INSTITUTO TECNOLÓGICO SUPERIOR CORDILLERA

ESCUELA DE SISTEMAS

Proyecto de grado, Previa a la obtención del título de:
Tecnólogo Analista de Sistemas

Tema de Proyecto de Grado

TEMA:

IMPLEMENTACIÓN DE GESTIÓN DE SEGURIDAD DE FRONTERA PARA UN SERVIDOR LINUX DE LA EMPRESA COONECTA.

AUTOR:

Jhon Molina

TUTOR

Ing. Jaime Padilla

2011

QUITO – ECUADOR

Instituto Tecnológico Superior Cordillera

DECLARACIÓN DE AUTENTICIDAD

El abajo firmante, declara que los contenidos y los resultados obtenidos en el presente proyecto, como requerimiento previo para la obtención del Título de Tecnólogo Analista de Sistemas, son absolutamente originales, auténticos y personales y de exclusiva responsabilidad legal y académica del autor

Jhon Edison Molina Moreno

171384812-3

AGRADECIMIENTO

Mi agradecimiento especial va dirigido a:

A Dios, por darme la vida y la salud para poder seguir adelante con mis metas.

A mis padres y hermanos por darme el ejemplo de lucha y constancia para salir adelante.

A mi esposa e hija por darme el amor y apoyo en los momentos difíciles de mi vida.

A mis compañeros y profesores por sus enseñanzas día a día para construir días mejores.

Gracias

DEDICATORIA

En cada una de las letras de este proyecto va expresado mi sacrificio.

A mi esposa, hija y padres, que con su amor me guiaron desde el inicio de mis estudios incondicionalmente y siempre contando con su total apoyo.

Por último quiero dedicar esta tesis a todas aquellas personas de una u otra manera compartimos conocimientos a lo largo de mis estudios.

El autor

Resumen Ejecutivo

El presente proyecto trata sobre la implementación de un servidor para optimizar y administrar el uso del Internet en COONECTA utilizando herramientas bajo Linux. El proyecto inicia con el reconocimiento de COONECTA, de la importancia que tiene el Internet y el impacto que este desarrolla si es mal utilizado. Después de tener una visión de lo que se desea hacer se procede a investigar las herramientas necesarias, que se aplicarán en el desarrollo del proyecto. Un servidor de seguridad puede disminuir el riesgo y proteger la integridad de la información en la institución. En busca de este fin es importante realizar un estudio de la situación en la que se encuentra en este momento COONECTA en lo que a seguridades se refiere, esto incluye un análisis de todas las funcionalidades de Internet que utilizan (navegación por las páginas web, publicación de weblogs y webs, mensajería instantánea, foros, chats, gestiones y comercio electrónico, entornos para el ocio) que pueden significar algún riesgo.

En el capítulo I, se plantean los objetivos generales y específicos que se debe cumplir para la correcta ejecución del proyecto.

El capítulo II, describe las características de la institución auspiciante como está constituida, ubicación, cumplimiento el ámbito legal, entre otros.

El capítulo III, describe las principales metodologías de investigación, y las técnicas de recolección de información.

El capítulo IV, enfoca todo el proceso de desarrollo del proyecto: metodología a utilizar, hardware, software. Se detalla la forma y lógica del proyecto, planteando alternativas que sean de beneficio para la institución.

El capítulo V, analiza e indica los principales impactos que ha tenido el desarrollo de proyecto, las conclusiones y recomendaciones para una utilidad óptima del proyecto.

ÍNDICE DE CONTENIDOS

Pág.

ÍNDICE TABLAS

pág.

ÍNDICE DE FIGURAS

pág.

ÍNDICE DE ANEXOS

pág.

CAPÍTULO I

1. El Problema

1.1 Planteamiento del Problema

Al realizar las diferentes investigaciones en la empresa a quien va dirigido este trabajo, nos dimos cuenta que una de las dificultades de la empresa Coonecta es dar protección, control y priorización de la información de la web a diferentes usuarios, ya que se maneja información confidencial de la empresa y de todos sus clientes, permitiendo controlar la calidad del servicio prestado en forma inmediata y personalizada.

Actualmente, las empresas dedicadas a prestar servicios informáticos se han visto obligadas a suspender temporalmente sus operaciones debido a incidentes ocurridos en los servidores de servicios tales como proxy, correo electrónico, ftp, web, etc., dando origen a brindar servicios de baja calidad a sus clientes, poniendo así en riesgo la continuidad del negocio, lo que ocasiona pérdidas económicas. Actualmente, en el país existen pocas empresas que han optado por instalar código abierto en sus servidores debido al poco personal técnico capacitado, pese a que el gobierno nacional promueve el uso de código abierto en las entidades públicas.

