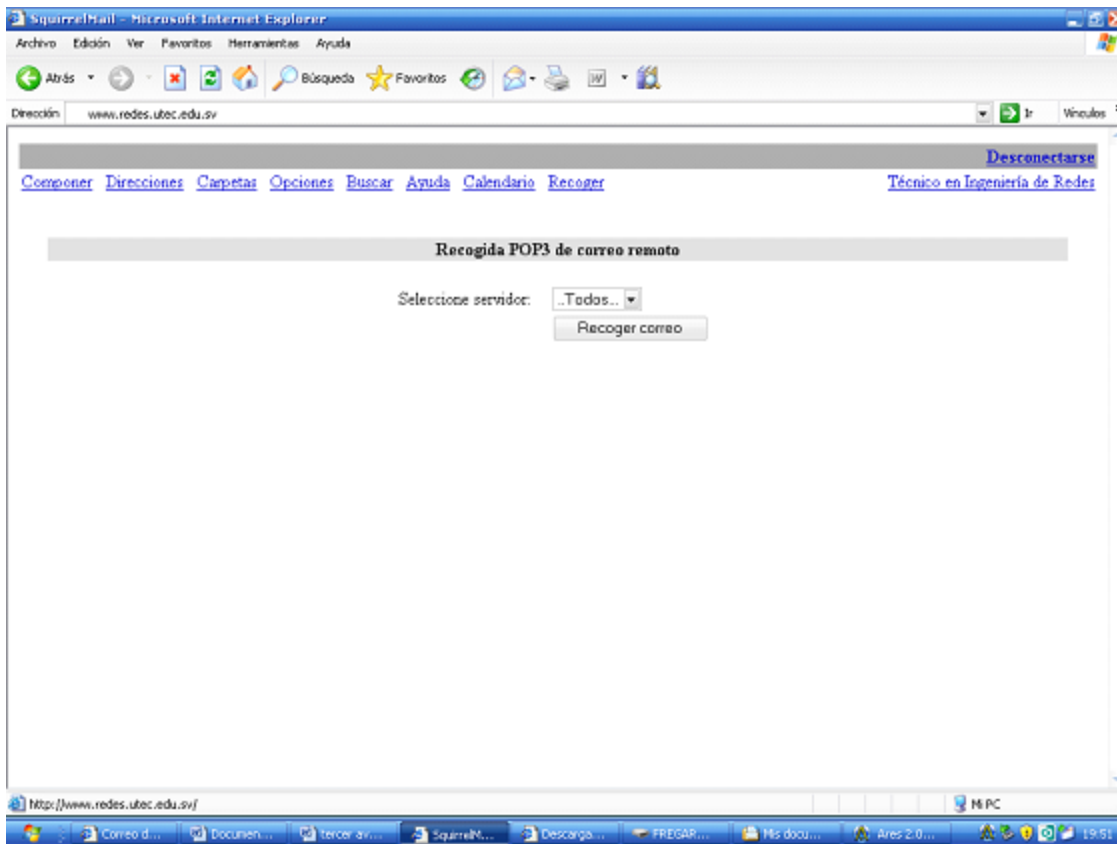




En estas pantallas se muestran las opciones de Ayuda con las que cuenta el correo electrónico.



En esta pantalla se muestra el calendario con el que cuenta el correo electrónico.



En esta pantalla se muestra donde se recogen los correos electrónicos que están por llegar.

CONCLUSIONES

- La Universidad Tecnológica de El Salvador (UTEC), contará con el contenido o la información para la implementación y configuración de servidores de correo electrónico seguros, con filtros antispam y antivirus, desarrollados en distribuciones de GNU/Linux, las cuales podrán ser

utilizada en las asignaturas afines de la carrera del Técnico en Ingeniería de Redes Computacionales

- Los alumnos de la carrera del Técnico en Ingeniería de Redes Computacionales contarán con un prototipo de servidor de correo electrónico, en el cual realizarán pruebas de implementación y configuración de dicho correo, a través de los manuales y guías.
- Los alumnos del Técnico en Ingeniería en Redes Computacionales saldrán con más oportunidades de venderse al mundo laboral, ya que en nuestro país contamos con poco personal humano con conocimientos en Software Abierto conocido como Open Source y GNU/Linux.

RECOMENDACIONES

- Se recomienda siempre estar revisando la capacidad del disco duro de la maquina donde este instalado el prototipo del Servidor de Correo Electrónico Seguro, con filtros AntiSpam y Antivirus, a manera de evitar lentitud en el envío/recepción de correos.
- Chequear periódicamente la memoria física de la PC donde este instalado el Servidor de Correo Electrónico a fin de lograr que los procesos que se estén ejecutando sean óptimos.
- Actualizar periódicamente las listas de actualizaciones de AntiSpam, para así evitar saturar la bandeja de entrada y por ende el servidor de correo electrónico.
- Actualizar a diario la lista de amenazas de virus a fin de evitar contraer alguna especie de virus que pueda llegar a afectar el sistema.
- No saturar de cuentas de usuarios el Servidor de Correo Electrónico y así de esta manera evitar lentitud en el tráfico de este.
- Darle el uso adecuado y necesario al Servidor de Correo Electrónico para poder así obtener el mayor beneficio y comodidad que este nos brinda.

BIBLIOGRAFIA

- LINUXRSP RUSIA, FIODOR SOREX, *Tabla de equivalencias y comparaciones entre Linux y Windows* [en línea] [Valery V. Kachurov](#), [Nesov Artem](#), [Consulta: 13 de Septiembre 2007]
Traducción al español [Carlos M. Cárdenas F.](#)
<<http://www.linuxrsp.ru/win-lin-soft/index-spanish.html>>
- LINUXSILO.NET, JAUME SABATER, *Configuración completa de un servidor de correo seguro con Postfix y Cyrus* [en línea] [Consulta: 13 de Septiembre 2007] Jaume Sabater
<<http://www.linuxsilo.net/articles/postfix.html>>
- UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO (UNAM), DSC/UNAM-CERT, *Instalación de un servidor de correo con Postfix Amavis y Spamassassin, Seguridad en el Departamento de Computo* [en línea] [Consulta: 15 de Septiembre 2007]
<<http://www.seguridad.unam.mx/doc/?ap=tutorial&id=182>>
- SYNETGY ORG, JESÚS M. GONZÁLEZ BARAHONA, *Que es el Software Libre* [en línea] [Consulta: 15 de Septiembre 2007] <
<http://sinetgy.org/~jgb/articulos/soft-libre-que-es/>>
- SERVITUX, PACO BRUFAL, *Instalación y configuración de Postfix en Debian, Guía Rápida de configuración* [en línea] [Consulta: 18 de Septiembre 2007]
< <http://www.servitux.org/view.php/page/postfix/>>

ANEXOS

ANEXO #1.

Instalación de Postfix, Amavis y Spamassasin

- [Servidor de correo](#)
- o [Introducción](#)
- o [Postfix](#)
- [Arquitectura](#)
- o [Instalación](#)
- o [Configuración](#)
- [Filtrando Spam desde Postfix](#)
- o [Detección de Spam](#)
- [Detección basada en información del origen](#)
- [Detección basada en contenido](#)
- o [Configuración Anti-Spam de Postfix](#)
- [Reglas restrictivas contra el Spam](#)
- [Parámetros de verificación de sintaxis](#)

- [Verificación de contenido](#)

- [Instalación de Amavis-new sobre Postfix](#)

- o [Instalación](#)

- o [Integrando Amavis a Postfix](#)

- o [Configuración de Amavis-new](#)

- [Sección I: Configuración del demonio y del MTA](#)

- [Sección II: Valores específicos para el MTA](#)

- [Sección III: Bitácora](#)

- [Sección IV: Notificaciones, destino, cuarentena](#)

- [Sección V: Administración por recipiente u origen](#)

- [Uso de recursos](#)

- [Programas externos, analizadores de virus](#)

- [Configuración de Spamassasin \(amavis.conf\)](#)

Servidor de correo

Introducción

El término Spam se define como el "Correo electrónico no deseado" que llega o que ha llegado a nuestra cuenta de correo electrónico. Este correo el cual el usuario nunca solicitó que se le enviara, y no tiene alguna relación ni motivo por el cual deba recibirlo, generalmente es con fines comerciales aunque pueden existir otros motivos los cuales orillen a los denominados spammers a enviarlo, como puede ser la propagación de un virus, ataques de denegación de servicio etc. El Spam se caracteriza por ser enviado a miles o millones de usuarios de la red, sin embargo aún cuando el correo no deseado es enviado a un sólo usuario, será Spam.

Existen servicios en la red, como subastas, listas de correo, grupos de usuarios, etc. Los cuales suelen enviar avisos sobre novedades en su servicio. Si el usuario pertenece o tiene alguna cuenta en sus servidores, es muy probable que reciba algún correo de este tipo. Para prestar un servicio eficiente de correo, tenemos que lidiar con este problema, y que mejor que contar con herramientas que nos ayuden a limitar la cantidad de Spam recibido en nuestro servidor de correo.

Este documento, tiene como finalidad explicar la implementación de un servidor de correo Postfix, en conjunto con el filtro Anti-Spam Amavis-New para limitar la cantidad de correo no deseado en el mismo. Las pruebas y configuraciones aquí mostradas, fueron realizadas en un sistema Linux *Gentoo 2004.1* con un kernel 2.4.25.

Postfix

Llamado anteriormente IBM Secure Mailer, Postfix fue desarrollado en los laboratorios de IBM y declarado como *open source* en Diciembre de 1998 por Wietse Zwart Venema, quien es reconocido en el mundo de la seguridad en cómputo, por sus trabajos basados en la protección de intrusiones en los sistemas informáticos. Desde entonces,

existía una alternativa al ya tan nombrado Sendmail, la cual prometía rapidez, facilidad de configuración y sobre todo, lo heredado por su creador, seguridad.

Arquitectura

La arquitectura de Postfix es muy diferente a un sistema monolítico como Sendmail, el cual tradicionalmente utiliza un simple programa muy grande para manipular los mensajes de correo. Postfix delega su funcionamiento en pequeños módulos que realizan una tarea específica. La mayoría de ellos son demonios, los cuales son procesos que corren en *background* en nuestro sistema. Uno de esos demonios es *Máster*, el cual es el que inicia primero, he invoca a los demás procesos conforme son necesarios, muy al estilo *Init* en Linux. El demonio Master, obtiene las opciones de configuración de dos archivos: *main.cf* y *master.cf* al iniciarse.

En pocas palabras, el funcionamiento de Postfix es el siguiente: recibe los mensajes, los encola y finalmente los entrega. Cada una estas etapas, es realizada por componentes diferentes de Postfix, lo que permite una configuración por separado, en cada una de ellas. Después de que el mensaje es recibido y encolado, el administrador de la cola de mensajes invoca al agente de entrega adecuado para la fase final. Los mensajes llegan al servidor con Postfix de la siguiente manera:

- Un mensaje puede ser aceptado por Postfix localmente, es decir, aquel que ha sido enviado por un usuario en la máquina local.
- Un mensaje puede ser aceptado por Postfix desde la red.
- Un mensaje que ya ha sido aceptado por Postfix a través de los métodos ya mencionados y es preparado para su reenvío a otra dirección.
- Un mensaje puede ser generado por el mismo Postfix, cuando sea necesario entregar una notificación.

Como se mencionó antes, varios son los componentes que trabajan en conjunto con la cola de mensajes. El administrador de cola es el encargado de administrar la cola de mensajes y alertar a un componente cuando tiene tarea por hacer. El camino que sigue un mensaje local al entrar a Postfix es el siguiente: los mensajes locales son depositados en el directorio *maildrop* de la cola de Postfix por el comando *postdrop*. El demonio *pickup* lee el mensaje de la cola y lo pasa al demonio *cleanup*. Algunos mensajes llegan sin información necesaria para un mensaje válido, de manera que además de una revisión del mensaje, el demonio *cleanup* en conjunto con el demonio *trivial-rewrite*, insertan las cabeceras faltantes, convierten las direcciones al formato *userdomain.tld* esperado por los programas de Postfix, y posiblemente transforma direcciones basadas en tablas canónicas o virtuales.

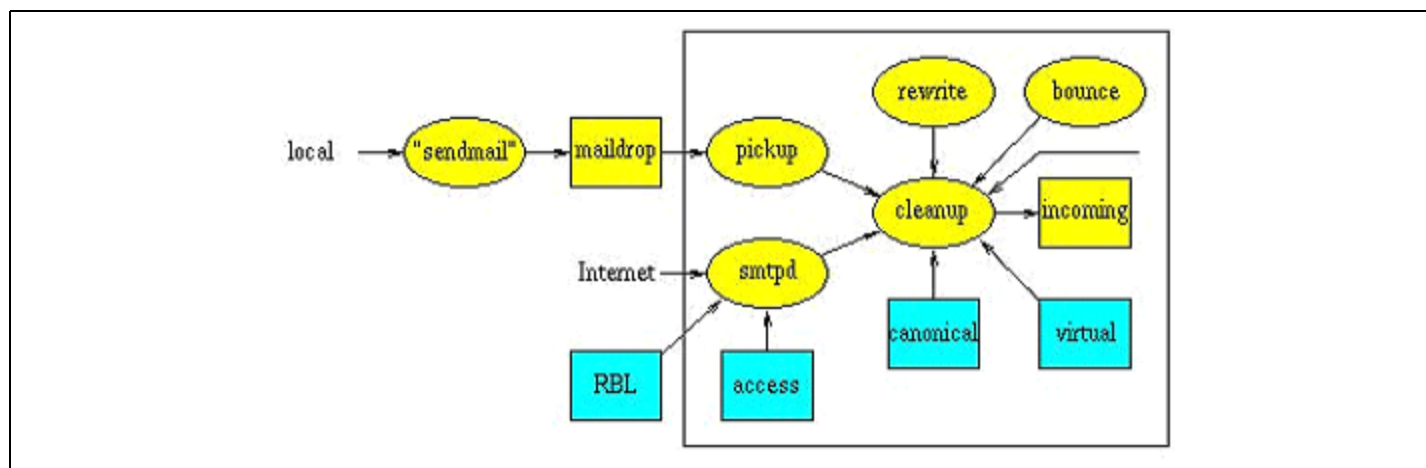


Figura 1.1: Diagrama de flujo Postfix

Después de este proceso, el demonio cleanup notifica al administrador de la cola que el mensaje ha sido procesado. Después se procede a la invocación del agente de entrega para hacerlo llegar a su destino final. Este proceso se mantiene casi intacto en el análisis que realizaremos posteriormente, sólo se agregará a la parte en la que actúa Amavis-New en el análisis y clasificación del mensaje.

Instalación

Antes de iniciar la instalación del servidor de correo Postfix, instalaremos algunos de los módulos que nos podrían ser útiles en la tarea Anti-Spam que estamos emprendiendo. Uno de estos módulos es el *Perl Compatible Regular Expressions* PCRE; este se compone de una serie de librerías que implementan el reconocimiento de patrones utilizando expresiones regulares, y la sintaxis y semántica de Perl 5, actualmente ha sido utilizado en proyectos de software libre como: Apache, PHP, KDE y por supuesto Postfix.

Para la instalación de PCRE, obtendremos la última versión del sitio <http://www.pcre.org>. Y para su instalación se ejecutarán los siguientes comandos:

```
# tar -zxvf pcre-4.5.tar.gz
# cd pcre-4.5
# ./configure
# make
# make install
```

Después de esto, continuamos con la instalación de Postfix. En esta sección, se instalará la versión 2.1.0 de Postfix, desde el código fuente. Para obtener esta versión sólo hay que dirigirse a la página <http://www.postfix.org/download.html> y descargarla.

Ahora que tenemos el código fuente de Postfix, vamos a instalarlo con los siguientes comandos:

```
# mv postfix-2.1.0.tar.gz /usr/local/src
# cd /usr/local/src
# tar -zxvf postfix-2.1.0.tar.gz
```

ya hemos desempquetado el código, resta compilarlo, sólo que hay que hacerlo con soporte para el PCRE:

```
# cd postfix-2.1.0
#make -f Makefile.init makefiles 1#1
"CCARGS=-DHAS_PCRE -I/usr/local/include" 1#1
"AUXLIBS=-L/usr/local/lib lpcre"
# make
# make install
```

Ahora necesitamos crear una cuenta de usuario y un grupo, esto sólo es necesario en la primera instalación de este servidor de correo. Crearemos el usuario *Postfix* con un userid y un groupid que no esté siendo utilizado por otro usuario, esta debe de ser una cuenta en la que nadie pueda obtener un shell y necesita un home directory inexistente, nuestras líneas en */etc/passwd* y */etc/group* lucen de la siguiente manera:

```
postfix:x:207:207:Postfix:/var/spool/postfix:/bin/false
postfix:x:207:
```

También necesitamos un grupo llamada *postdrop* con un groupid que no sea utilizado por ningún otro grupo.

Configuración

La configuración de Postfix se realiza por medio de 2 archivos principalmente, `main.cf` y `master.cf`, los cuales se encuentran por default en `/etc/postfix`. A continuación describiremos las opciones de configuración mas importantes utilizadas en este documento, tanto para el `main.cf` como para el `master.cf` respectivamente.

