# UNIVERSIDAD TÉCNICA DE COTOPAXI


## CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

## TEMA: "SERVICIOS Y SEGURIDADES PARA UNA INTRANET BAJO PLATAFORMA LINUX ENTERPRISE 3.0 EN LA EMPRESA AGLOMERADOS COTOPAXI S.A".

*Tesis de Grado previa la obtención del Título de Ingeniero en Informática y Sistemas Computacionales*

**DIRECTOR DE TESIS:**

Ing. Tito Recalde Chávez

**POSTULANTES:**

Bustillos Venegas Juan Carlos

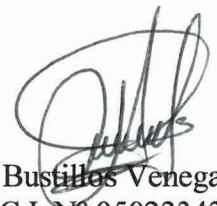
Herrera Panchi Guido Raúl

**LATACUNGA – ECUADOR**

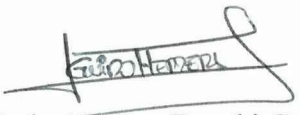
2007

# AUTORÍA

Las ideas, opiniones y comentarios en este documento son de exclusiva responsabilidad de los autores, egresados: Bustillos Venegas Juan Carlos y Herrera Panchi Guido Raúl.



Egdo. Bustillos Venegas Juan Carlos
C.I. N° 050233433-7



Egdo. Herrera Panchi Guido Raúl
C.I. N° 050251053-0

# CERTIFICACIÓN

Cumpliendo con lo estipulado en el Capítulo IV, Art. 9, Literal f., del Reglamento del Curso Preprofesional de la Universidad Técnica de Cotopaxi, informo que el grupo de postulantes conformado por los señores egresados. Juan Carlos Bustillos Venegas y Guido Raúl Herrera Panchi, han desarrollado su trabajo de Investigación de Grado, de acuerdo al planteamiento formulado en el Plan de Tesis:

1. El trabajo alcanza los objetivos propuestos y comprueba la verificación de los mismos.

2. La tesis aporta con propuestas y estrategias válidas orientadas hacia el desarrollo de la Empresa Aglomerados Cotopaxi S.A.

En tal virtud de lo mencionado anteriormente, considero que el grupo se encuentra apto para presentarse a la Defensa del Trabajo de Tesis: **"SERVICIOS Y SEGURIDADES PARA UNA INTRANET BAJO PLATAFORMA LINUX ENTERPRISE 3.0 EN LA EMPRESA AGLOMERADOS COTOPAXI S.A".**

Latacunga julio del 2007.

.....
Ing. Tito Recalde Chávez
**DIRECTOR DE TESIS**

# AGRADECIMIENTO

Este trabajo de investigación esta dedicado a mi familia, quienes siempre me han apoyado y me han ayudado a superarme día a día en especial a mis padres Raúl y Enma; además a la nueva personita que entró a formar parte de mi vida mi pequeño Mathy…

**GUIDO RAÚL**

Este trabajo de investigación lo dedico a mi familia en especial a mi esposa Catalina, mi hija Katty y mis padres, pues ellos son los gestores de este logro alcanzado, quienes me brindaron todo su apoyo, comprensión, la fuerza necesaria para culminar y alcanzar este título.

**JUAN CARLOS**

# DEDICATORIA

El siguiente proyecto de tesis no pudo haberse cristalizado sin la ayuda y colaboración de nuestras familias, quienes con su apoyo nos impulsaron a conseguir nuestras metas y seguir adelante.

También queremos hacer público nuestro agradecimiento a tan querida Alma Mater Universidad Técnica de Cotopaxi, quien nos acogió en su seno y nos abrió las puertas para forjarnos como profesionales útiles a la sociedad.

A la empresa Aglomerados Cotopaxi S.A, por permitirnos encontrar en ella toda la colaboración y confianza que nos permitieron desarrollar e implementar este proyecto, en especial al Ing. Ramiro Velásquez Jefe del Departamento de Sistemas, por apoyarnos en la realización del proyecto.

**JUAN – GUIDO**

# ÍNDICE GENERAL


| CONTENIDO | PÁG. |
|---|---|
| Portada..... | i |
| Página de responsabilidad de autoría..... | ii |
| Certificación del Director de Tesis..... | iii |
| Dedicatoria ..... | iv |
| Agradecimiento..... | v |
| Índice General..... | vi |
| Índice de Tablas..... | xii |
| Índice de Gráficos..... | xiii |
| Índice de Anexos..... | xvi |
| Resumen..... | xvii |
| Abstract..... | xix |
| Certificación de Abstract ..... | xxi |
| Introducción..... | 1 |

**CAPITULO I**

**FUNDAMENTO TEÓRICO**

| | | |
|---|---|---|
| 1.1 | Empresa Aglomerados Cotopaxi S.A..... | 3 |
| 1.1.1 | Generalidades..... | 3 |

**CONTENIDO** PÁG.


1.1.2 Descripción de la empresa..... 4

1.1.2.1 Historia..... 4

1.1.2.2 Infraestructura Funcional..... 5

1.1.2.3 Situación Económica..... 7

1.1.2.4 Servicios de la Empresa..... 8

1.2 Sistemas Operativos..... 8

1.2.1. Historia de los Sistemas Operativos..... 8

1.2.2 Clasificación de los Sistema Operativos..... 11

1.3 Linux..... 14

1.3.1 Reseña Histórica..... 14

1.3.2 Concepto de Linux..... 16

1.3.3 Linux en el Mundo..... 17

1.3.3.1 Sistema Operativo..... 18

1.3.3.2 Linux es software libre..... 19

1.4 Intranets..... 20

1.4.1 Generalidades..... 20

1.4.2 Concepto de Intranet..... 20

1.4.3 Linux como Servidor de Intranet..... 21

1.5 Servicios de Linux..... 22

1.5.1 Servidor de Archivos..... 23

1.5.2 Proxy Server..... 23

**CONTENIDO** **PÁG.**


1.5.3 Web Server, FTP Server y DNS Server..... 24

1.5.3.1 Tipos de Servidores DNS..... 24

1.5.4 Mail Server..... 25

1.6 Firewall y Seguridad en Internet..... 27

1.6.1 Generalidades..... 27

1.6.2 Firewalls..... 28

1.6.2.1 Beneficios de un Firewall en Internet..... 29

1.6.2.2 Bases para el Diseño Decisivo del Firewall..... 32

1.6.2.3 Políticas del Firewall..... 32

1.6.2.4 Política Interna de Seguridad..... 33

1.6.2.5 Componentes del Sistema Firewall..... 34

1.6.2.6 Uso de Iptables..... 34


## CAPITULO II

## TRABAJO DE CAMPO


2.1 Análisis e Interpretación de Resultados..... 37

2.2. Análisis FODA..... 38

2.3 Estudio de Procedimientos..... 39

2.4 Elaboración de Tablas..... 40

2.5 Análisis de Resultados..... 40

2.6 Interpretación de Resultados..... 41

**CONTENIDO** **PÁG.**

2.7 Comprobación de Hipótesis..... 54

2.7.1 Verificación de Hipótesis..... 54

2.7.2 Enunciado..... 54

2.7.3 Conclusión..... 55

## CAPITULO III

## PROPUESTA

3.1. Desarrollo de la propuesta..... 56

3.1.1 Tema..... 56

3.1.2 Presentación..... 56

3.1.3 Justificación..... 57

3.1.4 Objetivos..... 58

3.1.4.1 Objetivo General..... 58

3.1.4.2 Objetivos Específicos..... 59

3.1.5 Fundamentación..... 59

3.1.6 Desarrollo de la Propuesta..... 60

3.1.6.1 Servidor de Red TCP/IP ..... 64

3.1.6.1.1 Configuración de la Tarjeta RED TCP/IP..... 65

3.1.6.1.2 Seguridad de la Red..... 69

3.1.6.2 Servidor de Correo Electrónico (Sendmail)..... 69

3.1.6.2.1 Archivo de Configuración..... 70

**CONTENIDO** **PÁG.**

3.1.6.2.2 Seguridad para Sendmail..... 76

3.1.6.3 Configuración de Webmail..... 77

3.1.6.3.1 Instalación y Configuración de Software Webmail..... 79

3.1.6.3.2 Seguridad Antivirus para Sendmail y Webmail..... 84

3.1.6.4 Servidor Samba..... 94

3.1.6.4.1 Configuración de Samba..... 95

3.1.6.5 Servidor de Páginas WEB..... 101

3.1.6.5.1 Configurando el Servidor Apache..... 101

3.1.6.6 Servidor DNS..... 103

3.1.6.6.1 Configuración del DNS o BIND..... 103

3.1.6.7 Servidor Proxy ..... 108

3.1.6.7.1 Configuración del Servidor Proxy..... 108

3.1.6.7.2 Seguridad para el Servidor Proxy..... 156

3.1.6.8 Configuración de Firewall..... 157

**CAPITULO IV**

**CONCLUSIONES Y RECOMENDACIONES**

4.1 Conclusiones..... 160

4.2 Recomendaciones..... 161

BIBLIOGRAFÍA..... 163

GLOSARIO DE TÉRMINOS..... 168

**CONTENIDO** **PÁG.**

GLOSARIO DE SIGLAS..... 175

ANEXOS..... 179

# ÍNDICE DE TABLAS

**TABLA** **PÁG.**

Tabla 2-1: Capacitación en el manejo del Sistema..... 41

Tabla 2.2: Conocimiento del Sistema..... 42

Tabla 2.3: Información Confidencial..... 43

Tabla 2.4: Sistema que Brinda Mayor Seguridad..... 44

Tabla 2.5: Servicios Informáticos Satisfactorios..... 45

Tabla 2.6: Deficiencias de Equipo Causa de Problemas..... 46

Tabla 2.7 Conocimiento de Linux..... 47

Tabla 2.8: Utilizar Linux es Ventajoso..... 48

Tabla 2.9: Ventajas de Linux..... 50

Tabla 2.10: Linux, Mayor Control a la Información..... 51

Tabla 2.11: Servicios del Servidor Web..... 52

Tabla 2.12: Características de Linux Linux..... 53

# ÍNDICE DE GRÁFICOS

**GRÁFICOS** **PÁG.**

Gráfico 1.1: Test de Funcionamiento de SMTP..... 26

Gráfico 1.2: Test de Funcionamiento de POP..... 27

Gráfico 1.3: Funcionamiento Firewall..... 35

Gráfico 2.1: Capacitación en el Manejo del Sistema..... 41

Gráfico 2.2: Conocimiento del Sistema..... 42

Gráfico 2.3: Información Confidencial..... 43

Gráfico 2.4: Sistema que Brinda Mayor Seguridad..... 45

Gráfico 2.5: Servicios Informáticos Satisfactorios..... 46

Gráfico 2.6: Deficiencia de Equipo Causa de Problemas..... 47

Gráfico 2.7: Conocimiento de Linux..... 48

Gráfico 2.8: Utilizar Linux es Ventajoso..... 49

Gráfico 2.9: Ventajas de Linux..... 50

Gráfico 2.10: Linux, Mayor Control a la Información..... 51

Gráfico 2.11: Servicios del Servidor Web..... 52

Gráfico 2.12: Características de Linux..... 53

Gráfico 3.1: Configuración Archivo /etc/xinetd/imap..... 78

Gráfico 3.2: Configuración Archivo /etc/xinetd/d/imap..... 79

Gráfico 3.3: Verificación de Paquetes Instalados..... 80

**GRÁFICOS** **PÁG.**

Gráfico 3.4: Configuración Archivo /etc/mail/sendmail.mc..... 94

Gráfico 3.5: Configuración Archivo /etc/xinetd.d/swat..... 95

Gráfico 3.6: Configuración Archivo /etc/xinetd.d/swat ..... 96

Gráfico 3.7: Validación de Usuario Samba..... 96

Gráfico 3.8: Pantalla de Bienvenida Samba..... 97

Gráfico 3.9: Edición de Archivos para Samba..... 97

Gráfico 3.10: Edición Parámetros Globals..... 98

Gráfico 3.11: Guardar Cambios de la Configuración..... 98

Gráfico 3.12: Edición Parámetros Shares..... 99

Gráfico 3.13: Edición Parámetros Shares..... 99

Gráfico 3.14:Verificar Estado de Servicios Samba..... 100

Gráfico 3.15: Edición Archivo /etc/samba/smb.conf..... 100

Gráfico 3.16: Configuración Archivo /etc/httpd/conf/httpd.conf..... 102

Gráfico 3.17: Configuración Archivo /etc/httpd/conf/httpd.conf ..... 102

Gráfico 3.18: Edición Archivo /etc/named.conf..... 104

Gráfico 3.19: Edición Archivo /etc/named..... 104

Gráfico 3.20: Edición Archivo /etc/named.conf..... 105

Gráfico 3.21: Edición Archivo /var/named/192.168.3.zone..... 105

Gráfico 3.22: Edición Archivo /etc/named.conf..... 106

Gráfico 3.23: Edición Archivo /etc/named.conf..... 107

Gráfico 3.24: Verificar directorio Cache..... 156

**GRÁFICOS** **PÁG.**

Gráfico 3.25: Definir Usuarios para SQUID..... 156

# ÍNDICE DE ANEXOS

**ANEXO** **PÁG.**

Anexos..... 179

Anexo 1: Anteproyecto..... 180

Anexo 2: Encuesta..... 211

Anexo 3: Control de Usuarios..... 214

Anexo 4: Servidor..... 217

# RESUMEN

El siguiente proyecto de tesis **"SERVICIOS Y SEGURIDADES PARA UNA INTRANET BAJO PLATAFORMA LINUX ENTERPRISE 3.0 EN LA EMPRESA AGLOMERADOS COTOPAXI S.A",** en su totalidad fue desarrollado en la empresa Aglomerado Cotopaxi S.A., con la finalidad de brindar y mejorar los servicios proporcionados al cliente, de esta manera hacer mas fácil y eficiente el trabajo de los empleados.

Para lograr este objetivo se utilizo software con licencias de tipo GNU como lo es LINUX RED HAT ENTERPRISE 3.0, sistema operativo que durante los últimos años ha despertado el interés de los administradores, escogiéndolo como una de las mejores opciones, ya sea por su costo reducido sus ventajas y por ser un sistema que proporciona estabilidad en el manejo de información.

Entre los servicios que se configuró en el servidor de Aglomerado Cotopaxi S.A., podemos mencionar los siguientes:

- Un servidor de conexión a Internet con servicios como: ssh, ftp, e-mail
- Servidor de firewall que protegerá de intrusos externos mediante el uso de la definición de iptables
- Servidor de archivos para clientes Windows XP, W98, etc., a través del servicio samba

- Un servidor de correo utilizando sendmail y webmail
- Un servidor web con el uso de apache

Todas estas configuraciones se realizaron con la finalidad de mejorar el rendimiento y facilitar las tareas de los usuarios a través de los servicios que presta nuestro servidor; el siguiente documento además es una guía de administración y manejo que facilitará el trabajo del administrador o encargado de la red.

Con el manual de usuario presentado en el siguiente proyecto de tesis el administrador de la red estará en la capacidad de actualizar y dar mantenimiento al servidor de la intranet, configurando el mismo de acorde a las necesidades que vayan surgiendo en la empresa, en el documento se detalla de forma gráfica como se deben configurar los distintos servicios del servidor.

# ABSTRACT

The following thesis project "SERVICES AND SECURITIES FOR an Intranet UNDER PLATFORM 3,0 LINUX ENTERPRISE IN THE COMPANY AGLOMERADOS COTOPAXI S.A., in its totality was developed in the company Aglomerados Cotopaxi S.A., and it was developed to improve the services that it lend the internal consover.

In order to obtain this objective I used software of licenses GNU as LINUX; NETWORK HAT ENTERPRISE 3,0, during the last years, it indicates that every day more administrators of systems will choose Linux, by its reduced cost their advantages and it is a stable system. Between the services formed in our servant we can mention the following:

A connection service to Internet with services like: ssh, FTP, email. Firewall service it will protect of external intruders by means of the use of the definition of iptables. File service it is for consumers Windows XP, W98, etc., it is through service samba. A mail use sendmail and webmail. A Web service with the apache use service. These are some of the services that were formed in the Aglomerados Cotopaxi S.A. service, and it made with the purpose of to improve and to facilitate the tasks of the internal consumer through of the services; that give our service, following document in addition is a guide of administration and handling it will facilitate the job of the administrator.

# CERTIFICACIÓN DE TRADUCCIÓN

Yo, VERÓNICA ALEXANDRA LEMA PURUNCAJAS, portador de la Cédula de Identidad N° 0502570229, en calidad de Profesional del Área de Inglés, tengo a bien **CERTIFICAR:** que los egresados de la Universidad Técnica de Cotopaxi, señores: Juan Carlos Bustillos Venegas y Guido Raúl Herrera Panchi, han realizado la debida corrección con mi persona del Abstrac de la Tesis de Grado con el Tema: **"SERVICIOS Y SEGURIDADES PARA UNA INTRANET BAJO PLATAFORMA LINUX ENTERPRISE 3.0 EN LA EMPRESA AGLOMERADOS COTOPAXI S.A"** el cual se encuentra bien estructurado, por lo que doy fe del presente trabajo.

Por tal motivo faculto a los peticionarios hacer uso del presente certificado como a bien lo consideren.


.....
Lic. Verónica Lema Puruncajas

Latacunga julio 2007

# INTRODUCCION

El avance tecnológico ha provocado que día a día las compañías incrementen su competitividad, hoy las empresas destinan gran cantidad de presupuesto a mejorar su tecnología, de esta manera mejorar los servicios y la atención hacia el cliente; nuestra investigación es una recopilación que pretende demostrar porque las empresas han depositado la confianza en Linux, demostrando de una manera práctica como es el funcionamiento de este Sistema Operativo y las bondades que ofrece.

El presente trabajo de investigación esta establecido en cuatro capítulos, distribuidos de la siguiente manera:

El capitulo I, concerniente a la fundamentación teórica, se hace referencia a una breve descripción de la empresa Aglomerados Cotopaxi S.A., además de una breve historia de Sistemas Operativos, como también se describe las funcionalidades y los servicios que ofrece Linux para una Intranet, conocimientos científicos de vital importancia para fundamentar adecuadamente la presente propuesta investigación.

En el capitulo II, referente al trabajo de campo, se realizo primeramente un diagnóstico para conocer como se encontraba en esos momentos el funcionamiento del sistema, a través de la aplicación de la técnica FODA;

posteriormente la tabulación de los datos, así como su presentación por medio de gráficas de pastel, interpretación y análisis de los resultados obtenidos de la encuesta realizada al personal del departamento de sistemas y procesamiento de datos, los mismos que sirvieron de base para la comprobación de la hipótesis planteada.

En el capitulo III, relacionado con la propuesta de investigación, se presenta de manera detallada como se configuraron los servicios de la intranet, con sus respectivas seguridades.

En el capitulo IV, se enuncia las conclusiones y recomendaciones finales del trabajo de investigación, siendo estas resultados del trabajo de campo realizado en la empresa Aglomerados Cotopaxi S.A.

Finalmente, en la parte referente a los anexos se incluyen el anteproyecto de tesis y los instrumentos de investigación aplicados al personal involucrado directamente con el manejo técnico del sistema.

El presente trabajo de investigación es un aporte que entrega el grupo investigador a la empresa Aglomerados Cotopaxi S.A., relacionado a las seguridades que hoy en día es uno de los principales aspectos a considerarse dentro de la administración de los sistemas informáticos, que propenden a la optimización del manejo del recurso tecnológico por parte de los involucrados.

# CAPITULO I

# FUNDAMENTO TEORICO

## 1. EMPRESA AGLOMERADOS COTOPAXI S.A.

### 1.1. INTRODUCCIÓN

Aglomerados Cotopaxi S.A. pertenece a la corporación industrial-forestal maderera más importante del Ecuador. Con un patrimonio forestal propio, modernas instalaciones con tecnología de punta y un personal de alto nivel, capacitado para satisfacer al cambiante mercado mundial.

Aglomerados Cotopaxi S.A. fabrica y comercializa productos terminados de alta calidad como: tableros de aglomerado, tableros de MDF, tableros recubiertos, madera aserrada.

Generando más de 700 empleos directos y 2000 empleos indirectos, Aglomerados Cotopaxi S.A. ayuda al desarrollo industrial, productivo y económico del Ecuador inyectando en el mercado local productos de alta calidad a precios competitivos. La creciente actividad exportadora garantiza la continuidad de la empresa y deja en alto el nombre del Ecuador en más de 20 países que reciben nuestro producto como: Colombia, Venezuela, Perú, Panamá, Japón, África entre otros.

## 1.1. DESCRIPCIÓN DE LA EMPRESA

### 1.1.1. HISTORIA

Aglomerados Cotopaxi S.A. (ACOSA) fue fundada en el año de 1978 por un grupo de visionarios madereros liderados por el Sr. Juan Manuel Durini Palacios, quien había incursionado en la industria forestal maderera 30 años antes.

En el año 1979, Aglomerados Cotopaxi S.A (ACOSA), ubicada en la Parroquia Tanicuchi en el sector de Lasso, inicia su producción introduciendo en el Ecuador el tablero de partículas aglomeradas (Acoplac) con una moderna línea de producción, con tecnología de punta, importada desde Alemania.

La comercialización de su producto fue enfocada al mercado nacional e internacional como fue el, área andina, vendiendo desde el inicio el total de su producción a precios muy competitivos y con una calidad superior a la existente en el mercado. En menos de 10 años Aglomerados Cotopaxi S.A. (ACOSA) logra comercializar su producto en cuatro continentes y llegar con el mismo a países tan lejanos como Japón y Corea, y a mercados tan exigentes como Estados Unidos.

Como resultado de este éxito y devolviendo la confianza y el trabajo al país, Aglomerados Cotopaxi S.A. (ACOSA) expande sus operaciones industriales a fines del año de 1979 con la incorporación de la primera línea para recubrimiento

de tableros, dando así mayor valor agregado a sus productos y expandiendo la gama de los mismos según los requerimientos del mercado nacional e internacional.

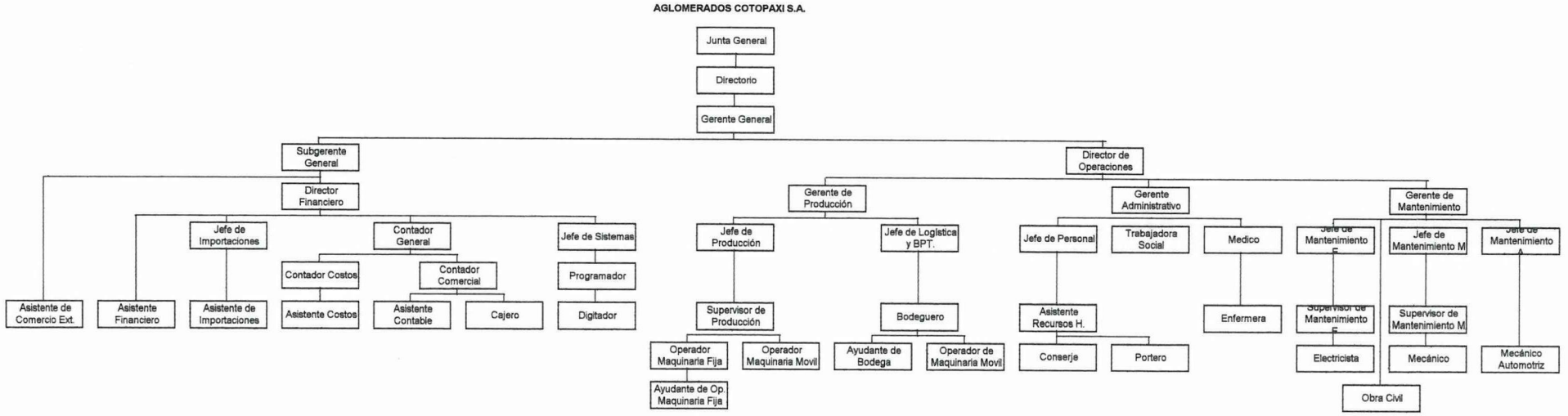
Por la alta demanda de productos de calidad, elaborada con madera sólida y queriendo aprovechar al máximo el recurso forestal Aglomerados Cotopaxi S.A. (ACOSA), en el año de 1985, actividad por la cual monta el primer aserradero para la producción de piezas de madera sólida de pino, trabajando en esta por diez años consecutivos, hasta el año de 1995 cuando es reemplazado por un Aserradero Industrial con el cual se garantiza la producción continua, con calidad constante y volúmenes importantes.

Bajo este marco operacional, que engloba no solo la industria sino también al recurso maderero, Aglomerados Cotopaxi S.A. (ACOSA) se consolida como la empresa maderera más grande del Ecuador y con sus empresas hermanas Endesa, Botrosa, Setrafor, Onix, Edimca, y la Fundación Forestal Juan Manuel Durini, forman uno de los grupos industriales madereros más importantes de América.

### 1.1.2. INFRAESTRUCTURA FUNCIONAL.

Aglomerados Cotopaxi S.A. cuenta dentro de su organización con varias áreas, departamentos y líneas de producción, como se muestra en el Organigrama.

# GRAFICO Nº 1.1: INFRAESTRUCTURA FUNCIONAL




| FECHA DE ELABORACION | ELABORADO POR: | REVISADO POR: |
|---|---|---|
| 15 DE JULIO DEL 2005 | Juan Carlos Bustillos<br>Guido Raul Herrera | Lcdo. Marco Cabrera R.<br>Jefe de Personal<br>Aglomerados Cotopaxi |

### 1.1.3. SITUACIÓN ECONOMICA

Aglomerados Cotopaxi S.A. es una compañía líder en la industria de tableros de partículas (Aglomerado), de fibra de densidad media (MDF) y de piezas aserradas de pino. Estos productos se comercializan en el país, a través de nuestro distribuidor exclusivo Edimca Quito y Edimca Guayaquil y su amplia red de distribuidores en todo el país.

En el mercado de exportación tiene clientes en Perú, Colombia, México, Panamá, Cuba, Estados Unidos, Venezuela, Brasil, Taiwán, Japón, Bolivia, Uruguay, Puerto Rico, Canadá, Chile, España, Honduras, El Salvador, entre otros.

Para proveer a los clientes con productos que tengan los más altos estándares internacionales de calidad, Aglomerados Cotopaxi S. A. cuenta con personal calificado y motivado, tecnología avanzada y suministro estable de materia prima.

Entre los productos que Aglomerados Cotopaxi S. A. fabrica y comercializa están los siguientes:

- Acoplac
- Pacoplac
- Duraplac
- Madeplac

- Fibraplac
- Finger joint
- Pinoplac
- Madera aserrada.

### 1.1.4. SERVICIOS DE LA EMPRESA

Aglomerados Cotopaxi S.A., empresa preocupada siempre por el esfuerzo y la dedicación de su personal busca siempre mantener motivado a su personal, para lo cual proporciona algunos servicios los mismos que son necesarios para cumplir sus metas y objetivos trazados, estos servicios son otorgados a todo el personal administrativo y operativo de su planta industrial, entre ellos tenemos: Transporte, Alimentación (Refrigerios – Almuerzos, Meriendas), Servicios médico y odontológico, Trabajo Social, Uniformes y dotación de seguridad, Ventas de productos y materiales de desperdicio, Préstamos y anticipos, Capacitación

## 1.2. SISTEMAS OPERATIVOS

### 1.2.1. HISTORIA DE LOS SISTEMAS OPERATIVOS

Para tratar de comprender los requisitos de un Sistema Operativo y el significado de las principales características de un Sistema Operativo contemporáneo, es útil considerar como han ido evolucionando éstos con el tiempo.

A finales de los 40's el uso de computadoras estaba restringido a aquellas empresas o instituciones que podían pagar su alto precio, y no existían los sistemas operativos. En su lugar, el programador debía tener un conocimiento y contacto profundo con el hardware, y en el infortunado caso de que su programa fallara, debía examinar los valores de los registros y paneles de luces indicadoras del estado de la computadora para determinar la causa del fallo y poder corregir su programa, además de enfrentarse nuevamente a los procedimientos de apartar tiempo del sistema y poner a punto los compiladores, ligadores, etc.; para volver a correr su programa, es decir, enfrentaba el problema del procesamiento serial (serial processing).

La importancia de los sistemas operativos nace históricamente desde los 50's, cuando se hizo evidente que el operar una computadora por medio de tableros enchufables en la primera generación y luego por medio del trabajo en lote en la segunda generación se podía mejorar notoriamente, pues el operador realizaba siempre una secuencia de pasos repetitivos, lo cual es una de las características contempladas en la definición de lo que es un programa; es decir, se comenzó a ver que las tareas mismas del operador podían plasmarse en un programa, el cual a través del tiempo y por su enorme complejidad se le llamó "Sistema Operativo".

Así, tenemos entre los primeros sistemas operativos alFortran Monitor System (FMS ) e IBSYS; posteriormente, en la tercera generación de computadoras nace uno de los primeros sistemas operativos con la filosofía de administrar

una familia de computadoras: el OS/360 de IBM. Fue este un proyecto tan novedoso y ambicioso que enfrentó por primera vez una serie de problemas conflictivos debido a que anteriormente las computadoras eran creadas para dos propósitos en general: el comercial y el científico. Así, al tratar de crear un solo sistema operativo para computadoras que podían dedicarse a un propósito, al otro o ambos, puso en evidencia la problemática del trabajo en equipos de análisis, diseño e implantación de sistemas grandes. El resultado fue un sistema del cual uno de sus mismos diseñadores patentizó su opinión en la portada de un libro: una horda de bestias prehistóricas atascadas en un foso de brea.

En la cuarta generación la electrónica avanza hacia la integración a gran escala, pudiendo crear circuitos con miles de transistores en un centímetro cuadrado de silicón y ya es posible hablar de las computadoras personales y las estaciones de trabajo. Surgen los conceptos de interfaces amigables intentando así atraer al público en general al uso de las computadoras como herramientas cotidianas.

Se hacen populares el MS-DOS y UNIX en estas máquinas. También es común encontrar clones de computadoras personales y una multitud de empresas pequeñas ensamblándolas por todo el mundo.

Para mediados de los 80's, comienza el auge de las redes de computadoras y la necesidad de sistemas operativos en red y sistemas operativos distribuidos. La red mundial Internet se va haciendo accesible a toda clase de instituciones y se

comienzan a dar muchas soluciones (y problemas) al querer hacer convivir recursos residentes en computadoras con sistemas operativos diferentes.

Para los 90's el paradigma de la programación orientada a objetos cobra auge, así como el manejo de objetos desde los sistemas operativos. Las aplicaciones intentan crearse para ser ejecutadas en una plataforma específica y poder ver sus resultados en la pantalla o monitor de otra diferente (por ejemplo, ejecutar una simulación en una máquina con UNIX y ver los resultados en otra con DOS). Los niveles de interacción se van haciendo cada vez más profundos.

### 1.2.2. CLASIFICACIÓN DE SISTEMAS OPERATIVOS.

#### 1.2.2.1. SISTEMA OPERATIVO POR USUARIOS

Los sistemas operativos por usuarios se han clasificado en dos grupos monousuario y multiusuarios, los mismos que se describen a continuación.

**a. SISTEMA OPERATIVO MONOUSUARIO.** Los sistemas operativos monousuarios son aquéllos que soportan a un usuario a la vez, sin importar el número de procesadores que tenga la computadora o el número de procesos o tareas que el usuario pueda ejecutar en un mismo instante; en otras palabras los sistemas monousuarios son aquellos que nada más puede atender a un solo

usuario, gracias a las limitaciones creadas por el hardware, los programas o el tipo de aplicación que se este ejecutando.

**b. SISTEMA OPERATIVO MULTIUSUARIO.** Los sistemas operativos multiusuarios son capaces de dar servicio a más de un usuario a la vez, ya sea por medio de varias terminales conectadas a la computadora o por medio de sesiones remotas en una red de comunicaciones. No importa el número de procesadores en la máquina ni el número de procesos que cada usuario puede ejecutar simultáneamente.

### 1.2.2.2. SISTEMA OPERATIVO POR TAREA

Los sistemas operativos por tarea se clasifican en dos grupos monotarea y multitarea, los mismos que se describen a continuación.

**a. SISTEMA OPERATIVO MONOTAREA.** Los sistemas monotarea son aquellos que sólo permiten una tarea a la vez por usuario.

Puede darse el caso de un sistema multiusuario y monotarea, en el cual se admiten varios usuarios al mismo tiempo pero cada uno de ellos puede estar haciendo solo una tarea a la vez; los sistemas operativos monotareas son más primitivos y, solo pueden manejar un proceso en cada momento o que solo puede ejecutar las tareas de una en una.

**b. SISTEMA OPERATIVO MULTITAREA.** Un sistema operativo multitarea es aquél que le permite al usuario estar realizando varias labores al mismo tiempo, se distingue por su capacidad para soportar la ejecución concurrente de dos o más procesos activos.

La multitarea se implementa generalmente manteniendo el código y los datos de varios procesos simultáneamente en memoria y multiplexando el procesador y los dispositivos de E/S entre ellos.

### 1.2.2.3. SISTEMA OPERATIVO POR PROCESADOR.

Esta clase de sistema operativo se clasifica en: Asimetrica, Simetrica; se las divide en estas dos clases por que hacen referencia a la utilización del procesador tal como se describe a continuación.

**a. ASIMETRICA.** Cuando se trabaja de manera asimétrica, el sistema operativo selecciona a uno de los procesadores el cual jugará el papel de procesador maestro y servirá como pivote para distribuir la carga a los demás procesadores, que reciben el nombre de esclavos.

**b. SIMETRICA.** Cuando se trabaja de manera simétrica, los procesos o partes de ellos (threads) son enviados indistintamente a cualquiera de los procesadores disponibles, teniendo, teóricamente, una mejor distribución y equilibrio en la

carga de trabajo bajo este esquema; linux ha dejado de ser el juguete de hackers universitarios, esta cada día más cerca de lo que pareciera y es importante que lo conozcamos a fondo, para conocer sus fortalezas y debilidades.

## 1.3. LINUX

### 1.3.1 RESEÑA HISTÓRICA

LINUX hace su aparición a principios de la década de los noventa, era el año 1991 y por aquel entonces un estudiante de informática de la Universidad de Helsinki, llamado Linus Torvalds empezó, como una afición y sin poderse imaginar a lo que llegaría este proyecto, a programar las primeras líneas de código de este sistema operativo llamado LINUX.

Este comienzo estuvo inspirado en MINIX, un pequeño sistema Unix desarrollado por Andy Tanenbaum. Las primeras discusiones sobre Linux fueron en el grupo de noticias compos. minix, en estas discusiones se hablaba sobre todo del desarrollo de un pequeño sistema Unix para usuarios de Minix que querían más.

Linus nunca anuncio la versión 0.01 de Linux (agosto 1991), esta versión no era ni siquiera ejecutable, solamente incluía los principios del núcleo del sistema, estaba escrita en lenguaje ensamblador y asumía que uno tenia acceso a un sistema Minix para su compilación.

El 5 de octubre de 1991, Linus anuncio la primera versión "Oficial" de Linux, versión 0.02. Con esta versión Linus pudo ejecutar Bash (GNU Bourne Again Shell) y gcc (El compilador GNU de C) pero no alcanzo buenos resultados de funcionamiento. En este estado de desarrollo ni se pensaba en los términos de soporte, documentación y distribución.

Después de la versión 0.03, Linus salto en la numeración hasta la 0.10, en la que participaron muchos programadores enlazándose a través del internet y empezaron a trabajar en el proyecto, después de sucesivas revisiones, se incrementa el número de versión hasta la 0.95 (Marzo 1992). Más de un año después (diciembre 1993) el núcleo del sistema estaba en la versión 0.99 y la versión 1.0 no llego hasta el 14 de marzo de 1994.

Desde entonces no se ha parado de desarrollar, la versión actual del núcleo es la 2.2 y sigue avanzando día a día con la meta de perfeccionar y mejorar el sistema; así pues, Linus tomó la decisión de cambiar la política debido a que el sistema Minix era ideal para los estudiantes de sistemas operativos, y su precio era considerablemente alto; llegamos de nuevo al año 1991, cuando Linus se acabó de comprar su primer 386; en aquellos momentos su intención era clara: crear un nuevo Kernel de UNIX basado en el Kernel de Minix y modificarlo periódicamente de manera que fuera capaz de ejecutar aplicaciones GNU. Es evidente que Unix ha retomado gran fuerza en el último tiempo, y la razón de esto es GNU, de hecho, muchas veces que se enfrentan a un Unix comercial deben

"GNU-nizarlo" instalando sus aplicaciones favoritas, porque el software GNU ha conseguido una calidad excepcional.