Este trabajo se enfoca en el uso de software libre (Linux) para encontrar soluciones al problema aquí planteado. Existen equipos que permiten el control de seguridades y alta

disponibilidad mediante hardware, pero la adquisición de estos equipos significa una inversión para las empresas tanto en hardware como en software, al contrario, las soluciones de software código abierto no necesitan pagar ningún valor de licenciamiento, ahorrando costos importantes en software.

De no contar con una solución al problema de alta disponibilidad y balanceo, descarga y seguridad por software, se perderá la opción de contribuir a una investigación e implementación de este tipo.

Mediante la implementación de un servidor de frontera, la empresa asegura el normal desenvolvimiento de sus operaciones, minimizando sustancialmente el riesgo tecnológico, dando continuidad al servicio y, por consiguiente, sus operaciones, se centrarán en la técnica de obtener una alta disponibilidad de seguridad, de acuerdo a las necesidades de cada usuario.

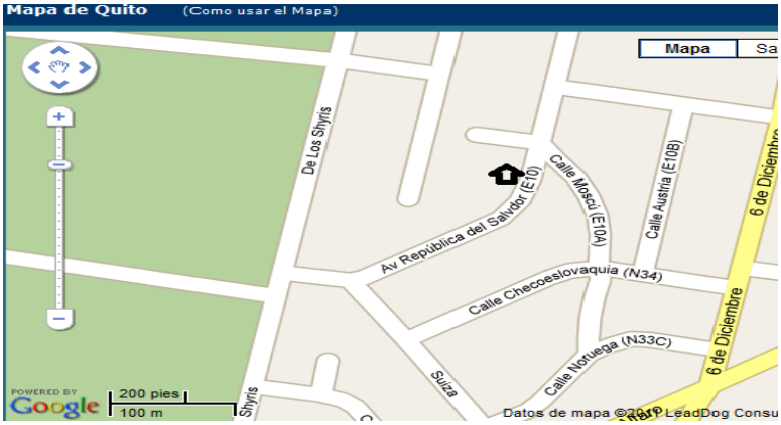
1.2 Formulación del Problema

¿Se encontrará la solución que permita mantener un alto nivel de seguridad y balanceo de carga, con herramientas código abierto, dando continuidad a los servicios de los usuarios de Coonecta?

1.3 Delimitación de la Investigación

El presente proyecto se realizará en la ciudad de Quito, capital de la República de Ecuador y también de la provincia de Pichincha; además, se la conoce como el Distrito Metropolitano de Quito. Su población sobrepasa hoy los 2’500.000 repartidos en el área rural y en la urbana, según los datos del Censo de Población del año 2010. La ciudad está dividida en 32 parroquias urbanas y 33 rurales, las que, a su vez, se dividen en diferentes barrios.

El proyecto objeto de este trabajo se realizará específicamente en la empresa COONECTA, ubicada en la ciudadela Benalcázar, al norte de la cuidad de Quito, en la Av. República de El Salvador N34-211 y Moscú, edificio Aseguradora del Sur, Piso 1. Oficina 1A.



Nombre: Ubicación COONECTA

Fuente: Google maps

Elaborado: JHON MOLINA

Figura: 1 Ubicación COONECTA

1.4 Objetivo

1.4.1 Objetivo General

Implementar una solución de alta seguridad informática de frontera, optimizar y administrar el uso del Internet en la red de Coonecta todo esto se va a realizar a través de software libre.

1.4.2 Objetivos Específicos

- Controlar el buen uso del Internet y brindar una herramienta de administración amigable al centro de cómputo de Coonecta.
- Investigar diferentes herramientas de software libre para desarrollar el objetivo general.
- En base a los estudios previos de seguridad implementar un Servidor Linux con herramientas de optimización y administración del Internet.
- Generar documentación pertinente sobre la implementación que aquí se propone como solución al problema.

1.5 Justificación e Importancia

La principal ventaja de esta solución radica en el hecho de poder atender al cliente cuando lo necesite, sin afectar la hora o el día, ya que la información de los servicios prestados estará levantada en el servidor.

Esta implementación tendrá su gestión en el área de seguridad informática, donde se creará este servidor con un alto nivel de seguridad, contando así con una herramienta potente para filtrar o detener posibles amenazas contra los usuarios de Coonecta. Así obtendremos un mejor rendimiento en las tareas diarias que desempeña cada usuario y optimizando el tiempo útil para la empresa.