La primera opción que configuraremos en nuestro servidor es la ruta de la cola de mensajes de Postfix. Generalmente cuando Postfix se ejecuta en un ambiente *chroot* esta suele ser la raíz de Postfix.

```
queue_directory = /var/spool/postfix
```

La ruta de todos los comandos de Postfix y los demonios (algunos de los cuales están listados en `main.cf`) están dadas por las siguientes líneas:

```
command_directory = /usr/sbin
```

```
daemon_directory = /usr/libexec/postfix
```

Cabe resaltar que la ruta que especifica la localización de los demonios, debe pertenecer a root. Un parámetro importante es el propietario de la cola de mensajes y de la mayoría de los demonios de Postfix:

```
mail_owner = postfix
```

Ahora debemos especificar el nombre del host, así como el nombre del dominio al que pertenece, en este caso tenemos:

```
myhostname = forense.seguridad.unam.mx
```

```
mydomain = seguridad.unam.mx
```

Estos parámetros son muy importantes así que comentaremos mas sobre ellos. Si el parámetro *myhostname* no se especifica Postfix utilizará la función *gethostname* para determinar el nombre del host. Si el sistema reporta correctamente el nombre del sistema, este parámetro se puede pasar por alto. Si el parámetro *mydomain* es especificado, Postfix genera el nombre completo del host en conjunto con el nombre del dominio.

Cuando los usuarios envían o reciben correo a través de Postfix sin ningún dominio especificado, el parámetro *myorigin* especifica el dominio a concatenar a las cabeceras del mensaje. El valor por default es el siguiente:

```
myorigin = $myhostname
```

También tenemos que indicarle a Postfix, por qué medio va a recibir mensajes, en este caso nos referimos a las interfaces activas del sistema con el parámetro:

```
inet_interfaces = all
```

El siguiente parámetro a configurar, es *mydestination*, este lista todos los dominios de los cuales Postfix va a aceptar la entrega o el envío de los usuarios locales, nuestra configuración es la siguiente:

```
mydestination = $myhostname, localhost.$mydomain, localhost
```

Además de recibir y enviar mensajes de usuarios locales, Postfix también puede reenviar correo a otros sistemas. Es muy importante restringir quien puede reenviar correo a través de nuestro sistema. Los sistemas en nuestra red deben

de tener la posibilidad de reenviar correo, sin embargo no se necesita el mismo servicio a todo el mundo. Por default Postfix no es un *OpenRelay*, los parámetros *mynetworks_style* y *mynetworks* determinan si otros sistemas pueden usar el nuestro para enviar correo. La configuración por default es permitir sólo aquellos equipos que estén conectados a la misma red que nuestro servidor. Nosotros hemos elegido limitar el *mail relay* sólo a la máquina local, con la siguiente opción:

```
mynetworks_style = host
```

Una de las líneas que agregaremos a nuestro archivo *main.cf*, es la que indica la existencia de Amavis-New, la cual es la siguiente:

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

Esto indica que Amavis-New trabajará sobre el puerto 10024 en la máquina local, que como explicaremos mas adelante, Postfix se encargará de enviar los mensajes a Amavis para su validación como Spam, y Amavis lo regresará a Postfix para su entrega final si es el caso. Además, le indicamos a Postfix en dónde se encuentra la tabla de aliases a utilizar:

```
Alias_database = hash:/etc/postfix/aliases
```

La última línea, indica algunas restricciones propias de Postfix que nos ayudarán a detener el Spam antes de pase a otra etapa dentro del proceso de los mensajes en el sistema, estas opciones las discutiremos mas adelante:

```
smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname, reject_maps_rbl
```

Hasta ahora nuestro archivo de configuración *main.cf* luce de la siguiente manera:

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
mail_owner = postfix
myhostname = forense.seguridad.unam.mx
mydomain = seguridad.unam.mx
myorigin = $myhostname
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 500
mynetworks_style = host
relay_domains =
relayhost =
mail_spool_directory = /var/spool/mail
mailbox_command = /usr/bin/procmail
debug_peer_level = 2
debugger_command =
PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq
setgid_group = postdrop
html_directory = no
```

```
manpage_directory = /usr/local/man
sample_directory = /etc/postfix
readme_directory = no
content_filter = smtp-amavis:[127.0.0.1]:10024
ALias_database = hash:/etc/postfix/aliases
smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname, reject_maps_rbl
```

Filtrando Spam desde Postfix

La operación de un servidor de correo sobre Internet, implica la responsabilidad de no permitir el open relay, con el cual los Spammers puedan utilizar nuestros recursos para realizar sus operaciones. Un servidor de open relay es un sistema de correo que permite el envío de mensajes de sistemas externos a otros sistemas externos por medio de nuestro servidor.

Detección de Spam

Después de resguardar nuestro servidor, lo próximo a realizar es reducir la cantidad de Spam recibido por nuestros usuarios. Debemos elegir un método eficiente que permita eliminar el correo Spam. Sin embargo la existencia de falsos positivos hará difícil nuestra decisión, debido a que la mala clasificación del correo deseado por nuestros usuarios, es un problema común en la clasificación de correo Spam.

Existen dos métodos principales para la detección de Spam: la identificación del origen del Spam y mediante el análisis del contenido del mensaje en busca de frases que revelen características clásicas o no del Spam.

Detección basada en información del origen

Utilizando información como direcciones IP, nombres de host así como direcciones de correo suministradas por los clientes cuando ellos envían algún mensaje, esta técnica compara estas piezas de información con datos conocidos sobre sistemas utilizados para el envío de Spam. Sin embargo la utilización de recursos ajenos a los Spammers para el envío de Spam, como puede ser la utilización de Open Relays, puede retrasar el proceso de investigación del verdadero origen del correo basura. Además, que toda la información obtenida mediante los encabezados de algún mensaje, puede ser generalmente, fácilmente alterada por los Spammers.

Listas negras de DNS

En un esfuerzo por detener el Spam, han sido desarrollados varios servicios Anti-Spam generalmente denominados *listas negras basadas en DNS* o *listas negras en tiempo real*. Estos servicios mantienen bases de datos en las cuales se encuentran registrados host que son conocidos como open relays, o que han sido utilizados para el envío de Spam. Algunos de los ataques más comunes en contra de estos equipos, es la instalación de un proxy propio del spammer el cual no solo podría ser utilizado para enviar Spam, si no también para generar ataques de denegación de servicio.

Detección basada en contenido

Además de identificar clientes que permiten el envío de Spam desde sus equipos, también se puede detectar Spam por medio de su contenido. Ciertas cadenas de texto marcan significativamente el nivel de posibilidad de que un correo sea Spam o no, por ejemplo *"Make more Money"*. Sin embargo este tipo de análisis puede llegar a ser muy problemático, debido a los falsos positivos que puede generar una mala clasificación del Spam.

Configuración Anti-Spam de Postfix

Existen 4 diferentes formas de detección de Spam en Postfix:

Reglas de detección de clientes Spam:

Reglas que trabajan con la identidad del cliente. Cada regla es una lista asignada de una o mas restricciones que pueden aceptar o rechazar un mensaje. Por ejemplo, podemos incluir una regla que rechace mensajes de una dirección IP en particular.

Parámetros de verificación de sintaxis:

Son parámetros que verifican el apego a los estándares actuales en la composición del mensaje. Debido a que varios Spammers no siguen al pie de la letra los estándares que rigen el correo electrónico, nuestro sistema puede estar configurado para rechazar mensajes que vienen de sistemas mal o pobremente configurados.

Verificación de contenido:

Se puede realizar una verificación de las cabeceras y del cuerpo del mensaje por medio de expresiones regulares, las cuales nos indicarán un mensaje que probablemente sea Spam.

Clases de restricción:

Se pueden definir reglas complejas para la detección de clientes Spam por medio de clases de restricción. Estas permiten combinar restricciones en grupos para formar nuevas restricciones.

Cuando se configura Postfix con características Anti-Spam, también se puede especificar qué hacer con los mensajes clasificados como Spam. En general, Postfix puede rechazar los mensajes, separarlos en una cola diferente, o entregarlos a un filtro externo.

Reglas restrictivas contra el Spam

Postfix proporciona las siguientes reglas de restricción basadas en la información del cliente:

- smtpd_client_restrictions
- smtpd_helo_restrictions
- smtpd_sender_restrictions
- smtpd_recipient_restrictions
- smtpd_data_restrictions

Cada una corresponde a una etapa en una transacción por medio del protocolo SMTP. En cada etapa, el cliente proporciona piezas de información. Utilizando la información proporcionada por el cliente, Postfix aplica las restricciones que se le hallan configurado. En la siguiente imagen se muestra una conversación SMTP, podemos ver en que etapa encaja cada regla. Podemos ver que las reglas que mencionamos anteriormente las cuales nos permiten verificar las cabeceras y el cuerpo del mensaje, también se ilustran en estos pasos, estas reglas se discutirán posteriormente.

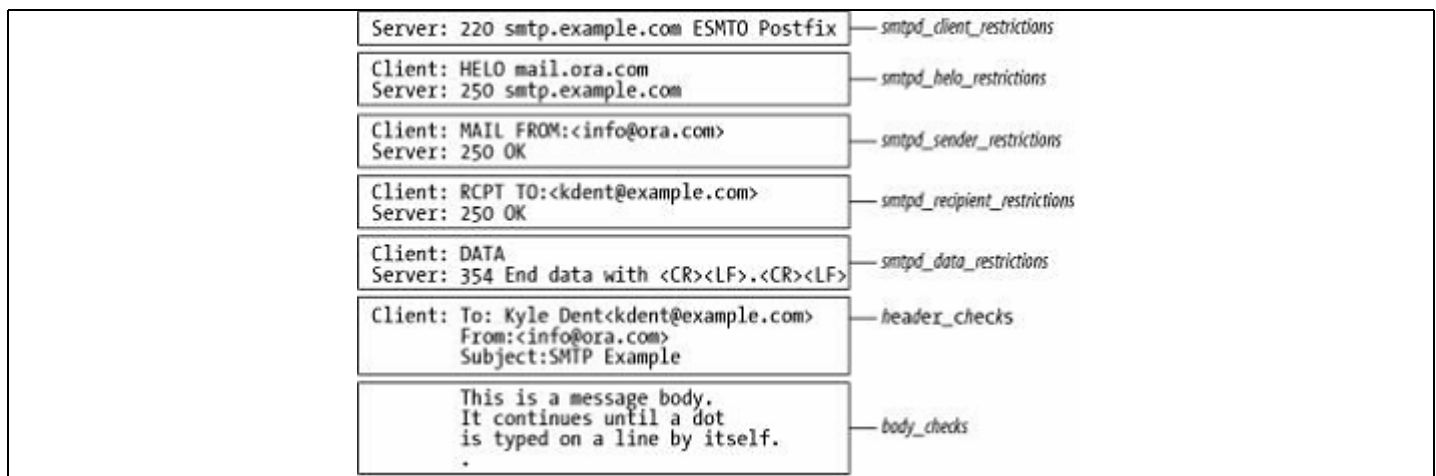


Figura 2.1: Comunicación por medio de SMTP

Como podemos ver en la imagen, el cliente tiene que realizar ciertas tareas antes de que su mensaje sea entregado. Primero tiene que conectarse por medio de un socket al servidor, con esto Postfix puede aceptar o rechazar mensajes de una dirección IP en específico, aunque en la imagen esta no aparece, Postfix conoce la dirección IP de cualquier cliente que se conecta. Después el cliente tiene que ejecutar una llamada al comando HELO, con el cual identifica al equipo en el que se encuentra, con esto Postfix puede bloquear correo por medio del nombre del equipo o del dominio del mismo. Si el mensaje llega a pasar hasta la etapa de DATA, se puede considerar que ha pasado la primera revisión Anti-Spam de Postfix, ahora se realizará una revisión de las cabeceras del mensaje así como del cuerpo del mismo.

Por default, la configuración de reglas de restricción en Postfix (si no se especificaron algunas en main.cf) son:

```
smtpd_client_restrictions =
smtpd_helo_restrictions =
smtpd_sender_restrictions =
smtpd_recipient_restrictions =
permit_mynetworks, reject_unauth_destination
```

Esta configuración permite el relaying, sólo a aquellos equipos dentro de la red del servidor de correo, y rechazando todos los demás excepto aquellos equipos que envíen mensajes a uno de nuestros usuarios.

Una de estas reglas, las definimos en el main.cf, y fue la última línea de nuestro archivo:

```
smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname, reject_maps_rbl
```

El parámetro *permit_mynetworks* hará que la petición se realice cuando la dirección IP del cliente, se encuentra dentro del parámetro *mynetworks*, el segundo parámetro *reject_invalid_hostname*, rechazará la petición cuando el nombre del equipo indicado en el comando HELO es inválido. El último parámetro *reject_maps_rbl*, rechazará la petición cuando la dirección del cliente se encuentra listado en algún servidor de RBLs listado en el parámetro *maps_rbl_domains*, sin embargo la búsqueda inversa sobre un servidor de RBLs es una propiedad que hemos dejado desactivada.

Parámetros de verificación de sintaxis

Existen dos parámetros que requieren de un estricto apego a los estándares del correo electrónico. Declarando la regla:

`smtpd_helo_required = yes`

Implica que cada cliente tendrá que iniciar la conversación SMTP con el comando HELO/EHLO, descrito en el RFC 821 del SMTP. Así, cualquier cliente que no inicie apropiadamente el envío del mensaje, sera rechazado por Postfix. Existe otro parámetro en el RFC 821, el cual dice que las direcciones deben de seguir un formato predeterminado, generalmente Postfix acepta direcciones que se asemejen al formato predeterminado, sin embargo si se especifica la regla:

`strict_rfc821_envelopes = yes`

Postfix rechazara cualquier intento de envío de un mensaje con una dirección con un formato incorrecto.

Verificación de contenido

La verificación de contenido es la última etapa en la que Postfix puede tomar una decisión sobre el destino del mensaje. Postfix ofrece 4 parámetros que nos permiten especificar el tipo de análisis a realizar:

header_checks:

Análisis de las cabeceras del mensaje.

mime_header_checks:

Análisis de las cabeceras MIME del mensaje.

nested_header_checks:

Análisis de las cabeceras de los datos adjuntos al mensaje.

body_checks:

Análisis del cuerpo del mensaje.

Cuando se especifica un parámetro, se indica la tabla de búsqueda en la que están las expresiones regulares a utilizar en el análisis del mensaje:

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

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

Un archivo ejemplo, el cual contenga expresiones regulares para evaluar las cabeceras del mensaje podría ser:

`/Make Money/ REJECT`

`/VIAGRA/ REJECT`

`/Marketing/ REJECT`

También se puede utilizar este tipo de verificación, para analizar los archivos adjuntos en el mensaje, por ejemplo, aquellos mensajes con ejecutables sospechosos, pueden ser evitados con la entrada:

`/name ?="?.*1#1.(bat|com|dll|exe|hta|pif|vbs)"?/ REJECT`

Instalación de Amavis-new sobre Postfix

Ya que hemos configurado nuestro servidor postfix y le hemos echado a andar, instalaremos el filtro Anti-Spam amavis-new, pero antes de eso necesitamos algunas configuraciones adicionales a nuestro servidor, las cuales se explican mas adelante en esta sección.

La versión utilizada en esta ocasión fue *amavisd-new-20030616-p9*, la cual puede ser descargada desde el sitio <http://www.ijs.si/software/amavisd/>. Existen diferentes versiones de *amavis*, la cuales se describen a continuación:

Amavis:

Es un scanner de virus de correo electrónico, realizado en Perl, incluye algunas características sobre el rendimiento del mismo. Para su configuración, se debe de estar familiarizado con Perl y la configuración del MTA que se este utilizando.

Amavisd:

Es la version en demonio de amavis, y su integración con el MTA puede ser diferente a la version original.

Amavisd-new:

Es una interfaz entre el MTA y algún verificador de contenido como scanners de virus y/o SpamAssassin, el cual nos ayuda a identificar el posible spam que recibe nuestro servidor.

Amavis-ng:

Es una versión script de amavis, la cual requiere de ciertos módulos de Perl instalados, además de algunas herramientas en el sistema, funciona como interfaz entre un MTA y un verificador de contenido.

Antes de iniciar con la instalación de amavis-new, existen algunos programas y módulos que son requisito para poder continuar con la instalación:

- Herramienta file
- Herramienta gzip
- Herramienta bzip2
- Herramienta compress
- Herramienta cpio
- Modulo Archive::Tar
- Modulo Archive::Zip
- Modulo Compress::Zlib
- Modulo Convert::TNEF
- Modulo Convert::UUlib
- Modulo MIME::Base64
- Modulo MIME::Parser
- Modulo Mail::Internet
- Modulo Net::Server
- Modulo Net::SMTP
- Modulo Digest::MD5
- Modulo IO::Stringy
- Modulo Time::HiRes
- Modulo Unix::Syslog

Todos estos módulos pueden ser descargados de la página del CPAN *Comprehensive Perl Archive Network*, y la instalación requiere de los siguientes comandos:

```
# tar -zxvf MODULO.tgz
# cd moduloDir
# perl Makefile.PL
# make
# make test
# make install
```

Las capacidades de filtrado de contenido, dependerá en parte, a la existencia o no de herramientas de este tipo. Los módulos pueden llegar a ser obligatorios para el funcionamiento de amavis.

Instalación

Para la instalación de amavis necesitamos la version 5.8.2 o superior de Perl, además de la creacion de un grupo dedicado al demonio de amavis. Este grupo no debe ser compartido ni con los usuarios ni con el MTA, su nombre bien podría ser *amavis*.

Además necesitamos una cuenta de usuario dedicada a la ejecución del demonio de amavis, no debe de ser una cuenta regular del sistema, y de igual manera no debe de ser compartida con el MTA, el nombre de este usuario podrá ser *amavis* por ejemplo. Debemos de escoger un directorio home para este usuario, que en este ejemplo se ha decidido por */var/amavis*. La creacion del directorio home del usuario amavis y de los permisos podrán realizarse con los siguientes comandos:

```
# mkdir /var/amavis
# chown amavis:amavis /var/amavis
# chmod 750 /var/amavis
```

Descomprimos el paquete de amavis-new en la ruta que se desee, por ejemplo */usr/local/src* y nos cambiamos a ese directorio. Copiamos el archivo *amavisd* a donde se desee que resida, por ejemplo */usr/local/sbin*, y nos aseguramos de que sus permisos nos permitan ejecutarlo pero no borrarlo por usuarios no autorizados:

```
# cp amavisd /usr/local/sbin
# chown root /usr/local/sbin/amavisd
# chmod 755 /usr/local/sbin/amavisd
```

Copiamos el archivo *amavis.conf* a donde deseemos que resida, por ejemplo */etc*, y le asignamos los permisos para impedir la escritura por parte de usuarios no autorizados:

```
# cp amavisd.conf /etc/
# chown root /etc/amavisd.conf
# chmod 644 /etc/amavisd.conf
```

Creamos un directorio llamado */var/viruspam/* el cual sera utilizado por amavis-new como area de cuarentena, solo si esta es deseada ya sea para virus o para posible Spam:

```
# mkdir /var/viruspam
# chown amavis:amavis /var/viruspam
# chmod 750 /var/viruspam
```

Ahora podemos instalar los módulos como SpamAssassin, el cual nos permitirá realizar un análisis en los mensajes que llegan a nuestro servidor, para poder clasificarlos como Spam o no.

Integrando amavis a Postfix

Ahora si tenemos que editar nuestro archivo *master.cf*, y agregar las siguientes líneas al final del archivo:

```
smtp-amavis unix - - y/n - 2 smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes

127.0.0.1:10025 inet n - y/n - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
```

Las opciones *y/n* se deben de cambiar dependiendo si se desea que smtp y postfix trabajen en un ambiente chroot o no. Para las opciones aquí listadas, bastara con colocar la misma opción que las opciones ya existentes en ese archivo. Para cargar la configuración de Postfix al vuelo, ejecutamos el siguiente comando:

```
# postfix reload
```

y verificamos si realmente esta funcionando postfix, ahora sobre el puerto 10025 (Esto no significa que deje de funcionar por el 25):