### 1.3.2. CONCEPTO DE LINUX

Para http://WWW.LINUX.ORG.VE/QUE.shtml, **LINUX** es: "Un Sistema Operativo para PC que usa procesadores 386, 486 y Pentium. Linux hace todo esto a un precio inmejorable. Es Gratis!!! A diferencia del sistema operativo Unix, Linux se distribuye de forma gratuita bajo una licencia pública general de GNU, poniéndolo a disposición de cualquiera que lo desee utilizar. Aún cuando Linux tenga registro de Copyright, y no sea estrictamente de dominio público.

La licencia tiene por objeto asegurar que Linux siga siendo gratuito y a la vez estándar. El hecho de que Linux sea gratis da a la gente a veces, la impresión equivocada que de algún modo es inferior a un sistema operativo profesional. Pero nosotros le demostraremos que eso, NO es verdad..."

Para PETERSON Richard (1996), Linux Manual de Referencia. Editorial Mc Graw Hill Interamericana S.A. **LINUX** es: "A simple vista, un Sistema Operativo, es una implementación de libre distribución UNIX para computadoras personales (PC), servidores, y estaciones de trabajo", (Pág. 526); fue desarrollado para el i386 y ahora soporta los procesadores i486, Pentium, Pentium Pro y Pentium II, así como los clones AMD y Cyrix. También soporta máquinas basadas en

SPARC, DEC Alpha, PowerPC/PowerMac, y Mac/Amiga Motorola 680x0, linux es sólo el kernel, o sea, el núcleo del sistema operativo. La parte que se carga primero y administra los demás elementos.

Como sistema operativo, Linux es muy eficiente y tiene un excelente diseño, es multitarea, multiusuario, multiplataforma y multiprocesador; en las plataformas Intel corre en modo protegido; protege la memoria para que un programa no pueda hacer caer al resto del sistema; carga sólo las partes de un programa que se usan; comparte la memoria entre programas aumentando la velocidad y disminuyendo el uso de memoria; usa un sistema de memoria virtual por páginas; utiliza toda la memoria libre para cache; permite usar bibliotecas enlazadas tanto estática como dinámicamente; se distribuye con código fuente; usa hasta 64 consolas virtuales; tiene un sistema de archivos avanzado pero puede usar los de los otros sistemas; y soporta redes tanto en TCP/IP como en otros protocolos.

### 1.3.3. LINUX EN EL MUNDO

Linux es hoy en día más importante de lo que parece (y de lo que algunas compañías desearían), es difícil saber exactamente cuantas máquinas Linux existen, pues no existe un vendedor central y es libremente distribuible, por esta razon la documentación de Linux tiene una amplia recopilación de escritores, correctores y editores que estan trabajando en un conjunto definitivo de manuales de Linux-

### 1.3.3.1. SISTEMA OPERATIVO

No existe un "Linux Workstation" o un "Linux Server". Cuando usted instala Linux, obtiene una potente estación de trabajo así como un servidor genérico, y las mayores distribuciones de Linux incorporan todo lo necesario para convertir a Linux en su servidor favorito como:

- webserver - apache
- mailserver - sendmail
- archivos - samba o nfs
- dns - bind
- directorios - nis o ldap
- firewall, router, nat - ipchains
- proxy - squid
- impresión - lpr o samba
- control de versiones - cvs
- etc.

Y se puede colocar todos estos servicios en una sola máquina, que incluso podría ser su estación de trabajo.

Por el lado del usuario, Linux ya cuenta con dos increíbles Desktops: KDE y GNOME y otros, ambos no tienen nada que envidiarle a interfaces como la de

Windows o Macintosh; y, son lo suficientemente estables y poderosas para el trabajo diario. Han acercado a los "end users", ocultando la complejidad de Unix con interfaces que prácticamente todo el mundo conoce.

Como Linux ya está embutido en el mundo empresarial, sufre como cualquier otro los achaques del mercado. El avance del sistema operativo open source padeció un leve catarro el año pasado, que sirvió a los analistas para reafirmarse en que tropezones como este no hacen peligrar su desarrollo, pero Linux es un proyecto open source, lo que significa que, al contrario de lo que ocurre con sistemas propietarios (cerrados) como Solaris de Sun o Windows de Microsoft, su código fuente se puede compartir, cambiar o distribuir libremente. Los linuxeros hacen dinero de empaquetar los programas y ofrecer asistencia técnica.

### 1.3.3.2. LINUX ES SOFTWARE LIBRE

El movimiento GNU/Linux tiene de trasfondo el concepto de «software libre» (free-software), pero, ¿qué quiere decir "libre" en «software libre»? Pues se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, instalar, cambiar y mejorar el programa tantas veces como quieran, en concreto se consideran tres niveles de libertad:

- Libertad para estudiar el programa, aprender de él e incluso usar todo o parte de él en otros proyectos.

- Libertad para distribuir, copiar a quien se quiera y sin límite alguno; cobrándose por ello lo que se quiera (por ejemplo, nada, o por ejemplo 18 euros).

- La libertad de toda la comunidad de usuarios de mejorar el programa y distribuirlo de tal manera que se puedan beneficiar todos lo integrantes de la propia comunidad.

Con el software libre, la única libertad que no se tiene es la de restringir estos derechos a otros usuarios, es decir, la libertad de eliminar libertades. Si se distribuye una copia o una modificación de un programa libre todos los usuarios disponen de los derechos antes citados.

## 1.4. INTRANETS

### 1.4.1. INTRODUCCION

Para GONZÁLES, José; (1998); manual avanzado, editorial multimedia, **INTRANET** es: "La implantación de tecnologías de Internet en una organización corporativa, en lugar de la conexión externa a Internet global". (Pág. 933).

Una Intranet es una red privada que la tecnología Internet usó como arquitectura elemental, una red interna se construye usando los protocolos TCP/IP para

comunicación de Internet, que pueden ejecutarse en muchas de las plataformas de hardware, el mismo que es fundamental no es lo que construye una Intranet, lo que importa son los protocolos del software.

Intranet de este modo es muy parecido a conectar con Internet, la operabilidad interna entre redes es otro suplemento sustancial; los sistemas de seguridad separan una Intranet de Internet, la red interna de una compañía está protegida por firewall: combinaciones de hardware y software que sólo permiten a ciertas personas acceder a ella para propósitos específicos, se puede utilizar para cualquier cosa para la que se empleaban las redes existentes

### 1.4.2. CONCEPTO DE INTRANET

La intranet es una red privada dentro de una compañía u organización que utiliza el mismo tipo de software usado en el Internet público, pero que es sólo para uso interno. Conforme el Internet se hace más popular, muchas de las herramientas usadas en el Internet están siendo usadas también en las redes privadas, por ejemplo, muchas compañías tienen web servers que están sólo disponibles para sus empleados.

### 1.4.3. LINUX COMO SERVIDOR DE INTRANET

Linux es un sistema muy usado por su versatilidad, se usa muchísimo en:

Servidores de Internet y grandes ordenadores, porque aprovecha al máximo los recursos. Además, se puede instalar sin necesidad de un sistema gráfico que garantice el ordenador.

En términos simples, Intranet es el término descriptivo que está siendo usado para la implantación de tecnologías de Internet en una organización corporativa, en lugar de la conexión externa a Internet global, esta implementación funciona como una alternativa al intercambio transparente de los inmensos recursos informacionales de una organización entre cada uno de los escritorios individuales con un mínimo costo, tiempo y esfuerzo; este documento intenta explicar en términos simples como configurar una Intranet usando herramientas que son fácilmente obtenibles.

## 1.5. SERVICIOS EN LINUX

Linux es probablemente el acontecimiento más importante del software gratuito desde el original Space War, o, mas recientemente Emacs, se ha convertido en el sistema operativo para los negocios, educación y provecho personal, la mayoría de servicios en Linux soporta una implementación completa de los protocolos de red TCP/IP (Transport Control Protocol / Internet Protocol). TCP/IP ha resultado ser hasta ahora el mejor mecanismo de comunicación entre ordenadores de todo el mundo. A continuación describimos los diferentes servicios que podemos configurar en un servidor Linux.

### 1.5.1. SERVIDOR DE ARCHIVOS

**a. SAMBA SERVER Y NFS SERVER.** Es utilizado para copiar, crear o modificar archivos, cada usuario tiene sus propios permisos y lugares para acceso fácilmente configurables; de esta forma comparte o protege sus datos en lugares ya señalados con solo un click del Mouse, y para cuidar su disco también asigna el espacio necesario para cada usuario.

El servidor SAMBA es una implementación del protocolo SMB (Session Messaje Block) que utilizan los sistemas operativos de Microsoft para que puedan correr ciertas aplicaciones de red en forma gráfica, una vez que se instala SAMBA, podemos compartir filesystems de Linux para que puedan ser accesados por máquinas Windows en la INTRANET, así como también impresoras conectadas al servidor Linux.

### 1.5.2. PROXY SERVER

Agregue velocidad y ahorro a su conexión a Internet, el Proxy Server crea un gran cache de sitios ya visitados para luego navegarlos off-line, y cuando se encuentra en Internet solo recoge los archivos que no están actualizados permitiendo así mayor velocidad, recuerde que generalmente los cambios en una Web son solo archivos de texto.

### 1.5.3. WEB SERVER, FTP SERVER Y DNS SERVER

Un Web Server de máximas prestaciones: HiperText Maker Leguage (HTML), Active Server Page (ASP), Common Gategay Interface (CGI), Personal Home Page Tools (PHP), Java, múltiples dominios, etc. Probar sus páginas Webs off-line o agregar multimedia a la base de datos de sus productos, fotografías, animaciones y descripciones fácilmente navegables e intuitivas para el cliente.

El servicio de nombres de dominio o DNS (Domain Name Server), convierte nombres de máquinas a direcciones IP, es decir, mapea de un nombre a una dirección y de una dirección a un nombre, hasta tomar alguna de las existentes como base, a ser la nueva.

#### 1.5.3.1 TIPOS DE SERVIDORES DNS

Un servidor DNS, es también conocido como "nameserver" (NS) y pueden ser de 3 variedades:

a) MASTER. (Conocido como primario). El master server para un dominio es el servidor en el cual todos lo datos acerca de ese dominio son derivados de él.

b) SLAVE. (o secundario). Al igual que un master Server, posee toda la información acerca del dominio, la diferencia es que al ser "slave" recibe los datos

directamente de un MASTER Server.

c) CATCHING. No mantiene toda la información de ningún dominio, únicamente mantiene cachete las consultas realizadas a él de sus clientes.

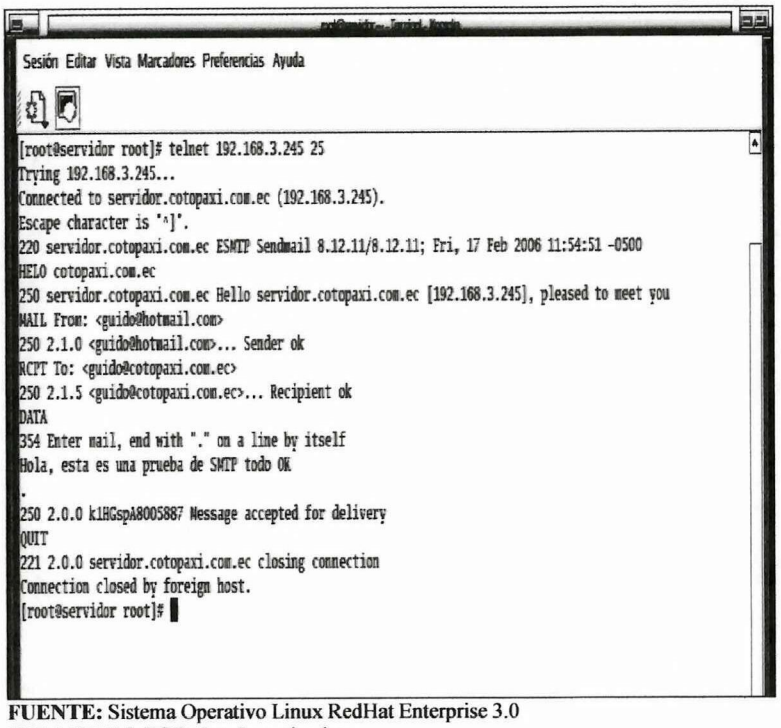
### 1.5.4. MAIL SERVER

El demonio que controla el servicio del correo llamado sendmail, para entender lo que sendmail realiza, se necesita saber un poco acerca de los protocolos que se utilizan en Internet para la transferencia de correos.

SMTP (Simple Mail Transfer Protocol) define como los programas intercambian correos sobre el Internet y no le importa si el programa que lo esta corriendo, esta funcionando en un SUN para Linux es decir se encarga de hacer el envío del correo.

Para probar el funcionamiento del protocolo SMTP lo hacemos mediante una conexión interna con el comando telnet al puerto 25, aquí se podra observar una pronta respuesta indicando que la conexión fue exitosa, para lo cual el servidor deberá estar configurado correctamente y la respuesta se puede evidenciar en el grafico siguiente.

**GRAFICO Nº 1.1: TEST FUNCIONANIENTO SMTP**

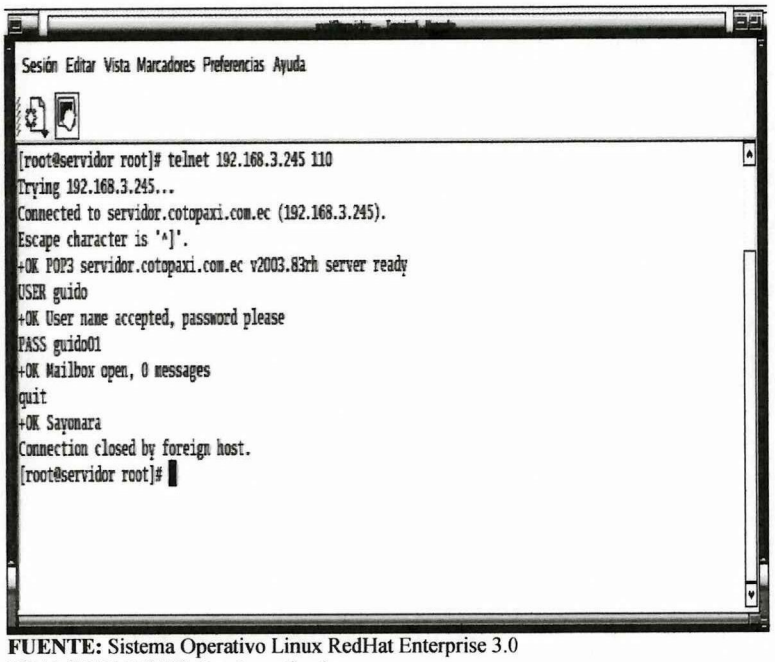



**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

POP (Post Office Protocol), es el encargado de terminar la acción de servidor de correo para el usuario. Es decir es el encargado de transmitir el mensaje que acaba de llegar a servidor de correos, mediante SMTP, a la aplicación de correos que utilice el cliente.

De igual manera para probar el funcionamiento de este servicio lo hacemos con un telnet al puerto 110 tal como se muestra en el grafico siguiente.

**GRAFICO Nº 1.2: TEST FUNCIONANIENTO POP**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

## 1.6. FIREWALLS Y SEGURIDAD EN INTERNET

### 1.6.1. INTRODUCCIÓN

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet, sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso publico en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los Expertos de Internet (*Internet Crakers*), para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información.

Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

### 1.6.2. FIREWALLS

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet, que determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización; para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información, el firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración.

El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información, esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento.

Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad, un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda; Se trata de uno de los métodos usados para proteger una red de intrusiones no autorizadas. Esto se realiza a través de dos mecanismos: uno para bloquear el tráfico de la red, y otro para dejar fluir dicho tráfico.

### 1.6.2.1. BENEFICIOS DE UN FIREWALL EN INTERNET

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet, esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crackers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles.

Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada, el firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos, esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque, esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall, también si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base, esto se vuelve innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona el sistema, por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios.

Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs), un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet, ya que esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas. Un firewall de Internet ofrece un punto de reunión para la organización, si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple, enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando únicamente el acceso al Internet esta perdido.

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet, estos dos puntos de acceso significan dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

### 1.6.2.2 BASES PARA EL DISEÑO DECISIVO DEL FIREWALL

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

- Posturas sobre la política del Firewall
- La política interna propia de la organización para la seguridad total
- El costo financiero del Proyecto "Firewall"
- Los componentes o la construcción de secciones del Firewall

### 1.6.2.3. POLÍTICAS DEL FIREWALL.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización, estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

- "No todo lo específicamente permitido esta prohibido"

- "Ni todo lo específicamente prohibido esta permitido"

La primera postura asume que un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso, esta idea es recomendada únicamente a un limitado número de servicios soportados cuidadosamente seleccionados en un servidor; desde el punto de vista de "seguridad", esto es más importante que facilitar el uso de los servicios.

La segunda postura asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso, esta propuesta crea ambientes más flexibles al disponer más servicios para los usuarios de la comunidad; la desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia seguridad del sistema.
En nuestro caso el administrador de la red esta en la potestad de incrementar seguridad en la intranet del sistema conforme crece la red, garantizando de esta manera los servicios y el acceso que cada uno de los usuarios debe tener hacia ellos.

### 1.6.2.4. POLÍTICA INTERNA DE LA SEGURIDAD

Tan discutidamente escuchada, un firewall de Internet no esta solo es parte de la política de seguridad total en una organización, la cual define todos los aspectos

en competentes al perímetro de defensa; para que esta sea exitosa, la organización debe de conocer que es lo se esta protegiendo.

La política de seguridad se basará en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación del negocio; si no se posee con la información detallada de la política a seguir, aun que sea un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

### 1.6.2.5. COMPONENTES DEL SISTEMA FIREWALL

Después de las decisiones acerca de los ejemplos previos, la organización puede determinar específicamente los componentes del sistema, un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

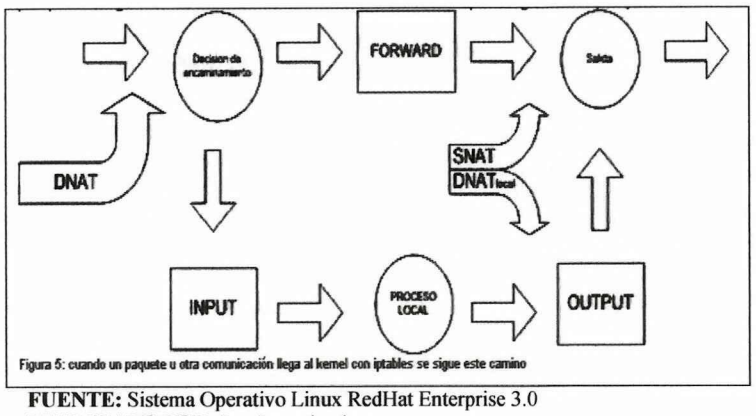
- Ruteador Filtra-paquetes
- Gateway a Nivel-aplicación
- Gateway a Nivel-circuito

### 1.6.2.6. USO DE IPTABLES

Iptables es un sistema de firewall vinculado al kernel de Linux, un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación (esto es una pequeña mentira, ha tenido alguna

vulnerabilidad que permite DoS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): iptables esta integrado con el kernel, es parte del sistema operativo.

**GRAFICO Nº 1.3: FUNCIONAMIENTO FIREWALL**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Realmente lo que se hace es aplicar reglas, para ello se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.

Como se ve en el gráfico, básicamente se mira si el paquete esta destinado a la propia maquina o si va a otra; para los paquetes (o datagramas, según el protocolo) que van a la propia maquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD, pero antes de aplicar esas reglas es posible aplicar reglas de

NAT; estas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino.

Por tanto tenemos tres tipos de reglas en iptables:

- MANGLE
- NAT: reglas PREROUTING, POSTROUTING
- FILTER: reglas INPUT, OUTPUT, FORWARD.

# CAPITULO II

# TRABAJO DE CAMPO

## 2.1 ANALISIS E INTERPRETACION DE RESULTADOS

La gran afluencia del desarrollo tecnológico y los sistemas operativos en el mundo han acaparado grandes áreas de crecimiento industrial, llegando así a conformar un amplio nivel informático, es así como en la actualidad el desarrollo de la tecnología informática a experimentado una verdadera incursión en la industria de desarrollo de software, sin embargo esto no ha impedido que se desarrollen sistemas libres como es el caso de Linux, sistema en el que para su evolución han participan varios programadores de todo el mundo, buscando siempre hacer de este un sistema ágil, confiable, rápido, y libre de virus.

Aglomerados Cotopaxi S.A. se ha visto en la obligación de adentrarse a este desarrollo tecnológico a través de un sistema que le permita establecer una estructura compleja de seguridad, que facilite a su recurso humano todas las ventajas de su utilización a través de seguridad en la red, con un ciclo de vida en su sistema operativo que cuente con una planificación adecuada y la información sea confiable para satisfacer las necesidades de los usuarios; mejorando sustancialmente el rendimiento, la capacitación y proporcionar a los usuarios mayores alternativas de eficiencia e interactividad.

## 2.2. ANALISIS FODA

Visión del entorno Laboral – Matriz FODA

| Fortaleza | Debilidad |
|---|---|
| • Apertura al cambio de sistemas informáticos, equipos de cómputo y seguridades informáticas.<br>• Experiencia en el manejo de este sistema informático<br>• Alta capacidad de respuesta técnica.<br>• Reconocimiento público | • Falta de capacitación e integración a nuevos sistemas de seguridad informática<br>• Maquinas obsoletas<br>• Sistema desactualizado<br>• Acceso limitado al flujo de información |
| **Oportunidad** | **Amenaza** |
| • Buenas alternativas para mejorar las seguridades en el flujo de información de la empresa<br>• Impulsar el desarrollo tecnológico de la empresa.<br>• Mejoramiento sustentable de los sistemas informáticos.<br>• Crecimiento profesional de los usuarios y trabajadores de la empresa. | Disminución sustancial de seguridades y protección a los sistemas informáticos<br>• Retrazar la integración de los usuarios a este nuevo sistema.<br>• No existen lineamientos para regular la participación interna de personal de ACOSA.<br>Exposición climática a los equipos de transmisión de señales |

**FUENTE:** Departamento de sistemas
**REALIZADO POR:** Grupo Investigador

Con el análisis de la presente investigación se demuestra claramente que con la aplicación de este nuevo sistema se obtendrá magníficos resultados para el

crecimiento constante de la empresa, los mismos que permitirán a los usuarios cambiar de una manera radical el desconocimiento que el personal tenía acerca de las nuevas tecnologías informáticas que aplicadas con una correcta y adecuada capacitación llegaran a desarrollarse ampliamente, permitiendo ampliar las perspectivas de mejoramiento.

## 2.3. ESTUDIO DE PROCEDIMIENTOS

Luego de haber determinado el problema, es decir que la plataforma actual de linux 7.3 que utiliza la empresa no se encuentra exenta de ataques que ponen en riesgo la información que manejan, fue necesario elegir las técnicas y metodologías más adecuadas, partiendo de la técnica investigativa con la aplicación de encuestas y entrevistas para recabar la información necesaria, seguidamente de la metodología formativa para el desarrollo del sistema tomando en cuenta sus parámetros.

La integración de estas metodologías ayudarán al buen desenvolvimiento del administrador y usuario del sistema, asimilando de esta manera que los individuos y la máquina se transformen en un solo elemento orientados al manejo efectivo.

Para ello se utilizará el modelo referencial existente, aplicando una metodología y técnicas de investigación.

Este modelo nos permite seguir los pasos anteriormente descritos como referencia para la implementación de nuestro nuevo sistema con mayor flexibilidad, permitiéndonos realizar análisis completos en lo que se refiere a cada una de las fases a seguir.

## 2.4. ELABORACIÓN DE TABLAS

Para la recopilación de información y elaboración de tablas se tomó una muestra a la que se sometieron el personal del departamento de sistemas y procesamiento de datos.

Es así, que a los usuarios se les aplicó una encuesta el formato se muestra en el Anexo 1.**(Formato de la encuesta realizada a los usuarios del sistema Informático)**

Esta técnica aplicada permitió obtener una adecuada información, para tener un panorama claro de la situación actual en que se halla.

## 2.5 ANALISIS DE RESULTADOS

Luego de realizar a una muestra de la población del departamento de sistemas a 9 personas que representa el 100%; para la interpretación de los resultados se

utilizará la estadística descriptiva, la representación de los datos se lo hará a través de los gráficos estadísticos como son el pastel.

## 2.6 INTERPRETACION DE RESULTADOS

A continuación se muestra el resultado de las encuestas realizadas al personal del departamento de Sistemas de la empresa Aglomerados Cotopaxi S.A.

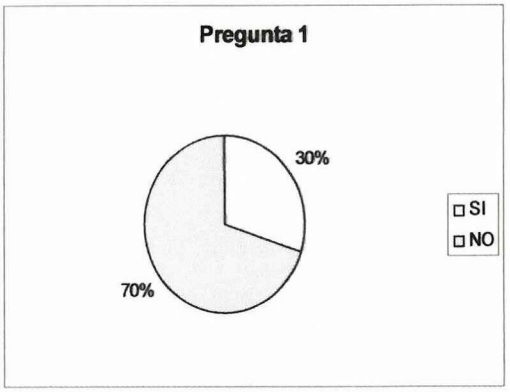
### 1. ¿RECIBIÓ CAPACITACIÓN ANTES DE UTILIZAR EL SISTEMA INFORMÁTICO?

**TABLA Nº . 2.1: CAPACITACIÓN EN EL MANEJO DEL SISTEMA**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 3 | 30 |
| NO | 7 | 70 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.1: CAPACITACIÓN EN EL MANEJO DEL SISTEMA**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## ANÁLISIS E INTERPRETACIÓN:

El 30% de los encuestados indican que si recibieron capacitación antes de empezar a utilizar el sistema, lo que les permitió un aprendizaje significativo para el desarrollo de actividades; sin embargo no así el 70% del personal recibió esta capacitación, hecho que junto a la falta de equipos se convierte como parte del descontento de los usuarios; lo que indica que la falta de capacitación puede ser uno de los inconvenientes que les impidió alcanzar los actuales niveles de seguridad informático.

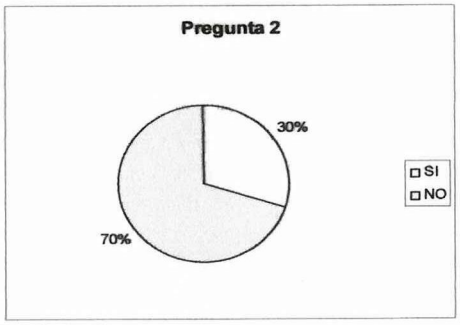
## 2. ¿CONOCE COMO FUNCIONA LA ESTRUCTURA DEL SISTEMA QUE UTILIZA?

**TABLA Nº 2.2: DIFUNDIR EL FUNCIONAMIENTO DEL SISTEMA.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 3 | 30 |
| NO | 7 | 70 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.2: DIFUNFIR EL FUNCIONAMIENTO DEL SISTEMA.**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## ANÁLISIS E INTERPRETACIÓN:

El 30% del personal entrevistado indica que conoce en su totalidad como funciona la estructura del sistema que están manejando, esto se debe a que recibió una breve capacitación misma que les ayudo a adquirir las bases necesarias para el desarrollo de nuevas actividades, sin embargo el 70% desconoce como funciona el sistema que han venido manipulando desde algún tiempo, obviamente les gustaría conocer nuevas alternativas y capacitarse en temas de seguridad informática.

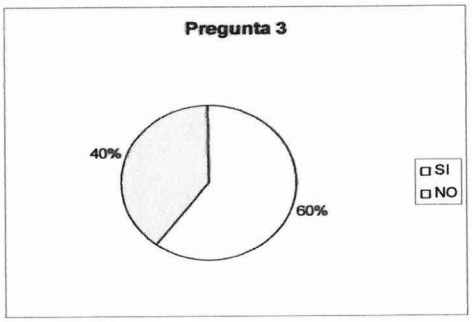
## 3. ¿LA INFORMACIÓN QUE UD. PROPORCIONA AL SISTEMA ES CONFIDENCIAL?

**TABLA Nº 2.3: MAYOR SEGURIDAD A LA INFORMACIÓN.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 6 | 60 |
| NO | 4 | 40 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.3: MAYOR SEGURIDAD A LA INFORMACIÓN.**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## ANÁLISIS E INTERPRETACIÓN

El 60% del personal considera que la información que esta bajo su responsabilidad es sumamente confidencial, pues el manejo indebido de esta información puede causar serios daños y perjudicar a varios de los procesos internos que se manejan, pero el 40% de los encuestados no considera que la información que esta bajo su control sea confidencial, y se sienten seguros con el sistema que controla y les brinda la seguridad necesaria para el cuidado de la información.

**4. ¿CONOCE CUAL ES EL SISTEMA QUE SE ENCARGA DE BRINDARLE MEJOR SEGURIDAD A LA INFORMACIÓN QUE ESTA BAJO SU RESPONSABILIDAD?**

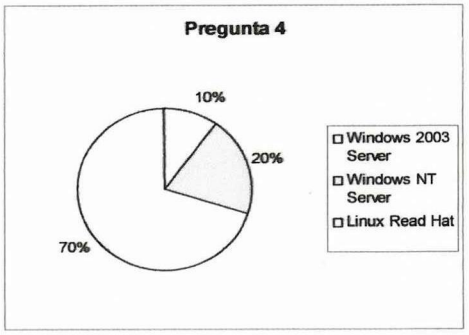
**a) Windows 2003 Server b) Windows NT Server c) Linux Red Hat 7**

**TABLA Nº 2.4: CONOCIMIENTO DEL SISTEMA.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| Windows 2003 | 1 | 10 |
| Windows NT | 2 | 20 |
| Linux Read Hat | 7 | 70 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.4: CONOCIMIENTO DEL SISTEMA.**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## ANÁLISIS E INTERPRETACIÓN:

El 70% de los encuestados conocen que el sistema que les provee de seguridad informática es Linux, sin embargo el 20% considera que es Windows 2003 Server es quién lo hace y el 10% en cambio afirma que es Windows NT Server; claramente podemos observar que la mayor parte de usuarios (administradores) conocen y manejan versiones anteriores a la que proponemos.

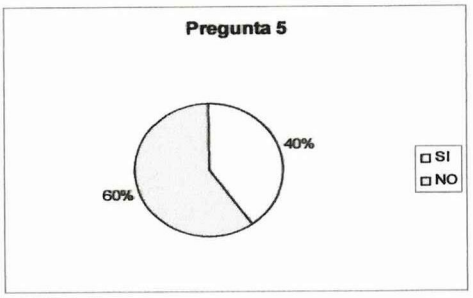
## 5. ¿LOS SERVICIOS INFORMÁTICOS CON LOS QUE CUENTA LA EMPRESA SON SATISFACTORIOS PARA LA REALIZACIÓN DE SU TRABAJO?

**TABLA Nº 2.5: MEJORAR LOS SERVICIOS INFORMÁTICOS.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 4 | 40 |
| NO | 6 | 60 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## GRÁFICO Nº 2.5: MEJORAR LOS SERVICIOS INFORMÁTICOS.




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## ANÁLISIS E INTERPRETACIÓN:

El 40% de los encuestados considera que los servicios informáticos con los que cuenta para la realización de su trabajo son adecuados y no les ha causado ningún tipo de inconveniente, sin embargo el 60% restante considera que no lo es, ya que según su criterio esta es la causa por la que se dan los problemas en el flujo de información y en buena parte se ha constituido en uno de lo factores que ha retrazado la entrega de resultados a las diferentes áreas productivas.

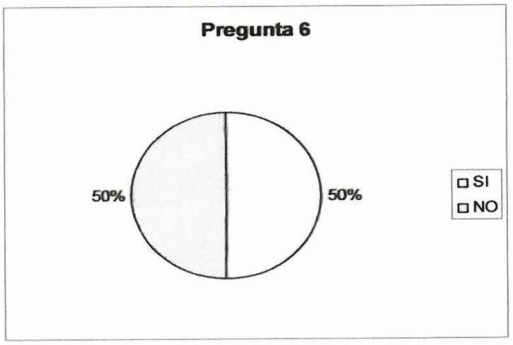
## 6. ¿CREE USTED QUE LA DEFICIENCIA DE LOS EQUIPOS SON LA CAUSA DE LOS RETRASOS Y PROBLEMAS QUE SE ENCUENTRAN EN EL PROCESAMIENTO DE LA INFORMACIÓN?

**TABLA Nº 2.6: DESECHAR LOS EQUIPOS OBSOLETOS.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 5 | 50 |
| NO | 5 | 50 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## GRÁFICO Nº 2.6: DESECHAR LOS EQUIPOS OBSOLETOS.




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## ANÁLISIS E INTERPRETACIÓN:

El 50% de los encuestados cree que la deficiencia en los equipos si es una causa para el retrazo en el procesamiento de la información, sin embargo el 50% restante piensa que no lo es, pues consideran que si a un equipo se le proporcionan todas las actualizaciones puede funcionar correctamente y permitir que una tarea se cumpla en el tiempo establecido.

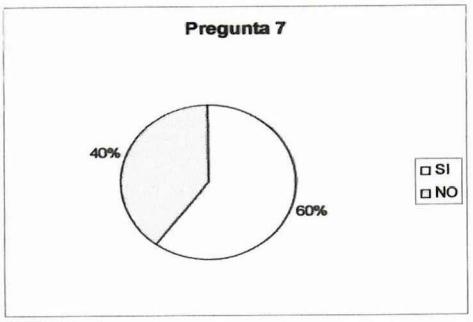
## 7. ¿CONOCE QUE ES LINUX?

**TABLA Nº 2.7: DIFUNDIR EL CONOCIMIENTO DE LINUX.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 6 | 60 |
| NO | 4 | 40 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## GRÁFICO Nº 2.7: DIFUNDIR EL CONOCIMIENTO DE LINUX.




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

## ANÁLISIS E INTERPRETACIÓN:

El 60% de los encuestados si conoce que es Linux, así como también los beneficios y ventajas de utilizar este sistema operativo, ya que muchos de ellos son encargados de administrar los servicios y seguridades que nos brinda esta plataforma, pero el 40% de los encuestados desconocen la existencia de este sistema operativo pero ven en él una forma segura en la aplicación de seguridades para el manejo de información.

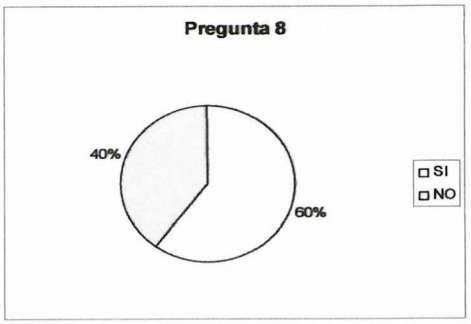
## 8. ¿LA UTILIZACIÓN DE LINUX ES VENTAJOSA?

**TABLA Nº 2.8: MEJORAR EL CONOCIMIENTO DE LINUX**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 4 | 40 |
| NO | 6 | 60 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.8: MEJORAR EL CONOCIMIENTO DE LINUX.**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**ANÁLISIS E INTERPRETACIÓN:**

El 60% de los encuestados considera que la utilización de Linux si es ventajosa por muchas alternativas, una de ellas es la escasez de virus para Linux, otra es la facilidad de acceder al código abierto y ajustarlo a nuestras necesidades, etc., sin embargo el 40% de las personas que participaron en esta encuesta no conocen las facilidades que proporciona Linux, obviamente por que no han escuchado de él.

**9. SI SU RESPUESTA ES SI A CUALQUIERA DE LAS DOS PREGUNTAS ANTERIORES, MARQUE DENTRO DE LOS PARÉNTESIS CUALES SON LAS VENTAJAS DE UTILIZAR LINUX.**

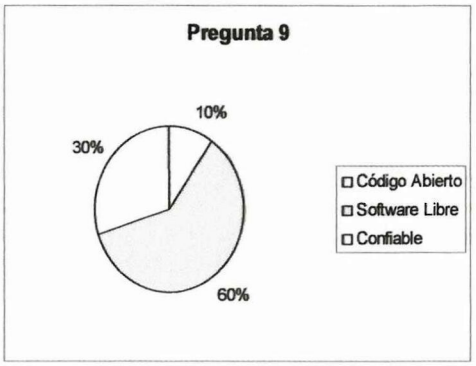
- **Código Abierto ( )**
- **Software libre ( )**
- **Confiable ( )**

**TABLA Nº 2.9: DIFUSIÓN DE LINUX**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| Código Abierto | 1 | 10 |
| Software Libre | 6 | 60 |
| Confiable | 3 | 30 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.9: DIFUSION DE LINUX.**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**ANÁLISIS E INTERPRETACIÓN.**

De los encuestados que respondieron la pregunta anterior el 60% considerando que la ventaja principal de Linux es su facilidad de acceso al código abierto que permitirá al administrador acceder rápidamente al sistema y poder dar soluciones inmediatas a los requerimientos de los usuarios, pero el 30% lo toma por su confiabilidad en su uso, y el 10% lo considera por ser un Software Libre de acceso rápido.

