ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO, PROXY Y SAMBA BAJO PLATAFORMA LINUX PARA EGAR S.A.

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

DAVID EDUARDO FREIRE HERRERA
dave_edu@hotmail.com

DIRECTOR: ING. CÉSAR GALLARDO
cgallardo11@yahoo.es

Quito, Abril 2008

DECLARACIÓN

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

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

David Eduardo Freire Herrera

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por David Eduardo Freire Herrera, bajo mi supervisión.

Ing. César Gallardo
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

En primer lugar a Dios por la salud, la vida y sabiduría para poder culminar un etapa importante de mi vida.

A mis padres por su carino y apoyo incondicional, quien con su claro ejemplo de esfuerzo, sacrificio y honestidad me ha dado la fortaleza para seguir adelante.

A mi hermano Edison por toda su ayuda y apoyo a lo largo de toda mi carrera universitaria, a mi hermanos Roberto y Diego por apoyarme y compartir conmigo los mejores momentos de mi vida.

Deseo exteriorizar mi gratitud imperecedera para mi tutor, Ing. César Gallardo, por su apoyo comprensión y paciencia pero sobre todo por su amistad brindada en el desarrollo del proyecto de tesis. A todos nuestros profesores, por la oportunidad de habernos realizado profesionalmente acrecentando nuestro acervo intelectual.

A mis amigos que de alguna manera contribuyeron con sus sabios consejos, demostrándome su amistad en todas las circunstancias a lo largo de esta etapa universitaria.

Y a la Ing. Mercedes Ashqui quien me brindó las facilidades necesarias para el desarrollo de la presente investigación así como la oportunidad de desarrollarme a nivel profesional.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

CAPITULO II

CAPITULO III

CAPITULO IV

ANEXO B: INSTALACIÓN DEL SISTEMA OPERATIVO

ÍNDICE DE TABLAS

CAPITULO II

ANEXO A: COSTOS DE IMPLEMENTACIÓN

CAPÍTULO I

1. IDENTIFICACIÓN DEL PROBLEMA

1.1 DESCRIPCIÓN GENERAL DE LA EMPRESA

EGAR S.A. es una empresa ecuatoriana productora de materiales de fricción con sede en Quito, y una planta de producción en Pifo, comprometida a cumplir con estándares mundiales de calidad y satisfacer las necesidades de los clientes.

Actualmente lidera el mercado de reposición ecuatoriano, sus productos son reconocidos a nivel nacional y en el mercado Internacional, especialmente en el Pacto Andino, Chile, Centro América y países de Oriente Medio Oriente.

EGAR S.A. cuenta con un Sistema de Gestión de Calidad ISO 9001:2000, certificado por BVQi, así como un Certificado de Conformidad con Sello de Calidad bajo norma técnica ecuatoriana INEN NTE 2 185 (Instituto Ecuatoriano de Normalización). Es miembro de organizaciones internacionales como el FMSI (Friction Materials Standards Institute). Su funcionamiento, basado en el compromiso formal de todo el personal, ha permitido desarrollar y mantener esquemas de mejoramiento continuo, que permite satisfacer las expectativas del mercado.

1.2 DESCRIPCIÓN DEL PROBLEMA ACTUAL DE LA EMPRESA

EGAR S.A. por motivos de marketing cuenta con tres dominios debidamente registrados que son de su propiedad.

- egar.com.ec
- ab-products.com.ec
- frenosautomotrices.com

Para uso del correo y aprovechando estos dominios, se ha asignado a los usuarios ubicados en cada uno de los puntos de la empresa a detallar, Oficinas

Administrativas en Quito y la planta de Producción en Pífo, un dominio distinto para diferenciar el correo que es dirigido hacia una y otra sede.
De esta forma la asignación de usuarios de correo es la siguiente:

- Para Usuarios ubicados en Quito
  nombreusuario@egar.com.ec
- Para Usuarios ubicados en Pífo
  nombreususario@ab-products.com.ec

EGAR S.A., tanto en sus oficinas Quito como en Pífo presenta en la actualidad problemas relacionados con el control de la navegación de los usuarios, la obtención de los respaldos de información y con la seguridad, rapidez y disponibilidad de su correo electrónico, problemas que han venido causando serias molestias dentro de la organización y han impedido un desarrollo normal de las actividades.
A continuación se detalla los mismos:

- Hay mucha dependencia hacia el proveedor de correos, impidiéndonos como administradores de red la administración y control del correo que llega a la empresa, de esta forma, no se tiene acceso a los logs del sistema para saber si el envío o recepción de los correos fue exitoso o no y si no lo fueron, qué razones tuvo.

  En el año 2007 el servidor del proveedor se cayó en al menos 3 ocasiones, con tiempos de uno a tres días para su rehabilitación, esto imposibilitó el envío y recepción de correos tanto externo como interno, causando una demora en la llegada de la información como en el desarrollo de las actividades.

  Esto porque para el envío y recepción del correo cada usuario se conecta directamente hacia el servidor del proveedor que está ubicado en los EEUU.

- No existe un servicio adecuado de antivirus y antispam por parte del proveedor de correos, atentando esto contra la seguridad, estabilidad de la red y la disponibilidad de los recursos.
  De esta forma la red es vulnerable a que contenidos maliciosos se depositen en cada máquina y que no solo atente contra la información de los usuarios sino que utilice al servidor de correo para que sea un generador de spam, lo que implicaría el ser bloqueado por los servidores de listas negras, impidiendo el enviar correo hacia cualquier parte del mundo.

- No hay un filtro adecuado que limite y restrinja el tipo de contenido web al que el usuario puede acceder.

- Inadecuado manejo de los respaldos de información de los usuarios, debido a que no existen políticas de obtención bien definidas, así como su automatización, de manera que permita respaldar la información en fechas pre-programadas.

1.3 OBJETIVOS

1.3.1 GENERAL

Implementar los servicios de correo electrónico, Proxy y Samba bajo plataforma Linux para concentrar el correo electrónico de la empresa en su servidor, mejorando la administración de la red en cuanto a seguridades, filtrado de paquetes y a obtención de respaldos.

1.3.2 ESPECÍFICOS

- ❖ Implementar y configurar un servicio de correo electrónico dentro de la propia red de Pífo y Quito.

- ❖ Instalar y configurar un software antispam y antivirus para tener un correo electrónico seguro.
- ❖ Instalar un Webmail para acceder al correo desde cualquier parte del mundo.
- ❖ Instalar y Configurar un proxy para permitir navegación de acuerdo a las políticas establecidas por la empresa.
- ❖ Implementar un servidor Samba para tener una política adecuada de los respaldos de información.

1.4 JUSTIFICACIÓN PRÁCTICA

El presente trabajo dará solución a los problemas anteriormente mencionados existentes en la red LAN de EGAR S.A. de Quito y Pifo.

La implementación y puesta en marcha de los servicios de correo electrónico, Samba y Proxy apoyará a mejorar la optimización de la seguridad tanto del correo entrante y saliente como el de la red en general, debido a la implementación de un firewall de web (Proxy). Asimismo en fechas preprogramadas se realizará la obtención de los respaldos de información de los usuarios, de manera automática.

1.5 PROPUESTA

Se instalará y pondrá en marcha un servidor bajo plataforma Linux tanto en Pifo como en Quito, implementando servicios como:

- ➢ **Servidor de correo**

Se configurarán servidores de correo independientes dentro de la red de Pifo y Quito, para concentrar todo el correo tanto interno como externo a cada red, el mail exchanger del proveedor quedará como servidor alternativo. El servidor en Quito se configurará para aceptar todo el correo que sea dirigido a la empresa, y actuará como un mail Gateway para el correo dirigido a Pìfo, esto quiere decir, que todo correo dirigido hacia el dominio ab-products.com.ec será enviado

directamente al servidor en Pifo. Cabe destacar que el servidor en Pìfo funcionará de manera independiente para el envío de correo en la red de Pìfo.
Además, se instalará y configurará adecuadamente en el servidor con software antispam y antivirus con altas técnicas de filtrado, que se actualicen periódicamente y permitan tener un correo electrónico seguro.

- **Servidor de internet (Proxy) en el cual:**

Se administrará las condiciones de navegación de cada usuario con base a un perfil determinado, esto es, por ejemplo, que la parte gerencial pueda tener acceso sin límites a internet, el departamento financiero solo a sitios relacionados con finanzas y, otros departamentos no puedan salir a internet.
Se instalará un Webmail que permita ver el correo desde cualquier parte del mundo, donde un usuario de la organización se encuentre. Esto será de utilidad para usuarios que, por situaciones de trabajo, viajen fuera de la ciudad o hacia el exterior y necesitan revisar periódicamente su correo.

- **Servidor Samba**

Se creará un script en el cual el servidor de manera automática y en fechas preestablecidas se conecte a la máquina de cada usuario que tiene Sistema Operativo Windows y respalde la información, comprimiéndola y anexando la fecha del respaldo a la vez. Este respaldo será guardado en el mismo servidor, en el home directory de cada usuario y posteriormente extraído y quemado en DVD.
Estas soluciones se implementarán en los dos servidores.
Los costos del proyecto de detallan en el Anexo A: Costos de Implementación.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 INTRODUCCIÓN A LAS REDES Y SISTEMAS OPERATIVOS

2.1.1 REDES [1]

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, se ha dado la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadores), así como a la puesta en orbita de los satélites de comunicación.

Cada vez más se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez.

Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se ha reemplazado con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas se conocen con

1 http://www.monografias.com/trabajos/introredes/introredes.shtml

el nombre de redes de ordenadores. Éstas dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información.

2.1.2 MODELO DE REFERENCIA OSI Y TCP/IP [2]

En 1977, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes.

El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

2.1.2.1 Estructura del Modelo OSI de ISO

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

- **Estructura multinivel:**

Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones específicas.

El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

2 http://www.monografias.com/trabajos13/modosi/modosi.shtml

- **Puntos de acceso:**

Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

- **Dependencias de Niveles:**

Cada nivel es dependiente del nivel inferior y también del superior.

- **Encabezados:**

En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora está enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje está constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

2.1.2.2 Niveles del Modelo OSI.

FIGURA 2. 1: NIVELES DEL MODELO OSI [3]

3 http://www.monografias.com/trabajos13/modosi/modosi.html

La descripción de los 7 niveles es la siguiente:

- **Nivel Físico:**

Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:
Definir conexiones físicas entre computadoras.

- Describir el aspecto mecánico de la interface física.
- Describir el aspecto eléctrico de la interface física.
- Describir el aspecto funcional de la interface física.
- Definir la Técnica de Transmisión.
- Definir el Tipo de Transmisión.
- Definir la Codificación de Línea.
- Definir la Velocidad de Transmisión.
- Definir el Modo de Operación de la Línea de Datos.

- **Nivel Enlace de Datos:**

Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:

- Detectar errores en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes.
- Realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para la sincronía.
- En general controla el nivel y es las interfaces con el nivel de red, al comunicarle a éste una transmisión libre de errores.

- **Nivel de Red:**

Este nivel define el enrutamiento y el envío de paquetes entre redes.
Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.

Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).

Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.

Define el estado de los mensajes que se envían a nodos de la red.

- **Nivel de Transporte:**

Este nivel actúa como un puente entre los tres niveles inferiores, totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados al procesamiento. Además, garantiza una entrega confiable de la información.

Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).

Este nivel define cómo direccionar la localidad física de los dispositivos de la red.

Asigna una dirección única de transporte a cada usuario.

Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.

Define la manera de habilitar y deshabilitar las conexiones entre los nodos.

Determina el protocolo que garantiza el envío del mensaje.

Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

- **Nivel Sesión:**

Proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

Establece el inicio y termino de la sesión.

Recuperación de la sesión.

Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.

Referencia a los dispositivos por nombre y no por dirección.

Permite escribir programas que correrán en cualquier instalación de red.

- **Nivel Presentación:**

Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.

Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.

Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.

Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.

- **Nivel Aplicación:**

Proporciona servicios al usuario del Modelo OSI.

Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.

Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), etc.

2.1.3 PROTOCOLO TCP/IP [4]

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP / IP.

TCP/IP es un protocolo DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa) que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes, el Transmission Controll Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de

4 http://elsitiodetelecomunicaciones.iespana.es/protocolo_tcp_ip.htm

todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. En Internet se diferencian cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- **Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).
- **Transporte:** Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- **Internet:** Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- **Enlace:** Los niveles OSI correspondientes son el de enlace y el nivel físico. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host, como puede ser una línea punto a punto o una red Ethernet.

2.1.4 DIRECCIONAMIENTO IPV4 [5]

2.1.4.1 Direccionamiento IP

IPv4 es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.
IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).
Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red determinará la clase de dirección IP que aplicaremos cuando proporcionemos direcciones IP a los equipos y otros hosts de nuestra red.

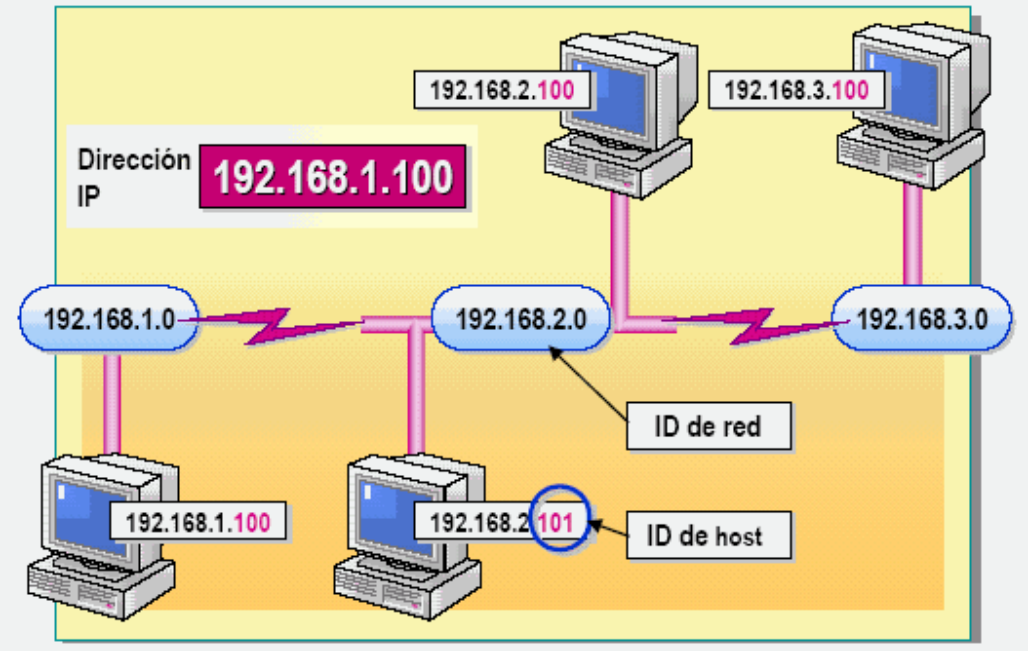

FIGURA 2. 2: ESQUEMA DE DIRECCIONAMIENTO IP [6]

5 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

6 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Se necesita una dirección IP para cada equipo y componente de red, como un router, que se comunique mediante TCP/IP.

La dirección IP identifica la ubicación de un equipo en la red, al igual que el número de la dirección identifica una casa en una ciudad. Al igual que sucede con la dirección de una casa específica, que es exclusiva pero sigue ciertas convenciones, una dirección IP debe ser exclusiva pero conforme a un formato estándar. Una dirección IP está formada por un conjunto de cuatro números, cada uno de los cuales puede oscilar entre 0 y 255.

2.1.4.2 Componentes de una dirección IP

Al igual que la dirección de una casa tiene dos partes (una calle y un código postal), una dirección IP también está formada por dos partes: el ID de host y el ID de red.

- **ID DE RED**

La primera parte de una dirección IP es el ID de red, que identifica el segmento de red en el que está ubicado el equipo.

Todos los equipos del mismo segmento deben tener el mismo ID de red, al igual que las casas de una zona determinada tienen el mismo código postal.

- **ID DE HOST**

La segunda parte de una dirección IP es el ID de host, que identifica un equipo, un router u otro dispositivo de un segmento.

El ID de cada host debe ser exclusivo en el ID de red, al igual que la dirección de una casa es exclusiva dentro de la zona del código postal.

Es importante observar que al igual que dos zonas de código postal distinto pueden tener direcciones iguales, dos equipos con diferentes IDs de red pueden tener el mismo ID de host. Sin embargo, la combinación del ID de red y el ID de host debe ser exclusivo para todos los equipos que se comuniquen entre sí.

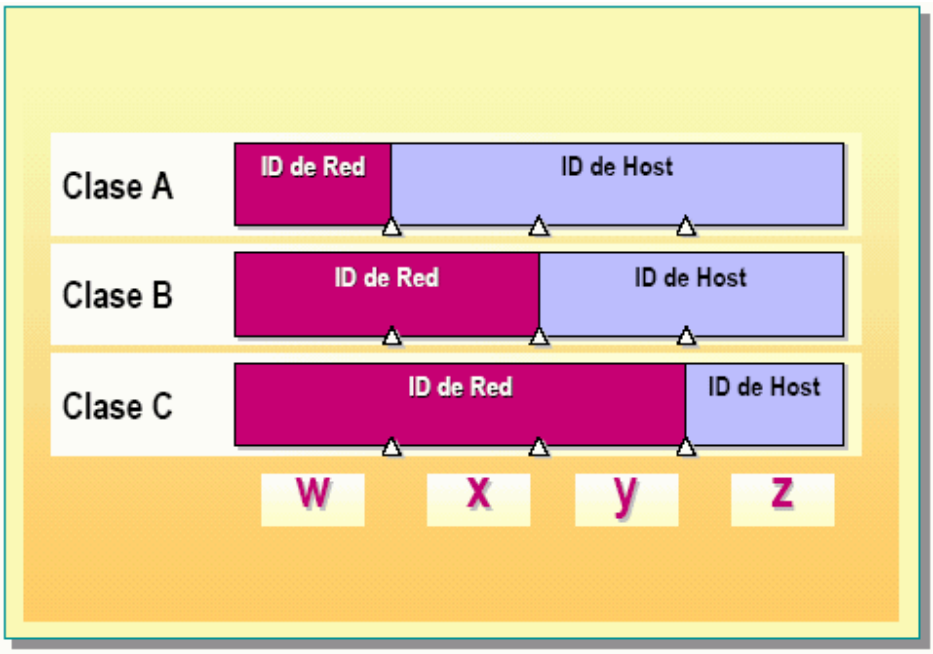

FIGURA 2. 3: CLASES DE DIRECCIONES IP [7]

Las clases de direcciones se utilizan para asignar IDs de red a organizaciones para que los equipos de sus redes puedan comunicarse en Internet. Las clases de direcciones también se utilizan para definir el punto de división entre el ID de red y el ID de host.

Se asigna a una organización un bloque de direcciones IP, que tienen como referencia el ID de red de las direcciones y que dependen del tamaño de la organización. Por ejemplo, se asignará un ID de red de clase C a una organización con 200 hosts, y un ID de red de clase B a una organización con 20.000 hosts.

CLASE A

Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16.777.214 hosts por red.

7 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

CLASE B

Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16.384 redes, utilizando los dos primeros números para el ID de red. Los dos números restantes se utilizan para el ID de host, permitiendo 65.534 hosts por red.

CLASE C

Las direcciones de clase C se utilizan para redes de área local (LANs) pequeñas. Esta clase permite aproximadamente 2.097.152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.

CLASES D Y E

Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.

2.1.4.3 Determinación de la clase de dirección

El direccionamiento IP en clases se basa en la estructura de la dirección IP y proporciona una forma sistemática de diferenciar IDs de red de IDs de host. Existen cuatro segmentos numéricos de una dirección IP. Una dirección IP puede estar representada como w.x.y.z, siendo w, x, y y z números con valores que oscilan entre 0 y 255. Dependiendo del valor del primer número, w en la representación numérica, las direcciones IP se clasifican en cinco clases de direcciones como se muestra en la siguiente tabla:

Clase de dirección IP	Dirección IP	ID de red	Valores de *w*
A	*w.x.y.z*	*w*.0.0.0	1 - 126*
B	*w.x.y.z*	*w.x*.0.0	128 – 191
C	*w.x.y.z*	*w.x.y*.0	192 – 223
D	*w.x.y.z*	No disponible	224 – 239
E	*w.x.y.z*	No disponible	240 - 255

*El ID de red 127.0.0.0 está reservado para las pruebas de conectividad.

FIGURA 2. 4: CLASES DE DIRECCIONES IP [8]

8 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

2.1.4.4 Determinación de los id de red y de host

En las direcciones IP de clase A, el ID de red es el primer número de la dirección IP. En la clase B, el ID de red son los dos primeros números; y en la clase C, el ID de red son los tres primeros números de la dirección IP. Los números restantes identifican el ID de host.

El ID de red tiene una estructura de cuatro números al igual que la dirección IP. Por tanto, si el primer número, w, de una dirección IP representa el ID de red, la estructura del ID de red es w.0.0.0, siendo 0 los tres números restantes. La estructura del ID de host es x.y.z. Observe que el host no va precedido de un 0.

Por ejemplo, la dirección IP 172.16.53.46 sería una dirección de clase B ya que w=172 y está entre 128 y 191. El ID de red sería 172.16.0.0 y el ID de host 53.46 (sin punto al final).

2.1.4.5 Subdivisión de una red

Se puede ampliar una red utilizando dispositivos físicos, como routers y puentes, para añadir segmentos de red. También es posible utilizar dispositivos físicos para dividir una red en segmentos más pequeños para incrementar la eficacia de la red.

Los segmentos de red separados por routers se denominan subredes. Cuando se crea subredes, se debe dividir el ID de red para los hosts de las subredes. La división del ID de red utilizado para comunicarse en Internet en IDs de red más pequeños (en función del número de direcciones IP identificadas) para una subred se denomina subdivisión de una red.

Para identificar el nuevo ID de red de cada subred, se debe utilizar una máscara de subred para especificar qué parte de la dirección IP va a ser utilizada por el nuevo ID de red de la subred. Se puede localizar un host en una red analizado su ID de red.

Los IDs de red coincidentes muestran qué hosts se encuentran en la misma subred. Si los IDs de red no son los mismos, se sabe que están en distintas subredes y que se necesitará un router para establecer comunicación entre ellos.

2.1.4.6 Planificación del direccionamiento IP

Una vez establecida una red, todos los equipos que se encuentran en ella necesitan una dirección IP; parecido a las viviendas de un edificio, que necesitan direcciones asignadas a ellas. Sin una dirección IP, un equipo no recibe los datos que van dirigidos a él. Y al igual que las direcciones de una vivienda, el formato de la dirección IP debe seguir ciertas directrices para garantizar que los datos se transmiten al equipo correcto.

Esta sección explica las directrices para asignar IDs de red y de host.

2.1.4.7 Directrices de Direccionamiento

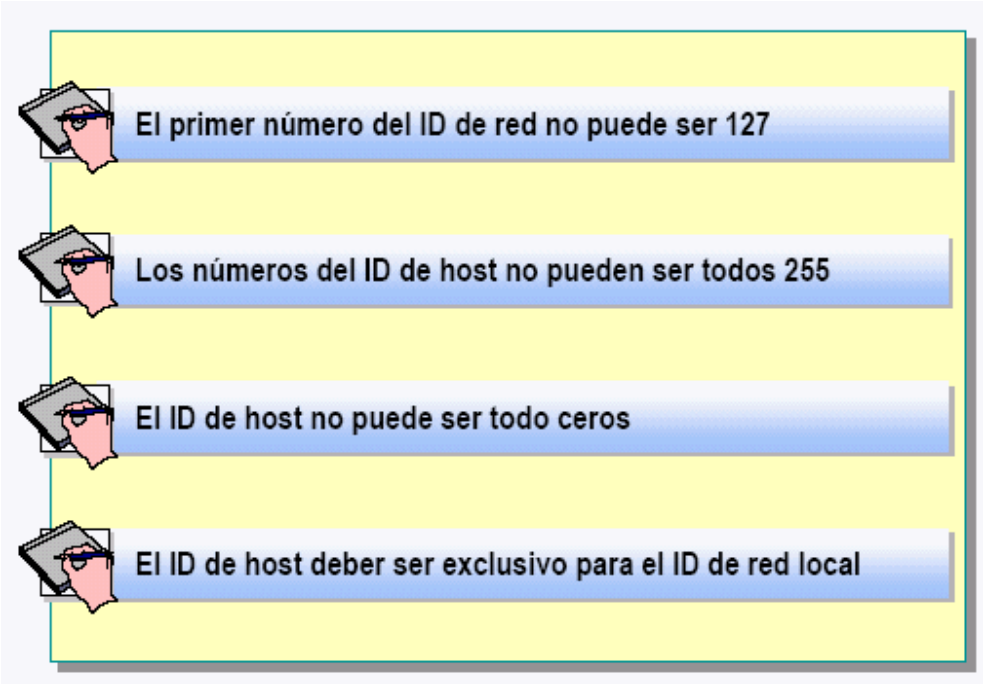

FIGURA 2. 5: DIRECTRICES DE DIRECCIONAMIENTO [9]

Hay que tener en cuenta algunas directrices sobre los números utilizados para el ID de red y el ID de host cuando se asigne una dirección IP utilizando clases. Estas directrices son las siguientes:

9 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

- El primer número del ID de red no puede ser 127. Este número de ID está reservado para pruebas de conexión, como realizar un bucle local.
- Los números del ID de host no pueden ser todos 255, ya que esta dirección se utiliza como dirección de difusión IP.
- El ID de host no puede ser todo ceros (0s), ya que esta dirección se utiliza para indicar un ID de red.
- El ID de host deber ser exclusivo para el ID de red local.

2.1.4.8 Asignación de IDs de red

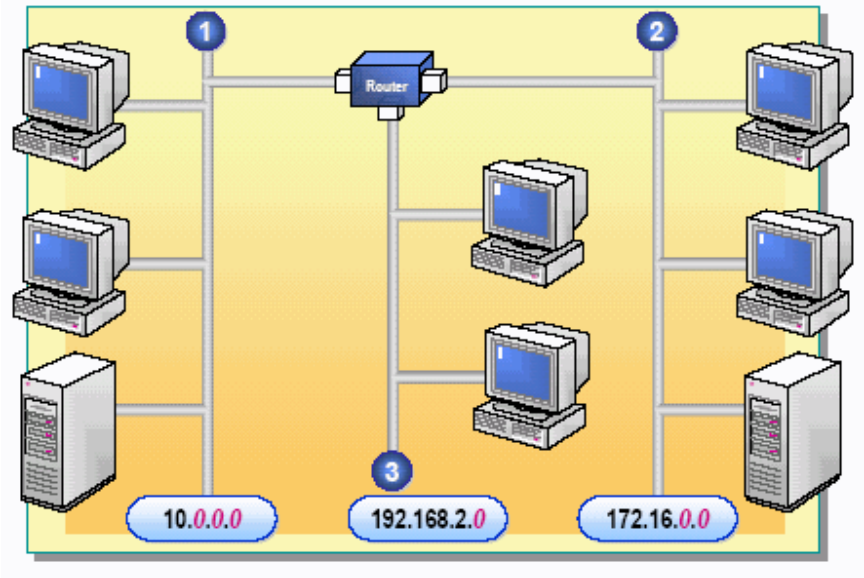

FIGURA 2. 6: ASIGNACIÓN DE ID DE RED [10]

El ID de red identifica los hosts TCP/IP ubicados en la misma subred física. Todos los hosts de la misma subred deben tener asignado el mismo ID de red para que puedan comunicarse entre sí.

Todas las subredes deben tener un ID de red exclusivo. Por ejemplo, la subred A podría tener el ID de red 10.0.0.0, la subred B podría tener el ID de red 192.168.2.0, y la subred C podría tener el ID de red 172.16.0.0. La siguiente tabla muestra una lista de intervalos válidos de IDs de red para una red.

10 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

Clase de dirección	Inicio del intervalo	Fin del intervalo
Clase A	1.0.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.0.0	223.255.255.0

2.1.4.9 Asignación de IDs de host

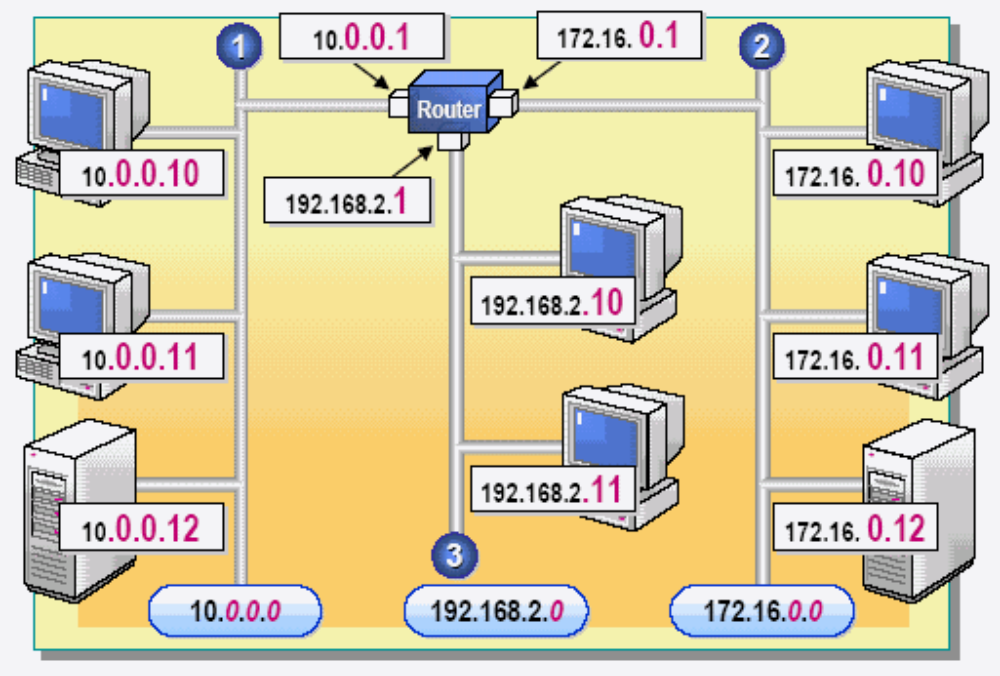

FIGURA 2. 7: ASIGNACIÓN DE ID DE HOST [11]

El ID de host identifica a un host TCP/IP de una red y debe ser exclusivo para un ID de red determinado. Todos los hosts TCP/IP, incluyendo los routers, requieren IDs de host exclusivos. No existen normas para la asignación de IDs de host en una subred. Por ejemplo, se puede numerar todos los hosts TCP/IP consecutivamente, o numerarlos para que puedan ser identificados fácilmente, por ejemplo asignando al router de cada subred el número 1 para el último número del ID de host.

11 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

IDs de host válidos La siguiente tabla muestra una lista de intervalos válidos de IDs de host para cada clase de red.

Clase de dirección	Inicio del intervalo	Fin del intervalo
Clase A	*w*.0.0.1	*w*.255.255.254
Clase B	*w.x*.0.1	*w.x*.255.254
Clase C	*w.x.y*.1	*w.x.y*.254

2.1.4.10 Direccionamiento IP estático

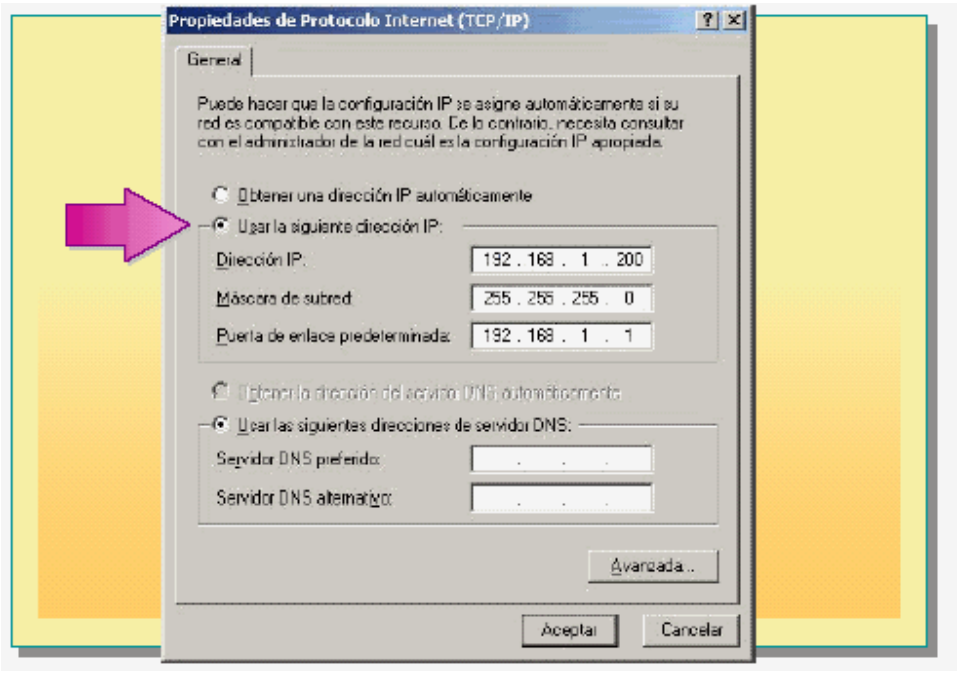

FIGURA 2. 8: DIRECCIONAMIENTO IP ESTÁTICO [12]

El direccionamiento IP estático hace referencia a configurar direcciones IP manualmente. En este método, se utiliza una utilidad proporcionada por Windows 2000 para asignar una dirección IP. Windows 2000 proporciona el cuadro de diálogo Propiedades del protocolo de Internet (TCP/IP) para asignar manualmente una dirección IP a un host o dispositivo TCP/IP.

12 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

2.1.4.11 Direccionamiento IP automático

- **DHCP**

DHCP es un estándar de TCP/IP para simplificar la administración de la configuración y asignación de direcciones IP en una red interconectada. DHCP utiliza un servidor DHCP para gestionar la asignación dinámica de direcciones IP. Los servidores DHCP contienen una base de datos de direcciones IP que pueden asignarse a hosts de la red. Par utilizar DHCP en una red, los hosts deben estar habilitados para usar DHCP. Para habilitar DHCP, debemos hacer clic en Obtener una dirección IP automáticamente, que está seleccionado de forma predeterminada en Windows 2000.

2.1.5 SOFTWARE [13]

Se denomina software (palabra proveniente del inglés, pronunciada "sóft-uer"), a los programas, equipamiento lógico o soporte lógico a todos los componentes intangibles de una computadora, es decir, al conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware). Esto incluye aplicaciones informáticas tales como un procesador de textos, que permite al usuario realizar una tarea, y software de sistema como un sistema operativo, que permite al resto de programas funcionar adecuadamente, facilitando la interacción con los componentes físicos y el resto de aplicaciones.

2.1.5.1 Tipos de software

Si bien esta distinción es, en cierto modo, arbitraria, y, a veces, difusa y confusa, se puede distinguir al software de la siguiente forma:

13 http://es.wikipedia.org/wiki/Computer_software

2.1.5.1.1 Software de programación

Proporciona herramientas para ayudar al programador a escribir programas informáticos y a usar diferentes lenguajes de programación de forma práctica. Incluye entre otros:

- Editores de texto
- Compiladores
- Intérpretes
- Enlazadores
- Depuradores

Los entorno de desarrollo integrados (IDE) agrupan estas herramientas de forma que el programador no necesite introducir múltiples comandos para compilar, interpretar, depurar, etcétera, gracias a que habitualmente cuentan con una interfaz gráfica de usuario (GUI) avanzada.

2.1.5.1.2 Software de aplicación

Permite a los usuarios llevar a cabo una o varias tareas más específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios. Incluye entre otros:

- Aplicaciones de automatización industrial
- Aplicaciones ofimáticas
- Software educativo
- Software médico
- Bases de datos
- Videojuegos

2.1.5.1.3 Software de sistema

Es la parte que permite funcionar al hardware. Su objetivo es aislar tanto como sea posible al programador de aplicaciones de los detalles del computador particular que se use, especialmente de las características físicas de la memoria, dispositivos de comunicaciones, impresoras, pantallas, teclados, etcétera. Incluye entre otros:

- Sistemas operativos
- Controladores de dispositivo
- Herramientas de diagnóstico
- Servidores
- Sistemas de ventanas

2.1.5.2 Sistemas Operativos [14]

El sistema operativo es el programa (o software) más importante de un ordenador. Para que funcionen los otros programas, cada ordenador de uso general debe tener un sistema operativo. Los sistemas operativos realizan tareas básicas, tales como reconocimiento de la conexión del teclado, enviar la información a la pantalla, no perder de vista archivos y directorios en el disco, y controlar los dispositivos periféricos tales como impresoras, escáner, etc.

En sistemas grandes, el sistema operativo tiene incluso mayor responsabilidad y poder, es como un policía de tráfico, se asegura de que los programas y usuarios que están funcionando al mismo tiempo no interfieran entre ellos. El sistema operativo también es responsable de la seguridad, asegurándose de que los usuarios no autorizados no tengan acceso al sistema.

14 http://www.masadelante.com/faq-sistema-operativo.htm

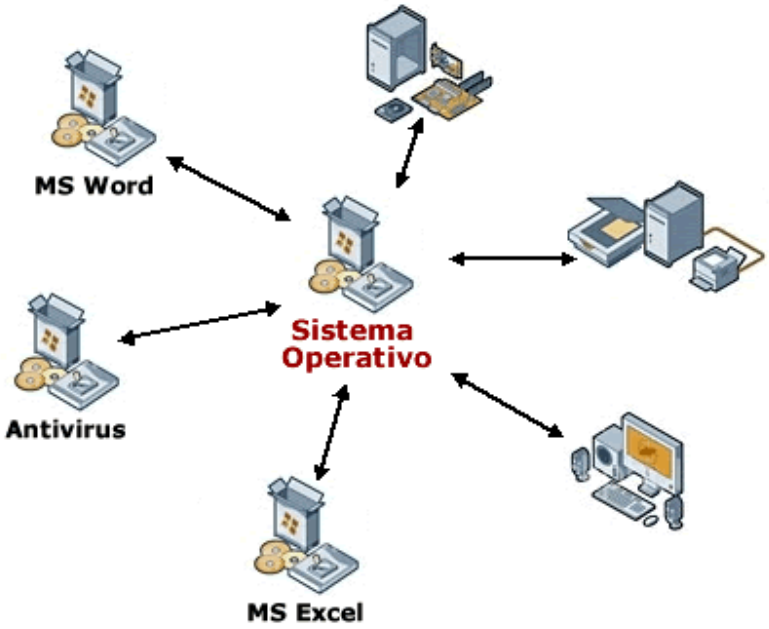

FIGURA 2. 9: SISTEMA OPERATIVO [15]

2.1.5.2.1 Clasificación de los sistemas operativos

Los sistemas operativos pueden ser clasificados de la siguiente forma:

- **Multiusuario**: Permite que dos o más usuarios utilicen sus programas al mismo tiempo. Algunos sistemas operativos permiten a centenares o millares de usuarios al mismo tiempo.
- **Multiprocesador**: soporta el abrir un mismo programa en más de una CPU.
- **Multitarea**: Permite que varios programas se ejecuten al mismo tiempo.
- **Multitramo**: Permite que diversas partes de un solo programa funcionen al mismo tiempo.
- **Tiempo Real**: Responde a las entradas inmediatamente. Los sistemas operativos como DOS y UNIX, no funcionan en tiempo real.

15 http://www.masadelante.com/faq-sistema-operativo.htm

2.1.5.2.2 Funcionamiento de un Sistema Operativo

Los sistemas operativos proporcionan una plataforma de software encima de la cual otros programas, llamados aplicaciones, puedan funcionar. Las aplicaciones se programan para que funcionen encima de un sistema operativo particular, por tanto, la elección del sistema operativo determina en gran medida las aplicaciones que puedes utilizar.

2.1.5.2.3 Ejemplos de Sistemas Operativos

- **WINDOWS**

Es una familia de sistemas operativos desarrollados y comercializados por Microsoft. Existen versiones para hogares, empresas, servidores y dispositivos móviles, como computadores de bolsillo y teléfonos inteligentes. Hay variantes para procesadores de 16, 32 y 64 bits.

Incorpora diversas aplicaciones como Internet Explorer, el Reproductor de Windows Media, Windows Movie Maker, Windows Mail, Windows Messenger, Windows Defender, entre otros.

Desde hace muchos años es el sistema operativo más difundido y usado del mundo, de hecho la mayoría de los programas (tanto comerciales como gratuitos y libres) se desarrolla originalmente para este sistema. Todos los fabricantes del planeta dedicados a equipos basados en procesadores Intel o compatibles con éstos (excepto Apple Inc.) preinstalan Windows en su versión más reciente y todas sus variantes.

Windows Vista es la versión más reciente para computadoras personales, Windows Server 2008 para servidores y Windows Mobile 6.0 en los dispositivos móviles.

- **LINUX** [16]

Linux es un sistema operativo, compatible con Unix. Dos características muy peculiares lo diferencian del resto de sistemas que se puede encontrar en el

16 http://www.linux-es.org/sobre_linux

mercado, la primera, es que es libre, esto significa que no se tiene que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente.

El sistema lo forman el núcleo del sistema (kernel) más un gran número de programas / bibliotecas que hacen posible su utilización. Muchos de estos programas y bibliotecas han sido posibles gracias al proyecto GNU (GNU IS NOT UNIX), por esto razón, muchos llaman a Linux, GNU/Linux, para resaltar que el sistema lo forman tanto el núcleo como gran parte del software producido por el proyecto GNU.

2.2 GNU LINUX [17]

2.2.1 INTRODUCCIÓN AL SISTEMA OPERATIVO LINUX

El proyecto GNU fue iniciado por Richard Stallman con el objetivo de crear un sistema operativo completo libre: el sistema GNU. Richard Stallman publicó un artículo conocido como el "Manifiesto GNU", en el que estableció sus motivaciones para realizar el proyecto GNU, entre las que destaca "retornar al espíritu de cooperación que prevaleció en los tiempos iniciales de la comunidad de usuarios de computadoras". GNU es un acrónimo recursivo que significa "GNU No es Unix".

Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en inglés como copyleft (en clara oposición a copyright), y está contenida en la Licencia General Pública de GNU (GPL).

En 1991, Linus Torvalds empezó a escribir el núcleo Linux y decidió distribuirlo bajo la GPL. Rápidamente, múltiples programadores se unieron a Linus en el desarrollo, colaborando a través de Internet y consiguiendo paulatinamente que

17 http://es.wikipedia.org/wiki/GNU

Linux llegase a ser un núcleo compatible con UNIX. En 1992, el núcleo Linux fue combinado con el sistema GNU, resultando en un sistema operativo libre y completamente funcional. El sistema operativo formado por esta combinación es usualmente conocido como "GNU/Linux" o como una "distribución Linux" y existen diversas variantes.

Desde su primer lanzamiento, Linux ha incrementado su popularidad en el mercado de servidores. Su gran flexibilidad ha permitido que sea utilizado en un rango muy amplio de sistemas de cómputo y arquitecturas: computadoras personales, supercomputadoras, dispositivos portátiles, etc.

Los sistemas Linux funcionan sobre más de 20 diferentes plataformas de hardware, entre ellas las más comunes son las de los sistemas compatibles con PC, computadoras Macintosh, procesadores PowerPC, Sparc y MIPS.

También es frecuente hallar componentes de GNU instalados en un sistema UNIX no libre, en lugar de los programas originales para UNIX. Esto se debe a que muchos de los programas escritos por el proyecto GNU han demostrado ser de mayor calidad que sus versiones equivalentes de UNIX. A menudo, estos componentes se conocen colectivamente como "herramientas GNU". Muchos de los programas GNU han sido también portados a otras plataformas como Microsoft Windows y Mac OS X.

2.2.2 SOFTWARE LIBRE

Software libre es el software que, una vez obtenido, puede ser usado, copiado, estudiado, modificado y redistribuido libremente. El software libre suele estar disponible gratuitamente en Internet, o a precio del costo de la distribución a través de otros medios; sin embargo no es obligatorio que sea así y, aunque conserve su carácter de libre, puede ser vendido comercialmente. Análogamente el software gratuito (denominado usualmente Freeware) incluye en algunas ocasiones el código fuente; sin embargo, este tipo de software no es libre en el mismo sentido que el software libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.

Por lo tanto libertad no significa gratuidad y al contrario tampoco se puede obtener software gratuito sin tener la libertad de ver el código y a su vez se puede usar software libre (free software) para ver su código, pero pagar por su soporte comercial, o por la distribución de las copias de software libre.

2.2.3 CODIGO COMERCIAL

Es aquel que:

a) El autor cobra un precio por el uso del software (licencias)
b) No se puede ceder ni alquilar el software en cuestión
c) El único autorizado a realizar modificaciones al software es el desarrollador de éste. Esto siempre y cuando les sea rentable. Por ejemplo: Cambio de plataforma, mejoras, customizaciones.
d) No se podrá realizar ingeniería inversa para estudiar su comportamiento.

2.2.4 EJEMPLOS DE CÓDIGO COMERCIAL Y LIBRE

Los ejemplos serán tomados mayormente de la empresa Microsoft.

Comercial	Libre
IIS	Apache, thttpd
Exchange	Sendmail, Postfix
Microsoft Office	Open Office, koffice
Internet Explorer	FireFox
Microsoft Outlook	Evolution, Thunderbird, pine, mutt
Decenas de antivirus comerciales	Clamav
TrendMicro antispam	Spamassassin
msn chat, yahoo messenger, trillian	Gaim

TABLA 2.1: CÓDIGO COMERCIAL VS CÓDIGO LIBRE

Existen otros tipos de licencia de aspecto libre, algunas son compatibles con la licencia GNU y otras tienen ciertas restricciones o libertades que la hacen

incompatibles; por ejemplo la licencia tipo Apache permite la distribución de binarios sin su correspondiente código fuente lo que imposibilita en muchos casos el que se pueda conocer las directivas de compilación o parches aplicados a un producto liberado.

Sin embargo esto no significa que una licencia para código libre deba dejar de ser usada o ignorada, muchas tienen elementos válidos a nuestros efectos y de hecho una distribución de Linux comprende no sólo software licenciado bajo GNU-GPL sino que incluye otros tipos de licenciamiento.

2.2.5 TIPOS DE LICENCIA EN SOFTWARE LIBRE

Una licencia es aquella autorización formal con carácter contractual que un autor de un software da a un interesado para ejercer "actos de explotación legales". Pueden existir tantas licencias como acuerdos concretos se den entre el autor y el licenciatario. Desde el punto de vista del software libre, existen distintas variantes del concepto o grupos de licencias:

2.2.5.1 GPL [18]

Las licencias de la mayoría del software están diseñadas para eliminar su libertad de compartir y modificar dicho software. Por contra, la Licencia Pública General de GNU (GPL) está diseñada para garantizar su libertad de compartir y modificar el software. Software libre para garantizar la libertad de sus usuarios. Esta licencia GNU General Public License (GPL) se aplica en la mayoría de los programas realizados por la Free Software Foundation (FSF, Fundación del Software Libre) y en cualquier otro programa en los que los autores quieran aplicarla. Cuando se habla de Software Libre, se habla de libertad, no de precio. La licencia General Public License (GPL) está diseñada para asegurar las libertades de distribuir copias de Software Libre (y cobrar por ese servicio si se desea), asegurar que se recibirá el código fuente del programa o bien podrá conseguirlo si quiere, asegurar que puede modificar el programa o modificar

18 http://es.wikipedia.org/wiki/C%C3%B3digo_libre#Tipos_de_Licencias

algunas de sus piezas para un nuevo programa y para garantizar que puede hacer todas estas cosas.