```
$ telnet 127.0.0.1 10025
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 forense.seguridad.unam.mx ESMTP Postfix
quit
221 Bye
Connection closed by foreign host.
```

Como vimos en [1.4](#), tenemos que indicarle a Postfix que reenvie todo el correo que recibe a amavis-new, (como lo muestra [3.1](#)) para una inspección basada en contenido, esto es con la siguiente linea en el archivo *main.cf*:

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

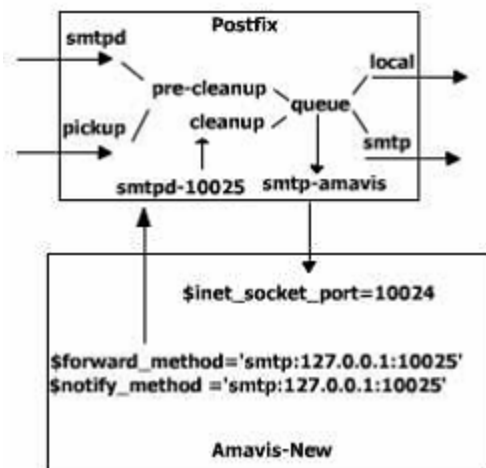


Figura 3.1: Diagrama de flujo Postfix-Amavis

también podemos usar un comando en el shell para agregar esta línea:

Servidor de correo

Introducción

El término Spam se define como el "Correo electrónico no deseado" que llega o que ha llegado a nuestra cuenta de correo electrónico. Este correo el cual el usuario nunca solicitó que se le enviara, y no tiene alguna relación ni motivo por el cual deba recibirlo, generalmente es con fines comerciales aunque pueden existir otros motivos los cuales orillen a los denominados spammers a enviarlo, como puede ser la propagación de un virus, ataques de denegación de servicio etc. El Spam se caracteriza por ser enviado a miles o millones de usuarios de la red, sin embargo aún cuando el correo no deseado es enviado a un sólo usuario, será Spam.

Existen servicios en la red, como subastas, listas de correo, grupos de usuarios, etc. Los cuales suelen enviar avisos sobre novedades en su servicio. Si el usuario pertenece o tiene alguna cuenta en sus servidores, es muy probable que reciba algún correo de este tipo. Para prestar un servicio eficiente de correo, tenemos que lidiar con este problema, y que mejor que contar con herramientas que nos ayuden a limitar la cantidad de Spam recibido en nuestro servidor de correo.

Este documento, tiene como finalidad explicar la implementación de un servidor de correo Postfix, en conjunto con el filtro Anti-Spam Amavis-New para limitar la cantidad de correo no deseado en el mismo. Las pruebas y configuraciones aquí mostradas, fueron realizadas en un sistema Linux *Gentoo 2004.1* con un kernel 2.4.25.

Postfix

Llamado anteriormente IBM Secure Mailer, Postfix fue desarrollado en los laboratorios de IBM y declarado como *open source* en Diciembre de 1998 por Wietse Zweitze Venema, quien es reconocido en el mundo de la seguridad en cómputo, por sus trabajos basados en la protección de intrusiones en los sistemas informáticos.

Desde entonces, existía una alternativa al ya tan nombrado Sendmail, la cual prometía rapidez, facilidad de configuración y sobre todo, lo heredado por su creador, seguridad.

Copyright® Todos los derechos reservados, cert.org.mx y cert.net.mx

DSC/UNAM-CERT DGSCA

[Aviso Legal](#)

[Créditos](#)

MD5: 51 00 27 60 B9 87 B3 7E EE 80 1E A7 B2 DC E7 A8

SHA1: 86 54 33 9B EA 63 85 67 1E 1D 55 49 BA 0F D1 16 11 A2 5B 37

ANEXO #2

Gigantes informáticos respaldan el software libre

EMAIL

domingo, 19 de noviembre de 2006

Oracle, con el respaldo de HP, Dell, Intel y AMD, anunció su apoyo a Linux y el software libre en general mediante su estrategia Unbreakable Linux.

En San Francisco (California, E.U.) se dio el espaldarazo. El llamado a apoyar las aplicaciones con tecnologías abiertas, como el sistema operativo Linux, lo hicieron varios gigantes de la informática. Hewlett-Packard, Dell, Intel y AMD, entre otras, respaldaron la presentación del programa Unbreakable Linux por parte de Oracle, una compañía líder de software empresarial.

El nuevo instrumento dará el soporte de esta empresa a las soluciones de estándares abiertos que brinda Linux y ofrecerá correcciones de virus a las anteriores, actuales y futuras versiones de este sistema operativo.

Linux está disponible gratis a empresas y usuarios, y constantemente es mejorado y modificado por desarrolladores de software, en una tendencia que se conoce como código abierto.

"Creemos que mejor soporte y mejores precios acelerarán la adopción de Linux", aseguró Larry Ellison, director ejecutivo de Oracle, durante el Oracle Open World 2006 que se realizó en el Moscone Center, y al que EL TIEMPO asistió por invitación de esta organización.

Las pymes también cuentan

De acuerdo con la firma de investigaciones IDC, las pequeñas y medianas empresas (pymes) en América Latina aumentarían sus inversiones en tecnología a 13.604 millones de dólares hacia el 2009. Una cifra que refleja por qué Oracle está interesada en este segmento. De hecho, hoy el 65 por ciento de los clientes de esta empresa en la región son pymes.

"Nosotros apoyamos a las pymes desde sus necesidades más básicas", resaltó Luiz Meisler, vicepresidente senior de Oracle para América Latina, quien además indicó que las pequeñas y medianas empresas necesitan contar con aplicaciones que les permitan incrementar su productividad y contar con la flexibilidad suficiente para adaptarse a las exigencias del mercado.

Anexo #3

¿Qué es el software libre?

Jesús M. González Barahona

Universidad Rey Juan Carlos

jgb@computer.org

Octubre 2002

©2002 Jesús M. González Barahona

Se otorga permiso para copiar y distribuir este documento completo en cualquier medio si se hace de forma literal y se mantiene esta nota

Publicado en el Monográfico Anual sobre Tecnologías de la Información/Internet, 2002, editado por Staff Empresarial.

Cada vez se habla más del software libre (a veces refiriéndose a él como "software de fuente abierta" o, en inglés, "open source software"). Probablemente el lector tenga claro que constituye una forma diferente y novedosa de entender

la producción y distribución de programas, con grandes consecuencias sobre los usuarios y los productores de software. Pero quizás tenga menos claro qué es exactamente... Esto es lo que vamos a tratar de aclarar en este pequeño artículo.

No hay una única definición de software libre, pero las aceptadas comúnmente son suficientemente parecidas como para que podamos definirlo, informalmente, mediante cuatro libertades que tiene quien lo recibe:

- Puede usarlo como mejor le parezca, para cualquier actividad, en cualquier momento, en cualquier ordenador, en cualquier lugar, con fines privados, comerciales o de cualquier otro tipo.
- Puede redistribuirlo (copiarlo) a quien quiera, cobrando por ello o no. Por ejemplo, puede colocarlo en un servidor de Internet para su descarga gratuita, o puede imprimir CDs con él y venderlos en kioscos.
- Puede modificarlo, adaptándolo a sus necesidades, personalizándolo, mejorándolo, ampliándolo, cambiando su funcionalidad, corrigiendo errores en él, etc.
- Puede redistribuir el software modificado.

Resumiendo, si recibes un programa libre estarás seguro de poder usarlo como quieras, redistribuirlo a quien quieras, por los medios que quieras, y modificarlo (y mejorarlo o adaptarlo). Naturalmente, para poder asegurar estas libertades, todas las definiciones reconocen como imprescindible que el código fuente esté disponible, y sea a su vez redistribuible. De este hecho nace, en gran medida, el término "open source" (fuente abierta) que es propuesto por algunos como término para referirse al software libre.

Por cierto, es importante destacar en este momento que el software libre no obliga a ejercer ninguna de estas libertades, sólo las posibilita. Por ejemplo, el usuario de software libre no está obligado a redistribuir sus programas, a modificarlos, ni siquiera a usarlos...

Para aplicar estas libertades a un programa se usan las llamadas "licencias de software libre". Según la legislación sobre derechos de autor (que es la que clásicamente se aplica a los programas de ordenador), cuando se recibe un

programa sólo se puede redistribuir o modificar según los términos de la licencia que lo ``protege''. Por eso, en el mundo del software libre las licencias son muy importantes, y nos marcan exactamente qué podemos, y qué no, con cada programa. Aunque es cierto que, atendiendo a las libertades mencionadas, y sin saber nada más sobre licencias, se puede estar seguro de que al recibir un programa libre, como mínimo estas libertades están garantizadas (si no, no sería libre), lo que ayuda mucho al que no quiera profundizar más en asuntos legales.

Algunos ejemplos de licencias de software libre son la GNU General Public Licence (GPL), o la licencia de la Berkely Software Distribution (BSD).

Si buscamos definiciones más rigurosas que la que acabamos de introducir, podemos acudir al detalle de las definiciones formales más aceptadas: las ``[Directrices de software libre de Debian](#)'', la ``[Open Source Definition](#)'' (que se basó en las directrices de Debian, y es muy parecida a ellas) y el artículo ``[¿Qué es el software libre?](#)'', de la Free Software Foundation. Estas definiciones son similares, y se diferencian sólo en algunos detalles (que sin embargo pueden ser muy importantes cuando se examina una licencia en particular).

Las características del software libre, y las implicaciones que tiene su uso, son en gran medida consecuencias de estas libertades a las que nos estamos refiriendo. Por ejemplo, la libertad de redistribución proporciona, en la práctica, una canal de distribución de gran eficiencia económica, y de muy bajo coste para el productor. Las posibilidades de modificación y de redistribución de las modificaciones facilitan la evolución y mejora técnica de los programas. Y de la aplicación de todas las libertades simultáneamente se deducen importantes sinergias, que hacen que el software libre se comporte de una forma tan especial.

Jesus M. Gonzalez-Barahona 2003-04-06

ANEXO #4

LICENCIA GPL

Programa 3 (22/9/2005) - Breve historia de GNU/Linux

En la actualidad **GNU/Linux** está cada vez más presente en nuestra sociedad. Raro es el día que no sale una noticia relacionada en un medio generalista, cada vez más estamentos gubernamentales de todo el mundo adoptan soluciones informáticas libres (en España varias comunidades autónomas tienen iniciativas al respecto), incluso si nos acercamos al quiosco de nuestro barrio probablemente ya tenga una sección de publicaciones de nuestro sistema operativo favorito. Este veloz aumento de popularidad, a veces, lleva consigo una incorrecta asimilación de conceptos en forma de falsos mitos ([libre no significa gratis](#)) o de [rumores falsos](#) alimentados premeditadamente por los detractores más activistas de las plataformas libres.

En nuestra sección, tras definir el concepto de software libre, esta semana hemos comentado brevemente la historia de [GNU/Linux](#) con el objeto de dar sentido y coherencia a todos esos términos y posiciones éticas que forman parte de la filosofía del software libre.

Si comenzamos desde el principio de esta historia, ya nos encontramos con el primer falso mito. Habitualmente se tiende a pensar que el software libre es algo moderno, un invento de los últimos años, pero la realidad es bien distinta. Tendríamos que remontarnos a la época en que las computadoras tenían un ámbito limitado (universidades y grandes empresas), era un tiempo en el que éstas se adquirían con el software instalado. Los programadores de entonces podían compartir sus ideas de programación libremente. Nadie se planteaba aspectos sobre las libertades del software por la sencilla razón de que no era necesario, por ello, se puede afirmar que el software libre nace antes

de que aparezca la necesidad de definirlo.

Más tarde, algunas grandes compañías del sector, anticipando el gran negocio que supondría la venta de software, empiezan a imponer compromisos de “no revelación” a los desarrolladores: el código deja de poder compartirse libremente.

En el Instituto [Tecnológico de Massachusetts \(MIT\)](#) trabajaba por aquel entonces un informático que según cuenta la historia tuvo un problema con una impresora, el cual no pudo solucionar por no poder acceder al código del software de control de la misma. Esta situación le pareció tan injusta que decidió buscar una solución.

En el año 1983, [Richard Mathew Stallman](#), así se llamaba este informático, [envió un mensaje](#) en el que exponía la idea de crear un sistema totalmente funcional. Este sistema operativo, estilo [UNIX](#), estaría íntegramente formado por software libre.

Es en 1984 cuando se funda [GNU](#), dejando claro hasta en su nombre (**GNU: GNU no es Unix**) que no tendría ninguna vinculación con UNIX. Stallman abandona su puesto en el MIT (como medio para ganarse la vida empieza a vender copias de programas libres en cintas - Libre no significa gratis) para comenzar a desarrollar GNU, además de reclamar participación y soporte a otros programadores. El software libre, como lo conocemos hoy, había nacido, pero un proyecto de estas dimensiones necesitaba mucha coordinación y fondos. Con estos objetivos se crea a mediados de la década de los 80 la [Fundación del Software Libre \(FSF\)](#) la cual entre otras muchas actividades definió la [Licencia Pública General \(GPL\)](#) que es adoptada por GNU para la mayoría de su software.

A principios de los 90, GNU estaba casi completo, pero le faltaba una pieza clave en el funcionamiento de cualquier sistema operativo, el [núcleo \(o kernel\)](#). A pesar de varios intentos de núcleos, ninguno llegó a buen puerto por una razón u otra (actualmente GNU trabaja en su propio núcleo, [Hurd](#), pero todavía no existe una versión estable).

Desde Helsinki (Finlandia), un estudiante de informática llamado [Linus Benedict Torvalds](#), [manda un mensaje](#) al grupo de noticias **comp.os.minix** anunciando la versión 0.01 de Linux, un núcleo basado en [minix](#) que cumplía el estándar [posix](#) de UNIX. ¡La pieza que le faltaba al sistema operativo GNU!

Linus licenció su núcleo bajo la GPL y al integrarlo con GNU formó el sistema operativo [GNU/Linux](#) (GNU: los programas, Linux: el núcleo) totalmente funcional. En el año 94, aparece la primera versión estable (1.0).

En este momento colaboran multitud de personas en el proyecto y aparece el concepto de distribución para facilitar la integración de software sobre el núcleo. Se crean las primeras empresas en torno a GNU/Linux ([Red Hat](#), [SUSE](#), ...) y se empieza a desarrollar la industria en torno a estos sistemas. Aparece también el proyecto [Debian](#), distribución en la que está basada Guadalinex.

Dada la ambigüedad del término anglosajón *free* (libre o gratis) y como respuesta a la dificultad, que según algunos grupos de empresas, experimentaban en la promoción de un producto con este apellido se crea la [Iniciativa de Fuente Abierta \(OSI\)](#) que la FSF no adopta por no mencionar las cuatro libertades. Actualmente se contempla como otra de las definiciones de software libre.

A finales del siglo XX llega la gran explosión de este movimiento. Es el momento en el que gobiernos y grandes empresas los respaldan. En España, por ejemplo, aparecen desarrollos en [Extremadura](#) (pionera en España), [Andalucía](#) o [Castilla La Mancha](#) entre otras, en torno a las metadistribuciones. Y todo no acaba aquí, las más importantes consultoras del mundo auguran que el Software Libre será uno de las áreas de negocios que más crecerá en el futuro próximo y es que **¡lo mejor está por venir!**

[Audio del Programa 3 \(Ogg Vorbis\)](#)

This entry was posted on Saturday, September 24th, 2005 at 2:57 pm and is filed under [Aviso para navegantes](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

3 Responses to “Programa 3 (22/9/2005) - Breve historia de GNU/Linux”

1. [JulioNC](#) Says:

[September 25th, 2005 at 4:18 am](#)

EXCELENTE.... resumen....

fácil y razonable para el nuevo usuario....y que de una vez se metan el la cabeza que software libre, no significa gratis.... se ha dicho... saludos desde Perú

2. [Juan Antonio Páez](#) Says:

[September 26th, 2005 at 3:51 pm](#)

Aparte de la mucha información que existe sobre la historia de Unix, GNU y Linux, en toda ella se extrae que compartir con la comunidad los progresos que se obtienen ha sido siempre el mejor método de mejorar el software.

Por desgracia las grandes empresas del sector no ven esta necesidad (obviamente es una ventaja), salvo Sun, Apple (con Darwin), IBM. Las empresas que den el paso se verán recompensadas, creo yo, con el aliciente del apoyo de los consumidores, y esto les garantizará la supervivencia en muchos casos.

Editorial: kernel source

Ultima fecha de actualizacion 22-9-2005

<http://kernelsource.org/2005/09/24/programa-3-2292005-breve-historia-de-gnulinux/>

ANEXO#5

La Tabla de equivalencias / reemplazos / de software análogo a Windows en Linux.

Last update: 7.03.03, 01.02.05, 27.05.05, 07.07.2007
URL: <http://www.linuxrsp.ru/win-lin-soft/index-spanish.html>.
The original english version is [here](#).

This page on other languages: [Russian](#), [Italian](#), [English](#), [French](#), [German](#), [Hungarian](#), [Chinese](#), [Polish](#).

Una de las mas grandes dificultades en la migración de Windows a Linux es la carencia de software equivalente. Los Newbies por lo general buscan los software equivalentes de Windows para Linux, y los usuarios avanzados de Linux no pueden contestar sus preguntas ya que ellos a menudo no conocen demasiado sobre windows :). Esta lista de equivalencias / reemplazos / de software análogo a Windows en Linux está basada en nuestra propia experiencia y en la información de los visitantes a esta página (gracias!).

Esta Tabla no está estática - nuevos programas pueden ser agregados a lados derechos en tanto se este en marcha, y esto no es el hecho que la columna derecha será llenada inmediatamente. En el futuro nosotros planeamos migrar esta tabla a PHP/MySQL, asi los mismos visitantes podrán agregar programas, votar por los programas equivalentes, agregar comentarios, etc.

Notas:

- 1) Por principio todos los programas de linux en esta tabla son libres y están en liberados. Los programas propietarios para Linux están marcados con un señal [Prop].
- 2) Si no hay nada en el campo de la tabla, excepto "???" - Los autores de la tabla no saben que colocar allí.
- 3) Si la señal (???) se encuentra detrás del nombre del programa - Los autores de la tabla no están seguros sobre este programa.

La importancia ideológica de la diferencia entre Windows y Linux:

La mayoría de los programas de Windows son echos con el principio de "Todo en uno" (cada desarrollador agrega todo a su producto). De la misma manera, a este principio le llaman el "estilo-Windows".

La Ideología de UNIX/Linux - Un componente o un programa deben ejecutar sólo una tarea, pero lo ejecuta bien. ("estilo-UNIX"). Los programas bajo linux pueden ser pensados como LEGOS componentes básicos. (Por ejemplo, si hay un programa para la comprobación de ortografía, esto puede ser usado con el editor de textos o por un cliente de email al enviarlo; o si hay un poderoso programa de líneas de comando para el uso de archivos, es simple escribir el Interfaz gráfica para el programa, etc.).

Este principio es muy importante y es necesario conocerlo para buscar programas programas equivalentes de Windows en Linux :).

Lugares donde puedes obtener software para linux:

[FreshMeat.net](#) | [SourceForge.net](#) - Dos portales grandiosos. Puedes encontrar todo lo que tu quieras!!

[LinuxApps.com](#) | [IceWalkers.com](#) | [Linux.Tucows.com](#) - Me gusta estos catálogos.

[Download.com / Linux](#) | [LinuxSoftware.org](#) | [FileWatcher.org](#) | [LinuxArchives.com](#) - otros catálogos.