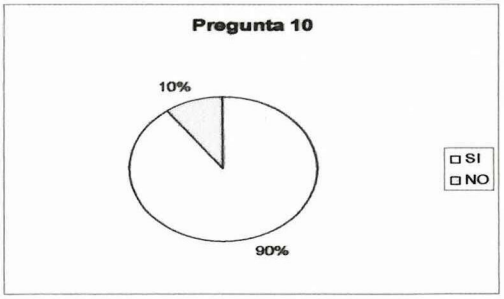
**10. ¿LA INCORPORACIÓN DE UN SISTEMA DE SEGURIDAD INFORMÁTICA COMO LINUX ENTERPRISE 3.0 BRINDARA MEJORES SOLUCIONES AL CONTROL DE LA INFORMACIÓN?**

**TABLA Nº 2.10: LINUX, MAYOR CONTROL DE INFORMACION.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| SI | 1 | 10 |
| NO | 9 | 90 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.10: LINUX, MAYOR CONTROL DE INFORMACION.**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**ANÁLISIS E INTERPRETACIÓN:**

El 90% de los encuestados considera que Linux enterprise 3.0 es una buena opción para mejorar la agilidad y seguridad en el entorno informático que maneja Aglomerados Cotopaxi S.A., hecho que le permitirá mejorar sustancialmente las seguridades a la información que se maneja en la empresa.

**11. ¿EL SERVIDOR WEB QUE CONTROLA LA INFORMACIÓN DE E-MAIL ES?**

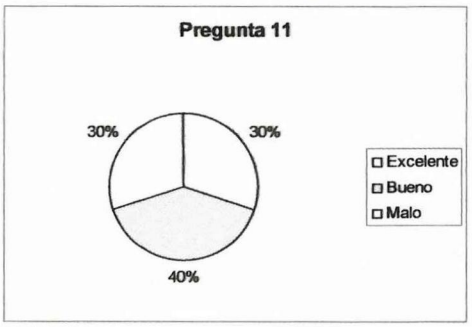
**a). Excelente** **b) Bueno** **c) Malo**

**TABLA Nº 2.11: SERVICIOS DEL SERVIDOR WEB.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| Excelente | 3 | 30 |
| Bueno | 4 | 40 |
| Malo | 3 | 30 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.11: SERVICIOS DEL SERVIDOR WEB**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**ANÁLISIS E INTERPRETACIÓN:**

El 30% de los encuestados señala que el servidor de e-mail es excelente, pues nunca se les ha congestionado este servicio, sin embargo el 40% de los encuestados cree que el servidor de e-mails que controla el servicio de correo interno y externo es bueno pero ven en un servidor controlado con Linux una magnifica opción para mejorar el servicio de correo interno; de igual manera hay un 30% de los encuestados que considera que este servicio es malo lo que les ha impedido recibir información a tiempo.

**12. MARQUE LAS CARACTERÍSTICAS QUE TIENE LINUX**

**a) Multitarea**

**b) Monousuario**

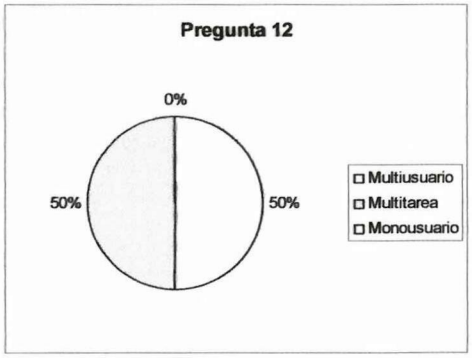
**c) Multiusuario**

**TABLA Nº 2.12: CONOCER LOS BENEFICIO DE LINUX.**

| ALTERNATIVAS | FRECUENCIAS | % |
|---|---|---|
| Monotarea | 5 | 50 |
| Monousuario | 0 | 00 |
| Multiusuario | 5 | 50 |
| TOTAL | 10 | 100 |

**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**GRÁFICO Nº 2.12: CONOCER LOS BENEFICIO DE LINUX.**




**FUENTE:** Encuesta
**REALIZADO POR:** Grupo Investigador

**ANÁLISIS E INTERPRETACIÓN:**

El 50% de los encuestados coinciden en que una de las características que ven en Linux es su facilidad de trabajar con multiusuarios es decir con varios usuarios a la vez; pero el otro 50% considera que Linux facilita el trabajo en multitarea, ambas características comparten las facilidades que brinda esta nueva alternativa de soporte informático que proponemos para la empresa Aglomerado Cotopaxi S.A.

## 2.7 COMPROBACIÓN DE HIPOTESIS.

### 2. 7. 1 VERIFICACIÒN DE HIPÓTESIS

### 2. 7. 2 ENUNCIADO:

Luego de haber aplicado las encuestas, tabulado y analizado los resultados obtenidos y cumpliendo con lo previsto se logró comprobar la siguiente hipótesis: **"La actualización de la Plataforma Linux 7.3 a Linux Enterprise 3.0, permitirá mejorar las destrezas y el desempeño en el trabajo; logrando satisfacer las necesidades de los usuarios de Aglomerados Cotopaxi S.A."**. Mediante doce preguntas (seis realizadas al personal de sistemas y tres a los usuarios); de las cuales la principal fue la siguiente:¿Conoce cual es el sistema que se encarga de brindarle mayor seguridad a la información que esta bajo su responsabilidad? Ante esta pregunta respondieron lo siguiente:

El 70% de los usuarios encuestados conocen que el sistema que provee de seguridad a todos los sistemas informáticos es Linux, considerándolo como una ventaja la facilidad de acceder al código y ajustarlo a las necesidades de la aplicación en la empresa, podemos decir entonces que como punto de partida no es del todo mala, pues como lo mencionan los usuarios, los conocimientos establecidos en ellos pueden adaptarse a la realidad de la empresa y lo único que haría falta es la constante preparación e información para los usuarios finales. Por

ende al decir que los conocimientos son similares no estamos afirmando que son efectivamente aplicables; ya que la realidad informática y tecnológica de países desarrollados es distinta a la de Ecuador.

El 20% señala que es Windows 2003 Server, quién se encarga de proporcionar y garantizar la seguridad de la información que manejan los usuarios del sistema, lo que nos indica que no todos los conocimientos son compartidos entre usuarios. El 10% señala que es Windows NT Server se encarga de la seguridad informática.

### 2.7.3 CONCLUSIÓN

El análisis establecido anteriormente, nos permite sostener que efectivamente la aplicación de un nuevo sistema de Seguridad Informática como lo es **una Intranet bajo Plataforma Linux Enterprise 3.0 en la Empresa Aglomerados Cotopaxi S.A.** permitirá desarrollar en los usuarios destrezas en el manejo de la aplicación que proponemos.

Al mismo tiempo este análisis nos ha permitido conocer el limitado conocimiento tecnológico de los usuarios y poder plantear una nueva alternativa que les permitirá brindar mayor seguridad a los sistemas informáticos con los que cuentan, así como también la capacitación para la explotación al máximo de Linux.

# CAPITULO III

# PROPUESTA

## 3.1. DESARROLLO DE LA PROPUESTA

### 3.1.1. TEMA:

**"SERVICIOS Y SEGURIDADES PARA UNA INTRANET BAJO PLATAFORMA LINUX ENTERPRISE 3.0 EN LA EMPRESA AGLOMERADOS COTOPAXI S.A."**

### 3.1.2. PRESENTACIÓN

Los servicios tecnológicos hoy es la principal preocupación de la empresa Aglomerados Cotopaxi S.A., puesto que con la automatización de algunos procesos se busca la excelencia y la calidad de los servicios; es así que hoy en día la organización se aprovecha del Internet para realizar transacciones bancarias, compras, correo electrónico, facturación y otros servicios.

Pero al mismo tiempo de la empresa establecida se aprovecha del avance tecnológico (Internet), se presentan problemas por la presencia de los famosos hackers y crackers, los cuales hacen que la información manejada tenga un alto riesgo; debido a lo cual se trata de proponer un estudio que nos indica las

bondades que tiene el plataforma Linux Enterprise buscan 3.0 como un servicio que ofrece mucha seguridad a los sistemas de información que en este caso lleva a cabo la organización empresarial mencionada.

En la propuesta investigativa se presentará un profundo análisis de las ventajas y desventajas que cuentan los sistemas operativos Windows y Linux, para concluir indicando las bondades con las que cuenta este último software.

Desafortunadamente la empresa objeto de la investigación deja la seguridad como algo para resolver luego, como un proceso que es ignorado y que pasa a segundo plano, tratando con la presente investigación concienciar la importancia de manejar información segura.

Finalmente este trabajo de investigación propuesto por los postulantes busca orientar soluciones a la seguridad, usando un Sistema Operativo de licencias GPL (GNU Public License) como lo es RedHat Linux 3.0 Advanced Server y conjuntamente con el hardware (servidor HP Proliant DL380 G3) para explotar al máximo las características de Linux.

### 3.1.3 JUSTIFICACIÓN

Al ser Linux es un sistema operativo muy potente y avanzado, capaz de manejar grandes portales de Internet o redes con centenares de estaciones de trabajo, su

permanencia está garantizada por la utilización de herramientas que abarcan procesos de mejora continua, en un esfuerzo sin precedentes de trabajo estable, libre y completo. Para Aglomerados Cotopaxi S.A. es una de las opciones más eficientes, para poner a esta empresa a la par con lo ultimo de la tecnología, mejorando los servicios que prestan para sus distintas áreas, tales como acceso a Internet, correo electrónico, servicios de compartición de archivos, etc.

Aglomerados Cotopaxi S.A. no puede estar al margen de esta modernización tecnológica, aún más al ser una empresa que cuenta con más de 27 años de vida, tiempo en el que se ha convertida en líder dentro del mercado maderero de la provincia como del país, manteniendo siempre presente como misión empresarial el brindar un servicio eficiente a sus clientes internos y generar servicios de calidad a sus clientes finales, lo que se garantizará con la implementación de un servidor de intranet con sistema operativo Linux Enterprise 3.0.

### 3.1.4 OBJETIVOS

#### 3.1.4.1 OBJETIVO GENERAL

Mejorar los servicios informáticos que actualmente presta Aglomerados Cotopaxi S.A., con el uso de Linux y brindar mayores beneficios en seguridad que le permita optimizar los recursos que le permita mantenerse como una empresa líder en el mercado maderero.

### 3.1.4.1 OBJETIVOS ESPECIFICOS

- Implementar RedHat Linux Enterprise 3.0 como el sistema operativo en el servidor principal de la empresa Aglomerados Cotopaxi S.A., para brindar una eficiente seguridad informática que permita a los usuarios recibir un servicio de calidad

- Verificar que los servicios proporcionados por el servidor mejoren sustancialmente políticas de seguridad tanto en la red interna como externa, así como en el servicio de Internet

- Utilizar un servidor con buenas características de hardware para lograr el cumplimiento de las metas propuestas por la empresa.

### 3.1.5 FUNDAMENTACION

La GPL (*GNU General Public License*) es el fundamento legal de la mayor parte de los programas libres. La GPL fija los derechos y obligaciones del poseedor de un determinado programa en relación al mismo. Se inventó a fin de asegurar que los programas que una vez fueron declarados libres continúen siéndolo, de suerte que no sea posible privatizarlos o arrebatarles su carácter público. La base legal de nuestro proyecto que en su totalidad esta desarrollado en Linux, está basado en licencias GPL que lo utilizaremos como sinónimo de *software* libre. Gnu/Linux es

un amplio conjunto de programas, que comprende un sistema operativo y numerosas aplicaciones, muy útil en las actividades concretas que lleva a cabo la empresa Aglomerados Cotopaxi S.A.

Gnu/Linux se levanta sobre una base de libertad, cosa que no sucede con ninguna mercancía, nadie le dice al desarrollador de Gnu/Linux qué ha de hacer, ni le remunera de alguna forma su actividad, todo lo que estas personas llevan a cabo lo hacen por propia iniciativa y por razones absolutamente personales, ningún jefe les dice lo que deben hacer, incluso cuando se someten a la coordinación de un proyecto lo hacen libremente, al entender que tal cosa es necesaria; en la sociedad GPL los bienes materiales estarían a disposición de cualquiera o se producirían cuando se necesitarán.

Al tener claro el concepto GPL sobre el cual esta desarrollado Linux y en el cual hemos basado nuestro trabajo de investigación, la empresa Aglomerados Cotopaxi S.A. aplicará políticas de seguridad y restricciones de acuerdo a sus necesidades.

### 3.1.6 DESARROLLO DE LA PROPUESTA

El siguiente proyecto de tesis está desarrollado en su totalidad en RedHat Linux Enterprise 3.0, fue implementado para mejorar los diferentes servicios informáticos que presta la empresa Aglomerados Cotopaxi S.A., para poder servir de mejor manera a sus clientes.

Para el presente trabajo de investigación se propuso la utilización de GNU/Linux que es un software de libre distribución, todo nuestro trabajo está dedicado a explotar el potencial de este producto; en una primera fase mostraremos paso a paso como se realizo la configuración de los principales servicios y después como se configuro las respectivas seguridades.

Al inicio se realizó un levantamiento de información sobre la situación actual de la empresa logrando recopilar ideas, sugerencias y sentimientos de los usuarios; con esta información se procedió a realizar un análisis de cómo mejorar la productividad de los usuarios.

Con este análisis se presentaron varias propuestas de mejoramiento, entre ellas una solución en Windows y otra en Linux, sobresaliendo con mucha acogida la solución presentada en Linux ya que por su costo reducido y mejores alternativas de seguridad se procedió a la ejecución del presente proyecto.

Para el presente trabajo de investigación se realizó la instalación de los siguientes servicios y seguridades de acuerdo al plan de trabajo o necesidades solicitadas por Aglomerados Cotopaxi S.A.

Configurar Servicios de DNS (Domain Name Server).

Configurar Servidor de Correo Electronico.

Configurar Servidor de Servicios WEB (Acceso a correo vía internet)

Configurar Servidor de Antivirus (Para el correo electrónico)

Configurar Servidor de Proxy

Configurar Reglas de Firewall (Acceso interno y externo)

Configurar Servidor SAMBA (Compartición de Archivos)

Configurar Servidor de Paginas WEB

Se recomendó al cliente el uso de IP estáticas para asegurar que el administrador tenga el registro sobre las IPs que están asignadas a cada usuario, así como también los permisos de acceso tal como se muestra en el ANEXO III, de igual manera se observa en el siguiente scrip:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1         localhost.localdomain    localhost

#Servidor de Red Interna
192.168.0.1       cotopaxi.com.ec         servidor
      www.cotopaxi.com.ec


# Red Externa
200.10.32.131           externo.cotopaxi.com.ec       firewall


#Usuarios de la RED INTERNA

192.168.0.10      pbarrera.cotopaxi.com.ec      pbarrera
192.168.0.11      mcabrera.cotopaxi.com.ec      mcabrera
192.168.0.12      xpinto.cotopaxi.com.ec        xpinto
192.168.0.13      pcaiza.cotopaxi.com.ec        pcaiza
192.168.0.14      jbustillos.cotopaxi.com.ec    jcbustillos
192.168.0.15      dacosa.cotopaxi.com.ec        dacosa
192.168.0.16      xruiz.cotopaxi.com.ec         xruiz
192.168.0.17      apaez.cotopaxi.com.ec         apaez
192.168.0.18      rpujos.cotopaxi.com.ec        rpujos
192.168.0.19      ejimenez.cotopaxi.com.ec      ejimenez
192.168.0.20      xvillaroel.cotopaxi.com.ec    xvillaroel
192.168.0.21      vavila.cotopaxi.com.ec        vavila
192.168.0.22      mtoaquiza.cotopaxi.com.ec     mtoaquiza
192.168.0.23      mvega.cotopaxi.com.ec         mvega
192.168.0.24      fdominguez.cotopaxi.com.ec    fdominguez
192.168.0.25      ftinoco.cotopaxi.com.ec       ftinoco
192.168.0.26      eguano.cotopaxi.com.ec        eguano
192.168.0.27      ebarbosa.cotopaxi.com.ec      ebarbosa
```

```
192.168.0.28      xvinueza.cotopaxi.com.ec       xvinueza
192.168.0.29      lsuntaxi.cotopaxi.com.ec       lsuntaxi
192.168.0.30      wchancusig.cotopaxi.com.ec     wchan
192.168.0.31      calbarracin.cotopaxi.com.ec    calbarracin
192.168.0.32      jzurita.cotopaxi.com.ec        jzurita
192.168.0.33      jcaÃ±izares.cotopaxi.com.ec    jcaÃ±izares
192.168.0.34      xbustillos.cotopaxi.com.ec     xbustillos
192.168.0.35      dponce.cotopaxi.com.ec         dponce
192.168.0.36      pargudo.cotopaxi.com.ec        pargudo
192.168.0.37      ysoria.cotopaxi.com.ec         ysoria
192.168.0.38      svera.cotopaxi.com.ec          svera
192.168.0.39      mheredia.cotopaxi.com.ec       mheredia
192.168.0.40      bperez.cotopaxi.com.ec         bperez
192.168.0.41      jfontecilla.cotopaxi.com.ec    jfontecilla
192.168.0.42      lrodriguez.cotopaxi.com.ec     lrodriguez
192.168.0.43      mmoreno.cotopaxi.com.ec        mmoreno
192.168.0.44      bhidalgo.cotopaxi.com.ec       bhidalgo
192.168.0.45      ealban.cotopaxi.com.ec         ealban
192.168.0.46      fcela.cotopaxi.com.ec          fcela
192.168.0.47      jpeÃ±aherrera.cotopaxi.com.ec jpeÃ±aherrera
192.168.0.48      dgarzon.cotopaxi.com.ec        dgarzon
192.168.0.49      mvanegas.cotopaxi.com.ec       mvanegas
192.168.0.50      clasificacion.cotopaxi.com.ec clasificacion
192.168.0.51      siempelkamp.cotopaxi.com.ec    siempelkamp
192.168.0.52      burkle.cotopaxi.com.ec         burkle
192.168.0.53      mdf.cotopaxi.com.ec            mdf
192.168.0.54      ccattani.cotopaxi.com.ec       ccattani
192.168.0.55      fgiron.cotopaxi.com.ec         fgiron
192.168.0.56      rvelasquez.cotopaxi.com.ec     rvelasquez
192.168.0.57      echuquilla.cotopaxi.com.ec     echuquilla
192.168.0.58      prosales.cotopaxi.com.ec       prosales
```

Se recomendó el uso de uno o 2 servidores para crear una DMZ, es decir crear una sola red de servidores a parte de la red interna, de esta manera segmentar el uso de los mismos pero el cliente por cuestiones de costos nos facilito un equipo modelo Proliant DL380 G3 (Ver ANEXO IV) que tiene las siguientes características de hardware:

- Un procesador Intel Xeon 3.20 Ghz / 2-MB L3 Cache / 533 Mhz
- Dos tarjetas de red incorporadas en la mainboard del servidor
- Una fuente de poder

- Una tarjeta controladora Smart Array 5i
- Seis discos de 18 GB (2 x RAID1 / 4 x RAID5)
- Una tarjeta PCI controladora U160
- Memoria RAM 6GB

Se creo a nivel de hardware dos unidades lógicas de discos distribuidas de la siguiente manera:

1. Unidad lógica de 18GB en RAID1 formada de 2 discos

2. Unidad lógica de 54GB en RAID5 formada de 4 discos

Debemos indicar que en el disco de 18GB se instalo el Sistema Operativo Red Hat Enterprise 3.0, en cambio el disco de 54GB se lo utilizó para guardar y respaldar todos los datos e información manejada por la empresa y que considera de vital importancia para lograr los objetivos que persiguen está industrial de reconocido prestigio nacional e internacional.

### 3.1.6.1 SERVIDOR DE RED TCP/IP

Una vez instalado el sistema operativo Red Hat Entreprise 3.0 en el equipo, se procedió a configurar las tarjetas de red y los demás servicios con sus respectivas seguridades, que a continuación detallamos.

#### 3.1.6.1.1 Configuración de la tarjeta RED TCP/IP

Se procedió a configurar las tarjetas de red del servidor, para lo cual Aglomerados Cotopaxi S.A. nos proporcionó información para configurar tanto la red interna, como la red externa:

**RED INTERNA**

- IP: 192.168.0.1
- Mascara: 255.255.255.0
- Red: 192.168.0.0
- Gateway: 192.168.0.1
- Nombre del Servidor de DNS 192.168.0.1

**RED EXTERNA**

- IP: 200.10.10.1
- Mascara: 255.255.255.240
- Red: 200.10.32.128
- Gateway: 200.10.32.158
- Nombre del Servidor de DNS 200.10.32.129

Los archivos necesarios para la configuración de la red son los siguientes:

- /etc/sysconfig/network
- /etc/sysconfig/network-scripts/ifcfg-eth*
- /etc/hosts
- /etc/host.conf
- /etc/resolv.conf

Utilizando lo archivos mencionados anteriormente se procedió como actividad siguiente a realizar la configuración de la red, para lo cual se empezó configurando el archivo /etc/sysconfig/network al cual accedimos de la siguiente manera:

- # vi /etc/sysconfig/network

El contenido de este archivo es el siguiente:

```
NETWORKING=yes
HOSTNAME=cotopaxi.com.ec
```

Es indispensable que se tome muy en cuenta y de manera particular que no es recomendable poner aquí el parámetro del GATEWAY, debido exclusivamente a que vamos a configurar más de dos tarjetas de red que utilizarán distinto GATEWAY.

Se continúa con la configuración del archivo /etc/sysconfig/network-scripts/ifcfg-eth0 como se muestra a continuación:

```
# Broadcom Corporation|NetXtreme BCM5705M_2 Gigabit Ethernet
DEVICE=eth0
#BOOTPROTO=dhcp
PROTO=static
HWADDR=00:14:C2:DC:F8:25
ONBOOT=yes
TYPE=Ethernet
IPADDR=192.168.0.1
NETMASK=255.255.255.0
NETWORK=192.168.0.0
BROADCAST=192.168.0.255
GATEWAY=200.10.32.131
```

De igual manera se configura el otro dispositivo de red eth1:

```
# 3Com Corporation|3cXFEM656C 10/100 LAN+Winmodem CardBus
[Tornado]
DEVICE=eth1
#BOOTPROTO=dhcp
PROTO=static
HWADDR=00:01:03:80:6F:D7
ONBOOT=yes
TYPE=Ethernet
IPADDR=200.10.32.131
NETMASK=255.255.255.240
NETWORK=200.10.32.128
BROADCAST=200.10.32.159
GATEWAY=200.10.32.158
```

A continuación se describen la funcionalidad de los parámetros utilizados:

- DEVICE: eth0, este parámetro es el identificador de la tarjeta de red, si tenemos mas de una tarjeta de red tendremos los siguientes parámetros eth1, eth2, etc.
- BOOTPROTO: static, tiene esta equivalencia debido a que la IP asignada es estática
- HWADDR, es el valor de la MAC ADDRESS
- IPADDR, es la IP asignada al equipo

- NETMASK, es la mascara de la red
- NETWORK, es el valor de la red
- ONBOOT, especifica si la red inicia al encender el equipo o reiniciarlo
- TYPE, es el tipo de red que tenemos
- GATEWAY, sirve como un equipo de pasarela par ver maquinas de otras redes

A continuación editamos el archivo /etc/hosts, aquí van los parámetros de identificación de las máquinas que forman parte de nuestra red e información de nuestro servidor, estas líneas indican los mecanismos de resolución que empiecen buscando en el fichero /etc/hosts y luego pregunten al servidor de nombres; el contenido del archivo configurado del servidor de Aglomerados Cotopaxi es el siguiente:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1   localhost.localdomain localhost
192.168.0.1 cotopaxi.com.ec   servidor www.cotopaxi.com.ec
200.10.32.131     externo.cotopaxi.com.ec firewall
```

En el siguiente archivo de configuración /etc/host.conf, se definen los parámetros para configurar el método por el cual nuestro servidor va ha resolver los nombres:

```
order hosts,bind
```

El parámetro hosts hace referencia que el equipo va ha resolver los nombres primero por el archivo /etc/hosts, en caso de no encontrarlos o no poder resolver

el nombre va ha consultar al servidor de DNS

En el archivo /etc/resolv.conf, definimos la IP de nuestro servidor de DNS

```
domain      cotopaxi.com.ec
nameserver  192.168.0.1
nameserver  200.10.32.129
nameserver  192.168.0.3
search cotopaxi.com.ec
```

Después de configurar estos parámetros de red, para que toda la configuración se haga efectiva se reinicia el servicio de red de la siguiente manera:

- #service network restart

### 3.1.6.1.2 SEGURIDAD DE LA RED

Para proveer la respectiva seguridad a la red y por el reducido número de personas que tienen acceso a las computadoras se decidió asignar IPs staticas para los usuarios, de esta manera se lleva un mejor control de acceso hacia los recursos de la intranet.

### 3.1.6.2 SERVIDOR DE CORREO ELECTRONICO (SENDMAIL)

Se procedió con la configuración del servidor de correo, para esto se verificó que estén instalados los paquetes necesarios para subir los servicios de correo, entonces el software para el servicio de correo electrónico se llama sendmail; este

software puede ser instalado, desde su código fuente que lo encontramos en www.sendmail.org o desde un rpm que viene en los cd de distribución, cualquier alternativa es valedera.

Con el siguiente comando instalamos el paquete:

- #rpm –iUvh sendmail-x.xx.x-x.i386.rpm

### 3.1.6.2.1 ARCHIVO DE CONFIGURACIÓN

Considerando la importancia que tiene este archivo para la empresa Aglomerados Cotopaxi S.A., se procede a configurar el servidor de correos MTA (Mail Transfer Agent) sendmail, creando un archivo de configuración del demónico del servicio llamado /etc/sendmail.cf desde un archivo "macro", alojado en /etc/mail/sendmail.mc.

Es altamente recomendado que no se cree ni se edite un archivo /etc/sendmail.mc manualmente. Este paquete viene con una utilidad llamada m4, que es la que genera el /etc/sendmail.mc.

A continuación veremos los parámetros para configurar el servidor de correo de la empresa industrial Aglomerados Cotopaxi S.A., esto se muestra en el siguiente script:

```
divert(-1)dnl
dnl #
dnl # This is the sendmail macro config file for m4. If you make
changes to
dnl # /etc/mail/sendmail.mc, you will need to regenerate the
dnl # /etc/mail/sendmail.cf file by confirming that the sendmail-
cf package is
dnl # installed and then performing a
dnl #
dnl #     make -C /etc/mail
dnl #
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
VERSIONID(`setup for Red Hat Linux')dnl
OSTYPE(`linux')dnl
dnl #
dnl # default logging level is 9, you might want to set it higher
to
dnl # debug the configuration
dnl #
dnl define(`confLOG_LEVEL', `9')dnl
dnl #
dnl # Uncomment and edit the following line if your outgoing mail
needs to
dnl # be sent out through an external mail server:
dnl #
dnl define(`SMART_HOST',`smtp.your.provider')
dnl #
define(`confDEF_USER_ID',``8:12'')dnl
dnl define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
define(`confTRY_NULL_MX_LIST',true)dnl
define(`confDONT_PROBE_INTERFACES',true)dnl
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`STATUS_FILE', `/var/log/mail/statistics')dnl
define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS',
`authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confAUTH_OPTIONS', `A')dnl
dnl #
dnl # The following allows relaying if the user authenticates, and
disallows
dnl # plaintext authentication (PLAIN/LOGIN) on non-TLS links
dnl #
dnl define(`confAUTH_OPTIONS', `A p')dnl
dnl #
dnl # PLAIN is the preferred plaintext authentication method and
used by
dnl # Mozilla Mail and Evolution, though Outlook Express and other
MUAs do
dnl # use LOGIN. Other mechanisms should be used if the connection
is not
dnl # guaranteed secure.
dnl #
dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
```

```
dnl define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5
CRAM-MD5 LOGIN PLAIN')dnl
dnl #
dnl # Rudimentary information on creating certificates for
sendmail TLS:
dnl #     make -C /usr/share/ssl/certs usage
dnl # or use the included makecert.sh script
dnl #
dnl define(`confCACERT_PATH',`/usr/share/ssl/certs')
dnl define(`confCACERT',`/usr/share/ssl/certs/ca-bundle.crt')
dnl define(`confSERVER_CERT',`/usr/share/ssl/certs/sendmail.pem')
dnl define(`confSERVER_KEY',`/usr/share/ssl/certs/sendmail.pem')
dnl #
dnl # This allows sendmail to use a keyfile that is shared with
OpenLDAP's
dnl # slapd, which requires the file to be readble by group ldap
dnl #
dnl define(`confDONT_BLAME_SENDMAIL',`groupreadablekeyfile')dnl
dnl #
dnl define(`confTO_QUEUEWARN', `4h')dnl
dnl define(`confTO_QUEUERETURN', `5d')dnl
dnl define(`confQUEUE_LA', `12')dnl
dnl define(`confREFUSE_LA', `18')dnl
define(`confTO_IDENT', `0')dnl
dnl FEATURE(delay_checks)dnl
FEATURE(`no_default_msa',`dnl')dnl
FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')dnl
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
dnl #
dnl # The -t option will retry delivery if e.g. the user runs over
his quota.
dnl #
FEATURE(local_procmail,`',`procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db',`hash -T<TMPF> -o /etc/mail/access.db')dnl
FEATURE(`blacklist_recipients')dnl
EXPOSED_USER(`root')dnl
dnl #
dnl # The following causes sendmail to only listen on the IPv4
loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the
loopback
dnl # address restriction to accept email from the internet or
intranet.
dnl #
DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port
587 for
dnl # mail from MUAs that authenticate. Roaming users who can't
reach their
```

```
dnl # preferred sendmail daemon due to port 25 being blocked or
redirected find
dnl # this useful.
dnl #
dnl DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port
465, but
dnl # starting immediately in TLS mode upon connecting. Port 25 or
587 followed
dnl # by STARTTLS is preferred, but roaming clients using Outlook
Express can't
dnl # do STARTTLS on ports other than 25. Mozilla Mail can ONLY
use STARTTLS
dnl # and doesn't support the deprecated smtps; Evolution <1.1.1
uses smtps
dnl # when SSL is enabled-- STARTTLS support is available in
version 1.1.1.
dnl #
dnl # For this to work your OpenSSL certificates must be
configured.
dnl #
dnl DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
dnl #
dnl # The following causes sendmail to additionally listen on the
IPv6 loopback
dnl # device. Remove the loopback address restriction listen to
the network.
dnl #
dnl DAEMON_OPTIONS(`port=smtp,Addr=::1, Name=MTA-v6,
Family=inet6')dnl
dnl #
dnl # enable both ipv6 and ipv4 in sendmail:
dnl #
dnl DAEMON_OPTIONS(`Name=MTA-v4, Family=inet, Name=MTA-v6,
Family=inet6')
dnl #
dnl # We strongly recommend not accepting unresolvable domains if
you want to
dnl # protect yourself from spam. However, the laptop and users on
computers
dnl # that do not have 24x7 DNS do need this.
dnl #
FEATURE(`accept_unresolvable_domains')dnl
dnl #
dnl FEATURE(`relay_based_on_MX')dnl
dnl #
dnl # Also accept email sent to "localhost.localdomain" as local
email.
dnl #
LOCAL_DOMAIN(`localhost.localdomain')dnl
dnl #
dnl # The following example makes mail from this host and any
additional
dnl # specified domains appear to be sent from mydomain.com
dnl #
```

```
MASQUERADE_AS(`cotopaxi.com.ec')dnl
MASQUERADE_DOMAIN(`cotopaxi.com.ec')
MASQUERADE_AS(cotopaxi.com.ec)
dnl #
dnl # masquerade not just the headers, but the envelope as well
dnl #
FEATURE(masquerade_envelope)dnl
dnl #
dnl # masquerade not just @mydomainalias.com, but
@*.mydomainalias.com as well
dnl #
FEATURE(masquerade_entire_domain)dnl
dnl #
dnl MASQUERADE_DOMAIN(localhost)dnl
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
```

Todas las líneas que empiezan con "dnl" son comentarios y no serán tomadas en cuenta al generar el /etc/sendmail.cf. Entonces para configurar nuestro servidor de sendmail de forma básica debemos cambiar las siguientes opciones:

Debemos cambiar la dirección IP donde se encuentre trabajando el servidor para que acepte todas las que se tienen configuradas.

DAEMON_OPTIONS(`Port=stmp,Addr=127.0.0.1, Name=MTA') por:

DAEMON_OPTIONS(`Port=stmp,Addr=0.0.0.0, Name=MTA')

También es necesario configurar el nombre completo del servidor, para esto es necesario que se cambie la línea:

- Cwlocalhost.localdomain; por la l,inea:

- Cwcotopaxi.com.ec

Cada vez que el servidor envié un correo a internet, deberá enviarlo añadiendo el nombre del dominio de su máquina, por eso debemos agregar las siguientes líneas al archivo macro:

- FEATURE(always_add_domain)dnl
- FEATURE(`masquerade_entire_domain')
- FEATURE(`masquerade_envelope')
- FEATURE(`allmasquerade')
- MASQUERADE_AS(`cotopaxi.com.ec')
- MASQUERADE_DOMAIN(`cotopaxi.com.ec')
- MASQUERADE_AS(cotopaxi.com.ec)

Posteriormente debemos proceder a generar el /etc/sendmail.cf, ejecutando el comando:

- # m4 /etc/mail/sendmail.mc > /etc/sendmail.mc

Finalmente para que funcione nuestro servidor de correo reiniciamos el servicio de sendmail con el siguiente comando:

- #/etc/rc.d/init.d/sendmail restart

### 3.1.6.2.2 SEGURIDAD PARA SENDMAIL

**a. FILTROS ANTISPAM.-** Una vez que tenemos funcionando nuestro servidor de correos, debemos saber donde podemos configurar ciertas seguridades con respecto al manejo del correo electrónico, por ejemplo para configurar sitios rechazados, usuarios rechazados y permitir el RELAY de ciertas máquinas debemos editar el archivo /etc/mail/access, como se muestra a continuación:

```
# Check the /usr/share/doc/sendmail/README.cf file for a
description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-
doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain   RELAY
localhost               RELAY
127.0.0.1               RELAY
192.168.0               RELAY
badspammer.com          550  NO ACEPTAMOS SPAMERS
```

El Antispam de la empresa Aglomerados Cotopaxi S.A. está configurado de la siguiente manera:

Estamos configurando para que todo los mail recibidos desde el dominio dadspammer.com sean rechazados y además reciban un mensaje de que "NO ACEPTAMOS SPAMERS", de igual manera en este archivo se agregaran los permisos correspondientes para que los dominios ACOSA, NOVACERO, COTOPAXI, etc., sean aceptados, con el relay solo estamos permitiendo de

nuestra red interna se configure para que este disponible al sendmail, para lo cual debemos ejecutar el siguiente comando:

#makemap hash /etc/mail/access < /etc/mail/access

Y al final debemos reiniciar nuevamente el servicio de sendmail y listo, además podemos configurar tanto, el máximo de bytes por mensaje y el máximo número de destinatarios por mensaje debemos editar el archivo /etc/sendmail.cf y configurar las siguientes líneas:

- MaxMessageSize=1000000
- MaxRecipientsPerMessage=100

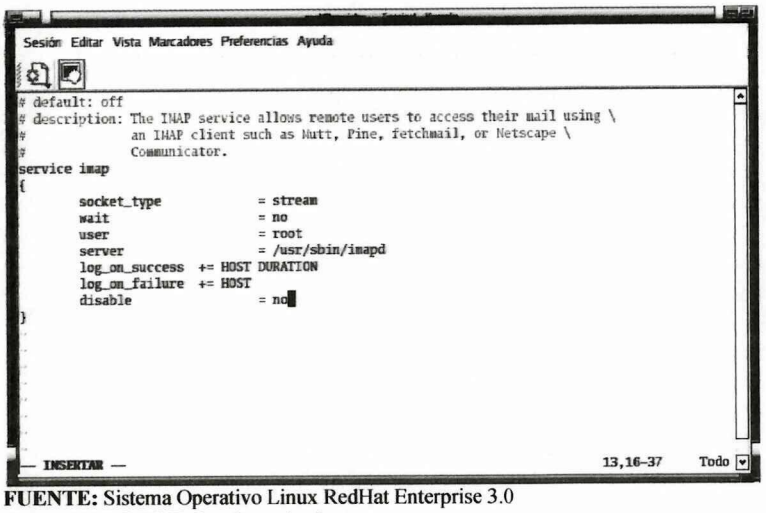
### 3.1.6.3 CONFIGURACIÓN DE WEBMAIL

Para configurar el servidor webmail de la empresa industrial Aglomerados Cotopaxi, S.A., se utiliza el protocolo IMAP que utiliza el puerto 143/tcp y en las distribuciones basadas en RedHat es instalado a traves del paquete imap-2002d-9.i386.