Por ejemplo, si un individuo recibe copias de un programa, ya sea gratuitamente o no, este a su vez tiene que otorgar a sus clientes todos los derechos que ha adquirido con el programa. Esto quiere decir asegurarse de que sus clientes reciban o puedan recibir el código fuente si lo solicitan, así como mostrarles los términos de la licencia para que conozcan sus derechos.

2.2.5.2 Licencia de Documentación Libre de GNU

La Licencia de Documentación Libre de GNU es una forma de copyleft para ser usada en un manual, libro de texto u otro documento que asegure que todo el mundo tiene la libertad de copiarlo y redistribuirlo, con o sin modificaciones, de modo comercial o no comercial.

2.2.6 EL KERNEL DE LINUX

El kernel de linux es la invención original de Linus Torvalds. Este Kernel es la base del sistema y ha sido ampliamente modificado por una enorme comunidad de personas a lo largo del planeta. De hecho la contribución en código que ha aportado Linus Torvalds es menor al 5% del kernel. Linus Torvalds a veces dice que se siente como si se aprovechara de las demás personas porque él es el que menos ha codificado.

Cierto o falso, es una realidad que fue capaz de crear un kernel muy maleable, muy modificable, que además es una persona que acepta retos, sugerencias y que siempre se mantiene en constante investigación y modernización del kernel.

El kernel básicamente es el sistema que permite administrar (manejar) los recursos del sistema de forma organizada y eficiente: La memoria, el uso de CPU, uso de disco, manejo de espacios de memoria virtual, swap y demás.

2.2.7 DISTRIBUCIONES DE LINUX

Linux es básicamente el kernel del sistema operativo, la base, el que maneja todas las operaciones de entrada/salida y mantiene saludable el manejo de memoria y asignación de recursos del procesador.

Sin embargo, hay que diferenciar bien entre el kernel de Linux, y una distribución de Linux.

Una distribución de Linux es básicamente una colección o conjunto de paquetes, recompilados por una empresa, normalmente comercial en uno o varios cds o dvd los cuales vienen con un proceso de instalación el cual permite entre otras cosas:

- Particionar el disco de la máquina.
- Definir una clave para el usuario de administrador.
- Escoger los paquetes a instalar y configurar ciertos aspectos del sistema como es la zona horaria, el ambiente gráfico, definir direcciones IP, etc.

  Estos paquetes incluidos en una distribución no son solamente GNU, en dependencia de la distribución se usan otros tipos de licenciamientos no comerciales (licencias tipo bsd, apache, X, etc) así como paquetes comerciales (adobe acrobat reader, etc).

El objetivo final de las empresas que realizan las distribuciones es lograr dar actualizaciones frecuentes a su distribución, estas actualizaciones pueden variar siendo algunas gratuitas, otras pagadas.

El tiempo de vida de una distribución también puede variar; así como el soporte técnico (normalmente es pagado) y cursos y certificaciones para la distribución en cuestión.

2.2.7.1 Distribuciones Basadas En Rpm

RPM es el acrónimo creado por redhat para definir un esquema de distribución de paquetes. Significa RedHat Package Manager o Manejador de paquetes de RedHat.

Los RPM fueron en su momento y todavía siguen siendo un paso de avance muy grande para el mundo de Linux, ya que los rpm no sólo incluyen una colección de binarios relativos a un determinado paquete o utilería sino que también incluye archivos de ayuda, de configuración y sobre todo incluye lo que se llama dependencias, esto es, qué otros paquetes rpm requiere este rpm para instalarse.
De esta forma se evita problemas que anteriormente ocurrían y ocurren cuando se instala un paquete que para funcionar correcta o completamente, requiere de otros. Por ejemplo:
El paquete php (php es un lenguaje interpretado que genera código html de amplio uso en estos momentos) tiene entre sus requerimientos el que exista un servidor web (apache) instalado. De esta forma si intentamos instalar el rpm del paquete php, este fallará diciendo que requiere del paquete rpm httpd (apache) para instalar.
Pero esto no es todo, los paquetes rpm permiten además desinstalar completamente una aplicación, pues se mantiene una lista de todos y cada uno de los ficheros de configuración, librerías, binarios, páginas de ayuda y demás que haya instalado un paquete rpm, así de esta forma al borrar un paquete rpm podemos tener la total seguridad de que hemos eliminado todas las referencias y archivos instalados por el rpm. Esto puede sonar natural para una persona que viene del mundo de Windows, pero un sistema de desinstalación en Linux era algo sumamente importante y requerido que no existía antes.
Además los paquetes rpm pueden ser actualizados, los rpm sobrescriben con total tranquilidad sus anteriores versiones instaladas, sustituyendo binarios y páginas manuales así como creando nuevos enlaces que se requieran, pero siempre respetan los archivos de configuración preexistentes, lo que permite actualizar una aplicación con una versión superior sin incurrir en una tarea completa de reconfiguración.
A continuación algunas distribuciones basadas en RPM.

- **Red Hat**

Es una empresa líder en desarrollo, implementación y administración de soluciones Linux y Open source para la Internet. Las aplicaciones de redhat se

orientan a los servidores web seguros. Red Hat fué fundado en 1994 por dos visionarios, Bob Young y Marc Ewing. El código libre es la base de su sistema de negocios. Redhat no sólo es el creador de la idea del rpm algo fundamental que sentó bases para un rápido desarrollo del Linux, sino que son los mantenedores y hospederos de una serie de proyectos y programadores muy conocidos para el mundo del Linux.

La lista de servicios de redhat es grande, pero uno de los fuertes de ellos es:

- Soporte técnico
- Actualizaciones frecuentes
- Certificaciones para trabajar en sus productos

Los productos y servicios de redhat tienen un costo. Pero el sistema operativo y paquetes incluidos en la distribución son distribuidos con el código fuente de éstos.

- **SUSE**

SUSE LINUX se cataloga como líder internacional y proveedor de soluciones en sistemas operativos de código abierto. La larga experiencia de Suse en linux y además su enorme cantidad de personas dedicadas a desarrollar en código abierto han contribuido indudablemente en reconocer a Suse como una de las soluciones de linux más completas disponibles al momento. Suse Linux fue adquirido por Novell, Inc en Noviembre del 2003.

- **FEDORA**

Fedora se convirtió desde inicios del siglo 21 en una distribución auspiciada por redhat, un sandbox, o caja de arena, donde redhat prueba y prepara los paquetes que serán implementados para sus distribuciones comercialmente soportadas (RHEL). Fedora básicamente contiene una serie de paquetes de última generación que son planteados, propuestos en sus distribuciones para que los interesados puedan probarlos y reportar problemas.

Fedora se compromete a liberar un nuevo core (se refiere a sus distribuciones, core1, core2, core3, core4, etc) cada 10 a 12 meses, y se compromete a

actualizar solamente la versión recién liberada y la anterior a la recién. Por ejemplo, la versión actual es Fedora core7, por lo tanto actualizan el core7 y el core6, Core4 y Core5 ya no son soportados ni actualizados por Fedora.

Si se mira estas dos opciones de redhat (RHEL y fedora) no se tiene mucha alternativa puesto que redhat distribuye su versión empresarial pero cobra por las actualizaciones y por usar su logo; mientras Fedora es sólo un juguete para desarrolladores y estudiantes.

Ante la necesidad de las empresas de un servicio estable, con actualizaciones por largos periodos de tiempo y que no pueden o no quieren pagar por el servicio de actualizaciones de redhat, surgen los denominados Clones de Red Hat.

- **CLONES DE RED HAT** [19]

Estos han surgido, gracias al código GNU y otros códigos no comerciales, son alternativas gratuitas o menos costosas para implementación y mantenimiento de servidores.

- **CENTOS:**

  Centos (acrónimo de Community Enterprise Operating System) es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de RHEL.

  Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia Pública GNU. Los desarrolladores de Centos usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat.

[19] http://es.wikipedia.org/w/index.php?title=Lineox&action=edit&redlink=1

- **Lineox Enterprise Linux**

  Lineox Enterprise Linux es el producto de una empresa finlandesa del mismo nombre, y al contrario de Centos, se enorgullecen de haber modificado las fuentes de RHEL para producir su distribución. Como resultado, en ella se incluyen paquetes de RHEL Advanced Server (AS), Entry/Mid Server (ES), Workstation (WS), Red Hat Cluster Suite, Red Hat Developer Suite, y otros como OpenOffice.

  Lineox ofrece un sistema de actualización de paquetes para su Enterprise Linux, con los lanzamientos oficiales de correcciones y actualizaciones de Red Hat para RHEL, basado en un sistema de activación, como el servicio de actutalización de Red Hat Network. Por el momento la empresa cobra una cuota anual por sus actulizaciones.

- **White Box Enterprise Linux**

  White Box Enterprise Linux es una distribución Linux gratis, alternativa a Red Hat Enterprise Linux, principalmente financiada por la Beauregard Parish Library (Biblioteca de la Parroquia de Beauregard) en Luisiana. White Box apunta a ser 100% compatible con los paquetes binarios de Red Hat Enterprise Linux. Esta distribución se deriva del software libre disponible hecho por Red Hat, pero no es producido, mantenido o soportado por Red Hat. Específicamente, este producto es una bifurcación del código fuente de la versión 3 de Red Hat Linux bajo los términos y condiciones de las licencias libres de software bajo las cuales se distribuye.

2.2.7.2 Distribuciones No Basadas En Rpm

- **DEBIAN**

El proyecto Debian es una sociedad de personas que han hecho causa común para crear un sistema operativo gratuito. Este SO se llama Debian GNU/Linux o simplemente Debian. Los sistemas Debian actualmente usan el Kernel de Linux.

Debian se caracteriza por ser totalmente gratuito, sin organizaciones que los mantengan y con una amplia cobertura de plataformas, tanto populares como ya obsoletas o muy nuevas.

Entre las dificultades que Debian está enfrentando ahora es una falta de soporte comercial (requerido por muchos clientes) así como una gran lentitud en liberar nuevas versiones y nuevas actualizaciones, así como peleas internas dentro del grupo de desarrolladores.

- **GENTOO**

Es una distribución que, aparte de ser gratuita y libre, es una distribución que puede adecuarse completamente a la máquina en que se instala. Esto es, a los efectos de una instalación se pueden mandar a instalar solamente los paquetes que se requiere, ni más ni menos, y estos paquetes bajarlos del Internet, de su sitio web y recompilarlos de acuerdo al hardware o plataforma disponible.
Gentoo además no tiene distribuciones propiamente dichas, se puede instalar desde cualquier cd de arranque de Gentoo, que él mismo se encargará de bajar el código fuente de todos los paquetes requeridos desde la Internet, y este código por supuesto será de la última versión disponible en Internet.

2.3 INTRODUCCIÓN A LOS SERVICIOS EN LINUX [20]

Linux tiene disponible todos los servicios habituales en una red:

- DNS
- Correo electrónico.
- Servicios de internet.
- Servicio de ficheros e impresión.
- Bases de datos
- Utilidades necesarias para mantener el nivel de seguridad requerido.

Pero además hay que reseñar que cada servicio funciona sin afectar al resto de los servicios. Se puede modificar la dirección IP de un equipo, las rutas, añadir, parar o reiniciar un servicio en concreto sin que el resto de los servicios se vean afectados. Sólo es necesario detener el equipo para realizar operaciones con el hardware, como añadir un disco duro, o utilizar un nuevo núcleo. No se tendrá,

20 http://www.iec.csic.es/CRIPTonOMICon/linux/servicios.html

pues, la necesidad de tener que ser uno mismo el atacante del propio sistema, a diferencia de lo que ocurre en otros sistemas operativos.

2.4 DNS [21]

2.4.1 INTRODUCCIÓN A DNS

DNS (acrónimo de Domain Name System) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio.

El DNS nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección IP.

Los servidores DNS utilizan TCP y UDP en el puerto 53 para responder las consultas.

21 http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

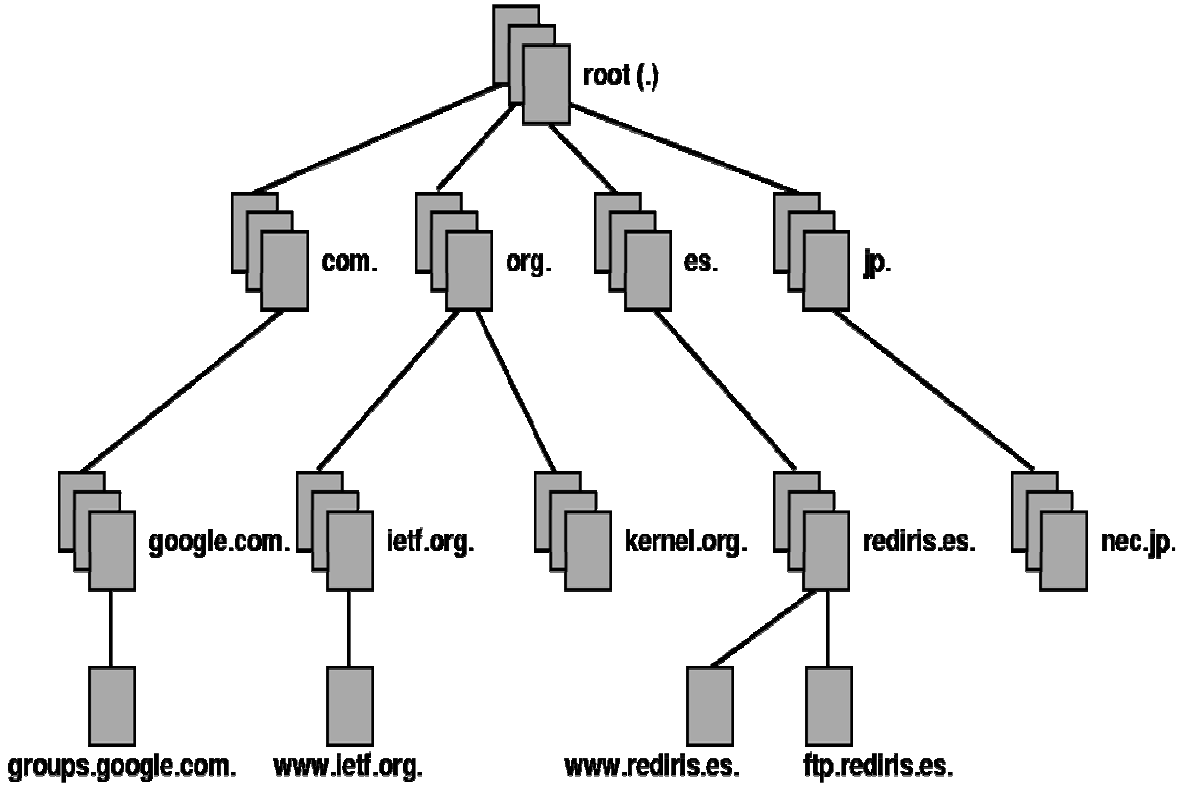

FIGURA 2. 10: JERARQUÍA DE DNS [22]

2.4.2 COMPONENTES DE UN DNS

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

2.4.2.1 Clientes Dns

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres.

Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

2.4.2.2 Servidores DNS

Son servicios que contestan las consultas realizadas por los clientes DNS.

22 http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

2.4.3 TIPOS DE DNS

2.4.3.1 DNS DE CACHE

Los DNS de caché son aquellos que no contienen zonas. Por zonas se entienden básicamente los records que componen un dominio, al no contener zonas (dominios) estos tienen que preguntar a otros.

Estos DNS son importantes, son los que se usa normalmente para preguntar por dominios en internet, por ejemplo, cuando se pregunta por www.google.com no se hace la pregunta a los DNS que tiene listado el dominio google.com sino que se pregunta a unos DNS definidos por el administrador de la red o por el proveedor de internet.

Estos DNS a su vez, verifican con los root servers, cuáles son los DNS que google tiene listado para su dominio google.com y entonces acudirán prestos a preguntarle a uno de esos DNS sobre el sitio www.google.com.

Por supuesto, si uno de esos DNS estuviera caído, el DNS de caché ya tiene una lista de los DNS de google y por lo tanto le procederá a preguntar a otro y a otro, hasta alcanzar la respuesta.

Los DNS de caché tienen una peculiaridad, es que no usan disco, básicamente estos almacenan toda la información que se ha consultado, con el objetivo de que si se pregunta de nuevo, estos no tengan que salir a buscarla, sino que inmediatamente la obtienen de su caché. Por esta razón se llaman DNS de caché, tienden a usar toda la memoria disponible, pero realmente no consumen mucha memoria, porque los tamaños de las respuestas son pequeños.

Los records cacheados son refrescados cada vez que el tiempo de vida de los records se cumple, este valor se llama TTL. Un TTL adecuado puede ser 2 horas (7200segundos) pero algunas personas gustan de usar un día (86400segundos). El problema de un TTL de un día es que si se decide a cambiar de IP, no se podrá hacerlo rápidamente pues algunos DNS de caché tendrán una respuesta cacheada por un día y durará un día el cambio de IP.

Es por esta razón que algunos proveedores mencionan que el cambio de DNS toma 24 horas o más, es porque el TTL puede ser alto y al estar cacheado por cientos o miles de DNS alrededor del mundo, estos no volverán a preguntar por ese record en un día ya que considerarán válida una respuesta mientras el TTL no sea cero.

2.4.3.2 DNS DE ZONA

Son los que contienen información específica sobre una zona. Cuando uno compra un dominio, básicamente le define los DNS de zona que manejarán este dominio, una vez comprado el dominio, se tiene que inmediatamente crear en esos DNS definidos por uno las zonas del dominio.
Dentro de los DNS de zona se puede tener.

2.2.3.2.1 DNS Maestro

Obtiene los datos del dominio a partir de un fichero que se encuenra hospedado en el mismo servidor.

2.2.3.2.1 DNS Esclavo

Al iniciar obtiene los datos del dominio a través de un servidor Maestro, realizando un proceso denominado transferencia de zona.
Una de las principales razones para tener al menos tres servidores para cada zona es permitir que la información de la zona este disponible siempre y de forma confiable hacia los clientes DNS a través de internet cuando un servidor DNS de dicha zona falle, no este disponible y/o este inalcanzable.

2.4.4 ZONAS DE AUTORIDAD

Permiten al servidor Maestro configurar la información de una zona. Cada zona de autoridad abarca al menos un dominio.

La información de cada Zona de Autoridad es almacenada de forma local en un fichero en el servidor DNS. Este fichero puede incluir varios tipos de records o registros.

Los records más conocidos son:

- **SOA:** Registro de inicio de autoridad que especifica el servidor DNS Maestro que proporcionará la información con autoridad acerca de un dominio de internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros del tiempo para la zona.
- **A(Adress):** Es quizá el record más usado, y el más fácil de entender, definitivamente define dado un nombre, su dirección IP. Es básicamente el concepto fundamental de los DNS.
- **MX (Mail Exchanger):** Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio así como la prioridad entre éstos.
- **CNAME (Canonical Name):** Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtiene los subdominios y registros DNS del dominio original.
- **PTR (Pointer):** Registro de apuntador que resuelve direcciones IPv4 hacia el nombre de anfitriones. Es decir hace lo contrario al record A. Se utiliza en zonas de Resolución Inversa.

2.4.5 ZONAS DE REENVÍO

Devuelven direcciones IP para las búsquedas hechas para nombres FQDN (Fully Qualified Domain Name).

En el caso de dominios públicos, la responsabilidad de que exista una zona de autoridad para cada zona de reenvío corresponde a la autoridad misma del dominio, es decir, y por lo general, quien está registrado como zona de autoridad del dominio tras consultar una base de datos WHOIS. Quienes compran dominios a través de un NIC (por ejemplo www.nic.mx) son quienes se hacen cargo del

reenvío, ya sea a través de su propio servidor DNS o bien a travéz de los servidores de su ISP.

Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un NIC como requisito legal a utilizarlo y poder propagarlo a través de internet.

2.4.6 ZONA DE RESOLUCIÓN INVERSA

Devuelve nombres FQDN (Fully Qualified Domain Name) para las búsquedas hechas para direcciones IP. En el caso de segmentos de red públicos, la responsabilidad de que exista una zona de autoridad para cada Zona de Resolución Inversa corresponde a la autoridad misma del segmento, es decir, y por lo general, quien esté registrado como autoridad del segmento tras consultar una base de datos WHOIS.

Los grandes ISP, y en algunos casos algunas empresas, son quienes se hacen cargo de las Zonas de Resolución Inversa.

En conclusión los DNS son la base del internet, y su incomprensión es lo que acarrea un mal uso de ellos y normalmente son el servicio que genera la mayor cantidad de quejas por parte de los usuarios. Muchas veces cuando una página web no se abre o da timeout, cuando el correo electrónico no funciona son síntomas de que un DNS está dando respuestas malas.

2.5 CORREO ELECTRÓNICO [23]

El nacimiento del correo electrónico (email) ocurrió a principios de los años 60. El buzón era un archivo en el directorio principal de un usuario al cual sólo el mismo podía acceder. Las aplicaciones de correo primitivas anexaban nuevos mensajes de texto a la parte inferior de un archivo, y el usuario tenía que buscar a lo largo del archivo en constante crecimiento para encontrar un mensaje particular. Este sistema sólo era capaz de enviar mensajes a usuarios en el mismo sistema.

23 http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

La primera transferencia verdadera de correo electrónico en la red se llevó a cabo en 1971 cuando un ingeniero de computación llamado Ray Tomlinson envió un mensaje de prueba entre dos máquinas a través de ARPANET — el precursor de Internet. La comunicación a través de correo electrónico rápidamente se volvió muy popular, pasando a formar el 75 por ciento del tráfico de ARPANET en menos de dos años.

Hoy día, los sistemas de correo electrónico basados en protocolos de red estandarizados han evolucionado para convertirse en uno de los servicios más usados de Internet. Red Hat ofrece muchas aplicaciones avanzadas para servir y acceder al correo electrónico.

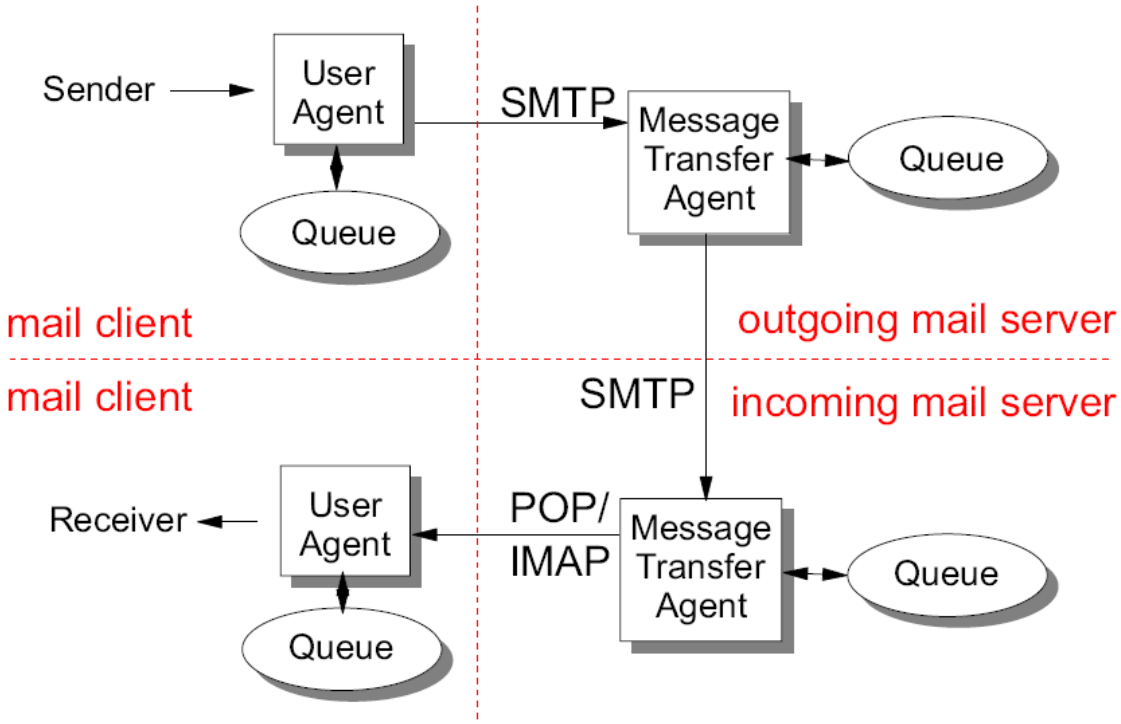

FIGURA 2. 11: MODELO DE E-MAIL [24]

Los costos de los servicios de Correo Electrónico, varían dependiendo del tipo de plataforma así como de los servicios adicionales que éstos requieran.

24 http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

En el caso de la utilización de software comercial el costo variará de manera significativa con respecto al software libre debido a la necesidad de adquirir derechos de licencia.

Para un servidor de correo electrónico, el presupuesto variará básicamente dependiendo del número de cuentas de usuario. Adicional a esto se suma el costo por servicios de Antispam, Antivirus, Webmail, Actualización y Mantenimiento.

El siguiente cuadro detalla la variación de precios entre un sistema y otro.

PRODUCTO	EMPRESA COMERCIAL	PLATAFORMA	COSTO PARA 50 CUENTAS DE CORREO
EXCHANGE	MICROSOFT	WINDOWS	1300 $
LOTUS SERVER	IBM	WINDOWS 2003	N/A
MAIL SERVER AVG	GRISOFT	LINUX/WINDOWS	700 $
AVIRA MAILSERVER	AVIRA	LINUX	800$

TABLA 2.2: COSTO DE PRODUCTOS DE CORREO ELECTRÓNICO

2.5.1 PROTOCOLOS DE CORREO ELECTRÓNICO

Hoy día, el correo electrónico es entregado usando una arquitectura cliente/servidor. Un mensaje de correo electrónico es creado usando un programa de correo cliente. Este programa luego envía el mensaje a un servidor. El servidor luego lo redirige al servidor de correo del recipiente y allí se le suministra al cliente de correo del recipiente.

Para permitir todo este proceso, existe una variedad de protocolos de red estándar que permiten que diferentes máquinas, a menudo ejecutando sistemas operativos diferentes y usando diferentes programas de correo, envíen y reciban correo electrónico o email.

2.5.2 PROTOCOLOS DE TRANSPORTE DE CORREO

2.5.2.1 Protocolo SMTP

La entrega de correo desde una aplicación cliente a un servidor, y desde un servidor origen al servidor destino es manejada por el Protocolo simple de transferencia de correo (Simple Mail Transfer Protocol o SMTP).

SMTP es un protocolo estándar de Internet del Nivel de Aplicación utilizado para la transmisión de correo electrónico a través de una conexión TCP/IP. Este es de hecho el único protocolo utilizado para la transmisión de correo electrónico a través de Internet. Es un protocolo basado sobre texto y relativamente simple donde se especifican uno o más destinatarios en un mensaje que es transferido.

El objetivo principal del protocolo simple de transferencia de correo, SMTP, es transmitir correo entre servidores de correo. Sin embargo, es crítico para los clientes de correo también. Para poder enviar correo, el cliente envía el mensaje a un servidor de correo saliente, el cual luego contacta al servidor de correo de destino para la entrega. Por esta razón, es necesario especificar un servidor SMTP cuando se esté configurando un cliente de correo.

Para determinar el servidor SMTP para un dominio dado, se utilizan los registros MX (Mail Exchanger) en la Zona de Autoridad correspondiente a ese mismo dominio contestado por un Servidor DNS. Después de establecerse una conexión entre el remitente (el cliente) y el destinatario (el servidor), se inicia una sesión SMTP, ejemplificada a continuación:

```
Cliente: $ telnet 127.0.0.1 25
Servidor: Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sat, 18 Mar
2006 16:02:27
-0600
Cliente: HELO localhost.localdomain
```

Servidor: 250 nombre.dominio Hello localhost.localdomain [127.0.0.1], pleased to
meet you

Cliente: MAIL FROM:<fulano@localhost.localdomain>
Servidor: 250 2.1.0 <fulano@localhost.localdomain>... Sender ok
Cliente: RCPT TO:<root@localhost.localdomain>
Servidor: 250 2.1.5 <root@localhost.localdomain>... Recipient ok
Cliente: DATA
Servidor: 354 Enter mail, end with "." on a line by itself
Cliente: Subject: Mensaje de prueba
From: fulano@localhost.localdomain
To: root@localhost.localdomain
Hola. Este es un mensaje de prueba.
Adios.
.
Servidor: 250 2.0.0 k2IM2RjA003987 Message accepted for delivery
Cliente: QUIT

Servidor: 221 2.0.0 nombre.dominio closing connection
Servidor: Connection closed by foreign host.

Una desventaja sobre el protocolo SMTP es que no requiere autenticación. Esto permite que cualquiera en la Internet pueda enviar correo a cualquier otra persona o a grandes grupos de personas. Esta característica de SMTP es lo que hace posible el correo basura o spam. Los servidores SMTP modernos intentan minimizar este comportamiento permitiendo que sólo los hosts conocidos accedan al servidor SMTP. Los servidores que no ponen estas restricciones son llamados servidores Open Relay.

2.5.3 PROTOCOLOS DE ACCESO A CORREO

Existen dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el Post Office Protocol (POP) y el Internet Message Access Protocol (IMAP). A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña.

2.5.3.1 POP 3

Es un protocolo estándar de Internet del Nivel de Aplicación que recupera el correo electrónico de un servidor remoto a través de una conexión TCP/IP desde un cliente local. El diseño de POP3 y sus predecesores es permitir a los usuarios recuperar el correo electrónico al estar conectado hacia una red y manipular los mensajes recuperados sin necesidad de permanecer conectados. A pesar de que muchos clientes de correo electrónico incluyen soporte para dejar el correo en el servidor, todos los clientes de POP3 recuperan todos los mensajes y los almacenan como mensajes nuevos en la computadora o anfitrión utilizado por el usuario, eliminan los mensajes en el servidor y terminan la conexión.
Ejemplo de POP:

```
$ telnet pop.abc.com 110
+OK POP3 pop.abc.com v6.50 server ready
user fred
+OK User name accepted, password please
pass wilma
+OK Maildrop open, 1 messages
list
+OK Mailbox scan listing follows
1 3239
.
retr 1
+OK 3239 octets
Status: U
```

```
From: Ed Beaver <ed@xyz.com>
To: Fred Flintstone <fred@abc.com>
Subject: Test Message
Hi there, Fred.
.
dele 1
+OK message deleted
quit
+OK Sayonara
```

2.5.3.2 IMAP

(Acrónimo inglés de Internet Message Access Protocol) es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

IMAP es utilizado frecuentemente en redes grandes; por ejemplo los sistemas de correo de un campus. IMAP permite a los usuarios acceder a los nuevos mensajes instantáneamente en sus computadoras, ya que el correo está almacenado en la red. Con POP3 los usuarios tendrían que descargar el email a sus computadoras o accederlo vía web. Ambos métodos toman más tiempo de lo que le tomaría a IMAP, y se tiene que descargar el email nuevo o refrescar la página para ver los nuevos mensajes.

IMAP y POP3 (Post Office Protocol versión 3) son los dos protocolos que prevalecen en la obtención de correo electrónico. Todos los servidores y clientes de email están virtualmente soportados por ambos.

2.5.3.3 DOVECOT

Dovecot es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y está diseñado teniendo como principal objetivo la seguridad.

Dovecot, es el paquete de CentOS que se encarga de servir los protocolos de:

- imap
- imaps
- pop3
- pop3s

Los más usados son el pop3 y el IMAP.

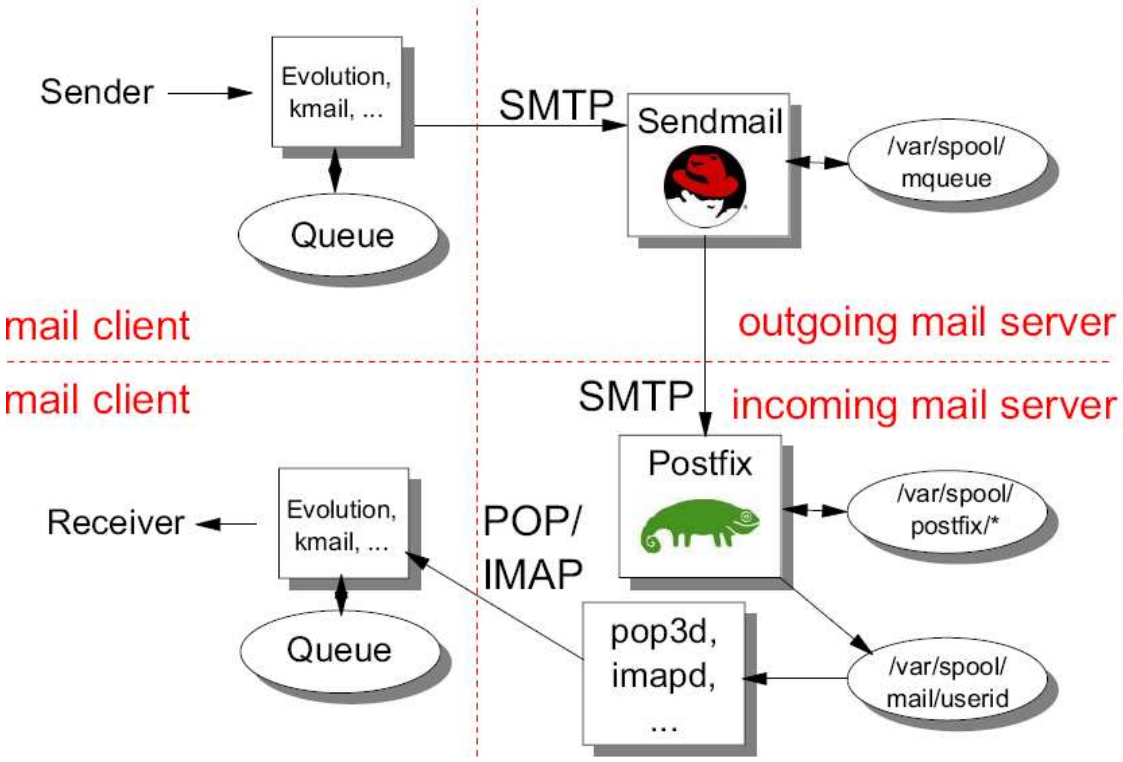

FIGURA 2. 12: IMPLEMENTACIÓN DE E-MAIL SOBRE LINUX [25]

2.5.4 CLASIFICACIÓN DE LOS PROGRAMAS DE CORREO

Todas las aplicaciones de email caen en al menos una de tres clasificaciones. Cada clasificación juega un papel específico en el proceso de mover y administrar los mensajes de correo. Mientras que la mayoría de los usuarios sólo están al

25 http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

tanto del programa de correo específico que usan para recibir o enviar mensajes, cada uno es importante para asegurar que el mensaje llegue a su destino correcto.

2.5.4.1 Agente De Transferencia De Correo

Un Agente de transferencia de correo (MTA) transfiere mensajes de correo electrónico entre hosts usando SMTP. Un mensaje puede envolver a muchos MTAs a medida que este se mueve hasta llegar a su destino.
Aunque la entrega de mensajes entre máquinas puede parecer bien simple, el proceso completo de decidir si un MTA particular puede o debería aceptar un mensaje para ser repartido, es más bien complicado. Además, debido a los problemas de spam, el uso de un MTA particular está usualmente restringido por la configuración del MTA o por la configuración de acceso a la red en la que reside el MTA.
Entre estos tenemos:
Centos Linux incluye dos tipos primarios de MTAs, Sendmail y Postfix.

2.5.4.1.1 Sendmail

El propósito principal de Sendmail, como cualquier otro MTA, es el de transferir correo de forma segura entre hosts, usualmente usando el protocolo SMTP. Sin embargo, Sendmail es altamente configurable, permitiendo el control sobre casi cada aspecto del manejo de correos, incluyendo el protocolo utilizado.
Actualmente es el más popular agente de transporte de correo (MTA o Mail Transport Agent), responsable quizá de poco más del 70% del correo electrónico del mundo. Aunque por largo tiempo se le ha criticado por muchos incidentes de seguridad, lo cierto es que éstos siempre han sido resueltos en pocas horas.
Es por esto que muchos administradores de sistemas seleccionan Sendmail como su MTA debido a su poder y escalabilidad.

❖ *LOGS DEL SENDMAIL*

En general todos los logs que tienen relación con la mensajería se guardan en /var/log/maillog.
Aquí un ejemplo de logs de un servidor de correo Sendmail:

Nov 25 17:00:32 srv4 sm-acceptingconnections[30106]: jAPM0In6030009: to=<marite@qoyllur-tours.com>, delay=00:00:13, xdelay=00:00:00, mailer=virthostmail, pri=179495, relay=qoyllur-tours.com, dsn=2.0.0, stat=Sent (jAPM0W5c030119 Message accepted for delivery)

Nov 25 17:00:32 srv4 virthostmail[30128]: Chrooting to /home/virtual/site307/fstNov 25 17:00:32 srv4 sendmail[30124]: jAPM0W5c030119: to=<marite@qoyllur-tours.com>, delay=00:00:00, xdelay=00:00:00, mailer=local, pri=89913, dsn=2.0.0, stat=Sent
Nov 25 17:00:32 srv4 sendmail[30128]: jAPM0W7U030128: from=<webmaster@hotmail.com>, size=75995, class=0, nrcpts=4, msgid=<72f0e6ada9.01a51@hotmail.com>, proto=ESMTP, relay=root@localhost
Nov 25 17:00:32 srv4 sm-acceptingconnections[30106]: jAPM0NdW030038: to=<lcampoverde-import@ordoviv.com>,<dvivar@ordoviv.com>,<fgalarza@ordoviv.com>,<info@ordoviv.com>, delay=00:00:08, xdelay=00:00:00, mailer=virthostmail, pri=285770, relay=ordoviv.com, dsn=2.0.0, stat=Sent (jAPM0W7U030128 Message accepted for delivery)

Nov 25 17:00:32 srv4 sendmail[30130]: jAPM0W7U030128: to=<lcampoverde-import@ordoviv.com>, delay=00:00:00, xdelay=00:00:00, mailer=local, pri=376148, dsn=2.0.0, stat=Sent

2.5.4.1.2 POSTFIX [26]

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

Postfix es el agente de transporte por omisión en diversas distribuciones de Linux y en las dos últimas versiones del Mac OS X (Panther y Tiger).

2.5.4.1.3 QMAIL [27]

Qmail fue desarrollado por Daniel J. Bernstein entre 1995-98, en la búsqueda de una mejor alternativa a Sendmail, y otros MTAs. Bernstein tenia en mente una arquitectura simple, pues mientras más simple el diseño, más seguro, estable y eficiente sería su operación. El programa ha demostrado ser absolutamente funcional en este sentido.

qmail es un servidor de correo electrónico (SMTP) hecho para Unix. Utiliza el formato maildir para almacenar mensajes (un archivo por mensaje), eliminando varios problemas asociados al manejo del formato mbox.

2.5.4.2 Agente De Entrega De Correos

Un MTA invoca a un Agente de entrega de correos (MDA) para archivar el correo entrante en el buzón de correo del usuario. En muchos casos, el MDA es en realidad un Agente de entrega local (LDA), tal como mail o Procmail.

Cualquier programa que maneje la entrega de mensajes hasta el punto en que puede ser leído por una aplicación cliente de correos se puede considerar un MDA. Por esta razón, algunos MTAs (tales como Sendmail y Postfix) pueden

26 http://es.wikipedia.org/wiki/Postfix

27 http://es.wikipedia.org/wiki/Qmail

tener el papel de un MDA cuando ellos anexan nuevos mensajes de correo al archivo spool de correo del usuario. En general, los MDAs no transportan mensajes entre sistemas tampoco proporcionan una interfaz de usuario; los MDAs distribuyen y clasifican mensajes en la máquina local para que lo acceda una aplicación cliente de correo.

2.5.4.3 Agente De Usuario De Correos

Un agente de usuario de correo (MUA) es sinónimo con una aplicación cliente de correo. Un MUA es un programa que, al menos, permite a los usuarios leer y redactar mensajes de correo. Muchos MUAs son capaces de recuperar mensajes a través de los protocolos POP o IMAP, configurando los buzones de correo para almacenar mensajes y enviando los mensajes salientes a un MTA.
Los MUAs pueden ser de interfaz gráfica, tal como Thunderbird o Outlook.

2.5.5 CORREO BASURA [28]

Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de correo basura incluyen grupos de noticias usenet, motores de búsqueda, wikis, foros, blogs, también a través de popups y todo tipo de imagenes y textos en la web. El correo basura también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes, etc.
El correo electrónico es, con diferencia, el medio más común de spamming en internet. Involucra enviar mensajes idénticos o casi idénticos a un gran número de direcciones. A diferencia de los correos electrónicos comerciales legítimos, el

28 http://es.wikipedia.org/wiki/Spam

spam generalmente es enviado sin el permiso explícito de los receptores, y frecuentemente contiene varios trucos para sortear los filtros de spam. El receptor de spam puede verse perjudicado al tener que invertir tiempo en eliminar mensajes de su cuenta de correo electrónico; sin embargo, diferentes sistemas de correo en línea (Windows Live, Yahoo! y Gmail) han incrementado sustancialmente la capacidad de almacenamiento de las respectivas cuentas (Yahoo! Correo tiene una capacidad de almacenamiento ilimitada). Por otro lado, la recepción de estos correos no deseados, genera una utilización del ancho de banda de acceso a internet sin ninguna necesidad por parte del usuario, que es quien paga por el servicio.

2.5.5.1 Técnicas de Correo Basura

2.5.5.1.1 Obtención De Dirección De Correos

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

- Las propias páginas web, que con frecuencia contienen la dirección de su creador, o de sus visitantes.
- Compra de bases de datos de direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).
- Entrada ilegal en servidores.
- Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales. Por ejemplo, para el dominio wikipedia.org, probar info@wikipedia.org, webmaster@wikipedia.org, staff@wikipedia.org, etc.

2.5.5.1.2 A través de Troyanos y Ordenadores Zombies

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

2.5.5.1.3 Servidores Mal Configurados

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

2.5.6 DETENER EL CORREO BASURA

2.5.6.1 Mailscanner [29]

MailScanner es un robusto servicio que se encarga de examinar el correo electrónico e identificar y etiquetar correo masivo no solicitado (Spam), así como también los fraudes electrónicos (Phishing). Combinado con un software antivirus y un antispam resultan una de las soluciones más robustas para obtener un correo seguro pues asegura la protección contra correo masivo no solicitado, fraudes electrónicos, virus, gusanos y troyanos desde el servidor de correo electrónico.

29 http://www.mailscanner.org

El servicio de MailScanner, para su buen funcionamiento, requiere de que tengamos instalado las herramientas antivirus y antispam necesarias para que él realice las revisiones correspondientes a los correos.

2.5.6.2 AMAVIS [30]

Amavis es un servicio similar a MailScanner capaz de tomar el correo y suministrárselo a otro programa para su procesamiento. Cuando el servidor de correo recibe algún mensaje, se lo hace llegar al servidor de AMaViS, que, en función de como haya sido configurado, le pasará el mensaje a uno o varios programas antivirus, que habrán de adquirirse independientemente, y opcionalmente a programas detectores de correo basura o “spam”. Estos procesan el mensaje y notifican a AMaViS si han encontrado virus o spam. En esos casos, AMaViS bien rechazará el mensaje devolviéndolo a su origen, lo entregará con un aviso, o lo mantendrá en un estado de cuarentena. En nuestro caso, hay que modificar el sendmail para que mande los mensajes por un socket al AMaViS, cuya versión para sendmail se llama milter, y configurar este en función de lo que pretendamos hacer. Por ultimo, se arrancan ambos servicios, y ya tenemos el sistema funcionando. Se puede jugar con las distintas opciones que nos ofrece el amavis para notificar acerca de los viruses, medidas a tomar, etc. Como comentario final, existe una versión de amavis, llamada amavis-ng, que está escrita en perl de forma modular, y que permitiría escribir un módulo propio para utilizar el antivirus que nosotros queramos, aunque se encuentra en fase de desarrollo todavía. También hay que tener en cuenta que en el propio AMaViS tiene sus fallos y limitaciones, particularmente se vuelve bastante lento en situaciones de mucha carga, es decir, cuando el numero de mensajes a procesar es muy elevado

30 http: http://interno.ehas.org/intranet/organizacion/administracion-de-sistemas/AMaViS

2.5.6.3 Clamav [31]

Es el antivirus por excelencia de Linux, es un poderoso y robusto motor, con licenciamiento libre, para la detección de gusanos, troyanos y virus, un componente para añadir a la biblioteca de filtros de correo de Sendmail, que se encarga de hacer pasar todo el correo entrante a través del ClamAV. Clamav verifica el correo electrónico durante la conexión con el servidor de correo que remite este ultimo, y lo rechaza automáticamente si éste incluye algún gusanos, troyanos o virus.

2.5.6.4 Spamassassin [32]

SpamAssassin es un filtro de correo para identificar Spam 33. Se trata de un filtro de correo electrónico inteligente que utiliza una amplia gama de pruebas para identificar correo electrónico no solicitado, más conocido como Spam. Estas pruebas se aplican a los encabezados de los correos y al contenido del correo electrónico mediante el uso de avanzados métodos estadísticos. Además, SpamAssassin tiene una arquitectura modular que permite adaptar rápidamente a las nuevas tecnologías que se ejercen contra el spam y está diseñado para su fácil integración en prácticamente cualquier sistema de correo electrónico.

2.5.7 WEBMAIL

Es una aplicación programada mediante algún lenguaje de programación dinámica vía web, que nos permita revisar el buzón de correos.
La aplicación lo que hace es conectarse al servicio de POP3 o de IMAP para leer los correos que se almacenan en el buzón.
El webmail permite listar, desplegar y borrar vía un navegador web los correos almacenados en el servidor remoto. Los correos pueden ser consultados

31 http:www.clamav.net

32 http:www.spamassassin.apache.org

33 Término que se refiere al todo el correo que no ha sido solicitado

posteriormente desde otro computador conectado a la misma red (por ejemplo Internet) y que disponga de un navegador web.

2.5.7.1 SQUIRRELMAIL [34]

Es uno de los más populares Webmail que existen, es un interesante, extensible, funcional y robusto sustento lógico para correo y que permite acceder al usuario a su correo electrónico desde el navegador de su predilección.
SquirrelMail está escrito en PHP y cumple con los estándares como correo a través de interfaz HTTP. Incluye su propio soporte para los protocolos IMAP y SMTP. Además todas las páginas se muestran con HTML 4.0 sin la necesidad de JavaScript para una máxima compatibilidad con cualquier navegador.
SquirrelMail incluye toda la funcionalidad deseada para un cliente de correo como un robusto soporte MIME, libreta de direcciones y administración de carpetas.

2.6 PROXY [35]

Un servidor proxy es un tipo de buffer (memoria intermedia) entre un ordenador y los recursos de Internet a los que se está accediendo. Éstos acumulan y guardan los archivos que más a menudo son solicitados por los usuarios de Internet en una base de datos especial llamada cache.
Por esta razón los servidores proxy pueden incrementar la velocidad de tu conexión a Internet. La cache de un servidor proxy puede contener la información que se necesita cuando se la solicita, haciendo posible que el proxy lo sirva inmediatamente. Por lo que el incremento de rendimiento puede ser muy alto.
Los Servidores Intermediarios (Proxies) generalmente trabajan simultáneamente como muro cortafuegos operando en el Nivel de Red, actuando como filtro de paquetes, también funcionan como caché de contenido de Red (principalmente HTTP), proporcionando a los clientes un caché de páginas y ficheros disponibles

34 http:www.squirrelmail.org

35 http://sindominio.net/~apm/articulos/proxy/

a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

2.6.1 FUNCIONAMIENTO DE UN PROXY [36]

Un servidor Proxy actúa como intermediario entre el programa cliente (Netscape, Mozilla, Internet Explorer...) y el servidor Web que contiene la información que se desee obtener. Su función consiste en almacenar páginas de Internet, gráficos, fotos, archivos de música, para que la próxima vez que se pida el mismo objeto no se deba acceder de nuevo al servidor web que lo alojaba, sino que se sirva directamente desde su memoria o lo que es lo mismo desde su caché.