Programas / paquetes / búsqueda de librerías de sistema: [RPMseek.org](#) | [Tuxfinder.com](#) | [RPMfind.net](#)

Programas y juegos para Windows, estos programas pueden correr bajo Wine/WineX:

- 1) **Juegos para Windows, estos pueden correr con WineX** (La información del sitio de funcionario Transgaming). Este es un [formulario de búsqueda](#), y en esta lugar una [lista completa de juegos](#) (muy grande!).
- 2) **El catálogo mas gran de Windows , correindo bajo wine.** La base de datos de Codeweavers contiene información de cerca 1000 aplicaciones, y el catálogo es estructurado y tiene un sistema de la navegación.

LasSecciones:

Las Secciones:

- 1) [Redes y Conectividad.](#)
- 2) [Trabajo con Archivos.](#)
- 3) [Escritorio / Software de Sistema.](#)
- 4) Multimedia:
 - 4.1) [Audio / CD.](#)
 - 4.2) [Gráficos.](#)
 - 4.3) [Video y Otros.](#)
- 5) [Offimatica/negocios.](#)
- 6) [Juegos.](#)
- 7) [Programación y Desarrollo.](#)
- 8) [Software para Servidores.](#)
- 9) [Científicos y Programas Especiales.](#)
- 10) [Otros / Humor :\).](#)

Descripción del programa, tareas ejecutadas	Windows	Linux
1) Redes y Conectividad.		
Navegadores Web	Internet Explorer, Netscape / Mozilla for Windows, Opera, Phoenix for Windows , ...	1) Netscape / Mozilla. 2) Galeon. 3) Konqueror. 4) Opera. [Prop] 5) Phoenix. 6) Nautilus. 7) Epiphany. 8) Links. (with "-g" key). 9) Dillo. (Parches language Ruso - aquí).
Navegadores web para Consola	Lynx para Windows	1) Links. 2) Lynx. 3) w3m. 4) Xemacs + w3.
Clientes de Email	Outlook Express, Mozilla for Windows, Eudora, Becky	1) Evolution. 2) Netscape / Mozilla messenger. 3) Sylpheed , Sylpheed-claws. 4) Kmail. 5) Gnus. 6) Balsa. 7) Bynari Insight GroupWare Suite. [Prop] 8) Arrow. 9) Gnumail. 10) Althea. 11) Liamail. 12) Aethera.

Cientes de email al estilo MS Outlook style	Outlook	1) Evolution . 2) Bynari Insight GroupWare Suite . [Prop] 3) Aethera .
Cientes de email al estilo The Bat	The Bat	1) Sylpheed . 2) Sylpheed-claws . 3) Kmail . 4) Gnus . 5) Balsa .
Ciente de email en Consola	Mutt for Windows [de], Pine para Windows	1) Pine . 2) Mutt . 3) Gnus . 4) Elm . 5) Xemacs .
News reader	Xnews , Outlook, Netscape / Mozilla	1) Knode . 2) Pan . 3) NewsReader . 4) Netscape / Mozilla . 5) Sylpheed / Sylpheed-claws . Console: 6) Pine . 7) Mutt . 8) Gnus . 9) tin . 10) slm . 11) Xemacs .
Gestor de Descargas	Flashget, Go!zilla, Reget, Getright, Wget for Windows , ...	1) Downloader for X . 2) Caitoo (former Kget). 3) Prozilla . 4) Wget (console, standard). GUI: Kmagoo , QTget, Xget, ... 5) Aria . 6) Axel . 7) Download Accelerator Plus .
Descargador de Sites Web	Teleport Pro, ...	1) Htrack . 2) WWW Offline Explorer . 3) Wget (console, standard). GUI: Kmagoo , QTget, Xget, ... 4) Downloader for X . 5) Pavuk . 6) Curl (console).
Cientes FTP	Bullet Proof FTP, CuteFTP, WSFTP, ...	1) Gftp . 2) Dpsftp . 3) KBear . 4) IglooFTP . 5) Nftp . 6) Wxftp . 7) axyFTP .

Cientes FTP para Consola	FTP in Far, ftp.exe	1) Ncftp . 2) Lftp . 3) mc . (cd ftp://...)
Cientes IRC	Mirc, Klient, VIRC, Xircon, Pirch, XChat for Windows	1) Xchat . 2) KVirc . 3) Irssi . 4) BitchX . 5) Ksirc . 6) Epic . 7) Sirc .
CLientes Locales de Chat sin Servidor	QuickChat	Echat.
Mensajería local con máquinas windows	WinPopUp	1) LinPopUp . 2) Kpopup .
Cientes para Mesajería Instantánea	ICQ, MSN, AIM, ... Trillian ICQ (freeware, can replace all common IM clients), Miranda	1) Licq (ICQ). 2) Centericq (ICQ, consola). 3) Alicq (ICQ). 4) Micq (ICQ). 5) GnomeICU (ICQ). 6) Gaim . (Supports nearly all IM protocols) 7) Kopete . 8) Everybuddy . 9) Simple Instant Messenger . 10) Imici Messenger . 11) Ickle (ICQ). 12) aMSN (MSN). 13) Kmerlin (MSN). 14) Kicq (ICQ). 15) YSM . (ICQ, consola). 16) kxicq .
Cientes Jabber IM	JAJC , Tkabber (+activestate tcl), Psi , Exodus , WinJab , myJabber , RhymBox , Rival , Skabber , TipicIM , Vista , Yabber	1) Tkabber . 2) Gabber . 3) Psi . 4) Gaim .
Monitoreo de web Sites o Bandejas de Mail, muestran los titulares o toda el artículo	WatzNew	1) Web Secretary . 2) Knewsticker & korn . 3) Mozilla (???). 4) watch -n seconds lynx -dump
Conferencias en línea con Video/audio	NetMeeting	GnomeMeeting .
Comunicación por voz	Speak Freely	1) Speak Freely for Unix . 2) TeamSpeak .

Firewall (paquetes de filtración)	BlackICE, ATGuard, ZoneAlarm, Agnitum Outpost Firewall, WinRoute Pro , ...	iptables or more outdated ipchains (console, standard). Front ends: 1) Kmyfirewall . 2) Easy Firewall Generator . 3) Firewall Builder . 4) Shorewall . 5) Guarddog . 6) FireStarter . 7) Smoothwall . 8) IPCop .
IDS (Detección de intrusos en el Sistema)	BlackICE, Agnitum Outpost Firewall	1) Snort . 2) Portsentry / Hostsentry / Logsentry .
Visual route	VisualRoute	1) Xtraceroute . 2) VisualRoute for Linux . 3) Mtr . 4) Geotrace .
Filtrando Contenido	Proxomitron, ATGuard, Agnitum Outpost Firewall, Privoxy , MS ISA server, ...	1) Squid . 2) DansGuardian . 3) Squidguard . 4) Privoxy . 5) JunkBuster . 6) Fork . 7) Mozilla (tiene una posibilidad de filtrar el contenido).
Restricción de Tráfico	???	1) IP Relay .
Contabilidad de tráfico	Tmeter , ...	1) Tcp4me . 2) Getstatd . 3) Ipacct . 4) Ipac-ng . 5) Ipaudit . 6) Lanbilling . 7) SARG (full Squid traffic). 8) Talinux . 9) NetUP UserTrafManager . 10) MTRG . 11) NetTop .

Compartiendo archivos clientes / servidor (redes punto a punto)	Morpheus (Gnutella), WinMX, Napster, KaZaA (Fasttrack), eDonkey / eMule , TheCircle , Bittorrent	1) LimeWire for Linux. (Gnutella) 2) Lopster. (OpenNAP) 3) Gnapster. (OpenNAP) 4) Mldonkey. (eDonkey) 5) eDonkey for Linux. (eDonkey) 6) cDonkey. (eDonkey) 7) Gift client / server (Fasttrack) 8) ed2k_gui. 9) Gtk-Gnutella. (Gnutella) 10) Qtella. (Gnutella) 11) Mutella. (Gnutella, consola) 12) TheCircle. 13) Freenet. 14) GNUnet. 15) Lmule. (eDonkey) 16) Bittorrent.
Programas para trabajar sonido con modem y muchas mas funciones - desde answerback and AON dispositivos para mandar por fax	Venta Fax, PrimaFax	1) Gfax. (???) 2) PrimaFax for Linux. [Proprietary, 99\$] 3) mgetty + voice + sendfax. 4) vgetty.
Trabajando con Faxes	WinFax	1) HylaFax. 2) Fax2Send. 3) Efax.
Dialup	Vdialer, etñ	1) Kppp. 2) X-isp. 3) wvdial. (Front ends: X-wvdial, kvdial, gtkdial). 4) Gppp. 5) Kinternet. 6) Rp3.
FTN editor	Golded	1) Golded. 2) Golded+. 3) Msged.
FTN tosser	FastEcho, hpt	1) hpt. 2) CrashEcho.
FTN mailer	SF-Mail, T-Mail	1) ifcico. 2) qico. 3) Bforce.
Administración Remota	VNC, Administrador Remoto, Asistencia Remota, Symantec pcAnywhere, Windows Terminal Server, Rdesktop , Radmin	1) VNC. 2) ssh / openssh. 3) Remote management is built-in in XFree86. 4) Rdesktop Client. 5) freeS/WAN (???)
Transmisión de archivos al modem	HyperTerminal, Terminate, etc	1) Minicom + lrzrz + Kermit. 2) Mstern. 3) Xtel.

Trabajando con ssh	Putty, Irlex, cygwin + ssh	1) Kssh. 2) ssh / openssh . 3) GTelnet. (Telnet, SSH, Rlogin)
Herramientas de Monitoreo de Redes	Dumeter, Netmedic	1) Gkrellm . 2) Big Brother . 3) Etherape . 4) Nagios . 5) Tkined . 6) MRTG . 7) Rrdtool. 8) PIKT . 9) Autostatus . 10) bcnu . 11) mon . 12) Sysmon . 13) Spong . 14) SNIPS . 15) iptraf (console).
Herramientas maintance para Redes	HP OpenView, MS SMS, Tivoli	1) HP OpenView agents for Linux. [Prop] 2) Big Brother . 3) Cheops . 4) Tkined .
Analizando Protocolos, sniffing	Sniffer, EtherPeek (TokenPeek, AiroPeek), Windump , Ethereal , MS Network Monitor, Iris	1) Ethereal . 2) Tcpdump . 3) Etherape . 4) ipxdump. (+ipxparse for parsing)
Escaneo de Redes	ShadowScan, ISS, Retina, Internet Scanner	1) Nessus . 2) Nmap . 3) Bastille (???).
Routing	MS RRAS	1) Iproute2. 2) iptables or more outdated ipchains (consola, standard).
Utililerías y librerías para el testeo Ethernet/IP	lcrzo	lcrzo
Telefonía IP	Buddyphone [Prop]	1) GNU Bayonne . 2) Openh323 .
Compartiendo Datos/Archivos	Windows shares	1) Samba . 2) Samba-TNG .
???	Windows Domain, Active Directory	1) Samba. 2) Ldap. 3) yp.
Visualizando redes-windows	Network neighborhood	1) Samba. 2) KDE Lan Browser, lisa 3) LinNeighborhood. 4) xSMBrowser .
ADSL	-	rp-pppoe.

2) Trabajando con Archivos.

Administrador de Archivos al estilo FAR y NC	FAR, Norton Commander, etc	1) Midnight Commander . 2) X Northern Captain . 3) Deco (Demos Commander) . 4) Portos Commander . 5) Konqueror in MC style .
Administrador de Archivos al estilo Windows Commander	Total Commander (former Windows Commander)	1) Midnight Commander . 2) Krusader . ~1.3 Mb. Suitable GUI file manager for KDE. Support archiver, FTP with suitable notebook, Samba, built-in editor and graphics viewer. 3) Kcommander . 4) FileRunner (written on TCL/TK). 5) Linux Commander . 6) LinCommander . 7) Rox . 8) Emelfm .
Administrador de Archivos al estilo Windows	Windows Explorer	1) Konqueror . 2) Gnome-Commander . 3) Nautilus . 4) Endeavour Mark II . 5) XWC .
Inspección rápida de documentos de HTML locales	Internet Explorer	1) Dillo . (Russian language patches - here). 2) Konqueror . 3) Nautilus . 4) Lynx / Links .
Visualizador de todas las Operaciones con Archivos	Filemon	Filemon para Linux .
Trabajando con UDF	Roxio (former Adaptec) UDF Reader, Roxio Direct CD	Linux-UDF .
Trabajando con Multi Secciones de CD+ recuperador de información defectuosa del disco multi sesión	IsoBuster	CDFS .

3) Sistemas de Software para Escritorio.

Editor de Texto	Notepad, WordPad, TextPad, ...	1) Kedit (KDE) . 2) Gedit (Gnome) . 3) Gnotepad . 4) Kate (KDE) . 5) KWrite (KDE) . 6) Nedit . 7) Vim . 8) Xemacs . 9) Xcoral . 10) Nvi .
-----------------	--------------------------------	--

Editor de Consola para Texto	FAR Editor, ...	1) Vim. 2) Emacs. 3) pico. 4) joe. 5) Fte. 6) Jed.
Editor de texto y código multi finalidad	SciTE , UltraEdit , MultiEdit, ...	1) Kate (KDE). 2) Nedit. 3) CodeCommander. 4) SciTE. 5) Quanta Plus. 6) Vim. 7) Xemacs. 8) Mcedit (como con mc). 9) Jed.
Editor de textos con soporte codificación cyrillic	Bred, Rpad32, Aditor	1) Kate (KDE). 2) Nedit. 3) Fte (console). 4) Parche para la versión de Midnight Commander. 5) Vim. 6) Xemacs.
Trabajando con compresores de archivos	WinZip, WinRar	1) FileRoller. 2) Gnozip. 3) LinZip. 4) Ark (kdeutils). 5) KArchiver. 6) Gnohive. 7) RAR for Linux. 8) CAB Extract.
Visualizador de PostScript	RoPS	1) GhostView. 2) Kghostview.
Visualizador de PDF	Adobe Acrobat Reader	1) Acrobat Reader para Linux. 2) Xpdf. 3) GV.
Creador de PDF	Adobe Acrobat Distiller	1) Muchos programas Linux WYSIWYG m -> imprimir el archivo -> ps2pdf. (Aquí esta el artículo about this). 2) Adobe Acrobat Distiller para Linux. [Prop] 3) PStill. [Shareware] 4) PDFLatex. 5) Xfig. 6) Ghostscript. 7) Tex2Pdf. 8) Reportlab. 9) GV.
Criptografía y Cifrado	PGP, GnuPG + Windows Privacy Tools	1) GnuPG (console) + GPA, KGpg, and other frontends. 2) PGP. [Prop]

Encriptación de volúmenes de disco	EFS (standard), PGP-Disk, BestCrypt, Private Disk Light	1) Loop-aes . 2) CFS . 3) TCFS . 4) BestCrypt . 5) CryptFS .
Task scheduler	mstask, nnCron	cron, at (standard, consola).
Outlook scheduler	Outlook scheduler	???
Virtual CD	VirtualDrive, VirtualCD, Daemon Tools, ...	1) Virtual CD Kernel Modul . 2) "cp /dev/cdrom /mycd" + "mount -o loop /mycd /mnt/cdrom/".
Reconocimiento de Texto (OCR)	Recognita, FineReader	1) ClaraOcr . 2) Gocr .
Traductores (cyrillic)	Prompt, Socrat	Ksocrat (???)
Diccionarios Eng-rus(cyrillic)	ABBYY Lingvo, Socrat	1) Mueller . 2) Ksocrat . 3) dict+Kdict. 4) DictX . 5) Groan . 6) Mova. 7) Slowo.
Trabajando con el Escaner	Programs on CD with scanner	1) Xsane . 2) Kooka . 3) Xvscan . [Prop]
Antivirus	AVG AntiVirus, NAV, Dr. Web, TrendMicro , F-Prot , Kaspersky, ...	1) Dr. Web for Linux . [Prop] 2) Trend ServerProtect for Linux . [Prop] 3) RAV Antivirus . [Prop] 4) OpenAntivirus + AMaViS / VirusHammer . 5) F-Prot . [Prop] 6) Sophie / Trophie . 7) Kaspersky for Linux . [Prop]
Configuración del Sistema	Msconfig	1) En la instalación de Red Hat Linux. 2) redhat-config-<feature>. El configurador gráfico de Redhat 8.0. 3) Linuxconf . 4) Drakeconf. 5) Webmin. 6) yast and yast2 in SuSE. 7) sysinstall in FreeBSD. 8) /dev/hands :).
Administradores de Buteo(BOOT)	System Commander, PowerQuest Boot Magic, ...	1) Grub . 2) Lilo. 3) ASPLoader. 4) Acronis OS Selector [Prop]. 5) Ranish Partition Manager . 6) osbs . 7) Symon . 8) Smart Boot Manager .

Administrador de las particiones del disco duro	PowerQuest Partition Magic	1) PartGUI. (GUI for partimage and parted) 2) GNU Parted . (GUI - QTParted). 3) Partition Image . 4) fips. 5) Diskdrake (Mandrake). 6) Paragon Partition Manager [Prop].
LVM + soft-RAID + parted + ...	-	EVMS .
Software para Backup	ntbackup (standard), Legato Networker	1) Legato Networker . 2) Lonetar . 3) Disk Archive . 4) Bacula . 5) Taper . 6) Amanda (console). 7) Mondo Rescue . (backups that boot and auto restore themselves to disk)
Hacer imágenes del as particiones de disco	DriveImage, Ghostpe	1) PartitionImage (GUI - PartGUI). 2) dd (consola, standard). 3) Mondo Rescue .
Administrador de Tareas	TaskMan (standard), TaskInfo, ProcessExplorer NT.	1) top (consola, standard). 2) Gtop, Ktop. 3) kSysGuard.
Gestor de Mouse	Sensiva	Kgesture .
Reconocimiento de texto por voz	MS text to speech	1) KDE Voice Plugins . 2) Festival . 3) Emacspeak .
Reconocimiento de Voz	ViaVoice, DragonNaturally Speaking	Si, aquí no hay programas para reconocimiento de voz. Pero: 1) Sphinx . 2) ViaVoice. (almost dead...)
Programas para comparar Archivos	Araxis Merge, Minimalist GNU For Windows (diff.exe)	1) WinMerge . 2) Mgdif. 3) diff, patch. 4) Xemacs .
Tratamiento de texto corrido	Minimalist GNU For Windows (sed.exe)	1) sed, awk. 2) perl .
PIM / DB / block de notas con visualizador por árboles	TreePad Lite, Leo	1) TreePad Lite for Linux . 2) Yank . 3) TreeLine. 4) Gjots . 5) Leo .
Program for quick switching between resolutions and frequencis	integrados al Sistema, comes on CD with video card	1) Multires for Linux . 2) Ctrl+Alt+"-", Ctrl+Alt+"+". 3) Fbset . (when using framebuffer)
Programas para meta Búsquedas	Integrated with system, Indexing service	find (console, standard). GUI: 1) Gsearchtool . 2) Kfind .

Monitorero de Sistemas	System monitor (integrado al sistema)	1) Gkrellm .
Programa visualizar logs	???	1) Xlogmaster . 2) Analog . 3) Fwlogview . (firewall)
Herramientas para recuperación de datos	R-Studio (supports Linux partitions)	1) e2undel . 2) myrescue . 3) TestDisk . 4) unrm . 5) Channel 16 .
Codificador de archivos de texto con la detección automática de caracteres	Total Recoder, ...	1) Enca .
"Analizando el tiempo tomador en la rutina de un programa" (¿Qué es esto ? y no lo conozco :).	???	1) Valgrind . 2) Kcachegrind .

4.1) Multimedia (audio / CD).

Links usuales:	-	Linux MIDI & Aplicaciones de Sonido - muchos links y recursos. Sound Software - Muchos de estos.
Reproductores Música / mp3 / ogg s	Winamp	1) XMMS (X multimedia system) . 2) Noatun . 3) Zinf . (former Freeamp) 4) Winamp para Linux. 5) Xamp. 6) GQmpeg . 7) SnackAmp .
Consola de música / mp3 / ogg players	mpg123 para Windows, dosamp	1) Cplayer. 2) mpg123 / ogg123. 3) mpg321 . 4) Orpheus .
Programas para quemar CD con GUI	Nero, Roxio Easy CD Creator, ...	1) K3b . (KDE) 2) XCDRoast . 3) KOnCd . 4) Eclipt Roaster . 5) Gnome Toaster . 6) CD Bake Oven . 7) KreateCD . 8) SimpleCDR-X . 9) GCombust . 10) WebCDWriter . (Servidor de quemado de CD , usable desde cualquier navegador con soporte para Java)

Reproductores de CD	CD player	1) KsCD. 2) Orpheus. (console) 3) Sadp. 4) WorkMan. 5) Xmcd. 6) Grip. 7) XPlayCD. 8) ccd / cccd. (consola)
Bajando la velocidad de rotación del CD	Slowcd, Cdslow	1) hdparm -E <speed> 2) eject -x <speed> 3) cdspeed.
CD ripping / grabación	Windows Media Player, AudioGrabber, Nero, VirtualDrive, VirtualCD, ...	1) Grip. 2) Audacity. 3) RipperX. 4) tkcOggRipper. 5) cdda2wav. 6) Gnome Ooaster. 7) Cdparanoia. 8) Cd2mp3. 9) Dagrab. 10) SimpleCDR-X. 11) RatRip. 12) AutoRip.
Reproductores Midi + karaoke	VanBasco	???
Decodificadores Mp3	Lame	1) Lame. 2) Bladeenc. 3) NotLame. 4) L3enc. [Prop] 5) gogo.
Trabajando con protocolos en Tiempo Real	RealPlayer	1) RealPlayer for Linux. 2) Mplayer + librerías.
Programas para recepción de estaciones de radio	VC Radio, FMRadio, Digband Radio	1) xradio. 2) cRadio. 3) Xmradio. 4) RDJ. 5) RadioActive. 6) XMMS-FMRadio. 7) Gqradio.
Editores de Audio	SoundForge, Cooledit, ...	1) Sweep. 2) WaveForge. 3) Sox. 4) Audacity. 5) GNU Sound. 6) Ecasound.
Procesadores de Audio Multitrack	Cubase	1) Ecasound.

Sound tracker	Fasttracker, ImpulseTracker	1) Soundtracker . 2) Insotracker . 3) CheeseTracker.
Mezcladores de Sonidos	sndvol32	1) Opmixer . 2) aumix. 3) mix2000. 4) Mixer_app (for WindowMaker)
Editor de Notas Musicales	Finale , Sibelius , SmartScore	1) LilyPond . 2) Noteedit . 3) MuX2d .
Secuenciador de Midi	Cakewalk	1) RoseGarden . 2) Brahms . 3) Anthem . 4) Melys . 5) MuSE . Más información: Midi-Howto .
Creadores de Música	Cakewalk, FruityLoops	1) RoseGarden . 2) Ardour .
Los sintetizadores	Virtual waves, Csound	1) Csound . 2) Arts Builder (???)
Editores de ID3-Tag	Mp3tag	EasyTAG .

4.2) Multimedia (Gráficos).

Visualizador de Archivos Gráficos	ACDSee, IrfanView	1) Xnview . 2) GQview . 3) Qiv . 4) CompuPic. 5) Kuickshow . 6) GTKSee . 7) xv . [Prop] 8) pornview. 9) imgv . 10) Gwenview . 11) Gliv . 12) Showing . 13) Fbi. 14) Gthumb .
Visualizador de Archivos gráficos en consola	QPEG	zgv .
Editores Simples de Gráficos	Paint	1) Kpaint. 2) Tuxpaint . 3) Xpaint . 4) Gpaint . 5) Killustrator .
Editores portentes de Gráficos tipo PhotoShop	Adobe Photoshop, Gimp para Windows , Paint Shop Pro	1) Gimp , FilmGimp . 2) ImageMagick .

Programas para Trabajos gráfico con Vectores	Adobe Illustrator, Corel Draw 14, Freehand, AutoSketch	1) Sodipodi . 2) xfig . 3) Sketch . 4) Karbon14 and Kontour . 5) OpenOffice Draw . 6) Dia . 7) Tgif . 8) Gestalter . 9) ImPress .
-	Corel Draw 9	Corel Draw 9 para Linux.
-	Corel PhotoPaint 9	Corel PhotoPaint 9 para Linux .
Programa para Decorar Texto	Wordart	OpenOffice Draw .
Programas para Dibujar con código ASCII	ANSI DRAW, Mazaika	1) CanvASCII . 2) Jave . 3) ANSI Draw.
Convertir los archivos Gráficos a pseudográficos	???	aalib.
Visualizadores de Flash	Flash Player	1) SWF Macromedia Flash Player . 2) Flash Player para Linux (???). 3) Plugin for Netscape/Mozilla (download here or here).
Creación de Flash	Macromedia Flash	1) DrawSWF . 2) Ming . (Creación de flash swf desde lenguajes de programación)
Creación de gráficos Web	Macromedia Fireworks	Gimp .
Gráficos 3D	3D Studio MAX, Maya , Povray , ...	1) Blender . 2) Maya . 3) KPovModeler . 4) K3Studio . 5) Moonlight . 6) GIG3DGO . 7) Povray . 8) K3D . 9) Wings 3D . 10) Softimage XSI . [Prop]
Instrumentos para hacer modelamiento fotográfico de calidad tipo ArchiCAD 3D	ArtLantis Render	???
Editores de Iconos	Microangelo	1) Gnome-iconedit. 2) Kiconedit.
Pequeños programas de captura de pantallas	Integrado con el sistema(PrintScreen), Snag it, ...	1) Ksnapshot. 2) Xwpick. 3) Xwd, xgrabsc. 4) Motv (xawtv) 5) Streamer (video)

Dibujo de Diagramas y Estructuras de Bases de Datos	Access	1) Dia . 2) Toolkit for Conceptual Modelling .
Creación de impresiones de calendario, tarjetas postales, etc., con colecciones de clip art	Broderbund Print Shop	???
4.3) Multimedia (video y Otros)		
Reproductores de Video / mpeg4	BSplayer, Zoomplayer, Windows Media Player, VideoLAN	1) Mplayer . 2) Xine . 3) Sinek . (frontend para libxine) 4) VideoLAN . 5) Aviplay .
Reproductores en Consola para video / mpeg4	do not exist	Mplayer .