Se editó el archivo /etc/xinetd.d/imap y debemos asegurarnos que la siguiente línea tenga el valor "no" para que el servicio este habilitado:

- disable=no

**GRÁFICO Nº 3.1: CONFIGURACIÓN ARCHIVO/etc/xinetd.d/imap**



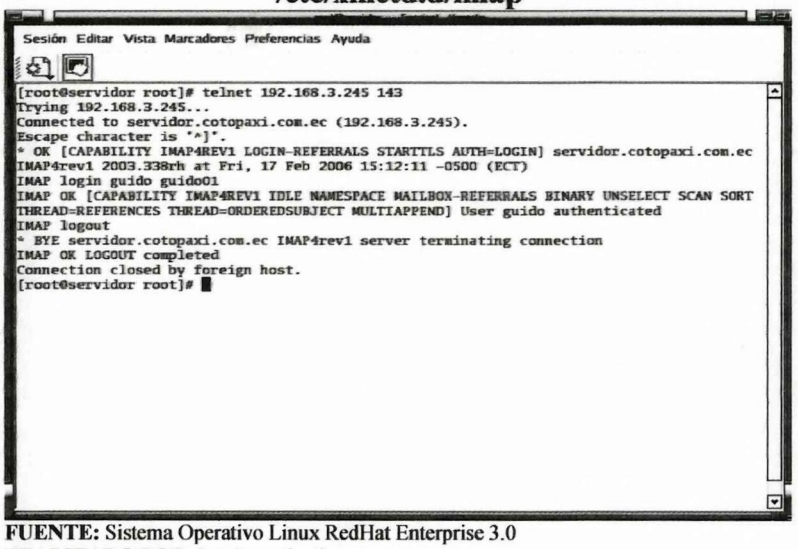

**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Es necesario, que una vez que realicemos el cambio de esta línea, debemos siempre en este caso asegurarnos de reiniciar el demónico de xinetd, con el siguiente comando:

- #/etc/rc.d/init.d/xinetd restart

Finalmente para verificar el funcionamiento del protocolo IMAP lo hacemos de la siguiente manera, haciendo un telnet a la IP de servidor en el puerto 143 debería responder como se muestra en el gráfico que a continuación se presenta:

**GRAFICO Nº 3.2: CONFIGURACIÓN ARCHIVO /etc/xinetd.d/imap**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

### 3.1.6.3.1 INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE WEBMAIL

Una vez configurado el IMAP necesitamos verificar que se encuentren instalados y funcionando; de no ser así se deberá realizar la instalación los siguientes paquetes.

- Sendmail 8.12.11-4-RHEL3.1.i386
- Apache -x-y-z.i386
- Imap 2002d-9.i386
- Php -4.3.2.-14-ent.i386

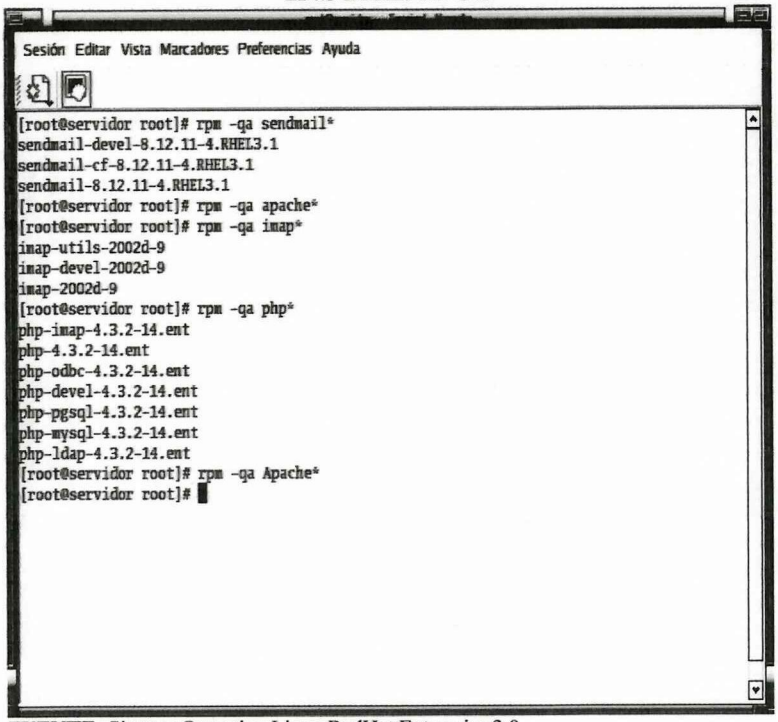
Esto lo hacemos de la siguiente manera:

Adicional a estos paquetes hay que instalar el siguiente que viene con los Cds de

la distribución de Linux.

#rpm –iUvh squirrelmail-1.4.3-0.e3.1.i386

**GRAFICO Nº 3.3: VERIFICACION DE PAQUETES INSTALADOS**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Y además editar el siguiente archivo /etc/squirrelmail/config.php y modificar las siguientes opciones:

- $domain {Poner aquí el dominio de la empresa}
- $imapServerAddress {Poner aquí la IP del servidor de correos}

```
<?php

/**
 * SquirrelMail Configuration File
 * Created using the configure script, conf.pl
```

```
 */

global $version;
$config_version = '1.4.0';
$config_use_color = 1;

$org_name      = "Aglomerados Cotopaxi S.A.";
$org_logo      = SM_PATH . 'images/sm_aglomerado.png';
$org_logo_width  = '308';
$org_logo_height = '111';
$org_title     = "Servidor de Correo Electronico $version";
$signout_page  = '';
$frame_top     = '_top';

$provider_uri     = 'http://www.squirrelmail.org/';

$provider_name     = 'SquirrelMail';

$motd = "";

$squirrelmail_default_language = 'en_US';

$domain                 = 'cotopaxi.com.ec';
$imapServerAddress      = '192.168.0.1';
$imapPort               = 143;
$useSendmail            = true;
$smtpServerAddress      = 'localhost';
$smtpPort               = 25;
$sendmail_path          = '/usr/sbin/sendmail';
$pop_before_smtp        = false;
$imap_server_type       = 'uw';
$invert_time            = false;
$optional_delimiter     = '/';

$default_folder_prefix          = 'mail/';
$trash_folder                   = 'Trash';
$sent_folder                    = 'Sent';
$draft_folder                   = 'Drafts';
$default_move_to_trash          = true;
$default_move_to_sent           = true;
$default_save_as_draft          = true;
$show_prefix_option             = true;
$list_special_folders_first     = true;
$use_special_folder_color       = true;
$auto_expunge                   = true;
$default_sub_of_inbox           = false;
$show_contain_subfolders_option = true;
$default_unseen_notify          = 2;
$default_unseen_type            = 1;
$auto_create_special            = true;
$delete_folder                  = false;
$noselect_fix_enable            = false;

$default_charset          = 'iso-8859-1';
$data_dir                 = '/var/lib/squirrelmail/prefs/';
$attachment_dir           = '/var/spool/squirrelmail/attach/';
```

```
$dir_hash_level           = 0;
$default_left_size        = '150';
$force_username_lowercase = false;
$default_use_priority     = true;
$hide_sm_attributions     = false;
$default_use_mdn          = true;
$edit_identity            = true;
$edit_name                = true;
$allow_thread_sort        = true;
$allow_server_sort        = true;
$allow_charset_search     = true;
$uid_support              = true;

$plugins[0] = 'delete_move_next';
$plugins[1] = 'squirrelspell';
$plugins[2] = 'newmail';

$theme_css = '';
$theme_default = 1;
$theme[0]['PATH'] = SM_PATH . 'themes/default_theme.php';
$theme[0]['NAME'] = 'Default';
$theme[1]['PATH'] = SM_PATH . 'themes/plain_blue_theme.php';
$theme[1]['NAME'] = 'Plain Blue';
$theme[2]['PATH'] = SM_PATH . 'themes/sandstorm_theme.php';
$theme[2]['NAME'] = 'Sand Storm';
$theme[3]['PATH'] = SM_PATH . 'themes/deepocean_theme.php';
$theme[3]['NAME'] = 'Deep Ocean';
$theme[4]['PATH'] = SM_PATH . 'themes/slashdot_theme.php';
$theme[4]['NAME'] = 'Slashdot';
$theme[5]['PATH'] = SM_PATH . 'themes/purple_theme.php';
$theme[5]['NAME'] = 'Purple';
$theme[6]['PATH'] = SM_PATH . 'themes/forest_theme.php';
$theme[6]['NAME'] = 'Forest';
$theme[7]['PATH'] = SM_PATH . 'themes/ice_theme.php';
$theme[7]['NAME'] = 'Ice';
$theme[8]['PATH'] = SM_PATH . 'themes/seaspray_theme.php';
$theme[8]['NAME'] = 'Sea Spray';
$theme[9]['PATH'] = SM_PATH . 'themes/bluesteel_theme.php';
$theme[9]['NAME'] = 'Blue Steel';
$theme[10]['PATH'] = SM_PATH . 'themes/dark_grey_theme.php';
$theme[10]['NAME'] = 'Dark Grey';
$theme[11]['PATH'] = SM_PATH . 'themes/high_contrast_theme.php';
$theme[11]['NAME'] = 'High Contrast';
$theme[12]['PATH'] = SM_PATH .
'themes/black_bean_burrito_theme.php';
$theme[12]['NAME'] = 'Black Bean Burrito';
$theme[13]['PATH'] = SM_PATH . 'themes/servery_theme.php';
$theme[13]['NAME'] = 'Servery';
$theme[14]['PATH'] = SM_PATH . 'themes/maize_theme.php';
$theme[14]['NAME'] = 'Maize';
$theme[15]['PATH'] = SM_PATH . 'themes/bluesnews_theme.php';
$theme[15]['NAME'] = 'BluesNews';
$theme[16]['PATH'] = SM_PATH . 'themes/deepocean2_theme.php';
$theme[16]['NAME'] = 'Deep Ocean 2';
$theme[17]['PATH'] = SM_PATH . 'themes/blue_grey_theme.php';
$theme[17]['NAME'] = 'Blue Grey';
```

```
$theme[18]['PATH'] = SM_PATH . 'themes/dompie_theme.php';
$theme[18]['NAME'] = 'Dompie';
$theme[19]['PATH'] = SM_PATH . 'themes/methodical_theme.php';
$theme[19]['NAME'] = 'Methodical';
$theme[20]['PATH'] = SM_PATH . 'themes/greenhouse_effect.php';
$theme[20]['NAME'] = 'Greenhouse Effect (Changes)';
$theme[21]['PATH'] = SM_PATH . 'themes/in_the_pink.php';
$theme[21]['NAME'] = 'In The Pink (Changes)';
$theme[22]['PATH'] = SM_PATH . 'themes/kind_of_blue.php';
$theme[22]['NAME'] = 'Kind of Blue (Changes)';
$theme[23]['PATH'] = SM_PATH . 'themes/monostochastic.php';
$theme[23]['NAME'] = 'Monostochastic (Changes)';
$theme[24]['PATH'] = SM_PATH . 'themes/shades_of_grey.php';
$theme[24]['NAME'] = 'Shades of Grey (Changes)';
$theme[25]['PATH'] = SM_PATH . 'themes/spice_of_life.php';
$theme[25]['NAME'] = 'Spice of Life (Changes)';
$theme[26]['PATH'] = SM_PATH . 'themes/spice_of_life_lite.php';
$theme[26]['NAME'] = 'Spice of Life - Lite (Changes)';
$theme[27]['PATH'] = SM_PATH . 'themes/spice_of_life_dark.php';
$theme[27]['NAME'] = 'Spice of Life - Dark (Changes)';
$theme[28]['PATH'] = SM_PATH . 'themes/christmas.php';
$theme[28]['NAME'] = 'Holiday - Christmas';
$theme[29]['PATH'] = SM_PATH . 'themes/darkness.php';
$theme[29]['NAME'] = 'Darkness (Changes)';
$theme[30]['PATH'] = SM_PATH . 'themes/random.php';
$theme[30]['NAME'] = 'Random (Changes every login)';
$theme[31]['PATH'] = SM_PATH . 'themes/midnight.php';
$theme[31]['NAME'] = 'Midnight';
$theme[32]['PATH'] = SM_PATH . 'themes/alien_glow.php';
$theme[32]['NAME'] = 'Alien Glow';
$theme[33]['PATH'] = SM_PATH . 'themes/dark_green.php';
$theme[33]['NAME'] = 'Dark Green';
$theme[34]['PATH'] = SM_PATH . 'themes/penguin.php';
$theme[34]['NAME'] = 'Penguin';

$default_use_javascript_addr_book = false;
$addrbook_dsn = '';
$addrbook_table = 'address';

$prefs_dsn = '';
$prefs_table = 'userprefs';
$prefs_user_field = 'user';
$prefs_key_field = 'prefkey';
$prefs_val_field = 'prefval';
$no_list_for_subscribe = false;
$smtp_auth_mech = 'none';
$imap_auth_mech = 'login';
$use_imap_tls = false;
$use_smtp_tls = false;
$session_name = 'SQMSESSID';

@include SM_PATH . 'config/config_local.php';

/**
 * Make sure there are no characters after the PHP closing
 * tag below (including newline characters and whitespace).
```

```
 * Otherwise, that character will cause the headers to be
 * sent and regular output to begin, which will majorly screw
 * things up when we try to send more headers later.
 */
?>
```

Para verificar el funcionamiento de nuestra página de webmail subimos primero el servicio de apache:

- # service httpd start

Y desde un browser cualquiera dentro de la red podemos acceder a nuestro correo mediante la siguiente dirección:

- http://192.168.3.245/webmail

### 3. 1.6.3.2 SEGURIDAD ANTIVIRUS PARA SENDMAIL Y WEBMAIL

Una vez instalado el servidor de mensajería electrónica (webmail y sendmail) de aglomerados Cotopaxi S.A., es posible que se convierta también en un medio de contagio informático para las máquinas con sistema operativo Windows, por este motivo a continuación se muestra como se instalo y configuro el producto Avira Antivirus Mister para Sendmail, un potente antivirus diseñado para trabajar muy ligadamente a sendmail con actualizaciones automáticas de vacunas y generación de alarmas hacia los administradores del sistema.

## a. INSTALACIÓN Y CONFIGURACIÓN DEL ANTIVIRUS

Después de obtener los instaladores del software antivirus en el sitio www.avira.com, y bajarse la versión para Sendmail Mister en S.O. Linux, el nombre del archivo debería ser ai-lx-milter-i386.tar.gz. Se lo descomprime ejecutando el siguiente comando.

#tar –zxvf ai-lx-milter-i386.tar.gz

Se creara una carpeta "avira-milter-1.0.0-6r3", que contendrá instaladores del software. Ingresamos al directorio y ejecutamos el programa que inicia el proceso de instalación llamado "aiinstall.pl" ejecútelo y responda las siguientes preguntas: Acepte los términos de la licencia, presionando "y", después las siguientes preguntas:

Enter the path where AVIRA for Sendmail-Milter V.1 binaries will be located
(default is: /usr/sbin): {PRESIONE ENTER}

The automatic internet updater will check every hour
if new updates are available. Default is yes.
Install the automatic internet updater? ([y]/n): {PRESIONE ENTER}

- AVIRA Feedback Agent Installer

Do you wish to install the AVIRA Feedback Agent? ([y]/n) {PRESIONE ENTER}

Please enter the path to the logs that will be parsed

[/var/log/aimilter.log] : {PRESIONE ENTER}

The Feedback Agent module will activate logging into

/var/log/aimilter.log in /etc/aimilter.conf .

Please enter the SMTP server to use: [localhost] 192.168.3.245

Please enther the SMTP port to use: [25]

The Feedback Agent module will send notices to server 192.168.3.245 on port 25.

Is it OK to add an entry in crontab to have the Feedback Agent

run every three hours? ([y]/n) {PRESIONE ENTER}

no crontab for root

no crontab for root

Installer finished sucessfully its job. The Feedback Agent

has been installed in /usr/lib/AVIRA/aviraFeedbackAgent.pl.

Y nos da un mensaje de que el proceso de instalación finalizo correctamente, en este momento se encuentra instalado el software de antivirus, con el proceso de actualización automática programada para que cada 2 horas se busquen actualizaciones de vacunas.

Para configurar cual es el email del administrador donde se enviaron los errores y notificaciones de alerta, debemos configurar la directiva "Postmaster" en el archivo /etc/aimilter.conf.

```
##########################################################################
#####
##                          aimilter.conf
##
##########################################################################
#####

# This file lists all the available parameters. Lines beginning
with '#'
# are comments and are ignored. When a parameter is not specified,
some
# default value is used.  The default values are the values shown
here,
# unless otherwise indicated.


# ------------------------------------------------------------------
--------
# AVIRA Milter will run as the specified user and group.

# User                              uucp
# Group                             uucp


# ------------------------------------------------------------------
--------
# Who will get errors and alert messages.

# Postmaster                        postmaster


# ------------------------------------------------------------------
--------
# MyHostName: FQDN of the local host.
```

```
# The default value, if not set in configuration file, is that
# obtained by gethostname(2), or if this fails, "localhost".

# MyHostName                        localhost


# ------------------------------------------------------------------
--------
# The spooldir must be owned by User:Group (as specified above)
# and must be accessible by only this user (mode = 0700).
# Both programs will yell and refuse to run if something is wrong.

# SpoolDir                          /var/spool/aimilter


# ------------------------------------------------------------------
--------
# AVIRADir: The AVIRA 'library' directory, where the VDF,
# the key, and some other files are stored.

# AVIRADir                        /usr/lib/AVIRA


# ------------------------------------------------------------------
--------
# TemporaryDir: Where the temporary files are stored
# (for example, attachments while checking them).
# It needs enough space to hold uncompressed attachments
# for each forwarder, and some more.
# Default: "/var/tmp" or else "/tmp".

# TemporaryDir                      /var/tmp


# ------------------------------------------------------------------
----------
# How to start aimilter if the -p command line argument
# is missing.

# ListenAddress inet:3333@localhost

# ------------------------------------------------------------------
--------
# Select the directory and binary of sendmail and the arguments
how to
# call sendmail.

# ForwardTo /usr/lib/sendmail -oem -oi


# ------------------------------------------------------------------
--------
# Maximum number of attachments to scan in single MIME mail.

# MaxAttachments                    100
```

```
# ------------------------------------------------------------------
--------
# Stop delivery of suspicious MIME mails. Occurs when
MaxAttachments
# has been reached.

# BlockSuspiciousMime             NO


# ------------------------------------------------------------------
--------
# Block mails which are coded as a fragmented message.
# "Message Fragmentation and Reassembly" (RFC2046, section
5.2.2.1).

# BlockFragmentedMessage              NO


# ------------------------------------------------------------------
--------
# Send notice mail to recipients.

# ExposeRecipientAlerts       NO


# ------------------------------------------------------------------
--------
# Send notice mail to sender.

# ExposeSenderAlerts                NO


# ------------------------------------------------------------------
--------
# Send notice mail to postmaster.


# ExposePostmasterAlerts            YES


# ------------------------------------------------------------------
--------
# User name of sender of alerts, if an alert was found in a mail.

# AlertsUser                  AvMilter
# or
# AlertsUser              someone@anywhere.tld


# ------------------------------------------------------------------
--------
# If RejectMailAlert is YES, a mail containing an alert will be
rejected
# to the mail client with the message "Alert found in email".
```

```
# It will be moved to the quarantine directory depending on the
setting
# QuarantineAlert.

# If RejectMailAlert is NO, mail will be accepted and moved to the
# quarantine directory.

# RejectAlertMail             NO


# ------------------------------------------------------------------
--------
# If QuarantineAlert is YES and RejectAlertMail is YES, a mail
# containing an alert will be rejected and the mail will be
quarantined.

# If QuarantineAlert is NO and RejectAlertMail is YES, the mail
will be
# rejected and will not be quarantined.

# QuarantineAlert       YES


# ------------------------------------------------------------------
--------
# If ScanInArchive is NO, no files in an archive will be scanned.

# If ScanInArchives is YES, all files in archives are going to be
extracted
# and scanned, depending on the resctrictions given with
# ArchiveMaxSize and ArchiveMaxRecursion.

# ScanInArchive       YES


# ------------------------------------------------------------------
--------
# If the compression ratio is above the value specified here,
# the mail will not be scanned completely.

# If ArchiveMaxRatio is 0, the mail be scanned completely.

# ArchiveMaxRatio 150


# ------------------------------------------------------------------
--------
# If ArchiveMaxSize is 0, all files in an archive will be
extracted,
# don't care of their unpacked size.

# If ArchiveMaxSize is >0, all files up to the adjusted size will
be
# extracted.

# ArchiveMaxSize        0
```

```
# ------------------------------------------------------------------
--------
# If ArchiveMaxRecursion is 0, recursive archives are going to be
# unpacked with an unlimited recursion depth.

# If ArchiveMaxRecursion is >0, recursive archives are going to be
# unpacked up to the adjusted recursion depth.

# ArchiveMaxRecursion        5


# ------------------------------------------------------------------
--------
# If BlockSuspiciousArchive is NO, don't stop delivery of mails
# containing archives with a suspicious recursion depth.

# If BlockSuspiciousArchive is YES, stop delivery of mails
# containing archives if ArchiveMaxRecursion has been reached.

# BlockSuspiciousArchive          NO


# ------------------------------------------------------------------
--------
# If BlockEncryptedArchive is NO, don't stop delivery of mails
# containing encrypted files in archives.

# If BlockEncryptedArchive is YES, stop delivery of mails
# containing encrypted files in an archive.

# BlockEncryptedArchive           NO


# ------------------------------------------------------------------
--------
# If AddXHeader is YES, information about scanning status is added
# to the header of checked mail. E.g.: "X-AntiVirus: Checked by
..."


# AddXHeader                  YES


# ------------------------------------------------------------------
--------
# ModifySubject adds the string "- Checked by ... -"  to the
# existing subject of a mail.

# ModifySubject                NO


# ------------------------------------------------------------------
--------
```

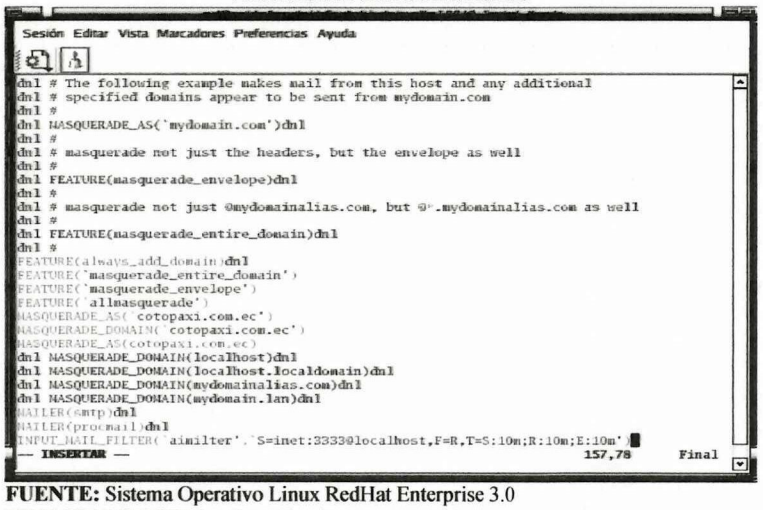
```
# ScanTimeout specifies the scan time of mail, in seconds, when to
stop
# scanning of mails.

# ScanTimeout                 300


# ------------------------------------------------------------------
--------
# Call external program or script if an alert was found. The
argument is the id of
# rejected message.

# ExternalProgram             /dir/my_own_script


# ------------------------------------------------------------------
--------
# Send notification mail every day 10 days before license will
expire.
# 0 means no notification mail.

# NotifyEndOfLicense                  10


# ------------------------------------------------------------------
--------
# If AddressFilter is YES, the recipient address and/or the sender
address of
# an email will be matched against a table of addresses.
# Two tables will be matched in a specified order (see option
"FilterTableOrder").
# For more details please have a look at the MANUAL.


# AddressFilter         NO


# ------------------------------------------------------------------
--------
# If AddressFilter is set to yes one can specify which table has
to be matched
# for a sender and/or recipient address first.
# Options are: scan,ignore | ignore,scan

# FilterTableOrder scan,ignore


# ------------------------------------------------------------------
--------
# If AddPrecedenceHeader is YES, a line (Precedence: junk) is
added to the
# header of a notice-mail. If neither YES nor NO is given, the
custom text
# will be inserted.
# This option causes some E-Mail-autoresponders to NOT respond
```

```
# to the received notice-mail.

# AddPrecedenceHeader         NO


# ------------------------------------------------------------------
--------
# The proxy feature in SAVAPI performs scans more efficiently
# by using and reusing a prepared pool of AVIRA scanners.  While
this
# pool increases throughput this feature requires the pool size
# to be wisely chosen -- too many scanners will put load on the
# machine without gaining more performance, too few scanners may
# have the SAVAPI using applications wait unnecessarily.

# UseProxy        NO


# ------------------------------------------------------------------
--------
# The number of prepared AVIRA scanners in the pool.
# See option "UseProxy"

# ProxyScanners         8


# ------------------------------------------------------------------
--------
# The maximum number of simultaneous allowed connections
# from AVIRA Milter to the scanner pool.

# ProxyConnections            32


# ------------------------------------------------------------------
--------
# Specify a full path with a filename to which AVIRA Milter
# will write its log messages. AVIRA Milter still logs to syslog
# even if this option is set.

# Default: NO - dont use custom logfile.

# E.g.: LogFile /var/log/aimilter.log

LogFile /var/log/aimilter.log


# ------------------------------------------------------------------
-----------
# Mail will not be accepted if an error occurs when connecting
# to the scan engine.

# RejectOnEngineError         yes
```

```
# ------------------------------------------------------------
-----------
# Do not use installed templates.

# UseTemplates          yes
```

Ahora debemos hacer que el servidor de correo envié antes de entregar el correo al buzón de los usuarios se lo envié a un socket de escucha donde se encuentra corriendo AVIRA y ejecutara el rastreo por Virus.Edite entonces el archivo /etc/mail/sendmail.mc y agregue al final la siguiente línea:

**GRAFICO Nº 3.4 CONFIGURACION ARCHIVO /etc/mail/sendmail.mc**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Una vez escrita esa línea en el /etc/mail/sendmail.mc debemos proceder a generar nuevamente un archivo de configuración

### 3.1.6.4 SERVIDOR SAMBA

El servidor SAMBA, de Aglomerados Cotopaxi S.A., esta configurado como se detalla a continuación pero primero explicaremos como se instalo el paquete

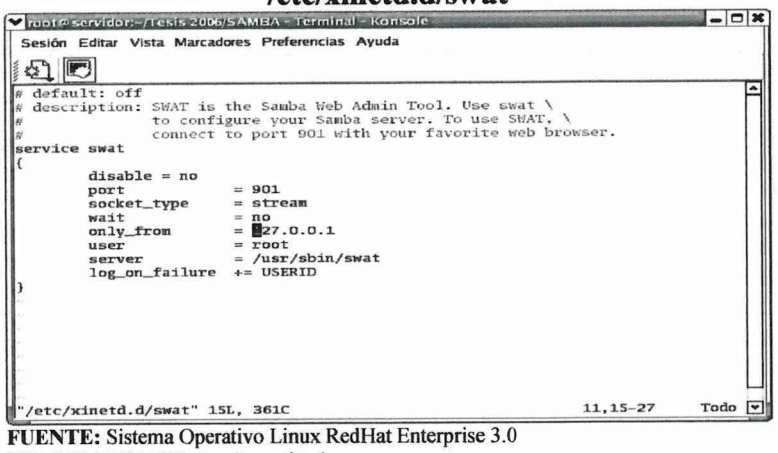
SAMBA durante el proceso de instalación de Linux, o desde el CDROM de instalación, ejecutando el siguiente comando:

# rpm –iUvh samba-3.0-6-2E.i386.rpm

### 3.1.6.4.1 CONFIGURACIÓN DE SAMBA

A continuación veremos como se edito los archivos de configuración de SAMBA de Aglomerados Cotopaxi S.A. esto para compartir archivos a determinados usuarios. Editamos el archivo /etc/xinetd.d/swat y verificamos que la opción disable sea igual a "no", esto es para habilitar el modo grafico de la configuración del servicio SAMBA. Como se muestra en el grafico:

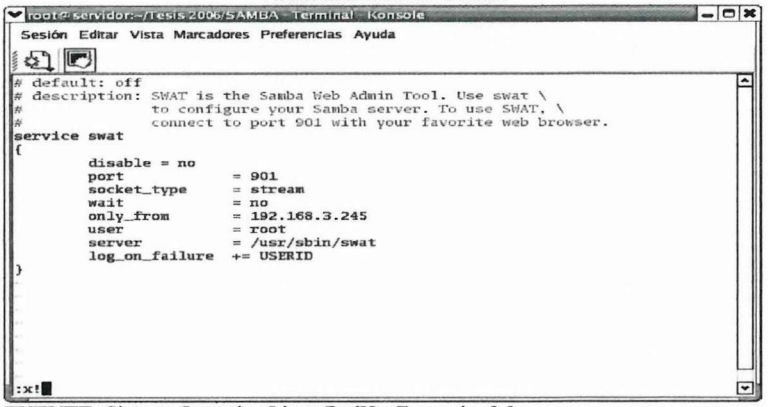
**GRAFICO Nº 3.5 CONFIGURACION ARCHIVO /etc/xinetd.d/swat**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Además en la opción only_from nos aseguramos de poner la "IP" de nuestro servidor; para que desde cualquier maquina que este en nuestra Intranet se pueda configurar este servicio. Como se muestra en el grafico:

**GRAFICO Nº 3.6 CONFIGURACION ARCHIVO /etc/xinetd.d/swat**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Ahora procederemos a configurar nuestro servidor SAMBA desde un browser de Internet digitando la IP de nuestro servidor y el puerto 901 Ej: 192.168.3.245:901. Este a su vez nos solicitara un "usuario" y "password", recordemos que se van a modificar archivos del Sistema por lo tanto solamente un usuario con permisos de ROOT puede acceder a este servicio.

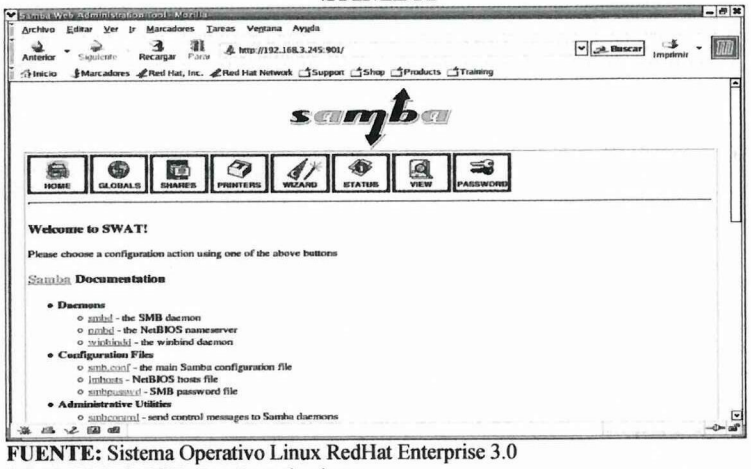
**GRAFICO Nº 3.7 VALIDACION DE USUARIO SAMBA**


**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Después de digitar el usuario y password tenemos la ventana de bienvenida donde podemos observar la ayuda de los archivos de configuración y comandos que nos

permiten configurar el servicio SAMBA, en el grafico se muestra esta pantalla de bienvenida.

**GRAFICO Nº 3.8 PANTALLA DE BIENVENIDA SAMBA**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

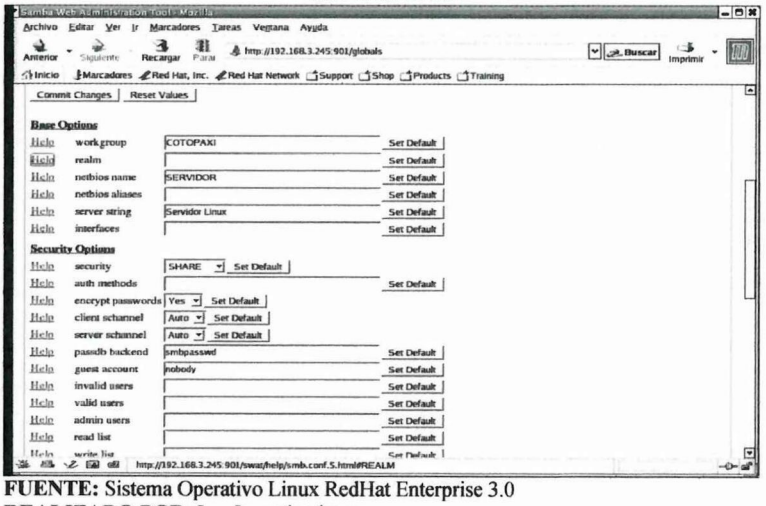
Para empezar a configurar nuestro servidor SAMBA desde el modo grafico nos vamos a la opción GLOBALS tal como se muestra en el grafico siguiente:

**GRAFICO Nº 3.9 EDICION DE ARCHIVOS PARA SAMBA**


**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Ahora procedemos a modificar esta información reemplazando por la información de la empresa como se muestra en el grafico siguiente:

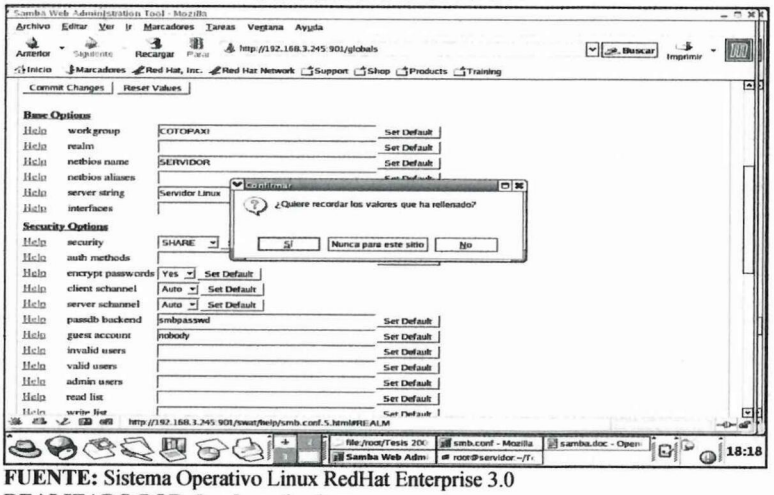
## GRAFICO Nº 3.10 EDICION PARAMETROS GLOBALS




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Una vez modificados con los datos de la empresa procedemos a guardar los cambios presionando el boton "Commit Changes" y nos pide una confirmación para guardar los cambios realizados tal como se muestra en el grafico

## GRAFICO Nº 3.11: GUARDAR CAMBIOS DE LA CONFIGURACION

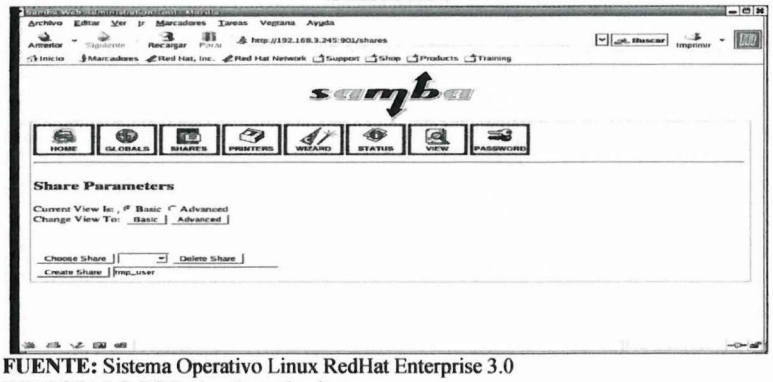



**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Después de que hemos configurado la información nuestro servidor vamos a proceder a compartir archivos que deben estar compartidos para los usuarios de

nuestra Intranet como se muestra a continuación en el siguiente grafico hacemos un clic en la opción "SHARES"

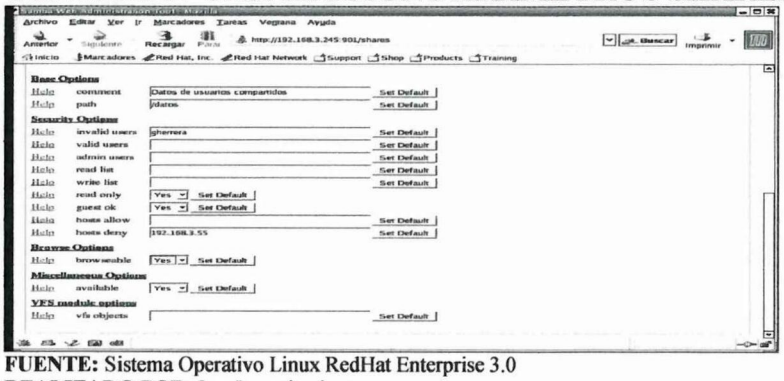
**GRAFICO Nº 3.12: EDICION PARAMETROS SHARES**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

A continuación damos un clic en el botón "Create Share" y procedemos a llenar los datos de la carpeta que deseemos compartir como se muestra en el grafico, en la opción "comment" ponemos un comentario sobre el archivos compartido, en la opción "path" digitamos el path de la carpeta que deseemos compartir y las demás opciones de acuerdo a la necesidad de los clientes

**GRAFICO Nº 3.13: EDICION PARAMETROS SHARES**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

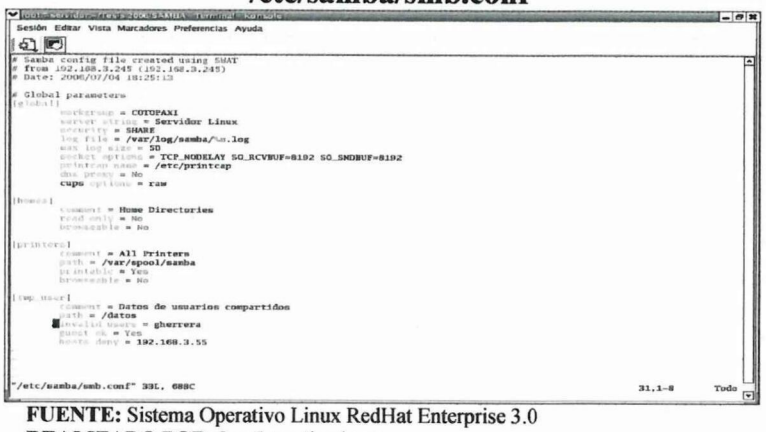
Para terminar de configurar nuestro servidor debemos reiniciar todos los servicios de SAMBA en la opcion "STATUS" como se muestra en el grafico, y hacemos un clic en la opción "Restart all".