El proxy web es un dispositivo que suele estar más cerca del propio ordenador que del servidor al que se está accediendo. Este suele tener lo que se denomina una caché, con una copia de las páginas web que se van visitando. Entonces, si varios usuarios que acceden a Internet a través del mismo proxy acceden al primer sitio web, el Proxy, la primera vez accede físicamente al servidor destino, solicita la página, la descarga y la guarda en la caché, además de enviarla al usuario que la ha solicitado. En sucesivos accesos a la misma información por distintos usuarios, el proxy sólo comprueba si la página solicitada se encuentra en la caché y no ha sido modificada desde la última solicitud. En ese caso, en lugar de solicitar de nuevo la página al servidor, envía al usuario la copia que tiene en la caché. Esto mejora el rendimiento o velocidad de la conexión a Internet de los equipos que están detrás del proxy.

Otro caso típico de uso de un proxy es para navegar anónimamente. Al ser el proxy el que accede al servidor web, el proxy puede o no decir quién es el usuario que lo está utilizando. El servidor web puede entonces tener constancia de que lo están accediendo, pero puede que piense que el usuario que lo accede es el propio proxy, en lugar del usuario real que hay detrás del proxy.

36 http://www.desarrolloweb.com/faq/que-es-proxy.html

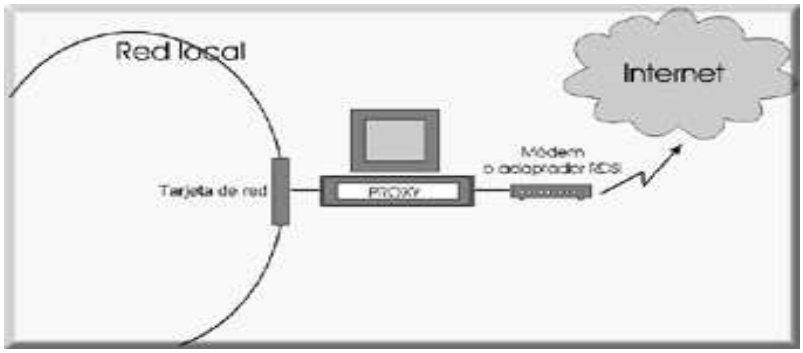

FIGURA 2. 13: ESQUEMA DE UN PROXY [37]

2.6.2 Ventajas de Un Proxy de Caché [38]

Las ventajas que ofrece la utilización de un proxy en una red local son las siguientes:

- Menor coste: El programa y la instalación tienen un precio mucho menor que cualquier router.
- Fácil instalación: La instalación emplea los dispositivos de la propia red local, por lo que se reduce la configuración de los programas.
- Seguridad: Puede controlar el acceso a Internet prohibiendo por ejemplo la entrada a determinadas páginas Web por su contenido erótico o por cualquier otro motivo, ya que un servidor Proxy puede realizar simplemente la función de pasarela sin realizar caché.
- Dirección IP única: La dirección IP es la que identifica de forma unívoca a cada máquina en Internet. Si se utiliza un proxy basta con una dirección IP para toda la red local en lugar de tener una IP para cada uno de los ordenadores.
- Menor tráfico de red:

37 http://www.ccm.itesm.mx/dinf/redes/indexproxy.html

38 http://www.ccm.itesm.mx/dinf/redes/indexproxy.html

2.6.3 PROXY SQUID [39]

Squid es el software para servidor Proxy, más popular y extendido entre los sistemas operativos basados sobre UNIX®. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios.

Entre otras cosas, Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

2.6.3.1 Algoritmos Utilizados Por Squid

A través de un parámetro (cache_replacement_policy) Squid incluye soporte para los siguientes algoritmos para el caché:

- **LRU** Acrónimo de Least Recently Used, que traduce como Menos Recientemente Utilizado. En este algoritmo los objetos que no han sido accedidos en mucho tiempo son eliminados primero manteniendo siempre en el caché a los objetos más recientemente solicitados. Ésta política es la utilizada por Squid de modo predefinido.
- **LFUDA** Acrónimo de Least Frequently Used with Dynamic Aging, que se traduce como Menos Frecuentemente Utilizado con Envejecimiento Dinámico. En este algoritmo los objetos más solicitados permanecen en el caché sin importar su tamaño optimizando la eficiencia (hit rate) por octetos (Bytes) a expensas de la eficiencia misma, de modo que un objeto

39 http://www.ccm.itesm.mx/dinf/redes/indexproxy.html

grande que se solicite con mayor frecuencia impedirá que se pueda hacer caché de objetos pequeños que se soliciten con menor frecuencia.

- **GDSF** Acrónimo de GreedyDual Size Frequency, que se traduce como Frecuencia de tamaño GreedyDual (codicioso dual), que es el algoritmo sobre el cual se basa GDSF. Optimiza la eficiencia (hit rate) por objeto manteniendo en el caché los objetos pequeños más frecuentemente solicitados de modo que hay mejores posibilidades de lograr respuesta a una solicitud (hit). Tiene una eficiencia por octetos (Bytes) menor que el algoritmo LFUDA debido a que descarta del caché objetos grandes que se han solicitado con frecuencia.

2.6.3.2 Listas De Control De Acceso (ACL) [40]

Las Listas de Control de Acceso son condiciones que definen una red o ciertas máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

```
acl  nombre_acl  tipo_acl descripción
acl  nombre_acl  tipo_acl  "fichero_de_descripciones"
```

Cuando usamos un "fichero_de_descripciones", cada descripción se corresponde con una línea del fichero.

2.6.3.2.1 Tipos de ACL

- *src*

Especifica una dirección origen de una conexión en formatio IP/máscara.

Por ejemplo, se utilizará una acl de tipo src para especificar la red local:

40 http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

- *acl red_local src 192.168.1.0/24*

También se puede especificar rangos de direcciones mediante una acl de tipo src:

- *acl jefes src 192.168.1.10-192.168.1.25/32*

- *dst*

Especifica una dirección destino de una conexión en formato IP/máscara.

- *acl google_es dst 216.239.0.0/24*

También se puede especificar hosts concretos mediante una acl de tipo dst:

- *acl google_es2 dst 216.239.59.104/32 216.239.39.104/32 216.239.57.104/32*

Las definiciones son idénticas a las acl de tipo src salvo que se aplican al destino de las conexiones, no al origen.

- *srcdomain y dstdomain*

Estos tipos de acl especifican un nombre de dominio.

En el caso de srcdomain es el dominio origen y se determina por resolución DNS inversa de la IP de la máquina, es decir, tendremos que tener bien configurado el DNS de la red local.

En el caso de dstdomain el nombre del dominio se comprueba con el dominio que se haya especificado en la petición de página web.

- *acl google_com dstdomain google.com*

- *time*

Este tipo de acl permite especificar una franja horaria concreta dentro de una semana. La sintaxis es la siguiente:

- *acl nombre_acl_horaria time [dias-abrev] [h1:m1-h2:m2]*

Donde la abreviatura del día es:

S - Sunday (domingo)

M - Monday (lunes)

T - Tuesday (martes)

W - Wednesday (miércoles)

H - Thursday (jueves)

F - Friday (viernes)

A - Saturday (sábado)

Además la primera hora especificada debe ser menor que la segunda, es decir h1:m1 tiene que ser menor que h2:m2

- *acl horario_laboral time M T W H F 8:00-15:00*

Se estaría especificando un horario de 8 a 15 y de lunes a viernes.

- *url_regex*

Permite especificar expresiones regulares para comprobar una url completa, desde el http:// inicial.

Por ejemplo, si se desea establecer una acl que verifique con todos los servidores cuyo nombre sea adserver:

- *url_regex serv_publicidad http://adserver*

En otro ejemplo podemos ver una acl que verifique las peticiones de ficheros mp3:

- *url_regex ficheros_mp3 -i mp3$*

Ejemplos de ACL:

- acl todos

Una acl que verifica todos los equipos de la red se podrá utilizar posteriormente para establecer una política preestablecida para denegarlo o aceptarlo todo.

- *acl todos src 0.0.0.0/0.0.0.0*

- acl localhost

Nuestra propia máquina como origen de conexiones

- *acl localhost src 127.0.0.1/255.255.255.255*

2.6.3.3 REGLAS DE CONTROL DE ACCESO (HTTP_ACCESS)

Este es el parámetro que permite o deniega accesos a una o más acl.

La sintaxis de uso es:

http_access allow|deny [!]acl ...

Por ejemplo, para permitir acceso fuera del horario laboral, según una acl que se definió anteriormente:

```
http_access  allow ! horario_laboral
Para denegar el acceso en horario laboral
http_access deny  horario_laboral
Para dar acceso completo a la red local
http_access allow  red_local
```

2.7 SAMBA [41]

Samba es un producto que se distribuye gratuitamente para varias versiones de UNIX(R), de acuerdo con los términos de la General Public License de GNU, y que básicamente permite al sistema Unix conversar con sistemas Windows a través de la red de forma nativa. De esta forma, el sistema Unix aparece en el "Entorno de red", y clientes Windows pueden acceder a sus recursos de red e impresoras compartidas como si de otro sistema Windows se tratase. Para ello, Samba implementa los protocolos NetBIOS y SMB.

NetBIOS es un protocolo de nivel de sesión que permite establecer sesiones entre dos ordenadores.

Samba es un servidor SMB libre, desarrollado por Andrew Tridgell y que en la actualidad es mantenido por un grupo de personas de todo el mundo, como casi todos los proyectos distribuidos bajo la Licencia Publica General de GNU. Samba es capaz de ejecutarse en una gran cantidad de variantes Unix, como Linux, Solaris, Unix de Digital, SCO Open Server y AIX por nombrar tan sólo algunas. Con Samba se puede hacer que el sistema Linux actúe como servidor SMB dentro de la red.

---

41 http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-samba

SMB ("Server Message Block") es parte del protocolo NetBEUI desarrollado por Microsoft e IBM que permite la comunicación entre Discos e Impresoras en Sistemas de Windows. En Unix (Linux) esta funcionalidad es denominada SAMBA y permite que un servidor ("Host") Unix , pueda accesar recursos en plataformas de Windows(95,98,NT,2000), al igual que permite a estas plataformas (Windows) accesar recursos en "Hosts" de Unix. [42]

Históricamente, este protocolo fue desarrollado inicialmente por IBM como el IBM PC Network SMB Protocol o Core Protocol a principios de los años 80. Desde entonces, diversos fabricantes (especialmente Microsoft) han ido ampliando su funcionalidad progresivamente, creando diferentes variantes (versiones) de SMB. Desafortunadamente, en ocasiones el cambio de versión ha conllevado el rebautizar el propio protocolo. En este sentido, SMB ha recibido, entre otros, los siguientes nombres: Core Protocol, DOS Lan Manager, LAN Manager, NTLM (NT Lan Manager), y en los últimos años, CIFS (Common Internet File System). Todos ellos, por tanto, hacen referencia a SMB, aunque se diferencien en algunos detalles de su funcionalidad y/o implementación.

Si se fija en su interfaz, SMB es un protocolo de tipo cliente/servidor, donde el ordenador "servidor" ofrece recursos (archivos, impresoras, etc.) que pueden ser utilizados remotamente por los ordenadores "cliente" a través de la red. Asimismo, es un protocolo de los denominados petición/respuesta, indicando que las comunicaciones se inician siempre desde el cliente como una petición de servicio al servidor (dicha petición se denomina precisamente SMB), que la procesa y retorna una respuesta a dicho cliente.La respuesta del servidor puede ser positiva (con el resultado de procesar la petición del cliente) o negativa (mensaje de error), en función del tipo de petición, la disponibilidad del recurso, el nivel de acceso (permisos) del cliente, etc. [43]

42 http://www.osmosislatina.com/linux/win_samba.jsp

43 http://fferrer.dsic.upv.es/cursos/Integracion/html/ch04s02.html

2.7.1 SERVICIOS DE SAMBA

SMB (Server Message Block), implementado sobre NetBIOS, es el protocolo que permite a los sistemas Windows compartir ficheros e impresoras.
Esencialmente, Samba consiste en dos programas, denominados smbd y nmbd. Ambos programas utilizan el protocolo NetBIOS para acceder a la red, con lo cual pueden conversar con ordenadores Windows. Haciendo uso de estos dos programas, Samba ofrece los siguientes servicios, todos ellos iguales a los ofrecidos por los sistemas Windows:

- Servicios de acceso remoto a ficheros e impresoras.
- Autenticación y autorización.
- Resolución de nombres.
- Anuncio de servicios.

2.7.1.1 Utilidades de SAMBA

Adicionalmente a los dos programas anteriores, Samba ofrece varias utilidades. Algunas de las más relevantes son las siguientes:

- **Smbclient:**

  Una interfaz similar a la utilidad FTP, que permite a un usuario de un sistema Unix conectarse a recursos SMB y listar, transferir y enviar ficheros.

- **swat (Samba Web Administration Tool):**

  Esta utilidad permite configurar Samba de forma local o remota utilizando un navegador de web.

- **Smbfs:**

  Sistema de ficheros SMB para Linux. Linux puede montar recursos SMB en su jerarquía, al igual que sucede con directorios compartidos vía NFS.

- **Winbind:**

  Permite integrar un servidor Samba en un dominio Windows sin necesidad de crear usuarios Unix en el servidor Samba que correspondan con los usuarios del dominio Windows, simplificando así la labor de administración.

2.7.2 DEMONIOS SAMBA [44]

Lo siguiente es una breve introducción a los demonios individuales y servicios de Samba.

Samba está compuesta por tres demonios (smbd, nmbd y winbindd). Dos servicios (smb y windbind) controlan los demonios son detenidos arrancados y otras funcionalidades relacionadas a servicios. Cada demonio se lista en detalle, así como también qué servicio específico tiene control sobre él.

2.7.2.1 Demonio smbd

El demonio de servidor smbd suministra servicios para compartir archivos e impresión a clientes Windows. Además, es responsable por la autenticación de usuarios, el bloqueo de recursos y compartir datos a través del protocolo SMB. Los puertos predeterminados en los cuales el servidor escucha por tráfico SMB, son los puertos TCP 139 y 445.

El demonio smbd es controlado por el servicio smb.

2.7.2.2 Demonio nmvd

El demonio del servidor nmbd entiende y responde a las peticiones de servicio de nombres NetBIOS tales como aquellas producidas por SMB/CIFS en sistemas basados en Windows. Estos sistemas incluyen clientes 95/98/ME, Windows NT, Windows 2000, Windows XP y LanManager. También participa en los protocolos de navegación que forman la vista Entorno de red de Windows. El puerto predeterminado en el que el servidor escucha por tráfico NMB es el puerto UDP 137.

El demonio nmbd es controlado por el servicio smb.

44 http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-samba-daemons.html

2.7.2.3 Demonio winbindd

El servicio winbind resuelve la información de usuarios y grupos en un servidor Windows NT y lo hace entendible para las plataformas UNIX. Esto se logra usando las llamadas RPC, Pluggable Authentication Modules (PAM) y el Name Service Switch (NSS). Esto permite que los usuarios del dominio Windows NT aparezcan y operen como usuarios UNIX en un máquina UNIX. Aunque está enlazado con la distribución Samba, el servicio winbind se controla separadamente de smb.

2.7.3 FUNCIONAMIENTO INTERNO DEL PROTOCOLO SMB [45]

Se revisará brevemente el funcionamiento interno del protocolo SMB, utilizando para ello un ejemplo concreto. Suponiendo que un sistema cliente desea acceder a una carpeta compartida que exporta el servidor (en modo user). En este escenario, se produciría el siguiente intercambio de mensajes entre ellos:

- Petición Sesión NetBIOS:

  El objetivo de este mensaje es establecer una sesión fiable para subsiguientes mensajes entre los ordenadores cliente y servidor. Es imprescindible que el cliente conozca el nombre NetBIOS del servidor para poder alcanzarlo; el nombre NetBIOS del cliente es parte del mensaje, por lo que ambos saben quién es el otro.

- Respuesta Sesión NetBIOS:

  Si no hay error en el mensaje anterior, el servidor envía un mensaje de reconocimiento (ACK), aceptando la conexión.

- Petición: Dialecto SMB:

  El cliente envía en este mensaje una lista con los dialectos o variantes de SMB que soporta, puesto que es habitual que un sistema Windows soporte varias versiones de SMB simultáneamente.

45 http://fferrer.dsic.upv.es/cursos/Integracion/html/ch04s02.html

- Respuesta Dialecto SMB:

El servidor contesta con el dialecto que prefiere para la comunicación subsiguiente, o un código de error si no soporta ninguna de las alternativas ofrecidas por el cliente.

- Petición Inicio de sesión:

El cliente envía las credenciales de usuario (usuario, dominio, contraseña) con las que éste desea conectarse al servidor. Recuérdese que por defecto, se emplean las credenciales con las que el usuario se conectó interactivamente al sistema cliente, pero se pueden especificar otras explícitamente.

- Respuesta Inicio de sesión:

El servidor autentifica las credenciales de usuario.

Si las credenciales son buenas, el servidor posee ya un SID válido que le permite, antes que nada, comprobar si el usuario posee el derecho de conectarse .En caso afirmativo, se acepta la conexión y el servidor construye un identificador numérico particular para esa conexión (denominado User ID o UID) que devuelve al cliente. Los UIDs pueden ser reutilizados durante la vida del sistema, pero son únicos para todas las conexiones simultáneas que mantiene el servidor en un momento dado, por lo que identifican unívocamente una conexión (aceptada). Todos los mensajes posteriores del cliente deben contener este identificador para ser aceptados por el servidor.

Por otro lado, si las credenciales estaban mal (o si los derechos eran insuficientes), el servidor envía un código de error en lugar del UID.

- Petición Conexión a un recurso concreto:

El cliente envía entonces un mensaje que contiene una cadena que identifica el recurso al que desea acceder (por ejemplo, \\pc01\impresora o \\pc01\carpeta).

Respuesta: Conexión a un recurso concreto: Si el recurso solicitado por el cliente existe (y el SID asociado a la conexión posee suficientes permisos), el servidor construye un identificador denominado Tree ID o TID, que será

utilizado por el cliente para hacer referencia a dicho recurso en posteriores mensajes de esa conexión.

Tras esta secuencia típica de conexión al recurso (carpeta compartida), y si todo ha funcionado correctamente, el sistema cliente ya está en condiciones de acceder a la carpeta. Mediante el envío de los SMBs correspondientes, el cliente ya puede abrir archivos, leerlos, modificarlos, etc., utilizando siempre los identificadores (UID y TID) que el servidor ha construido durante el intercambio de mensajes inicial.

2.7.4 TIPOS DE SERVIDORES SAMBA

La configuración de Samba es bien directa. Todas las modificaciones a Samba se realizan en el archivo de configuración /etc/samba/smb.conf. Aunque el archivo predeterminado smb.conf está bien documentado, no menciona tópicos complejos como LDAP, Active Directory y numerosas implementaciones de controladores de dominio.

Las secciones siguientes describen las diferentes formas en que se puede configurar un servidor Samba.

2.7.4.1 Servidor independiente

Un servidor independiente puede ser un servidor de un grupo de trabajo o un miembro de entorno de grupo de trabajo. Un servidor independiente no es un controlador de dominio y no participa en un dominio de ninguna manera.

2.7.4.2 Servidor de impresión anónimo

El siguiente archivo smb.conf muestra una configuración de muestra necesaria para implementar un servidor de impresión anónimo. Configurando browseable a no como se muestra, no lista la impresora en el Entorno de red. Aunque está oculto para propósitos de navegación, se puede configurar la impresora explícitamente. Al conectar DOCS_SRV usando NetBIOS, el cliente puede tener

acceso a la impresora si el cliente también es parte del grupo de trabajo DOCS. También se asume que el cliente tiene el controlador de impresora correcto, pues la directriz de use client driver está configurada a Yes. En este caso, el servidor Samba no tiene responsabilidad de compartir los controladores de impresora con el cliente.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = share
printcap name = cups
disable spools= Yes
show add printer wizard = No
printing = cups

[printers]
comment = All Printers
path = /var/spool/samba
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = Yes
```

2.7.3.3 Servidor de miembro de dominio

Un miembro de dominio, aunque es similar a un servidor independiente, es conectado a un controlador de dominio (bien sea Windows o Samba) y está sujeto a las reglas de seguridad del dominio. Un ejemplo de un servidor miembro de dominio podría ser un servidor departamental ejecutando Samba que tiene una cuenta de máquina en el Controlador de Dominio Primario (PDC). Todos los clientes del departamento todavía se autentifican con el PDC y se incluyen los perfiles del escritorio y todos los archivos de políticas. La diferencia es que el

servidor departamental tiene la habilidad de controlar las impresoras y recursos de red compartidos.

2.7.5 Comandos de acceso SMB

2.7.5.1 FINDSMB

El programa es un script de Perl que reporta información sobre los sistemas compatibles con SMB en una subred específica. Si no se especifica ninguna subred, se utilizará la subred local. Los items mostrados incluyen direcciones IP, nombres NetBIOS, nombre de dominio o grupo de trabajo, sistema operativo y versión.

El ejemplo siguiente muestra la salida de la ejecución de findsmb como cualquier usuario válido en un sistema:

```
findsmb

IP ADDR       NETBIOS NAME  WORKGROUP/OS/VERSION
------------------------------------------------------------------
10.1.59.25    VERVE          [MYGROUP] [Unix] [Samba 3.0.0-15]
10.1.59.26    STATION22      [MYGROUP] [Unix] [Samba 3.0.2-7.FC1]
10.1.56.45    TREK          +[WORKGROUP] [Windows 5.0] [Windows 2000 LAN Manager]
10.1.57.94    PIXEL          [MYGROUP] [Unix] [Samba 3.0.0-15]
10.1.57.137   MOBILE001      [WORKGROUP] [Windows 5.0] [Windows 2000 LAN Manager]
10.1.57.141   JAWS          +[KWIKIMART] [Unix] [Samba 2.2.7a-security-rollup-
fix]
10.1.56.159   FRED          +[MYGROUP] [Unix] [Samba 3.0.0-14.3E]
10.1.59.192   LEGION        *[MYGROUP] [Unix] [Samba 2.2.7-security-rollup-fix]
10.1.56.205   NANCYN        +[MYGROUP] [Unix] [Samba 2.2.7a-security-rollup-fix]
```

2.6.5.2 NET

net <protocol> <function> <misc_options> <target_options>

La utilidad net es similar a la utilidad net utilizada por Windows y MS-DOS. El primer argumento es utilizado para especificar el protocolo utilizado cuando se ejecuta un comando. La opción <protocol> puede ser ads, rap o rpc para especificar el tipo de conexión al servidor. Active Directory utiliza ads, Win9x/NT3

usa rap y Windows NT4/2000/2003 utiliza rpc. Si se omite el protocolo, net intentará determinarlo automáticamente.

El ejemplo siguiente muestra una lista de los directorios compartidos para un host llamado wakko:

```
net -l share -S wakko
Password:

Enumerating shared resources (exports) on remote server:


Share name   Type     Description
----------   ----     -----------
data         Disk     Wakko data share
tmp          Disk     Wakko tmp share
IPC$         IPC      IPC Service (Samba Server)
ADMIN$       IPC      IPC Service (Samba Server)
```

2.7.5.3 SMBCLIENT

smbclient <//server/share> <password> <options>

El programa smbclient es un cliente UNIX versátil que proporciona una funcionalidad similar a FTP.

2.7.5.4 SMBMOUNT

smbmount <//server/share> <mount_point> <-o options>

El programa smbmount utiliza el programa de bajo nivel smbmnt para montar un sistema de archivos smbfs (recurso Samba compartido). El comando mount -t smbfs <//server/share> <mount_point> <-o options> también funciona.

Por ejemplo:

```
smbmount //wakko/html /mnt/html -o username=kristin
Password: <password>
[root@yakko /]# ls -l /mnt/html
total 0
-rwxr-xr-x    1 root     root            0 Jan 29 08:09 index.html
```

2.8 EJECUCIÓN DE TAREAS AUTOMÁTICAS [46]

2.8.1 CRONTAB

Existe en Linux una utilidad que no muchos conocen y que resulta a veces imprescindible: crontab.

Crontab permite programar lo que se conoce como crones, esto es, tareas que se ejecutarán en un momento determinado del tiempo de manera automática. El sistema Linux (y cualquier UNIX en general) comprueba regularmente, guiándose por el evento de reloj del sistema, si existe alguna tarea programada para ejecutarse y, en caso afirmativo, la ejecuta sin necesidad de que nadie (ningún usuario) lo haga explícitamente.

En primera instancia, algunas aplicaciones que se pueden utilizar para ser ejecutadas en el crontab podrían ser:

- Apagar un equipo a una hora deseada: Por ejemplo, mientras se duerme se puede dejarlo bajando cosas de internet haciendo que se apague solo por la mañana.
- Crear backups: Se puede programar un cron para que, a cierta hora de ciertos días de la semana o del mes, el sistema realice un backup de la información de manera automática, sin tener que recordar por parte del usuario el hacerlo.
- Poner mensajes recordatorios: Para que salgan en pantalla una ventana recordando una tarea a realizar.

La herramienta crontab permite programar una tarea para que se ejecute especificando:

- La hora (0-23)
- Los minutos (0-59)
- El día del mes (1-31)
- El día de la semana (0-7: tanto 0 como 7 representan al domingo)

46 http://www.elrincondelprogramador.com/default.asp?pag=trucos/truco.asp&truco=58

- El mes (1-12)

Además en cualquiera de estos parámetros se puede especificar, mediante un *, que se desea que una tarea se ejecute todos los minutos, las horas, los días del mes, los meses, o los días de la semana.

2.9 ACCESO A INTERNET

2.9.1 PROVEEDOR DE SERVICIOS DE INTERNET (ISP) [47]

Proveedor de servicios de Internet (ISP por la sigla en idioma inglés de Internet Service Provider) es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros.

2.9.2 BANDA ANCHA [48]

Se refiere al acceso a Internet de alta velocidad. La Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) define al servicio de banda ancha como la transmisión de datos a una velocidad mayor de 200 kilobits por segundo (Kbps) o 200,000 bits por segundo, en por lo menos una dirección: transmisión de bajada (del Internet a la computadora del usuario) o de subida (de la computadora del usuario al Internet).

2.9.2.1 Tipos de Banda Ancha

La banda ancha incluye varias tecnologías de transmisión de alta velocidad tales como:

- **Línea Digital de Suscriptor (DSL)**

La Línea Digital de Suscriptor (DSL, por sus siglas en inglés) es una tecnología de transmisión telefónica que transmite datos más rápido a través de las líneas

47 http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

48 http://www.fcc.gov/cgb/broadband_spanish.html#Wireless

telefónicas de cobre ya instaladas en casas y empresas. La banda ancha de DSL proporciona velocidades de transmisión que van desde varios cientos de kilobits por segundo (Kbps) hasta millones de bits por segundo (Mbps). La disponibilidad y velocidad de su servicio de DSL puede depender de la distancia que hay entre su casa o negocio a las instalaciones más próximas de la compañía de teléfonos.

- **Módem de Cable**

El servicio de módem de cable permite a los operadores de cable suministrar acceso a Internet de alta velocidad usando los cables coaxiales que envían imágenes y sonidos a su televisor.

La mayoría de los módems de cable son dispositivos externos que tienen dos conectores, uno en la salida de pared del cable y el otro en la computadora. La velocidad de transmisión de datos es de 1.5 Mbps o más.

Los suscriptores pueden tener acceso al servicio de módem de cable simplemente prendiendo sus computadores sin tener que marcar al proveedor del servicio de Internet (ISP, por sus siglas en inglés). Podrá ver la TV por cable y usar el Internet al mismo tiempo. Las velocidades de transmisión varían dependiendo del tipo de módem de cable, red del cable y carga de tráfico. Las velocidades son comparables con la DSL.

- **Fibra óptica**

La fibra o fibra óptica es una tecnología muy nueva que proporciona servicio de banda ancha. La tecnología de fibra óptica convierte las señales eléctricas que llevan los datos en luz y envía la luz a través de fibras de vidrio transparentes con un diámetro cercano al del cabello humano. La fibra transmite los datos a velocidades muy superiores a las velocidades de la DSL o módem de cable actuales, normalmente en diez o cien veces más Mbps.

La velocidad real que experimenta variará dependiendo de diversos factores como qué tan cerca lleva su proveedor de servicio la fibra a su computadora y la forma cómo configura el servicio, incluyendo la cantidad de ancho de banda utilizada. La misma fibra que provee su banda ancha puede también simultáneamente suministrar servicios de telefonía por Internet (VoIP) y de vídeo, incluyendo vídeo según demanda.

Los proveedores de servicios de telecomunicaciones (en su mayoría compañías telefónicas) están ofreciendo banda ancha por fibra óptica en áreas limitadas y han anunciado planes para ampliar sus redes de fibra y ofrecer un paquete de servicios de voz, acceso a Internet y vídeo.

Las variantes de esta tecnología permiten que la fibra llegue hasta el hogar o empresa del cliente, hasta la esquina de su casa o algún lugar entre las instalaciones del proveedor y el cliente.

- **Inalámbrica**

La banda ancha inalámbrica conecta su casa o negocio a Internet usando un enlace de radio entre la localidad del cliente y las instalaciones del proveedor del servicio. La banda ancha inalámbrica puede ser móvil o fija.

Las tecnologías inalámbricas que usan equipo direccional con un rango mayor proveen el servicio de banda ancha en áreas remotas o muy poco pobladas donde el servicio de la DSL o del módem de cable sería muy costoso. Generalmente las velocidades son comparables a las de la DSL y el módem de cable. Normalmente se requiere de una antena externa.

Cada vez es más frecuente el servicio de banda ancha inalámbrica fija en aeropuertos, parques de la ciudad, bibliotecas y otros lugares públicos llamados "hotspots". Los "hotspots" usan generalmente una tecnología de rango corto con velocidades de transmisión de hasta 54 Mbps. La tecnología de fidelidad inalámbrica (Wi-Fi) se usa con frecuencia también en conjunto con el servicio de la DSL o módem de cable para conectar los dispositivos de una casa o negocio al Internet vía una conexión de banda ancha.

Los servicios de banda ancha inalámbrica móvil se pueden obtener también de compañías de telefonía móvil y otros. Estos servicios generalmente son adecuados para los clientes que tienen mucha movilidad y requieren una tarjeta especial para PC con una antena integrada que se conecta a la computadora portátil del usuario. Generalmente proveen velocidades menores de transmisión en el rango de varios cientos de Kbps.

- **Satélite**

Así como los satélites que giran alrededor de la tierra proveen los enlaces necesarios para los servicios de telefonía y televisión, también proveen enlaces para la banda ancha. La banda ancha por satélite es otra forma de banda ancha inalámbrica, muy útil también para dar servicio a áreas remotas o muy poco pobladas.

Las velocidades de transmisión de datos de subida y bajada para la banda ancha por satélite dependen de varios factores, incluyendo el paquete de servicios que se compra y el proveedor, la línea de visibilidad directa del consumidor al satélite y el clima. Normalmente un consumidor puede esperar recibir (descargar) los datos a una velocidad de aproximadamente 500 Kbps y enviarlos (cargar) a una velocidad de aproximadamente 80 Kbps. Estas velocidades pueden ser menores que las que se tienen con la DSL o el módem de cable, pero la velocidad para descargar los datos es aproximadamente 10 veces más rápida que la velocidad que se tiene con el Internet de marcación telefónica. El servicio puede interrumpirse en condiciones climáticas severas.

- **Banda ancha por la línea eléctrica (BPL)**

La banda ancha por la línea eléctrica (BPL, por sus siglas en inglés) es el servicio que se proporciona a través de la red existente de distribución de energía eléctrica de bajo y medio voltaje. Las velocidades de transmisión de la BPL son comparables a las de la DSL y el módem de cable. La BPL puede llegar a las casas usando las conexiones y salidas eléctricas existentes.

La BPL es una tecnología emergente, actualmente disponible en áreas muy limitadas. Tiene un potencial significativo ya que las líneas eléctricas están instaladas virtualmente en todos lados, aliviando la necesidad de construir nuevas instalaciones de banda ancha para cada consumidor.

2.9.3 DIRECCIÓN IP PÚBLICA

Una dirección IP pública es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente un ordenador) dentro de una red, en este caso el número identifica el punto de enlace con internet.

Hay tres clases de direcciones IP que una organización puede recibir de parte de Internet Assigned Numbers Authority (IANA): clase A, clase B y clase C. En la actualidad, IANA reserva las direcciones de clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura como, por ejemplo, Hewlett Packard) y las direcciones de clase B para las medianas empresas. Se otorgan direcciones de clase C para todos los demás solicitantes.

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan "direcciones privadas". Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT), o un servidor Proxy, para conectarse a una red pública, o por los hosts que no se conectan a Internet.

Las Direcciones IP Privadas de una red aislada, pueden ser cualesquiera, mientras pertenezcan a la misma subred determinada por la correspondiente Máscara. Pero si esa LAN va a estar conectada a Internet, pueden darse problemas de direccionamiento, ya que pueden coincidir las direcciones de la red, con las de otros host en Internet. Para estas situaciones, se reservan para redes privadas los siguientes rangos de direcciones: 10.x.x.x, 192.168.x.x, y desde 172.16.x.x a 172.31.x.x (dónde x es un número entre 0 y 255 ambos inclusive).

CAPÍTULO III

3. ANÁLISIS DE REQUERIMIENTOS Y DISEÑO

3.1 SITUACIÓN ACTUAL DE LA EMPRESA

Actualmente, EGAR S.A dispone tanto en Pifo como en Quito de un enlace inalámbrico, con un canal dedicado para el uso de Internet y un ancho de banda de 128 Kbps de bajada y 128 Kbps de subida, lo cual ayuda a tener amplitud de navegación tanto en el envío como para la recepción de los datos.

También cuenta con dos IP públicas que son provistas por el ISP. Las dos IP públicas son:

Para Quito 157.100.98.22

Para Pifo 157.100.98.18

3.1.1 SITUACIÓN ACTUAL CON RESPECTO A LA NAVEGACIÓN WEB.

EGAR S.A. carece de un sistema eficiente de seguridad para controlar y administrar la navegación de los usuarios hacia el Internet. Actualmente la navegación se realiza directamente con el gateway del proveedor ISP utilizando reglas de NAT.

La falta de un software de control provoca lo siguiente:

- La falta de protección de la información.
- La falta de control en el acceso a URL's o páginas web no deseadas.
- La propagación de virus y amenazas provenientes de Internet.
- La acumulación de software espía (spyware).

Como estrategia para superar los problemas existentes, se puede utilizar software que ayude a mejorar el control del acceso web, y poder aprovechar de una mejor manera los recursos de la misma. A través de la utilización de un Proxy se ayudará a poder proteger, controlar y administrar toda la información proveniente de la Internet.

3.1.2 SITUACIÓN ACTUAL CON RESPECTO AL CORREO ELECTRÓNICO

Actualmente, para el envío y recepción del correo electrónico, cada usuario se conecta directamente al servidor de correo ubicado en los EEUU, que es mantenido por un proveedor de servicios.
Para realizar el respectivo envío y recepción se utilizan los protocolos POP e SMTP.
Esto ha implicado problemas como:

- Demasiada dependencia hacia el proveedor de correo.
- No se asegura una disponibilidad del correo electrónico interno si el Internet no está disponible.
- Por cuanto el correo se almacena en el servidor ubicado en EEUU, no hay seguridad de la confidencialidad del mismo.
- No hay un control adecuado de virus y spam del correo entrante y saliente.
- No hay control de logs del correo.

3.1.2 SITUACIÓN ACTUAL CON RESPECTO A LOS RESPALDOS DE INFORMACIÓN.

No hay una adecuada obtención de los respaldos de información tanto del Sistema Contable como de la información de cada usuario.
Muchos de estos respaldos se realizan de manera manual ocasionando problemas como:

- No hay disponibilidad de los respaldos de información cuando un usuario así lo requiera.
- Consumo innecesario de horas hombre en ejecutar los respaldos manualmente.

3.1.4 ESQUEMA DE LA SITUACIÓN ACTUAL

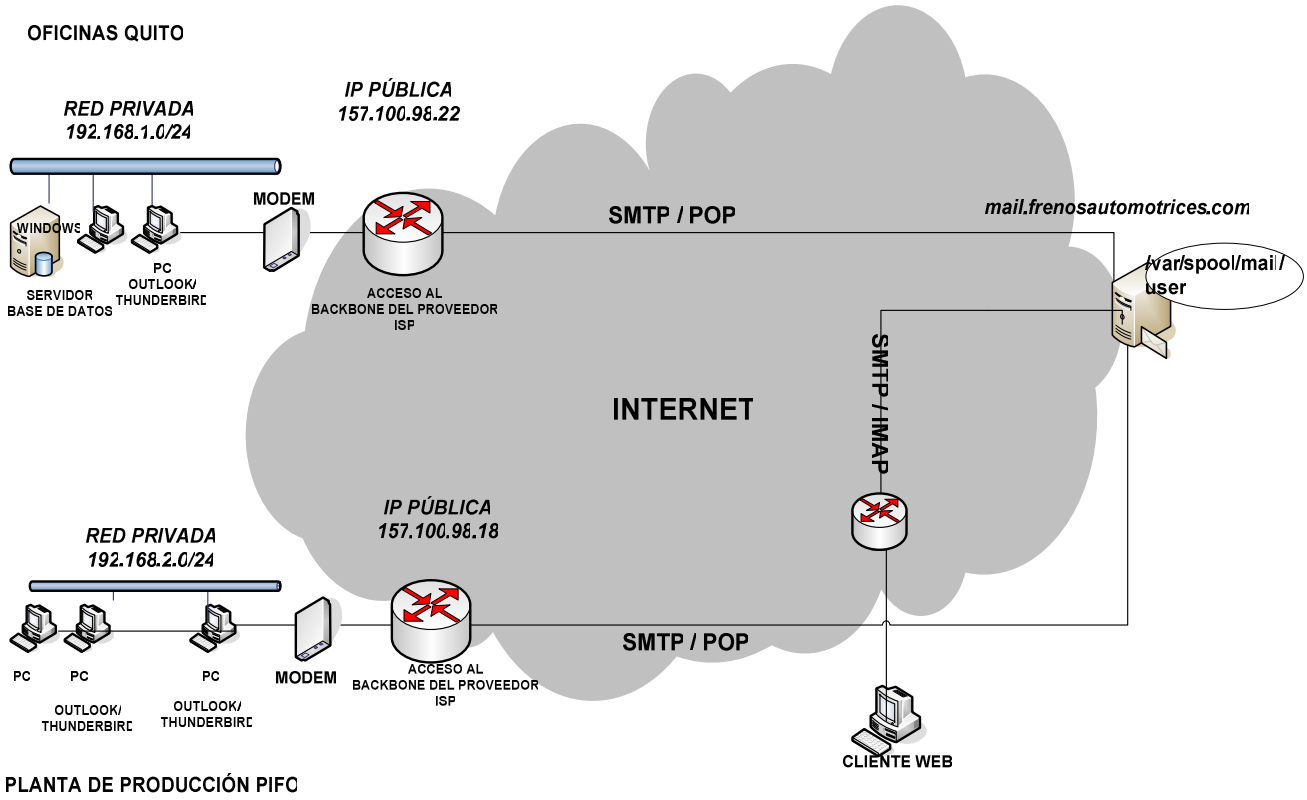

FIGURA 3. 1: ESQUEMA DE LA SITUACIÓN ACTUAL
ELABORADO POR: DAVID FREIRE

3.2 ANÁLISIS DE REQUERIMIENTOS

En esta etapa se procederá a detallar las respectivas necesidades de hardware y software para poder implementar los servicios de Proxy, Correo Electrónico y Samba. Se establecerán descripciones de los paquetes necesarios así como algunas características de los mismos.

3.2.4 SELECCIÓN DEL SISTEMA OPERATIVO

3.2.4.1 CENTOS

El Sistema Operativo a utilizar será Centos un Sistema Operativo que es 100% compatible con Red Hat Enterprise Linux gozando de sus mismos privilegios en cuanto a la estabilidad y rendimiento. De esta manera se puede tener un

conocimiento completo de cómo funciona un servidor Red Hat, pero a diferencia que al usar Centos no requiere pago por el soporte ni por las actualizaciones. Las actualizaciones de las diferentes versiones de Centos seguirán siendo soportadas por un período de 7 años a partir del lanzamiento de cada versión.

3.2.4.2 Requerimientos de Hardware

Hardware recomendado para operar:

- Velocidades

Centos soporta (casi) todas las mismas arquitecturas que el original Red Hat Enterprise Linux.

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

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

- Alpha procesador (DEC_Alpha)
- SPARC

- Memoria RAM: 64 MB (mínimo).
- Espacio en Disco Duro: 1024 MB (mínimo) - 2 GB (recomendado).

3.2.5 ANÁLISIS DE REQUERIMIENTOS SERVICIO PROXY

3.2.5.1 Squid [49]

Squid tiene una amplia variedad de utilidades, desde acelerar un Servidor Web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

Características:

- Squid proporciona un servicio de Proxy que soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentra fuera de la red interna.
- Squid también es compatible con SSL (Secure Socket Layer) con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios.
- Squid puede ser configurado para ser usado como proxy transparente de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo, se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

49 http://es.wikipedia.org/wiki/Squid

3.2.6 ANÁLISIS DE REQUERIMIENTOS SERVICIO DE CORREO ELECTRÓNICO

3.2.6.1 Dovecot [50]

Dovecot es un código abierto del servidor IMAP y POP3 para Linux / UNIX-como sistemas, escrito principalmente con la seguridad en mente. Dovecot es una excelente opción para pequeñas y grandes instalaciones. Es rápido, fácil de configurar, no requiere administración especial y consume muy poca memoria.

Características:

- Servicio de entrega de mensajes local fácilmente integrable con cualquier MTA.
- Permite modificar el formato para que presente el aspecto de otros servidores, facilitando la migración.
- Genera diversos índices que reducen el tiempo de localización de mensajes.
- Fácil de instalar e implementar.

IMAP [51]

El servidor por defecto IMAP bajo Red Hat Enterprise Linux es /usr/sbin/imapd y es proporcionado por el paquete imap. Cuando se utiliza un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leerlos o borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.

Características:

- A diferencia del protocolo POP3, el correo no es descargado inmediatamente sino que es leído o consultado directamente en el servidor.
- Permite ver únicamente los encabezados del mensaje antes de decidir si abrirlo o eliminarlo.
- El servidor retiene el correo hasta que se solicite su eliminación.
- Puede consultarse el mismo correo desde diferentes computadoras ya que solo se lee lo que hay en el servidor.

50 www.dovecot.org, http://www.uco.es/ccc/sistemas/doc_ccc/dovecot_JJTTRediris_2006.pdf

51 http://web.userservers.net/soporte/docview.php?articulo=50

- ❖ Permite operaciones avanzadas como creación de carpetas y buzones en el servidor.

POP3 [52]

POP3 o Post Office Protocol es el protocolo más común para descarga de correo electrónico desde un servidor. Debido a su simplicidad, la mayora de los programas o 'clientes' de correo electrónico (Thunderbird [53] , Outlook, etc) utilizan este protocolo por 'default' aunque pueden soportar otros más sofisticados como IMAP.

Características:

- ❖ Permite que los usuarios con conexiones intermitentes (tales como las conexiones módem), descarguen su correo electrónico cuando se encuentren conectados de tal manera que puedan ver y manipular sus mensajes sin necesidad de permanecer conectados.
- ❖ POP3 al conectarse con el servidor obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta.

3.2.6.2 BIND [54]

BIND (Berkeley Internet Name Domain, anteriormente: Berkeley Internet Name Daemon) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un standard de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley

52 http://web.uservers.net/soporte/docview.php?articulo=34, http://es.wikipedia.org/wiki/Post_Office_Protocol

53 Cliente de correo electrónico de la Fundación Mozilla, soporta IMAP/POP, correo HTML, noticias, RSS, etiquetas, corrector ortográfico incorporado, soporte de extensiones y skins

54 http://es.wikipedia.org/wiki/BIND

3.2.6.3 SENDMAIL [55]

Sendmail es un popular "agente de transporte de correo" (MTA - Mail Transport Agent) en Internet, cuya tarea consiste en "encaminar" los mensajes correos de forma que estos lleguen a su destino. Se afirma que es el más popular MTA, corriendo sobre sistemas Unix [56] y el responsable de la mayoría de envío del correo de internet, aunque se le critica su alto número de alertas de seguridad (la mayoría de ellas parchadas a las pocas horas), además de no ser sencillo de configurar.

Características:

- Soporte para múltiples dominios. Permite gestionar desde un solo servidor el correo correspondiente a varios dominios. [57]
- Soporta alias, o sinónimos de un nombre de usuario. Normalmente una lista de alias es un fichero que contiene pares de nombres: un alias y la cuenta a la que se debe redirigir el correo.
- Procesamiento del correo. Permite generar acciones cuando se recibe correo a determinadas cuentas o dominios. Un ejemplo típico de procesamiento son los servidores de listas, que aveces se incluyen como módulos externos, independientes del servidor SMTP.
- Acuse de recibo, autoreenvío (forward) y otras opciones para los usuarios del servidor.
- Soporte AntiSpam. Se conoce como Spam al correo no deseado que llega desde Internet. Un buen servidor de correo debe tener mecanismos que minimicen la entrada de este tipo de correo, o que el propio servidor pueda ser empleado para enviarlo.

55 http://es.wikipedia.org/wiki/Sendmail

56 Unix (registrado oficialmente como UNIX®) es un sistema operativo portátil, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy

57 www.itq.edu.mx/vidatec/espacio/aisc/windowsnt/Servidordecorreo.htm - 19k

3.2.6.4 CLAMAV [58]

Clamav representa una excelente alternativa pues tiene un bajo consumo de recursos de sistema, haciéndolo idóneo para servidores con sustento físico obsoleto, o donde otras aplicaciones tiene mayor prioridad en la utilización de recursos de sistema.

Características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Detecta más de 44 mil virus, gusanos y troyanos, incluyendo virus para MS Office.
- Capacidad para examinar contenido de ficheros ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.
- El clamav es un paquete que tiene actualizaciones automáticas (a través del yum) y además tiene una herramienta para actualizar la Base de Datos de virus conocida como freshclam.

3.2.6.5 SPAMASSASSIN [59]

El spamassassin es la herramienta usada por el MailScanner para determinar mediante un sistema de pesos si un correo es spam o no. Es un equipamiento lógico que utiliza un sistema de puntuación basado sobre algoritmos de tipo genético, para identificar mensajes que pudieran ser sospechosos de ser correo masivo no solicitado, añadiendo cabeceras a los mensajes de modo que pueda ser filtrados por el cliente de correo electrónico o MUA (Mail User Agent).

Características:

- Filtro Bayesiano (Auto Aprendizaje de nuevo Spam)
- Chequeo de listas negras en tiempo real.
- Posibilidad de crear manualmente listas negras y blancas a nivel local.

58 http://www.clamav.net

59 http://wiki.apache.org/spamassassin/SpamAssassin

- ❖ Colaboración para reportar Spam hacia las bases de datos de listas negras.
- ❖ Configuración de reglas para el chequeo de correo electrónico.

3.2.6.6 MAILSCANNER [60]

Combinado con Clamav y Spamassassin, resulta una de las soluciones más robustas para la protección contra correo masivo no solicitado, fraudes electrónicos, virus, gusanos y troyanos desde el servidor de correo electrónico.

Características:

- ❖ Revisa el correo electrónico en busca de virus utilizando cualquier combinación de entre más de una docena de distintos programas anti-virus.
- ❖ Automáticamente actualiza todo los anti-virus instalados cada hora.
- ❖ Identifica alrededor del 95% del correo masivo no solicitado (Spam) utilizando diferentes técnicas, incluyendo técnicas altamente avanzadas de heurística (capacidad de un sistema para realizar de forma inmediata innovaciones positivas para sus fines).
- ❖ El correo identificado como peligroso puede ser etiquetado, rechazado, descartado, archivado o reenviado hacia otras direcciones para su inspección por los administradores.
- ❖ Es altamente configurable, proporciona a los Proveedores de Servicios de Internet (ISP o Internet Service Provider y Proveedores de Servicios de Aplicaciones (ASP o Application Service Provider) la posibilidad de utilizar miles de diferentes reglas y configuraciones para cualquier combinación de usuarios y dominios.
- ❖ Es fácil de instalar y configurar puesto que sus opciones predefinidas permiten trabajar al servicio de correo sin complicaciones.

60 http://www.mailscanner.info/.

3.2.6.7 SQUIRRELOUTLOOK [61]

SquirrelMail es una aplicación webmail al estilo Outlook creada por Nathan y Luke Ehresman y escrita en PHP [62]. Puede ser instalado en la mayoría de servidores web siempre y cuando éste soporte PHP y el servidor web[63] tenga acceso a un servidor IMAP y a otro SMTP.

SquirrelMail sigue el standard HTML 4.0 para su presentación, haciéndolo compatible con la mayoría de servidores web. SquirrelMail está diseñado para trabajar con plugins, lo cual hace más llevadera la tarea de agregar nuevas características entorno al núcleo de la aplicación.

Características:

- Interfaz Gráfica parecida a Outlook 2003
- Gestión de carpetas.
- Gestión de attachments.
- Filtros de mensajes según direcciones de correo o subject.
- Posibilidad de añadir direcciones de correo de emails entrantes o contenidas en un email a nuestro libro de direcciones de forma automática.

3.2.6.8 APACHE [64]

Servidor Apache HTTP es un servidor Web de tecnología Open Source diseñado para plataformas Unix, Linux Windows, Macintosh etc. Sólido y para uso comercial desarrollado por la Apache Software Fundation.

Características:

- Apache es extremadamente popular, sobre todo porque es un servidor web portable entre diferentes plataformas de sistemas operativos, tales como Windows, Linux.

---

61 http://es.wikipedia.org/wiki/Webmail - 19k

62 http://es.wikipedilenguaje de programación interpretado usado normalmente para la creación de páginas web dinámicas. PHP es un acrónimo recursivo que significa "PHP Hypertext Pre-processor"

63 Programa que implementa el protocolo HTTP (hipertexto transfer protocol), diseñado para transferir, páginas web o páginas HTML por medio de un navegador web.

64 http://es.wikipedia.org/wiki/Servidor_HTTP_Apache

- Acepta la instalación de módulos realizados por terceras personas para agregarle funcionalidad.
- Facilidad de configuración.
- Soporta lenguajes Perl y Php entre otros.
- Permite conexiones encriptadas vía SSL.

3.2.7 ANÁLISIS DE REQUERIMIENTOS SERVICIO SAMBA

3.2.7.1 SAMBA [65]

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX.

Características:

Samba es una aplicación de servidor poderosa y versátil. Hasta los administradores bien empapados deben conocer sus habilidades y limitaciones antes de intentar una instalación y configuración.

Lo que Samba puede hacer: [66]

- Sirve árboles de directorios e impresoras a clientes Linux, UNIX y Windows
- Asiste en la navegación de la red (con o sin NetBIOS)
- Autentifica las conexiones a dominios Windows
- Proporciona resolución de nombres de Windows Internet Name Service (WINS)
- Actúa como un Controlador de Dominio Primario (Primary Domain Controller, PDC) estilo Windows NT®

Lo que Samba no puede hacer:

- Actúa como un BDC para un Windows PDC (y viceversa)
- Actúa como un controlador de dominio de Active Directory

65 http://es.wikipedia.org/wiki/Samba_(programa)

66 http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-samba.html

3.3 DISEÑO

3.3.1 DISEÑO DEL SERVICIO PROXY.

El diseño del servicio Proxy aportará en la preservación de la seguridad de la red a través de un firewall de web. Es decir garantizar que solo aquellas personas autorizadas accedan a un determinado sitio web cada vez que lo requiera.

Además minimizará el riesgo a los cuales está expuesta las redes de la organización tanto en Pifo como en Quito frente a la gran red de Internet. La red de Internet es muy amplia y las posibilidades de enfrentar problemas causados por cualquier tipo de virus son cada vez mayores.

En la implementación de este servicio se utilizará el firewall de web squid, el cual es un software que facilita el control de acceso web por parte de los usuarios.

Squid mejora la seguridad de la red permitiendo la configuración de listas de control de acceso a determinados sitios web dependiendo de las necesidades de cada usuario, esto ayudará a terminar con el mal uso y abuso del recurso de Internet.

Este diseño se aplicará a los dos servidores.

3.3.1.1 Esquema de la solución propuesta servicio PROXY.

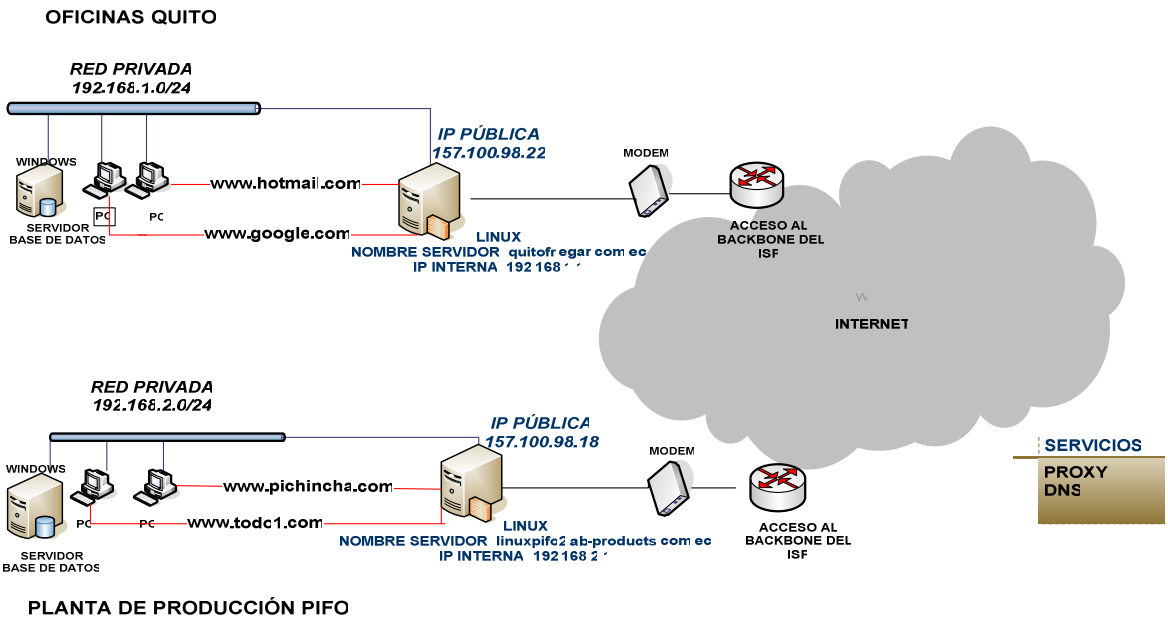

FIGURA 3. 2: ESQUEMA DE LA SOLUCIÓN PROPUESTA SERVICIO PROXY
ELABORADO POR: DAVID FREIRE

3.3.2 DISEÑO DEL SERVICIO DE CORREO ELECTRÓNICO

El diseño del servicio de Correo Electrónico tiene como objetivo ayudar a garantizar la disponibilidad de la mensajería en la organización. Además, minimizará los riesgos de seguridad a los cuales está expuesto el servidor de correo y la red local debido a la gran cantidad de spam y virus informáticos que circulan a través del correo electrónico.

Se configurará dos servidores de correo ubicados en Quito y Pifo respectivamente.

El software a ser utilizado como servidor smtp será sendmail, un software estable y de buen rendimiento.

El diseño del servicio de Correo Electrónico constará de dos partes:

- Diseño Primario
- Diseño Secundario.

3.3.2.1 Diseño Primario

El diseño del proyecto en su primera etapa estará en capacidad de enviar y recibir correo electrónico por medio del servidor smtp.

Se configurará al servidor ubicado en Quito de tal manera que reciba todo el correo que es dirigido a la empresa, y actuará como un mail gateway para el correo que es dirigido a Pifo esto es el correo recibido que sea destinado al dominio ab-products.com.ec lo reenviará de manera directa hacia el servidor ubicado en Pifo.

Ambos servidores estarán en la capacidad de enviar correo de manera independiente.

Para realizar la entrega de correo a los usuarios finales se utilizará dovecot, un software que gestiona por medio del protocolo POP3 la descarga de mensajes.

3.3.2.2 Diseño Secundario

Una vez configurados ambos servidores se procederá con la instalación de una aplicación antivirus y antispam. Para esta tarea se utilizará el software MailScanner

como un intermediario entre el correo entrante y las aplicaciones antivirus y antispam.

Además del software MailScanner se configurará técnicas avanzadas de seguridad contra la entrada de virus y spam directamente en el servidor sendmail.

También se instalará un Webmail, necesario para poder visualizar el correo por medio de la web en cualquier parte del mundo.

El software a ser utilizado para esta aplicación será Squirrelmail con una interfaz parecida a Outlook 2003, lo que permitirá mayor facilidad en la gestión del correo por parte del usuario.

3.3.2.3 Esquema de la solución propuesta Servicio de Correo Electrónico.

A continuación se describen las diferentes situaciones que podrían presentarse en el servicio de correo electrónico:

- Situación Normal de funcionamiento.

  El servidor en Quito estará en la capacidad de recibir el correo electrónico de toda la organización (líneas rojas y líneas azules), el correo dirigido al dominio egar.com.ec lo almacenará en los respectivos INBOX del servidor, mientras que el correo dirigido al dominio ab-products.com.ec lo reenviará de manera directa al servidor ubicado en Pifo (líneas verdes).

  De igual manera un usuario de la empresa podrá visualizar su correo en cualquier lugar donde se encuentre mediante una aplicación web instalada en el servidor como squirrelmail.

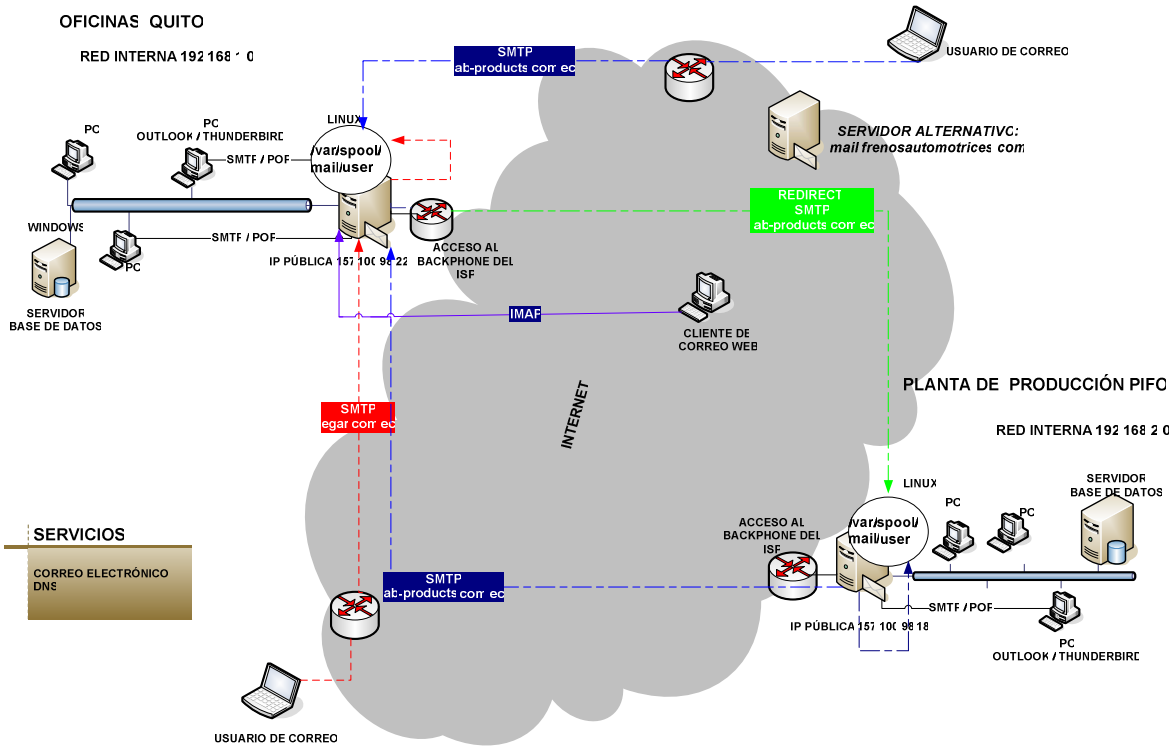

FIGURA 3. 3: ESQUEMA NORMAL DE FUNCIONAMIENTO DEL CORREO ELECRÓNICO
ELABORADO POR: DAVID FREIRE

- Funcionamiento del Servidor de Correo Alternativo (mail.frenosautomotrices.com).
  - FASE 1:

  La utilidad del mail exchanger alternativo consistirá en tener la capacidad de recibir y almacenar temporalmente todo el correo de la organización cuando por un motivo de fuerza mayor el servidor ubicado en Quito no esté en la capacidad de hacerlo, estos motivos pueden ser por mantenimiento, corte prologando de energía electrica o suspensión del servicio de Internet etc.

  De esta manera se garantiza que dada una eventualidad el correo externo no se pierda y funcione la mensajería interna tanto en Pifo como en Quito.

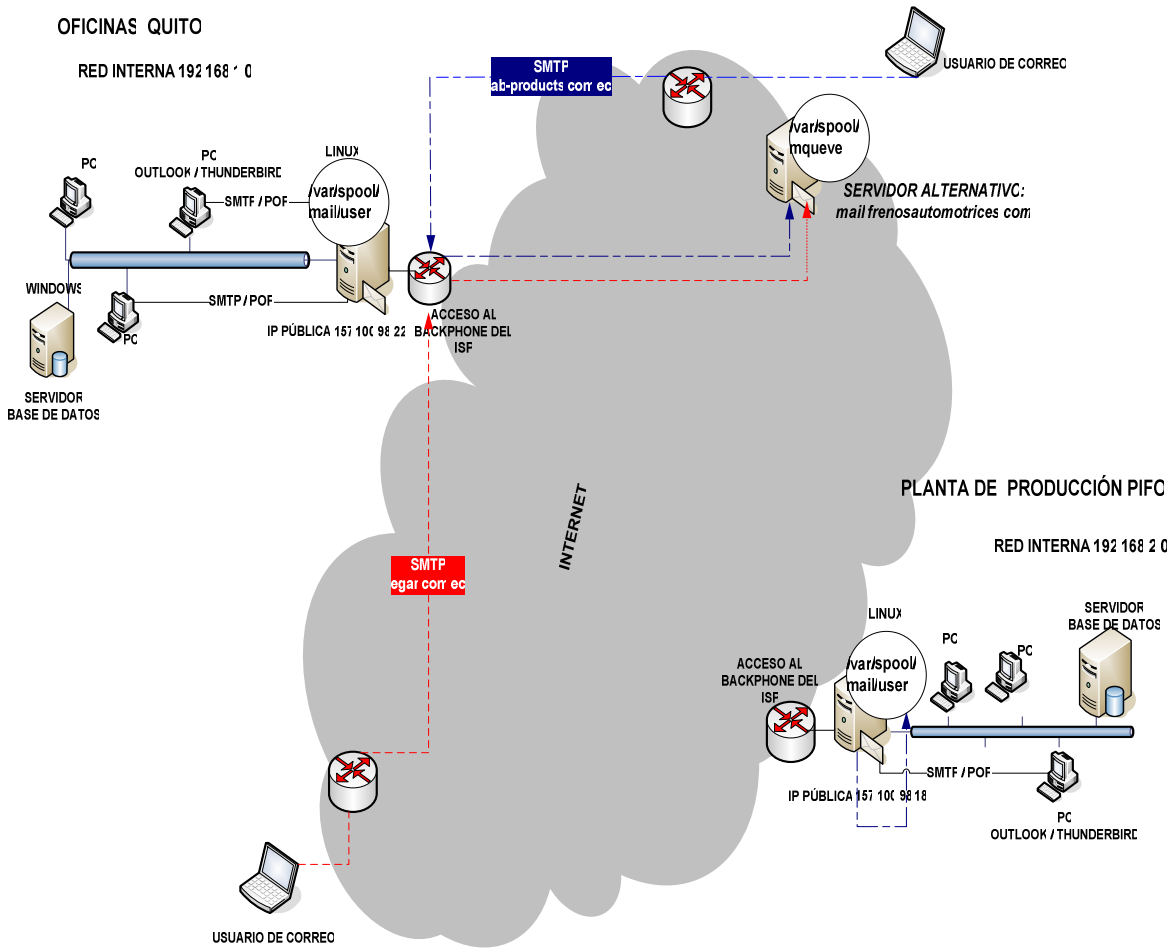

FIGURA 3. 4: FUNCIONAMIENTO DEL MAIL EXCHANGER ALTERNATIVO
ELABORADO POR: DAVID FREIRE

El mail exchanger alternativo realizará repetitivos intentos de conexión hacia el servidor en Quito para enviar el correo que esté almacenado temporalmente.

Para lograr esto es necesario configurar en los DNS princiales al servidor mail.frenosautomotrices.com como servidor alternativo de correo. El manejo del DNS principales es manejado por el proveedor de Internet dueño de las IP públicas 157.100.98.22 y 157.100.98.18

- Fase 2:

Cuando se reestablece el funcionamiento del servidor de Quito, el mail exchanger alternativo eviará todo el correo que tenga almacenado.

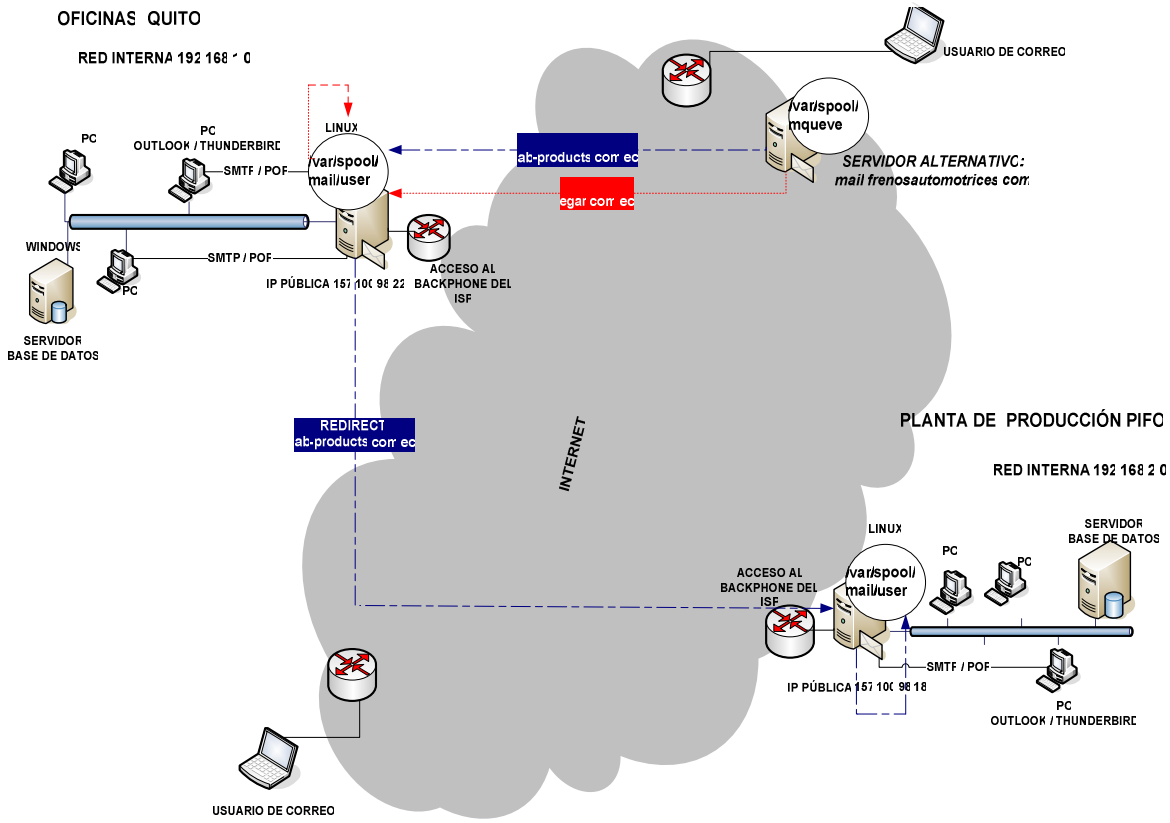

FIGURA 3. 5: FUNCIONAMIENTO DEL MAIL EXCHANGER ALTERNATIVO
ELABORADO POR: DAVID FREIRE

3.3.3 DISEÑO DEL SERVICIO SAMBA

El diseño tiene como objetivo el respaldo automático de información de los usuarios, sistema contable y declaraciones al SRI.

El proceso consistirá en que el servidor samba se conecte a cada máquina bajo plataforma Windows y respalde la información realizando una compresión y anexando la fecha de respaldo. La conexión se realizará por medio de montaje de unidades de red.

Este respaldo se hará de manera automática y en fechas y horas preestablecidas.

Los respaldos a realizar corresponden a:

- Respaldos de información de usuarios.
- Respaldos del Sistema Contable de la empresa.
- Respaldo de declaraciones al SRI.

CAPÍTULO IV

4. IMPLEMENTACIÓN

4.1 INTRODUCCIÓN

En este capítulo se procederá a realizar la respectiva implementación de cada uno de los paquetes necesarios para proveer los servicios de Correo electrónico, Proxy y Samba.

Aquí se detallan los procedimientos de instalación, configuración y pruebas de funcionalidad de los servicios especificados en el diseño.

4.2 OBJETIVO

Mantener un adecuado control de cada uno de los procedimientos de instalación y configuración para la implementación de los servicios de Correo electrónico, Proxy y Samba.

4.3 MODO DE OPERACIÓN

El presente proyecto está elaborado de modo que sean comprendidos por personas con conocimientos básicos de administración de servidores Linux.

En este proyecto se adjuntan ciertas explicaciones necesarias para comprender de mejor manera las configuraciones que se realizarán en la implementación de este proyecto.

La implementación de cada servicio está desarrollada en el ámbito de la descripción de los procesos de instalación, configuración de los diferentes archivos, de las pruebas de funcionalidad y también de los criterios de mantenimiento de los servicios.

La configuración de cada uno de los servicios se aplicará de igual manera a los servidores de quito y pifo.

Es importante que el lector respete rigurosamente los comandos que son ejecutados en la consola para realizar las respectivas configuraciones.

El formato general de comandos será el siguiente:

```
[root@quitofr ~]# rpm -q squid
```

El formato general de ubicación de los archivos será el siguiente:

```
[root@quitofr ~]# cd /mnt/respaldar/
```

4.4 INSTALACIÓN Y CONFIGURACIÓN DE CENTOS.

- La instalación y configuración inicial de Centos se detalla en el ANEXO INSTALACIÓN DEL SISTEMA OPERATIVO.

4.5 IMPLEMENTACIÓN DE UN REPOSITORIO YUM

4.5.1CREACIÓN DE UN REPOSITORIO YUM PARA CENTOS

- Instalación del repositorio dagwieers (http://dag.wieers.com/)

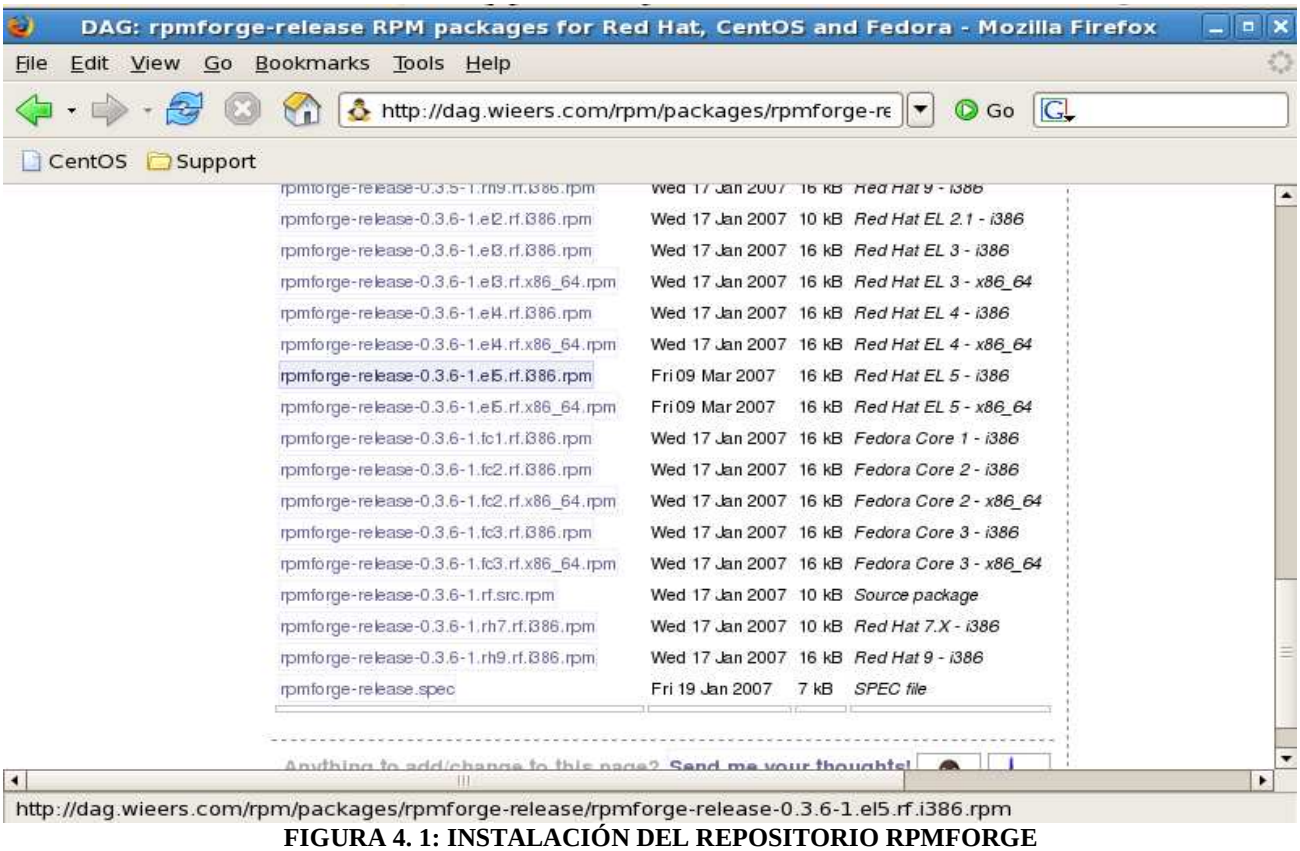

FIGURA 4. 1: INSTALACIÓN DEL REPOSITORIO RPMFORGE

- YUM es una herramienta utilizada para la instalación, actualización de paquetes rpm.

  Para esto utilizan repositorios en Internet que contienen paquetes para cada distribución.

- Escoger el rpm que corresponda la distribución en uso en este caso para centos 5 será rpmforge-release-0.3.6-1.el5.rf.i386.rpm.El link de descarga será:

http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-.3.6.1.el5.rf.i386.rpm

- Descarga del rpm directamente desde el sitio dagwieers.com

```
[root@quitofr ~]# wget http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-0.3.6
-1.el5.rf.i386.rpm
```

- Comprobar la descarga del paquete rpmforge-release-0.3.6-1.el5.rf.i386.rpm

```
[root@quitofr ~]# ls
anaconda-ks.cfg  fetch.txt  install.log         rpmforge-release-0.3.6-1.el5.rf.i386.rpm
Desktop          hosts      install.log.syslog
[root@quitofr ~]#
```

- Instalación del repositorio rpmforge.
  - La instalación del repositorio yum consiste en la creación de una llave pública necesaria para la descarga de paquetes desde el repositorio dagwieers.

```
[root@quitofr ~]# rpm -Uvh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
warning: rpmforge-release-0.3.6-1.el5.rf.i386.rpm: Header V3 DSA signature: NOKEY, key ID 6b8c
6
Preparing...                ########################################### [100%]
   1:rpmforge-release       ########################################### [100%]
[root@quitofr ~]#
```

- Comprobación de la creación del repositorio rpmforge. Para esto verificar que en el directorio /etc/yum.repos.d/ se han creado los archivos mirros-rpmforge y rpmforge.repo

```
[root@quitofr ~]# cd /etc/yum.repos.d/
[root@quitofr yum.repos.d]# ls
CentOS-Base.repo  CentOS-Media.repo  mirrors-rpmforge  rpmforge.repo
[root@quitofr yum.repos.d]#
```

4.6 IMPLEMENTACIÓN DEL SERVICIO PROXY

4.6.1 REVISIÓN DE LOS PAQUETES NECESARIOS

- Revisar si el paquete squid se encuentra instalado.

```
[root@quitofr ~]# rpm -q squid
squid-2.6.STABLE6-3.el5
[root@quitofr ~]#
```

  - ❖ El paquete squid viene por defecto instalado con la instalación de Centos en modo servidor Apache.

4.6.2 OPCIONES DE INSTALACIÓN

  - ❖ Las opciones de instalación se aplicarán en el caso de que el paquete no se encuentre instalado.

- Por Yum

```
[root@quitofr ~]# yum -y install squid
```

- Mediante los CD's de Instalación de Centos 5.0
  - ➢ Insertar el CD #2 de Centos 5.0 y Montar la Unidad de CDROM en el directorio /media/

```
[root@quitofr ~]# mount /dev/hda /media
```

  - ➢ Ir al directorio CentOs que se encuentra dentro de la unidad montada /media/

```
[root@quitofr ~]# cd /media/CentOs
```

  - ➢ Instalar el paquete squid-2.6.STABLE6-3.el5.i386.rpm

```
root@quitofr CentOs]# rpm -ivh squid-2.6.STABLE6-3.el5.i386.rpm
```

4.6.3 CONFIGURACIÓN DE SQUID

- Editar el archivo de configuración principal de squid.

```
[root@quitofr ~]# vi /etc/squid/squid.conf
```

```
#
#        WELCOME TO SQUID 2.6.STABLE6
#        ----------------------------
#
#        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 [options]
#                hostname:port [options]
#                1.2.3.4:port [options]
#
#        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, 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, you
#        probably want to listen on port 80 also, or instead.
#
#        The -a command line option will override the *first* port
"squid.conf.back" 4325L, 148129C
```

- El archivo principal de configuración de SQUID es bastante extenso, y tiene muchas opciones de configuración de acuerdo a las necesidades de cada organización. Por tal motivo se creará un nuevo archivo de configuración con las opciones requeridas para este proyecto.

- Previamente se procederá a realizar un respaldo del archivo de configuración original.

```
[root@quitofr squid]# mv squid.conf squid.conf.back
```

- Creación de un nuevo archivo de configuración.

```
[root@quitofr ~]# vi /etc/squid/squid.conf
```

- Parámetros a configurar.

  - Establecer dirección y puerto por el cual squid va a atender peticiones
  - Especificar en que directorio se van a guardar los logs del squid
  - Determinar *acl* (condiciones que revisará squid) y las acciones a tomar si se cumplen estas condiciones. (*https_access*)

```
http_port 192.168.1.1:3128

cache_mem 128 MB

cache_dir ufs /var/spool/squid 128 16 32

access_log /var/log/squid/access.log squid


request_body_max_size 50 MB


ftp_user juvi@andinanet.net

#ftp_passive on

acl manager proto cache_object
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl 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 Safe_ports port 6801        # net2phone

acl CONNECT method CONNECT

acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl nohttps src "/etc/squid/nohttps"
acl redlocal src "/etc/squid/permitidos"
acl sitiospermitidos url_regex "/etc/squid/sitiospermitidos"
acl https  src "/etc/squid/https"
acl sitiosnegados url_regex "/etc/squid/negados"

http_access allow localhost
http_access deny sitiosnegados
http_access deny CONNECT !https !sitiospermitidos
http_access allow nohttps
http_access allow redlocal sitiospermitidos
http_access deny all


icp_access allow localhost
icp_access allow redlocal
icp_access deny all

cache_mgr ashquim@egar.com.ec
```

- Creación de los archivos definidos en el archivo squid.conf
  - Creación del archivo https

```
[root@quitofr squid]# vi https
```

```
192.168.1.4
192.168.1.7
192.168.1.8
192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
```

    - Las IP's definidas en este archivo tendrán acceso exclusivo a sitios web con conexiones de tipo https.
  - Creación del archivo nohttps

```
root@quitofr squid]# vi nohttps
```

```
192.168.1.4
192.168.1.5
192.168.1.7
192.168.1.8
192.168.1.12
192.168.1.11
192.168.1.13
192.168.1.14
192.168.1.21
192.168.1.33
192.168.1.61
```

    - Las IP's definidas en este archivo tendrán acceso a todo contenido web, pero restringido el acceso a sitios web con conexiones https.
  - Creación del archivo permitidos

```
[root@quitofr squid]# vi permitidos
```

```
192.168.1.2
192.168.1.3
192.168.1.6
192.168.1.17
192.168.1.19
192.168.1.39
```

    - Las IP's definidas en este archivo tendrán acceso solo a ciertas páginas que se definirán más adelante.

- Creación del archivo sitiospermitidos

```
[root@quitofr squid]# vi sitiospermitidos
```

```
http://www.frenosautomotrices.com
http://www.egar.com.ec
http://157.100.98.18/
http://157.100.98.22/webmail
http://www.corpei.org/inde.asp?LN=SP
http://www.ecuador.fedexpor.com/
http://www.sesa.mag.gov.ec
http://www.todo1.com
https://www.todo1.com
https://www.todo1.com:443
http://cash.pichincha.com
http://www.andinatel.com
http://www.intermatico.com
http://www.bancodelpacifico.com
http://www.bancobolivariano.com
https://www.bancobolivariano.com:443
http://www.sri.gov.ec/
http://www.iess.gov.ec
https://facturacion.pichincha.com/cashm/frames.asp
https://facturacion.pichincha.com/cashm
http://www.bp.fin.ec/Directorio/publico/default.asp
http://www.bancobanco.ec/FondosReservaCompania/SolicitarFRCompania.do
http://www.bancobanco.ec/FondosReserva/SolicitudFR.do
http://www.bancobanco.ec/FondosReserva/ConsultaFR.do
http://www.bolivariano.com/main.asp?
http://www.corpei.org
http://sri.gov.ec
http://bancodelpacifico.com
http://bancobolivariano.com
http://pichincha.com
http://www.aduana.gov.ec
http://www.supercias.gov.ec
http://www.pacificard.com.ec
http://sice1.aduana.gov.ec/ied/workflow/logon.jsp
http://sice1.aduana.gov.ec/ied/servlet/workf.servlets.com.workfSLogin
http://sice1.aduana.gov.ec/ied/workflow/index.jsp
http://sice1.aduana.gov.ec/ied/workflow/frame_principal.jsp?
http://www.iess.gov.ec
http://www.pacifictel.net/
http://saldos.pacifictel.net.ec/pacifictel
http://elcomercio.terra.com.ec/
http://www.supercias.gov.ec/
http://www.superban.gov.ec/
http://www.superban.gov.ec:443
http://www.corpei.org
http://www.corpei.org/certificados
http://www.corpei.org/FrameCenter.asp?Ln=SP&Opcion=1_3_4
http://intranet.corpei.ec/eCert/index.php
http://intranet.corpei.ec/eCert/cert_i00.html
http://intranet.corpei.ec/eCert/cert_i01a.php
http://www.corpei.org/
```

- En este archivo se listan sitios web a los cuales podrán acceder las IP's definidas en el archivo permitidos.
- Se incluyen sitios web necesarios con conexión https tales como bancos, sitios gubernamentales que podrán ser accedidas también por las IP's definidas en el archivo nohttps.

➢ Creación del archivo negados

```
[root@quitofr squid]# vi negados
hi5
www.amigos.com
musicmatch
audiogalaxy
```

- Con este archivo se bloquea el acceso a páginas web que en su url contienen cualquiera de las palabras definidas en este archivo, ej. Se negará el acceso a www.hi5.com.

▪ Asociar cada IP de la red con el respactivo hostname por medio del archivo hosts.

```
[root@quitofr ~]# cd /etc/
[root@quitofr etc]# vi hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost.localdomain   localhost
192.168.1.1     quitofr.egar.com.ec     quitofr.ab-products.com.ec
157.100.98.21   gateway.egar.com.ec     gateway
192.168.1.3     puentej.egar.com.ec      puentej
192.168.1.4     basantef.egar.com.ec    basantef
192.168.1.5     bedoyal.egar.com.ec     bedoyal
192.168.1.6     bahamondet.egar.com.ec  bahamondet
192.168.1.7     garridom.egar.com.ec    garridom
192.168.1.8     garridoc.egar.com.ec    garridoc
192.168.1.10    duquea.egar.com.ec      duquea
192.168.1.11    freired.egar.com.ec     freired
192.168.1.12    malenag.egar.com.ec     malenag
192.168.1.13    albornoza.egar.com.ec   albornoza
192.168.1.14    andradee.egar.com.ec    andradee
192.168.1.17    zambranol.egar.com.ec   zambranol
192.168.1.19    cardenasc.egar.com.ec   cardenasc
192.168.1.21    ashquim.egar.com.ec     ashquim
192.168.1.20    salajuntas.egar.com.ec  sala
192.168.1.61    fgarcia.egar.com.ec     invitado
192.168.1.33    cuevajs.egar.com.ec     cuevajs
192.168.1.40    chamorrog.egar.com.ec   chamorrog
```

4.6.4 INICIAR EL SERVICIO

- Inicio del servicio

```
[root@quitofr squid]# cd
[root@quitofr ~]# service squid start
Starting squid: .                                          [  OK  ]
[root@quitofr ~]# chkconfig --level 2345 squid on
[root@quitofr ~]#
```

  - ❖ Con el parámetro chkconfig squid on se le indica al sistema que el servicio se inicie automáticamente cada vez que se levante el sistema.

4.6.5 PRUEBAS DE FUNCIONALIDAD DESDE UNA MÁQUINA WINDOWS XP

- ❖ Las pruebas de funcionalidad se realizarán con un usuario cuya máquina tiene un sistema operativo Windows XP y su IP es 192.168.1.11

- Configuración de la IP 192.168.1.11 en Windows XP.

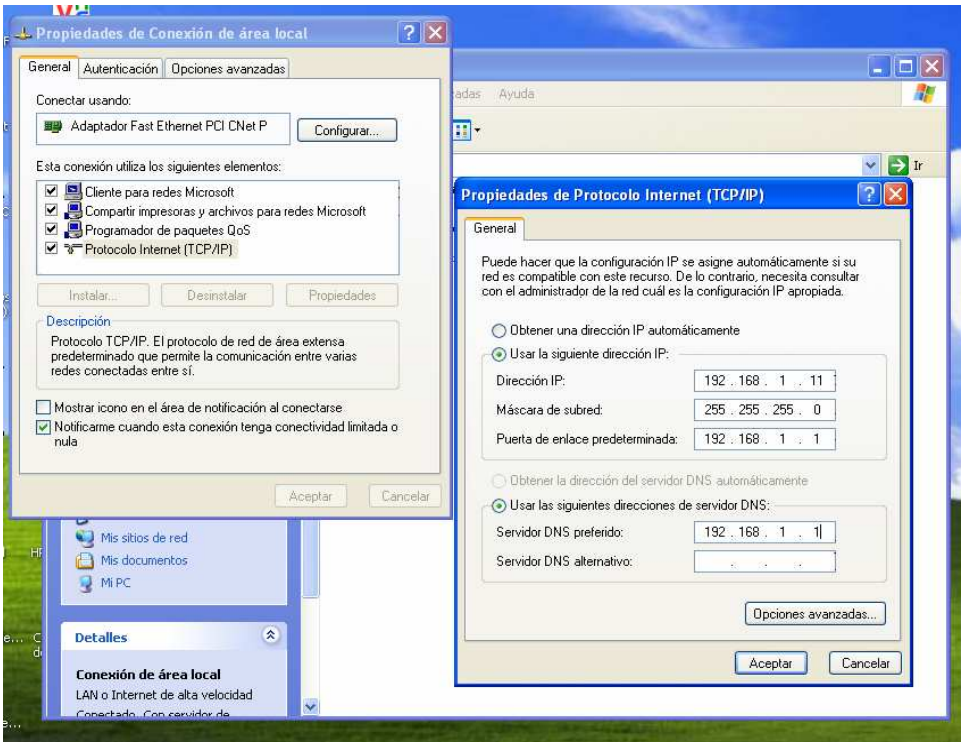

FIGURA 4. 2: CONFIGURACIÓN DE RED EN WINDOWS XP

- Configuración de Internet Explorer para que salga por el puerto 3128 del squid.

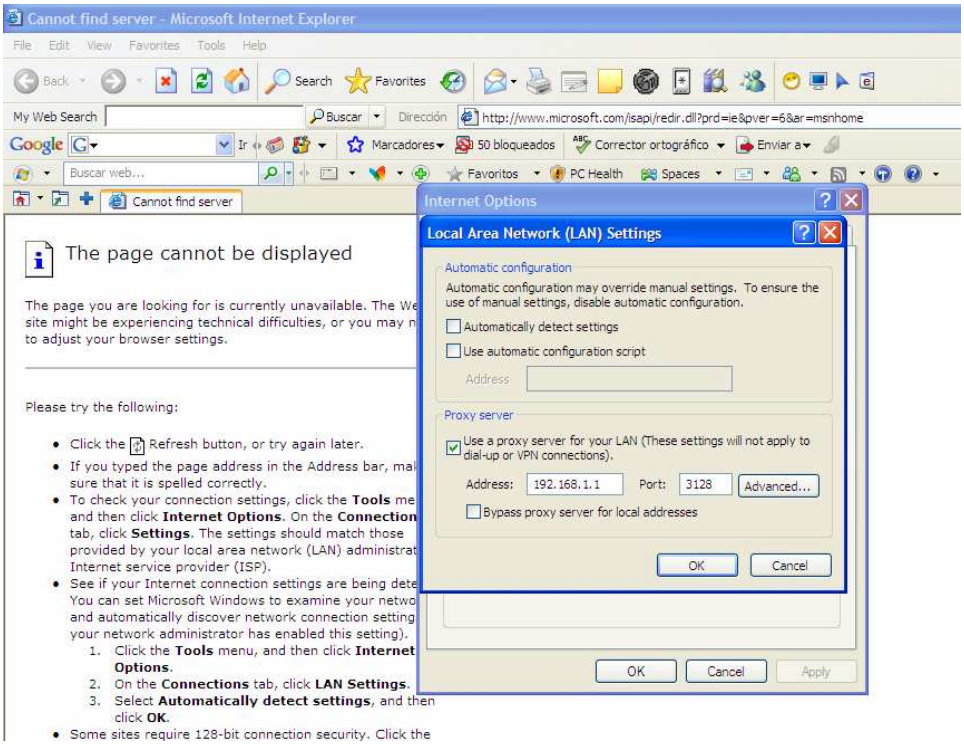

FIGURA 4. 3: CONFIGURACIÓN DEL PROXY EN INTERNET EXPLORER

- Pruebas como IP listada solo en el archivo nohttps.