Reproductores de DVD	PowerDVD, WinDVD, MicroDVD, Windows Media Player, VideoLAN	1) Ogle . 2) Mplayer . 3) Xine . 4) Aviplay . 5) VideoLAN .
Decodificadores de DVD rippers	Gordian Knot	1) Drip . 2) Mencoder .
Creación y edición sencilla de video	Windows Movie Maker	1) iMira Editing . 2) MainActor . 3) Broadcast 2000 .
Creación y edición Profesional de Video	Adobe Premiere, Media Studio Pro	1) iMira Editing . 2) Cinelerra . 3) MainActor . 4) Broadcast 2000 . 5) Lives .
Cortando video	Virtual Dub	1) Avidemux . 2) Kino .
Convertidores de video	Virtual Dub	1) Transcode . 2) Mencoder (from Mplayer).
Trabajando con Sintonizadores de TV	AVerTV, PowerVCR 3.0, CinePlayer DVR, ...	1) Kwintv . 2) Xawtv . 3) Zapping . 4) GnomeTV . 5) Mplayer .
Trabajando con Sintonizadores TV-tuner en consola	-	1) Mplayer . 2) fbtv . 3) aatv .
Trabajando con formatos QuickTime	QuickTime Player	1) QuickTime Player para Linux. 2) Mplayer + Sorenson codec.
Programas para creació de efectos 2D y 3D , animación y composición	Adobe After Effects	1) Shake . [Proprietario, \$129.95] 2) Plugins para Gimp.

generación Landscape / terrain	Bryce	Terraform.
Contrucción de Mundos Virtuales	World Construction Set, Animatek World Builder	???
Framework para desarrollo de aplicaciones en video	???	Gstreamer.

5) Offimatica/Negocios. .

Paquetes de oficina	MS Office, StarOffice / OpenOffice , 602Software	1) Openoffice. 2) Staroffice. [Prop] 3) Koffice. 4) HancomOffice. [Prop] 5) Gnome Office. 6) Applixware Office. 7) Siag Office. 8) TeX, LaTeX, ...
Suite de oficina	WordPerfect Office 2000	WordPerfect Office 2000 para Linux. (No longer available at Corel website. Esto fue en la versión de Windows, corre bajo Wine :).
Procesador de Word	Word, StarOffice / OpenOffice Writer, 602Text	1) Abiword. 2) WordPerfect. 3) Ted. 4) StarOffice / OpenOffice Writer. 5) Kword. 6) LyX. 7) Kile (KDE Integrado a LaTeX).
Hojas de Cálculo	Excel, StarOffice / OpenOffice Calc, 602Tab	1) Gnumeric. 2) Abacus. 3) StarOffice / OpenOffice Calc. 4) Kspread.
Dibujo de Gráficos	Excel, ...	1) Kivio. 2) Dia. 3) KChart. 4) xfig. 5) Gnuplot. 6) GtkGraph.
Creación de Presentaciones	MS PowerPoint, StarOffice Presentation, OpenOffice Impress	1) StarOffice Presentation. 2) OpenOffice Impress. 3) Kpresenter. 4) MagicPoint. 5) Kuickshow & gimp :).
Bases de Datos Locales	Access	1) KNoda. 2) Gnome DB Manager. 3) OpenOffice + MySQL. 4) InterBase. 5) BDB. 6) Rekall. [Prop] 7) StarOffice Adabase.

Paquetes de Contabilidad Financiera (global)	???	1) Hansa Business Solutions . [Prop]
Paquetes de Contabilidad Financiera(Ruso)	"1C: Accounting"	1) Hansa Business Solutions . [Prop] 2) IceB . 3) "Finances without problems" . 4) Ananas . 5) E/AS . 6) 1L: Project .
Paquetes de Contabilidad Financiera (Indio & Asia)	???	Kalculate . [Prop]
Administrador Personal de Finanzas	MS Money, Quicken	1) GNUcash . 2) GnoFin . 3) Kmymoney . 4) Grisbi .
Administrador de Proyectos	MS Project, Project Expert 7	Mr Project .
Automación de empresas (Russia)	"1C: Enterprise"	1) Keeper . [Prop] 2) Oblik . [Prop] 3) IceB . 4) Compiere .
Recibiendo las cotizaciones, noticias, construyendo gráficos y analizando de el Mercado financiero.	Omega Research Trade Station 2000	???
Software para e-commerce y web business	Weblogic, Websphere , iPlanet	1) Weblogic for Linux . [Prop] 2) JBoss . 3) IBM WebSphere Application Server . [Prop]

6) Juegos.

Donde Obtenerlos	Si usted Quiere :).	The Linux Game Tome (happypenguin.org) LinuxGames.com Kde Games Linux Game Publishing
Lista de Juegos en Linux	-	http://www.icculus.org/igfaq/gamelist.php
Juegos para Windows, esto también corre bajo WineX	-	This is a Formulario de búsqueda , y esto es una full lista de juegos (muy grande!).
-	Tetris	1) LTris . 2) XWelltris .
-	Juegos Standard en Windows	Kdegames .
-	Mines	1) KMines . 2) Perlmines .
-	Civilization	FreeCiv .
-	Civilization: Call to Power	Civilization: Call to Power para Linux.
-	Sid Meyer Alpha Centauri	Sid Meyer Alpha Centauri para Linux.
-	Sim City 3000	Sim City 3000 para Linux.
-	Command&Conquer	FreeCNC .
-	Warcraft 2, Starcraft (?)	FreeCraft .
-	(Win)Digger	1) Digger . 2) XDigger .

-	Arkanoid, Zball, ...	Lbreakout2.
-	Quake 1, 2, 3	Quake 1, 2, 3 para Linux.
-	CounterStrike	CounterStrike bajo WineX.
-	Urban Terror	Urban Terror para Linux.
-	DOOM	1) Jdoom. 2) Zdoom. 3) DOOM Legacy. 4) LxDOOM. 5) PrBoom.
-	Return to Castle Wolfenstein	Return to Castle Wolfenstein para Linux.
-	Descent	Descent para Linux.
-	Never Winter Nights	Never Winter Nights para Linux.
-	Unreal Tournament / Unreal Tournament 2003	Unreal Tournament / Unreal Tournament 2003 para Linux.
-	Soldier Of Fortune	Soldier Of Fortune para Linux.
-	Tribes 2	Tribes 2 para Linux.
-	Blood 1	Qblood.
-	Worms	Nil.
-	Lines	GtkBalls.
-	MS Flight Simulator	FlightGear
-	Lemmings	Pingus
Emulador de Sony PlayStation	ePSXe para Windows	ePSXe.
Racing	Need para Speed	Tux Racer :).
Chess	ChessMaster, ...	1) Glchess. 2) Xboard. 3) Eboard.

7) Programación y Desarrollo.

IDE	Microsoft VisualStudio .net	1) CodeForge. 2) Kdevelop + Qt3 Designer. 3) Eclipse. 4) Glade + Motor or + Xwpe or + any text editor. 5) Emacs, XEmacs.
-----	-----------------------------	--

Visual C++ IDE	Borland C++ Builder, MS Visual C	1) Anjuta + Glade + Devhelp. 2) KDE Studio Gold. [Prop] 3) Dev-C++. 4) Kylx. [Prop] (Kylx la edición personal es libre). 5) vtkBuilder. 6) foxBuilder. 7) wxDesigner. 8) Arriba. [Prop] 9) Code Crusader. [Prop] 10) CodeWarrior. [Prop] 11) Gbuilder. 12) Source Navigator. 13) TimeStorm. [Prop] 14) Understand for C++. [Prop] 15) SlickEdit. [Prop] 16) Vide.
C++ IDE	Borland Turbo C++ 3.0 para DOS, , Minimalist GNU para Windows (mingw32-gcc.exe)	1) GCC (+ Motor or + Xwpe). 2) LinEdit. 3) Rhide. 4) Wxstudio. 5) Eclipse.
Objetos en Pascal IDE	Delphi	1) Kylx. [Prop] (Kylx la edición personal es libre). 2) Lazarus + FPC.
Pascal	Pascal, BP	1) Freepascal. 2) GNU Pascal. 3) RShell (al estilo de Borland Pascal 7.0)
Basic	Basic	1) Hbasic. 2) X-basic. 3) Yabasic. 4) SmallBASIC.
Prolog	VisualProlog, Mercury	1) GNU Prolog. 2) Mercury. 3) SWI-Prolog.
Assembler	TASM, MASM, NASM	1) NASM. 2) FLAT Assembler.
Disassembler, ingeniería en reversa	SoftIce	El código es abierto :) 1) ldasm.
Debugger	Minimalist GNU For Windows (gdb.exe)	1) gdb. 2) ddd (frontend para gdb).
Editor Html WYSIWYG	Macromez Dreamweaver, Frontpage	1) Netscape / Mozilla Composer. 2) Openoffice HTML editor. 3) Amaya. 4) GINF (Ginf no es Frontpage) 5) IBM WebSphere Homepage Builder. [Prop]

Editores potentes para la creación de sitios web, con tiene un set de ejemplos y puede ser complementado con algunas pequeños tipos de plug-ins	Dreamweaver Ultradev	???
Editores HTML	HomeSite	1) Quanta Plus . 2) Bluefish . 3) WebMaker . 4) Screem . 5) Toppage . 6) WebDesigner . 7) ScriptEditor . 8) August .
Editor HTML	Arachnofilia	Arachnofilia . [Prop]
Perl/Python/Tcl IDE	-	Komodo . [Prop]
IDE de Java	JBuilder	Link: Java Tools for Linux . 1) Jbuilder äÿ Linux . 2) NetBeans . 3) Eclipse . 4) Sun ONE Studio . [formerly Forte] 5) Vide .
IDE para Desarrollo de Bases de Datos Oracle	T.O.A.D., SQL Navigator, PL/SQL Developer	Tora .
CASE-facilesity para UML	ArgoUML , Together ControlCenter [Prop]	1) Umbrello UML Modeller . 2) Dia+Dia2Code . 3) PoceidonCE (community edition) . 4) ArgoUML . 5) Together ControlCenter [Prop]
Elevados sistemas de CASE	Rational Rose.	Rational Rose for Linux . [Prop]
Editores HEX	Hiew	1) Biew . 2) KHexEdit .
Compiladores y preprocesadores Clipper	CA-Clipper, The Harbour Project	1) Clip . 2) The Harbour Project . 3) xHarbour .
Plataformas al estilo dot-net	M\$.Net	1) Mono . 2) DotGNU/Portable.NET
Trabajando con CVS	WinCVS, TortoiseCVS, cvs for Windows, BitKeeper [Prop]	1) cvs (consola). 2) Cervisia (KDE). 3) Lincvs . (Front-end para CVS) 4) BitKeeper . [Prop] 5) SubVersion . (enhanced CVSi-like platform + WebDAV -> SCM)
IDE para desarrollo de Interbase/Firebird	IBExpert	???
Visual Basic	Visual Basic	Phoenix .

Librerías Gráficas	-	1) gtk . 2) qt . 3) ftk .
8) Software para Servidores.		
Servidores Web	Internet Information Server, Apache para Windows, roxen / roxen2, wn, cern-httpd, dhttpd, caudium, aolserver, boa, ...	1) Apache . 2) Xitami. 3) Thttp. 4) Tux. 5) PublicFile .
Servidores FTP	Internet Information Server, ServU , War FTP, BulletProof FTP server	1) pure-ftp . 2) vsftpd. 3) wu-ftp . 4) proftpd . 5) gl-ftp . 6) ftp. 7) PublicFile .
Languages para Desarrollo Web	PHP para Windows	PHP .
Languages para desarrollo web	Perl para Windows	Perl .
Languages para desarrollo web	ASP	ASP módulos para Apache.
Motores de Bases de Datos	MS SQL, MySQL para Windows	1) Sybase Adaptive Server Enterprise . [Prop] 2) PostgreSQL . Las mas avanzada base de datos. 3) MySQL . Las mas popular base de datos abierta. 4) mSQL. 5) SAP DB .
Motores de Bases de Datos	IBM DB2	IBM DB2 para Linux . [Prop]
Motores de Bases de Datos	Oracle para Windows	1) Oracle . [Prop] 2) PostgreSQL . 3) Linter . (cyrillic)
Motores de Bases de Datos	Informix	Informix.
Motores de Bases de Datos	Borland Interbase, FireBird	FireBird .
Servidores Email	MDaemon , Hamster	1) Sendmail . 2) Qmail . 3) Postfix . 4) Exim .

Email + Groupware	Microsoft Exchange	1) CommuniGate Pro . [Prop] 2) Bynari's Insight GroupWare Suite . [Prop] 3) Samsung Contact . [Prop] 4) Teamware Office para Linux . [Prop] 5) Novell Netmail . [Prop] 6) Amphora . Basado en zope y qmail. 7) Tutos . Based on Linux / Apache / PHP / Mysql / Sendmail. 8) Kroupware . Del proyecto de KDE desarrollo de PIM, que comienza a financiarse por el gobierno Alemán. 9) SuSe Linux Openexchange Server . [Prop] 10) phpGroupWare . [Prop] 11) SCOoffice Mail Server . [Prop]
Filtro Mail / Eliminador de spam	cygwin+Exim port	1) SpamAssassin . 2) Procmail . 3) Mailfilter. 4) Ñyrus-imap . 5) Exim.
Descargador de Mail	MDaemon	Fetchmail .
???	Lotus Domino para Windows	Lotus Domino para Linux . [Prop]
Server / router en un diskette.	Impossible	Tanots como usted quiere :). 1) muLinux . 2) Dachstein (firewall / dhcp). 3) Serverdisk (http / ftp). 4) Fli4L .
Servidores Proxy	MS Proxy Server, WinGate	1) Squid . 2) Paco . 3) Privoxy . 4) Wwwoffle .
Servidores para soportar Java Servlets y JSP, puede trabajar con Apache	Tomcat	Tomcat .

9) Científicos y Programas Especiales.

Sistemas Matemáticos al estilo MathCad	Mathcad	Gap.
Sistemas Matemáticos al estilo Matlab	Matlab	1) Matlab para Linux . [FTP] 2) Octave . (+ Gnuplot) 3) Scilab . 4) R. 5) Yorick. 6) rlab. 7) Yacas . 8) Euler .
Sistemas Matemáticos al estilo Mathematica	Mathematica	1) Mathematica for Linux . 2) Maxima. 3) MuPad.

Sistemas Matemáticos al estilo Maple	Maple	1) Maple para Linux . [Prop] 2) Maxima . 3) MuPad .
Editor de Ecuaciones matemáticas	Mathtype, MS Equation Editor	1) OpenOffice Math . 2) MathMLed . 3) Kformula (Koffice) . 4) LyX .
Programas para modelado tri dimensional	SolidWorks, ...	ProEngineer Linux .
ditto	CATIA para Windows	CATIA. esto fue diseñado bajo Unix, y en la versión 4 (2000) esto fue portado para funcionar bajo Windows (No completamente satisfactorio).
ditto	SolidEdge para Windows	SolidEdge (Parte de paquete más poderoso Unigraphics).
Engineering	ANSYS para Windows	ANSYS.
CAD/CAM/CAE	Autocad, Microstation	1) Varkon . 2) Linuxcad . [Proprietario, ~100\$] 3) Varicad . [Prop] 4) Cycas . 5) Tomcad . 6) Thancad . 7) Fandango . 8) Lignumcad . 9) Giram . 10) Jcad . 11) QSCad . 12) FreeEngineer . 13) Ocadis . 14) Microform . 15) PythonCAD .
CAD/CAM/CAE, simplificado	ArchiCAD	Qcad .
Sistemas de Publicación apoyada por el ordenador	Adobe PageMaker, QuarkXPress	Adobe Framemaker . [Proprietario, cancelado]
Pequeños Sistemas de Publicación apoyada por el ordenador	MS Publisher	1) Scribus - Desktop Publishing para Linux . 2) KWord .
Digramción y Diseño Cartográfico	Microsoft Visio	1) Kivio (Koffice) . 2) Dia . 3) KChart . 4) xfig . 5) Tgif + dotty . 6) Tulip .
Software de procesamiento de imágenes geográficas	Erdas Imagine, ER Mapper , ENVI	ENVI para Linux .
GIS (Sistema de información Geográfica)	ArcView	1) Grass . 2) Quantum GIS . 3) PostGIS .

Vectorizador del tramado de mapas	MapEdit, Easy Trace	???
Software CNC, controlador de herramientas de máquinas	OpenCNC [Prop]	EMC .
Sistema de tratamiento de texto Avanzado en estilo TeX	MikTex, emTeX (DOS)	1) TeX. 2) TeTeX / LaTeX 3) LyX (WYSIWYM). 4) Kile .
Convenientes funcionales y amigables de usar editores de archivos TEX y dvi .	WinEdt	1) Kile (KDE Integrado en el Ambiente de LaTeX). 2) Ktexmaker2. 3) Tk LaTeX Editor . 4) Texmacs .
Lenguajes integrados de ambiente Estadísticos	S-PLUS	R .
Análisis Estadístico	Statistica	"Utilidades de Probabilidad y Estadísticas para usuarios de Linux"
Software Económico	Eviews, Gretl	1) Gretl .
Emuladores de circuitos	Electronic Workbench	1) Geda . 2) Oregano . 3) Xcircuit . 4) Gnome Assisted Electronics . 5) SPICE . 6) SPICE OPUS . 7) NG-SPICE .
Programas de dibujo de estructuras químicas	Chemdraw , Isisdraw	Xdrawchem .
Downloader and player for Olympus dictophone	Olympus DSS Player	???
Análisis de Mercados	MetaStock	???
Diseño de esquemas electrónicos	PCAD	1) Eagle . 2) Geda .
Emulador de osciloscopio	Winosillo	Xoscope .
Medida de la temperatura y voltajes sobre placa madre	MBMonitor, PCAlert	KHealthCare (KDE).
S.M.A.R.T-atributos y temperatura del disco Duro	Come on CD with mainboard, Active SMART	1) smartctl . 2) Hddtemp-0.3 . 3) IDEload-0.2 . 4) Smartsuite-2.1 . 5) Smartmontools . 6) Ide-smart . 7) Smartsuite .
Testeo de Memoria	SiSoft SANDRA	Memtest86 .
Programas para observar temperaturas, fanspeeds, etc	SiSoft SANDRA, SiSoft SAMANTHA	1) Ksensors . 2) Lm_sensors .

Para testeo y pruebas HDD	SiSoft SANDRA, SiSoft SAMANTHA	1) hdparm. 2) Bonnie++ . 3) IOzone . 4) Dbench . 5) Bonnie . 6) IO Bench . 7) Nhfsstone . 8) SPEC SFS . [Prop]
Para testeo y pruebas Video	Final Reality	1) X11perf. 2) Viewperf.
Control de Tiempo Real	SHA Sybera Hardware Access	DIAPM RTAI - Realtime Application Interface .
Simulador de Redes	???	1) NS .
Simulador de Redes neuronales biológicas	???	1) Xnbc .
"Sensor para LCD"	???	1) Sensors-lcd .
Visualizador para Electrocardiogramas	???	1) ecg2png .

10) Otros / Humor :)

Simulador Espacial	1) Openuniverse . 2) Celestia .	1) Openuniverse . 2) Celestia .
TV driver	-	RivaTV .
Sistemas, corriendo desde un CD sin instalarse (Live CD)	Imposible	1) Knoppix . 2) Cool Linux . 3) Blin . 4) DemoLinux . 5) DyneBolic . 6) Gentoo (live CD) . 7) Lonix . 8) Virtual Linux . 9) Bootable Business Card (LNX-BBC) . 10) ByzantineOS . 11) FreeLoader Linux . 12) MoviX . 13) Freeduc CD . 14) SuSE live-eval CD . 15) Freedom Linux . 16) Eagle Linux .
Herramientas de rescate boot diskette	Windows system diskette	1) Linux system diskette . 2) Tomsrtdt . 3) BanShee Linux .
Sistemas de montaje de Archivos	ext2fs (driver), explore2fs (programa) - ext2/3 bajo Windows	Linux-NTFS . (driver para el montaje de particiones NTFS)
Software Instalador y Desinstalador	InstallShield, WISE, GhostInstaller, Microsoft Installer - análogo del rpm	1) Rpm & frontends. 2) Urpm . 3) Apt & frontends (synaptic, ...). 4) Apt-rpm . (for RedHat, SuSE, ALT Linux, etc)

Software Instalador y Desinstalador desde archivos fuentes	Minimalist GNU For Windows	1) make install, make uninstall 2) CheckInstall . 3) Sinstall .
Sistema de Actualización	Windows Update	1) Ximian Red Carpet . 2) Red Hat Network . 3) MandrakeOnline . 4) SuSE YaST Online Update . 5) Caldera Volution Online . 6) Apt . 7) Gentoo ebuilds (portage). 8) Debian GNU/Linux package search . 9) Yum .
Certificaciones	MCSD, MCT, MCSE	1) Red Hat Certification . 2) Sair Linux and GNU Certification . 3) Linux Professional Institute Certification (LPIC) . 4) Linux+ . 5) Prometric . 6) VUE .
Emulador de Spectrum ZX	X128, Speccyal, SpecX, SpecEmu, UnrealSpeccy, ...	1) Xzx . 2) Glukalka . 3) Fuse . 4) ZXSP-X . 5) FBZX .
Máquinas Virtuales	VMWare para Windows	1) VMWare for Linux . [Prop] 2) Win4Lin . [Proprietario, \$89]. 3) Bochs . 4) Plex86 . 5) Uso modo Linux .
Trabajando con Palm	Escritorios Palm	1) Kpilot . 2) Jpilot .
Allows to carry on Palm .html files	iSilo	1) iSilo for Linux . 2) Plucker .
Optimización	WinBoost, TweakXP, Customizer XP, X-Setup, PowerToys, etc	Powertweak-Linux .
Bible	On-Line Bible, The SWORD	1) BibleTime (KDE) 2) Gnomesword (Gnome)
Iconos en el Escritorio	Explorer	1) Desktop File Manager. 2) Idesk .
Trabajando con Salvapantallas	Desktop properties	1) xset . 2) xlockmore . 3) xscreensaver . 4) kscreensaver .
Lugar para mantener los archivos removidos	Trash	1) Trash Can . 2) Libtrash .
Checkeando el disco duro	Scandisk	fsck -check or reiserfsck -check. Not needed with journaled file systems! (reiserfs, ext3, jfs, xfs)

De los sistemas GUI	Windows Explorer	Kde, Gnome, IceWM, Windowmaker, Blackbox, Fluxbox, ...
Windows 9x GUI	Windows 9x	Macrosoft Desktop Environment.
Windows XP GUI	Windows XP	XPde.
Sabores del Sistema	9x, NT, XP	RedHat, Mandrake, ALT, Knoppix, Debian, SuSE, Gentoo, Slackware, ...
Tácticas	FUD (Miedo, incertidumbre, duda)	Código Abierto! "Primero ellos no le hacen caso, entonces ellos se ríen de usted, entonces ellos se pelean, entonces usted gana".
Código Fuente del Kernel disponible	No	Claro!! :)
Intrépretes de Comandos	command.com :), cmd.exe, Windows Scripting Host, 4dos/4NT , Minimalist GNU para Windows	1) Bash . 2) Csh. 3) Zsh . 4) Ash. 5) Tcsh .
Emulador de Consola Linux	1) CygWin . 2) MKS Toolkit. 3) Bash apra Windows. 3) Minimalist GNU para Windows .	-
X Window System (XFree) emulador	XFree bajo CygWin	-
Emulador de Windows	-	1) Wine . (GUI: gwine , tkwine) 2) Transgaming WineX . (GUI: tqgui) 3) Crossover Office .
Sistema Operativo Libre	Microsoft Windows. (imaginate esto en Rusia el 95% de usuarios tiene una copia pirata de Windows :).	Linux - EL Sistema Operativo Libre!!
-	Nimda	Slapper .
-	Winch, klez, etc	No hay análogos
Puertas Traseras y llaves ocultas	Decidalo Usted Mismo :).	-
Easter eggs , posibilidades no documentadas	Logo con desarrolladores Windows, Doom en Excel 95, 3D-racing en Excel 2000, etc, etc...	-
The magazines	Windows Magazine	1) Linux Journal . 2) Linux Gazette . 3) Linux magazine . 4) Linux pratico (Italy).
-	Blue Screen Of Death (BSOD)	1) Kernel panic. 2) Screensaver "bsod" :).

A quien hay que maldecir cada vez que se encuentre un bug o defecto en el sistema	M\$, Bill Gates personalmente	1) Desarrolladores de las Distribuciones. 2) Toda la Gente de Linux y Linus Torvalds personalmente :). 3) Tu mismo y tus propias /dev/manos :)).
-	M\$.com	GNU.org , FSF.org
-	Windows.com	Linux.org
-	Bill Gates, "Road ahead"	Linus Torvalds, "Solo por Diversión" :).
-	Bill Gates, "Negocios @ la velocidad del pensamiento"	Richard M. Stallman, " El derecho a leer ".

Esta página esta liberada bajo la licencia [GNU FDL](#).

(c) [Fiodor Sorex](#) 2005 - 2007

(c) [Valery V. Kachurov](#), [Nesov Artem](#), 2002-2003

Traducción al español [Carlos M. Cárdenas F.](#)

GUIA DE CONFIGURACION DE AMAVIS-NEW

Ahora editaremos el archivo *amavis.conf* el cual copiamos a */etc*, este archivo esta dividido en varias secciones, en las cuales describiremos las opciones de configuración mas importantes y después presentaremos un archivo de configuración ejemplo.

Sección I: Configuración del demonio y del MTA

Aquí ajustaremos los valores de las variables `$daemon_group` y `$daemon_user` al nombre de usuario y grupo que creamos anteriormente. Además establecemos los valores de `$MYHOME` y `$TEMPBASE`, la dirección del home de amavis, así como las variables `$mydomain` y `$myhostname` con los valores que asignamos en el `main.cf` de Postfix:

```
$MYHOME = '/var/amavis';  
$mydomain = 'seguridad.unam.mx';  
$myhostname = 'forense.seguridad.unam.mx';  
$daemon_user = 'amavis';  
$daemon_group = 'amavis';  
$TEMPBASE = $MYHOME;
```

Como vemos en [3.1](#), Amavis necesita regresar por algún medio los mensajes que verifica y notificaciones necesarias a Postfix, esto se lo indicamos por medio de las variables `$forward_method` y `$notify_method`:

```
$forward_method = 'smtp:127.0.0.1:10025';  
$notify_method = $forward_method;
```

Podemos indicarle a Amavis, el número de procesos que leerán el pipe que el MTA mantiene con amavisd, este número podemos sacarlo de la línea que agregamos en `master.cf`:

```
smtp-amavis unix - - y/n - 2 smtp
```

Con esto, desde nuestro archivo de configuración podemos decirle a amavis, el número de procesos hijo a ejecutar, así como cuantas peticiones puede manejar cada hijo como máximo, así como el tiempo máximo que tiene el proceso hijo para terminar cada tarea, esto lo hacemos con los parámetros `$max_servers`, `$max_requests` y `$child_timeout` respectivamente:

```
$max_servers = 2;  
$max_requests = 10;  
$child_timeout=5*60;
```

Desde el archivo de configuración de amavis, también podemos especificar

parámetros que nos permitan realizar el análisis de los mensajes por medio de una herramienta antivirus, sin embargo esta característica no fue utilizada en este documento, de manera que deshabilitaremos esta característica con la siguiente línea:

```
@bypass_virus_checks_acl = qw( . );
```

Amavis necesita determinar, si un mensaje es local o no, o en otras palabras, si es mensaje es externo o no. Esto es muy útil para reducir el numero de notificaciones que podrían generarse por el correo local, esto si consideramos que localmente no se genera Spam para nosotros mismos =|. Esta configuración la especificamos en el parámetro *@local_domains_acl* de la siguiente manera:

```
@local_domains_acl=( ".$mydomain");
```

Sección II: Valores específicos para el MTA

Ahora como lo hemos manejado antes, tenemos que especificar a amavis los parámetros necesarios para que la comunicación con el MTA se realice con éxito, asignaremos el nombre el archivo socket que utilizara en la comunicación, así como el puerto y la interfaz que utilizara, esto por medio de los siguientes parámetros:

```
$unix_socketname = "$MYHOME/amavisd.sock";
```

```
$inet_socket_port = 10024;
```

```
@inet_acl = qw( 127.0.0.1 );
```

Sección III: Bitácora

La configuración en esta sección es muy sencilla, podemos especificarle a amavis si deseamos que la bitácora la maneje *SYSLOG* o si deseamos mandarla a un archivo de texto, para este ejemplo utilizamos las siguientes opciones:

```
$DO_SYSLOG = 0;
```

```
$LOGFILE = "$MYHOME/logs/amavis.log";
```

```
$log_level = 4;
```

Con el primer parámetro, amavis entenderá que deberá utilizar un archivo de texto como bitácora, la ruta de este archivo, esta indicada por el segundo parámetro. Si se quisiese llevar la bitácora por medio de syslog, el parámetro *DO_SYSLOG* debe ser establecido a 1. El parámetro *log_level* denota el nivel de detalle de la bitácora,

existen 6 niveles los cuales podemos usar en este parámetro:

0:

Mensajes de inicio/salida/falla, detección de virus.

1:

Argumentos pasados por el cliente, además de algunos mensajes interesantes.

2:

Salida del herramienta antivirus, tiempos.

3:

Servidor, cliente.

4:

Partes separadas.

5:

Detalles adicionales de depurado.

Sección IV: Notificaciones, destino, cuarentena

Ahora le indicaremos a amavis que hacer con el correo que sea clasificado como Spam, así como las posibles notificaciones a enviar por parte del MTA o por el mismo amavis al destino del mensaje. Existen varias opciones que podemos utilizar dependiendo del tipo de análisis, por ejemplo, podemos definir que se envíe una notificación al origen del mensaje, si se determino que este contenía algún virus en sus cuerpo, y otra acción para el origen del Spam, en este caso no es recomendable enviar una notificación al origen, de que su mensaje ha sido clasificado como Spam, debido a que no sabemos quien esta del otro lado, y podemos indicarle al Spammer información que no debería de conocer. Las posibles opciones a utilizar en el parámetro *final_spam_destiny* son:

D_PASS:

El mensaje será entregado aún sin importar la clasificación de su contenido.

D_DISCARD:

El mensaje no será entregado, y no se enviara ninguna notificación al origen del mensaje.

D_BOUNCE:

El mensaje no será entregado, y una notificación *non-delivery* será enviada al origen del mensaje por Amavis. Sin embargo no se enviara dicha notificación, si algún nombre de virus que se encuentra en el parámetro *\$viruses_that_fake_sender_re* se encuentra en el mensaje, o para aquellos mensajes que son de listas de correo (Precedencia: bulk, list o junk).

D_REJECT:

El mensaje no será entregado, el origen debería de ser notificado con una respuesta de rechazo permanente, o con una respuesta *non-delivery* desde el MTA. Para indicarle a nuestro filtro que el mensaje que ha sido clasificado como Spam no sea entregado, y que no se envíe ninguna notificación al origen del mensaje, utilizaremos la siguiente entrada:

```
$final_spam_destiny = D_DISCARD;
```

Amavis tiene la capacidad en enviar notificaciones al administrador de una posible alerta ya sea de detección de virus o de la recepción de Spam. Para esta ultima, el siguiente parámetro denota de qué dirección saldrán esas notificaciones:

```
$spam_admin = "spamalert1#1@forense.seguridad.unam.mx";
```

Sin embargo los reportes de las notificaciones pueden ser enviadas por otro usuario, con el parámetro siguiente, asignamos a *postmaster*:

```
$mailfrom_notify_spamadmin = "postmaster1#1@forense.seguridad.unam.mx";
```

Para los mensajes de cuarentena, nos es muy importante mantener la dirección de origen inicial, ósea, que amavis no modifique esta cabecera, para esto utilizamos este parámetro:

```
$mailfrom_to_quarantine = "";
```

Los mensajes que han sido clasificados como Spam, habría que colocarlos en cuarentena para un análisis posterior, para esto, nosotros elegimos enviar por correo el mensaje a una cuenta de usuario, para esto utilizamos el parámetro:

```
$spam_quarantine_to = "spam-quarantine1#1@forense.seguridad.unam.mx";
```

Si por algún motivo, el análisis de algún mensaje no se completo, una cadena puede ser concatenada en la cabecera de asunto, para hacer esta indicación, con la variable *\$undecipherable_subject_tag* configuramos este mensaje:

```
$undecipherable_subject_tag = '***UNCHECKED*** ';
```

Sección V: Administración por recipiente u origen

En esta sección, podemos definir algunas reglas para que aquellos usuarios que no requieran del filtrado tanto de correo spam, como de virus, puedan quedarse recibir su correo sin ningún problema. Existen parámetros como *%virus_lovers*, *@virus_lovers_acl* y *\$virus_lovers_re* donde podremos especificar que usuarios pueden recibir correo aún si este, este contenga algún virus. De igual manera, existe este tipo de configuración para Spam, con *%spam_lovers*, *@spam_lovers_acl*, *\$spam_lovers_re*. Esta configuración no se utilizó en este ejemplo, debido a las características del uso del servidor de correo.

Listas blancas

Son utilizadas para asegurar la entrega de los mensajes de un remitente el cual forma parte de estas listas, aun si el mensaje allí sido reconocido como Spam. Los mensajes que vengan de remitentes los cuales están en este tipo de listas, no serán editados con la etiqueta de *****POSIBLE SPAM*****, además de que algunas tareas como la cuarentena no aplicaran a estos. Un ejemplo de la declaración de listas blancas es el siguiente:

```
%whitelist_sender, @whitelist_sender_acl, $whitelist_sender_re
@whitelist_sender_acl = qw( .example.com );
```

Listas negras

Para los mensajes cuyo remitente se encuentre en este tipo de parámetro, el nivel de probabilidad de que sea Spam es automáticamente puesto en un valor alto, el resultado de esto es una clasificación como Spam automática y el mensaje será tratado como tal.

Uso de recursos

Aquí podemos asignar valores a las tareas de extracción y decodificación, para definir el número de archivos así como el nivel de recursión en la extracción de archivos. Los valores utilizados en este documento, se listarán en el archivo de configuración de muestra.

Programas externos, analizadores de virus

En esta sección podemos asignar la ruta en la cual se encuentran la mayoría de las herramientas, que instalamos al inicio de este capítulo, además de especificar una cadena de *PATH* que funciona para la localización de los programas externos a *amavis*.

```
$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';
```

GUÍA DE CONFIGURACIÓN DE ANTISPAM DE POSTFIX

Existen 4 diferentes formas de detección de Spam en Postfix:

1. Reglas de detección de clientes Spam:

Reglas que trabajan con la identidad del cliente. Cada regla es una lista asignada de una o más restricciones que pueden aceptar o rechazar un mensaje. Por ejemplo, podemos incluir una regla que rechace mensajes de una dirección IP en particular.

2. Parámetros de verificación de sintaxis:

Son parámetros que verifican el apego a los estándares actuales en la composición del mensaje. Debido a que varios Spammers no siguen al pie de la letra los estándares que rigen el correo electrónico, nuestro sistema puede estar configurado para rechazar mensajes que vienen de sistemas mal o

pobremente configurados.

3. Verificación de contenido:

Se puede realizar una verificación de las cabeceras y del cuerpo del mensaje por medio de expresiones regulares, las cuales nos indicarán un mensaje que probablemente sea Spam.

4. Clases de restricción:

Se pueden definir reglas complejas para la detección de clientes Spam por medio de clases de restricción. Estas permiten combinar restricciones en grupos para formar nuevas restricciones.

Cuando se configura Postfix con características Anti-Spam, también se puede especificar qué hacer con los mensajes clasificados como Spam. En general, Postfix puede rechazar los mensajes, separarlos en una cola diferente, o entregarlos a un filtro externo.

Reglas restrictivas contra el Spam

Postfix proporciona las siguientes reglas de restricción basadas en la información del cliente:

- smtpd_client_restrictions
- smtpd_helo_restrictions
- smtpd_sender_restrictions
- smtpd_recipient_restrictions

- `smtpd_data_restrictions`

Cada una corresponde a una etapa en una transacción por medio del protocolo SMTP. En cada etapa, el cliente proporciona piezas de información. Utilizando la información proporcionada por el cliente, Postfix aplica las restricciones que se le hayan configurado. En la siguiente imagen se muestra una conversación SMTP, podemos ver en que etapa encaja cada regla. Podemos ver que las reglas que mencionamos anteriormente las cuales nos permiten verificar las cabeceras y el cuerpo del mensaje, también se ilustran en estos pasos, estas reglas se discutirán posteriormente.



Por default, la configuración de reglas de restricción en Postfix (si no se especificaron algunas en `main.cf`) es:

```
smtpd_client_restrictions =  
smtpd_helo_restrictions =  
smtpd_sender_restrictions =  
smtpd_recipient_restrictions =  
permit_mynetworks, reject_unauth_destination
```

Esta configuración permite el relaying, sólo a aquellos equipos dentro de la red del servidor de correo, y rechazando todos los demás excepto aquellos equipos que envíen mensajes a uno de nuestros usuarios.

Una de estas reglas, las definimos en el `main.cf`, y fue la última línea de nuestro archivo:

smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname, reject_maps_rbl

El parámetro `permit_mynetworks` hará que la petición se realice cuando la dirección IP del cliente, se encuentra dentro del parámetro `mynetworks`, el segundo parámetro `reject_invalid_hostname`, rechazará la petición cuando el nombre del equipo indicado en el comando HELO es inválido. El último parámetro *reject_maps_rbl*, rechazará la petición cuando la dirección del cliente se encuentra listado en algún servidor de RBLs listado en el parámetro *maps_rbl_domains*, sin embargo la búsqueda inversa sobre un servidor de RBLs es una propiedad que hemos dejado desactivada.

Parámetros de verificación de sintaxis

Existen dos parámetros que requieren de un estricto apego a los estándares del correo electrónico. Declarando la regla:

`smtpd_helo_required = yes`

Implica que cada cliente tendrá que iniciar la conversación SMTP con el comando HELO/EHLO, descrito en el RFC 821 del SMTP. Así, cualquier cliente que no inicie apropiadamente el envío del mensaje, será rechazado por Postfix. Existe otro parámetro en el RFC 821, el cual dice que las direcciones deben de seguir un formato predeterminado, generalmente Postfix acepta direcciones que se asemejen al formato predeterminado, sin embargo si se especifica la regla:

`strict_rfc821_envelopes = yes`

Postfix rechazara cualquier intento de envío de un mensaje con una dirección con un formato incorrecto.

Verificación de contenido

La verificación de contenido es la última etapa en la que Postfix puede tomar una decisión sobre el destino del mensaje. Postfix ofrece 4 parámetros que nos permiten especificar el tipo de análisis a realizar:

header_checks:

Análisis de las cabeceras del mensaje.

mime_header_checks:

Análisis de las cabeceras MIME del mensaje.

nested_header_checks:

Análisis de las cabeceras de los datos adjuntos al mensaje.

body_checks:

Análisis del cuerpo del mensaje.

Cuando se especifica un parámetro, se indica la tabla de búsqueda en la que están las expresiones regulares a utilizar en el análisis del mensaje:

header_checks = regexp:/etc/postfix/header_checks

body_checks = regexp:/etc/postfix/body_checks

Un archivo ejemplo, el cual contenga expresiones regulares para evaluar las cabeceras del mensaje podría ser:

/Make Money/ REJECT

/VIAGRA/ REJECT

/Marketing/ REJECT

También se puede utilizar este tipo de verificación, para analizar los archivos adjuntos en el mensaje, por ejemplo, aquellos mensajes con ejecutables sospechosos, pueden ser evitados con la entrada:

/name ?="?.*1#1.(bat|com|dll|exe|hta|pif|vbs)"?/ REJECT

GUÍA DE CONFIGURACIÓN DE POSTFIX

La configuración de postfix se realiza por medio de dos archivos principales, el archivo **main.cf** y **master.cf**. Estos dos archivos se encuentran por default en **/etc/postfix**. A continuación se encuentran las opciones de configuración más importantes utilizadas para tu servidor de correo electrónico, tanto para el **main.cf** como para **master.cf** respectivamente.

PASO1.

El primer paso que darás es configurar en tu servidor la ruta de la cola de mensajes de postfix. Generalmente cuando postfix se ejecuta en un ambiente root esta se le da ser la raíz de postfix.

queue_directory = /var/spool/postfix

La ruta de todos los comandos de Postfix y los demonios (algunos de los cuales están listados en main.cf) están dadas por las siguientes líneas:

command_directory = /usr/sbin

daemon_directory = /usr/libexec/postfix

Cabe resaltar que la ruta que especifica la localización de los demonios, debe pertenecer a root. Un parámetro importante es el propietario de la cola de mensajes y de la mayoría de los demonios de Postfix:

mail_owner = postfix

PASO2.

Ahora debemos especificar el nombre del host, así como el nombre del dominio al que pertenece, en este caso tenemos:

myhostname = frijolito.utec.edu.sv

mydomain = utec.edu.sv

Cuando los usuarios envían o reciben correo a través de Postfix sin ningún dominio especificado, el parámetro **myorigin** especifica el dominio a concatenar a las cabeceras del mensaje. El valor por default es el siguiente:

myorigin = \$myhostname

También tenemos que indicarle a Postfix, por qué medio va a recibir mensajes, en este caso nos referimos a las interfaces activas del sistema con el parámetro:

inet_interfaces = all

PASO3.

El siguiente parámetro a configurar, es **mydestination**, este lista todos los dominios de los cuales Postfix va a aceptar la entrega o el envío de los usuarios locales, nuestra configuración es la siguiente:

mydestination = \$myhostname, localhost.\$mydomain, localhost

Además de recibir y enviar mensajes de usuarios locales, Postfix también puede reenviar correo a otros sistemas. Es muy importante restringir quien puede reenviar correo a través de nuestro sistema. Los sistemas en nuestra red deben de tener la posibilidad de reenviar correo, sin embargo no se necesita el mismo servicio a todo el mundo. Por default Postfix no es un **OpenRelay**, los parámetros

mynetworks_style y **mynetworks** determinan si otros sistemas pueden usar el nuestro para enviar correo. La configuración por default es permitir sólo aquellos equipos que estén conectados a la misma red que nuestro servidor. Nosotros hemos elegido limitar el *mail relay* sólo a la máquina local, con la siguiente opción:

mynetworks_style = host

PASO4.

Una de las líneas que agregaremos a nuestro archivo main.cf, es la que indica la existencia de Amavis-New, la cual es la siguiente:

content_filter = smtp-amavis:[127.0.0.1]:10024

Esto indica que Amavis-New trabajará sobre el puerto 10024 en la máquina local, que como explicaremos mas adelante, Postfix se encargará de enviar los mensajes a Amavis para su validación como Spam, y Amavis lo regresará a Postfix para su entrega final si es el caso. Además, le indicamos a Postfix en dónde se encuentra la tabla de aliases a utilizar:

Alias_database = hash:/etc/postfix/aliases

La última línea, indica algunas restricciones propias de Postfix que nos ayudarán a detener el Spam antes de pase a otra etapa dentro del proceso de los mensajes en el sistema, estas opciones las discutiremos mas adelante:

**smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname,
reject_maps_rbl**

Hasta ahora nuestro archivo de configuración *main.cf* luce de la siguiente manera:

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
mail_owner = postfix
myhostname = forense.seguridad.unam.mx
mydomain = seguridad.unam.mx
myorigin = $myhostname
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 500
mynetworks_style = host
relay_domains =
relayhost =
mail_spool_directory = /var/spool/mail
mailbox_command = /usr/bin/procmail
debug_peer_level = 2
debugger_command =
PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq
setgid_group = postdrop
html_directory = no
```

manpage_directory = /usr/local/man

sample_directory = /etc/postfix

readme_directory = no

content_filter = smtp-amavis:[127.0.0.1]:10024

ALias_database = hash:/etc/postfix/aliases

smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname,
reject_maps_rbl

GUÍA DE CONFIGURACIÓN DE SPAMASSASSIN

Esta sección no es la única en la cual podamos configurar nuestro SpamAssassin, ni la mas recomendable, sin embargo, podemos indicar las configuraciones básicas de SpamAssassin sobre Amavis. De los parámetros configurables en esta sección son los niveles en los cuales, SpamAssassin se basara para clasificar un mensaje como SPAM, posible Spam o lo que denomina HAM (correo que no es Spam), estos valores fueron establecidos a los siguientes valores:

\$sa_tag_level_deflt = -999;

\$sa_tag2_level_deflt = 3.0;

```
$sa_kill_level_deflt = 5.0;
```

El valor del parámetro `$sa_tag_level_deflt` nos indica que cualquier mensaje que tenga un puntaje arriba del indicado por este parámetro, se le agregaran las cabeceras de SpamAssassin, con el valor que le hemos asignado, aseguramos que cualquier mensaje contendrá estas cabeceras. El parámetro `$sa_tag2_level_deflt` nos indica que si un mensaje alcanza este puntaje, se agregara al asunto del mensaje, la cadena descrita por el valor del parámetro `$sa_spam_subject_tag` la cual en nuestro ejemplo tiene el siguiente valor:

```
$sa_spam_subject_tag = '***Posible SPAM*** ';
```

Este parámetro es también configurable en el archivo `local.cf` de SpamAssassin, sin embargo, el valor que contenga en `amavis.conf`, anulará el posible valor en el archivo de configuración `local.cf`. Los mensajes que caigan en este caso, llegaran al destinatario, sin embargo la cabecera de asunto le indicara al usuario la posibilidad de que sea un falso negativo o un falso positivo, será tarea del usuario clasificar este tipo de mensajes. El valor del parámetro `$sa_kill_level_deflt` nos indicara que con un mensaje que alcance este puntaje, este pasara a cuarentena (si es el caso) y se mandara la alerta correspondiente.

Ahora podemos iniciar nuestro filtro amavis con la opción

```
debug
```

, para ver en tiempo real, las tareas que realiza al iniciar:

```
# amavisd debug
```

Desde otra consola, podemos verificar que efectivamente esta trabajando como debería de ser, por el puerto 10024:

```
# $ telnet 127.0.0.1 10024
```

```
Trying 127.0.0.1...
```

Connected to 127.0.0.1.

Escape character is '^'].

220 [127.0.0.1] ESMTP amavisd-new service ready

GUÍA DE INTEGRACIÓN DE AMAVIS A POSTFIX

PASO1.

Ahora si tenemos que editar nuestro archivo *master.cf*, y agregar las siguientes líneas al final del archivo:

smtp-amavis Unix - - y/n - 2 smtp

-o smtp_data_done_timeout=1200

-o smtp_send_xforward_command=yes

-o disable_dns_lookups=yes

127.0.0.1:10025 inet n - y/n - - smtpd

-o content_filter=

-o local_recipient_maps=

-o relay_recipient_maps=

-o smtpd_restriction_classes=

-o smtpd_client_restrictions=

```
-o smtpd_helo_restrictions=  
-o smtpd_sender_restrictions=  
-o smtpd_recipient_restrictions=permit_mynetworks,reject  
-o mynetworks=127.0.0.0/8  
-o strict_rfc821_envelopes=yes  
-o smtpd_error_sleep_time=0  
-o smtpd_soft_error_limit=1001  
-o smtpd_hard_error_limit=1000
```

Las opciones *y/n* se deben de cambiar dependiendo si se desea que smtp y postfix trabajen en un ambiente chroot o no. Para las opciones aquí listadas, bastara con colocar la misma opción que las opciones ya existentes en ese archivo. Para cargar la configuración de Postfix al vuelo, ejecutamos el siguiente comando:

```
# postfix reload
```

y verificamos si realmente esta funcionando postfix, ahora sobre el puerto 10025 (Esto no significa que deje de funcionar por el 25):

```
$ telnet 127.0.0.1 10025
```

```
Trying 127.0.0.1...
```

```
Connected to 127.0.0.1.
```

```
Escape character is '^['.
```

```
220 forense.seguridad.unam.mx ESMTP Postfix
```

```
quit
```

```
221 Bye
```

```
Connection closed by foreign host.
```

Como vimos en [1.4](#), tenemos que indicarle a Postfix que reenvie todo el correo que recibe a amavis-new, (como lo muestra [3.1](#)) para una inspección basada en contenido, esto es con la siguiente línea en el archivo main.cf:

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

También podemos usar un comando en el shell para agregar esta línea:

```
# postconf -e 'content_filter=smtp-amavis:[127.0.0.1]:10024'
```

Esta opción afecta de manera global al sistema de entrada de Postfix (smtp y pickup), si se requiriese una configuración más selecta, la opción:

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

Debe ser proporcionada al servicio que se desee que realiza la inspección de contenido.

Otra opción interesante a analizar es la utilización del protocolo SMTP en vez de SMTP cuando Postfix envía mensajes a amavis, esto nos brinda la capacidad de contar con transacciones multi-sesión además de que las respuestas de status se generaran por recipiente. Para contar con esta funcionalidad, debemos modificar las siguientes líneas:

```
smtp-amavis Unix - - y/n - 2 lmt  
-o lmt_data_done_timeout=1200  
-o lmt_send_xforward_command=yes
```

Esto funciona en versiones recientes de Postfix, sin embargo existen 2 bugs en el código del cliente SMTP de Postfix, estos son al realizar un análisis del número de

puerto de SMTP y en la conversión de direcciones. Así que si se utiliza esta opción, es recomendable tener al día la versión de nuestro servidor Postfix.

Después de esto, cargamos la configuración de Postfix al vuelo con el comando antes visto.

Guía de Instalación de paquetes a utilizar para la implementación de un servidor de correo electrónico seguro con filtros Antispam y Antivirus basado en open source.

Para la instalación de los paquetes que vamos a necesitar no esta demás mencionar que todas las guías están basadas en la distribución GNU/LINUX DEBIAN 4.0 ETCH para el cual instalaremos los siguientes paquetes que son de mucha importancia para la implementación del servidor de correo electrónico con filtros antivirus y Antispam:

Paquetes a instalar:

Cyrus-22 imapd

Cyrus-22pop3d

Cyrus-22docs

Postfix

Pcre

ClamAV (ANTIVIRUS)

Amavis-new

Spamassassin

Antes de instalar los paquetes aquí van unos tips que ahorrara tiempo en la búsqueda de los paquetes y sus instalaciones.

- ✓ Introdúctete en modo consola con la combinación de teclas ctrl+alt+f3
- ✓ Una vez estando en modo consola entraras no con tu usuario común sino que

con el superusuario root después de ello montaras el CD-ROM para crear el índice de paquetes que tenemos en nuestros discos de debían con el siguiente comando `apt-cdrom add` y posteriormente a ello te pedirá que introduzcas el CD o DVD en la bandeja y presiona ENTER y repetimos este paso hasta que se te terminen los tres DVD de debían 4.0 etch.

- ✓ Luego te doy una herramienta muy fácil para instalar paquetes pero te sugiero que la utilices solo para ver el nombre exacto de los archivos para instalarlos, esta herramienta es APTITUDE cuando estés en modo consola digita `APTITUDE` y se te desplegara una grafica similar a la de DOS donde te aparecerán diferentes opciones así como paquetes nuevos, paquetes instalados, paquetes no instalados, paquetes virtuales solo tienes que poner tu mirada fija en el nombre de los archivos y no tendrás ningún problema para instalarlos.
- ✓ Después de hacer eso presiona la tecla Q para salir de APTITUDE, ahora que estas de nuevo en modo consola tienes que digitar los siguientes comandos para poder instalar cada uno de los paquetes que vas a necesitar el comando es `apt-get install` para instalar y `apt-get remove` para desinstalar paquetes.
- ✓ Una recomendación que te propongo es que desinstales por completo EXIM-4 para que no vayas a tener ningún conflicto durante la configuración de tu servidor de correo electrónico en GNU/LINUX.

INSTALACIÓN DE CYRUS

1. En modo superusuario claro esta en modo consola digita el siguiente comando, `apt-get install cyrus-22 imapd` y presionas enter.
2. Luego de eso te pedirá si estas de acuerdo en instalar el paquete que has

seleccionado te da la opción S/N solo presionas S y das enter y empieza el proceso de instalación de cyrus-22 imapd.

3. Ahora que ya tienes instalado cyrus-22 imapd repite el proceso anterior para instalar cryrus-22 pop3d, cyrus-22 docs

INSTALACIÓN DE POSTFIX

1. En modo superusuario y en modo consola digita el siguiente comando: apt-get install postfix y presionas enter.
2. Luego de esto te pedirá si estas de acuerdo en instalar el paquete que has seleccionado te da la opción S/N presionas S y das enter en tu teclado.
3. Después empieza el proceso de instalación de postfix y después de ello ya tienes listo postfix.

INSTALACIÓN DE PCRE PARA POSTFIX

1. En modo superusuario y en modo consola digita el siguiente comando: apt-get install PCRE ojo aquí fíjate bien y respeta las letras mayúsculas y presionas enter.
2. Luego te pedirá si estas de acuerdo en instalar el paquete que seleccionaste da la misma opción S/N y como tú ya sabes presionas S y das enter a tu teclado.
3. Ahora bien hay algo diferente te dice que hubo un problema y que tienes que visitar apt-update o utilizar el comando
-fix-missing? Te recomiendo de utilices el ultimo por si no tienes conexión a internet

4. Ahora tendrás de digitar el comando `apt-get install PCRE --fix-missing` y presionas enter y continuas con el procedimiento normal y tendrás instalado PCRE en tu debían

INSTALACIÓN DE CLAMAV (ANTIVIRUS)

1. Si te encuentras todavía en modo superusuario vamos a hacer el mismo procedimiento digitaras el comando: `apt-get install Clamav` y presionas enter
2. Luego te pedirá si estas de acuerdo en instalar el paquete que seleccionaste da la misma opción S/N y como tú ya sabes presionas S y das enter a tu teclado.
3. Como siempre empieza el proceso de instalación con el DVD indicado y que paso ahora ya tienes antivirus instalado en tu debían

INSTALACIÓN DE AMAVIS-NEW

1. En modo superusuario y en modo consola digita el siguiente comando: `apt-get install postfix` y presionas enter.
2. Luego te pedirá si estas de acuerdo en instalar el paquete que seleccionaste da la misma opción S/N y como tú ya sabes presionas S y das enter a tu teclado.
3. Ahora tienes instalado en tu debían un scanner para tu servidor de correo.

INSTALACIÓN DE SPAMASSASSIN

1. Como tu te podrás imaginar estamos por instalar el filtro Antispam para tu servidor de correo para realizarlo tendrás que hacer lo que hasta el momento ya te aburraste de hacer y es digitar el comando: apt-get install Spamassassin presionas enter en tu teclado
2. Se te pide el famoso S/N presionas S y presionas enter
3. Ahora tienes instalados los paquetes necesarios para poder configurar tu servidor de correo electrónico con filtros antivirus y Antispam en una distribución GNU/LINUX