Es cada día más importante que los servicios puedan funcionar con un alto nivel de SLA (calidad de servicio), ya sea para dar soporte interno, o para ofrecer servicios a través de Internet (https, ssh, ftp, etc.).

Se utiliza código abierto porque es software libre, es decir, la empresa no incurre en gastos de licencia para su uso, otra ventaja radica en el hecho de que personal especializado puede revisar el código de programación para desarrollarlo de acuerdo a las necesidades de la empresa, igualmente al estar este código abierto a la vista de programadores a nivel mundial las soluciones y actualizaciones de seguridad son implementadas con rapidez.

Desde el punto de vista metodológico, esta investigación generará conocimiento válido y confiable dentro del área de las Tecnologías de la Información y la Comunicación (TICS) para futuras implementaciones. Ésta investigación abrirá nuevos caminos en empresas que presenten situaciones similares, convirtiéndose en un buen marco referencial.

1.6 Alcance

El proyecto tiene como finalidad optimizar y administrar el uso del Internet en Coonecta, brindando diferentes soluciones como: Filtro de Contenidos, Proxy, Firewall.

La implementación del servidor constará de las siguientes tareas:

1. Instalación y configuración de Linux CentOS destinado a levantar los servicios de frontera de seguridad para la empresa COONECTA.

2. Monitoreo de navegación: Esta tarea crea reportes y estadísticas que permitirán generar informes sobre el acceso a páginas web. Para esto utilizaremos el programa SARG (Squid Analysi Report Generator), el cual entregará la siguiente información:

    - Top Ten de sitios más visitados
    - Reportes diarios, semanales y mensuales
    - Reportes por usuarios
    - Reportes por tiempo de navegación
    - Reportes de descargas

3. Control de contenido: Esta tarea permitirá bloquear el acceso a determinadas páginas WEB cuyo contenido sea calificado como inseguro. Se controlará el acceso a contenidos indeseables utilizando diferentes categorías:

    - Chats
    - Descargas directas: rapidshare
    - Apuestas
    - Trabajos

- Música
- Videos
- Noticias
- Pornografía
- Warez y Spyware
- Radio y TV Web.

Para todas estas tareas se necesita la completa colaboración del departamento de Sistemas ya que son los que manejan el área de telecomunicaciones dentro de Coonecta.

CAPÍTULO II

2. Marco Teórico

2.1 Antecedentes

A pesar de los actuales avances tecnológicos en computación, la empresa COONECTA aún no cuenta con un sistema de frontera que ayude a que su imagen corporativa crezca.

Otro aspecto de importancia radica en poder brindar seguridad y rapidez. Tenemos la certeza de que con la implementación de un servidor código abierto Linux de frontera, los usuarios podrán acceder al internet con más seguridad y control.

2.2 Reseña Histórica

La RED TRANSACCIONAL COOPERATIVA S.A., RTC, es una Institución de servicios auxiliares del Sistema Financiero. Esta red ha sido calificada por la Superintendencia de Bancos y Seguros mediante Resolución No. SBS-2007-172 de 28 de febrero de 2007.

La constitución de la empresa fue aprobada por la Superintendencia de Compañías con Resolución No. 06.Q.IJ.004284 de 06 de noviembre de 2006.

La empresa se forma por la decisión de las Cooperativas del Ecuador para integrarse mediante servicios transaccionales. Las Cooperativas de la Red están interconectadas en forma permanente.

El objetivo de la empresa es actuar como facilitadora de las transacciones entre Cooperativas de Ahorro y Crédito.

Participantes

34 Cooperativas de Ahorro y Crédito del Ecuador (70% de AT de Cooperativas reguladas).

Empresa del Sistema Cooperativo.

2.2.1 Misión

Contribuir a la integración operativa y el crecimiento del sistema cooperativo de ahorro y crédito mediante la prestación de servicios transaccionales y la ejecución de procesos de consultoría bajo una estrategia de innovación, calidad, competitividad y sostenibilidad de los servicios.

2.2.2 Visión

"Ser la red de negocios transaccionales del sector cooperativo y de microfinanzas con una cobertura al 100% de cantones del Ecuador, integrada internacionalmente y referente de éxito en las redes a nivel mundial."[1]

2.2.3 Valores Corporativos.

[1] http://www.coonecta.com.ec/coonecta/index.php?system=14&sessid=

"Cooperación / Integración: Manteniendo una actitud de cooperación con las otras personas que integran el equipo de trabajo, compartiendo responsabilidades.