```
[root@quitofr squid]# vi nohttps

192.168.1.4
192.168.1.7
192.168.1.8
#192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14

[root@quitofr squid]# vi https

192.168.1.4
192.168.1.5
192.168.1.7
192.168.1.8
192.168.1.12
192.168.1.11
192.168.1.13
192.168.1.14
192.168.1.21
192.168.1.33
192.168.1.61
```

```
[root@quitofr ~]# service squid reload
[root@quitofr ~]#
```

- Procedimiento realizado:
  - Editar el archivo https y comentar con # la línea correspondiente a la IP 192.168.1.11
  - Comprobar que en el archivo nohttps se encuentre listada la IP 192.168.1.11
  - Recargar el servicio para que los cambios tengan efecto.

- Intento de acceso a *www.hotmail.com* desde Internet Explorer.

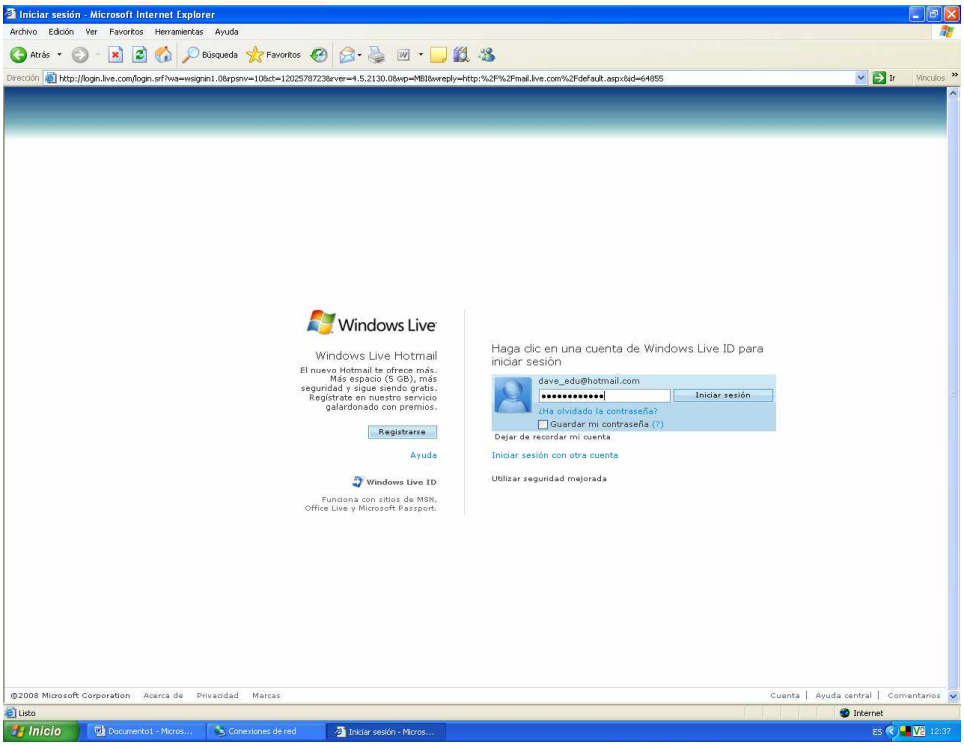

FIGURA 4. 4: INGRESO A CORREO DE HOTMAIL

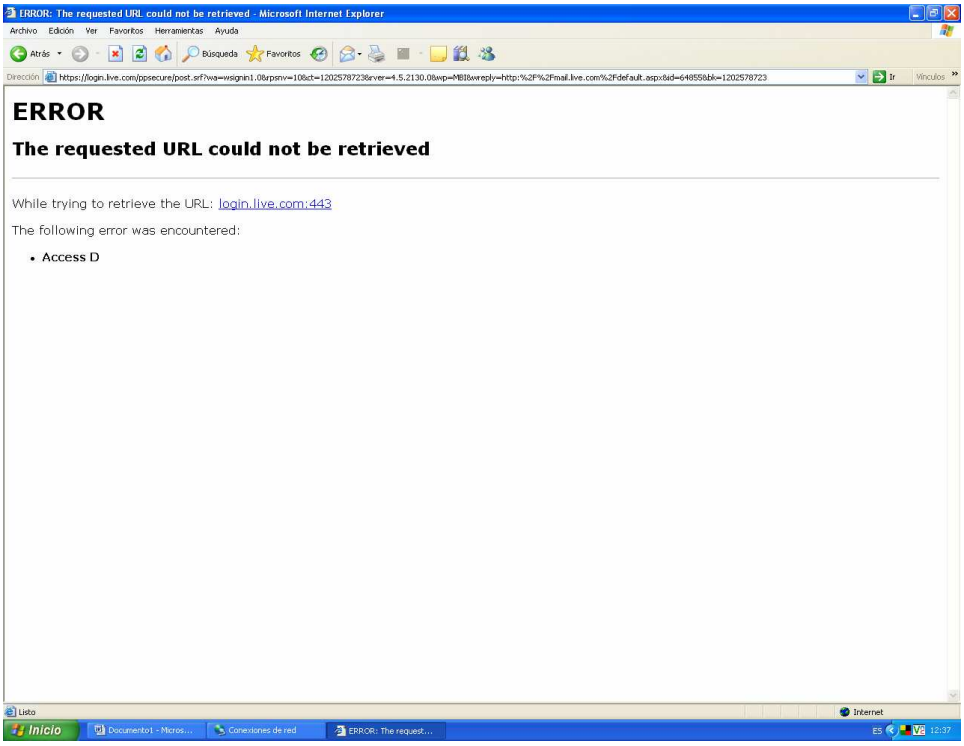

FIGURA 4. 5: ACCESO DENEGADO AL CORREO DE HOTMAIL

- Acceso a *www.google.com*

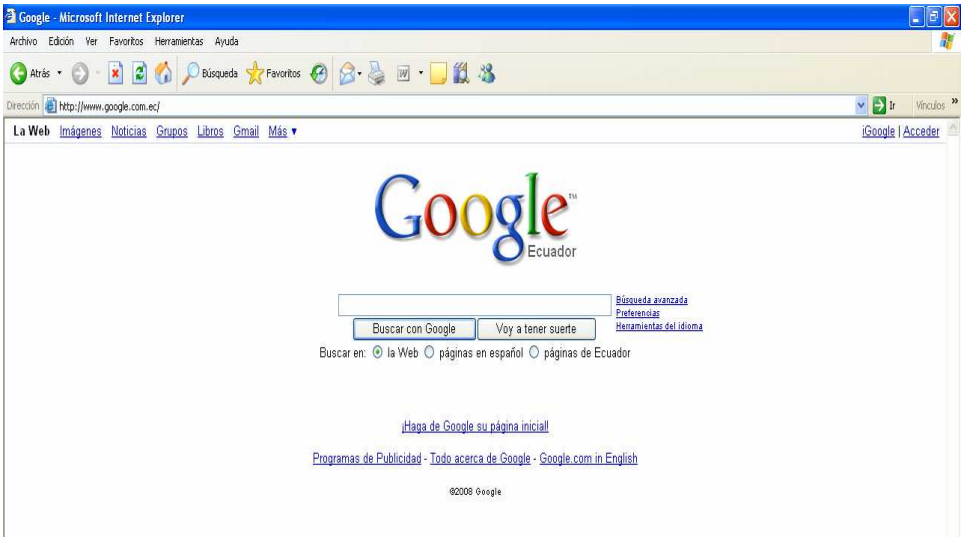

FIGURA 4. 6: ACCESO A LA PÁGINA www.goole.com

- El usuario de Windows XP cuya IP se encuentra listado en el archivo nohttps, pudo acceder a *www.google.com* sin embargo se restringió el acceso a *www.hotmail.com* puesto que es un sitio que establece una conexión de tipo HTTPS.

- Pruebas con la IP 192.168.1.11 listada solo en el archivo permitidos

```
[root@quitofr ~]# vi /etc/squid/permitidos

192.168.1.2
192.168.1.3
192.168.1.6
192.168.1.17
192.168.1.19
192.168.1.39
192.168.1.11
```

```
[root@quitofr squid]# vi nohttps

192.168.1.4
192.168.1.7
192.168.1.8
#192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
192.168.1.5
192.168.1.21
192.168.1.33
 192.168.1.61
```

```
[root@quitofr squid]# vi https

192.168.1.4
192.168.1.7
192.168.1.8
#192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
```

```
[root@quitofr ~]# service squid reload
[root@quitofr ~]#
```

- Procedimiento realizado.

  - Se aumenta la IP 192.168.1.11 en el archivo permitidos, se comenta la IP 192.168.11 de los archivos nohttps y https.
  - Se recarga el servicio para que los cambios tengan efecto.

- Acceso a www.google.com desde Internet Explorer.

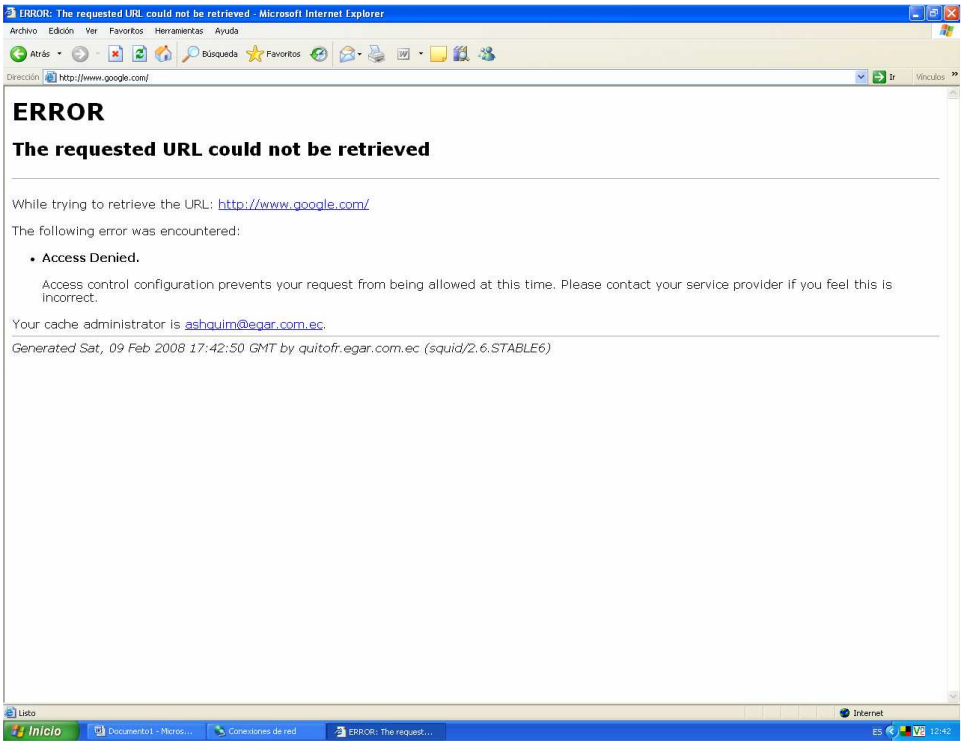

FIGURA 4. 7: ACCESO DENEGADO A LA PÁGINA www.google.com

- Acceso a *www.todo1.com* sitio listado en el archivo sitiospermitidos

FIGURA 4. 8: ACCESO A LA PÁGINA www.todo1.com

- Al usuario de Windows XP cuya IP 192.168.1.11 se encuentra listado en el archivo permitidos, no pudo acceder a *www.google.com*, sin embargo accedió al sitio www.todo1.com que se encuentra listado en el archivo de sitiospermitidos.

- Pruebas con IP 192.168.1.11 listada en archivo https y nohttps

```
[root@quitofr squid]# vi https
```

```
192.168.1.4
192.168.1.7
192.168.1.8
192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
```

```
[root@quitofr squid]# vi nohttps

192.168.1.4
192.168.1.5
192.168.1.7
192.168.1.8
192.168.1.12
192.168.1.11
192.168.1.13
192.168.1.14
192.168.1.21
192.168.1.33
192.168.1.61


[root@quitofr ~]# service squid reload
[root@quitofr ~]#
```

- Procedimiento realizado:
  - Descomentar la IP 192.168.1.11 de los archivos https y nohttps.
  - Recargar el servicio para que los cambios tengan efecto.

- Acceso a *www.google.com*

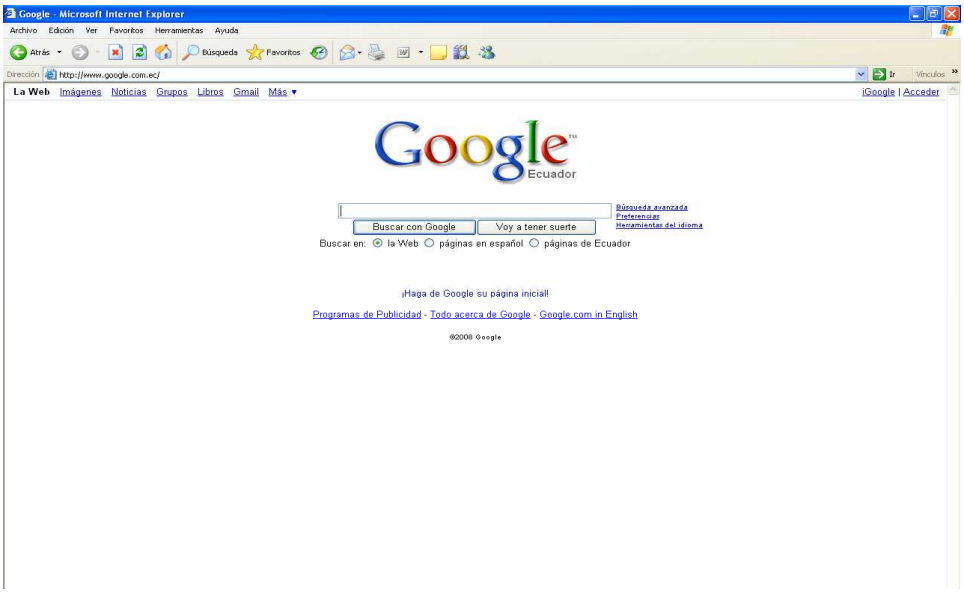

FIGURA 4. 9: ACCESO A LA PÁGINA www.google.com

- Acceso a *www.hotmail.com*

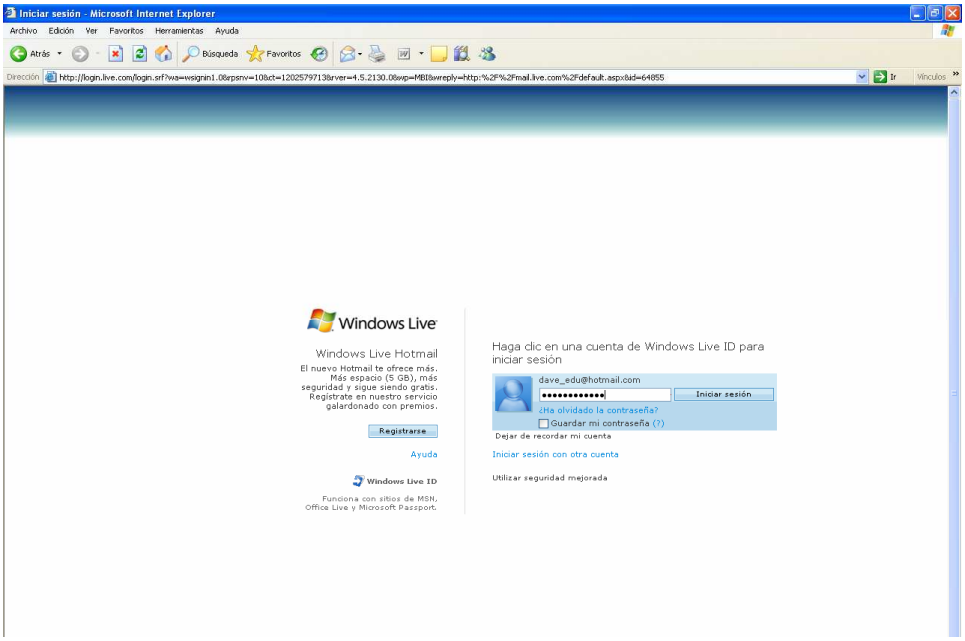

FIGURA 4. 10: INTENTO DE ACCESO A LA PÁGINA www.hotmail.com

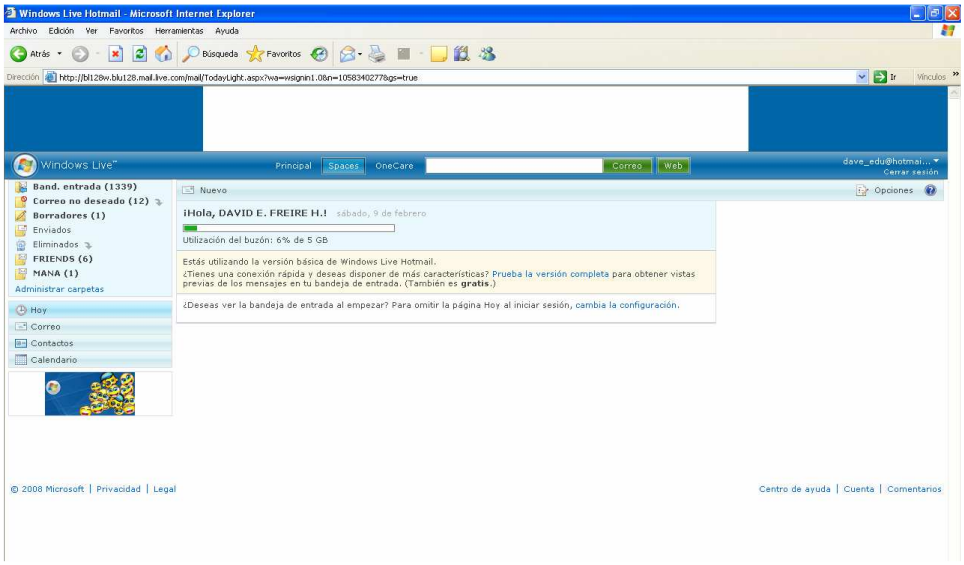

FIGURA 4. 11: VISUALIZACIÓN DEL CORREO ELETRÓNICO DE HOTMAIL

- Intento de acceso a *www.hi5.com*

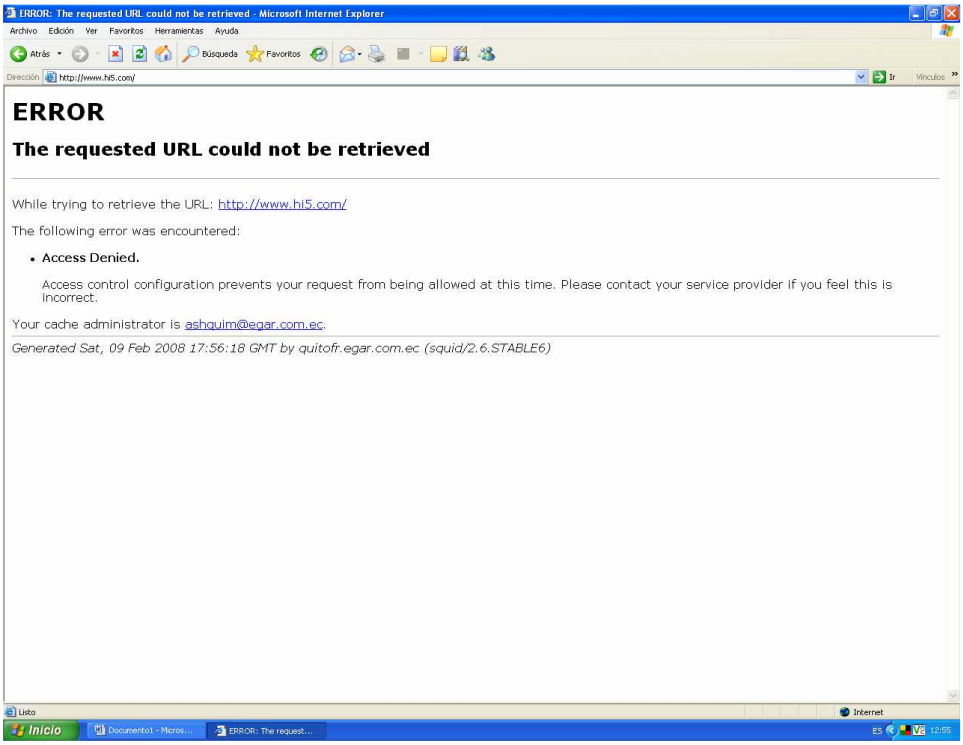

FIGURA 4. 12: ACCESO DENEGADO A LA PÁGINA www.hi5.com

- Al usuario de Windows XP cuya IP 192.168.1.11 se encuentra listado en el archivo https y nohttps accedió a www.google.com, inició sesión en www.hotmail.com, sin embargo se bloqueó el acceso a www.hi5.com.

- Prueba con una IP 192.168.1.55 que no está listada en ninguno de los archivos anteriormente mencionados (https, nohttps, permitidos).

  - Se configurará la máquina con Windows XP con la IP 192.168.1.55, la prueba consiste que en el momento de abrir internet Explorer se deniegue el acceso a la página de inicio que tenga configurada en este caso será *www.frenosautomotrices.com*

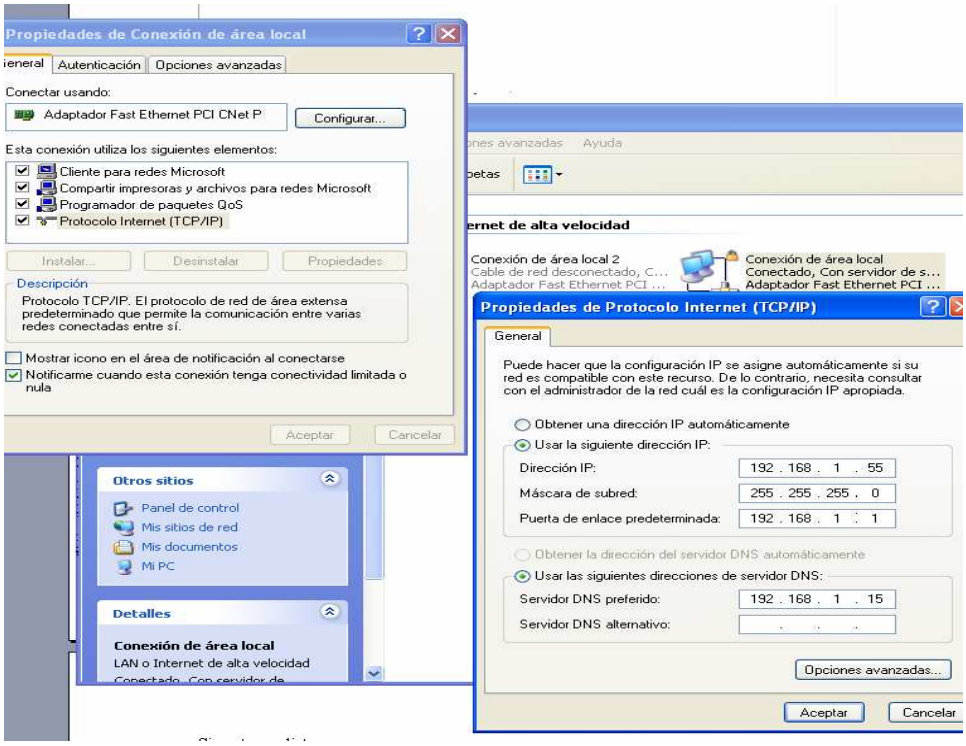

FIGURA 4. 13: CONFIGURACIÓN DE RED EN WINDOWS XP

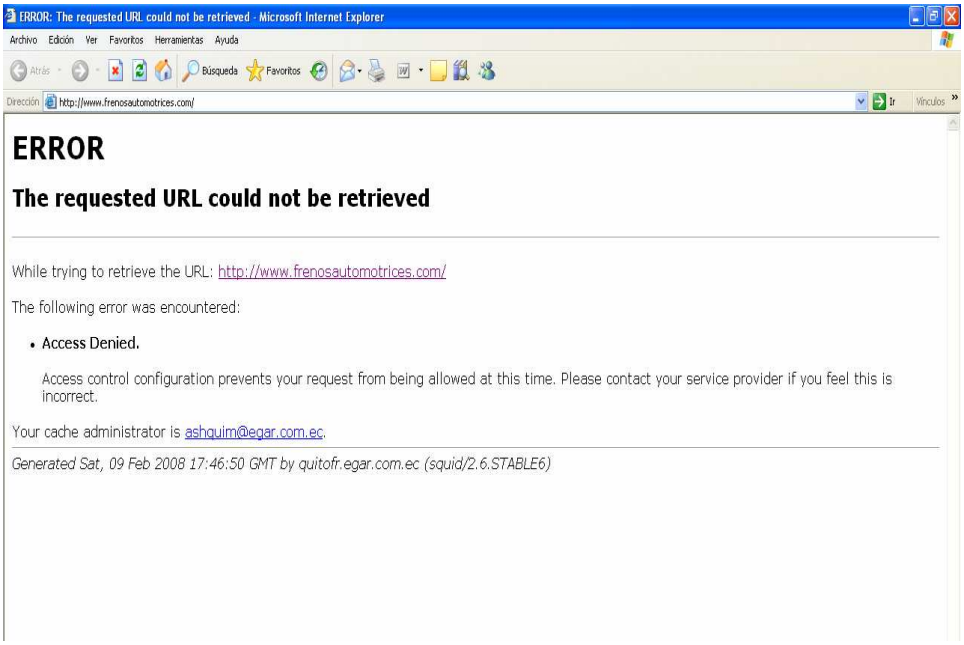

FIGURA 4. 14: ACCESO DENEGADO A LA PÁGINA www.frenosautomotrices.com

4.7 IMPLEMENTACIÓN DEL SERVICIO DE CORREO ELECTRÓNICO

4.7.1 IMPLEMENTACIÓN DISEÑO PRIMARIO

4.7.1.1 Implementación de DNS INTERNO

4.7.1.1.1 Instalación de los paquetes necesarios

- Instalación por yum del paquete caching-nameserver

```
[root@quitofr ~]# yum -y install caching-nameserver


Transaction Summary
================================================================================
Install      1 Package(s)
Update       4 Package(s)
Remove       0 Package(s)

Total download size: 2.0 M
Downloading Packages:
(1/5): bind-chroot-9.3.3- 100% |=========================|  39 kB    00:02
(2/5): bind-libs-9.3.3-10 100% |=========================| 838 kB    01:05
(3/5): bind-9.3.3-10.el5. 100% |=========================| 954 kB    01:12
(4/5): bind-utils-9.3.3-1 100% |=========================| 162 kB    00:16
(5/5): caching-nameserver 100% |=========================|  56 kB    00:06
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating  : bind-libs                    ######################### [1/9]
  Updating  : bind                         ######################### [2/9]
  Updating  : bind-chroot                  ######################### [3/9]
  Updating  : bind-utils                   ######################### [4/9]
  Installing: caching-nameserver           ######################### [5/9]
/etc/sysconfig/network: line 4: /root: is a directory
Stopping named: .[  OK  ]
Starting named: [  OK  ]
  Cleanup   : bind-chroot                  ######################### [6/9]
  Cleanup   : bind-libs                    ######################### [7/9]
  Cleanup   : bind                         ######################### [8/9]
  Cleanup   : bind-utils                   ######################### [9/9]

Installed: caching-nameserver.i386 30:9.3.3-10.el5
Dependency Updated: bind.i386 30:9.3.3-10.el5 bind-chroot.i386 30:9.3.3-10.el5 bind-libs.i386 30:9.3.3-10.el5 bind-utils.i386
 30:9.3.3-10.el5
Complete!
[root@quitofr ~]#
```

- La instalación por yum instala el paquete y todas sus dependencias, en este caso se puede observar que a parte de la instalación del paquete *caching-nameserver* se descargan, instalan y actualizan los paquetes *bind-chroot, bind-libs, bind*, todos necesarios para la implementación de un DNS.

- Instalación mediante los CD's de Instalación de Centos 5.0
  Insertar el CD #2 de Centos 5.0 y Montar la Unidad de CDROM en el directorio /media/

```
[root@quitofr ~]# mount /dev/hda /media/
```

  - Ir al directorio CentOs que se encuentra dentro de la unidad montada /media/

```
[root@quitofr ~]# cd /media/CentOs
```

  - Instalar los paquetes bind-chroot-9.3.3-7.el5.i386.rpm y bind-9.3.3-7.el5.i386.rpm

```
[root@quitofr CentOs]# rpm -ivh bind-chroot-9.3.3-7.el5.i386.rpm bind-9.3.3-7.el5.i386.rpm
```

  - Insertar el CD #5 de Centos 5.0 y Montar la Unidad de CDROM

```
[root@quitofr ~]# mount /dev/hda /media/
```

  - Ir al directorio CentOs que se encuentra dentro de la unidad montada /media/

```
[root@quitofr ~]# cd /media/CentOs
```

  - Instalar el paquete caching-nameserver-9.3.3-7.el5.i386.rpm

```
[root@quitofr CentOs]# rpm -ivh caching-nameserver-9.3.3-7.el5.i386.rpm
```

- Comprobar si el paquete caching-nameserver se instaló correctamente.

```
[root@quitofr ~]# rpm -q caching-nameserver
caching-nameserver-9.3.3-10.el5
[root@quitofr ~]#
```

- Comprobar que en el directorio /var/named/chroot/etc/ se han creado los archivos necesarios para la configuración de DNS, estos son:
  - named.caching-nameserver.conf
  - named.rfc1912.zones

```
[root@quitofr ~]# cd /var/named/chroot/etc/
[root@quitofr etc]# ls
localtime  named.caching-nameserver.conf  named.rfc1912.zones  rndc.key
[root@quitofr etc]#
```

nota:

- El directorio /var/named/chroot se crea a partir de la instalación del paquete bind-chroot. Este paquete se instaló automáticamente por yum al momento de instalar el paquete caching-nameserver.
- El directorio /var/named/chroot se crea como medida de seguridad ante una vulneración del servicio DNS.

4.7.1.1.2 Configuración de DNS

- Configuración del puerto y la IP por la que el DNS atenderá peticiones.

```
[root@quitofr ~]# vi /var/named/chroot/etc/named.caching-nameserver.conf
```

```
// named.caching-nameserver.conf
//
// Provided by Red Hat caching-nameserver package to configure the
// ISC BIND named(8) DNS server as a caching only nameserver
// (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// DO NOT EDIT THIS FILE - use system-config-bind or an editor
// to create named.conf - edits to this file will be lost on
// caching-nameserver package upgrade.
//
options {
        listen-on port 53 { 127.0.0.1; 192.168.1.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        query-source    port 53;
        query-source-v6 port 53;
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
view localhost_resolver {
//      match-clients      { localhost; };
//      match-destinations { localhost; };
        recursion yes;
        include "/etc/named.rfc1912.zones";
};
```

- El parámetro a configurar en este archivo será el : *listen on port 53 {127.0.0.1; 192.168.1.1; }*

El puerto por defecto que abre el servicio de DNS es el 53, como medida de seguridad solo atenderá al propio local host y toda petición generada por medio de la interfaz interna (192.168.1.1)

- Determinar las zonas a manejar por el DNS y sus respectivos archivos de configuración.

```
[root@quitofr ~]# vi /var/named/chroot/etc/named.rfc1912.zones

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};

zone "egar.com.ec" IN {
        type master;
        file "egar.com.ec.zone";

};

zone "ab-products.com.ec" IN {
        type master;
        file "ab-products.com.ec.zone";

};

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "1.168.192.in-addr.arpa.zone";
};

zone "98.100.157.in-addr.arpa" IN {
        type master;
        file "98.100.157.in-addr.arpa.zone";
};
```

- Las zonas a manejar por el DNS Interno serán:
  - egar.com.ec
  - ab-products.com.ec

  Además se manejará también los respectivos reversos de DNS de cada zona estos son:
  - 1.168.192.in-addr.arpa
  - 98.100.157.in-addr.arpa.zone

- En cada zona se define mediante el parámetro file el respectivo archivo de configuración.

- Configuración de las zonas definidas en el archivo named.rfc1912.zones
  - ❖ Los parámetros generales a configurar en cada zona serán:

  TTL: Time to live (tiempo de vida) para cada consulta de DNS recibida.

  Serial: Corresponde al número de actualizaciones que ha tenido determinada zona. Generalmente este serial corresponde al ano mes y número secuencial.

  IN MX: Indica el mailexchanger para determinada zona, este record MX vine acompañado de un número cualesquiera para indicarle que es el mailexchanger de mayor prioridad.

  IN A: Especifica un record A para determinada zona, generalmente se asocia en este tipo de record el hostname con la respectiva IP

  IN PTR: Especifica el reverso de DNS de una determinada zona. Generalmente para este tipo de record se asocia el respectivo hostname con el último octeto de si dirección IP.

```
[root@quitofr ~]# cd /var/named/chroot/var/named/
[root@quitofr named]# vi egar.com.ec.zone
```

```
$TTL    86400
@               IN SOA  quitofr.egar.com.ec.  freired.egar.com.ec. (

                                2007110909              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
                IN NS           quitofr.egar.com.ec.

                IN MX   10      quitofr.egar.com.ec.


quitofr                 IN    A    192.168.1.1
```

```
[root@quitofr named]# vi ab-products.com.ec.zone

$TTL    86400

@        IN SOA  linuxpifo2.ab-products.com.ec.  freired.egar.com.ec. (

                                2007110909              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
                IN NS           linuxpifo2.ab-products.com.ec.

                IN MX   10      linuxpifo2.ab-products.com.ec.


linuxpifo2                IN    A    157.100.98.18
```

- Configuración del reverso DNS para la IP 192.168.1.1 definida en el archivo de zona egar.com.ec.zone

```
root@quitofr named]# vi 1.168.192.in-addr.arpa.zone
$TTL    86400
@               IN SOA  quitofr.egar.com.ec.  freired.egar.com.ec. (

                                2007110901              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
                IN NS           quitofr.egar.com.ec.

                IN MX   10      quitofr.egar.com.ec.


1               IN    PTR       quitofr.egar.com.ec.
```

- Configuración del reverso de DNS para la IP 157.100.98.18 definida en el archivo de zona ab-products.com.ec.zone

```
[root@quitofr named]# vi 98.100.157.in-addr.arpa.zone
$TTL    86400
@               IN SOA  quitofr.egar.com.ec.  freired.egar.com.ec. (

                                2007110909              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
                IN NS           quitofr.egar.com.ec.

                IN MX   10      quitofr.egar.com.ec.


18              IN      PTR     linuxpifo2.ab-products.com.ec.
```

4.7.1.1.3 Iniciar servicio DNS

- Inicio del servicio DNS

```
[root@quitofr ~]# service named restart
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]
[root@quitofr ~]#
```

- Revisar los logs del sistema para comprobar que se cargaron correctamente todas las zonas del DNS.

```
Feb 11 13:57:18 quitofr named[5528]: starting BIND 9.3.3rc2 -u named -c /etc/named.caching-namese
rver.conf -t /var/named/chroot
Feb 11 13:57:18 quitofr named[5528]: found 2 CPUs, using 2 worker threads
Feb 11 13:57:18 quitofr named[5528]: loading configuration from '/etc/named.caching-nameserver.co
nf'
Feb 11 13:57:18 quitofr named[5528]: listening on IPv6 interface lo, ::1#53
Feb 11 13:57:18 quitofr named[5528]: listening on IPv4 interface lo, 127.0.0.1#53
Feb 11 13:57:18 quitofr named[5528]: listening on IPv4 interface eth1, 192.168.1.1#53
Feb 11 13:57:18 quitofr named[5528]: command channel listening on 127.0.0.1#953
Feb 11 13:57:18 quitofr named[5528]: command channel listening on ::1#953
Feb 11 13:57:18 quitofr named[5528]: zone 0.in-addr.arpa/IN/localhost_resolver: loaded serial 42
Feb 11 13:57:18 quitofr named[5528]: zone 0.0.127.in-addr.arpa/IN/localhost_resolver: loaded seri
al 1997022700
Feb 11 13:57:18 quitofr named[5528]: zone 98.100.157.in-addr.arpa/IN/localhost_resolver: loaded s
erial 2007110909
Feb 11 13:57:18 quitofr named[5528]: zone 1.168.192.in-addr.arpa/IN/localhost_resolver: loaded se
rial 2007110909
Feb 11 13:57:18 quitofr named[5528]: zone 255.in-addr.arpa/IN/localhost_resolver: loaded serial 4
2
Feb 11 13:57:18 quitofr named[5528]: zone 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
.0.0.ip6.arpa/IN/localhost_resolver: loaded serial 1997022700
Feb 11 13:57:18 quitofr named[5528]: zone ab-products.com.ec/IN/localhost_resolver: loaded serial
 2007110909
Feb 11 13:57:18 quitofr named[5528]: zone egar.com.ec/IN/localhost_resolver: loaded serial 200711
0909
Feb 11 13:57:18 quitofr named[5528]: zone localdomain/IN/localhost_resolver: loaded serial 42
Feb 11 13:57:18 quitofr named[5528]: zone localhost/IN/localhost_resolver: loaded serial 42
Feb 11 13:57:18 quitofr named[5528]: running
```

- Indicar al sistema operativo la dirección de DNS a utilizar
  - El DNS principal del sistema será el propio DNS configurado (192.168.1.1)

```
[root@quitofr ~]# vi /etc/resolv.conf

nameserver 192.168.1.1
```

- Reiniciar el servicio de red.

```
[root@quitofr ~]# service network start
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Bringing up interface eth1:                                [  OK  ]
[root@quitofr ~]#
```

4.7.1.1.4 Pruebas de funcionalidad de DNS

- Ping a google.com para comprobar que el DNS principal funcione correctamente en la resolución de nombres.

```
[root@quitofr ~]# ping google.com
PING google.com (64.233.167.99) 56(84) bytes of data.
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=2 ttl=237 time=119 ms
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=4 ttl=237 time=111 ms
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=5 ttl=237 time=113 ms
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=6 ttl=237 time=121 ms
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=7 ttl=237 time=119 ms
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=8 ttl=237 time=119 ms
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=10 ttl=237 time=112 ms
64 bytes from py-in-f99.google.com (64.233.167.99): icmp_seq=11 ttl=237 time=119 ms
```

- Verificación por medio de la herramienta nslookup.
  - La herramienta nslookup permite realizar consultas por diversos tipos de records DNS.

  En este caso con el parámetro set type=any se especifica que se realizará consultas por cualquier tipo de record. Como respuesta se obtendrá para un determinado dominio su respectivo mail exchanger.

```
[root@quitofr ~]# nslookup
> set type=any

> egar.com.ec
Server:         192.168.1.1
Address:        192.168.1.1#53

egar.com.ec
        origin = quitofr.egar.com.ec
        mail addr = freired.egar.com.ec
        serial = 2007110909
        refresh = 10800
        retry = 900
        expire = 604800
        minimum = 86400
egar.com.ec     nameserver = quitofr.egar.com.ec.
egar.com.ec     mail exchanger = 10 quitofr.egar.com.ec.
```

  - Se realiza la consulta por el dominio egar.com.ec.

```
> ab-products.com.ec
Server:         192.168.1.1
Address:        192.168.1.1#53

ab-products.com.ec
        origin = linuxpifo2.ab-products.com.ec
        mail addr = freired.egar.com.ec
        serial = 2007110909
        refresh = 10800
        retry = 900
        expire = 604800
        minimum = 86400
ab-products.com.ec      nameserver = linuxpifo2.ab-products.com.ec.
ab-products.com.ec      mail exchanger = 10 linuxpifo2.ab-products.com.ec.
>
```

  - Se realiza la consulta por el record ab-products.com.ec

4.7.1.2 Instalación de Sendmail.

- Por Yum

```
[root@quitofr ~]# yum y install sendmail sendmail-cf
```

- Mediante los CD's de Instalación de Centos 5.0 .
  - Insertar el CD #1 de Centos 5.0 y Montar la Unidad de CDROM en el directorio /media/

```
[root@quitofr ~]# mount /dev/hda /media
```

  - Ir al directorio CentOs que se encuentra dentro de la unidad montada /media/

```
[root@quitofr ~]# cd /media/CentOs
```

  - Instalar los paquetes sendmail-8.13.8-2.el5.i386.rpm , sendmail-cf-8.13.8-2.el5.i386.rpm

```
[root@quitofr CentOs]# rpm - ivh sendmail-8.13.8-2.el5.i386.rpm  sencmail-cf-8.13.8-2.el5.i386.rpm
```

4.7.1.2.1 Revisión de los paquetes

- Verificar que se encuentre instalado el paquete sendmail y sendmail-cf
  - La instalación del paquete sendmail viene de forma predeterminada al momento de instalar centos como servidor de correo.

```
[root@quitofr ~]# rpm -qa|grep sendmail
sendmail-8.13.8-2.el5
sendmail-cf-8.13.8-2.el5
[root@quitofr ~]#
```

4.7.1.3 Configuración de Sendmail

- Edición del archivo de configuración de sendmail
  - El archivo principal de sendmail es el sendmail.cf sin embargo de manera inicial este archivo no permite que se acepten conexiones de red desde ningún host mas que el propio localhost.
  - Para añadir funcionalidad a sendmail utilizaremos el archivo sendmail.mc y a través de este se procederá a regenerar un nuevo sendmail.cf

```
[root@quitofr ~]# cd /etc/mail/
[root@quitofr mail]# vi sendmail.mc
```

- Parámetros a tomar en consideración

  - Comentar con dnl la línea en negrilla para que sendmail acepte conexiones de red.

    dnl #DAEMON OPTIONS(‘Port=smtp,Addr=127.0.0.1, Name=MTA’)dnl

```
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 #
dnl #DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, 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.
```

  - Buscar la siguiente línea en el archivo:

    dnl MASQUERADE_AS(‘mydomain.com’)dnl

```
dnl # The following example makes mail from this host and any additional
dnl # specified domains appear to be sent from mydomain.com
dnl #
dnl MASQUERADE_AS(`mydomain.com')dnl
dnl #
dnl # masquerade not just the headers, but the envelope as well
dnl #
dnl FEATURE(masquerade_envelope)dnl
dnl #
dnl # masquerade not just @mydomainalias.com, but @*.mydomainalias.com as well
dnl #
dnl FEATURE(masquerade_entire_domain)dnl
```

  - Quitar el comentario a la línea y la modificarla de forma que quede así:

    MASQUERADE_AS(‘egar.com.ec’)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(`egar.com.ec')dnl
dnl #
dnl # masquerade not just the headers, but the envelope as well
dnl #
dnl FEATURE(masquerade_envelope)dnl
dnl #
dnl # masquerade not just @mydomainalias.com, but @*.mydomainalias.com as well
dnl #
dnl FEATURE(masquerade_entire_domain)dnl
```

    - Con esta opción se logra enmascarar el correo con el dominio egar.com.ec

- Impedir que sendmail acepte correo de dominios no resolvibles
  - Buscar la siguiente línea en el archivo:

    FEATURE(‘accept_unresolvable_domains’)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.
```

  - Comentar la línea con dnl de la siguiente forma:

    dnl #FEATURE(‘accept_unresolvable_domains’)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 #
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.
```

- Establecer que direcciones ip pueden hacer relay a través del servidor
  - Relay quiere decir que ip’s pueden o no enviar correo a través del servidor. Es una medida de seguridad permitir solo a la red interna 192.168.1 y al localhost el envío de correo.

```
[root@quitofr ~]# vi /etc/mail/access
```

```
# 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...
Connect:localhost.localdomain           RELAY
Connect:localhost                       RELAY
Connect:127.0.0.1                       RELAY
192.168.1                               RELAY
```

- Especificar que dominios aceptará el servidor
  - Ubicarse en el directorio /etc/mail

```
[root@quitofr ~]# cd /etc/mail
```

```
   ab-products.com.ec      smtp:linuxpifo2.ab-products.com.ec
[root@quitofr mail]# touch relay-domains
[root@quitofr mail]#
```

  - Crear un archivo vacío de nombre relay-domains

  - Editar el nuevo archivo creado
    - En el archivo local-host-names se especifica que dominios aceptará el servidor de correo, en este caso aceptará el correo proveniente de los dominios egar.com.ec y ab-products.com.ec

```
[root@quitofr mail]# vi relay-domains
egar.com.ec
ab-products.com.ec
```

- Especificar los dominios a manejar por el servidor
  - Editar el archivo local-host-names

```
[root@quitofr ~]# vi /etc/mail/local-host-names

# local-host-names - include all aliases for your machine here
egar.com.ec
```

    - En el archivo local-host-names se especifica que dominios manejará el servidor de correo, en este caso manejará el dominio egar.com.ec
- Especificar que Sendmail actúe como Gateway para el dominio ab-products.com.ec
  - Editar el archivo /etc/mail/mailertable y añadir el dominio ab-products.com.ec

```
[root@quitofr ~]# cd /etc/mail
[root@quitofr mail]# vi mailertable
```

    - Se especifica el dominio y mediante el parámetro smtp el servidor a reenviar el correo. Cabe destacar que para que este reenvío sea exitoso debe estar bien configurado el DNS interno para el dominio ab-products.com.ec.

- Compilación del archivo sendmail.mc para generar las bases de datos de sendmail y el archivo sendmail.cf

```
[root@quitofr mail]# make -C /etc/mail
make: Entering directory `/etc/mail'
make: Leaving directory `/etc/mail'
[root@quitofr mail]#
```

4.7.1.4 Iniciar el Servicio de Correo Electrónico

- Iniciar el servicio de sendmail

```
[root@quitofr ~]# service sendmail status
sendmail (pid 2079 2071) is running...
[root@quitofr ~]#
```

4.7.1.5 Instalación de Dovecot

- Por Yum

```
[root@quitofr ~]# yum -y install dovecot
```

- Mediante los CD's de Instalación de Centos.
  - Insertar el CD #3 de Centos y Montar la Unidad de CDROM

```
[root@quitofr ~]# mount /dev/hda /media
```

  - Ir al directorio CentOs

```
[root@quitofr ~]# cd /media/CentOs
```

  - Instalar los paquetes sendmail-8.13.8-2.el5.i386.rpm , sendmail-cf-8.13.8-2.el5.i386.rpm

```
[root@quitofr CentOs]# rpm -ivh dovecot-1.0-1.2.rc15.el5.i386.rpm
```

4.7.1.5.1 Revisión de los paquetes

```
[root@quitofr ~]# rpm -q dovecot
dovecot-1.0-1.2.rc15.el5
[root@quitofr ~]#
```

- El paquete dovecot viene instalado de manera predeterminada al momento de instalar Centos como servidor de correo.

4.7.1.6 Configuración de Dovecot

```
[root@quitofr ~]# vi /etc/dovecot.conf


# Default values are shown for each setting, it's not required to uncomment
# any of the lines.

# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Protocols we want to be serving: imap imaps pop3 pop3s
# If you only want to use dovecot-auth, you can set this to "none".
protocols = imap  pop3

# IP or host address where to listen in for connections. It's not currently
# possible to specify multiple addresses. "*" listens in all IPv4 interfaces.
```

- Activar el parámetro *protocols= imap pop3*

4.7.1.7 Iniciar el Servicio DOVECOT

```
[root@quitofr ~]# service dovecot start
Starting Dovecot Imap:                                     [  OK  ]
[root@quitofr ~]#
```

4.7.1.8 Pruebas de funcionalidad Diseño Básico

- Envío de correo usando telnet
  - Se utilizarán dos cuentas de usuarios freired@egar.com.ec y ribadeneiram@ab-products.com.ec. La forma de añadir usuarios en general al sistema será el siguiente:

```
[root@quitofr ~]# useradd acostaa
[root@quitofr ~]# passwd acostaa
Changing password for user acostaa.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfull
[root@quitofr ~]#
```

- Envío de correo usando telnet a través del puerto SMTP (25)
  - El envío se hace de la cuenta freired@egar.com.ec a la cuenta ribadeneiram@ab-products.com.ec

```
[root@quitofr ~]# telnet 192.168.1.1 25
Trying 192.168.1.1...
Connected to quitofr.egar.com.ec (192.168.1.1).
Escape character is '^]'.
220 quitofr.egar.com.ec ESMTP ; Sat, 26 Jan 2008 12:45:59 -0500
ehlo egar.com.ec
250-quitofr.egar.com.ec Hello quitofr.egar.com.ec [192.168.1.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
mail from: freired@egar.com.ec
250 2.1.0 freired@egar.com.ec... Sender ok
rcpt to:ribadeneiram@ab-products.com.ec
250 2.1.5 ribadeneiram@ab-products.com.ec... Recipient ok
data
354 Enter mail, end with "." on a line by itself
subject: Correo de Prueba
Esto es una prueba de correo dirigido al usuario ribadeneira
Saludos
.
250 2.0.0 m0QHjxbe015373 Message accepted for delivery
quit
221 2.0.0 quitofr.egar.com.ec closing connection
Connection closed by foreign host.
[root@quitofr ~]#
```

- Verificación del envío y recepción del mensaje enviado a través de logs

```
[root@quitofr ~]# tail -fn2 /var/log/maillog
Jan 26 12:51:04 quitofr sendmail[15420]: m0QHnNa3015420: from=freired@egar.com.ec, size=98, class=0, nrcpts=1, msgid=<2008012
61750.m0QHnNa3015420@quitofr.egar.com.ec>, proto=ESMTP, daemon=MTA, relay=quitofr.egar.com.ec [192.168.1.1]
Jan 26 12:51:04 quitofr sendmail[15428]: m0QHnNa3015420: to=ribadeneiram@ab-products.com.ec, ctladdr=freired@egar.com.ec (514
/514), delay=00:01:00, xdelay=00:00:00, mailer=local, pri=30442, dsn=2.0.0, stat=Sent
```

- Envío de correo usando telnet a través del puerto SMTP (25) de la cuenta freired@egar.com.ec a la cuenta de hotmail dave_edu@hotmail.com

```
[root@quitofr ~]# telnet 192.168.1.1 25
Trying 192.168.1.1...
Connected to quitofr.egar.com.ec (192.168.1.1).
Escape character is '^]'.
220 quitofr.egar.com.ec ESMTP ; Sat, 26 Jan 2008 13:00:57 -0500
ehlo egar.com.ec
250-quitofr.egar.com.ec Hello quitofr.egar.com.ec [192.168.1.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
mail from: freired@egar.com.ec
250 2.1.0 freired@egar.com.ec... Sender ok
rcpt to: dave_edu@hotmail.com
250 2.1.5 dave_edu@hotmail.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Subject: Prueba de correo a hotmail
Esto es una prueba de correo
Saludos
.
250 2.0.0 m0QI0v3k015534 Message accepted for delivery
quit
221 2.0.0 quitofr.egar.com.ec closing connection
Connection closed by foreign host.
[root@quitofr ~]#
```

- Verificación del envío y recepción del mensaje a través de logs

```
[root@quitofr ~]# tail -fn2 /var/log/maillog
Jan 26 13:02:34 quitofr sendmail[15534]: m0QI0v3k015534: from=freired@egar.com.ec, size=76, class=0, nrcpts=1, msgid=<200
61801.m0QI0v3k015534@quitofr.egar.com.ec>, proto=ESMTP, daemon=MTA, relay=quitofr.egar.com.ec [192.168.1.1]
Jan 26 13:02:35 quitofr sendmail[15544]: m0QI0v3k015534: to=dave_edu@hotmail.com, ctladdr=freired@egar.com.ec (514/514),
 pri=120394, relay=mx3.hotmail.com. [65.54.244.72], dsn=2.0.0, stat=Sent ( <200801261801.m0QI0v3k015534@quitofr.egar.
Queued mail for delivery)
```

  - Se observa que el mx de Hotmail responde Queued mail for delivery. Indicativo de que el correo fué aceptado sin problemas.