**GRAFICO Nº 3.14: VERIFICAR ESTADO DE SERVICIOS SAMBA**


**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Y listo hemos configurado nuestro servidor SAMBA, ahora si deseamos o si se tiene mayor experiencia con Linux solamente podemos configurar el archivo /etc/samba/smb.conf como se muestra en el grafico, después de editar este archivo reiniciamos el servicio SAMBA de la siguiente manera: #service smb restart

**GRAFICO Nº 3.15: EDICION ARCHIVO /etc/samba/smb.conf**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

### 3.1.6.5 SERVIDOR DE PÁGINAS WEB

Se configuro el servidor web de Aglomerados Cotopaxi en su forma más básica para la publicación de su sitio web a la intranet.

Para instalar Apache Web Server tenemos dos formas posibles, la manera más sencilla vía RPM y la forma un poco menos fácil que es instalándola desde las fuentes del programa. Nos enfocaremos en la instalación vía RPM.

El Apache RPM instala archivos en los siguientes directorios:

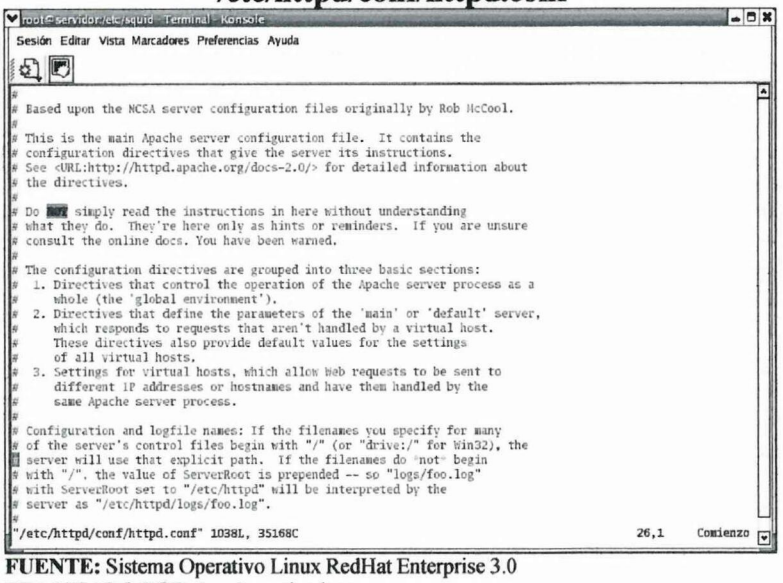
/etc/http/conf. Contiene los archivos de configuración del servidor Apache.
/etc/rc.d/. Contiene un arbol de directorios que contienen los scripts de inicio para apache.
/var/www/html. Estan los iconos del Server default, programas CGI y archivos HTML
/usr/doc /usr/man. Contine manuales y archivos README.
/usr/bin. Aquí se alojan los programas ejecutables de Apache.
/var/log/http. Los logs de eventos y errores son ubicados aquí.

#### 3.1.6.5.1 CONFIGURANDO EL SERVIDOR APACHE

Para configurar el servidor Apache de Aglomerados Cotopaxi S.A. se modifica el

siguiente archivo de configuración http.conf como se muestra en el grafico.

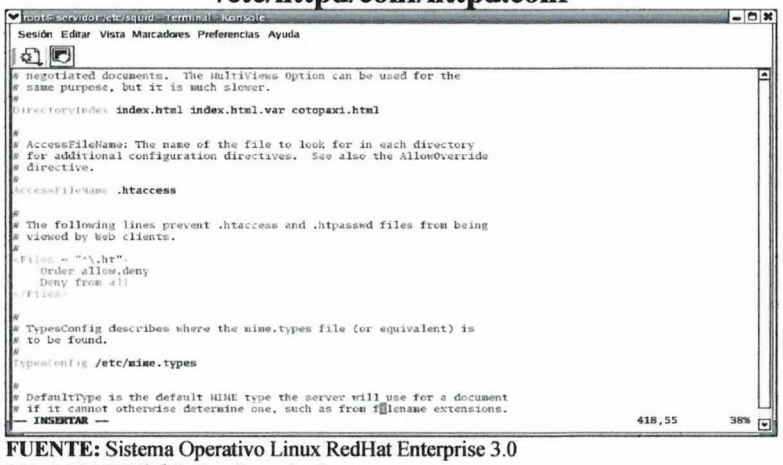
**GRAFICO Nº 3.16: CONFIGURACION ARCHIVO /etc/httpd/conf/httpd.conf**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Debemos verificar en este archivo que la opcion "DirectoryRoot" este apuntando al path /var/www/html, entonces nuestra pagina WEB debe estar dentro de este directorio, y configuramos la opción "DirectoryIndex" donde le decimos cuales son las paginas a abrirse por default, tal como se muestra en el grafico.

**GRAFICO Nº 3.17: CONFIGURACION ARCHIVO /etc/httpd/conf/httpd.conf**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

### 3.1.6.6 SERVIDOR DNS

Primero procedemos a verificar que los paquetes necesarios para este servicio, esten instalados, caso contrario hay que instalar los siguientes paquetes RPM que vienen en los CDs de distribución de Linux.

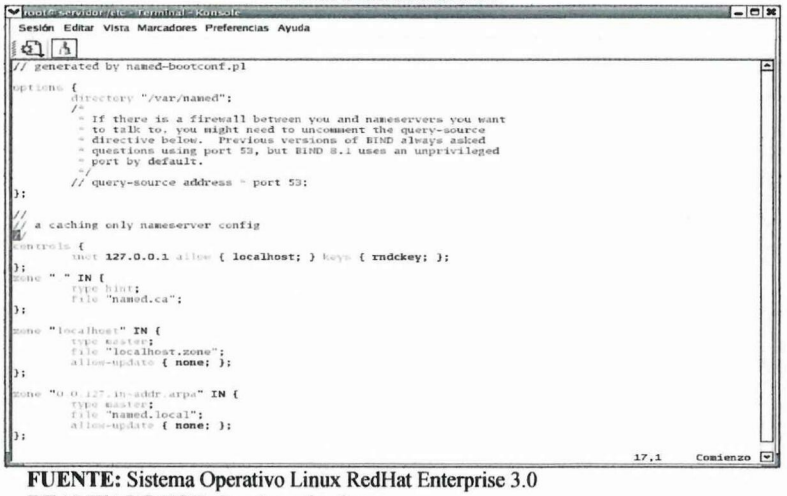
- rpm –i bind-9.2.4.EL3_10.i386
- rpm –i bind-utils-9.2.4.EL3_10.i386
- rpm –i caching-nameserver-7.2-7.i386

#### 3.1.6.6.1 CONFIGURACIÓN DEL DNS O BIND

La configuración del DNS pueden ser divididas en 2 áreas: la configuración propia del DNS y los archivos de las "zonas", los cuales son los que mantienen el mapeo de nombre/número actualizado; la configuración esta normalmente guardada en /etc/named.conf.

El /etc/named.conf utiliza una sintaxis estructurada que le permitirá realizar la configuración del DNS, con sentencias terminadas con punto y coma ";" y las llaves "{}" utilizadas para agrupar y determinar las acciones que cada comando o instrucción debe realizar para permitir activación configurada como se muestra a continuación en el gráfico en el que se describe paso a paso la configuración que se hace mención en el texto.

**GRAFICO Nº 3.18: EDICION ARCHIVO /etc/named.conf**

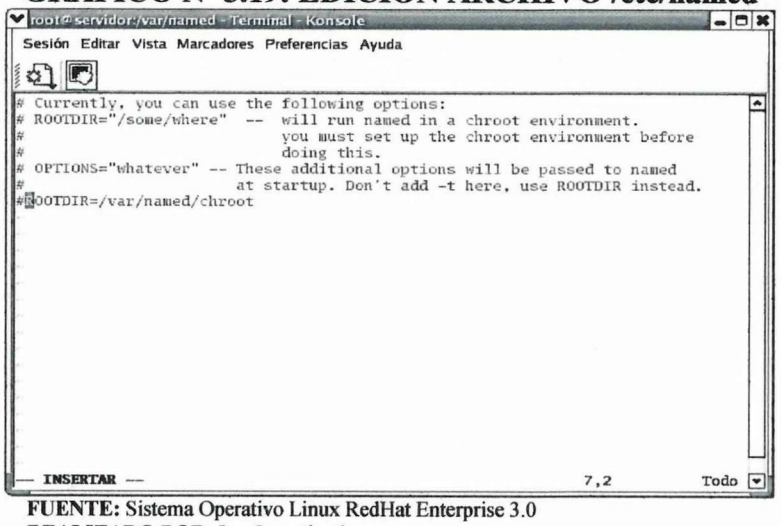



**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

El archivo de configuración del DSN de Aglomerados Cotopaxi S.A. esta configurado de la siguiente manera:

Para poner a funcionar correctamente nuestro servidor DNS es necesario primero editar el archivo /etc/named y comentar la siguiente línea de este archivo: ROOTDIR=/var/named/chroot como se muestra en el siguiente grafico

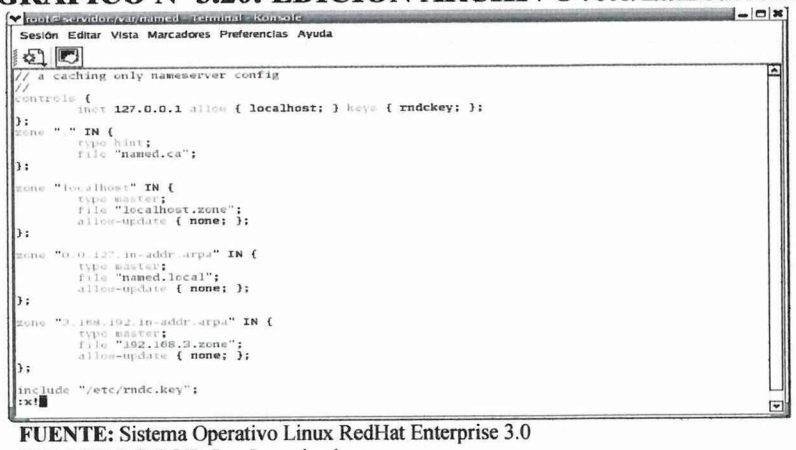
**GRAFICO Nº 3.19: EDICION ARCHIVO /etc/named**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Editamos el archivo /etc/named.conf, añadiendo la zona de resolución de direcciones IP reversa, como se muestra en la figura, haciendo referencia al archivo de configuración "192.168.3.zone".

**GRAFICO Nº 3.20: EDICION ARCHIVO /etc/named.conf**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Después procedemos a crear el archivo /var/named/192.168.3.zone, y lo editamos de la siguiente manera, indicando en la primera línea el nombre del servidor

**GRAFICO Nº 3.21: EDICION ARCHIVO /var/named/192.168.3.zone**


**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

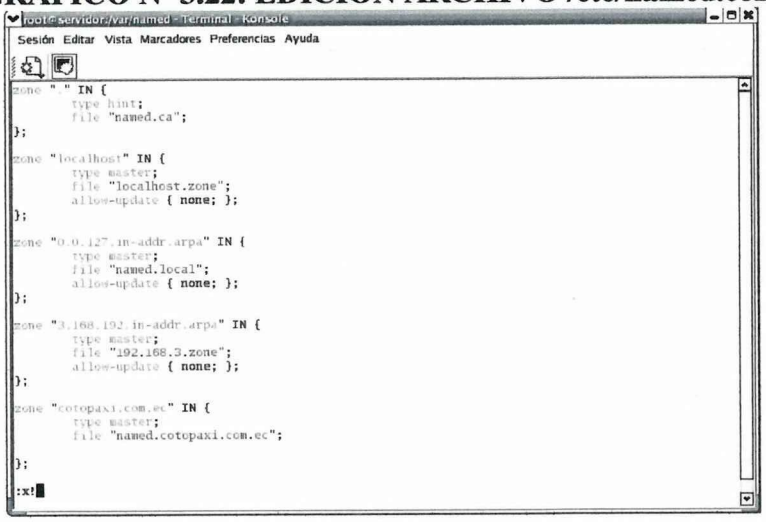
Esto son los primeros pasos para configurar nuestro servidor DNS, hasta este momento nuestro servidor seria un servidor de DNS CATCHING, es decir al

realizar una consulta de resolución de nombres este "recordara" la respuesta para una próxima consulta hacia ese mismo nombre.

Entonces el siguiente paso seria configurar nuestro servidor como un DNS MASTER, es decir que contenga archivos de zonas autorizadas, en este caso nuestra red es clase C (192.168.3.0/24).

Añadimos la zona master cotopaxi.com.ec como se muestra en el siguiente grafico, apuntando al archivo de configuración del DNS MASTER "named.cotopaxi.com.ec"

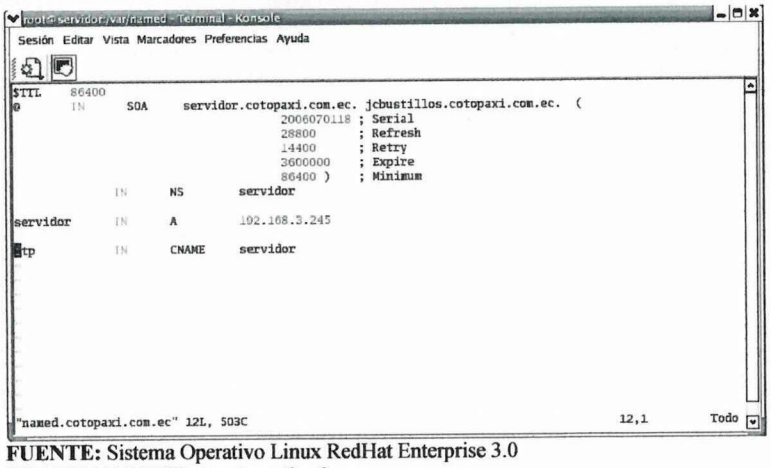
**GRAFICO Nº 3.22: EDICION ARCHIVO /etc/named.conf**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Creamos el archivo de configuración /etc/named/named.cotopaxi.com.ec y editamos de la siguiente manera como se muestra en el gráfico.

**GRAFICO Nº 3.23: EDICION ARCHIVO /etc/named.conf**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Con este paso hemos definido el archivo de resolución inversa.

Para que el sistema actualice los cambios realizados, como último paso debemos reiniciar el demonio de DNS, ejecutando el siguiente comando:

```
[root@servidor named]# /etc/rc.d/init.d/named restart
Parando named:                                [ OK ]
Iniciando named:                              [ OK ]
[root@servidor named]#
```

Y con la ayuda del comando NSLOOKUP, probaremos el funcionamiento de nuestro servidor DNS:

```
[root@servidor named]# nslookup -sil servidor.cotopaxi.com.ec
Server:         192.168.3.245
Address:        192.168.3.245#53

Name:   servidor.cotopaxi.com.ec
Address: 192.168.3.245

[root@servidor named]#
```

Se puede verificar que tenemos respuesta desde el servidor 192.168.3.245.

### 3.1.6.7 SERVICIO PROXY

El software en Linux para instalar un servidor Proxy se llama SQUID, el cual es un servidor Proxy de alto rendimiento para HTTP y FTP además de poseer cache. A continuación explicaremos la forma de cómo se instalo y como lo configuramos en Aglomerados Cotopaxi S.A.