- Verificación de recepción del mensaje de subject ´´prueba de correo a hotmail ´´ en la página de www.homail.com

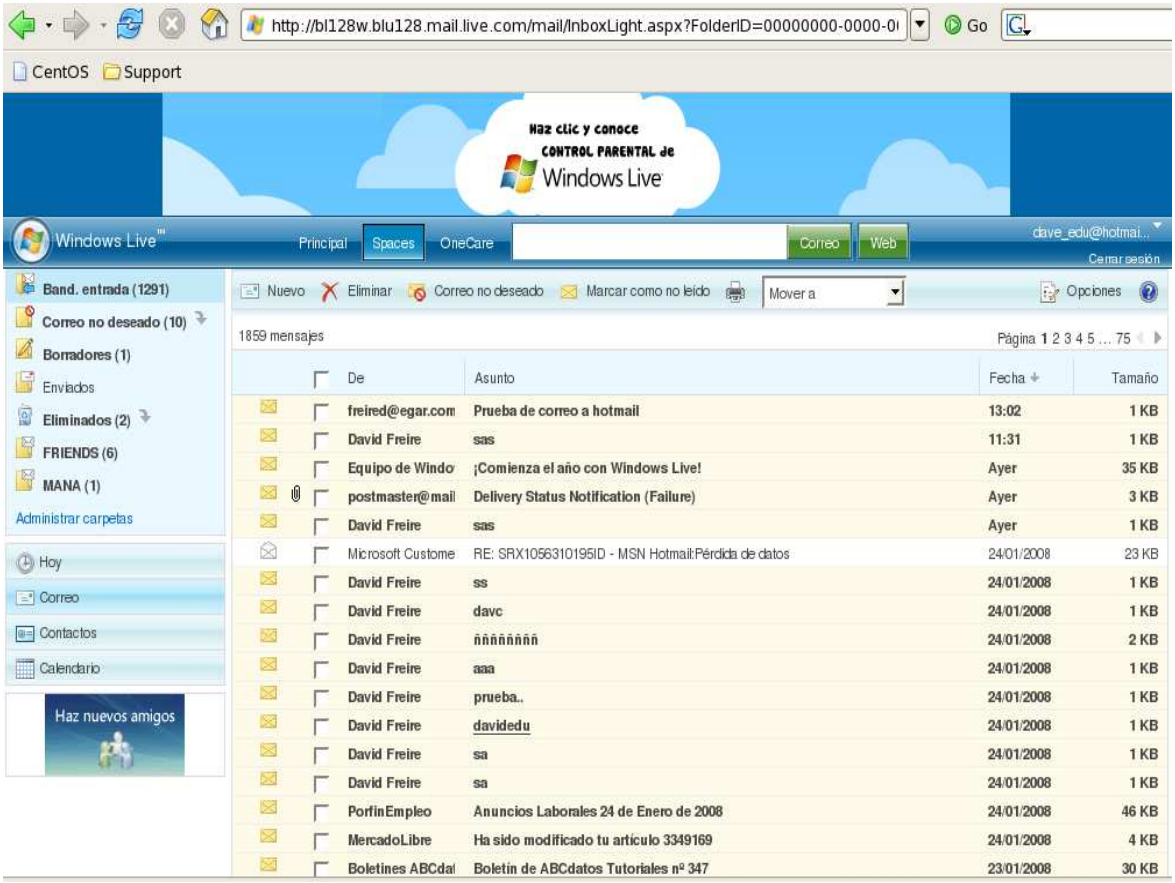

FIGURA 4. 15: VISUALIZACIÓN DEL MENSAJE ENVIADO A LA CUENTA DE HOTMAIL

- Envío de correo desde una cuenta de gmail.com a las cuentas de freired@egar.com.ec y ribadeniram@ab-products.com.ec

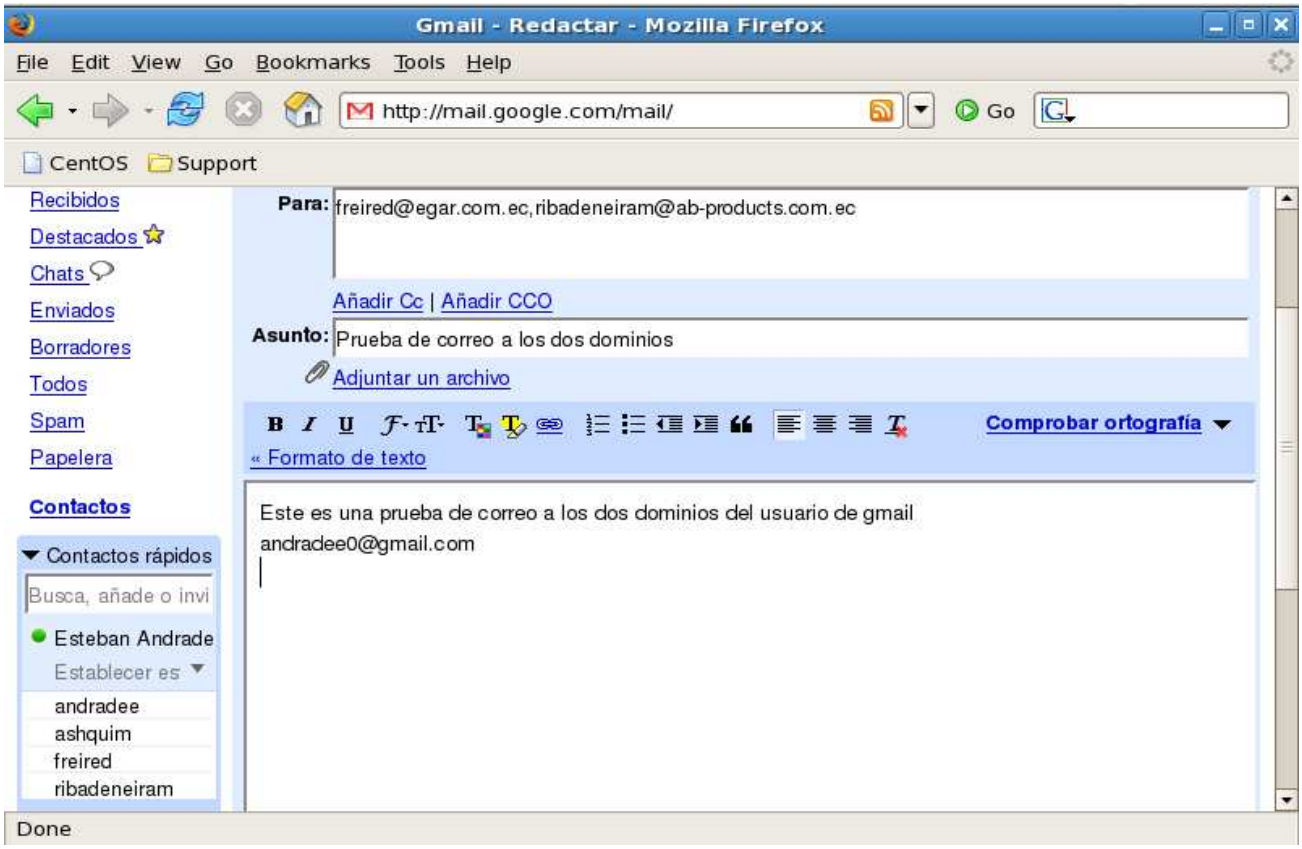

FIGURA 4. 16: ENVÍO DE MENSAJE ELECTRÓNICO DESDE ww.gmail.com

- Comprobación por medio de logs de que el servidor acepte correo de los dominios egar.com.ec y ab-products.com.ec y actúe de GATEWAY para el dominio ab-products.com.ec

```
[root@quitofr ~]# tail -fn0 /var/log/maillog
Feb 23 14:38:57 quitofr sendmail[27407]: m1NJcqR4027407: from=<andradee0@gmail.com>, size=2025, c
lass=0, nrcpts=1, msgid=<6733bf630802231142y31b0041ah281eabaca8cde013@mail.gmail.com>, proto=ESMT
P, daemon=MTA, relay=an-out-0708.google.com [209.85.132.248]
Feb 23 14:38:57 quitofr sendmail[27408]: m1NJcqWD027408: from=<andradee0@gmail.com>, size=2036, c
lass=0, nrcpts=1, msgid=<6733bf630802231142y31b0041ah281eabaca8cde013@mail.gmail.com>, proto=ESMT
P, daemon=MTA, relay=an-out-0708.google.com [209.85.132.246]
Feb 23 14:38:57 quitofr sendmail[27408]: m1NJcqWD027408: to=<ribadeneiram@ab-products.com.ec>, de
lay=00:00:00, mailer=smtp, pri=32036, stat=queued

Feb 23 14:39:04 quitofr sendmail[27422]: m1NJcqR4027407: to=<freired@egar.com.ec>, delay=00:00:07
, xdelay=00:00:00, mailer=local, pri=122025, dsn=2.0.0, stat=Sent
Feb 23 14:39:05 quitofr sendmail[27422]: m1NJcqWD027408: to=<ribadeneiram@ab-products.com.ec>, de
lay=00:00:08, xdelay=00:00:01, mailer=smtp, pri=122036, relay=linuxpifo2.ab-products.com.ec. [157
.100.98.18], dsn=2.0.0, stat=Sent (m1NJj85R000598 Message accepted for delivery)
```

4.7.2 IMPLEMENTACIÓN DISEÑO SECUNDARIO DEL SERVICIO DE CORREO ELECTRÓNICO

4.7.2.1 Implementación del Webmail squirreloutlook

4.7.2.1.1 Instalación de paquetes necesarios.

- Instalación por yum del paquete httpd.

```
[root@quitofr ~]# yum -y install httpd
```

- Instalación del paquete httpd mediante los CD's de Instalación de Centos 5.0 .
  - Insertar el CD #2 de Centos 5.0 y Montar la Unidad de CDROM

```
[root@quitofr ~]# mount /dev/hda /media/
```

  - Ir al directorio CentOs que se encuentra dentro de la unidad montada /media/

```
[root@quitofr ~]# cd /media/CentOs
```

  - Instalar el paquete httpd-2.2.3-6.el5.centos1

```
[root@quitofr CentOs]# rpm -ivh httpd-2.2.3-6.el5.centos1
```

- Verificar que el paquete httpd esté instalado correctamente.

```
[root@quitofr ~]# rpm -q httpd
httpd-2.2.3-6.el5.centos.1
[root@quitofr ~]#
```

  - El paquete httpd viene instalado de manera predeterminada al momento de instalar Centos 5.0 como servidor Apache. En caso de no estar instalado se puede utilizar cualquier opción de instalación ya sea por yum o por los CD's de instalación.

- Descarga del paquete squirreloutlook
  - Squirreloutlook es un webmail adaptado con una interfaz parecida a Outlook 2003, la descarga se realizará desde el sitio sourceforge.net utilizando el comando wget.

```
[root@quitofr ~]# wget http://downloads.sourceforge.net/squirreloutlook/squirreloutlook-1.0.3.tar
.gz?modtime=1166459952&big_mirror=0
[1] 4083
[root@quitofr ~]# --12:57:46--  http://downloads.sourceforge.net/squirreloutlook/squirreloutlook-
1.0.3.tar.gz?modtime=1166459952
Resolving downloads.sourceforge.net... 66.35.250.203
Connecting to downloads.sourceforge.net|66.35.250.203|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://ufpr.dl.sourceforge.net/sourceforge/squirreloutlook/squirreloutlook-1.0.3.tar.gz
 [following]
--12:57:47--  http://ufpr.dl.sourceforge.net/sourceforge/squirreloutlook/squirreloutlook-1.0.3.ta
r.gz
Resolving ufpr.dl.sourceforge.net... 200.17.202.1
Connecting to ufpr.dl.sourceforge.net|200.17.202.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2007632 (1.9M) [application/x-gzip]
Saving to: `squirreloutlook-1.0.3.tar.gz'

100%[======================================================>] 2,007,632   6.67K/s   in 3m 28s

13:01:16 (9.43 KB/s) - `squirreloutlook-1.0.3.tar.gz' saved [2007632/2007632]


[1]+  Done                    wget http://downloads.sourceforge.net/squirreloutlook/squirreloutlo
ok-1.0.3.tar.gz?modtime=1166459952
[root@quitofr ~]#
```

- Verificación de la realización exitosa de la descarga.
  - Comprobar que se descargó el archivo de nombre squirreloutlook-1.0.3.tar.gz

```
[root@quitofr ~]# ls -l squirreloutlook-1.0.3.tar.gz
-rw-r--r-- 1 root root 2007632 Dec 18  2006 squirreloutlook-1.0.3.tar.gz
[root@quitofr ~]#
```

- Descomprimir el paquete squirreloutlook-1.0.3.tar.gz

```
[root@quitofr ~]# tar -zxvf squirreloutlook-1.0.3.tar.gz
squirreloutlook-1.0.3/contrib/squirrelmail.mailto.NT2KXP.reg
squirreloutlook-1.0.3/contrib/squirrelmail.mailto.reg
squirreloutlook-1.0.3/contrib/squirrelmail.mailto.Win9x.reg
squirreloutlook-1.0.3/locale
squirreloutlook-1.0.3/locale/pt_BR
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/unsafe_image_rules.po
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/abook_import_export.po
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/archive_mail.mo
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/archive_mail.po
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/notes.po
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/squirrelmail.mo
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/squirrelmail.po
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/unsafe_image_rules.mo
squirreloutlook-1.0.3/locale/pt_BR/LC_MESSAGES/abook_import_export.mo
squirreloutlook-1.0.3/locale/pt_BR/setup.php
squirreloutlook-1.0.3/locale/index.php
squirreloutlook-1.0.3/locale/README.locales
squirreloutlook-1.0.3/locale/timezones.cfg
squirreloutlook-1.0.3/UPGRADE
squirreloutlook-1.0.3/ChangeLog
squirreloutlook-1.0.3/configure
squirreloutlook-1.0.3/COPYING
squirreloutlook-1.0.3/index.php
squirreloutlook-1.0.3/INSTALL
squirreloutlook-1.0.3/README
squirreloutlook-1.0.3/ReleaseNotes
squirreloutlook-1.0.3/AUTHORS
```

- Comprobar la creación de la carpeta squirreloutlook1.0.3

```
[root@quitofr ~]# ls -l squirreloutlook-1.0.3
total 212
-rw-r--r--   1 root wheel  8603 Dec 18  2006 AUTHORS
-rw-r--r--   1 root wheel 74951 Dec 18  2006 ChangeLog
drwxr-xr-x   5 root wheel  4096 Dec 18  2006 class
drwxr-xr-x   2 root wheel  4096 Dec 18  2006 config
-rw-r--r--   1 root wheel   107 Dec 18  2006 configure
drwxr-xr-x   3 root wheel  4096 Dec 18  2006 contrib
-rw-r--r--   1 root wheel 15509 Dec 18  2006 COPYING
drwxr-xr-x   2 root wheel  4096 Dec 18  2006 data
drwxr-xr-x   3 root wheel  4096 Dec 18  2006 doc
drwxr-xr-x   4 root wheel  4096 Dec 18  2006 functions
drwxr-xr-x   4 root wheel  4096 Dec 18  2006 help
drwxr-xr-x   4 root wheel  4096 Dec 18  2006 images
drwxr-xr-x   3 root wheel  4096 Dec 18  2006 include
-rw-r--r--   1 root wheel   684 Dec 18  2006 index.php
-rw-r--r--   1 root wheel  9037 Dec 18  2006 INSTALL
drwxr-xr-x   3 root wheel  4096 Dec 18  2006 locale
drwxr-xr-x 41 root wheel  4096 Dec 18  2006 plugins
drwxr-xr-x   2 root wheel  4096 Dec 18  2006 po
drwxr-xr-x   2 root wheel  4096 Dec 18  2006 psd
-rw-r--r--   1 root wheel  2692 Dec 18  2006 README
-rw-r--r--   1 root wheel  4704 Dec 18  2006 ReleaseNotes
drwxr-xr-x   2 root wheel  4096 Dec 18  2006 src
drwxr-xr-x   3 root wheel  4096 Dec 18  2006 themes
drwxr-xr-x   2 root wheel  4096 Dec 18  2006 tmp
-rw-r--r--   1 root wheel  4845 Dec 18  2006 UPGRADE
[root@quitofr ~]#
```

- Mover la carpeta squirreloutlook1.0.3 al directorio /var/www/html

```
[root@quitofr ~]# mv squirreloutlook-1.0.3 /var/www/html/
[root@quitofr ~]#
```

- Ubicarse en el directorio /var/www/html y listar el contenido

```
[root@quitofr ~]# cd /var/www/html/ ; ls -l
total 4
drwxr-xr-x 18 root wheel 4096 Dec 18  2006 squirreloutlook-1.0.3
[root@quitofr html]#
```

4.7.2.2 Adaptación de squirreloutlook

- Ubicarse dentro del directorio squirreloutlook-1.0.3/config

```
[root@quitofr html]# cd squirreloutlook-1.0.3/
[root@quitofr squirreloutlook-1.0.3]# ls
AUTHORS    config     COPYING  functions  include    locale   psd          src      UPGRADE
ChangeLog  configure  data     help       index.php  plugins  README       themes
class      contrib    doc      images     INSTALL    po       ReleaseNotes  tmp
```

```
[root@quitofr squirreloutlook-1.0.3]# cd config
[root@quitofr config]# ls
config_default.php  config_ok.php  config.php       conf.pl
config_local.php    _config.php    config.php_dist  index.php
[root@quitofr config]#
```

- Ejecutar el comando ./conf.pl
  - configuración del nombre de la empresa y logo

```
[root@quitofr config]# ./conf.pl
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Organization Preferences
1.  Organization Name      : EGAR S.A
2.  Organization Logo      : ../images/egar.jpg
3.  Org. Logo Width/Height : (184/46)
4.  Organization Title     : SquirrelMail Outlook Theme
5.  Signout Page           :
6.  Top Frame              : _top
7.  Provider link          : http://www.squirrelmail.org/
8.  Provider name          : SquirrelMail

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

Command >>
```

- Configuración del dominio y del servidor smtp

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

General
-------
1.  Domain                 : egar.com.ec
2.  Invert Time            : false
3.  Sendmail or SMTP       : SMTP

SMTP Settings
-------------
4.   SMTP Server           : 157.100.98.22
5.   SMTP Port             : 25
6.   POP before SMTP       : false
7.   SMTP Authentication   : none
8.   Secure SMTP (TLS)     : false
9.   Header encryption key :

A.  Update IMAP Settings   : 127.0.0.1:143 (other)
H.  Hide SMTP Settings

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

Command >>
```

- Grabar los cambios con la letra S

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> S
```

- Cambiar de nombre a la carpeta squirreloutlook-1.0.3 por EGAR

  - El cambio de nombre de la carpeta squirreloutlook-1.0.3 es para referirnos por el nuevo nombre en este caso EGAR.

- Asignar la carpeta EGAR al usuario apache y al grupo apache

```
[root@quitofr html]# chown apache EGAR/*
[root@quitofr html]# chgrp apache EGAR/*
[root@quitofr html]#
```

- Comprobación de los cambios realizados

  - Verificamos que todos los archivos y directorios pertenezcan al usuario y grupo apache.

```
[root@quitofr html]# cd EGAR/
[root@quitofr EGAR]# ls -l
total 212
-rw-r--r--  1 apache apache  8603 Dec 18  2006 AUTHORS
-rw-r--r--  1 apache apache 74951 Dec 18  2006 ChangeLog
drwxr-xr-x  5 apache apache  4096 Dec 18  2006 class
drwxr-xr-x  2 apache apache  4096 Dec 18  2006 config
-rw-r--r--  1 apache apache   107 Dec 18  2006 configure
drwxr-xr-x  3 apache apache  4096 Dec 18  2006 contrib
-rw-r--r--  1 apache apache 15509 Dec 18  2006 COPYING
drwxr-xr-x  2 apache apache  4096 Dec 18  2006 data
drwxr-xr-x  3 apache apache  4096 Dec 18  2006 doc
drwxr-xr-x  4 apache apache  4096 Dec 18  2006 functions
drwxr-xr-x  4 apache apache  4096 Dec 18  2006 help
drwxr-xr-x  4 apache apache  4096 Feb 18 13:16 images
drwxr-xr-x  3 apache apache  4096 Dec 18  2006 include
-rw-r--r--  1 apache apache   684 Dec 18  2006 index.php
-rw-r--r--  1 apache apache  9037 Dec 18  2006 INSTALL
drwxr-xr-x  3 apache apache  4096 Dec 18  2006 locale
drwxr-xr-x 41 apache apache  4096 Dec 18  2006 plugins
drwxr-xr-x  2 apache apache  4096 Dec 18  2006 po
drwxr-xr-x  2 apache apache  4096 Dec 18  2006 psd
-rw-r--r--  1 apache apache  2692 Dec 18  2006 README
-rw-r--r--  1 apache apache  4704 Dec 18  2006 ReleaseNotes
drwxr-xr-x  2 apache apache  4096 Dec 18  2006 src
drwxr-xr-x  3 apache apache  4096 Dec 18  2006 themes
drwxr-xr-x  2 apache apache  4096 Dec 18  2006 tmp
-rw-r--r--  1 apache apache  4845 Dec 18  2006 UPGRADE
[root@quitofr EGAR]#
```

- Inciar el servicio httpd

```
[root@quitofr ~]# service httpd start
Starting httpd:                                            [  OK  ]
[root@quitofr ~]# chkconfig --level 2345 httpd on
[root@quitofr ~]#
```

4.7.2.3 Pruebas de Funcionalidad de Webmail

- Pruebas desde el navegador mozila firefox.

FIGURA 4. 17: PANTALLA DE ACCESO AL WEBMAIL DE EGAR S.A.

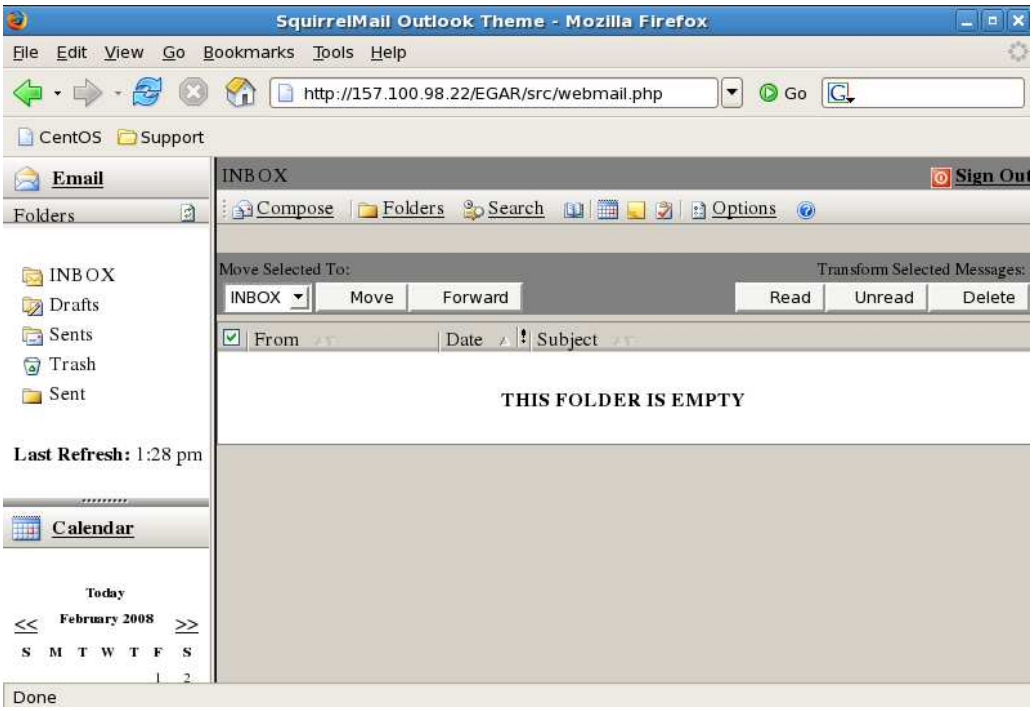

FIGURA 4. 18: PANTALLA PRINCIPAL DEL WEBMAIL DE EGAR S.A.

- Envío de correo desde Webmail
  - El envío de correo se hará desde la cuenta freired@egar.com.ec a la cuenta acostaa@egar.com.ec .

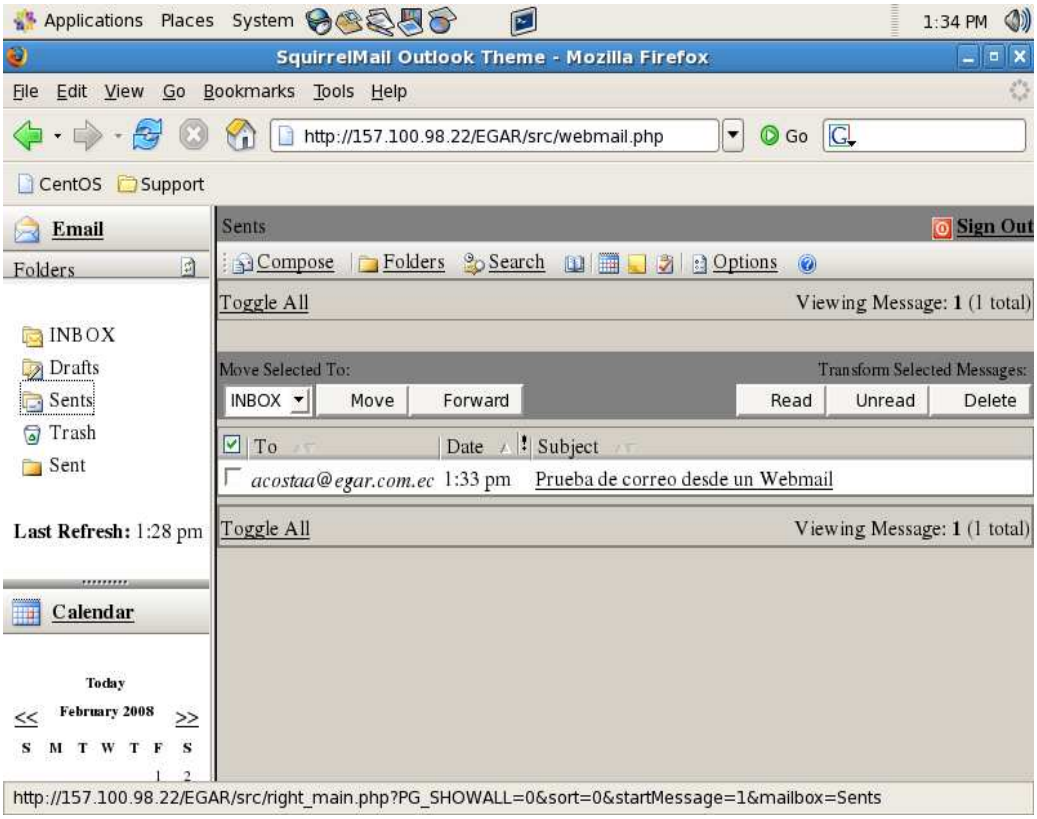

FIGURA 4. 19: ENVÍO DE CORREO ELECTRÓNICO POR WEBMAIL

- Comprobar que el mensaje llegó al destinatario acostaa@egar.com.ec

FIGURA 4. 20: ACCESO AL WEBMAIL DE EGAR S.A.

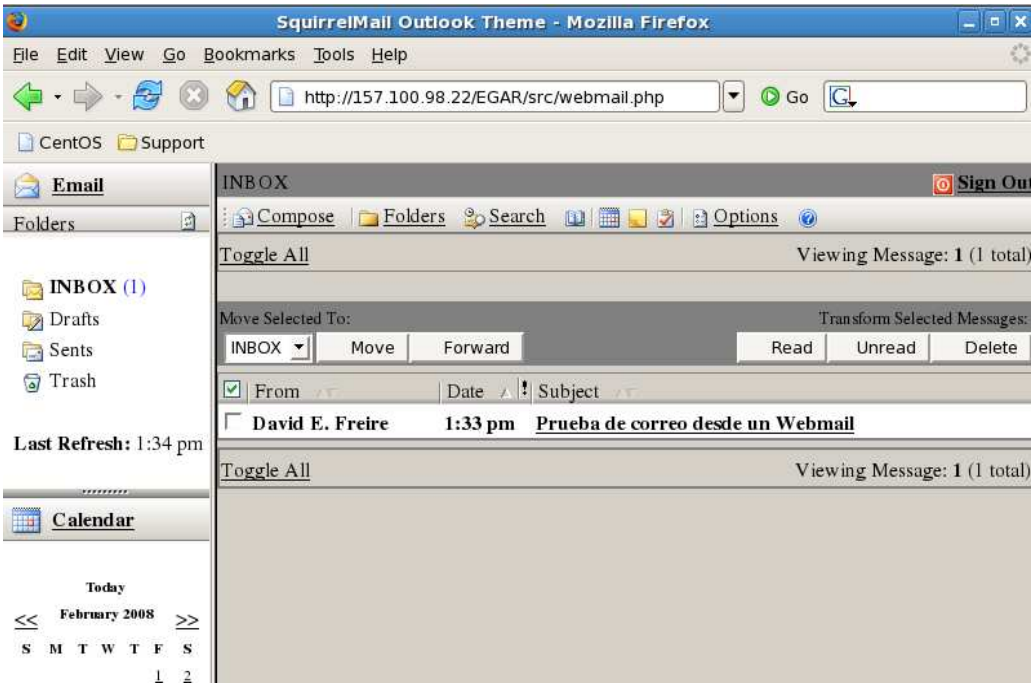

FIGURA 4. 21: RECEPCIÓN DE MENSAJES DE CORREO EN WEBMAIL

4.7.2.4 Instalación del Sistema Antispam

- El paquete spamassassin viene por defecto al momento de instalar Centos 5.0 como servidor de correo.

- Revisar si está instalado el paquete spamassassin

```
[root@quitofr ~]# rpm -qa |grep spamassassin
spamassassin-3.1.7-4.el5
[root@quitofr ~]#
```

4.7.2.5 Instalación de Sistema Antivirus

- Instalación del antivirus clamav a travéz de yum.

```
[root@quitofr ~]# yum -y install clamav
--> Processing Dependency: clamav-db = 0.92-1.el5.rf for package: clamav
--> Restarting Dependency Resolution with new changes.
--> Populating transaction set with selected packages. Please wait.
---> Downloading header for clamav-db to pack into transaction set.
clamav-db-0.92-1.el5.rf.i 100% |=========================| 3.7 kB    00:00
---> Package clamav-db.i386 0:0.92-1.el5.rf set to be updated
--> Running transaction check

Dependencies Resolved

================================================================================
 Package                 Arch       Version          Repository        Size
================================================================================
Installing:
 clamav                  i386       0.92-1.el5.rf    rpmforge          1.2 M
Installing for dependencies:
 clamav-db               i386       0.92-1.el5.rf    rpmforge           11 M

Transaction Summary
================================================================================
Install      2 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 12 M
Downloading Packages:
(1/2): clamav-db-0.92-1.e 100% |=========================|  11 MB    12:41
(2/2): clamav-0.92-1.el5. 100% |=========================| 1.2 MB    01:22
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: clamav-db                    ######################### [1/2]
  Installing: clamav                       ######################### [2/2]

Installed: clamav.i386 0:0.92-1.el5.rf
Dependency Installed: clamav-db.i386 0:0.92-1.el5.rf
Complete!
[root@quitofr ~]#
```

- La instalación por medio de yum primero resuelve dependencias, en este caso previo la instalación del paquete clamav instala el paquete clamav-db.
- Clamav no está contenida en ningún cd de Instalación de Centos

- Instalación por yum de los paquetes clamav-devel y clamd.

```
[root@quitofr ~]# yum -y install clamav-devel clamd
Resolving Dependencies
--> Populating transaction set with selected packages. Please wait.
---> Downloading header for clamd to pack into transaction set.
clamd-0.92-1.el5.rf.i386. 100% |=========================| 6.2 kB    00:00
---> Package clamd.i386 0:0.92-1.el5.rf set to be updated
---> Downloading header for clamav-devel to pack into transaction set.
clamav-devel-0.92-1.el5.r 100% |=========================| 3.7 kB    00:00
---> Package clamav-devel.i386 0:0.92-1.el5.rf set to be updated
--> Running transaction check

Dependencies Resolved

================================================================================
 Package                 Arch       Version          Repository        Size
================================================================================
Installing:
 clamav-devel            i386       0.92-1.el5.rf    rpmforge          7.4 k
 clamd                   i386       0.92-1.el5.rf    rpmforge           82 k

Transaction Summary
================================================================================
Install      2 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 89 k
Downloading Packages:
(1/2): clamd-0.92-1.el5.r 100% |=========================|  82 kB    00:05
(2/2): clamav-devel-0.92- 100% |=========================| 7.4 kB    00:00
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: clamav-devel                 ########################## [1/2]
  Installing: clamd                        ########################## [2/2]

Installed: clamav-devel.i386 0:0.92-1.el5.rf clamd.i386 0:0.92-1.el5.rf
Complete!
[root@quitofr ~]#
```

  - Clamd es un motor de actualización de virus en las bases de datos de clamav.

- Verificar la que se realizó la instalación de todos los paquetes necesarios para el sistema antivirus.

```
[root@quitofr ~]# rpm -qa |grep clam
clamav-0.92-1.el5.rf
clamav-devel-0.92-1.el5.rf
clamd-0.92-1.el5.rf
clamav-db-0.92-1.el5.rf
[root@quitofr ~]#
```

4.7.2.6 Instalación de MailScanner

- La descarga del software mailscanner se hará directamente desde el sitio web oficial www.mailscanner.info, debido a que no está disponible en ningún otro repositorio. .

```
[root@quitofr ~]# wget http://www.mailscanner.info/files/4/rpm/MailScanner-4.66.5-3.rpm.tar.gz
--12:37:40--  http://www.mailscanner.info/files/4/rpm/MailScanner-4.66.5-3.rpm.tar.gz
Resolving www.mailscanner.info... 81.17.252.15
[root@quitofr ~]# ls
1                ftp-0.17-33.fc6.i386.rpm  MailScanner-4.66.5-3.rpm.tar.gz
anaconda-ks.cfg  hosts                     msnner.doc
Desktop          install.log               rpmforge-release-0.3.6-1.el5.rf.i386.rpm
fetch.txt        install.log.syslog        yum.doc
[root@quitofr ~]# tar -zxvf MailScanner-4.66.5-3.rpm.tar.gz
1

12:43:56 (11.8 KB/s) - `MailScanner-4.66.5-3.rpm.tar.gz' saved [4540345/4540345]

[root@quitofr ~]#
```

- Revisión de descarga del paquete mailscanner-4.66.5-3.rpm.tar.gz

  - El paquete mailscanner viene en formato tar.gz por lo tanto es necesario descomprimirlo y compilarlo.
  - La compilación de este archivo se hace para obtener el rpm que finalmente utilizará el sistema.

- Instalación de paquetes necesarios previo la compilación de MailScanner.

  - Revisar si está instalado el paquete cpp

```
[root@quitofr ~]# rpm -qa |grep cpp
cpp-4.1.1-52.el5
[root@quitofr ~]#
```

  - El paquete cpp viene por defecto en la instalación de Centos 5.

  - Instalación de los paquetes cpp y gcc por Yum.

```
[root@quitofr ~]# yum - y install gcc cpp
```

  - Los paquetes gcc y cpp son necesarios para un buena compilación del paquete MailScanner.

```
 Package                 Arch       Version          Repository        Size
================================================================================
Installing:
 gcc                     i386       4.1.2-14.el5     base              5.2 M
Installing for dependencies:
 glibc-devel             i386       2.5-18.el5_1.1   updates           2.0 M
 glibc-headers           i386       2.5-18.el5_1.1   updates           609 k
 libgomp                 i386       4.1.2-14.el5     base               76 k
Updating for dependencies:
 cpp                     i386       4.1.2-14.el5     base              2.6 M
 glibc                   i686       2.5-18.el5_1.1   updates           5.1 M
 glibc-common            i386       2.5-18.el5_1.1   updates            16 M
 libgcc                  i386       4.1.2-14.el5     base               87 k

Transaction Summary
================================================================================
Install      4 Package(s)
Update       4 Package(s)
Remove       0 Package(s)

Total download size: 32 M
Downloading Packages:
(1/8): gcc-4.1.2-14.el5.i 100% |=========================| 5.2 MB    08:44
(2/8): libgcc-4.1.2-14.el 100% |=========================|  87 kB    00:12
(3/8): libgomp-4.1.2-14.e 100% |=========================|  76 kB    00:07
(4/8): glibc-devel-2.5-18 100% |=========================| 2.0 MB    02:41
(5/8): cpp-4.1.2-14.el5.i  99% |======================== | 2.6 MB    00:04 ETA
(6/8): glibc-headers-2.5- 100% |=========================| 609 kB    00:57
(7/8): glibc-common-2.5-1 100% |=========================|  16 MB    23:27
(8/8): glibc-2.5-18.el5_1 100% |=========================| 5.1 MB    08:21
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating  : libgcc                       ######################### [ 1/12]
  Updating  : glibc-common                 ######################### [ 2/12]
  Updating  : glibc                        ######################### [ 3/12]
  Installing: libgomp                      ######################### [ 4/12]
  Updating  : cpp                          ######################### [ 5/12]
  Installing: glibc-headers                ######################### [ 6/12]
  Installing: glibc-devel                  ######################### [ 7/12]
  Installing: gcc                          ######################### [ 8/12]
  Cleanup   : libgcc                       ######################### [ 9/12]
  Cleanup   : cpp                          ######################### [10/12]
  Cleanup   : glibc-common                 ######################### [11/12]
  Cleanup   : glibc                        ######################### [12/12]

Installed: gcc.i386 0:4.1.2-14.el5
Dependency Installed: glibc-devel.i386 0:2.5-18.el5_1.1 glibc-headers.i386 0:2.5-18.el5_1.1
mp.i386 0:4.1.2-14.el5
Dependency Updated: cpp.i386 0:4.1.2-14.el5 glibc.i686 0:2.5-18.el5_1.1 glibc-common.i386 0
8.el5_1.1 libgcc.i386 0:4.1.2-14.el5
Complete!
[root@quitofr ~]#
```

- Revisar si está instalado el paquete rpm-build.

```
[root@quitofr ~]# rpm -q rpm-build
package rpm-build is not installed
[root@quitofr ~]#
```

- Instalación del paquete rpm-build por Yum.

```
[root@quitofr ~]# yum - y install rpm-build

Total download size: 2.4 M
Downloading Packages:
(1/6): rpm-python-4.4.2-4 100% |=========================|  54 kB    00:06
(2/6): rpm-build-4.4.2-47 100% |=========================| 551 kB    00:50
(3/6): elfutils-libs-0.12 100% |=========================| 105 kB    00:10
(4/6): rpm-4.4.2-47.el5.i 100% |=========================| 639 kB    01:03
(5/6): elfutils-0.125-3.e 100% |=========================| 163 kB    00:17
(6/6): rpm-libs-4.4.2-47. 100% |=========================| 968 kB    02:17
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: elfutils-libs               ########################## [1/9]
  Installing: elfutils                    ########################## [2/9]
  Updating  : rpm-libs                    ########################## [3/9]
  Updating  : rpm                         ########################## [4/9]
  Updating  : rpm-python                  ########################## [5/9]
  Installing: rpm-build                   ########################## [6/9]
  Cleanup   : rpm-python                  ########################## [7/9]
  Cleanup   : rpm                         ########################## [8/9]
  Cleanup   : rpm-libs                    ########################## [9/9]

Installed: rpm-build.i386 0:4.4.2-47.el5
Dependency Installed: elfutils.i386 0:0.125-3.el5 elfutils-libs.i386 0:0.125-3.el5
Dependency Updated: rpm.i386 0:4.4.2-47.el5 rpm-libs.i386 0:4.4.2-47.el5 rpm-python.i386 0:4.4.2-
47.el5
Complete!
[root@quitofr ~]#
```

- El paquete rpm-build es indispensable para la creación de paquetes rpm a través del código fuente.