rpm –i squid-2.5.STABLE-6.3E.i386

#### 3.1.6.7.1 CONFIGURACIÓN DEL SERVIDOR PROXY

Una vez instalado el squid debemos configurarlo apropiadamente; para esto modificamos el siguiente archivo /etc/squid/squid.conf, de acuerdo a las necesidades de Aglomerados Cotopaxi S.A., tal como se muestra en el script

```
#       WELCOME TO SQUID 2
#       ------------------
#
#       This is the default Squid configuration file. You may wish
#       to look at the Squid home page (http://www.squid-cache.org/)
#       for the FAQ and other documentation.
#
#       The default Squid config file shows what the defaults for
#       various options happen to be.  If you don't need to change the
#       default, you shouldn't uncomment the line.  Doing so may cause
#       run-time problems.  In some cases "none" refers to no default
#       setting at all, while in other cases it refers to a valid
#       option - the comments for that keyword indicate if this is the
#       case.
#
```

```
# NETWORK OPTIONS
# -----------------------------------------------------------------------------

#  TAG: http_port
#       Usage: port
#              hostname:port
#              1.2.3.4:port
#
#       The socket addresses where Squid will listen for HTTP client
#       requests.  You may specify multiple socket addresses.
#       There are three forms: port alone, hostname with port, and
#       IP address with port.  If you specify a hostname or IP
#       address, then Squid binds the socket to that specific
#       address.  This replaces the old 'tcp_incoming_address'
#       option.  Most likely, you do not need to bind to a specific
#       address, so you can use the port number alone.
#
#       The default port number is 3128.
#
#       If you are running Squid in accelerator mode, then you
#       probably want to listen on port 80 also, or instead.
#
#       The -a command line option will override the *first* port
#       number listed here.   That option will NOT override an IP
#       address, however.
#
#       You may specify multiple socket addresses on multiple lines.
#
#       If you run Squid on a dual-homed machine with an internal
#       and an external interface then we recommend you to specify the
#       internal address:port in http_port. This way Squid will only be
#       visible on the internal address.
#
#Default:
 http_port 3128

#  TAG: https_port
#        Usage:  [ip:]port cert=certificate.pem [key=key.pem] [options...]
#
#        The socket address where Squid will listen for HTTPS client
#        requests.
#
#        This is really only useful for situations where you are running
#        squid in accelerator mode and you want to do the SSL work at the
#        accelerator level.
#
#       You may specify multiple socket addresses on multiple lines,
#       each with their own SSL certificate and/or options.
#
#       Options:
#
#          cert=       Path to SSL certificate (PEM format)
#
#          key=        Path to SSL private key file (PEM format)
#                      if not specified, the certificate file is
#                      assumed to be a combined certificate and
#                      key file
#
#          version=    The version of SSL/TLS supported
#                          1  automatic (default)
#                          2  SSLv2 only
#                          3  SSLv3 only
#                          4  TLSv1 only
#
#          cipher=     Colon separated list of supported ciphers
#
#          options=    Varions SSL engine options. The most important
#                      being:
#                          NO_SSLv2  Disallow the use of SSLv2
#                          NO_SSLv3  Disallow the use of SSLv3
#                          NO_TLSv1  Disallow the use of TLSv1
```

```
#                     See src/ssl_support.c or OpenSSL documentation
#                     for a more complete list.
#
#Default:
# none

#  TAG: ssl_unclean_shutdown
#       Some browsers (especially MSIE) bugs out on SSL shutdown
#       messages.
#
#Default:
# ssl_unclean_shutdown off

#  TAG: icp_port
#       The port number where Squid sends and receives ICP queries to
#       and from neighbor caches.  Default is 3130.  To disable use
#       "0".  May be overridden with -u on the command line.
#
#Default:
# icp_port 3130

#  TAG: htcp_port
# Note: This option is only available if Squid is rebuilt with the
#       --enable-htcp option
#
#       The port number where Squid sends and receives HTCP queries to
#       and from neighbor caches.  Default is 4827.  To disable use
#       "0".
#
#Default:
# htcp_port 4827

#  TAG: mcast_groups
#       This tag specifies a list of multicast groups which your server
#       should join to receive multicasted ICP queries.
#
#       NOTE!  Be very careful what you put here!  Be sure you
#       understand the difference between an ICP _query_ and an ICP
#       _reply_.  This option is to be set only if you want to RECEIVE
#       multicast queries.  Do NOT set this option to SEND multicast
#       ICP (use cache_peer for that).  ICP replies are always sent via
#       unicast, so this option does not affect whether or not you will
#       receive replies from multicast group members.
#
#       You must be very careful to NOT use a multicast address which
#       is already in use by another group of caches.
#
#       If you are unsure about multicast, please read the Multicast
#       chapter in the Squid FAQ (http://www.squid-cache.org/FAQ/).
#
#       Usage: mcast_groups 239.128.16.128 224.0.1.20
#
#       By default, Squid doesn't listen on any multicast groups.
#
#Default:
# none

#  TAG: udp_incoming_address
#  TAG: udp_outgoing_address
#       udp_incoming_address  is used for the ICP socket receiving packets
#                             from other caches.
#       udp_outgoing_address  is used for ICP packets sent out to other
#                             caches.
#
#       The default behavior is to not bind to any specific address.
#
#       A udp_incoming_address value of 0.0.0.0 indicates that Squid should
#       listen for UDP messages on all available interfaces.
#
#       If udp_outgoing_address is set to 255.255.255.255 (the default)
#       then it will use the same socket as udp_incoming_address. Only
```

```
#       change this if you want to have ICP queries sent using another
#       address than where this Squid listens for ICP queries from other
#       caches.
#
#       NOTE, udp_incoming_address and udp_outgoing_address can not
#       have the same value since they both use port 3130.
#
#Default:
# udp_incoming_address 0.0.0.0
# udp_outgoing_address 255.255.255.255


# OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
# -----------------------------------------------------------------------------

#  TAG: cache_peer
#       To specify other caches in a hierarchy, use the format:
#
#              cache_peer hostname type http_port icp_port
#
#       For example,
#
#       #                                        proxy  icp
#       #          hostname             type     port   port  options
#       #          -------------------- -------- -----  -----  -----------
#       cache_peer parent.foo.net       parent    3128  3130  [proxy-only]
#       cache_peer sib1.foo.net         sibling   3128  3130  [proxy-only]
#       cache_peer sib2.foo.net         sibling   3128  3130  [proxy-only]
#
#            type:  either 'parent', 'sibling', or 'multicast'.
#
#       proxy_port:  The port number where the cache listens for proxy
#                    requests.
#
#         icp_port:  Used for querying neighbor caches about
#                    objects.  To have a non-ICP neighbor
#                    specify '7' for the ICP port and make sure the
#                    neighbor machine has the UDP echo port
#                    enabled in its /etc/inetd.conf file.
#
#           options: proxy-only
#                    weight=n
#                    ttl=n
#                    no-query
#                    default
#                    round-robin
#                    multicast-responder
#                    closest-only
#                    no-digest
#                    no-netdb-exchange
#                    no-delay
#                    login=user:password | PASS | *:password
#                    connect-timeout=nn
#                    digest-url=url
#                    allow-miss
#                    max-conn
#                    htcp
#                    carp-load-factor
#
#                    use 'proxy-only' to specify that objects fetched
#                    from this cache should not be saved locally.
#
#                    use 'weight=n' to specify a weighted parent.
#                    The weight must be an integer.  The default weight
#                    is 1, larger weights are favored more.
#
#                    use 'ttl=n' to specify a IP multicast TTL to use
#                    when sending an ICP queries to this address.
#                    Only useful when sending to a multicast group.
#                    Because we don't accept ICP replies from random
#                    hosts, you must configure other group members as
```

```
#                peers with the 'multicast-responder' option below.
#
#                use 'no-query' to NOT send ICP queries to this
#                neighbor.
#
#                use 'default' if this is a parent cache which can
#                be used as a "last-resort." You should probably
#                only use 'default' in situations where you cannot
#                use ICP with your parent cache(s).
#
#                use 'round-robin' to define a set of parents which
#                should be used in a round-robin fashion in the
#                absence of any ICP queries.
#
#                'multicast-responder' indicates that the named peer
#                is a member of a multicast group.  ICP queries will
#                not be sent directly to the peer, but ICP replies
#                will be accepted from it.
#
#                'closest-only' indicates that, for ICP_OP_MISS
#                replies, we'll only forward CLOSEST_PARENT_MISSes
#                and never FIRST_PARENT_MISSes.
#
#                use 'no-digest' to NOT request cache digests from
#                this neighbor.
#
#                'no-netdb-exchange' disables requesting ICMP
#                RTT database (NetDB) from the neighbor.
#
#                use 'no-delay' to prevent access to this neighbor
#                from influencing the delay pools.
#
#                use 'login=user:password' if this is a personal/workgroup
#                proxy and your parent requires proxy authentication.
#                Note: The string can include URL escapes (i.e. %20 for
#                spaces). This also means that % must be written as %%.
#
#                use 'login=PASS' if users must authenticate against
#                the upstream proxy. This will pass the users credentials
#                as they are to the peer proxy. This only works for the
#                Basic HTTP authentication sheme. Note: To combine this
#                with proxy_auth both proxies must share the same user
#                database as HTTP only allows for one proxy login.
#                Also be warned that this will expose your users proxy
#                password to the peer. USE WITH CAUTION
#
#                use 'login=*:password' to pass the username to the
#                upstream cache, but with a fixed password. This is meant
#                to be used when the peer is in another administrative
#                domain, but it is still needed to identify each user.
#                The star can optionally be followed by some extra
#                information which is added to the username. This can
#                be used to identify this proxy to the peer, similar to
#                the login=username:password option above.
#
#                use 'connect-timeout=nn' to specify a peer
#                specific connect timeout (also see the
#                peer_connect_timeout directive)
#
#                use 'digest-url=url' to tell Squid to fetch the cache
#                digest (if digests are enabled) for this host from
#                the specified URL rather than the Squid default
#                location.
#
#                use 'allow-miss' to disable Squid's use of only-if-cached
#                when forwarding requests to siblings. This is primarily
#                useful when icp_hit_stale is used by the sibling. To
#                extensive use of this option may result in forwarding
#                loops, and you should avoid having two-way peerings
#                with this option. (for example to deny peer usage on
#                requests from peer by denying cache_peer_access if the
```

```
#                   source is a peer)
#
#                   use 'max-conn' to limit the amount of connections Squid
#                   may open to this peer.
#
#                   use 'htcp' to send HTCP, instead of ICP, queries
#                   to the neighbor.  You probably also want to
#                   set the "icp port" to 4827 instead of 3130.
#
#                   use 'carp-load-factor=f' to define a parent
#                   cache as one participating in a CARP array.
#                   The 'f' values for all CARP parents must add
#                   up to 1.0.
#
#
#       NOTE: non-ICP/HTCP neighbors must be specified as 'parent'.
#
#Default:
# none

#  TAG: cache_peer_domain
#       Use to limit the domains for which a neighbor cache will be
#       queried.  Usage:
#
#       cache_peer_domain cache-host domain [domain ...]
#       cache_peer_domain cache-host !domain
#
#       For example, specifying
#
#              cache_peer_domain parent.foo.net     .edu
#
#       has the effect such that UDP query packets are sent to
#       'bigserver' only when the requested object exists on a
#       server in the .edu domain.  Prefixing the domainname
#       with '!' means that the cache will be queried for objects
#       NOT in that domain.
#
#       NOTE:   * Any number of domains may be given for a cache-host,
#                 either on the same or separate lines.
#               * When multiple domains are given for a particular
#                 cache-host, the first matched domain is applied.
#               * Cache hosts with no domain restrictions are queried
#                 for all requests.
#               * There are no defaults.
#               * There is also a 'cache_peer_access' tag in the ACL
#                 section.
#
#Default:
# none

#  TAG: neighbor_type_domain
#       usage: neighbor_type_domain parent|sibling domain domain ...
#
#       Modifying the neighbor type for specific domains is now
#       possible.  You can treat some domains differently than the the
#       default neighbor type specified on the 'cache_peer' line.
#       Normally it should only be necessary to list domains which
#       should be treated differently because the default neighbor type
#       applies for hostnames which do not match domains listed here.
#
#EXAMPLE:
#       cache_peer  parent cache.foo.org 3128 3130
#       neighbor_type_domain cache.foo.org sibling .com .net
#       neighbor_type_domain cache.foo.org sibling .au .de
#
#Default:
# none

#  TAG: icp_query_timeout     (msec)
#       Normally Squid will automatically determine an optimal ICP
#       query timeout value based on the round-trip-time of recent ICP
```

```
#       queries.  If you want to override the value determined by
#       Squid, set this 'icp_query_timeout' to a non-zero value.  This
#       value is specified in MILLISECONDS, so, to use a 2-second
#       timeout (the old default), you would write:
#
#               icp_query_timeout 2000
#
#Default:
# icp_query_timeout 0

#  TAG: maximum_icp_query_timeout     (msec)
#       Normally the ICP query timeout is determined dynamically.  But
#       sometimes it can lead to very large values (say 5 seconds).
#       Use this option to put an upper limit on the dynamic timeout
#       value.  Do NOT use this option to always use a fixed (instead
#       of a dynamic) timeout value. To set a fixed timeout see the
#       'icp_query_timeout' directive.
#
#Default:
# maximum_icp_query_timeout 2000

#  TAG: mcast_icp_query_timeout       (msec)
#       For Multicast peers, Squid regularly sends out ICP "probes" to
#       count how many other peers are listening on the given multicast
#       address.  This value specifies how long Squid should wait to
#       count all the replies.  The default is 2000 msec, or 2
#       seconds.
#
#Default:
# mcast_icp_query_timeout 2000

#  TAG: dead_peer_timeout     (seconds)
#       This controls how long Squid waits to declare a peer cache
#       as "dead."  If there are no ICP replies received in this
#       amount of time, Squid will declare the peer dead and not
#       expect to receive any further ICP replies.  However, it
#       continues to send ICP queries, and will mark the peer as
#       alive upon receipt of the first subsequent ICP reply.
#
#       This timeout also affects when Squid expects to receive ICP
#       replies from peers.  If more than 'dead_peer' seconds have
#       passed since the last ICP reply was received, Squid will not
#       expect to receive an ICP reply on the next query.  Thus, if
#       your time between requests is greater than this timeout, you
#       will see a lot of requests sent DIRECT to origin servers
#       instead of to your parents.
#
#Default:
# dead_peer_timeout 10 seconds

#  TAG: hierarchy_stoplist
#       A list of words which, if found in a URL, cause the object to
#       be handled directly by this cache.  In other words, use this
#       to not query neighbor caches for certain objects.  You may
#       list this option multiple times.
#We recommend you to use at least the following line.
hierarchy_stoplist cgi-bin ?

#  TAG: no_cache
#       A list of ACL elements which, if matched, cause the request to
#       not be satisfied from the cache and the reply to not be cached.
#       In other words, use this to force certain objects to never be cached.
#
#       You must use the word 'DENY' to indicate the ACL names which should
#       NOT be cached.
#
#We recommend you to use the following two lines.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
```

```
# OPTIONS WHICH AFFECT THE CACHE SIZE
# -----------------------------------------------------------------------------

#  TAG: cache_mem     (bytes)
#       NOTE: THIS PARAMETER DOES NOT SPECIFY THE MAXIMUM PROCESS SIZE.
#       IT ONLY PLACES A LIMIT ON HOW MUCH ADDITIONAL MEMORY SQUID WILL
#       USE AS A MEMORY CACHE OF OBJECTS. SQUID USES MEMORY FOR OTHER
#       THINGS AS WELL. SEE THE SQUID FAQ SECTION 8 FOR DETAILS.
#
#       'cache_mem' specifies the ideal amount of memory to be used
#       for:
#              * In-Transit objects
#              * Hot Objects
#              * Negative-Cached objects
#
#       Data for these objects are stored in 4 KB blocks.  This
#       parameter specifies the ideal upper limit on the total size of
#       4 KB blocks allocated.  In-Transit objects take the highest
#       priority.
#
#       In-transit objects have priority over the others.  When
#       additional space is needed for incoming data, negative-cached
#       and hot objects will be released.  In other words, the
#       negative-cached and hot objects will fill up any unused space
#       not needed for in-transit objects.
#
#       If circumstances require, this limit will be exceeded.
#       Specifically, if your incoming request rate requires more than
#       'cache_mem' of memory to hold in-transit objects, Squid will
#       exceed this limit to satisfy the new requests.  When the load
#       decreases, blocks will be freed until the high-water mark is
#       reached.  Thereafter, blocks will be used to store hot
#       objects.
#
#Default:
# cache_mem 8 MB

#  TAG: cache_swap_low(percent, 0-100)
#  TAG: cache_swap_high       (percent, 0-100)
#
#       The low- and high-water marks for cache object replacement.
#       Replacement begins when the swap (disk) usage is above the
#       low-water mark and attempts to maintain utilization near the
#       low-water mark.  As swap utilization gets close to high-water
#       mark object eviction becomes more aggressive.  If utilization is
#       close to the low-water mark less replacement is done each time.
#
#       Defaults are 90% and 95%. If you have a large cache, 5% could be
#       hundreds of MB. If this is the case you may wish to set these
#       numbers closer together.
#
#Default:
# cache_swap_low 90
# cache_swap_high 95

#  TAG: maximum_object_size   (bytes)
#       Objects larger than this size will NOT be saved on disk.  The
#       value is specified in kilobytes, and the default is 4MB.  If
#       you wish to get a high BYTES hit ratio, you should probably
#       increase this (one 32 MB object hit counts for 3200 10KB
#       hits).  If you wish to increase speed more than your want to
#       save bandwidth you should leave this low.
#
#       NOTE: if using the LFUDA replacement policy you should increase
#       this value to maximize the byte hit rate improvement of LFUDA!
#       See replacement_policy below for a discussion of this policy.
#
#Default:
# maximum_object_size 4096 KB

#  TAG: minimum_object_size   (bytes)
```

```
#       Objects smaller than this size will NOT be saved on disk.  The
#       value is specified in kilobytes, and the default is 0 KB, which
#       means there is no minimum.
#
#Default:
# minimum_object_size 0 KB

#  TAG: maximum_object_size_in_memory       (bytes)
#        Objects greater than this size will not be attempted to kept in
#        the memory cache. This should be set high enough to keep objects
#        accessed frequently in memory to improve performance whilst low
#        enough to keep larger objects from hoarding cache_mem .
#
#Default:
# maximum_object_size_in_memory 8 KB

#  TAG: ipcache_size  (number of entries)
#  TAG: ipcache_low   (percent)
#  TAG: ipcache_high  (percent)
#       The size, low-, and high-water marks for the IP cache.
#
#Default:
# ipcache_size 1024
# ipcache_low 90
# ipcache_high 95

#  TAG: fqdncache_size(number of entries)
#       Maximum number of FQDN cache entries.
#
#Default:
# fqdncache_size 1024

#  TAG: cache_replacement_policy
#       The cache replacement policy parameter determines which
#       objects are evicted (replaced) when disk space is needed.
#
#           lru       : Squid's original list based LRU policy
#           heap GDSF : Greedy-Dual Size Frequency
#           heap LFUDA: Least Frequently Used with Dynamic Aging
#           heap LRU  : LRU policy implemented using a heap
#
#       Applies to any cache_dir lines listed below this.
#
#       The LRU policies keeps recently referenced objects.
#
#       The heap GDSF policy optimizes object hit rate by keeping smaller
#       popular objects in cache so it has a better chance of getting a
#       hit.  It achieves a lower byte hit rate than LFUDA though since
#       it evicts larger (possibly popular) objects.
#
#       The heap LFUDA policy keeps popular objects in cache regardless of
#       their size and thus optimizes byte hit rate at the expense of
#       hit rate since one large, popular object will prevent many
#       smaller, slightly less popular objects from being cached.
#
#       Both policies utilize a dynamic aging mechanism that prevents
#       cache pollution that can otherwise occur with frequency-based
#       replacement policies.
#
#       NOTE: if using the LFUDA replacement policy you should increase
#       the value of maximum_object_size above its default of 4096 KB to
#       to maximize the potential byte hit rate improvement of LFUDA.
#
#       For more information about the GDSF and LFUDA cache replacement
#       policies see http://www.hpl.hp.com/techreports/1999/HPL-1999-69.html
#       and http://fog.hpl.external.hp.com/techreports/98/HPL-98-173.html.
#
#Default:
# cache_replacement_policy lru

#  TAG: memory_replacement_policy
```

```
#       The memory replacement policy parameter determines which
#       objects are purged from memory when memory space is needed.
#
#       See cache_replacement_policy for details.
#
#Default:
# memory_replacement_policy lru


# LOGFILE PATHNAMES AND CACHE DIRECTORIES
# -----------------------------------------------------------------------------

#  TAG: cache_dir
#       Usage:
#
#       cache_dir Type Directory-Name Fs-specific-data [options]
#
#       cache_dir diskd Maxobjsize Directory-Name MB L1 L2 Q1 Q2
#
#       You can specify multiple cache_dir lines to spread the
#       cache among different disk partitions.
#
#       Type specifies the kind of storage system to use. Only "ufs"
#       is built by default. To eanble any of the other storage systems
#       see the --enable-storeio configure option.
#
#       'Directory' is a top-level directory where cache swap
#       files will be stored.  If you want to use an entire disk
#       for caching, then this can be the mount-point directory.
#       The directory must exist and be writable by the Squid
#       process.  Squid will NOT create this directory for you.
#
#       The ufs store type:
#
#       "ufs" is the old well-known Squid storage format that has always
#       been there.
#
#       cache_dir ufs Directory-Name Mbytes L1 L2 [options]
#
#       'Mbytes' is the amount of disk space (MB) to use under this
#       directory.  The default is 100 MB.  Change this to suit your
#       configuration.  Do NOT put the size of your disk drive here.
#       Instead, if you want Squid to use the entire disk drive,
#       subtract 20% and use that value.
#
#       'Level-1' is the number of first-level subdirectories which
#       will be created under the 'Directory'.  The default is 16.
#
#       'Level-2' is the number of second-level subdirectories which
#       will be created under each first-level directory.  The default
#       is 256.
#
#       The aufs store type:
#
#       "aufs" uses the same storage format as "ufs", utilizing
#       POSIX-threads to avoid blocking the main Squid process on
#       disk-I/O. This was formerly known in Squid as async-io.
#
#       cache_dir aufs Directory-Name Mbytes L1 L2 [options]
#
#       see argument descriptions under ufs above
#
#       The diskd store type:
#
#       "diskd" uses the same storage format as "ufs", utilizing a
#       separate process to avoid blocking the main Squid process on
#       disk-I/O.
#
#       cache_dir diskd Directory-Name Mbytes L1 L2 [options] [Q1=n] [Q2=n]
#
#       see argument descriptions under ufs above
```

```
#
#       Q1 specifies the number of unacknowledged I/O requests when Squid
#       stops opening new files. If this many messages are in the queues,
#       Squid won't open new files. Default is 64
#
#       Q2 specifies the number of unacknowledged messages when Squid
#       starts blocking.  If this many messages are in the queues,
#       Squid blocks until it recevies some replies. Default is 72
#
#       Common options:
#
#       read-only, this cache_dir is read only.
#
#       max-size=n, refers to the max object size this storedir supports.
#       It is used to initially choose the storedir to dump the object.
#       Note: To make optimal use of the max-size limits you should order
#       the cache_dir lines with the smallest max-size value first and the
#       ones with no max-size specification last.
#
#Default:
 cache_dir ufs /var/spool/squid 100 16 256

#  TAG: cache_access_log
#       Logs the client request activity.  Contains an entry for
#       every HTTP and ICP queries received. To disable, enter "none".
#
#Default:
# cache_access_log /var/log/squid/access.log

#  TAG: cache_log
#       Cache logging file. This is where general information about
#       your cache's behavior goes. You can increase the amount of data
#       logged to this file with the "debug_options" tag below.
#
#Default:
# cache_log /var/log/squid/cache.log

#  TAG: cache_store_log
#       Logs the activities of the storage manager.  Shows which
#       objects are ejected from the cache, and which objects are
#       saved and for how long.  To disable, enter "none". There are
#       not really utilities to analyze this data, so you can safely
#       disable it.
#
#Default:
# cache_store_log /var/log/squid/store.log

#  TAG: cache_swap_log
#       Location for the cache "swap.log."  This log file holds the
#       metadata of objects saved on disk.  It is used to rebuild the
#       cache during startup.  Normally this file resides in each
#       'cache_dir' directory, but you may specify an alternate
#       pathname here.  Note you must give a full filename, not just
#       a directory. Since this is the index for the whole object
#       list you CANNOT periodically rotate it!
#
#       If %s can be used in the file name then it will be replaced with a
#       a representation of the cache_dir name where each / is replaced
#       with '.'. This is needed to allow adding/removing cache_dir
#       lines when cache_swap_log is being used.
#
#       If have more than one 'cache_dir', and %s is not used in the name
#       then these swap logs will have names such as:
#
#               cache_swap_log.00
#               cache_swap_log.01
#               cache_swap_log.02
#
#       The numbered extension (which is added automatically)
#       corresponds to the order of the 'cache_dir' lines in this
#       configuration file.  If you change the order of the 'cache_dir'
```

```
#       lines in this file, then these log files will NOT correspond to
#       the correct 'cache_dir' entry (unless you manually rename
#       them).  We recommend that you do NOT use this option.  It is
#       better to keep these log files in each 'cache_dir' directory.
#
#Default:
# none

#  TAG: emulate_httpd_log     on|off
#       The Cache can emulate the log file format which many 'httpd'
#       programs use.  To disable/enable this emulation, set
#       emulate_httpd_log to 'off' or 'on'.  The default
#       is to use the native log format since it includes useful
#       information that Squid-specific log analyzers use.
#
#Default:
# emulate_httpd_log off

#  TAG: log_ip_on_direct      on|off
#       Log the destination IP address in the hierarchy log tag when going
#       direct. Earlier Squid versions logged the hostname here. If you
#       prefer the old way set this to off.
#
#Default:
# log_ip_on_direct on

#  TAG: mime_table
#       Pathname to Squid's MIME table. You shouldn't need to change
#       this, but the default file contains examples and formatting
#       information if you do.
#
#Default:
# mime_table /etc/squid/mime.conf

#  TAG: log_mime_hdrs on|off
#       The Cache can record both the request and the response MIME
#       headers for each HTTP transaction.  The headers are encoded
#       safely and will appear as two bracketed fields at the end of
#       the access log (for either the native or httpd-emulated log
#       formats).  To enable this logging set log_mime_hdrs to 'on'.
#
#Default:
# log_mime_hdrs off

#  TAG: useragent_log
#       Squid will write the User-Agent field from HTTP requests
#       to the filename specified here.  By default useragent_log
#       is disabled.
#
#Default:
# none

#  TAG: referer_log
#       Squid will write the Referer field from HTTP requests to the
#       filename specified here.  By default referer_log is disabled.
#
#Default:
# none

#  TAG: pid_filename
#       A filename to write the process-id to.  To disable, enter "none".
#
#Default:
# pid_filename /var/run/squid.pid

#  TAG: debug_options
#       Logging options are set as section,level where each source file
#       is assigned a unique section.  Lower levels result in less
#       output,  Full debugging (level 9) can result in a very large
#       log file, so be careful.  The magic word "ALL" sets debugging
#       levels for all sections.  We recommend normally running with
```

```
#       "ALL,1".
#
#Default:
# debug_options ALL,1

#  TAG: log_fqdn      on|off
#       Turn this on if you wish to log fully qualified domain names
#       in the access.log. To do this Squid does a DNS lookup of all
#       IP's connecting to it. This can (in some situations) increase
#       latency, which makes your cache seem slower for interactive
#       browsing.
#
#Default:
# log_fqdn off

#  TAG: client_netmask
#       A netmask for client addresses in logfiles and cachemgr output.
#       Change this to protect the privacy of your cache clients.
#       A netmask of 255.255.255.0 will log all IP's in that range with
#       the last digit set to '0'.
#
#Default:
# client_netmask 255.255.255.255


# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS
# ------------------------------------------------------------------------------

#  TAG: ftp_user
#       If you want the anonymous login password to be more informative
#       (and enable the use of picky ftp servers), set this to something
#       reasonable for your domain, like wwwuser@somewhere.net
#
#       The reason why this is domainless by default is that the
#       request can be made on the behalf of a user in any domain,
#       depending on how the cache is used.
#       Some ftp server also validate that the email address is valid
#       (for example perl.com).
#
#Default:
# ftp_user Squid@

#  TAG: ftp_list_width
#       Sets the width of ftp listings. This should be set to fit in
#       the width of a standard browser. Setting this too small
#       can cut off long filenames when browsing ftp sites.
#
#Default:
# ftp_list_width 32

#  TAG: ftp_passive
#       If your firewall does not allow Squid to use passive
#       connections, then turn off this option.
#
#Default:
# ftp_passive on

#  TAG: ftp_sanitycheck
#       For security and data integrity reasons Squid by default performs
#       sanity checks of the addresses of FTP data connections ensure the
#       data connection is to the requested server. If you need to allow
#       FTP connections to servers using another IP address for the data
#       connection then turn this off.
#
#Default:
# ftp_sanitycheck on

#  TAG: cache_dns_program
# Note: This option is only available if Squid is rebuilt with the
#       --disable-internal-dns option
#
```

```
#       Specify the location of the executable for dnslookup process.
#
#Default:
# cache_dns_program /usr/lib/squid/dnsserver

#  TAG: dns_children
# Note: This option is only available if Squid is rebuilt with the
#       --disable-internal-dns option
#
#       The number of processes spawn to service DNS name lookups.
#       For heavily loaded caches on large servers, you should
#       probably increase this value to at least 10.  The maximum
#       is 32.  The default is 5.
#
#       You must have at least one dnsserver process.
#
#Default:
# dns_children 5

#  TAG: dns_retransmit_interval
#       Initial retransmit interval for DNS queries. The interval is
#       doubled each time all configured DNS servers have been tried.
#
#
#Default:
# dns_retransmit_interval 5 seconds

#  TAG: dns_timeout
#       DNS Query timeout. If no response is received to a DNS query
#       within this time then all DNS servers for the queried domain
#       is assumed to be unavailable.
#
#Default:
# dns_timeout 5 minutes

#  TAG: dns_defnames  on|off
# Note: This option is only available if Squid is rebuilt with the
#       --disable-internal-dns option
#
#       Normally the 'dnsserver' disables the RES_DEFNAMES resolver
#       option (see res_init(3)).  This prevents caches in a hierarchy
#       from interpreting single-component hostnames locally.  To allow
#       dnsserver to handle single-component names, enable this
#       option.
#
#Default:
# dns_defnames off

#  TAG: dns_nameservers
#       Use this if you want to specify a list of DNS name servers
#       (IP addresses) to use instead of those given in your
#       /etc/resolv.conf file.
#       On Windows platforms, if no value is specified here or in
#       the /etc/resolv.conf file, the list of DNS name servers are
#       taken from the Windows registry, both static and dynamic DHCP
#       configurations are supported.
#
#       Example: dns_nameservers 10.0.0.1 192.172.0.4
#
#Default:
# none

#  TAG: hosts_file
#       Location of the host-local IP name-address associations
#       database.  Most Operating Systems have such a file: under
#       Un*X it's by default in /etc/hosts MS-Windows NT/2000 places
#       that in %SystemRoot%(by default
#       c:\winnt)\system32\drivers\etc\hosts, while Windows 9x/ME
#       places that in %windir%(usually c:\windows)\hosts
#
#       The file contains newline-separated definitions, in the
```

```
#       form ip_address_in_dotted_form name [name ...] names are
#       whitespace-separated.  lines beginnng with an hash (#)
#       character are comments.
#
#       The file is checked at startup and upon configuration.  If
#       set to 'none', it won't be checked.  If append_domain is
#       used, that domain will be added to domain-local (i.e. not
#       containing any dot character) host definitions.
#
#Default:
# hosts_file /etc/hosts

#  TAG: diskd_program
#       Specify the location of the diskd executable.
#       Note that this is only useful if you have compiled in
#       diskd as one of the store io modules.
#
#Default:
# diskd_program /usr/lib/squid/diskd

#  TAG: unlinkd_program
#       Specify the location of the executable for file deletion process.
#
#Default:
# unlinkd_program /usr/lib/squid/unlinkd

#  TAG: pinger_program
# Note: This option is only available if Squid is rebuilt with the
#       --enable-icmp option
#
#       Specify the location of the executable for the pinger process.
#
#Default:
# pinger_program /usr/lib/squid/pinger

#  TAG: redirect_program
#       Specify the location of the executable for the URL redirector.
#       Since they can perform almost any function there isn't one included.
#       See the FAQ (section 15) for information on how to write one.
#       By default, a redirector is not used.
#
#Default:
# none

#  TAG: redirect_children
#       The number of redirector processes to spawn. If you start
#       too few Squid will have to wait for them to process a backlog of
#       URLs, slowing it down. If you start too many they will use RAM
#       and other system resources.
#
#Default:
# redirect_children 5

#  TAG: redirect_rewrites_host_header
#       By default Squid rewrites any Host: header in redirected
#       requests.  If you are running an accelerator then this may
#       not be a wanted effect of a redirector.
#
#Default:
# redirect_rewrites_host_header on

#  TAG: redirector_access
#       If defined, this access list specifies which requests are
#       sent to the redirector processes.  By default all requests
#       are sent.
#
#Default:
# none

#  TAG: auth_param
#       This is used to pass parameters to the various authentication
```

```
#       schemes.
#       format: auth_param scheme parameter [setting]
#
#       auth_param basic program /usr/bin/ncsa_auth /usr/etc/passwd
#       would tell the basic authentication scheme it's program parameter.
#
#       The order that authentication prompts are presented to the client_agent
#       is dependant on the order the scheme first appears in config file.
#       IE has a bug (it's not rfc 2617 compliant) in that it will use the basic
#       scheme if basic is the first entry presented, even if more secure schemes
#       are presented. For now use the order in the file below. If other browsers
#       have difficulties (don't recognise the schemes offered even if you are
using
#       basic) then either put basic first, or disable the other schemes (by
commenting
#       out their program entry).
#
#       Once an authentication scheme is fully configured, it can only be shutdown
#       by shutting squid down and restarting. Changes can be made on the fly and
#       activated with a reconfigure. I.E. You can change to a different helper,
#       but not unconfigure the helper completely.
#
#       === Parameters for the basic scheme follow. ===
#
#       "program" cmdline
#       Specify the command for the external authenticator.  Such a
#       program reads a line containing "username password" and replies
#       "OK" or "ERR" in an endless loop.  If you use an authenticator,
#       make sure you have 1 acl of type proxy_auth.  By default, the
#       basic authentication sheme is not used unless a program is specified.
#
#       If you want to use the traditional proxy authentication,
#       jump over to the ../auth_modules/NCSA directory and
#       type:
#               % make
#               % make install
#
#       Then, set this line to something like
#
#       auth_param basic program /usr/bin/ncsa_auth /usr/etc/passwd
#
#       "children" numberofchildren
#       The number of authenticator processes to spawn (no default).
#       If you start too few Squid will have to wait for them to
#       process a backlog of usercode/password verifications, slowing
#       it down. When password verifications are done via a (slow)
#       network you are likely to need lots of authenticator
#       processes.
#       auth_param basic children 5
#
#       "realm" realmstring
#       Specifies the realm name which is to be reported to the
#       client for the basic proxy authentication scheme (part of
#       the text the user will see when prompted their username and
#       password). There is no default.
#       auth_param basic realm Squid proxy-caching web server
#
#       "credentialsttl" timetolive
#       Specifies how long squid assumes an externally validated
#       username:password pair is valid for - in other words how
#       often the helper program is called for that user. Set this
#       low to force revalidation with short lived passwords.  Note
#       that setting this high does not impact your susceptability
#       to replay attacks unless you are using an one-time password
#       system (such as SecureID).  If you are using such a system,
#       you will be vulnerable to replay attacks unless you also
#       use the max_user_ip ACL in an http_access rule.
#
#       === Parameters for the digest scheme follow ===
#
#       "program" cmdline
```

```
#       Specify the command for the external authenticator.  Such
#       a program reads a line containing "username":"realm" and
#       replies with the appropriate H(A1) value base64 encoded.
#       See rfc 2616 for the definition of H(A1).  If you use an
#       authenticator, make sure you have 1 acl of type proxy_auth.
#       By default, authentication is not used.
#
#       If you want to use build an authenticator,
#       jump over to the ../digest_auth_modules directory and choose the
#       authenticator to use. It it's directory type
#              % make
#               % make install
#
#       Then, set this line to something like
#
#       auth_param digest program /usr/bin/digest_auth_pw /usr/etc/digpass
#
#
#       "children" numberofchildren
#       The number of authenticator processes to spawn (no default).
#       If you start too few Squid will have to wait for them to
#       process a backlog of H(A1) calculations, slowing it down.
#       When the H(A1) calculations are done via a (slow) network
#       you are likely to need lots of authenticator processes.
#       auth_param digest children 5
#
#       "realm" realmstring
#       Specifies the realm name which is to be reported to the
#       client for the digest proxy authentication scheme (part of
#       the text the user will see when prompted their username and
#       password). There is no default.
#       auth_param digest realm Squid proxy-caching web server
#
#       "nonce_garbage_interval" timeinterval
#       Specifies the interval that nonces that have been issued
#       to client_agent's are checked for validity.
#
#       "nonce_max_duration" timeinterval
#       Specifies the maximum length of time a given nonce will be
#       valid for.
#
#       "nonce_max_count" number
#       Specifies the maximum number of times a given nonce can be
#       used.
#
#       "nonce_strictness" on|off
#       Determines if squid requires strict increment-by-1 behaviour
#       for nonce counts, or just incrementing (off - for use when
#       useragents generate nonce counts that occasionally miss 1
#       (ie, 1,2,4,6)). Default off.
#
#       "check_nonce_count" on|off
#       This directive if set to off can disable the nonce count check
#       completely to work around buggy digest qop implementations in
#       certain mainstream browser versions. Default on to check the
#       nonce count to protect from authentication replay attacks.
#
#       "post_workaround" on|off
#       This is a workaround to certain buggy browsers who sends
#       an incorrect request digest in POST requests when reusing
#       the same nonce as aquired earlier on a GET request.
#
#       === NTLM scheme options follow ===
#
#       "program" cmdline
#       Specify the command for the external ntlm authenticator.
#       Such a program reads a line containing the uuencoded NEGOTIATE
#       and replies with the ntlm CHALLENGE, then waits for the
#       response and answers with "OK" or "ERR" in an endless loop.
#       If you use an ntlm authenticator, make sure you have 1 acl
#       of type proxy_auth.  By default, the ntlm authenticator_program
```

```
#       is not used.
#
#       auth_param ntlm program /usr/bin/ntlm_auth
#
#       "children" numberofchildren
#       The number of authenticator processes to spawn (no default).
#       If you start too few Squid will have to wait for them to
#       process a backlog of credential verifications, slowing it
#       down. When crendential verifications are done via a (slow)
#       network you are likely to need lots of authenticator
#       processes.
#       auth_param ntlm children 5
#
#       "max_challenge_reuses" number
#       The maximum number of times a challenge given by a ntlm
#       authentication helper can be reused. Increasing this number
#       increases your exposure to replay attacks on your network.
#       0 means use the challenge only once.  (disable challenge
#       caching) See max_ntlm_challenge_lifetime for more information.
#       auth_param ntlm max_challenge_reuses 0
#
#       "max_challenge_lifetime" timespan
#       The maximum time period that a ntlm challenge is reused
#       over.  The actual period will be the minimum of this time
#       AND the number of reused challenges.
#       auth_param ntlm max_challenge_lifetime 2 minutes
#
#Recommended minimum configuration:
#auth_param digest program <uncomment and complete this line>
#auth_param digest children 5
#auth_param digest realm Squid proxy-caching web server
#auth_param digest nonce_garbage_interval 5 minutes
#auth_param digest nonce_max_duration 30 minutes
#auth_param digest nonce_max_count 50
#auth_param ntlm program <uncomment and complete this line to activate>
#auth_param ntlm children 5
#auth_param ntlm max_challenge_reuses 0
#auth_param ntlm max_challenge_lifetime 2 minutes
#auth_param basic program <uncomment and complete this line>
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours

#  TAG: authenticate_cache_garbage_interval
#       The time period between garbage collection across the
#       username cache.  This is a tradeoff between memory utilisation
#       (long intervals - say 2 days) and CPU (short intervals -
#       say 1 minute). Only change if you have good reason to.
#
#Default:
# authenticate_cache_garbage_interval 1 hour

#  TAG: authenticate_ttl
#       The time a user & their credentials stay in the logged in
#       user cache since their last request. When the garbage
#       interval passes, all user credentials that have passed their
#       TTL are removed from memory.
#
#Default:
# authenticate_ttl 1 hour

#  TAG: authenticate_ip_ttl
#       If you use proxy authentication and the 'max_user_ip' ACL,
#       this directive controls how long Squid remembers the IP
#       addresses associated with each user.  Use a small value
#       (e.g., 60 seconds) if your users might change addresses
#       quickly, as is the case with dialups.   You might be safe
#       using a larger value (e.g., 2 hours) in a corporate LAN
#       environment with relatively static address assignments.
#
#Default:
```

```
# authenticate_ip_ttl 0 seconds

#  TAG: external_acl_type
#       This option defines external acl classes using a helper program
#       to look up the status
#
#         external_acl_type name [options] FORMAT.. /path/to/helper [helper
arguments..]
#
#       Options:
#
#         ttl=n         TTL in seconds for cached results (defaults to 3600
#                       for 1 hour)
#         negative_ttl=n
#                       TTL for cached negative lookups (default same
#                       as ttl)
#         concurrency=n         Concurrency level / number of processes spawn
#                       to service external acl lookups of this type.
#         cache=n       result cache size, 0 is unbounded (default)
#
#       FORMAT specifications
#
#         %LOGIN        Authenticated user login name
#         %IDENT        Ident user name
#         %SRC          Client IP
#         %DST          Requested host
#         %PROTO        Requested protocol
#         %PORT         Requested port
#         %METHOD       Request method
#         %{Header}     HTTP request header
#         %{Hdr:member}         HTTP request header list member
#         %{Hdr:;member}
#                       HTTP request header list member using ; as
#                       list separator. ; can be any non-alphanumeric
#                       character.
#
#       In addition, any string specified in the referencing acl will
#       also be included in the helper request line, after the specified
#       formats (see the "acl external" directive)
#
#       The helper receives lines per the above format specification,
#       and returns lines starting with OK or ERR indicating the validity
#       of the request and optionally followed by additional keywords with
#       more details.
#
#       General result syntax:
#
#         OK/ERR keyword=value ...
#
#       Defined keywords:
#
#         user=         The users name (login)
#         error=        Error description (only defined for ERR results)
#
#       Keyword values need to be enclosed in quotes if they may contain
#       whitespace, or the whitespace escaped using \. Any quotes or \
#       characters within the keyword value must be \ escaped.
#
#Default:
# none


# OPTIONS FOR TUNING THE CACHE
# ------------------------------------------------------------------------

#  TAG: wais_relay_host
#  TAG: wais_relay_port
#       Relay WAIS request to host (1st arg) at port (2 arg).
#
#Default:
# wais_relay_port 0
```

```
#  TAG: request_header_max_size      (KB)
#       This specifies the maximum size for HTTP headers in a request.
#       Request headers are usually relatively small (about 512 bytes).
#       Placing a limit on the request header size will catch certain
#       bugs (for example with persistent connections) and possibly
#       buffer-overflow or denial-of-service attacks.
#
#Default:
# request_header_max_size 10 KB

#  TAG: request_body_max_size (KB)
#       This specifies the maximum size for an HTTP request body.
#       In other words, the maximum size of a PUT/POST request.
#       A user who attempts to send a request with a body larger
#       than this limit receives an "Invalid Request" error message.
#       If you set this parameter to a zero (the default), there will
#       be no limit imposed.
#
#Default:
# request_body_max_size 0 KB

#  TAG: refresh_pattern
#       usage: refresh_pattern [-i] regex min percent max [options]
#
#       By default, regular expressions are CASE-SENSITIVE.  To make
#       them case-insensitive, use the -i option.
#
#       'Min' is the time (in minutes) an object without an explicit
#       expiry time should be considered fresh. The recommended
#       value is 0, any higher values may cause dynamic applications
#       to be erroneously cached unless the application designer
#       has taken the appropriate actions.
#
#       'Percent' is a percentage of the objects age (time since last
#       modification age) an object without explicit expiry time
#       will be considered fresh.
#
#       'Max' is an upper limit on how long objects without an explicit
#       expiry time will be considered fresh.
#
#       options: override-expire
#                override-lastmod
#                reload-into-ims
#                ignore-reload
#
#               override-expire enforces min age even if the server
#               sent a Expires: header. Doing this VIOLATES the HTTP
#               standard.  Enabling this feature could make you liable
#               for problems which it causes.
#
#               override-lastmod enforces min age even on objects
#               that was modified recently.
#
#               reload-into-ims changes client no-cache or ``reload''
#               to If-Modified-Since requests. Doing this VIOLATES the
#               HTTP standard. Enabling this feature could make you
#               liable for problems which it causes.
#
#               ignore-reload ignores a client no-cache or ``reload''
#               header. Doing this VIOLATES the HTTP standard. Enabling
#               this feature could make you liable for problems which
#               it causes.
#
#       Basically a cached object is:
#
#               FRESH if expires < now, else STALE
#               STALE if age > max
#               FRESH if lm-factor < percent, else STALE
#               FRESH if age < min
#               else STALE
```

```
#
#       The refresh_pattern lines are checked in the order listed here.
#       The first entry which matches is used.  If none of the entries
#       match, then the default will be used.
#
#       Note, you must uncomment all the default lines if you want
#       to change one. The default setting is only active if none is
#       used.
#
#Suggested default:
refresh_pattern ^ftp:         1440    20%     10080
refresh_pattern ^gopher:      1440    0%      1440
refresh_pattern .             0       20%     4320

#  TAG: quick_abort_min       (KB)
#  TAG: quick_abort_max       (KB)
#  TAG: quick_abort_pct       (percent)
#       The cache by default continues downloading aborted requests
#       which are almost completed (less than 16 KB remaining). This
#       may be undesirable on slow (e.g. SLIP) links and/or very busy
#       caches.  Impatient users may tie up file descriptors and
#       bandwidth by repeatedly requesting and immediately aborting
#       downloads.
#
#       When the user aborts a request, Squid will check the
#       quick_abort values to the amount of data transfered until
#       then.
#
#       If the transfer has less than 'quick_abort_min' KB remaining,
#       it will finish the retrieval.
#
#       If the transfer has more than 'quick_abort_max' KB remaining,
#       it will abort the retrieval.
#
#       If more than 'quick_abort_pct' of the transfer has completed,
#       it will finish the retrieval.
#
#       If you do not want any retrieval to continue after the client
#       has aborted, set both 'quick_abort_min' and 'quick_abort_max'
#       to '0 KB'.
#
#       If you want retrievals to always continue if they are being
#       cached then set 'quick_abort_min' to '-1 KB'.
#
#Default:
# quick_abort_min 16 KB
# quick_abort_max 16 KB
# quick_abort_pct 95

#  TAG: negative_ttl  time-units
#       Time-to-Live (TTL) for failed requests.  Certain types of
#       failures (such as "connection refused" and "404 Not Found") are
#       negatively-cached for a configurable amount of time.  The
#       default is 5 minutes.  Note that this is different from
#       negative caching of DNS lookups.
#
#Default:
# negative_ttl 5 minutes

#  TAG: positive_dns_ttl      time-units
#       Time-to-Live (TTL) for positive caching of successful DNS lookups.
#       Default is 6 hours (360 minutes).  If you want to minimize the
#       use of Squid's ipcache, set this to 1, not 0.
#
#Default:
# positive_dns_ttl 6 hours

#  TAG: negative_dns_ttl      time-units
#       Time-to-Live (TTL) for negative caching of failed DNS lookups.
#
#Default:
```

```
# negative_dns_ttl 5 minutes

#  TAG: range_offset_limit    (bytes)
#       Sets a upper limit on how far into the the file a Range request
#       may be to cause Squid to prefetch the whole file. If beyond this
#       limit then Squid forwards the Range request as it is and the result
#       is NOT cached.
#
#       This is to stop a far ahead range request (lets say start at 17MB)
#       from making Squid fetch the whole object up to that point before
#       sending anything to the client.
#
#       A value of -1 causes Squid to always fetch the object from the
#       beginning so that it may cache the result. (2.0 style)
#
#       A value of 0 causes Squid to never fetch more than the
#       client requested. (default)
#
#Default:
# range_offset_limit 0 KB


# TIMEOUTS
# -----------------------------------------------------------------------------

#  TAG: connect_timeout       time-units
#       Some systems (notably Linux) can not be relied upon to properly
#       time out connect(2) requests.  Therefore the Squid process
#       enforces its own timeout on server connections.  This parameter
#       specifies how long to wait for the connect to complete.  The
#       default is two minutes (120 seconds).
#
#Default:
# connect_timeout 2 minutes

#  TAG: peer_connect_timeout  time-units
#       This parameter specifies how long to wait for a pending TCP
#       connection to a peer cache.  The default is 30 seconds.   You
#       may also set different timeout values for individual neighbors
#       with the 'connect-timeout' option on a 'cache_peer' line.
#
#Default:
# peer_connect_timeout 30 seconds

#  TAG: read_timeout  time-units
#       The read_timeout is applied on server-side connections.  After
#       each successful read(), the timeout will be extended by this
#       amount.  If no data is read again after this amount of time,
#       the request is aborted and logged with ERR_READ_TIMEOUT.  The
#       default is 15 minutes.
#
#Default:
# read_timeout 15 minutes

#  TAG: request_timeout
#       How long to wait for an HTTP request after initial
#       connection establishment.
#
#Default:
# request_timeout 5 minutes

#  TAG: persistent_request_timeout
#       How long to wait for the next HTTP request on a persistent
#       connection after the previous request completes.
#
#Default:
# persistent_request_timeout 1 minute

#  TAG: client_lifetime       time-units
#       The maximum amount of time that a client (browser) is allowed to
#       remain connected to the cache process.  This protects the Cache
```

```
#       from having a lot of sockets (and hence file descriptors) tied up
#       in a CLOSE_WAIT state from remote clients that go away without
#       properly shutting down (either because of a network failure or
#       because of a poor client implementation).  The default is one
#       day, 1440 minutes.
#
#       NOTE:  The default value is intended to be much larger than any
#       client would ever need to be connected to your cache.  You
#       should probably change client_lifetime only as a last resort.
#       If you seem to have many client connections tying up
#       filedescriptors, we recommend first tuning the read_timeout,
#       request_timeout, persistent_request_timeout and quick_abort values.
#
#Default:
# client_lifetime 1 day

#  TAG: half_closed_clients
#       Some clients may shutdown the sending side of their TCP
#       connections, while leaving their receiving sides open.     Sometimes,
#       Squid can not tell the difference between a half-closed and a
#       fully-closed TCP connection.  By default, half-closed client
#       connections are kept open until a read(2) or write(2) on the
#       socket returns an error.  Change this option to 'off' and Squid
#       will immediately close client connections when read(2) returns
#       "no more data to read."
#
#Default:
# half_closed_clients on

#  TAG: pconn_timeout
#       Timeout for idle persistent connections to servers and other
#       proxies.
#
#Default:
# pconn_timeout 120 seconds

#  TAG: ident_timeout
#       Maximum time to wait for IDENT lookups to complete.
#
#       If this is too high, and you enabled IDENT lookups from untrusted
#       users, then you might be susceptible to denial-of-service by having
#       many ident requests going at once.
#
#Default:
# ident_timeout 10 seconds

#  TAG: shutdown_lifetime     time-units
#       When SIGTERM or SIGHUP is received, the cache is put into
#       "shutdown pending" mode until all active sockets are closed.
#       This value is the lifetime to set for all open descriptors
#       during shutdown mode.  Any active clients after this many
#       seconds will receive a 'timeout' message.
#
#Default:
# shutdown_lifetime 30 seconds


# ACCESS CONTROLS
# -----------------------------------------------------------------------------

#  TAG: acl
#       Defining an Access List
#
#       acl aclname acltype string1 ...
#       acl aclname acltype "file" ...
#
#       when using "file", the file should contain one item per line
#
#       acltype is one of the types described below
#
#       By default, regular expressions are CASE-SENSITIVE.  To make
```

```
#       them case-insensitive, use the -i option.
#
#       acl aclname src      ip-address/netmask ... (clients IP address)
#       acl aclname src      addr1-addr2/netmask ... (range of addresses)
#       acl aclname dst      ip-address/netmask ... (URL host's IP address)
#       acl aclname myip     ip-address/netmask ... (local socket IP address)
#
#       acl aclname srcdomain   .foo.com ...    # reverse lookup, client IP
#       acl aclname dstdomain   .foo.com ...    # Destination server from URL
#       acl aclname srcdom_regex [-i] xxx ...   # regex matching client name
#       acl aclname dstdom_regex [-i] xxx ...   # regex matching server
#         # For dstdomain and dstdom_regex  a reverse lookup is tried if a IP
#         # based URL is used. The name "none" is used if the reverse lookup
#         # fails.
#
#       acl aclname time     [day-abbrevs]  [h1:m1-h2:m2]
#           day-abbrevs:
#              S - Sunday
#              M - Monday
#              T - Tuesday
#              W - Wednesday
#              H - Thursday
#              F - Friday
#              A - Saturday
#           h1:m1 must be less than h2:m2
#       acl aclname url_regex [-i] ^http:// ...     # regex matching on whole URL
#       acl aclname urlpath_regex [-i] \.gif$ ...   # regex matching on URL path
#       acl aclname urllogin [-i] [^a-zA-Z0-9] ...  # regex matching on URL login
field
#       acl aclname port     80 70 21 ...
#       acl aclname port     0-1024 ...             # ranges allowed
#       acl aclname myport   3128 ...        # (local socket TCP port)
#       acl aclname proto    HTTP FTP ...
#       acl aclname method   GET POST ...
#       acl aclname browser  [-i] regexp ...
#         # pattern match on User-Agent header
#        acl aclname referer_regex  [-i] regexp ...
#          # pattern match on Referer header
#          # Referer is highly unreliable, so use with care
#       acl aclname ident    username ...
#       acl aclname ident_regex [-i] pattern ...
#         # string match on ident output.
#         # use REQUIRED to accept any non-null ident.
#       acl aclname src_as   number ...
#       acl aclname dst_as   number ...
#         # Except for access control, AS numbers can be used for
#         # routing of requests to specific caches. Here's an
#         # example for routing all requests for AS#1241 and only
#         # those to mycache.mydomain.net:
#         # acl asexample dst_as 1241
#         # cache_peer_access mycache.mydomain.net allow asexample
#         # cache_peer_access mycache_mydomain.net deny all
#
#       acl aclname proxy_auth username ...
#       acl aclname proxy_auth_regex [-i] pattern ...
#         # list of valid usernames
#         # use REQUIRED to accept any valid username.
#         #
#         # NOTE: when a Proxy-Authentication header is sent but it is not
#         # needed during ACL checking the username is NOT logged
#         # in access.log.
#         #
#         # NOTE: proxy_auth requires a EXTERNAL authentication program
#         # to check username/password combinations (see
#         # auth_param directive).
#         #
#         # WARNING: proxy_auth can't be used in a transparent proxy. It
#         # collides with any authentication done by origin servers. It may
#         # seem like it works at first, but it doesn't.
#
#       acl aclname snmp_community string ...
```

```
#         # A community string to limit access to your SNMP Agent
#         # Example:
#         #
#         #    acl snmppublic snmp_community public
#
#       acl aclname maxconn number
#         # This will be matched when the client's IP address has
#         # more than <number> HTTP connections established.
#
#       acl aclname max_user_ip [-s] number
#         # This will be matched when the user attempts to log in from more
#         # than <number> different ip addresses. The authenticate_ip_ttl
#         # parameter controls the timeout on the ip entries.
#         # If -s is specified then the limit is strict, denying browsing
#         # from any further IP addresses until the ttl has expired. Without
#         # -s Squid will just annoy the user by "randomly" denying requests.
#         # (the counter is then reset each time the limit is reached and a
#         # request is denied)
#         # NOTE: in acceleration mode or where there is mesh of child proxies,
#         # clients may appear to come from multiple addresses if they are
#         # going through proxy farms, so a limit of 1 may cause user problems.
#
#       acl aclname req_mime_type mime-type1 ...
#         # regex match agains the mime type of the request generated
#         # by the client. Can be used to detect file upload or some
#         # types HTTP tunelling requests.
#         # NOTE: This does NOT match the reply. You cannot use this
#         # to match the returned file type.
#
#       acl aclname rep_mime_type mime-type1 ...
#         # regex match against the mime type of the reply recieved by
#         # squid. Can be used to detect file download or some
#         # types HTTP tunelling requests.
#         # NOTE: This has no effect in http_access rules. It only has
#         # effect in rules that affect the reply data stream such as
#         # http_reply_access.
#
#       acl acl_name external class_name [arguments...]
#         # external ACL lookup via a helper class defined by the
#         # external_acl_type directive.
#
#Examples:
#acl myexample dst_as 1241
#acl password proxy_auth REQUIRED
#acl fileupload req_mime_type -i ^multipart/form-data$
#acl javascript rep_mime_type -i ^application/x-javascript$
#
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80        # http
acl Safe_ports port 21        # ftp
acl Safe_ports port 443 563   # https, snews
acl Safe_ports port 70        # gopher
acl Safe_ports port 210               # wais
acl Safe_ports port 1025-65535        # unregistered ports
acl Safe_ports port 280               # http-mgmt
acl Safe_ports port 488               # gss-http
acl Safe_ports port 591               # filemaker
acl Safe_ports port 777               # multiling http
acl CONNECT method CONNECT

#  TAG: http_access
#       Allowing or Denying access based on defined access lists
#
#       Access to the HTTP port:
#       http_access allow|deny [!]aclname ...
#
```

```
#       NOTE on default values:
#
#       If there are no "access" lines present, the default is to deny
#       the request.
#
#       If none of the "access" lines cause a match, the default is the
#       opposite of the last line in the list.  If the last line was
#       deny, then the default is allow.  Conversely, if the last line
#       is allow, the default will be deny.  For these reasons, it is a
#       good idea to have an "deny all" or "allow all" entry at the end
#       of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
#
# We strongly recommend to uncomment the following to protect innocent
# web applications running on the proxy server who think that the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Exampe rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

acl     pbarrera        src     192.168.0.10/32
acl     mcabrera        src     192.168.0.11/32
acl     xpinto          src     192.168.0.12/32
acl     pcaiza          src     192.168.0.13/32
acl     jbustillos      src     192.168.0.14/32
acl     dacosa          src     192.168.0.15/32
acl     xruiz           src     192.168.0.16/32
acl     apaez           src     192.168.0.17/32
acl     rpujos          src     192.168.0.18/32
acl     ejimenez        src     192.168.0.19/32
acl     xvillaroel      src     192.168.0.20/32
acl     vavila          src     192.168.0.21/32
acl     mtoaquiza       src     192.168.0.22/32
acl     mvega           src     192.168.0.23/32
acl     fdominguez      src     192.168.0.24/32
acl     ftinoco         src     192.168.0.25/32
acl     eguano          src     192.168.0.26/32
acl     ebarbosa        src     192.168.0.27/32
acl     xvinueza        src     192.168.0.28/32
acl     lsuntaxi        src     192.168.0.29/32
acl     wchancusig      src     192.168.0.30/32
acl     calbarracin     src     192.168.0.31/32
acl     jzurita         src     192.168.0.32/32
acl     jcaÃ±izares     src     192.168.0.33/32
acl     xbustillos      src     192.168.0.34/32
acl     dponce          src     192.168.0.35/32
acl     pargudo         src     192.168.0.36/32
acl     ysoria          src     192.168.0.37/32
acl     svera           src     192.168.0.38/32
acl     mheredia        src     192.168.0.39/32
acl     bperez          src     192.168.0.40/32
acl     jfontecilla     src     192.168.0.41/32
acl     lrodriguez      src     192.168.0.42/32
```

```
acl     mmoreno         src     192.168.0.43/32
acl     bhidalgo        src     192.168.0.44/32
acl     ealban          src     192.168.0.45/32
acl     fcela           src     192.168.0.46/32
acl     jpeÃ±aherrera   src     192.168.0.47/32
acl     dgarzon         src     192.168.0.48/32
acl     mvanegas        src     192.168.0.49/32
acl     clasificacion   src     192.168.0.50/32
acl     siempelkamp     src     192.168.0.51/32
acl     burkle          src     192.168.0.52/32
acl     mdf             src     192.168.0.53/32
acl     ccattani        src     192.168.0.54/32
acl     fgiron          src     192.168.0.55/32
acl     rvelasquez      src     192.168.0.56/32
acl     echuquilla      src     192.168.0.57/32
acl     prosales        src     192.168.0.58/32
acl     red_interna     src     192.168.0.0/24


acl     gobierno    dstdomain   .gov.ec
acl     bcopichincha    dstdomain .bancopichincha.com
acl     capacitacion    dstdomain .cfnet.com
acl     webinterna      dstdomain .cotopaxi.com.ec
acl     google   dstdomain      .google.com
acl     ecuador   dstdomain     .com.ec

http_access allow dponce  all
http_access allow pbarrera  webinterna
http_access allow jbustillos gobierno capacitacion bcopichincha
http_access deny all ecuador
http_access allow red_interna webinterna

http_access deny all

# And finally deny all other access to this proxy
http_access allow localhost
http_access deny all

#  TAG: http_reply_access
#        Allow replies to client requests. This is complementary to http_access.
#
#        http_reply_access allow|deny [!] aclname ...
#
#        NOTE: if there are no access lines present, the default is to allow
#       all replies
#
#        If none of the access lines cause a match, then the opposite of the
#        last line will apply. Thus it is good practice to end the rules
#        with an "allow all" or "deny all" entry.
#
#Default:
# http_reply_access allow all
#
#Recommended minimum configuration:
#
# Insert your own rules here.
#
#
# and finally allow by default
http_reply_access allow all

#  TAG: icp_access
#       Allowing or Denying access to the ICP port based on defined
#       access lists
#
#       icp_access  allow|deny [!]aclname ...
#
#       See http_access for details
#
#Default:
# icp_access deny all
```

```
#
#Allow ICP queries from everyone
icp_access allow all

#  TAG: miss_access
#       Use to force your neighbors to use you as a sibling instead of
#       a parent.  For example:
#
#              acl localclients src 172.16.0.0/16
#              miss_access allow localclients
#              miss_access deny  !localclients
#
#       This means that only your local clients are allowed to fetch
#       MISSES and all other clients can only fetch HITS.
#
#       By default, allow all clients who passed the http_access rules
#       to fetch MISSES from us.
#
#Default setting:
# miss_access allow all

#  TAG: cache_peer_access
#       Similar to 'cache_peer_domain' but provides more flexibility by
#       using ACL elements.
#
#       cache_peer_access cache-host allow|deny [!]aclname ...
#
#       The syntax is identical to 'http_access' and the other lists of
#       ACL elements.  See the comments for 'http_access' below, or
#       the Squid FAQ (http://www.squid-cache.org/FAQ/FAQ-10.html).
#
#Default:
# none

#  TAG: ident_lookup_access
#       A list of ACL elements which, if matched, cause an ident
#       (RFC 931) lookup to be performed for this request.  For
#       example, you might choose to always perform ident lookups
#       for your main multi-user Unix boxes, but not for your Macs
#       and PCs.  By default, ident lookups are not performed for
#       any requests.
#
#       To enable ident lookups for specific client addresses, you
#       can follow this example:
#
#       acl ident_aware_hosts src 198.168.1.0/255.255.255.0
#       ident_lookup_access allow ident_aware_hosts
#       ident_lookup_access deny all
#
#       Only src type ACL checks are fully supported.  A src_domain
#       ACL might work at times, but it will not always provide
#       the correct result.
#
#Default:
# ident_lookup_access deny all

#  TAG: tcp_outgoing_tos
#       Allows you to select a TOS/Diffserv value to mark outgoing
#       connections with, based on the username or source address
#       making the request.
#
#       tcp_outgoing_tos ds-field [!]aclname ...
#
#       Example where normal_service_net uses the TOS value 0x00
#       and normal_service_net uses 0x20
#
#       acl normal_service_net src 10.0.0.0/255.255.255.0
#       acl good_service_net src 10.0.1.0/255.255.255.0
#       tcp_outgoing_tos 0x00 normal_service_net 0x00
#       tcp_outgoing_tos 0x20 good_service_net
#
```

```
#       TOS/DSCP values really only have local significance - so you should
#       know what you're specifying. For more, see RFC 2474
#
#       The TOS/DSCP byte must be exactly that - a byte, value  0 - 255, or
#       "default" to use whatever default your host has.
#
#       Processing proceeds in the order specified, and stops at first fully
#       matching line.
#
#Default:
# none

#  TAG: tcp_outgoing_address
#       Allows you to map requests to different outgoing IP addresses
#       based on the username or sourceaddress of the user making
#       the request.
#
#       tcp_outgoing_address ipaddr [[!]aclname] ...
#
#       Example where requests from 10.0.0.0/24 will be forwareded
#       with source address 10.1.0.1, 10.0.2.0/24 forwarded with
#       source address 10.1.0.2 and the rest will be forwarded with
#       source address 10.1.0.3.
#
#       acl normal_service_net src 10.0.0.0/255.255.255.0
#       acl good_service_net src 10.0.1.0/255.255.255.0
#       tcp_outgoing_address 10.0.0.1 normal_service_net
#       tcp_outgoing_address 10.0.0.2 good_service_net
#       tcp_outgoing_address 10.0.0.3
#
#       Processing proceeds in the order specified, and stops at first fully
#       matching line.
#
#Default:
# none

#  TAG: reply_body_max_size  bytes allow|deny acl acl...
#        This option specifies the maximum size of a reply body in bytes.
#       It can be used to prevent users from downloading very large files,
#       such as MP3's and movies. When the reply headers are recieved,
#       the reply_body_max_size lines are processed, and the first line with
#       a result of "allow" is used as the maximum body size for this reply.
#       This size is then checked twice. First when we get the reply headers,
#       we check the content-length value.  If the content length value exists
#       and is larger than the allowed size, the request is denied and the
#       user receives an error message that says "the request or reply
#       is too large." If there is no content-length, and the reply
#       size exceeds this limit, the client's connection is just closed
#       and they will receive a partial reply.
#
#       WARNING: downstream caches probably can not detect a partial reply
#       if there is no content-length header, so they will cache
#       partial responses and give them out as hits.  You should NOT
#       use this option if you have downstream caches.
#
#       WARNING: A maximum size smaller than the size of squid's error messages
#       will cause an infinite loop and crash squid. Ensure that the smallest
#       non-zero value you use is greater that the maximum header size plus
#       the size of your largest error page.
#
#       If you set this parameter to zero (the default), there will be
#       no limit imposed.
#
#Default:
# reply_body_max_size 0 allow all


# ADMINISTRATIVE PARAMETERS
# -----------------------------------------------------------------------------

#  TAG: cache_mgr
```

```
#       Email-address of local cache manager who will receive
#       mail if the cache dies.  The default is "root".
#cache_mgr root
#
#Default:
# cache_mgr root

#  TAG: cache_effective_user
#  TAG: cache_effective_group
#
#       If you start Squid as root, it will change its effective/real
#       UID/GID to the UID/GID specified below.  The default is to
#       change to UID to "squid".  If you define cache_effective_user,
#       but not cache_effective_group, Squid sets the GID the
#       effective user's default group ID (taken from the password
#       file).
#
#       If Squid is not started as root, the cache_effective_user
#       value is ignored and the GID value is unchanged by default.
#       However, you can make Squid change its GID to another group
#       that the process owner is a member of.  Note that if Squid
#       is not started as root then you cannot set http_port to a
#       value lower than 1024.
#cache_effective_user squid
#cache_effective_group squid
#
#Default:
# cache_effective_user squid
# cache_effective_group squid

#  TAG: visible_hostname
#       If you want to present a special hostname in error messages, etc,
#       then define this.  Otherwise, the return value of gethostname()
#       will be used. If you have multiple caches in a cluster and
#       get errors about IP-forwarding you must set them to have individual
#       names with this setting.
#
#Default:
# none

#  TAG: unique_hostname
#       If you want to have multiple machines with the same
#       'visible_hostname' then you must give each machine a different
#       'unique_hostname' so that forwarding loops can be detected.
#
#Default:
# none

#  TAG: hostname_aliases
#       A list of other DNS names that your cache has.
#
#Default:
# none


# OPTIONS FOR THE CACHE REGISTRATION SERVICE
# ----------------------------------------------------------------------------
#
#       This section contains parameters for the (optional) cache
#       announcement service.  This service is provided to help
#       cache administrators locate one another in order to join or
#       create cache hierarchies.
#
#       An 'announcement' message is sent (via UDP) to the registration
#       service by Squid.  By default, the announcement message is NOT
#       SENT unless you enable it with 'announce_period' below.
#
#       The announcement message includes your hostname, plus the
#       following information from this configuration file:
#
#               http_port
```

```
#              icp_port
#              cache_mgr
#
#       All current information is processed regularly and made
#       available on the Web at http://www.ircache.net/Cache/Tracker/.

#  TAG: announce_period
#       This is how frequently to send cache announcements.  The
#       default is `0' which disables sending the announcement
#       messages.
#
#       To enable announcing your cache, just uncomment the line
#       below.
#
#Default:
# announce_period 0
#
#To enable announcing your cache, just uncomment the line below.
#announce_period 1 day

#  TAG: announce_host
#  TAG: announce_file
#  TAG: announce_port
#       announce_host and announce_port set the hostname and port
#       number where the registration message will be sent.
#
#       Hostname will default to 'tracker.ircache.net' and port will
#       default default to 3131.  If the 'filename' argument is given,
#       the contents of that file will be included in the announce
#       message.
#
#Default:
# announce_host tracker.ircache.net
# announce_port 3131


# HTTPD-ACCELERATOR OPTIONS
# -----------------------------------------------------------------------------

#  TAG: httpd_accel_host
#  TAG: httpd_accel_port
#       If you want to run Squid as an httpd accelerator, define the
#       host name and port number where the real HTTP server is.
#
#       If you want IP based virtual host support then specify the
#       hostname as "virtual". This will make Squid use the IP address
#       where it accepted the request as hostname in the URL.
#
#       If you want virtual port support then specify the port as "0".
#
#       NOTE: enabling httpd_accel_host disables proxy-caching and
#       ICP.  If you want these features enabled also, then set
#       the 'httpd_accel_with_proxy' option.
#
#Default:
# httpd_accel_port 80

#  TAG: httpd_accel_single_host      on|off
#       If you are running Squid as an accelerator and have a single backend
#       server then set this to on. This causes Squid to forward the request
#       to this server irregardles of what any redirectors or Host headers
#       says.
#
#       Leave this at off if you have multiple backend servers, and use a
#       redirector (or host table or private DNS) to map the requests to the
#       appropriate backend servers. Note that the mapping needs to be a
#       1-1 mapping between requested and backend (from redirector) domain
#       names or caching will fail, as cacing is performed using the
#       URL returned from the redirector.
#
#       See also redirect_rewrites_host_header.
```

```
#
#Default:
# httpd_accel_single_host off

#  TAG: httpd_accel_with_proxy       on|off
#       If you want to use Squid as both a local httpd accelerator
#       and as a proxy, change this to 'on'. Note however that your
#       proxy users may have trouble to reach the accelerated domains
#       unless their browsers are configured not to use this proxy for
#       those domains (for example via the no_proxy browser configuration
#       setting)
#
#Default:
# httpd_accel_with_proxy off

#  TAG: httpd_accel_uses_host_header on|off
#       HTTP/1.1 requests include a Host: header which is basically the
#       hostname from the URL.  The Host: header is used for domain based
#       virutal hosts. If your accelerator needs to provide domain based
#       virtual hosts on the same IP address then you will need to turn this
#       on.
#
#       Note that Squid does NOT check the value of the Host header matches
#       any of your accelerated server, so it may open a big security hole
#       unless you take care to set up access controls proper.  We recommend
#       that this option remain disabled unless you are sure of what you
#       are doing.
#
#       However, you will need to enable this option if you run Squid
#       as a transparent proxy.  Otherwise, virtual servers which
#       require the Host: header will not be properly cached.
#
#Default:
# httpd_accel_uses_host_header off


# MISCELLANEOUS
# -----------------------------------------------------------------------------

#  TAG: dns_testnames
#       The DNS tests exit as soon as the first site is successfully looked up
#
#       This test can be disabled with the -D command line option.
#
#Default:
# dns_testnames netscape.com internic.net nlanr.net microsoft.com

#  TAG: logfile_rotate
#       Specifies the number of logfile rotations to make when you
#       type 'squid -k rotate'.  The default is 10, which will rotate
#       with extensions 0 through 9.  Setting logfile_rotate to 0 will
#       disable the rotation, but the logfiles are still closed and
#       re-opened.  This will enable you to rename the logfiles
#       yourself just before sending the rotate signal.
#
#       Note, the 'squid -k rotate' command normally sends a USR1
#       signal to the running squid process.  In certain situations
#       (e.g. on Linux with Async I/O), USR1 is used for other
#       purposes, so -k rotate uses another signal.  It is best to get
#       in the habit of using 'squid -k rotate' instead of 'kill -USR1
#       <pid>'.
#
#logfile_rotate 0
#
#Default:
# logfile_rotate 0

#  TAG: append_domain
#       Appends local domain name to hostnames without any dots in
#       them.  append_domain must begin with a period.
#
```

```
#       Be warned that there today is Internet names with no dots in
#       them using only top-domain names, so setting this may
#       cause some Internet sites to become unavailable.
#
#Example:
# append_domain .yourdomain.com
#
#Default:
# none

#  TAG: tcp_recv_bufsize      (bytes)
#       Size of receive buffer to set for TCP sockets.  Probably just
#       as easy to change your kernel's default.  Set to zero to use
#       the default buffer size.
#
#Default:
# tcp_recv_bufsize 0 bytes

#  TAG: err_html_text
#       HTML text to include in error messages.  Make this a "mailto"
#       URL to your admin address, or maybe just a link to your
#       organizations Web page.
#
#       To include this in your error messages, you must rewrite
#       the error template files (found in the "errors" directory).
#       Wherever you want the 'err_html_text' line to appear,
#       insert a %L tag in the error template file.
#
#Default:
# none

#  TAG: deny_info
#       Usage:   deny_info err_page_name acl
#       or       deny_info http://... acl
#       Example: deny_info ERR_CUSTOM_ACCESS_DENIED bad_guys
#
#       This can be used to return a ERR_ page for requests which
#       do not pass the 'http_access' rules.  A single ACL will cause
#       the http_access check to fail.  If a 'deny_info' line exists
#       for that ACL then Squid returns a corresponding error page.
#
#       You may use ERR_ pages that come with Squid or create your own pages
#       and put them into the configured errors/ directory.
#
#       Alternatively you can specify an error URL. The browsers will then
#       get redirected (302) to the specified URL. %s in the redirection
#       URL will be replaced by the requested URL.
#
#       Alternatively you can tell Squid to reset the TCP connection
#       by specifying TCP_RESET.
#
#Default:
# none

#  TAG: memory_pools  on|off
#       If set, Squid will keep pools of allocated (but unused) memory
#       available for future use.  If memory is a premium on your
#       system and you believe your malloc library outperforms Squid
#       routines, disable this.
#
#Default:
# memory_pools on

#  TAG: memory_pools_limit    (bytes)
#       Used only with memory_pools on:
#       memory_pools_limit 50 MB
#
#       If set to a non-zero value, Squid will keep at most the specified
#       limit of allocated (but unused) memory in memory pools. All free()
#       requests that exceed this limit will be handled by your malloc
#       library. Squid does not pre-allocate any memory, just safe-keeps
```

```
#       objects that otherwise would be free()d. Thus, it is safe to set
#       memory_pools_limit to a reasonably high value even if your
#       configuration will use less memory.
#
#       If not set (default) or set to zero, Squid will keep all memory it
#       can. That is, there will be no limit on the total amount of memory
#       used for safe-keeping.
#
#       To disable memory allocation optimization, do not set
#       memory_pools_limit to 0. Set memory_pools to "off" instead.
#
#       An overhead for maintaining memory pools is not taken into account
#       when the limit is checked. This overhead is close to four bytes per
#       object kept. However, pools may actually _save_ memory because of
#       reduced memory thrashing in your malloc library.
#
#Default:
# none

#  TAG: forwarded_for on|off
#       If set, Squid will include your system's IP address or name
#       in the HTTP requests it forwards.  By default it looks like
#       this:
#
#               X-Forwarded-For: 192.1.2.3
#
#       If you disable this, it will appear as
#
#               X-Forwarded-For: unknown
#
#Default:
# forwarded_for on

#  TAG: log_icp_queries       on|off
#       If set, ICP queries are logged to access.log. You may wish
#       do disable this if your ICP load is VERY high to speed things
#       up or to simplify log analysis.
#
#Default:
# log_icp_queries on

#  TAG: icp_hit_stale on|off
#       If you want to return ICP_HIT for stale cache objects, set this
#       option to 'on'.  If you have sibling relationships with caches
#       in other administrative domains, this should be 'off'.  If you only
#       have sibling relationships with caches under your control, then
#       it is probably okay to set this to 'on'.
#       If set to 'on', then your siblings should use the option "allow-miss"
#       on their cache_peer lines for connecting to you.
#
#Default:
# icp_hit_stale off

#  TAG: minimum_direct_hops
#       If using the ICMP pinging stuff, do direct fetches for sites
#       which are no more than this many hops away.
#
#Default:
# minimum_direct_hops 4

#  TAG: minimum_direct_rtt
#       If using the ICMP pinging stuff, do direct fetches for sites
#       which are no more than this many rtt milliseconds away.
#
#Default:
# minimum_direct_rtt 400

#  TAG: cachemgr_passwd
#       Specify passwords for cachemgr operations.
#
#       Usage: cachemgr_passwd password action action ...
```

```
#
#       Some valid actions are (see cache manager menu for a full list):
#               5min
#               60min
#               asndb
#               authenticator
#               cbdata
#               client_list
#               comm_incoming
#               config *
#               counters
#               delay
#               digest_stats
#               dns
#               events
#               filedescriptors
#               fqdncache
#               histograms
#               http_headers
#               info
#               io
#               ipcache
#               mem
#               menu
#               netdb
#               non_peers
#               objects
#               offline_toggle *
#               pconn
#               peer_select
#               redirector
#               refresh
#               server_list
#               shutdown *
#               store_digest
#               storedir
#               utilization
#               via_headers
#               vm_objects
#
#       * Indicates actions which will not be performed without a
#         valid password, others can be performed if not listed here.
#
#       To disable an action, set the password to "disable".
#       To allow performing an action without a password, set the
#       password to "none".
#
#       Use the keyword "all" to set the same password for all actions.
#
#Example:
# cachemgr_passwd secret shutdown
# cachemgr_passwd lesssssssecret info stats/objects
# cachemgr_passwd disable all
#
#Default:
# none

#  TAG: store_avg_object_size (kbytes)
#       Average object size, used to estimate number of objects your
#       cache can hold.  See doc/Release-Notes-1.1.txt.  The default is
#       13 KB.
#
#Default:
# store_avg_object_size 13 KB

#  TAG: store_objects_per_bucket
#       Target number of objects per bucket in the store hash table.
#       Lowering this value increases the total number of buckets and
#       also the storage maintenance rate.  The default is 50.
#
#Default:
```

```
# store_objects_per_bucket 20

#  TAG: client_db     on|off
#       If you want to disable collecting per-client statistics, then
#       turn off client_db here.
#
#Default:
# client_db on

#  TAG: netdb_low
#  TAG: netdb_high
#       The low and high water marks for the ICMP measurement
#       database.  These are counts, not percents.  The defaults are
#       900 and 1000.  When the high water mark is reached, database
#       entries will be deleted until the low mark is reached.
#
#Default:
# netdb_low 900
# netdb_high 1000

#  TAG: netdb_ping_period
#       The minimum period for measuring a site.  There will be at
#       least this much delay between successive pings to the same
#       network.  The default is five minutes.
#
#Default:
# netdb_ping_period 5 minutes

#  TAG: query_icmp    on|off
#       If you want to ask your peers to include ICMP data in their ICP
#       replies, enable this option.
#
#       If your peer has configured Squid (during compilation) with
#       '--enable-icmp' then that peer will send ICMP pings to origin server
#       sites of the URLs it receives.  If you enable this option then the
#       ICP replies from that peer will include the ICMP data (if available).
#       Then, when choosing a parent cache, Squid will choose the parent with
#       the minimal RTT to the origin server.  When this happens, the
#       hierarchy field of the access.log will be
#       "CLOSEST_PARENT_MISS".  This option is off by default.
#
#Default:
# query_icmp off

#  TAG: test_reachability     on|off
#       When this is 'on', ICP MISS replies will be ICP_MISS_NOFETCH
#       instead of ICP_MISS if the target host is NOT in the ICMP
#       database, or has a zero RTT.
#
#Default:
# test_reachability off

#  TAG: buffered_logs on|off
#       cache.log log file is written with stdio functions, and as such
#       it can be buffered or unbuffered. By default it will be unbuffered.
#       Buffering it can speed up the writing slightly (though you are
#       unlikely to need to worry unless you run with tons of debugging
#       enabled in which case performance will suffer badly anyway..).
#
#Default:
# buffered_logs off

#  TAG: reload_into_ims       on|off
#       When you enable this option, client no-cache or ``reload''
#       requests will be changed to If-Modified-Since requests.
#       Doing this VIOLATES the HTTP standard.  Enabling this
#       feature could make you liable for problems which it
#       causes.
#
#       see also refresh_pattern for a more selective approach.
#
```

```
#Default:
# reload_into_ims off

#  TAG: always_direct
#       Usage: always_direct allow|deny [!]aclname ...
#
#       Here you can use ACL elements to specify requests which should
#       ALWAYS be forwarded directly to origin servers.  For example,
#       to always directly forward requests for local servers use
#       something like:
#
#               acl local-servers dstdomain my.domain.net
#               always_direct allow local-servers
#
#       To always forward FTP requests directly, use
#
#               acl FTP proto FTP
#               always_direct allow FTP
#
#       NOTE: There is a similar, but opposite option named
#       'never_direct'.  You need to be aware that "always_direct deny
#       foo" is NOT the same thing as "never_direct allow foo".  You
#       may need to use a deny rule to exclude a more-specific case of
#       some other rule.  Example:
#
#               acl local-external dstdomain external.foo.net
#               acl local-servers dstdomain  .foo.net
#               always_direct deny local-external
#               always_direct allow local-servers
#
#       This option replaces some v1.1 options such as local_domain
#       and local_ip.
#
#Default:
# none

#  TAG: never_direct
#       Usage: never_direct allow|deny [!]aclname ...
#
#       never_direct is the opposite of always_direct.  Please read
#       the description for always_direct if you have not already.
#
#       With 'never_direct' you can use ACL elements to specify
#       requests which should NEVER be forwarded directly to origin
#       servers.  For example, to force the use of a proxy for all
#       requests, except those in your local domain use something like:
#
#               acl local-servers dstdomain .foo.net
#               acl all src 0.0.0.0/0.0.0.0
#               never_direct deny local-servers
#               never_direct allow all
#
#       or if squid is inside a firewall and there is local intranet
#       servers inside the firewall then use something like:
#
#               acl local-intranet dstdomain .foo.net
#               acl local-external dstdomain external.foo.net
#               always_direct deny local-external
#               always_direct allow local-intranet
#               never_direct allow all
#
#       This option replaces some v1.1 options such as inside_firewall
#       and firewall_ip.
#
#Default:
# none

#  TAG: header_access
#       Usage: header_access header_name allow|deny [!]aclname ...
#
#       WARNING: Doing this VIOLATES the HTTP standard.  Enabling
```

```
#       this feature could make you liable for problems which it
#       causes.
#
#       This option replaces the old 'anonymize_headers' and the
#       older 'http_anonymizer' option with something that is much
#       more configurable. This new method creates a list of ACLs
#       for each header, allowing you very fine-tuned header
#       mangling.
#
#       You can only specify known headers for the header name.
#       Other headers are reclassified as 'Other'. You can also
#       refer to all the headers with 'All'.
#
#       For example, to achieve the same behaviour as the old
#       'http_anonymizer standard' option, you should use:
#
#               header_access From deny all
#               header_access Referer deny all
#               header_access Server deny all
#               header_access User-Agent deny all
#               header_access WWW-Authenticate deny all
#               header_access Link deny all
#
#       Or, to reproduce the old 'http_anonymizer paranoid' feature
#       you should use:
#
#               header_access Allow allow all
#               header_access Authorization allow all
#               header_access WWW-Authenticate allow all
#               header_access Cache-Control allow all
#               header_access Content-Encoding allow all
#               header_access Content-Length allow all
#               header_access Content-Type allow all
#               header_access Date allow all
#               header_access Expires allow all
#               header_access Host allow all
#               header_access If-Modified-Since allow all
#               header_access Last-Modified allow all
#               header_access Location allow all
#               header_access Pragma allow all
#               header_access Accept allow all
#               header_access Accept-Charset allow all
#               header_access Accept-Encoding allow all
#               header_access Accept-Language allow all
#               header_access Content-Language allow all
#               header_access Mime-Version allow all
#               header_access Retry-After allow all
#               header_access Title allow all
#               header_access Connection allow all
#               header_access Proxy-Connection allow all
#               header_access All deny all
#
#       By default, all headers are allowed (no anonymizing is
#       performed).
#
#Default:
# none

#  TAG: header_replace
#       Usage:   header_replace header_name message
#       Example: header_replace User-Agent Nutscrape/1.0 (CP/M; 8-bit)
#
#       This option allows you to change the contents of headers
#       denied with header_access above, by replacing them with
#       some fixed string. This replaces the old fake_user_agent
#       option.
#
#       By default, headers are removed if denied.
#
#Default:
# none
```

```
#  TAG: icon_directory
#       Where the icons are stored. These are normally kept in
#       /usr/share/squid/icons
#
#Default:
# icon_directory /usr/share/squid/icons

#  TAG: error_directory
#       Directory where the error files are read from.
#       /usr/lib/squid/errors contains sets of error files
#       in different languages. The default error directory
#       is /etc/squid/errors, which is a link to one of these
#       error sets.
#
#       If you wish to create your own versions of the error files,
#       either to customize them to suit your language or company,
#       copy the template English files to another
#       directory and point this tag at them.
#
#error_directory /etc/squid/errors
#
#Default:
# error_directory /etc/squid/errors

#  TAG: minimum_retry_timeout (seconds)
#       This specifies the minimum connect timeout, for when the
#       connect timeout is reduced to compensate for the availability
#       of multiple IP addresses.
#
#       When a connection to a host is initiated, and that host has
#       several IP addresses, the default connection timeout is reduced
#       by dividing it by the number of addresses.  So, a site with 15
#       addresses would then have a timeout of 8 seconds for each
#       address attempted.  To avoid having the timeout reduced to the
#       point where even a working host would not have a chance to
#       respond, this setting is provided.  The default, and the
#       minimum value, is five seconds, and the maximum value is sixty
#       seconds, or half of connect_timeout, whichever is greater and
#       less than connect_timeout.
#
#Default:
# minimum_retry_timeout 5 seconds

#  TAG: maximum_single_addr_tries
#       This sets the maximum number of connection attempts for a
#       host that only has one address (for multiple-address hosts,
#       each address is tried once).
#
#       The default value is three tries, the (not recommended)
#       maximum is 255 tries.  A warning message will be generated
#       if it is set to a value greater than ten.
#
#Default:
# maximum_single_addr_tries 3

#  TAG: snmp_port
#       Squid can now serve statistics and status information via SNMP.
#       A value of "0" disables SNMP support. If you wish to use SNMP,
#       set this to "3401" to use the normal SNMP support.
#
#Default:
# snmp_port 0

#  TAG: snmp_access
#       Allowing or denying access to the SNMP port.
#
#       All access to the agent is denied by default.
#       usage:
#
#       snmp_access allow|deny [!]aclname ...
```

```
#
#Example:
# snmp_access allow snmppublic localhost
# snmp_access deny all
#
#Default:
# snmp_access deny all

#  TAG: snmp_incoming_address
#  TAG: snmp_outgoing_address
#       Just like 'udp_incoming_address' above, but for the SNMP port.
#
#       snmp_incoming_address is used for the SNMP socket receiving
#                             messages from SNMP agents.
#       snmp_outgoing_address is used for SNMP packets returned to SNMP
#                             agents.
#
#       The default snmp_incoming_address (0.0.0.0) is to listen on all
#       available network interfaces.
#
#       If snmp_outgoing_address is set to 255.255.255.255 (the default)
#       then it will use the same socket as snmp_incoming_address. Only
#       change this if you want to have SNMP replies sent using another
#       address than where this Squid listens for SNMP queries.
#
#       NOTE, snmp_incoming_address and snmp_outgoing_address can not have
#       the same value since they both use port 3401.
#
#Default:
# snmp_incoming_address 0.0.0.0
# snmp_outgoing_address 255.255.255.255

#  TAG: as_whois_server
#       WHOIS server to query for AS numbers.  NOTE: AS numbers are
#       queried only when Squid starts up, not for every request.
#
#Default:
# as_whois_server whois.ra.net
# as_whois_server whois.ra.net

#  TAG: wccp_router
#       Use this option to define your WCCP ``home'' router for
#       Squid.   Setting the 'wccp_router' to 0.0.0.0 (the default)
#       disables WCCP.
#
#Default:
# wccp_router 0.0.0.0

#  TAG: wccp_version
#       According to some users, Cisco IOS 11.2 only supports WCCP
#       version 3.  If you're using that version of IOS, change
#       this value to 3.
#
#Default:
# wccp_version 4

#  TAG: wccp_incoming_address
#  TAG: wccp_outgoing_address
#        wccp_incoming_address   Use this option if you require WCCP
#                                messages to be received on only one
#                                interface.  Do NOT use this option if
#                                you're unsure how many interfaces you
#                                have, or if you know you have only one
#                                interface.
#
#       wccp_outgoing_address Use this option if you require WCCP
#                                messages to be sent out on only one
#                                interface.  Do NOT use this option if
#                                you're unsure how many interfaces you
#                                have, or if you know you have only one
#                                interface.
```

```
#
#        The default behavior is to not bind to any specific address.
#
#        NOTE, wccp_incoming_address and wccp_outgoing_address can not have
#        the same value since they both use port 2048.
#
#Default:
# wccp_incoming_address 0.0.0.0
# wccp_outgoing_address 255.255.255.255


# DELAY POOL PARAMETERS (all require DELAY_POOLS compilation option)
# -----------------------------------------------------------------------------

#  TAG: delay_pools
#       This represents the number of delay pools to be used.  For example,
#       if you have one class 2 delay pool and one class 3 delays pool, you
#       have a total of 2 delay pools.
#
#Default:
# delay_pools 0

#  TAG: delay_class
#       This defines the class of each delay pool.  There must be exactly one
#       delay_class line for each delay pool.  For example, to define two
#       delay pools, one of class 2 and one of class 3, the settings above
#       and here would be:
#
#Example:
# delay_pools 2      # 2 delay pools
# delay_class 1 2    # pool 1 is a class 2 pool
# delay_class 2 3    # pool 2 is a class 3 pool
#
#       The delay pool classes are:
#
#              class 1        Everything is limited by a single aggregate
#                             bucket.
#
#              class 2        Everything is limited by a single aggregate
#                             bucket as well as an "individual" bucket chosen
#                             from bits 25 through 32 of the IP address.
#
#              class 3        Everything is limited by a single aggregate
#                             bucket as well as a "network" bucket chosen
#                             from bits 17 through 24 of the IP address and a
#                             "individual" bucket chosen from bits 17 through
#                             32 of the IP address.
#
#       NOTE: If an IP address is a.b.c.d
#              -> bits 25 through 32 are "d"
#              -> bits 17 through 24 are "c"
#              -> bits 17 through 32 are "c * 256 + d"
#
#Default:
# none

#  TAG: delay_access
#       This is used to determine which delay pool a request falls into.
#       The first matched delay pool is always used, i.e., if a request falls
#       into delay pool number one, no more delay are checked, otherwise the
#       rest are checked in order of their delay pool number until they have
#       all been checked.  For example, if you want some_big_clients in delay
#       pool 1 and lotsa_little_clients in delay pool 2:
#
#Example:
# delay_access 1 allow some_big_clients
# delay_access 1 deny all
# delay_access 2 allow lotsa_little_clients
# delay_access 2 deny all
#
#Default:
```

```
# none

#  TAG: delay_parameters
#       This defines the parameters for a delay pool.  Each delay pool has
#       a number of "buckets" associated with it, as explained in the
#       description of delay_class.  For a class 1 delay pool, the syntax is:
#
#delay_parameters pool aggregate
#
#       For a class 2 delay pool:
#
#delay_parameters pool aggregate individual
#
#       For a class 3 delay pool:
#
#delay_parameters pool aggregate network individual
#
#       The variables here are:
#
#              pool            a pool number - ie, a number between 1 and the
#                              number specified in delay_pools as used in
#                              delay_class lines.
#
#              aggregate       the "delay parameters" for the aggregate bucket
#                              (class 1, 2, 3).
#
#              individual      the "delay parameters" for the individual
#                              buckets (class 2, 3).
#
#              network         the "delay parameters" for the network buckets
#                              (class 3).
#
#       A pair of delay parameters is written restore/maximum, where restore is
#       the number of bytes (not bits - modem and network speeds are usually
#       quoted in bits) per second placed into the bucket, and maximum is the
#       maximum number of bytes which can be in the bucket at any time.
#
#       For example, if delay pool number 1 is a class 2 delay pool as in the
#       above example, and is being used to strictly limit each host to 64kbps
#       (plus overheads), with no overall limit, the line is:
#
#delay_parameters 1 -1/-1 8000/8000
#
#       Note that the figure -1 is used to represent "unlimited".
#
#       And, if delay pool number 2 is a class 3 delay pool as in the above
#       example, and you want to limit it to a total of 256kbps (strict limit)
#       with each 8-bit network permitted 64kbps (strict limit) and each
#       individual host permitted 4800bps with a bucket maximum size of 64kb
#       to permit a decent web page to be downloaded at a decent speed
#       (if the network is not being limited due to overuse) but slow down
#       large downloads more significantly:
#
#delay_parameters 2 32000/32000 8000/8000 600/8000
#
#       There must be one delay_parameters line for each delay pool.
#
#Default:
# none

#  TAG: delay_initial_bucket_level   (percent, 0-100)
#       The initial bucket percentage is used to determine how much is put
#       in each bucket when squid starts, is reconfigured, or first notices
#       a host accessing it (in class 2 and class 3, individual hosts and
#       networks only have buckets associated with them once they have been
#       "seen" by squid).
#
#Default:
# delay_initial_bucket_level 50

#  TAG: incoming_icp_average
```

```
#  TAG: incoming_http_average
#  TAG: incoming_dns_average
#  TAG: min_icp_poll_cnt
#  TAG: min_dns_poll_cnt
#  TAG: min_http_poll_cnt
#       Heavy voodoo here.  I can't even believe you are reading this.
#       Are you crazy?  Don't even think about adjusting these unless
#       you understand the algorithms in comm_select.c first!
#
#Default:
# incoming_icp_average 6
# incoming_http_average 4
# incoming_dns_average 4
# min_icp_poll_cnt 8
# min_dns_poll_cnt 8
# min_http_poll_cnt 8

#  TAG: max_open_disk_fds
#       To avoid having disk as the I/O bottleneck Squid can optionally
#       bypass the on-disk cache if more than this amount of disk file
#       descriptors are open.
#
#       A value of 0 indicates no limit.
#
#Default:
# max_open_disk_fds 0

#  TAG: offline_mode
#       Enable this option and Squid will never try to validate cached
#       objects.
#
#Default:
# offline_mode off

#  TAG: uri_whitespace
#       What to do with requests that have whitespace characters in the
#       URI.  Options:
#
#       strip:  The whitespace characters are stripped out of the URL.
#               This is the behavior recommended by RFC2616.
#       deny:   The request is denied.  The user receives an "Invalid
#               Request" message.
#       allow:  The request is allowed and the URI is not changed.  The
#               whitespace characters remain in the URI.  Note the
#               whitespace is passed to redirector processes if they
#               are in use.
#       encode: The request is allowed and the whitespace characters are
#               encoded according to RFC1738.  This could be considered
#               a violation of the HTTP/1.1
#               RFC because proxies are not allowed to rewrite URI's.
#       chop:   The request is allowed and the URI is chopped at the
#               first whitespace.  This might also be considered a
#               violation.
#
#Default:
# uri_whitespace strip

#  TAG: broken_posts
#       A list of ACL elements which, if matched, causes Squid to send
#       an extra CRLF pair after the body of a PUT/POST request.
#
#       Some HTTP servers has broken implementations of PUT/POST,
#       and rely on an extra CRLF pair sent by some WWW clients.
#
#       Quote from RFC 2068 section 4.1 on this matter:
#
#         Note: certain buggy HTTP/1.0 client implementations generate an
#         extra CRLF's after a POST request. To restate what is explicitly
#         forbidden by the BNF, an HTTP/1.1 client must not preface or follow
#         a request with an extra CRLF.
#
```

```
#Example:
# acl buggy_server url_regex ^http://....
# broken_posts allow buggy_server
#
#Default:
# none

#  TAG: mcast_miss_addr
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_STREAM option
#
#       If you enable this option, every "cache miss" URL will
#       be sent out on the specified multicast address.
#
#       Do not enable this option unless you are are absolutely
#       certain you understand what you are doing.
#
#Default:
# mcast_miss_addr 255.255.255.255

#  TAG: mcast_miss_ttl
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_TTL option
#
#       This is the time-to-live value for packets multicasted
#       when multicasting off cache miss URLs is enabled.  By
#       default this is set to 'site scope', i.e. 16.
#
#Default:
# mcast_miss_ttl 16

#  TAG: mcast_miss_port
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_STREAM option
#
#       This is the port number to be used in conjunction with
#       'mcast_miss_addr'.
#
#Default:
# mcast_miss_port 3135

#  TAG: mcast_miss_encode_key
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_STREAM option
#
#       The URLs that are sent in the multicast miss stream are
#       encrypted.  This is the encryption key.
#
#Default:
# mcast_miss_encode_key XXXXXXXXXXXXXXXX

#  TAG: nonhierarchical_direct
#       By default, Squid will send any non-hierarchical requests
#       (matching hierarchy_stoplist or not cachable request type) direct
#       to origin servers.
#
#       If you set this to off, then Squid will prefer to send these
#       requests to parents.
#
#       Note that in most configurations, by turning this off you will only
#       add latency to these request without any improvement in global hit
#       ratio.
#
#       If you are inside an firewall then see never_direct instead of
#       this directive.
#
#Default:
# nonhierarchical_direct on

#  TAG: prefer_direct
#       Normally Squid tries to use parents for most requests. If you by some
```

```
#       reason like it to first try going direct and only use a parent if
#       going direct fails then set this to on.
#
#       By combining nonhierarchical_direct off and prefer_direct on you
#       can set up Squid to use a parent as a backup path if going direct
#       fails.
#
#Default:
# prefer_direct off

#  TAG: strip_query_terms
#       By default, Squid strips query terms from requested URLs before
#       logging.  This protects your user's privacy.
#
#Default:
# strip_query_terms on

#  TAG: coredump_dir
#       By default Squid leaves core files in the directory from where
#       it was started. If you set 'coredump_dir' to a directory
#       that exists, Squid will chdir() to that directory at startup
#       and coredump files will be left there.
#
#Default:
# coredump_dir none
#
# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#  TAG: redirector_bypass
#       When this is 'on', a request will not go through the
#       redirector if all redirectors are busy.  If this is 'off'
#       and the redirector queue grows too large, Squid will exit
#       with a FATAL error and ask you to increase the number of
#       redirectors.  You should only enable this if the redirectors
#       are not critical to your caching system.  If you use
#       redirectors for access control, and you enable this option,
#       then users may have access to pages that they should not
#       be allowed to request.
#
#Default:
# redirector_bypass off

#  TAG: ignore_unknown_nameservers
#       By default Squid checks that DNS responses are received
#       from the same IP addresses that they are sent to.  If they
#       don't match, Squid ignores the response and writes a warning
#       message to cache.log.  You can allow responses from unknown
#       nameservers by setting this option to 'off'.
#
#Default:
# ignore_unknown_nameservers on

#  TAG: digest_generation
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This controls whether the server will generate a Cache Digest
#       of its contents.  By default, Cache Digest generation is
#       enabled if Squid is compiled with USE_CACHE_DIGESTS defined.
#
#Default:
# digest_generation on

#  TAG: digest_bits_per_entry
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the number of bits of the server's Cache Digest which
#       will be associated with the Digest entry for a given HTTP
#       Method and URL (public key) combination.  The default is 5.
```