- Descompresión del archivo MailScanner-4.66.5-3.rpm.tar.gz

```
[root@quitofr ~]# tar -zxvf MailScanner-4.66.5-3.rpm.tar.gz

MailScanner-4.66.5-3/perl-Math-BigInt-1.86-1.src.rpm
MailScanner-4.66.5-3/MailScanner-perl-MIME-Base64-3.05-5.src.rpm
MailScanner-4.66.5-3/perl-HTML-Tagset-3.03-1.src.rpm
MailScanner-4.66.5-3/perl-DBD-SQLite-1.13-1.src.rpm
MailScanner-4.66.5-3/perl-bignum-0.21-1.src.rpm
MailScanner-4.66.5-3/mailscanner-4.66.5-3.noarch.rpm
MailScanner-4.66.5-3/perl-Storable-2.16-1.src.rpm
MailScanner-4.66.5-3/perl-Net-IP-1.25-1.src.rpm
MailScanner-4.66.5-3/perl-Test-Simple-0.70-1.src.rpm
MailScanner-4.66.5-3/README
MailScanner-4.66.5-3/perl-Scalar-List-Utils-1.19-1.src.rpm
MailScanner-4.66.5-3/perl-DBI-1.56-1.src.rpm
MailScanner-4.66.5-3/perl-Math-BigRat-0.19-1.src.rpm
MailScanner-4.66.5-3/perl-Pod-Escapes-1.04-1.src.rpm
MailScanner-4.66.5-3/perl-Time-HiRes-1.9707-1.src.rpm
MailScanner-4.66.5-3/perl-MIME-Base64-3.07-1.src.rpm
MailScanner-4.66.5-3/install.sh
MailScanner-4.66.5-3/perl-IO-stringy-2.110-1.src.rpm
MailScanner-4.66.5-3/perl-MIME-tools-5.425-1.src.rpm
MailScanner-4.66.5-3/perl-Test-Harness-2.64-1.src.rpm
MailScanner-4.66.5-3/perl-HTML-Parser-3.56-1.src.rpm
MailScanner-4.66.5-3/perl-ExtUtils-MakeMaker-6.32-1.src.rpm
MailScanner-4.66.5-3/QuickInstall.txt
MailScanner-4.66.5-3/perl-Convert-TNEF-0.17-1.src.rpm
MailScanner-4.66.5-3/perl-File-Temp-0.19-1.src.rpm
MailScanner-4.66.5-3/perl-Sys-Syslog-0.18-1.src.rpm
MailScanner-4.66.5-3/perl-File-Spec-0.82-1.src.rpm
MailScanner-4.66.5-3/perl-TimeDate-1.16-3.src.rpm
[root@quitofr ~]#
```

- Verificar que se ha creado una carpeta de nombre MailScanner-4.66.5-3

```
[root@quitofr ~]# ls
1                ftp-0.17-33.fc6.i386.rpm  MailScanner-4.66.5-3
anaconda-ks.cfg  hosts                     MailScanner-4.66.5-3.rpm.tar.gz
Desktop          install.log               msnner.doc
fetch.txt        install.log.syslog        rpmforge-release-0.3.6-1.el5.rf.i386.rpm
[root@quitofr ~]#
```

- Ubicarse en la carpeta MailScanner

```
[root@quitofr ~]# cd MailScanner-4.66.5-3
```

- Listar los contenidos de la carpeta MailScanner

```
[root@quitofr MailScanner-4.66.5-3]# ls
CheckModuleVersion                          perl-MailTools-2.02-1.src.rpm
ExtUtils-MakeMaker-6.30.tar.gz              perl-Math-BigInt-1.86-1.src.rpm
install.sh                                  perl-Math-BigRat-0.19-1.src.rpm
mailscanner-4.66.5-3.noarch.rpm             perl-MIME-Base64-3.07-1.src.rpm
MailScanner-perl-MIME-Base64-3.05-5.src.rpm perl-MIME-tools-5.425-1.src.rpm
perl-Archive-Zip-1.16-1.src.rpm             perl-Net-CIDR-0.11-1.src.rpm
perl-bignum-0.21-1.src.rpm                  perl-Net-IP-1.25-1.src.rpm
perl-Compress-Zlib-1.41-1.src.rpm           perl-Pod-Escapes-1.04-1.src.rpm
perl-Convert-BinHex-1.119-2.src.rpm         perl-Pod-Simple-3.05-1.src.rpm
perl-Convert-TNEF-0.17-1.src.rpm            perl-Scalar-List-Utils-1.19-1.src.rpm
perl-DBD-SQLite-1.13-1.src.rpm              perl-Storable-2.16-1.src.rpm
perl-DBI-1.56-1.src.rpm                     perl-Sys-Hostname-Long-1.4-1.src.rpm
perl-Digest-MD5-2.36-1.src.rpm              perl-Sys-Syslog-0.18-1.src.rpm
perl-ExtUtils-MakeMaker-6.32-1.src.rpm      perl-Test-Harness-2.64-1.src.rpm
perl-File-Spec-0.82-1.src.rpm               perl-Test-Pod-1.26-1.src.rpm
perl-Filesys-Df-0.90-1.src.rpm              perl-Test-Simple-0.70-1.src.rpm
perl-File-Temp-0.19-1.src.rpm               perl-TimeDate-1.16-3.src.rpm
perl-Getopt-Long-2.36-1.src.rpm             perl-Time-HiRes-1.9707-1.src.rpm
perl-HTML-Parser-3.56-1.src.rpm             QuickInstall.txt
perl-HTML-Tagset-3.03-1.src.rpm             README
perl-IO-1.2301-1.src.rpm                    tnef-1.4.3-1.i386.rpm
perl-IO-stringy-2.110-1.src.rpm
[root@quitofr MailScanner-4.66.5-3]#
```

- Compilación de MailScanner

  - El La compilación se debe hacer ubicado dentro de la carpeta MailScanner-4.66.5-3.

```
[root@quitofr MailScanner-4.66.5-3]# ./install.sh


Good. You have the patch command.

Good, you have /usr/src/redhat in place.
You are running release 5 of RedHat, or a clone.
So I will only force the installation of a very few Perl modules.

Writing a .rpmmacros file in your home directory to stop
unpackaged files breaking the build process.
You can delete it once MailScanner is installed if you want to.
```

  - La utilería install.sh procedrá con la compilación del paquete MailScanner

- El proceso de instalación durará un tiempo estimado de media hora al finalizar la instalación se mostrará la siguiente pantalla.

```
Preparing...                ########################################### [100%]
   1:tnef                   ########################################### [100%]

Now to install MailScanner itself.

NOTE: If you get lots of errors here, run the install.sh script
NOTE: again with the command "./install.sh nodeps"

Preparing...                ########################################### [100%]
   1:mailscanner            ########################################### [100%]
Good, SpamAssassin site rules found in /etc/mail/spamassassin

To activate MailScanner run the following commands:

service sendmail stop
chkconfig sendmail off
chkconfig MailScanner on
service MailScanner start

For technical support, please read the MAQ at www.mailscanner.biz/maq/
and buy the book at www.mailscanner.info/store

-----------------------------------------------------------
Please buy the MailScanner book from www.mailscanner.info!
It is a very useful administration guide and introduction
to MailScanner. All the proceeds go directly to making
MailScanner a better supported package than it is today.

[root@quitofr MailScanner-4.66.5-3]#
```

- Comprobar que se instaló MailScanner de manera correcta.

```
[root@quitofr ~]# rpm -q mailscanner
mailscanner-4.66.5-3
[root@quitofr ~]#
```

4.7.2.7 Levantamiento Del Servicio MailScanner

- Bajar el servicio sendmail

```
[root@quitofr ~]# service sendmail stop

Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [  OK  ]
[root@quitofr ~]# chkconfig --level 2345 sendmail off
[root@quitofr ~]#
```

- Iniciar el servicio de MailScanner

```
[root@quitofr MailScanner]# service MailScanner restart
Shutting down MailScanner daemons:
         MailScanner:                                          [FAILED]
         incoming sendmail:                                    [  OK  ]
         outgoing sendmail:                                    [  OK  ]
Waiting for MailScanner to die gracefully  dead.
Starting MailScanner daemons:
         incoming sendmail:                                    [  OK  ]
         outgoing sendmail:                                    [  OK  ]
         MailScanner:                                          [  OK  ]
[root@quitofr MailScanner]#
```

4.7.2.8 Configuración De MailScanner

- Editar el archivo de configuración de MailScanner

```
[root@quitofr ~]# cd /etc/MailScanner/
[root@quitofr MailScanner]# vi MailScanner.conf
```

  - Configurar el nombre de la organización para esto cambiar por el respectivo nombre a la línea

    %org-long-name%=Your Organisation Name Here

```
# Enter the full name of your organisation below, this is used in the
# signature placed at the bottom of report messages sent by MailScanner.
# It can include pretty much any text you like. You can make the result
# span several lines by including "\n" sequences in the text. These will
# be replaced by line-breaks.
%org-long-name% = Your Organisation Name Here

# Enter the location of your organisation's web site below. This is used
# in the signature placed at the bottom of report messages sent by
# MailScanner. It should preferably be the location of a page that you
# have written explaining why you might have rejected the mail and what
# the recipient and/or sender should do about it.


# Enter the full name of your organisation below, this is used in the
# signature placed at the bottom of report messages sent by MailScanner.
# It can include pretty much any text you like. You can make the result
# span several lines by including "\n" sequences in the text. These will
# be replaced by line-breaks.
%org-long-name% = EGAR S.A

# Enter the location of your organisation's web site below. This is used
# in the signature placed at the bottom of report messages sent by
# MailScanner. It should preferably be the location of a page that you
# have written explaining why you might have rejected the mail and what
# the recipient and/or sender should do about it.
```

- Buscar el parámetro Maximum Attachments Per Message = 200 para configurar el número de attachments permitidos por mensaje.

```
# The maximum number of attachments allowed in a message before it is
# considered to be an error. Some email systems, if bouncing a message
# between 2 addresses repeatedly, add information about each bounce as
# an attachment, creating a message with thousands of attachments in just
# a few minutes. This can slow down or even stop MailScanner as it uses
# all available memory to unpack these thousands of attachments.
# This can also be the filename of a ruleset.
Maximum Attachments Per Message = 200

# Expand TNEF attachments using an external program (or a Perl module)?
# This should be "yes" unless the scanner you are using (Sophos, McAfee) has
# the facility built-in. However, if you set it to "no", then the filenames
# within the TNEF attachment will not be checked against the filename rules.
Expand TNEF = yes
```

- Cambiarla por 10

```
# The maximum number of attachments allowed in a message before it is
# considered to be an error. Some email systems, if bouncing a message
# between 2 addresses repeatedly, add information about each bounce as
# an attachment, creating a message with thousands of attachments in just
# a few minutes. This can slow down or even stop MailScanner as it uses
# all available memory to unpack these thousands of attachments.
# This can also be the filename of a ruleset.
Maximum Attachments Per Message = 10

# Expand TNEF attachments using an external program (or a Perl module)?
# This should be "yes" unless the scanner you are using (Sophos, McAfee) has
# the facility built-in. However, if you set it to "no", then the filenames
# within the TNEF attachment will not be checked against the filename rules.
Expand TNEF = yes
```

- Activación del Sistema Antivirus por medio de MailScanner, para esto verificar que el parámetro Virus Scanning se encuentre activado con yes.

```
# Do you want to scan email for viruses?
# A few people don't have a virus scanner licence and so want to disable
# all the virus scanning.
# If you use a ruleset for this setting, then the mail will be scanned if
# *any* of the rules match (except the default). That way unscanned mail
# never reaches a user who is having their mail virus-scanned.
#
# If you want to be able to switch scanning on/off for different users or
# different domains, set this to the filename of a ruleset.
# This can also be the filename of a ruleset.
Virus Scanning = yes

# Which Virus Scanning package to use:
# sophos    from www.sophos.com, or
# sophossavi (also from www.sophos.com, using the SAVI perl module), or
```

- Asignar el antivirus a utilizar por MailScanner, para esto buscar el parámetro Virus Scanners=Auto

```
# Note: If you specify "auto" then MailScanner will search for all the
#       scanners you have installed and will use all of them. If you really
#       want none, then specify "none".
#
# This *cannot* be the filename of a ruleset.
Virus Scanners = auto

# The maximum length of time the commercial virus scanner is allowed to run
# for 1 batch of messages (in seconds).
```

- Cambiarla por Virus Scanners=Clamav

```
#
# Note: If you specify "auto" then MailScanner will search for all the
#       scanners you have installed and will use all of them. If you really
#       want none, then specify "none".
#
# This *cannot* be the filename of a ruleset.
Virus Scanners = clamav

# The maximum length of time the commercial virus scanner is allowed to run
# for 1 batch of messages (in seconds).
```

- Activación del sistema Antispam, para esto verificar que se encuentre activado el parámetro Spam Checks=yes.

```
# Do you want to check messages to see if they are spam?
# Note: If you switch this off then *no* spam checks will be done at all.
#       This includes both MailScanner's own checks and SpamAssassin.
#       If you want to just disable the "Spam List" feature then set
#       "Spam List =" (i.e. an empty list) in the setting below.
# This can also be the filename of a ruleset.
Spam Checks = yes

# This is the list of spam blacklists (RBLs) which you are using.
# See the "Spam List Definitions" file for more information about what
```

- Activar spamassassin con el parámetro Use SpamAssassin=yes.

```
# SpamAssassin
# ------------
#

# Do you want to find spam using the "SpamAssassin" package?
# This can also be the filename of a ruleset.
Use SpamAssassin = yes

# SpamAssassin is not very fast when scanning huge messages, so messages
# bigger than this value will be truncated to this length for SpamAssassin
# testing. The original message will not be affected by this. This value
# is a good compromise as very few spam messages are bigger than this.
```

- Configurar el record para el spam, para esto buscar los parámetros:

  Required SpamAssassin Score=6

  High SpamAssassin Score=10

```
# This replaces the SpamAssassin configuration value 'required_hits'.
# If a message achieves a SpamAssassin score higher than this value,
# it is spam. See also the High SpamAssassin Score configuration option.
# This can also be the filename of a ruleset, so the SpamAssassin
# required_hits value can be set to different values for different messages.
Required SpamAssassin Score = 6


# If a message achieves a SpamAssassin score higher than this value,
# then the "High Scoring Spam Actions" are used. You may want to use
# this to deliver moderate scores, while deleting very high scoring messsages.
# This can also be the filename of a ruleset.
High SpamAssassin Score = 10
```

- Cambiarlo por:

  Required SpamAssassin Score=3.9

  High SpamAssassin Score=5

```
# This replaces the SpamAssassin configuration value 'required_hits'.
# If a message achieves a SpamAssassin score higher than this value,
# it is spam. See also the High SpamAssassin Score configuration option.
# This can also be the filename of a ruleset, so the SpamAssassin
# required_hits value can be set to different values for different messages.
Required SpamAssassin Score = 3.9

# If a message achieves a SpamAssassin score higher than this value,
# then the "High Scoring Spam Actions" are used. You may want to use
# this to deliver moderate scores, while deleting very high scoring messsages.
# This can also be the filename of a ruleset.
High SpamAssassin Score = 5
```

  - Con esto se especifíca bajo que records será identificado el spam.

- Especificar que acciones tomar contra el spam, para esto buscar el parámetro Spam Actions.

```
#
# The default value I have set here enables Thunderbird 1.5 to automatically
# handle spam when set to trust the "SpamAssassin" headers.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
#Spam Actions = store forward anonymous@ecs.soton.ac.uk
Spam Actions = deliver header "X-Spam-Status: Yes"
```

- Cambiarlo por Spam Actions= delete

```
# The default value I have set here enables Thunderbird 1.5 to automatically
# handle spam when set to trust the "SpamAssassin" headers.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
#Spam Actions = store forward anonymous@ecs.soton.ac.uk
Spam Actions = delete
```

- Acciones a tomar con el spam que sobrepase el record asignado en el parámetro High SpamAssassin Score=5. Para esto buscar el parámetro Hight Scoring Spam Actions=deliver header ´´X-Spam-Status: yes ´´

```
# The default value I have set here enables Thunderbird 1.5 to automatically
# handle spam when set to trust the "SpamAssassin" headers.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
High Scoring Spam Actions = deliver header "X-Spam-Status: Yes"
```

- Cambiarlo por: Hight Scoring Spam Actions= delete

```
# The default value I have set here enables Thunderbird 1.5 to automatically
# handle spam when set to trust the "SpamAssassin" headers.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
High Scoring Spam Actions = delete
```

- Acciones a tomar con el correo identificado como no spam. Para esto el parámetro:

  Non Spam Actions=deliver header ´´X-Spam-Status: No´´

```
# The default value I have set here enables Thunderbird 1.5 to automatically
# handle spam when set to trust the "SpamAssassin" headers.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
Non Spam Actions = deliver header "X-Spam-Status: No"
```

- Cambiarlo por:

  Non Spam Actions=deliver

```
# The default value I have set here enables Thunderbird 1.5 to automatically
# handle spam when set to trust the "SpamAssassin" headers.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
Non Spam Actions = deliver
```

- Reiniciar el servicio de MailScanner para que los cambios tengan efecto

```
[root@quitofr MailScanner]# service MailScanner restart
Shutting down MailScanner daemons:
         MailScanner:                                          [FAILED]
         incoming sendmail:                                    [  OK  ]
         outgoing sendmail:                                    [  OK  ]
Waiting for MailScanner to die gracefully  dead.
Starting MailScanner daemons:
         incoming sendmail:                                    [  OK  ]
         outgoing sendmail:                                    [  OK  ]
         MailScanner:                                          [  OK  ]
[root@quitofr MailScanner]#
```

4.7.2.9 Pruebas de Funcionalidad De MailScanner

- Envío por webmail de un mensaje con virus de prueba de la página www.eicar.org.
  - Copiar el texto de la página www.eicar.org/download/eicar.com.txt

FIGURA 4. 22: TEXTO PARA TEST DE FUNCIONAMIENTO DEL SISTEMA ANTIVIRUS

- El texto copiado enviarlo como mensaje de correo.

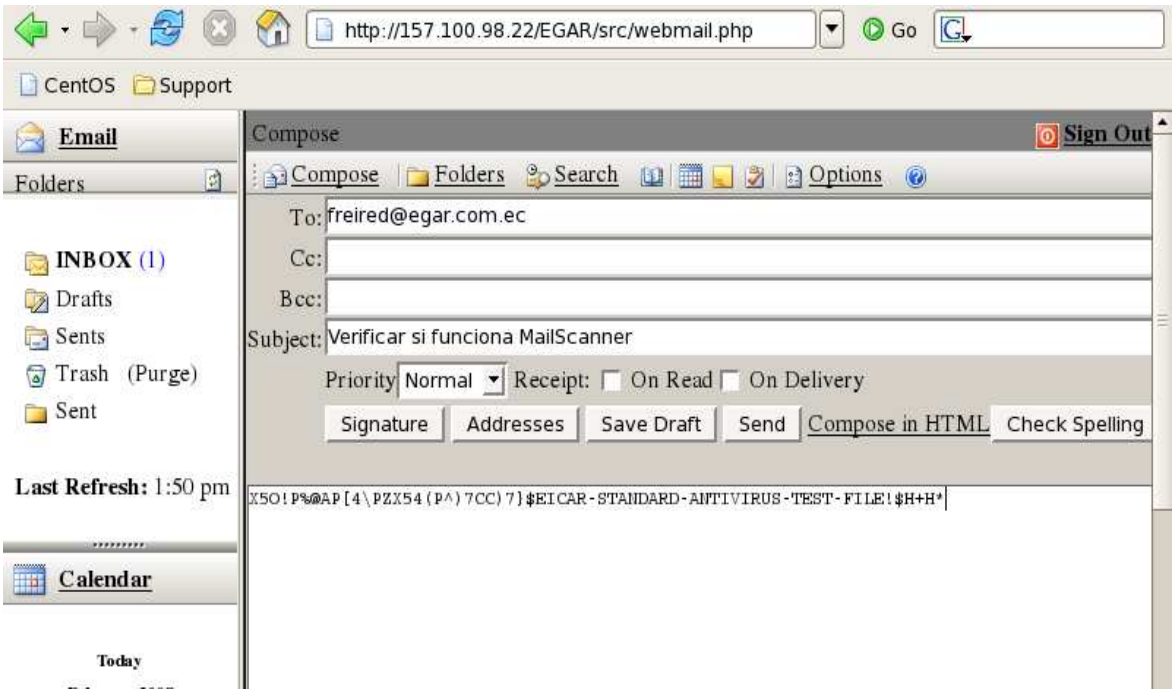

FIGURA 4. 23: PRUEBA DE FUNCIONAMIENTO DE MAILSCANER

- Verificar que se detectó un virus mediante el mensaje en la bandeja de entrada

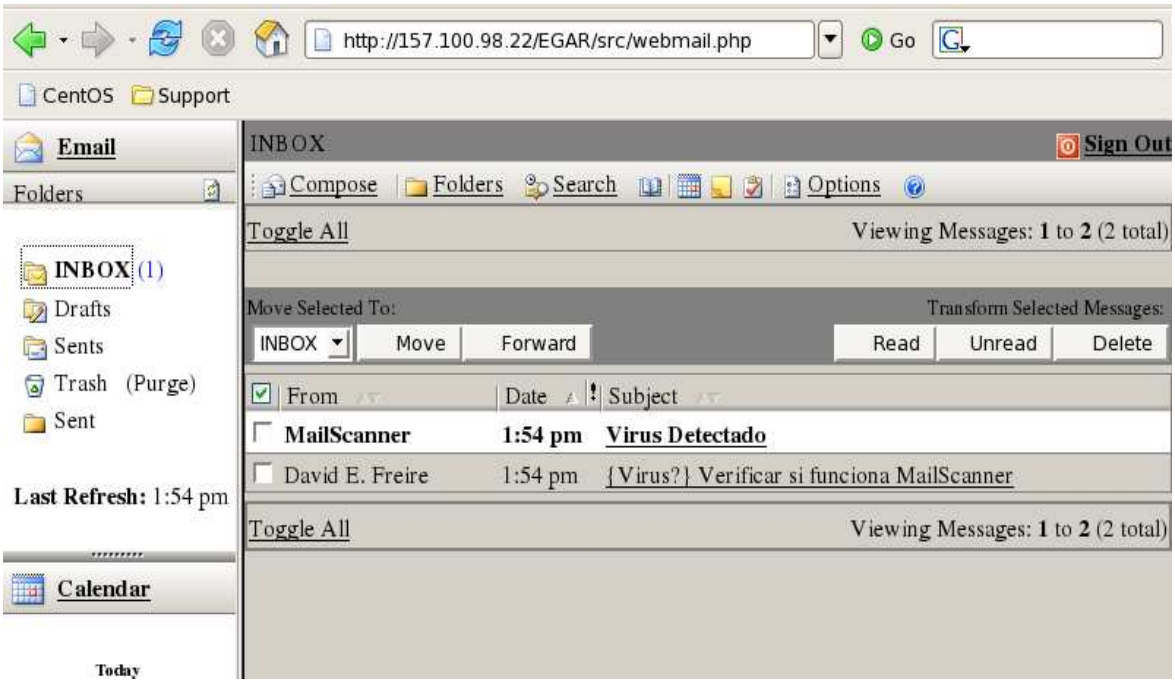

FIGURA 4. 24: DETECCIÓN DE VIRUS POR PARTE DE MAILSCANNER

- Envío por medio de webmail de un mensaje con spam.

- De la página http://spamassassin.apache.org/gtube/, escoger el siguiente texto: XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

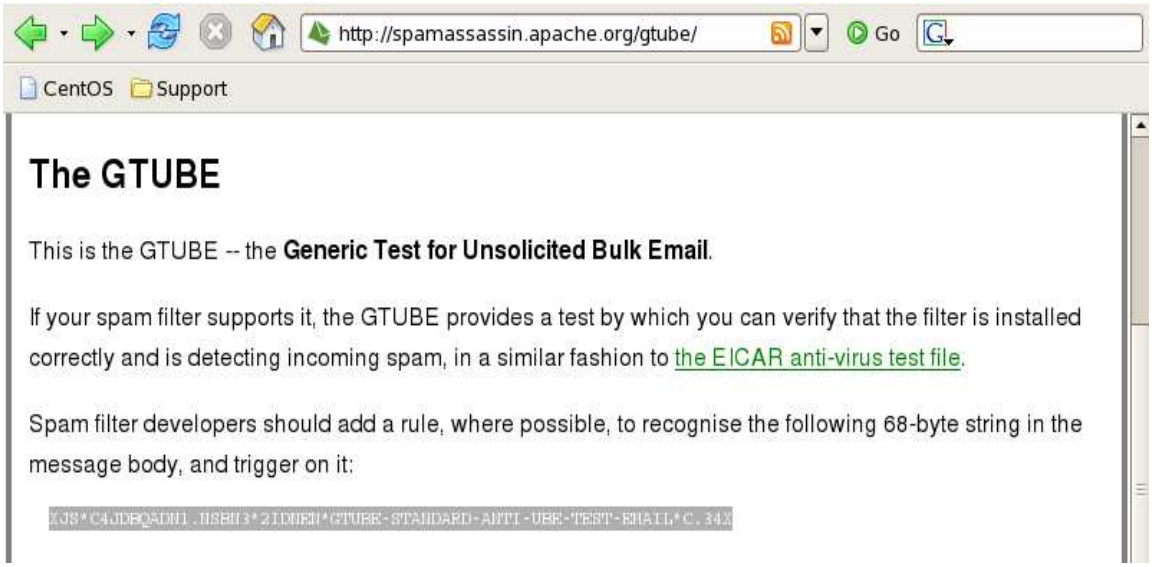

FIGURA 4. 25: TEXTO DE PRUEBA PARA FUNCIONAMIENTO DEL SISTEMA ANTISPAM

- El texto copiado enviar como mensaje de correo.

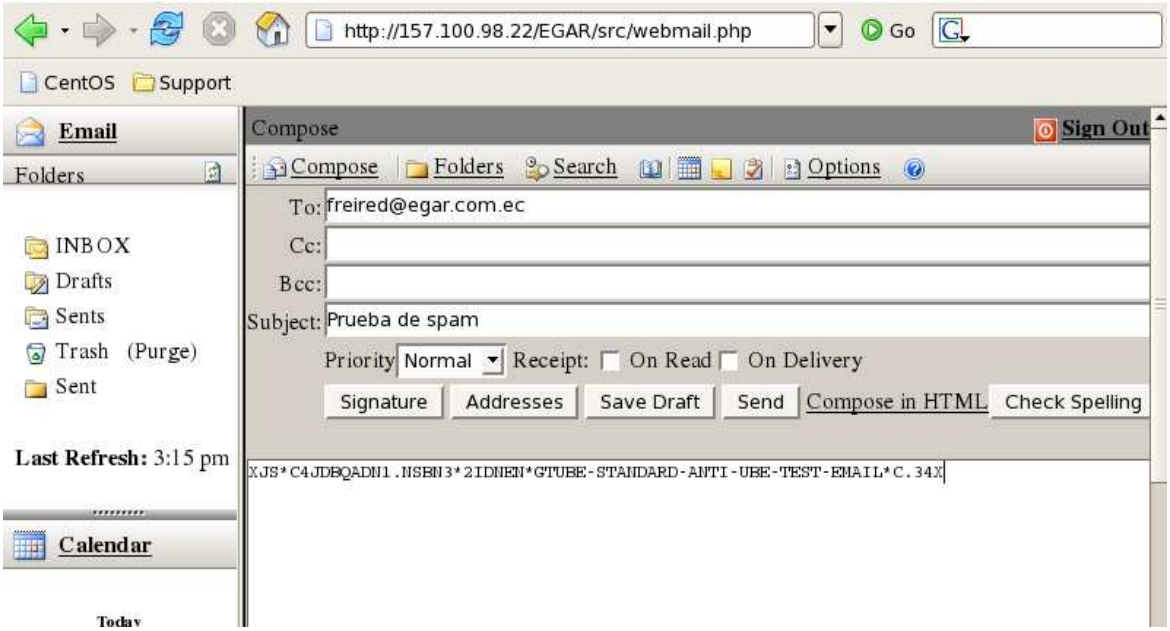

FIGURA 4. 26: PRUEBA DE FUNCIONAMIENTO DEL SISTEMA ANTISPAM

- Verificar por logs que se detectó el mensaje como spam.

```
[root@quitofr ~]# tail -fn2 /var/log/maillog
Feb 18 15:18:30 quitofr sendmail[9461]: m1IKHeQ4009419: to=freired, delay=00:00:24, xdelay=00:00:
00, mailer=local, pri=169077, dsn=2.0.0, stat=Sent
Feb 18 15:18:39 quitofr sendmail[9432]: m1IKHsXg009432: from=<webmaster@promote-bz.net>, size=331
8, class=0, nrcpts=1, msgid=<20080219042046.E10A50B310A93AA5@from.header.has.no.domain>, proto=ES
MTP, daemon=MTA, relay=[58.244.217.47]
Feb 18 15:18:39 quitofr MailScanner[8614]: New Batch: Scanning 1 messages, 3813 bytes
Feb 18 15:18:41 quitofr MailScanner[8614]: Spam Checks: Found 1 spam messages
Feb 18 15:18:41 quitofr MailScanner[8614]: Virus and Content Scanning: Starting
```

4.7.2.10 Configuraciones Avanzadas De Seguridad para Sendmail

- Se configurará técnicas avanzadas de seguridad para Sendmail para combatir de mejor manera la entrada de virus y spam.

- Técnica del greet_pause
  - La técnica del greet_pause consiste en retardar el mensaje de bienvenida de sendmail para después aceptar correo electrónico. El tiempo en este caso será de 3sg expresados en milisegundos.

- Editar el archivo sendmail.mc

```
[root@quitofr ~]# vi /etc/mail/sendmail.mc
```

- Buscar el parámetro:

  FEATURE(‘ access_db’ , ‘hash –T<TMPF> -o /etc/mail/access.db’)dnl

```
dnl define(`confCONNECTION_RATE_THROTTLE', `3')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
```

- A continuación aumentar el parámetro de los 3000 milsegundos:

  FEATURE(‘ greet_pause’ , ‘3000’)

```
dnl define(`confCONNECTION_RATE_THROTTLE', `3')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(`greet_pause', `3000')
FEATURE(`blacklist_recipients')dnl
EXPOSED_USER(`root')dnl
```

- Prohibir conexiones desde sitios listados en listas negras
  - Las listas negras a utilizar serán las de sorbs.net, spamhaus.org y spamcop.net

➢ Buscar el parámetro: FEATURE(delay_checks)dnl

```
dnl #
dnl define(`confDONT_BLAME_SENDMAIL', `groupreadablekeyfile')dnl
dnl #
define(`confTO_QUEUEWARN', `1h')dnl
define(`confTO_QUEUERETURN', `1d')dnl
dnl define(`confQUEUE_LA', `12')dnl
dnl define(`confREFUSE_LA', `18')dnl
define(`confTO_IDENT', `0')dnl
FEATURE(delay_checks)dnl
FEATURE(`no_default_msa', `dnl')dnl
```

➢ A continuación aumentar las siguientes líneas:

FEATURE(`dnsbl',`dul.dnsbl.sorbs.net',`"554 Rejected " $" – see
http://www.sorbs.net/lookup.shtml?"$')dnl
FEATURE(`dnsbl',`nomail.rhsbl.sorbs.net',`"554 Rejected " $" – see
http://www.sorbs.net/lookup.shtml?"$')dnl
FEATURE(dnsbl, `sbl-xbl.spamhaus.org', `"554 Rejected – see
http://www.spamhaus.org/query/bl?ip=+"$')dnl
FEATURE(`dnsbl', `bl.spamcop.net', `554 Rejected - see http://spamcop.net/')dnl

```
define(`confTO_IDENT', `0')dnl
FEATURE(delay_checks)dnl
FEATURE(`dnsbl',`dul.dnsbl.sorbs.net',`"554 Rejected " $" - see http://www.sorbs.net/lookup.shtm
?"$')dnl
FEATURE(`dnsbl',`nomail.rhsbl.sorbs.net',`"554 Rejected " $" - see http://www.sorbs.net/lookup.s
tml?"$')dnl
FEATURE(dnsbl, `zen.spamhaus.org', `"554 Rejected - see  http://www.spamhaus.org/query/bl?ip=+"$
)dnl
FEATURE(`dnsbl', `bl.spamcop.net', `554 Rejected - see http://spamcop.net/')dnl
FEATURE(`no_default_msa', `dnl')dnl
```

- Pruebas de chequeo en listas negras por sendmail.

```
[root@quitofr ~]# tail -fn2 /var/log/maillog

Feb 18 13:43:31 quitofr sendmail[6360]: m1IIhKjg006360: ruleset=check_rcpt, arg1=<hidalgo@egar.co
m.ec>, relay=3.45.73-86.rev.gaoland.net [86.73.45.3] (may be forged), reject=554 5.7.1 Rejected -
 see http://www.sorbs.net/lookup.shtml?$
Feb 18 13:43:31 quitofr sendmail[6360]: m1IIhKjg006360: ruleset=check_rcpt, arg1=<garrido@egar.co
m.ec>, relay=3.45.73-86.rev.gaoland.net [86.73.45.3] (may be forged), reject=554 5.7.1 Rejected -
 see http://www.sorbs.net/lookup.shtml?$
Feb 18 13:43:31 quitofr sendmail[6360]: m1IIhKjg006360: ruleset=check_rcpt, arg1=<andradee@egar.c
om.ec>, relay=3.45.73-86.rev.gaoland.net [86.73.45.3] (may be forged), reject=554 5.7.1 Rejected
- see http://www.sorbs.net/lookup.shtml?$
Feb 18 13:43:31 quitofr sendmail[6360]: m1IIhKjg006360: ruleset=check_rcpt, arg1=<garridogarridom
@egar.com.ec>, relay=3.45.73-86.rev.gaoland.net [86.73.45.3] (may be forged), reject=554 5.7.1 Re
jected - see http://www.sorbs.net/lookup.shtml?$
```

- Prevenir El Spam De Imágenes
  - Ir al directorio /etc/mail/spamassassin
  - Descargar de la página www.rulesemporium.com/plugins/ los plugins ImageInfo.pm y ImageInfo.cf necesarios para detectar el spam de imágenes.

```
[root@quitofr ~]# cd /etc/mail/spamassassin/
[root@quitofr spamassassin]# wget http://www.rulesemporium.com/plugins/ImageInfo.pm
--13:51:16--  http://www.rulesemporium.com/plugins/ImageInfo.pm
Resolving www.rulesemporium.com... 72.52.4.74
Connecting to www.rulesemporium.com|72.52.4.74|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13495 (13K) [text/plain]
Saving to: `ImageInfo.pm'

100%[======================================================>] 13,495      15.1K/s   in 0.9s

13:51:18 (15.1 KB/s) - `ImageInfo.pm' saved [13495/13495]

[root@quitofr spamassassin]# wget http://www.rulesemporium.com/plugins/imageinfo.cf
--13:51:33--  http://www.rulesemporium.com/plugins/imageinfo.cf
Resolving www.rulesemporium.com... 72.52.4.74
Connecting to www.rulesemporium.com|72.52.4.74|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5447 (5.3K) [text/plain]
Saving to: `imageinfo.cf'

100%[======================================================>] 5,447       17.2K/s   in 0.3s

13:51:34 (17.2 KB/s) - `imageinfo.cf' saved [5447/5447]

[root@quitofr spamassassin]#
```

- Editar el archivo init.pre y al final del archivo agregar :

```
[root@quitofr spamassassin]# vi init.pre
```

```
loadplugin Mail::SpamAssassin::Plugin::URIDNSBL

# Hashcash - perform hashcash verification.
#
loadplugin Mail::SpamAssassin::Plugin::Hashcash

# SPF - perform SPF verification.
#
loadplugin Mail::SpamAssassin::Plugin::SPF
loadplugin Mail::SpamAssassin::Plugin::ImageInfo /etc/mail/spamassassin/ImageInfo.pm
```

  - La línea agregada habilitará a spamassassin con funciones de detecciones de spam de imágenes.

loadplugin Mail::Spamassassin::Plugin::ImageInfo /etc/mail/spamassassin/ImageInfo.pm

- Recompilar el archivo de configuración sendmail.cf para los nuevos cambios realizados.

```
[root@quitofr ~]# make -C /etc/mail
make: Entering directory `/etc/mail'
make: Leaving directory `/etc/mail'
[root@quitofr ~]#
```

- Reiniciar MailScanner

```
[root@quitofr ~]# service MailScanner restart
Shutting down MailScanner daemons:
         MailScanner:                                          [FAILED]
         incoming sendmail:                                    [  OK  ]
         outgoing sendmail:                                    [  OK  ]
Waiting for MailScanner to die gracefully  dead.
Starting MailScanner daemons:
         incoming sendmail:                                    [  OK  ]
         outgoing sendmail:                                    [  OK  ]
         MailScanner:                                          [  OK  ]
[root@quitofr ~]#
```

4.8 IMPLEMENTACIÓN DEL SERVICIO SAMBA.

4.8.1 INSTALACIÓN DE LOS PAQUETES NECESARIOS

- Los paquetes necesarios para la implementación del Samba son:

  samba-client

  samba-common

  samba.

```
[root@quitofr ~]# rpm -qa |grep sam
system-config-samba-1.2.39-1.el5
samba-client-3.0.23c-2
samba-common-3.0.23c-2
samba-3.0.23c-2
[root@quitofr ~]#
```

- Por Yum

```
[root@quitofr ~]# yum -y install smb-client samba-common samba
```

- Mediante los CD's de Instalación de Centos 5.0
  - Insertar el CD #2 de Centos y Montar la Unidad de CDROM

```
[root@quitofr ~]# mount /dev/hda /media
```

  - Ir al directorio CentOs que se encuentra dentro de la unidad montada /media/

```
[root@quitofr ~]# cd /media/CentOs
```

  - Instalar los paquetes samba-3.0.23c-2.i386.rpm , samba-client-3.0.23c-2.i386.rpm , samba-common-3.0.23c-2.i386.rpm

```
[root@quitofr CentOs]# rpm - ivh samba-3.0.23c-2.i386.rpm samba-client-3.0.23c-2.i386.rpm samba-common-3.0.23c-2.i386.rpm
```

4.8.2 VERIFICACIÓN DE INSTALACIÓN DE LOS PAQUETES

- Los paquetes necesarios para la implementación del Samba son:
  - samba-client
  - samba-common
  - samba

```
[root@quitofr ~]# rpm -qa |grep sam
system-config-samba-1.2.39-1.el5
samba-client-3.0.23c-2
samba-common-3.0.23c-2
samba-3.0.23c-2
[root@quitofr ~]#
```

- Estos paquetes vienen instalados de forma predeterminada con la instalación de Centos 5.0 en modo de servidor Samba. En caso de no estar instalados se puede utilizar la instlación por Yum o por los cd's de instalación descritos anteriormente.

4.8.3 CONFIGURACIÓN DE SAMBA

- Creación de usuarios samba
  - El formato de creación de usuarios samba es el siguiente: Se creará el usuario freired

```
[root@quitofr ~]# smbpasswd -a freired
New SMB password:
Retype new SMB password:
[root@quitofr ~]#
```

  - La opción –a permite crear el usuario y a la vez configurar su password.
  - Los usuarios de samba son diferentes a los usuarios del sistema, para la conexión con máquinas Windows es necesario que el password del usuario samba coincida con la clave del usuario Windows.
- Editar el archivo de configuración de samba (smb.conf)

```
[root@quitofr ~]# cd /etc/samba/
[root@quitofr samba]# vi smb.conf
```

- Determinar que redes podrán acceder al servidor

```
[root@quitofr ~]# cd /etc/samba/
[root@quitofr samba]# vi smb.conf


# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
 hosts allow = 192.168.1.  127.

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
```

  - Por medio del parámetro host allow se indica que red prodrá acceder al servidor.

En este caso se configurará como redes permitidas a la red 192.168.1 y allocal host 127.0.0.0

- Determinar la interfaz por el cual el servidor samba atenderá peticiones.
  - Por medio del parámetro interfaces se indica por que interfaz de red atenderá peticiones.
    En este caso atenderá peticiones por medio de la interfaz interna 192.168.1.1

```
# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting.
# Note: Consider carefully the location in the configuration file of
#       this line.  The included file is read at that point.
;   include = /usr/local/samba/lib/smb.conf.%m

# Configure Samba to use multiple interfaces
# If you have multiple network interfaces then you must list them
# here. See the man page for details.
interfaces = 192.168.1.1/24
```

4.8.4 INICIAR EL SERVICIO SAMBA.

```
[root@quitofr ~]# service smb start
Starting SMB services:                                     [  OK  ]
Starting NMB services:                                     [  OK  ]
[root@quitofr ~]#
```

4.8.5 PRUEBAS DE FUNCIONALIDAD ACCEDIENDO A RECURSOS COMPARTIDOS DE UNA MÁQUINA WINDOWS.

- Listar las carpetas compartidas del usuario freired en una máquina Windows XP de nombre ASISTEMAS.

```
[root@quitofr ~]# smbclient -U freired -L ASISTEMAS
Password:
Domain=[EGAROFC] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
        Instaladores    Disk
        RESPALDOS       Disk
        E$              Disk      Recurso predeterminado
        IPC$            IPC       IPC remota
        RESPALDOS DECWIN Disk
        DAVE            Disk
        RESPALDOSENERO  Disk
        Resflujo        Disk
        ADMIN$          Disk      Admin remota
        MAIL            Disk
        C$              Disk      Recurso predeterminado
        AVG             Disk
Domain=[EGAROFC] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
[root@quitofr ~]#
```

- Acceso al recurso compartido DAVE

```
[root@quitofr ~]# smbclient -U freired //ASISTEMAS/DAVE
Password:
Domain=[EGAROFC] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> ls
  REPORTE DE VENTAS                   D        0  Thu Dec 27 15:05:29 2007
  REPORTES TÉCNICOS                   D        0  Fri Feb  8 12:48:48 2008
  reportesaldos2006.doc               A    94720  Thu Dec 27 15:05:29 2007
  respaldar                           A     4028  Thu Dec 27 15:05:29 2007
  respaldo                            D        0  Thu Dec 27 15:05:29 2007
  Respaldo Flash                      D        0  Thu Dec 27 15:06:37 2007
  Respaldo SCIE                       A  9049600  Mon Feb 26 17:25:19 2007
  Respaldo SCIE26-02                  A  4525568  Mon Feb 26 11:00:51 2007
  RESPALDOS directorios LINUX         D        0  Thu Dec 27 15:06:40 2007
  RESPALDP                            D        0  Sat Dec 29 12:03:23 2007
  SALDOS                              D        0  Sat Dec 29 11:53:01 2007
  SALDOS.XLS                          A  2263040  Thu Dec 27 15:07:16 2007
  SCIE161107                          A 18171392  Fri Nov 16 18:05:19 2007
  SCIE31-11-2007                      A  9483776  Fri Nov 30 17:48:19 2007
  SISTEMA DE GESTION DE CALIDAD       D        0  Thu Dec 27 15:07:16 2007
  sm_sep.dbf                          A    13074  Thu Dec 27 15:07:16 2007
  spp16-11-07                         A  2704896  Fri Nov 16 18:09:30 2007
  tener huevos.JPG                    A    59258  Thu Dec 27 15:07:16 2007
  Thumbs.db                         AHS    53248  Thu Dec 27 15:07:16 2007
  Top10deMujeresalVolante_1_.pps      A   358912  Thu Dec 27 15:07:16 2007
  tutoriales                          D        0  Thu Dec 27 15:07:16 2007
  Tu_Angel1[1][1][1]....pps           A   568320  Thu Dec 27 15:07:16 2007
  UTILIDADES LINUX                    D        0  Thu Dec 27 15:16:15 2007
  Versiones SQL Server                D        0  Thu Dec 27 15:16:16 2007
  winzip80.exe                        A  1259448  Thu Dec 27 15:16:16 2007
  ZOOM.pps                            A   757760  Thu Dec 27 15:16:17 2007

                39997 blocks of size 1048576. 9017 blocks available
smb: \>
```

- Acceso a recursos compartidos por medio de montajes de unidades de red
  - Crear un punto de montaje en este caso de nombre respaldar en el directorio /mnt/

```
[root@quitofr ~]# mkdir /mnt/respaldar/
```

  - Montar el directorio DAVE en el punto de montaje /mnt/respaldar/

```
[root@quitofr ~]# mount -t cifs -o username=freired,password=Asis777 //192.168.1.11/DAVE /mnt/res
paldar/
[root@quitofr ~]#
```

  - Listar el contenido de /mnt/respaldar

```
[root@quitofr ~]# cd /mnt/respaldar/
[root@quitofr respaldar]# ls |less

REPORTE DE VENTAS
reportesaldos2006.doc
REPORTES TÉCNICOS
respaldar
respaldo
Respaldo Flash
Respaldo SCIE
Respaldo SCIE26-02
RESPALDOS directorios LINUX
RESPALDP
SALDOS
SALDOS.XLS
SCIE161107
SCIE31-11-2007
SISTEMA DE GESTION DE CALIDAD
sm_sep.dbf
spp16-11-07
tener huevos.JPG
Thumbs.db
Top10deMujeresalVolante_1_.pps
Tu_Angel1[1][1][1]....pps
tutoriales
UTILIDADES LINUX
Versiones SQL Server
winzip80.exe
ZOOM.pps
```

- Respaldo comprimido de un directorio que se encuentra en una máquina Windows.
  - Para efectos prácticos se montará un directorio de menor tamaño.
  - Compartir la carpeta AVG ubicada en el Disco C de una máquina WINDOWS XP.

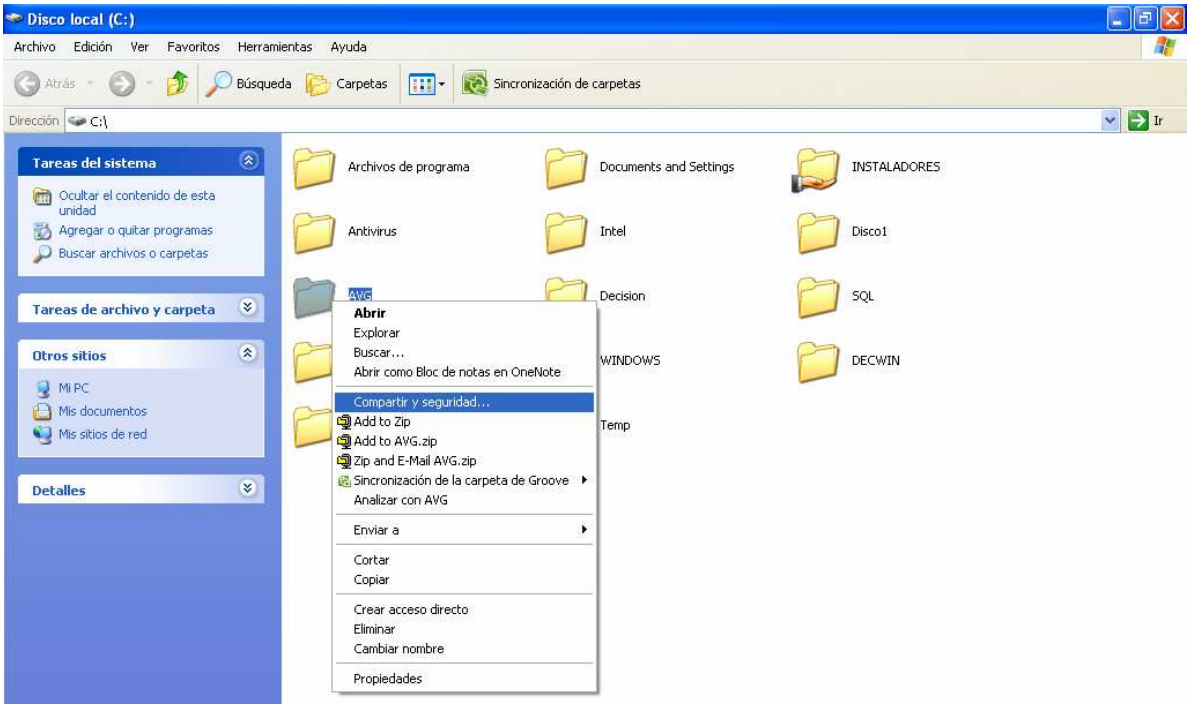

FIGURA 4. 27: COMPARTIR RECURSOS EN WINDOWS XP

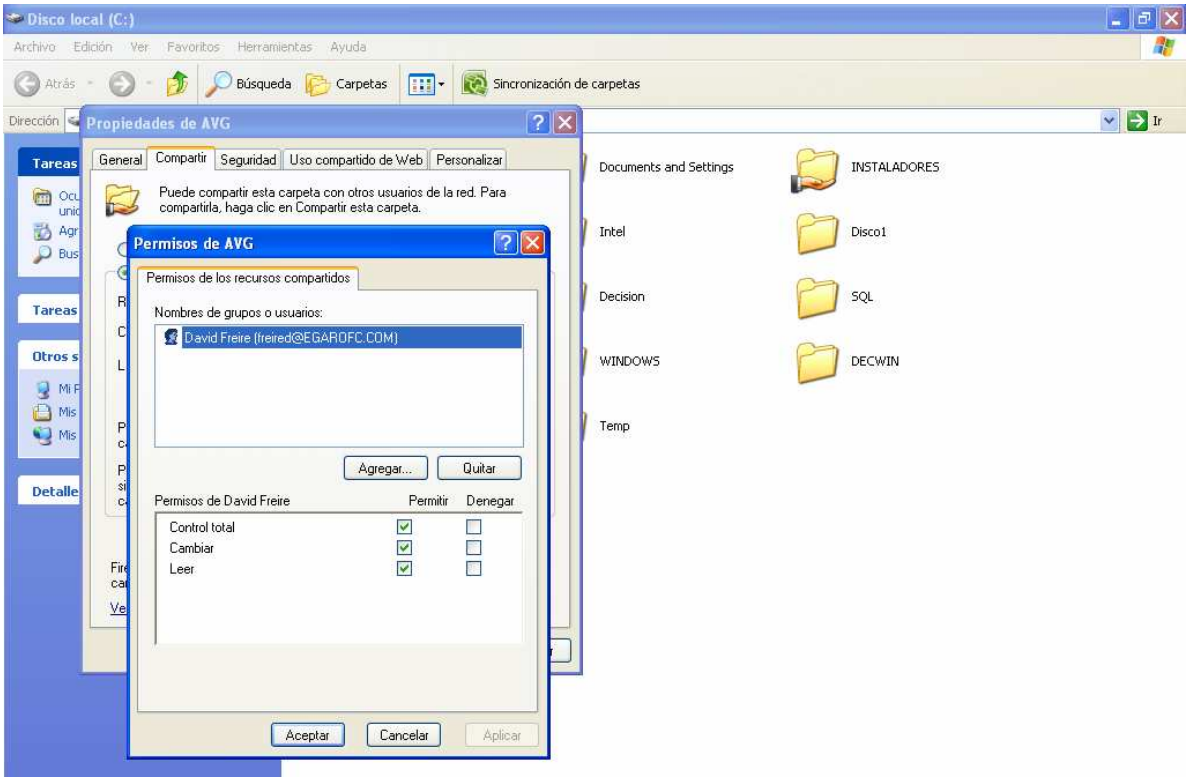

FIGURA 4. 28 : ASIGNACIÓN DE PERMISOS PARA RECURSOS COMPARTIDOS EN WINDOWS XP

- MONTAJE DE LA CARPETA AVG EN LINUX AVG////

```
[root@quitofr ~]# mount -t cifs -o username=freired,password=Asis777 //192.168.1.11/AVG /mnt/respaldar
```

- Listar el contenido de /mnt/respaldar.

```
[root@quitofr ~]# cd /mnt/respaldar/
[root@quitofr respaldar]# ls
AVG  f210.exe  sql
[root@quitofr respaldar]# cd AVG/
[root@quitofr AVG]# ls
avg75f_516a1225.exe  Licencia AVG.txt
[root@quitofr AVG]#
```

  - Se lista el contenido del directorio /mnt/respaldar y posteriormente del directorio AVG.

- Compresión en formato tar.gz del directorio /mnt/respaldar.

```
[root@quitofr ~]# tar -zcf /home/freired/AVG09-02-2008.tar.gz /mnt/respaldar/
tar: Removing leading `/' from member names
[root@quitofr ~]#
```

  - tar es una herramienta que permite el respaldo de archivos en forma de filesystem.
  - Con el parámetro –zcf se indica que cree un archivo comprimido de nombre AVG09-02-2008.tar.gz

- Verificar que se creó el archivo comprimido AVG09-02-2008.tar.gz en el directorio /home/freired.

```
[root@quitofr ~]# cd /home/freired/
[root@quitofr freired]# ls
AVG09-02-2008.tar.gz  mail
[root@quitofr freired]#
```

- Recuperación del archivo AVG09-02-2008.tar.gz

```
[root@quitofr freired]# ls
AVG09-02-2008.tar.gz  mail
[root@quitofr freired]# tar -zxf /home/freired/AVG09-02-2008.tar.gz
```

- Acceso por medio de Explorador de Windows al archivo descomprimido AVG

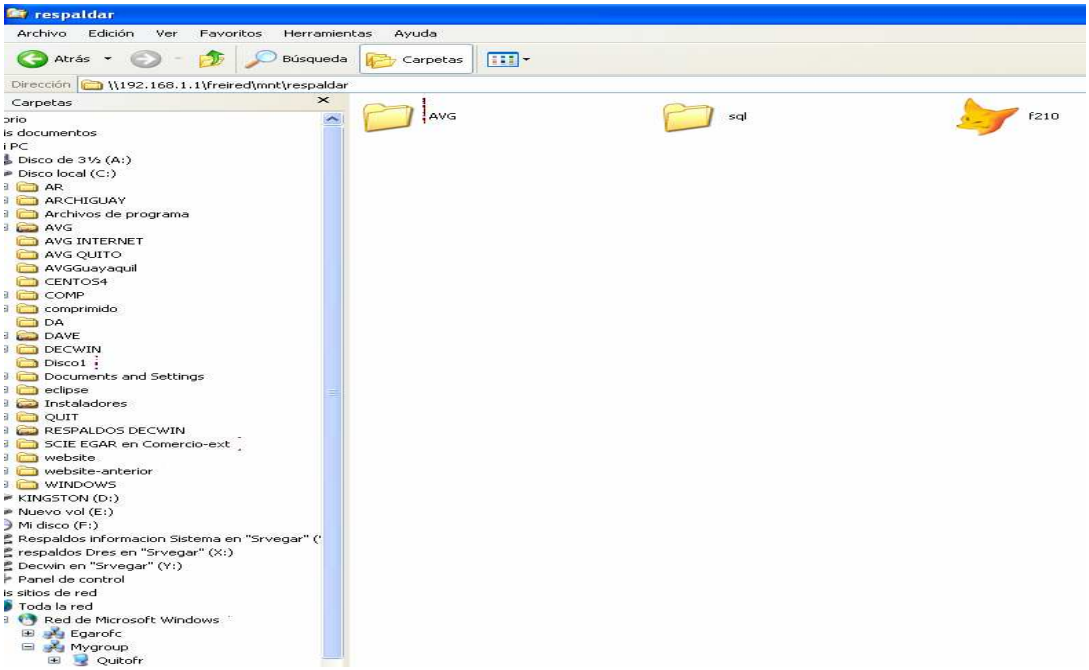

FIGURA 4. 29 : ACCESO AL SERVIDOR SAMBA POR MEDIO DE INTERNET EXPLORER

4.8.6 Scripts para ejecución de respaldos de información.

4.8.6.1 Script para el respaldo del directorio que contiene las declaraciones al SRI.

- El script consistirá en conectarse a una máquina WindowsXP de IP 192.168.1.5 para respaldar la información de declaraciones al SRI. Para esto se enviá como parámetros generales del archivo la IP de la máquina, el nombre de usuario, la contraseña, el punto de montaje, y la tarea a realizar.