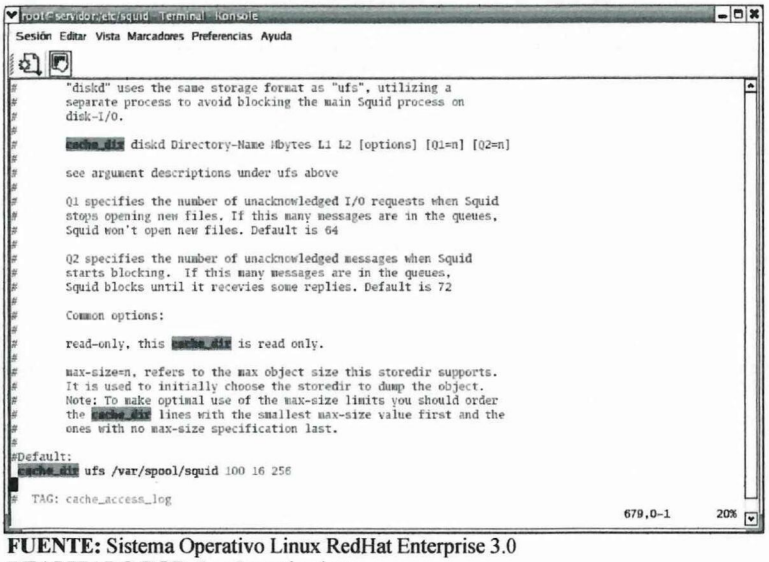
```
#
#Default:
# digest_bits_per_entry 5

#  TAG: digest_rebuild_period (seconds)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the number of seconds between Cache Digest rebuilds.
#
#Default:
# digest_rebuild_period 1 hour

#  TAG: digest_rewrite_period (seconds)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the number of seconds between Cache Digest writes to
#       disk.
#
#Default:
# digest_rewrite_period 1 hour

#  TAG: digest_swapout_chunk_size    (bytes)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the number of bytes of the Cache Digest to write to
#       disk at a time.  It defaults to 4096 bytes (4KB), the Squid
#       default swap page.
#
#Default:
# digest_swapout_chunk_size 4096 bytes

#  TAG: digest_rebuild_chunk_percentage      (percent, 0-100)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the percentage of the Cache Digest to be scanned at a
#       time.  By default it is set to 10% of the Cache Digest.
#
#Default:
# digest_rebuild_chunk_percentage 10

#  TAG: chroot
#       Use this to have Squid do a chroot() while initializing.  This
#       also causes Squid to fully drop root privileges after
#       initializing.  This means, for example, that if you use a HTTP
#       port less than 1024 and try to reconfigure, you will get an
#       error.
#
#Default:
# none

#  TAG: client_persistent_connections
#  TAG: server_persistent_connections
#       Persistent connection support for clients and servers.  By
#       default, Squid uses persistent connections (when allowed)
#       with its clients and servers.  You can use these options to
#       disable persistent connections with clients and/or servers.
#
#Default:
# client_persistent_connections on
# server_persistent_connections on

#  TAG: pipeline_prefetch
#       To boost the performance of pipelined requests to closer
#       match that of a non-proxied environment Squid can try to fetch
#       up to two requests in parallell from a pipeline.
#
#       Defaults to off for bandwidth management and access logging
```

```
#       reasons.
#
#Default:
# pipeline_prefetch off

#  TAG: extension_methods
#       Squid only knows about standardized HTTP request methods.
#       You can add up to 20 additional "extension" methods here.
#
#Default:
# none

#  TAG: request_entities
#       Squid defaults to deny GET and HEAD requests with request entities,
#       as the meaning of such requests are undefined in the HTTP standard
#       even if not explicitly forbidden.
#
#       Set this directive to on if you have clients which insists
#       on sending request entities in GET or HEAD requests.
#
#Default:
# request_entities off

#  TAG: high_response_time_warning   (msec)
#       If the one-minute median response time exceeds this value,
#       Squid prints a WARNING with debug level 0 to get the
#       administrators attention.  The value is in milliseconds.
#
#Default:
# high_response_time_warning 0

#  TAG: high_page_fault_warning
#       If the one-minute average page fault rate exceeds this
#       value, Squid prints a WARNING with debug level 0 to get
#       the administrators attention.  The value is in page faults
#       per second.
#
#Default:
# high_page_fault_warning 0

#  TAG: high_memory_warning
#       If the memory usage (as determined by mallinfo) exceeds
#       value, Squid prints a WARNING with debug level 0 to get
#       the administrators attention.
#
#Default:
# high_memory_warning 0

#  TAG: store_dir_select_algorithm
#       Set this to 'round-robin' as an alternative.
#
#Default:
# store_dir_select_algorithm least-load

#  TAG: forward_log
# Note: This option is only available if Squid is rebuilt with the
#       -DWIP_FWD_LOG option
#
#       Logs the server-side requests.
#
#       This is currently work in progress.
#
#Default:
# none

#  TAG: ie_refresh    on|off
#       Microsoft Internet Explorer up until version 5.5 Service
#       Pack 1 has an issue with transparent proxies, wherein it
#       is impossible to force a refresh.  Turning this on provides
#       a partial fix to the problem, by causing all IMS-REFRESH
#       requests from older IE versions to check the origin server
```

```
#       for fresh content.  This reduces hit ratio by some amount
#       (~10% in my experience), but allows users to actually get
#       fresh content when they want it.  Note that because Squid
#       cannot tell if the user is using 5.5 or 5.5SP1, the behavior
#       of 5.5 is unchanged from old versions of Squid (i.e. a
#       forced refresh is impossible).  Newer versions of IE will,
#       hopefully, continue to have the new behavior and will be
#       handled based on that assumption.  This option defaults to
#       the old Squid behavior, which is better for hit ratios but
#       worse for clients using IE, if they need to be able to
#       force fresh content.
#
#Default:
# ie_refresh off

#  TAG: vary_ignore_expire    on|off
#       Many HTTP servers supporting Vary gives such objects
#       immediate expiry time with no cache-control header
#       when requested by a HTTP/1.0 client. This option
#       enables Squid to ignore such expiry times until
#       HTTP/1.1 is fully implemented.
#       WARNING: This may eventually cause some varying
#       objects not intended for caching to get cached.
#
#Default:
# vary_ignore_expire off

#  TAG: sleep_after_fork      (microseconds)
#       When this is set to a non-zero value, the main Squid process
#       sleeps the specified number of microseconds after a fork()
#       system call. This sleep may help the situation where your
#       system reports fork() failures due to lack of (virtual)
#       memory. Note, however, that if you have a lot of child
#       processes, then these sleep delays will add up and your
#       Squid will not service requests for some amount of time
#       until all the child processes have been started.
#
#Default:
# sleep_after_fork 0
```