- Crear un punto de montaje de nombre sri en el directorio /mnt/

```
[root@quitofr ~]# mkdir /mnt/sri
```

- Crear un archivo de script de nombre respaldarsri.

```
[root@quitofr ~]# vi respaldarsri
x=`date +%d%b%Y`
mount -t cifs -o username=bedoyal,workgroup=EGAROFC,password=Cont5522 //192.168.1.5/E /mnt/sri/
mkdir /home/freired/SRI$x
cp -r /mnt/sri/rentados/ /home/freired/SRI$x/rentados
cp -r /mnt/sri/XML_ANEXO_RENTA/ /home/freired/SRI$x/XML_ANEXO_RENTA
cp -r /mnt/sri/XML_ANEXO_TRANSACCIONAL/ /home/freired/SRI$x/XML_ANEXO_TRANSACCIONAL
cp -r /mnt/sri/XML_DECLARACIONES/ /home/freired/SRI$x/XML_DECLARACIONES
tar -zcf  /home/freired/bedoyal$x.tar.gz /mnt/sri/Contabilidad
umount /mnt/sri/
```

- Ejecución del script creado.
  - sh permite ejecutar el código de shell que se encuentre en el archivo respaldarsri. Con el parámetro & se indica que se ejecute en segundo plano.

```
[root@quitofr ~]# sh respaldarsri &
[1] 30104
[root@quitofr ~]#
```

- Comprobar que el proceso de compresión tar-zcf este activo.

```
[root@quitofr ~]# ps au
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      3125  0.0  0.0   1628   440 tty2     Ss+  Feb05   0:00 /sbin/mingetty tty2
root      3126  0.0  0.0   1628   464 tty3     Ss+  Feb05   0:00 /sbin/mingetty tty3
root      3127  0.0  0.0   1628   444 tty4     Ss+  Feb05   0:00 /sbin/mingetty tty4
root      3130  0.0  0.0   1624   436 tty5     Ss+  Feb05   0:00 /sbin/mingetty tty5
root      3134  0.0  0.0   1628   444 tty6     Ss+  Feb05   0:00 /sbin/mingetty tty6
root      3196  0.0  0.1   4616  1464 tty1     Ss+  Feb05   0:00 -bash
connect  29377  0.0  0.1   4488  1396 pts/0    Ss   14:43   0:00 -bash
root     29399  0.0  0.1   4792  1196 pts/0    S    14:43   0:00 su -
root     29400  0.0  0.1   4620  1476 pts/0    S    14:43   0:00 -bash
root     30104  0.0  0.0   4436  1008 pts/0    S    15:04   0:00 sh respaldarsri
root     30114  1.6  0.1   4496  1044 pts/0    R    15:04   0:00 tar -zcf /home/freired/bedoyal09
root     30115 49.5  0.0   1860   648 pts/0    R    15:04   0:13 gzip
root     30119  0.0  0.0   4216   944 pts/0    R+   15:05   0:00 ps au
[root@quitofr ~]#
```

- Comprobar que el proceso de compresión tar.gz finalizó correctamente

```
[root@quitofr ~]# ps au
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      3125  0.0  0.0   1628   440 tty2     Ss+  Feb05   0:00 /sbin/mingetty tty2
root      3126  0.0  0.0   1628   464 tty3     Ss+  Feb05   0:00 /sbin/mingetty tty3
root      3127  0.0  0.0   1628   444 tty4     Ss+  Feb05   0:00 /sbin/mingetty tty4
root      3130  0.0  0.0   1624   436 tty5     Ss+  Feb05   0:00 /sbin/mingetty tty5
root      3134  0.0  0.0   1628   444 tty6     Ss+  Feb05   0:00 /sbin/mingetty tty6
root      3196  0.0  0.1   4616  1464 tty1     Ss+  Feb05   0:00 -bash
connect  29377  0.0  0.1   4488  1396 pts/0    Ss   14:43   0:00 -bash
root     29399  0.0  0.1   4792  1196 pts/0    S    14:43   0:00 su -
root     29400  0.0  0.1   4620  1476 pts/0    S    14:43   0:00 -bash
root     30401  0.0  0.0   4216   948 pts/0    R+   15:16   0:00 ps au
[1]+  Done                    sh respaldarsri
[root@quitofr ~]#
```

4.8.6.2 Script para respaldo de información del sistema contable.

- El script consistirá en conectarse a una máquina Windows2003 Server de IP 192.168.1.15 para respaldar la información de la carpeta DECWIN, donde se encuentra la información contable. Para esto se enviá como parámetros generales del archivo la IP de la máquina, el nombre de usuario, la contraseña, el punto de montaje, y la tarea a realizar.

- Crear un punto de montaje de nombre RESDECWIN en el directorio /mnt/

```
[root@quitofr ~]# mkdir /mnt/RESDECWIN/
[root@quitofr ~]# vi respaldardecwin
x=`date +%d%b%Y`
mount -t cifs -o username=Administrador,password=Userver11 //192.168.1.15/DECWIN /mnt/RESDECWIN
tar -zcf /home/freired/decwin$x.tar.gz /mnt/RESDECWIN
umount /mnt/RESDECWIN
```

- Crear un archivo de nombre respaldardecwin.

4.8.6.3 Script para respaldos de información de usuarios.

- El script consistirá en conectarse a cada máquina de la red 192.168.1 para respaldar la información de cada usuario. Para esto se enviá como parámetros generales del archivo la IP de la máquina, el nombre de usuario, la contraseña de usuario de Windows XP, el punto de montaje, y la tarea a realizar.

- Crear un archivo de nombre respaldarnuevo.

```
[root@quitofr ~]# vi respaldarnuevo


x=`date +%d%b%Y`

mount -t cifs -o username=malenag,password=Finan91,workgroup=EGAROFC //192.168.1.12/malenag /mnt/
respaldar/
tar -zcf /home/malenag/malenag$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar/

mount -t cifs -o username=bahamondet,workgroup=EGAROFC,password=Vent005 //192.168.1.6/bahamondet
/mnt/respaldar/
tar -zcf /home/bahamondet/bahamondet$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar/

mount -t cifs -o username=zambranol,workgroup=EGAROFC,password=Credito83 //192.168.1.17/zambranol
 /mnt/respaldar/
tar -zcf /home/zambranol/zambranol$x.zip /mnt/respaldar/
umount /mnt/respaldar

mount -t cifs -o username=cardenasc,workgroup=EGAROFC,password=Costos17 //192.168.1.19/cardenasc
/mnt/respaldar/
tar -zcf /home/cardenasc/cardenasc$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar/

mount -t cifs -o username=garridom,workgroup=EGAROFC,password=Asistg64 //192.168.1.7/garridom /mn
t/respaldar/
tar -zcf /home/garridom/garridom$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar/
```

```
mount -t cifs -o username=andradee,workgroup=EGAROFC,password=Ventas2 //192.168.1.14/Andradee /mn
t/respaldar/
tar -zcf /home/andradee/andradee$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar

mount -t cifs -o username=ashquim,workgroup=EGAROFC,password=sISTEMAS11 //192.168.1.21/ashquim /m
nt/respaldar/
tar -zcf /home/ashquim/ashquim$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar

mount -t cifs -o username=credito,workgroup=EGAROFC,password=Credi0809 //192.168.1.39/Credito /mn
t/respaldar
tar -zcf /home/acostaa/acostaa$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar

mount -t cifs -o username=puentej,workgroup=EGAROFC,password=Ventas006 //192.168.1.3/puentej /mnt
/respaldar
tar -zcf /home/puentej/puentej$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar

 mount -t cifs -o username=acuriov,password=Ventas004,workgroup=EGAROFC //192.168.1.37/acuriov /m
nt/respaldar/
tar -zcf /home/acuriov/acuriov$x.tar.gz /mnt/respaldar/
umount /mnt/respaldar
```

4.8.7 PROGRAMACIÓN PARA EJECUCIÓN AUTOMÁTICA DE RESPALDOS

4.8.7.1 Instalación del paquete Crontabs.

- Mediante los CD's de Instalación de Centos 5.0
  - Insertar el CD #1 de Centos y Montar la Unidad de CDROM en el directorio /media/

```
[root@quitofr ~]# mount /dev/hda /media.
```

  - Ir al directorio CentOs que se encuentra dentro de la unidad montada /media/

```
[root@quitofr ~]# cd /media/CentOs
```

  - Instalar los paquetes crontabs-1.10-8.noarch.rpm.

```
[root@quitofr CentOs]# rpm - ivh crontabs-1.10-8.noarch.rpm
```

  - Revisión que se encuentre instalado correctamente el paquete crontabs.

```
[root@quitofr ~]# rpm -qa |grep cron
vixie-cron-4.1-72.el5
crontabs-1.10-8
anacron-2.3-45.el5.centos
[root@quitofr ~]#
```

- La herramienta crontab viene instalada por defecto en cualquier versión de Centos.

4.8.7.2 Programación de Tareas Automáticas.

- Una vez que se crearon y probaron cada uno de los scripts de respaldos de información, se procederá a automatizar estos respaldos. La automatización consiste en que estos scripts se ejecuten de manera automática y en fechas preestablecidas.
  Para esto se utilizará laherramineta CRONTAB.

- Editar el archivo principal de configuración de Crontab.

```
[root@quitofr ~]# crontab -e

#EJECUCIÓN AUTOMÁTICA CADA 15 DIAS DE LAS DECLARACIONES AL SRI MAQUINA DE CONTABILIDAD
30 11  * * 4  sh /root/respaldarsri% > /dev/null
#EJECUCIÓN AUTOMÁTICA DE RESPALDOS DE INFORMACIÓN GENERAL DE LOS USUARIOS
1 10 */15 * * sh /root/respaldarnuevo% > /dev/null
#EJECUCIÓN AUTOMÁTICA DEL RESPALDO DEL SISTEMA CONTABLE
30 23 16 * * sh /root/respaldardecwin% > /dev/null
```

- El formato del archivo Crontab consta de 6 partes las cuales son :

1 Columna: Corresponde al tiempo en minutos (0 a 60 minutos)

2. Columna: Corresponde a la hora. (0 a 24 h)

3.- Columna: Corresponde al día del mes (1 a 31 dias)

4.- Columna: Corresponde al me del año (1 a 12 meses)

5. Columna: Corresponde a los días de la semana (1 a 7 dias)

Los días de la semana se asocian de la siguiente forma:

1- Lunes
2- Martes
3- Miércoles
4- Jueves
5- Viernes
6- Sábado
7- Domingo.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Uno de los peligros más latentes en Internet que amenaza la productividad de las empresas es la problemática de virus y correos no deseados que llegan de manera constante a los sistemas de mensajería, por lo que existe la necesidad de implementar medidas de seguridad como son un software Antivirus y Antispam.

  La instalación de software Antivirus y Antispam ha permitido mejorar notablemente la productividad de la empresa debido a la reducción de entrada del correo no deseado y virus llevandolo a niveles de tolerancia entre tres a cuatro mensajes diarios.

- El verdadero costo de un computador no está en los programas adquiridos sino en el trabajo original e irrepetible que se pueda generar, ante esto existe la necesidad de implementar un sistema automático para extraer periódicamente respaldos de información que permita al usuario trabajar de manera despreocupada y a la vez protegida.

- Proxy una administración adecuada de la navegación de los usuarios. Se deben establecer políticas de salida a internet por parte de los usuarios internos para impedir la mala utilización de este recurso.

- La implementación del presente proyecto ha permitido estar actualizado en temas de suma importancia que se dan en el campo de las redes de información y que es requerido en las empresas.

- El buen funcionamiento del correo electrónico depende en gran medida de una correcta configuración de los DNS. Se puede decir que la correcta

implementación de un DNS es la clave para el buen funcionamiento del Internet. De igual manera para el redireccionamiento del correo electrónico es necesario que esté bien configurado el DNS.

- Linux es una excelente alternativa para la implementación se servicios de red, debido a su gran estabilidad, su bajo costo y el soporte que se obtiene por la comunidad de usuarios de Linux en Internet.

5.2 RECOMENDACIONES

- Debido a que cada red de Pifo y Quito cuenta con la debida infrestructura de acceso a internet, se recomienda la implementación de una VPN entre estas dos redes para obtener una mayor protección en la transferencia de los datos y control de los mismos. De la misma manera apoyará a la creación de nuevos proyectos de integridad de datos entre estas dos redes.

- Se recomienda la implementación de una DMZ para de esta forma aislar a cada servidor de su respectiva red local. De esta manera si el servidor es vulnerado la red local no se encontraría comprometida ante un posible ataque.

- Se recomienda utilizar al servidor de Pifo como mail exchanger alternativo en lugar del mail exchanger ubicado en los EE.UU. De esta manera se logrará una disminución de los costos por mantenimiento del servidor en EE.UU. así como independencia y se garantizará de mejor manera la confidencialidad de los datos.

- Se recomienda al Administrador del servidor generar respaldos cada vez que se realice alguna modificación a los archivos de configuración de cada servicio. Para en caso de cualquier fallo del sistema poder restaurar la última configuración del equipo.

- Se recomienda al Administrador de cada servidor realizar periódicamente un monitoreo de los servicios activos en el sistema, asi como de los puertos abiertos por cada uno de estos. De esta manera estar alerta para detener cualquier servicio innecesario y que puede ser aprovechado por un atacante.

- Se recomienda mantener en permanente capacitación al personal responsable del desempeño de cada servidor. Esto debido a la constante actualización de las versiones del software así como para estar prevenidos de nuevas formas de intrusión.

5.3 BIBLIOGRAFÍA

- Tesis de grado (P. López y F. Narváez)
- Implementación de servidores Linux de Joel Barrios Dueñas

INTERNET

TEMA: INTRODUCCIÓN A REDES

http://www.monografias.com/trabajos/introredes/introredes.shtml

http://www.monografias.com/trabajos13/modosi/modosi.shtml

http://www.monografias.com/trabajos13/modosi/modosi.html

http://elsitiodetelecomunicaciones.iespana.es/protocolo_tcp_ip.htm

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

http://es.wikipedia.org/wiki/Computer_software
http://www.masadelante.com/faq-sistema-operativo.htm
http://www.masadelante.com/faq-sistema-operativo.htm
http://www.linux-es.org/sobre_linux
http://es.wikipedia.org/wiki/GNU
http://es.wikipedia.org/wiki/C%C3%B3digo_libre#Tipos_de_Licencias

TEMA: GNU LINUX Y CORREO ELECTRÓNICO

http://es.wikipedia.org/w/index.php?title=Lineox&action=edit&redlink=1
http://es.wikipedia.org/wiki/Postfix
http://es.wikipedia.org/wiki/Qmail
http://es.wikipedia.org/wiki/Spam
http://www.mailscanner.org
http: http://interno.ehas.org/intranet/organizacion/administracion-de-sistemas/AMaViS
http:www.clamav.net
http:www.spamassassin.apache.org

TEMA: PROXY

http:www.squirrelmail.org
http://sindominio.net/~apm/articulos/proxy/
http://www.desarrolloweb.com/faq/que-es-proxy.html
http://www.ccm.itesm.mx/dinf/redes/indexproxy.html
http://www.ccm.itesm.mx/dinf/redes/indexproxy.html
http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

TEMA: SAMBA

http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-samba
http://www.osmosislatina.com/linux/win_samba.jsp
http://fferrer.dsic.upv.es/cursos/Integracion/html/ch04s02.html
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-samba-daemons.html
http://fferrer.dsic.upv.es/cursos/Integracion/html/ch04s02.html

http://www.elrincondelprogramador.com/default.asp?pag=trucos/truco.asp&truco=58

TEMA: ACCESO A INTERNET

http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet
http://www.fcc.gov/cgb/broadband_spanish.html#Wireless

TEMA: ANALISIS DE REQUERIMIENTOS

http://www.dovecot.org
http://www.uco.es/ccc/sistemas/doc_ccc/dovecot_JJTTRediris_2006.pdf
http://web.uservers.net/soporte/docview.php?articulo=34,
http://es.wikipedia.org/wiki/Post_Office_Protocol
http://es.wikipedia.org/wiki/BIND
http://es.wikipedia.org/wiki/Sendmail
www.itq.edu.mx/vidatec/espacio/aisc/windowsnt/Servidordecorreo.htm - 19k
http://www.clamav.net
http://wiki.apache.org/spamassassin/SpamAssassin
http://www.mailscanner.info/.
http://es.wikipedia.org/wiki/Webmail - 19k
http://es.wikipedia.org/wiki/Samba_(programa)
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-samba.html

TEMA: INSTALACIÓN DEL SISTEMA OPERATIVO CENTOS 5.0

http://joel-barrios.blogspot.com/2007/02/mi-libro-en-formato-pdf.html

GLOSARIO

Antivirus.- Brinda protección contra los archivos que entran a la red a través del correo electrónico, descargas de Internet, discos extraíbles, etc.

DHCP.- Dynamic Host Configuration Protocol, es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

DNS.- Domain Name System o Sistema de Nombres de Dominio, es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

Firewall.- También llamado cortafuegos, es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que se hayan definido en la red.

FTP.- File Transfer Protocol, es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle sus propios archivos independientemente del sistema operativo utilizado en cada equipo. El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.

HTTP.- El protocolo de transferencia de hipertexto es usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página y la respuesta con el contenido.

HTTPS.- Es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. El puerto estándar para este protocolo es el 443.

IP.- Internet Protocol o Protocolo Internet, es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Malware.- es software que tiene como objetivo infiltrarse en o dañar un computador sin el consentimiento informado de su dueño. Existen muchísimos tipos de malware, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso los bots.

MTU.- La unidad máxima de transferencia (Maximum Transfer Unit) es un término de redes de computadoras que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones. Los datagramas pueden pasar por varios tipos de redes con diferentes protocolos antes de llegar a su destino. Por tanto, para que un datagrama llegue sin fragmentación al destino, ha de ser menor o igual que el mínimo MTU de las redes por las que pase. Ejemplos de MTU: Ethernet: 1500 bytes. ATM (AAL5): 8190 bytes. FDDI: 4470 bytes. PPP: 576 bytes.

Phishing: El phishing consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada.

Spam: Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.

Spyware.- Son aquellos programas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Dichos datos son transmitidos a los propios fabricantes o a terceros, cabiendo la posibilidad de que sean almacenados de alguna manera para ser posteriormente recuperados.

TCP.- Transmission Control Protocol o Protocolo de Control de Transmisión, este protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión.

Telnet.- Sirve para acceder mediante una red a otra máquina, para manejarla como si se estuviera dentro de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

TTL.- Tiempo de Vida o Time To Live, es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen. El TTL como tal es un campo en la estructura del paquete del protocolo IP. Sin este campo, paquetes enviados a través rutas no existentes, o a direcciones erróneas, estarían vagando por la red de manera infinita, utilizando ancho de banda sin una razón positiva.

UDP.- User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama

incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

Virus.- es un programa que permanece oculto, reproduciéndose hasta que se activa y causa daño.

ANEXO A:

COSTOS DE IMPLEMENTACIÓN

COSTO DE INFRAESTRUCTURA ANTES DE IMPLEMENTACIÓN

EQUIPOS	CARACTERÍSTICAS	COSTO ANUAL	COSTO TOTAL
Conexión a Internet en Quito y Pifo.	Banda Ancha de 128 Kbps de bajada y subida.	1200	1200

TABLA A.1: COSTO INFRAESTRUCTURA ANTES DE IMPLEMENTACIÓN

COSTOS DE HARDWARE ANTES DE IMPLEMENTACIÓN

HARDWARE	LICENCIAS DE FUNCIONAMIENTO	CUENTAS DE CORREO	COSTO ANUAL	COSTO TOTAL
Linux Servidor en EEUU	0	Ilimitado	600	600

TABLA A.2: COSTO HARDWARE ANTES DE IMPLEMENTACIÓN

COSTOS DEL RECURSO HUMANO

RECURSO HUMANO	COSTO APROXIMADO ANUAL	COSTO TOTAL
Soporte Técnico del Proveedor de Correo Electrónico.	1500	1500

TABLA A.3: COSTOS DE RECURSO HUMANO

COSTO TOTAL REQUERIDO ANTES DE IMPLEMENTACIÓN

DESCRIPCIÓN	CANTIDAD
Costo Infraestructura	1200
Costo Hardware	600
Costo Recurso Humano	1500
COSTO TOTAL	**3300**

TABLA A.4: COSTO TOTAL ANTES DE IMPLEMENTACIÓN

COSTO INFRAESTRUCTURA POSTERIOR A IMPLEMENTACIÓN

EQUIPOS	CARACTERÍSTICAS	COSTO ANUAL	COSTO TOTAL
Conexión a Internet en Quito y Pifo.	Banda Ancha de 128 Kbps de bajada y subida.	1200	1200

TABLA A.5: COSTO INFRAESTRUCTURA POSTERIOR A IMPLEMENTACIÓN

COSTOS DE HARDWARE POSTERIOR A IMPLEMENTACIÓN

SISTEMA OPERATIVO	LICENCIAS DE FUNCIONAMIENTO	CANTIDAD DE MÁQUINAS	COSTO UNITARIO	COSTO TOTAL
Máquina Linux Centos 5.0 Para Implementación de Correo Electrónico, Proxy y Samba para redes de Pifo y Quito	0	2	800	1600
Linux Servidor de Correo Alternativo en EEUU	0	1	300	300

TABLA A. 6: COSTOS DE HARDWARE POSTERIOR A IMPLEMENTACIÓN

COSTOS DEL RECURSO HUMANO Y CAPACITACIÓN

RECURSO HUMANO	COSTO MENSUAL	TIEMPO (MESES)	COSTO TOTAL
Implementación	800	2	1600
Capacitación			1500

TABLA A.7: COSTOS DE RECURSO HUMANO Y CAPACITACIÓN

COSTO TOTAL ADICIONAL REQUERIDO POSTERIOR A IMPLEMENTACIÓN

DESCRIPCIÓN	CANTIDAD
Costo Infraestructura	1200
Costo Hardware	1900
Costo Recurso Humano	3100
COSTO TOTAL	**6200**

TABLA A.8: COSTO TOTAL DE IMPLEMENTACIÓN

ANEXO B:

INSTALACIÓN DEL SISTEMA OPERATIVO CENTOS

INSTALACIÓN DEL SISTEMA OPERATIVO CENTOS 5.0

INSTALACIÓN DE CENTOS 5.0

1.- Inserte el dvd1 de instalación de Centos 5, y cuando aparezca el diálogo de inicio (boot) pulsar la tecla enter.

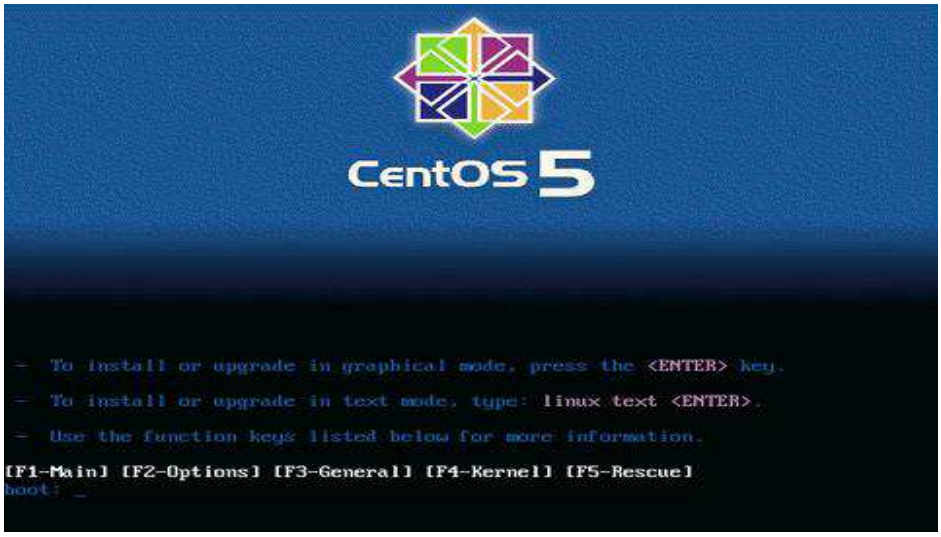

FIGURA B.1: PANTALLA INICIAL DE INSTALACIÓN DE CENTOS 5.0

- Si se desea instalar en modo texto en el diálogo de inicio (boot) escribir la palabra linux text seguido de la tecla enter.
- Si se tiene instalado un sistema de versión anterior y se desea actualizar en el cuadro de diálogo de (boot) digitar la tecla enter.

2.- Si se desea verificar la integridad del disco a partir del cual se realizará la instalación seleccione OK. Y pulse la tecla enter. Si se está seguro que el disco se encuentra en buen estado seleccione Skip y digite la tecla enter.

FIGURA B.2: CHEQUEO INTEGRIDAD DE LOS DISCOS DE INSTALACIÓN

3.- En la pantalla de bienvenida hacer clic sobre el icono Next

FIGURA B.3: PANTALLA DE BIENVENIDA DE LA INSTALACIÓN

4.- Seleccione el idioma que se usará durante la instalación

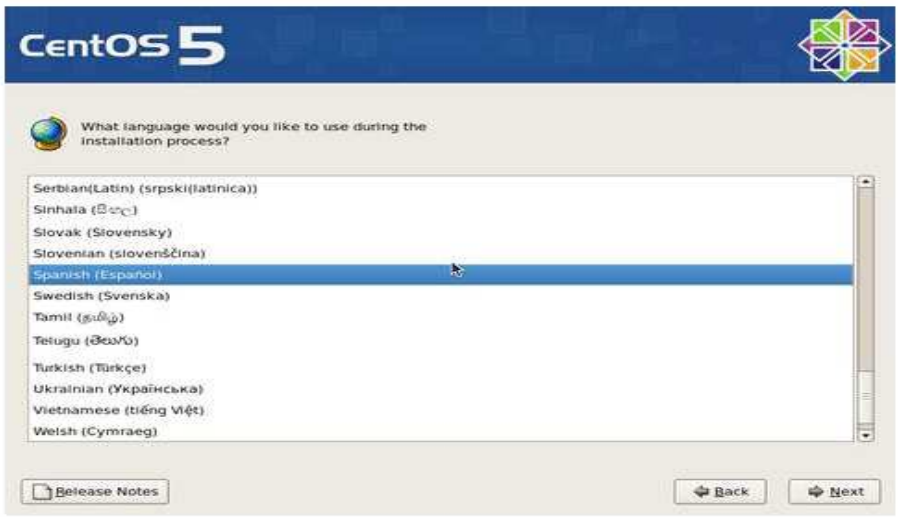

FIGURA B.4 : SELECCIÓN DEL IDIOMA DE INSTALACIÓN

5.- Seleccione el idioma del teclado. Puede escogerse español o latinoamericano según corresponda.

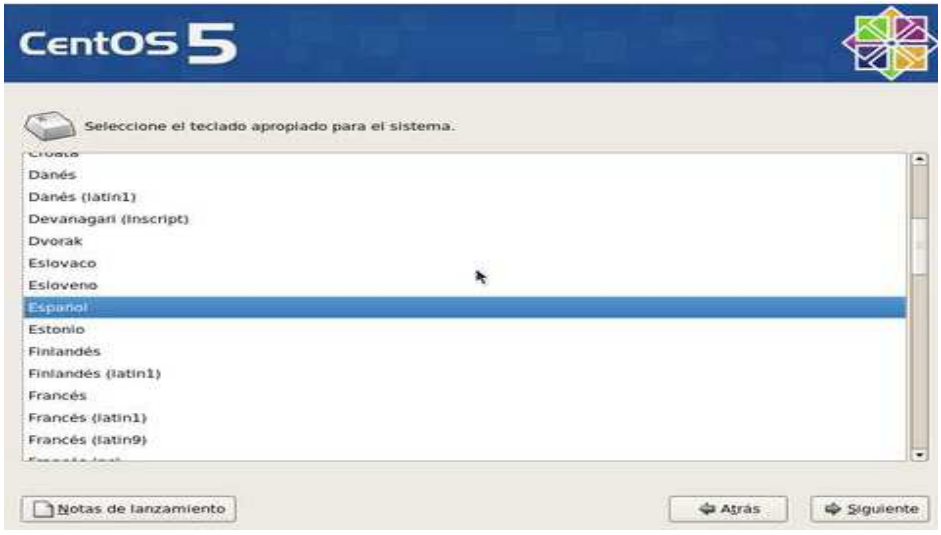

FIGURA B. 5: SELECCIÓN DE TECLADO DEL SISTEMA

6.- Seleccione la opción instalar Centos.

FIGURA B.6: SELECCIÓN DE TIPO DE INSTALACIÓN

7.- Escoger la opción crear particiones personalizadas, ideal para usuarios avanzados. A continuación damos clic en siguiente

FIGURA B.7: SELECCIÓN DEL TIPO DE PARTICIONAMIENTO

8.- Se mostrará el espacio disponible. Haga clic en el boton Nuevo

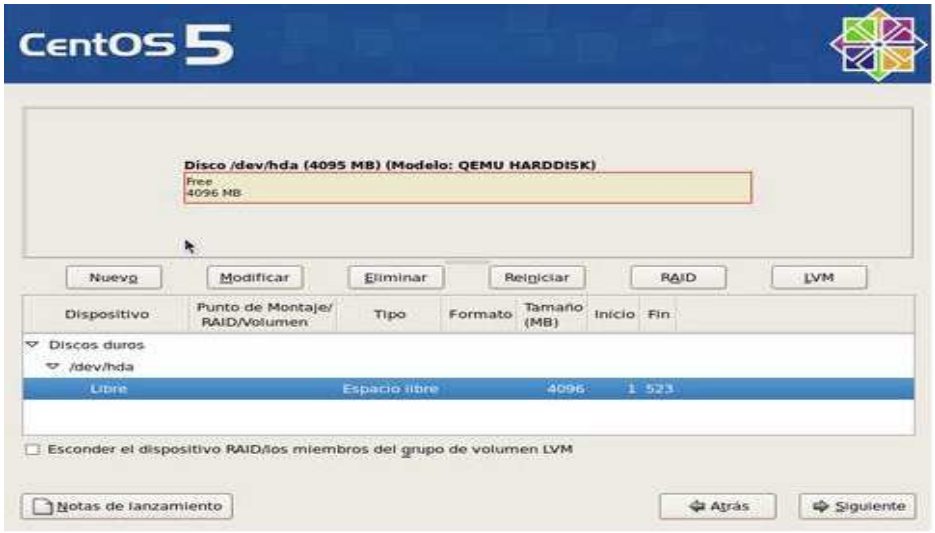

FIGURA B.8: ESTADO DE DISCOS DEL SISTEMA

9.- Cree la partición boot de 100 MB y definir como partición primaria.

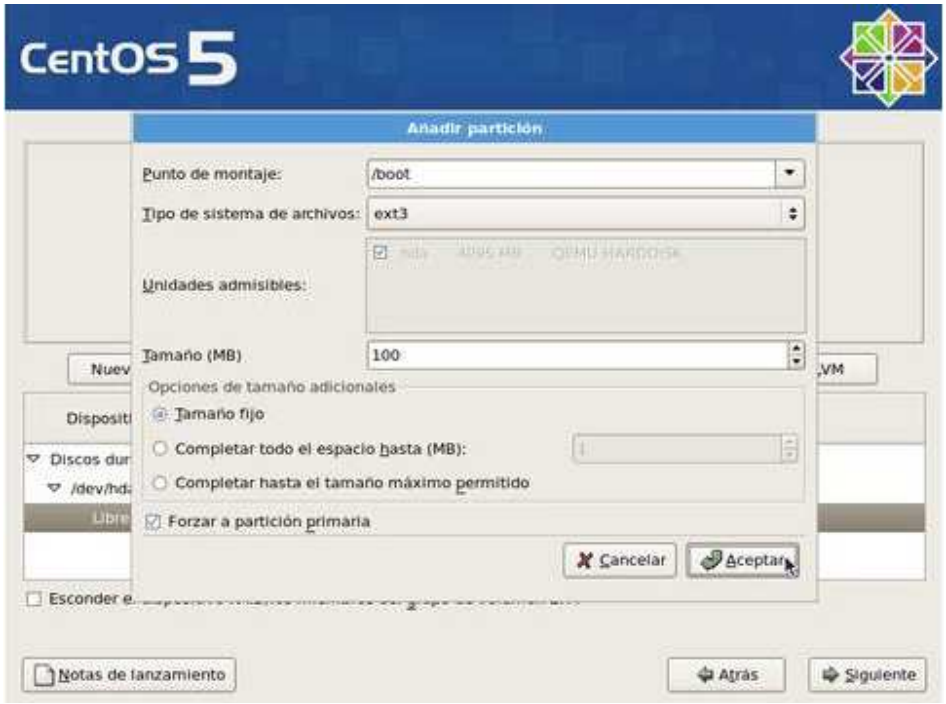

FIGURA B.9: ASIGNACIÓN DE PARTICIÓN BOOT

10.- Si se está conforme hacer clic en el botón nuevo para crear la siguiente partición.

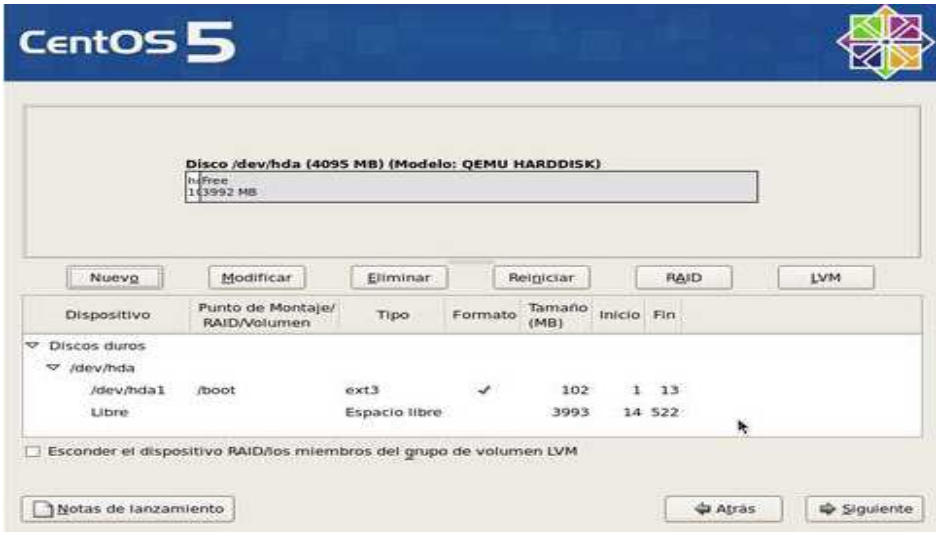

FIGURA B.10: TABLA DE PARTICIONES DEL SISTEMA

11.- Crear la partición Swap. Asignar el doble del tamano de la memoria RAM. Si la memoria es de1 GB la partición Swap sería de 2 GB.

FIGURA B.11: ASIGNACIÓN DE PARTICIÓN SWAP

12.- Asignar el resto de espacio disponible para crear la partición /

FIGURA B.12: ASIGNACIÓN DE PARTICIÓN /

Sugerencias para un correcto particionamiento.

El particionamiento es un tema esencial a la hora de instalar , se indicará algunos factores a tomar en cuenta a la hora de particionar. Sin embargo siempre debe tenerse en cuenta las características propias de la instalación que se está haciendo y lo que requerirá la empresa o lugar donde se esté instalando.

El particionamiento es útil por diversas razones como por ejemplo:

- Permite controlar que un disco no se llene completo, si por casualidad un proceso comienza a escribir descontroladamente a disco, solamente podrá llenar la partición hacia donde escribe, mas no podrá llenar el disco completo.
- La partición / requiere siempre de tener espacio disponible, si no se realiza una partición correcta s podría llenar / y por lo tanto dejar el sistema sin funcionar.

- Si un pedazo del disco se dañara, muy posiblemente el resto podrá ser todavía utilizado y recuperado. Por supuesto un disco dañado requiere de una migración inmediata hacia otro disco. Pero no es lo mismo perder la única partición que se tiene a perder sólo una de las varias.

Si se dispone de espacio en disco se recomienda crear las siguientes particiones de manera adicional a las anteriormente creadas.

/home/ : Lugar donde se crean las carpetas de los usuarios, al crear un usuario, el sistema Linux le asigna un directorio raíz o base para este usuario, donde podrá escribir y guardar su información.

/var/: Almacena datos variables. Estos son datos que eventualmente ingresarán al sistema pero pueden ser eliminados por la aplicación que los usa. Por ejemplo, var sirve para:

- almacenar los logs del sistema (/var/log)
- almacenar la caché del proxy del sistema (/var/cache/squid)
- almacenar los mensajes entrantes a los usuarios (/var/spool/mail)
- almacenar los mensajes salientes (/var/spool/mqueue)

13.- Se ingresará a la configuración del Sector de Arranque. Si se desea se puede introducir una contraseña para el Gestor de Arranque si no es así digitar Siguiente.

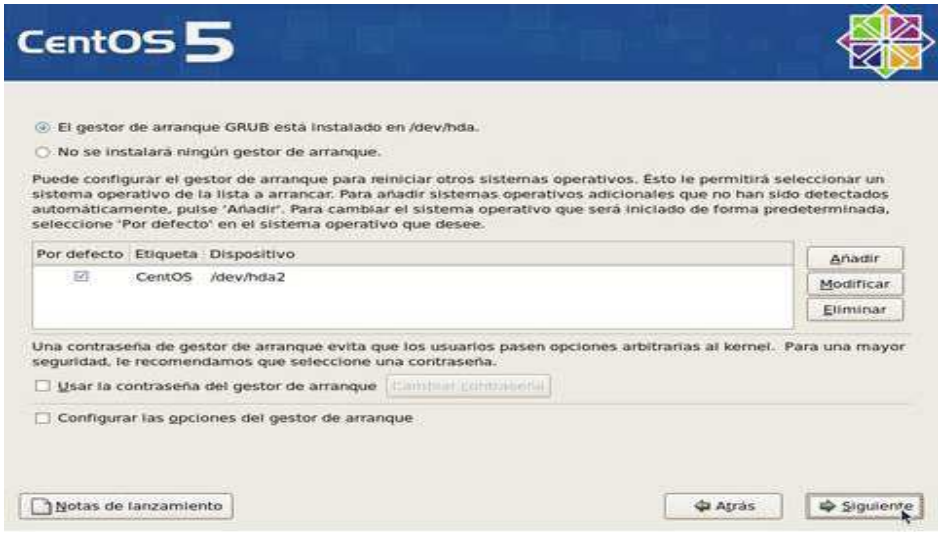

FIGURA B.13: CONFIGURACIÓN DEL SECTOR DE ARRANQUE

14.- Para modificar los parámetros de red del sistema, hacer clic sobre el botón EDIT para las interfaces de red. El sistema reconocerá las tarjetas de red instaladas.

- En la interfaz eth0 estará configurada la IPpública 157.100.98.18, para el servidor en Quito será 157.100.98.22
- En la interfaz eth1 estará configurada la IP Interna 192.168.2.1 para el servidor en Quito la IP interna será 192.168.1.1
- El hostname del servidor de Pifo es linuxpifo2.ab-products.com.ec, para el servidor en Quito será quitofr.egar.com.ec
- El Gateway del servidor de Pifo será la IP 157.100.98.17 asignado por el ISP. Para el servidor en Quito será 157.100.98.21
- Las direcciones DNS serán proporcionados por el ISP

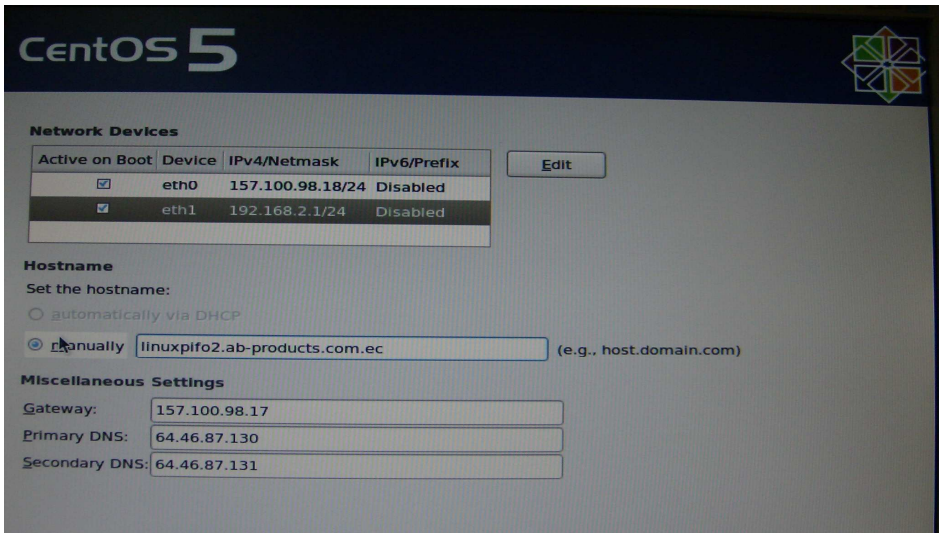

FIGURA B. 14: CONFIGURACIÓN DE RED

15.- Seleccionar la zona horaria dependiendo de la ubicación.

FIGURA B.15: SELECCIÓN DE LA ZONA HORARIA

16.- Asignar clave de root. La clave debe ser introducida dos veces para confirmar que es la que realmente se espera.

FIGURA B.16: CONFIGURACIÓN DE CONTRASEÑA DE ROOT

17.- Al finalizar hacer clic en Siguiente y esperar a que el sistema haga la lectura de información de los grupos de paquetes

18.- Aparecerá la pantalla de selección de paquetes que se desea instalar en el sistema. Añadir paquetes de acuerdo a las necesidades.

FIGURA B.17: SELECCIÓN DE MODO DE INSTALACIÓN

Para el caso de un servidor lo ideal es instalar en modo Server y solo el sistema base mínimo sin ambiente gráfico.

Los servicios a escoger son:

- DNS Name Server
- Mail Server

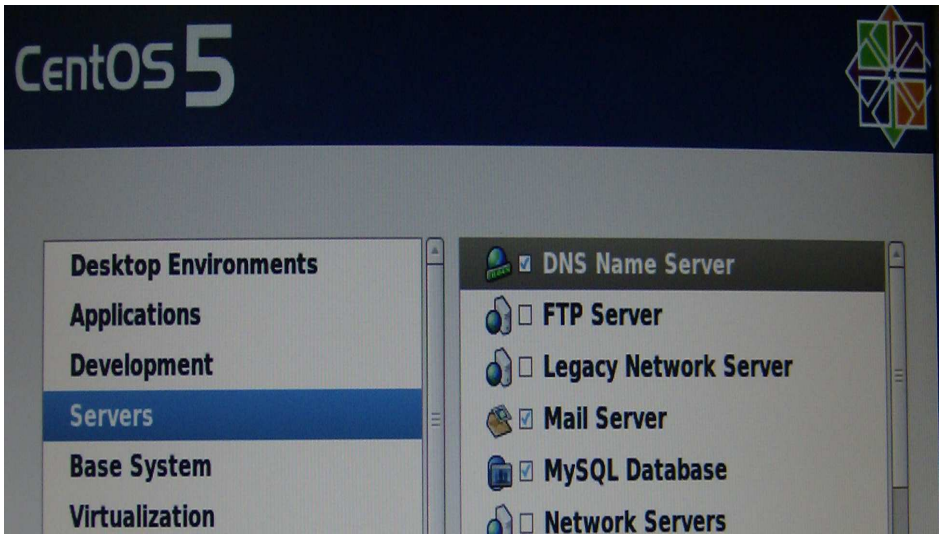

FIGURA B.18: SELECCIÓN DE PAQUETES PARA INSTALACIÓN EN MODO SERVIDOR SERVIDOR

- Web Server (Apache y Proxy).
- Windows File Server (Samba).

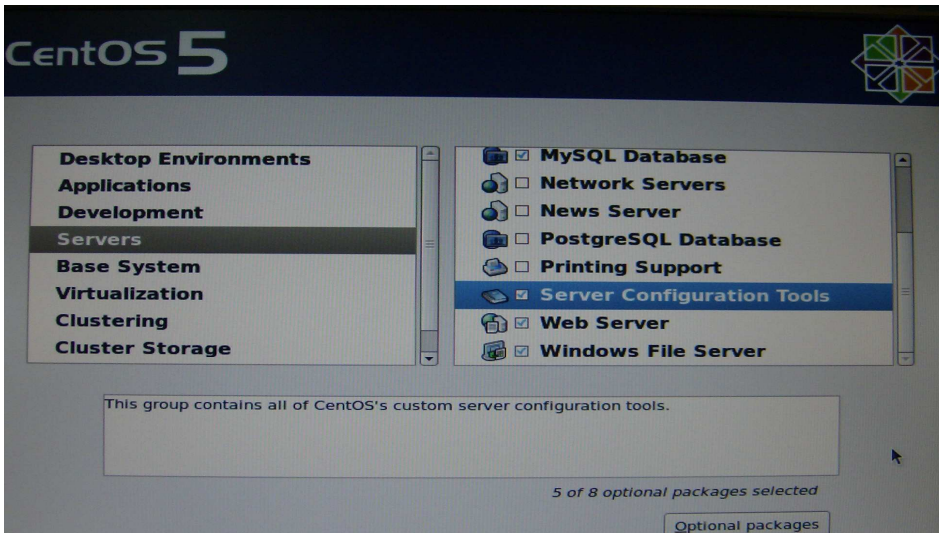

FIGURA B.19: SELECCIÓN DE PAQUETES PARA INSTALACIÓN EN MODO SERVIDOR

19.- Antes de iniciar la instalación, el sistema informará respecto a que se guardará un registro del proceso de instalación en el fichero /root/install.log. Para continuar hacer clic en siguiente.

20.- Se iniciará de manera automática el proceso de formato de las particiones que se hayan creado para instalar el Sistema Operativo.

21.- Se realizarán preparativos para la instalación de paquetes necesarios para el funcionamiento del Sistema Operativo.

FIGURA B. 20: PANTALLA DE INICIO DE LA INSTALACIÓN

22.- Una vez finalizado el proceso de los paquetes hacer clic en el botón de reiniciar.

FIGURA B. 21: PANTALLA DE FINALIZACIÓN DE LA INSTALACIÓN