Además es recomendable verificar que la opción "cache_dir" este debe estar desconectada para que nuestro servidor guarde en un archivo temporal que funcionara como memoria cache, en donde se guardaran paginas que son comúnmente visitadas por los usuarios de nuestra Intranet, tal como se muestra en el grafico Nº 3.24.

**GRAFICO Nº 3.24: VERIFICAR DIRECTORIO CACHE**

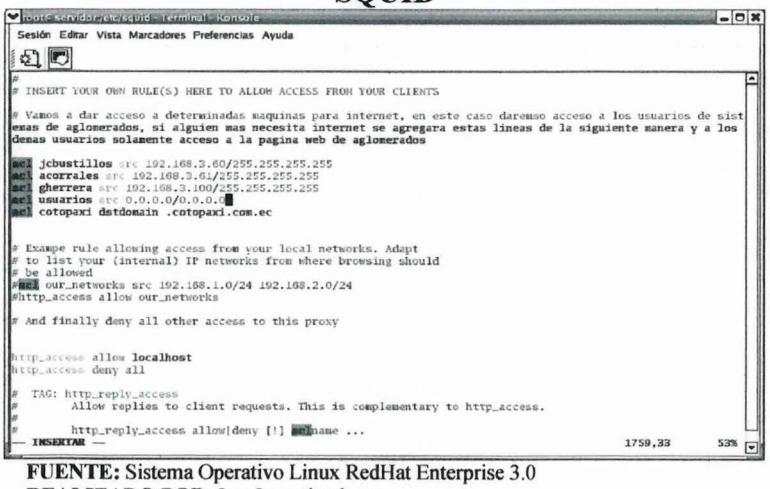



**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

### 3.1.6.7.2 SEGURIDAD PARA EL SERVIDOR PROXY

Un paso para tener seguro nuestro servidor Proxy seria la definición de usuarios a través de ACL, a continuación definimos usuarios y dominios a los que voy a permitir o denegar el acceso a Internet tal como se muestra en el grafico Nº 3.25.

**GRAFICO Nº 3.25: DEFINIR USUARIOS PARA SQUID**




**FUENTE:** Sistema Operativo Linux RedHat Enterprise 3.0
**REALIZADO POR:** Los Investigadores

Después de definir los usuarios procedemos a permitir o a denegar el acceso a Internet tal como se muestra en el grafico, los usuarios de sistemas jcbustillos, gherrera, acorrales tiene acceso ilimitado a Internet, pero los demás usuarios de nuestra red tienen solamente acceso al dominio "cotopaxi.com.ec", al final cierro cualquier conexión.

### 3.1.6.8 CONFIGURACIÓN DEL FIREWALL

Además de definir políticas de seguridad de ACL se procederá con la configuración de un firewall a nivel de IPTABLES. Esto lo haremos para proteger a nuestra red interna de agentes que pueden estar en el Internet; teniendo claro la definición de firewall procedemos a indicar a continuación como quedo configurado el servidor de Aglomerados Cotopaxi S.A. en su forma mas simple, el administrador estará en toda la potestad de modificar el mismo como necesite:

```
#!/bin/sh
## SCRIPT de IPTABLES - ejemplo del manual de iptables
## Ejemplo de script para proteger la propia máquina
## con política por defecto DROP
echo -n Aplicando Reglas de Firewall...

## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

## Establecemos politica por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

```
## Empezamos a filtrar

# El localhost se deja (por ejemplo conexiones locales a mysql)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# A nuestra IP le dejamos todo
iptables -A INPUT -s 192.168.3.69 -j ACCEPT
iptables -A OUTPUT -d 192.168.3.69 -j ACCEPT

# A un usuario le dejamos entrar al mysql para que mantenga la BBDD
iptables -A INPUT -s 231.45.134.23 -p tcp --dport 3306 -j ACCEPT
iptables -A OUTPUT -d 231.45.134.23 -p tcp --sport 3306 -j ACCEPT

# A un diseñador le dejamos usar el FTP
iptables -A INPUT -s 80.37.45.194 -p tcp --dport 20:21 -j ACCEPT
iptables -A OUTPUT -d 80.37.45.194 -p tcp --sport 20:21 -j ACCEPT

## Servidor WEB 211.34.149.2
# Acceso a puerto 80
iptables -A FORWARD -d 211.34.149.2 -p tcp --dport 80 -j ACCEPT

# Acceso a nuestra ip para gestionarlo
iptables -A FORWARD -s 210.195.55.15 -d 211.34.149.2 -p tcp --dport 22 -j
ACCEPT

# El resto, cerrar
iptables -A FORWARD -d 211.34.149.2 -j DROP

## Servidor MAIL 211.34.149.3
# Acceso a puerto 25, 110 y 143
iptables -A FORWARD -d 211.34.149.3 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -d 211.34.149.3 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -d 211.34.149.3 -p tcp --dport 143 -j ACCEPT

# Acceso a gestion SNMP
iptables -A FORWARD -s 210.195.55.15 -d 211.34.149.3 -p udp --dport 169 -j
ACCEPT

# Acceso a nuestra ip para gestionarlo
iptables -A FORWARD -s 210.195.55.15 -d 211.34.149.3 -p tcp --dport 22 -j
ACCEPT

# El resto, cerrar
iptables -A FORWARD -d 211.34.149.3 -j DROP


## Servidor IRC 211.34.149.4
```

```
# Acceso a puertos IRC
iptables -A FORWARD -d 211.34.149.4 -p tcp --dport 6666:6668 -j ACCEPT

# Acceso a nuestra ip para gestionarlo
iptables -A FORWARD -s 210.195.55.15 -d 211.34.149.4 -p tcp --dport 22 -j
ACCEPT

# El resto, cerrar
iptables -A FORWARD -d 211.34.149.4 -j DROP


# Aquí están las reglas de cerrar. Como hemos comentado en la configuración
# anterior conviene tener esto escrito por si en algún momento se relaja el
# firewall y s cambia a de DROP a ACCEPT por defecto
# Cerramos rango de los puertos privilegiados. Cuidado con este tipo de
# barreras, antes hay que abrir a los que si tienen acceso.
iptables -A INPUT -p tcp --dport 1:1024
iptables -A INPUT -p udp --dport 1:1024

# Cerramos otros puertos que estan abiertos
iptables -A INPUT -p tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp --dport 10000 -j DROP
iptables -A INPUT -p udp --dport 10000 -j DROP

echo " OK . Verifique que lo que se aplica con: iptables -L -n"

# Fin del script
```

# CAPITULO IV

# CONCLUSIONES Y RECOMENDACIONES

## 4.1 CONCLUSIONES

Luego de haber concluido el presente trabajo de investigación, con la implementación del servidor para la intranet podemos indicar las siguientes conclusiones:

- Con el presente sistema se pretende difundir las seguridades informáticas que existen utilizando para ello las nuevas técnicas de transmisión y representación de información mejorando la calidad del aprendizaje.
- La planificación y ejecución del proyecto en la empresa Aglomerados Cotopaxi S.A. ha impulsado el interés de los usuarios y todas las personas involucradas directa e indirectamente al manejo de información, debido a que la difusión de Linux y la gran aceptación que ha tenido así como la facilidad de adquirirlo han hecho de este sistema operativo una gran opción para proporcionar seguridad confiable a la información.
- Luego de realizado el proyecto de tesis se pudo apreciar la importancia del avance tecnológico con el uso de las herramientas que ofrece el Internet y los sistemas operativos.
- Se ha logrado enmarcar el uso de un nuevo Servicio de Seguridad Informática

para el manejo de información en ACOSA, puesto que con la implementación del Sistema, se complementará y reforzara la confianza del usuario.

- Se ha llegado a cumplir a cabalidad con el objetivo general, dándole la respectiva solución a los objetivos específicos probando de esta manera la implementación de los Servicios y Seguridades adquiridas por la empresa.

## 4.3 RECOMENDACIONES

Después de haber culminado con la implementación de Linux como sistema de seguridad informática creemos que es necesario realizar las siguientes recomendaciones.

- Se debe capacitar a los usuarios del sistema de la mejor manera, con la finalidad de que los usuarios y administradores se familiaricen con el mismo, de esta manera se encuentren en la capacidad de explotar al máximo todas las bondades que ofrece Linux y sus aplicaciones.
- Se debe adiestrar a una o varias personas en el manejo de Linux para que sean ellos los encargados de la administración de este servidor de intranet, ya que estos se dedicaran a la tarea de ajustar el sistema a las necesidades y exigencias del usuario.
- El administrador debe realizar el respectivo mantenimiento del servidor y efectuar actualizaciones periódicas de parches de seguridades de esta versión de Linux, conforme a las necesidades de la Empresa.

- El administrador deberá estar en la capacidad de realizar el respectivo monitoreo del servidor y depurar los Servidores de Seguridad para un mejor flujo de la información.
- Se recomienda revisar datos importantes del servidor y en base a esto realizar políticas para el respaldo de esta información, de esta manera es necesario contar con planes de contingencia para la recuperación de la información.

# BIBLIOGRAFÍA

## BÁSICA


- ALVAREZ, Rubén; SINTAXIS DE PHP; http://www.desarrolloWeb.com/articulos/307.php?manual=12.

- BANKHACKER; Requerimientos de MySQL; Todoexperto.com; 1999 – 2003

- BARBERO, Elisabet; Tutorial HTML; http://www:elCursillo - HTML - Básicos - Sintaxis de HTML.htm

- CABERO Almenara, J. et al. (1999). Practicas fundamentales de tecnología educativa

- CARACTERÍSTICAS TÉCNICAS DE FLASH; [http://www.cipotes.com/servicios/publicidad/advrequirements.asp]

- CEKIT, Curso Práctico sobre Internet, Apéndice A.

- ESPINOSA DE RIOS Mireya Lic., MORILLO V. Rosa A. Lic., Nociones Básicas de Investigación Científica.

- ESPINOZA H., Juan Carlos; "Red Hat Linux 7.0"; Instalación y Configuración Básica; 2001Alfaomega grupo editor, SA de CV.

- ESPOL, "Manual de Internet"; Primera edición; Espol; 1997.

- FTP;http//:FTP_archivos/extr@Internet/Informaciónsobreternet/FTP.htm junio,2003.

- GONZÁLES Sánchez José Luis, Red Hat Linux 8 Manual Avanzado, Editorial Multimedia

- KORTH, Henry F.; SILBERSCHATZ, Abraham; Fundamentos de Base de Datos; Segunda Edición.

- LARA, Luis Rodolfo Ing.; Análisis de los recursos interactivos en las aulas virtuales; Área: Educación, investigación científica y nuevas tecnologías.

- MANUAL INFORMATICA, Internet Colección N° 30,32,33, Capitulo 8.

- ORTEGA CARRILLO José Antonio, Universidad de Granada - Centro Unesco de Andalucía página WWW.

- PEARSON Educación. S.A. Madrid 2000. Linux Read Hat

- PETERSON Richard, Linux Manual de Referencia. Editorial Mc Graw Hill Interamericana S.A. 1996.

- PRESSMAN, Roger S; Ingeniería del Software; Un Enfoque Práctico; Cuarta Edición.

- RIVERA, Porto Eduardo Dr.; Sistema de Educación a Distancia en el Sistemas de Información; julio 2003; http//.ConceptosytendenciasenEducacionaDistancia.htm;

- SALNET; "MySQL"; Primera Edición; Salnet; 2002.

- SÁNCHEZ Madrigal, Carlos; Instalación y Configuración de Apache; http://www.linux.cu/manual/node88.html.

- SHAT, Steves, Manual de Administración de Linux, Editorial Mc Graw Hill Interamericana S.A. 2000

- Traducido por Salvador Fernández Barquín *sferbar@internetica.net.mx* Linux como Servidor de Intranets

- ULLOA Francisco, Guía de Investigación, Edición 2000.

- VETTER, Ronald J.; Las clases virtuales están más cerca de lo que imaginamos; Webmaster@xalapa.lania.mx; año 1994 LANIA, A.C.

- VILLATE, Jaime; "Manual de Apache"; Primera Edición; Software Web Ring 2002.

- VVAA. Manual Practico de Corel Linux, Editorial Prensa Técnica 2000.


**VIRTUAL**


- http://www.apmadrid.es/servicio/default.htm

- http://david.f.v.free.fr/ponencias/Seguridad_y_Linux/node1.html

- http://www.geocities.com/SiliconValley/Campus/2208/LIpag2.html

- http://www.linux.org.ve/que.shtml

- www.linux-es.org.que_es.php_files

- www.javara.tripod.com_files

- www.linux-es.org.que_es.php

- www.comp.os.linux.alpha
- www.alt.os.linux
- www.linuxdoc.org
- www.linuxapps.com
- www.counter.li.org
- www.pobox.com/newt/
- www.visar.csutan.edu:8000/giveaway.html
- www.caldera.com
- www.cdrom.com
- www.cs.utexas.edu/users/kharker/linux-laptop
- www.debian.org
- www.webwatcher.org

- www.infomagic.com
- www.kernel.org
- www.mcp.com
- www.rahul.net/kenton/index.shtml
- www.redhat.com
- www.linuxjournal.com
- www.xfree86.org


# GLOSARIO

A

- **ATRIBUTO:** Los atributos definen las propiedades de un objeto de datos y toman una de las tres características diferentes. Se puede utilizar para (1) nombrar una ocurrencia del objeto de datos, (2) describir la ocurrencia, o (3) hacer referencias a otra ocurrencia en otra tabla.

- **APACHE:** Servidor HTTP de dominio público basado en el sistema operativo Linux. Apache fue desarrollado en 1995 y actualmente es uno de los servidores HTTP más utilizados en la red.

**B**

- **BASE DE DATOS:** Conjunto de datos interrelacionados y estructurados, almacenados de forma que puedan servir para todos los programas que lo puedan utilizar.
- **BITS:** Código de un número binario que consiste en dos valores: cero (0) y uno 8 (1). También es la información que se puede almacenar en una celda sencilla de memoria.
- **BROWSER:** Navegador, programa que permite visualizar paginas Web y acceder a otros servicios de Internet.
- **BYTE:** Es un grupo de bits que tienen un significado singular. Un byte representa ocho bits.

**C**

- **CODIGO:** Conjunto de signos convencionales o instrucciones que permiten representar los datos para el manejo en la computadora.
- **CÓDIGO FUENTE:** Programa en su forma original, tal y como fue escrito por el programador, el código fuente no es ejecutable directamente por el computador, debe convertirse en lenguaje de máquina mediante compiladores, ensambladores o interpretes

- **CONEXIÓN:** Proceso por medio del cual se reciben, almacena y se transfieren paquetes a puerto del destino correcto.

**D**

- **DICCIONARIO DE DATOS:** Es una gráfica casi formal para describir el contenido de los objetos definidos durante el análisis estructurado.
- **DIAGRAMA DE FLUJO**: Es la representación gráfica de una secuencia de instrucciones de un programa que ejecuta un computador para obtener un resultado determinado.

**E**

- **E-MAIL:** Correo Electrónico.
- **ENCRIPTACIÓN:** Método para codificar datos y prevenir el acceso desautorizado, comúnmente utilizado en Internet para proteger al mensaje e-mail de miradas curiosas.

**F**

- **FIREWALLS:** Corta fuegos.

**G**

- **GIGABYTE:** GB (gigabyte ,giga octeto). Un GB corresponde a 1.024 millones de bytes.

**H**

- **HAKERS:** Persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, ordenador o red de ordenadores.
- **HARDWARE:** La maquinaria y circuitos electrónicos que conforman un computador.

**I**

- **INTRANET:** Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.
- **IP:** Forma parte del TCP / IP y se encarga de administrar el envío de paquetes.

**J**

- **JAVA SCRIPS:** Lenguaje de programación para WWW desarrollado por Netscape, pertenece a la familia Java pero se diferencia en que los programas están incorporados en el fichero HTML.

**K**

- **KERNEL:** Núcleo

**L**

- **LAN:** Red de Áreas Local

- **LINUX:** Versión de libre distribución del sistema operativo UNIX; fue desarrollada por Linus Torvald.
- **LOGINS:** Sistema de identificación del usuario para el ingreso a un sistema computarizado, previo al password o palabra clave.

**M**

- **MODEM:** Modulador / Demodulador; es un convertidor de señales, dispositivo que convierte señales de datos digitales y binarias a una señal compatible con el medio que se esta utilizando.
- **MÓDULO:** Cada uno de los elementos de un equipo, programa o proceso que son idénticos de manera individual.

**N**

- **NAVEGADOR:** Son programas del ordenador que permiten visualizar la World Wide Web.
- **NETSCAPE NAVIGATOR:** Navegador WWW creado en 1995 por Marc Andreessen, de la empresa norteamericana Netscape. Es uno de los navegadores Internet más difundidos.

**O**

- **ON-LINE:** Conexión directa entre dos computadoras a través de módem en tiempo real.

**P**

- **PASSWORD: (palabra de paso, contraseña)** Conjunto de caracteres alfanuméricos que permite al usuario el acceso a un determinado recurso o la utilización de un servicio.
- **PIRATAS:** Personas que violan claves de seguridad apropiándose o modificando información causando daños en los sistemas o aún realizando transacciones financieras fraudulentas.
- **PROTOCOLO:** Conjunto de reglas que definen los procedimientos para que dos o más procesos intercambien información.

**R**

- **RED:** Conexión de dos o más computadoras para facilitar su comunicación. Gracias a esto se puede compartir información y recursos.
- **RED HAT:** Versión de Linux.

**S**

- **SISTEMA OPERATIVO:** Programa especial que se carga en un ordenador tras ser encendido y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán en dicho ordenador.
- **SITE WEB:** Conjunto de páginas Web de una instrucción o persona.
- **SOFTWARE:** Constituyen los compiladores, ensambladores, monitores, del sistema operativo, los programas utilitarios que permiten explorar eficientemente el Hardware.

**T**

- **TCP / IP:** Protocolo de control de transmisión, parte los mensajes en pequeños paquetes y que de este modo asegura su correcta recepción.
- **TELNET:** Referencias a Sesiones Interactivas.

**U**

- **URL:** (Uniform Ressorce Locator.) Denominación Estándar de la dirección en la Wold Wide Web de Internet.
- **USER NAME:** Por contraposición a UserID suele ser un nombre intangible que identifica al usuario de un sistema o red.
- **USUARIO:** Persona que interactúa con la computadora a nivel de aplicación.
- **USER/ID:** Identificacor de Usuario

**V**

- **VIRUS:** Programa cuyo objetivo es causar daños en un sistema informático y que se oculta o se disfraza para no ser detectado.
- **VERSIÓN:** Número que indica lo reciente que es un programa. Por ejemplo: Windows 3.0 es más antiguo que Windows 3.11. Windows 3.11 es básicamente el mismo Windows 3.0 pero con algunas mejoras.

**W**

- **WINDOWS:** Sistema operativo desarrollado por la empresa Microsoft y cuyas diversas versiones (3.1, 95, 98, NT, 2000, Me) dominan de forma abrumadora el mercado de los ordenadores personales.

- **WORK STATION:** Estación de Trabajo.

## Glosario de Siglas

**A**

- **ACOSA:** Empresa Industrial Aglomerados Cotopaxi S.A.

**B**

- **BD:** Base de Datos

**C**

- **CPU:** Unidad de Procesamiento Central.

**D**

- **DNS:** (Data Source Name); Servidor de Nombre de Dominio.
- **DOS:** (Disk Operating System); Sistema Operativo en Disco.
- **DLL's:** Lenguaje de Definición de Datos.

**F**

- **FAT:** Tabla de Dirección de Archivos.
- **FAQ:** (Frequently Asked Questions); Preguntas y Respuestas más Frecuentes.
- **FTP:** (Anonymous File Transfer Protocol); Protocolo anónimo de transferencia de archivos.

**G**

- **GIF:** (Graphics Interactive Format); Formato de Gráficos Interactivos

**H**

- **HTTP:** (Hyper Text Transfer Protocol); Protocolo de Transferencia de Hipertexto.
- **HTML:** (HiperText Maker Leguage); Lenguaje constructor de Hipertexto.

**I**

- **IP:** (Internet Protocol); Protocolo Internet.
- **ISP:** (Internet Service Provide); Proveedor de Servicio de Internet.
- **ITSA:** Instituto Tecnológico Superior Aeronáutico.

**J**

- **JPG:** (Joint Photographers Expert Group), Grupo Conjunto de Fotógrafos Expertos.

**K**

- **KB:** Kilobyte.

**L**

- **LAN:** Red área local.

**M**

- **MB:** Megabyte
- **MBYTES:** Megabits por segundo.

**N**

- **NFS:** Sistema de Ficheros de Red.

**O**

- **ODBC:** (Open DataBase Connectivity), Abriendo Conexión a una Base de Datos.
- **OS:** (Operatin System), Sistema Operativo.

**P**

- **PCI:** (Peripheral Component Interconnect), Interconexión de componentes periféricos.
- **PHP:** (Personal Home Page Tools) Herramientas para Páginas Iniciales Personales.
- **POSIX:** (Portable Operating System Interface for Unix), Interfaz de sistema operativo portátil para Unix.

**R**

- **RAM:** ( RADOM ACCESS MEMORY ), memoria de acceso aleatorio.

**S**

- **SSL:** (Secure Socket Layer), Capa de Conexión Segura.

**T**

- **TCP / IP:** (transmisión Control Protocol / Internet Protocol), Protocolo de Control de Transmisión / Protocolo de Internet.

**U**

- **URL:** (Uniform Resourse Locator), Localización Universal de Recursos.

**V**

- **VGA:** Controlador de video

# ANEXOS