A nivel de las cooperativas, disponiendo de apertura a generar alianzas que permitan implementar procesos que impliquen economías de escala entre los integrantes de la RTC.

Innovación: Ser pioneros y ejercer un liderazgo a través de ideas novedosas y creativas, con el fin de producir cambios en la institución, las cooperativas integradas a la Red y los sistemas sociales.

Compromiso: Estar orgulloso de pertenecer y trabajar como parte integrante de la institución.

Competitividad: tener un permanente afán de superarse y de dar lo mejor de uno mismo en las responsabilidades asignadas. A nivel institucional mantener una actitud constante de mejoramiento y de brindar los mejores servicios a las cooperativas."[2]

2.3 Marco Referencial

Para todas estas tareas se dispondrá de aplicaciones tales como:

1.- Microsoft Project 2007

Microsoft Project (o MSP) es un software de administración de proyectos diseñado, desarrollado y comercializado por Microsoft para asistir a administradores de proyectos en el desarrollo de planes, asignación de recursos a tareas, seguimiento al progreso, administrar presupuesto y analizar cargas de trabajo.

[2]. http://www.coonecta.com.ec/coonecta/index.php?system=14&sessid=

Nos ayudará a desarrollar nuestro proyecto verificando los tiempos propuestos para la investigación.

2.- QoS

QoS (Quality of Service *o* Calidad de Servicio*)* es un conjunto de protocolos y tecnologías que garantizan la entrega de datos a través de la red en un momento dado. De este modo, nos aseguramos de que las aplicaciones que requieran un tiempo de latencia bajo o un mayor consumo de ancho de banda, dispongan real y óptimamente de los recursos suficientes cuando los necesiten.

Por esta razón, uno de las principales metas de QoS es la priorización, es decir, el poder dar más relevancia a unas conexiones frente a otras.

3.- Código abierto

"Código abierto" es el término con el que se conoce al software distribuido y desarrollado libremente. El "Código abierto" tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones morales y/o filosóficas las cuales se destaca en el llamado "software libre"[3].

4.- Software libre

"El Software libre" suele estar disponible gratuitamente, o al precio de costo de la distribución a través de otros medios; sin embargo, no es obligatorio que sea así, por

[3] http://es.wikipedia.org/wiki/Software_libre

lo tanto no hay que asociar software libre a "software gratuito" (denominado usualmente freeware), ya que, conservando su carácter de libre, puede ser distribuido comercialmente ("software comercial").

Análogamente, el "software gratis" o "gratuito" incluye en ocasiones el código fuente; no obstante, este tipo de software libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.

5.- Firewall

Un Firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un Firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y, en función de lo que sean, permite o deniega su paso. Para permitir o denegar una comunicación, el Firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio, el firewall decide si lo permite o no. Además, el Firewall examina si la comunicación es entrante o saliente y, dependiendo de su dirección, puede permitirla o no.

6.- Squid

Squid, es un programa que sirve de Proxy-Cache de Internet, lo que significa que si accedes más de una vez a una página, esta página se almacena en el disco duro, y si no lo encuentra, lo buscara en Internet.

Esta operación acelera la navegación en internet y normalmente se usa en servidores que se conectan a Internet para que naveguen unos cuantos ordenadores a través de una conexión.

7.- Microsoft Word 2007

Microsoft Word 2007 es una herramienta muy importante para la digitación de texto; esta herramienta es utilizada para generar toda la documentación que tiene que ver con el desarrollo de sistemas. Además es muy fácil de usar, pues el entorno que presenta no es muy complejo. Adicionalmente, Microsoft Word 2007 cuenta con asistente y ayudas. Como se puede ver en el grafico los botones y accesos rápidos y son fáciles de usar.

Microsoft Office Word 2007 ayuda a elaborar documentos de aspecto profesional proporcionando un completo conjunto de herramientas para crear documentos y aplicarles formato a través de una nueva interfaz de usuario. Sus funciones ampliadas de revisión, comentarios y comparación ayudan a recopilar y administrar rápidamente los comentarios y opiniones de sus compañeros. La integración avanzada de datos garantiza que los documentos permanecen en conexión con fuentes importantes de información empresarial.

8.- Linux

GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre, similar a Unix, denominado Linux, que es usado con herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes

de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera, bajo los términos de la GPL (Licencia Pública General de GNU, *en inglés:* General Public License) y otra serie de licencias libres.

9.- Kernel

En informática, un núcleo o kernel (de la raíz germánica *Kern*) es un software que constituye la parte más importante del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

Como hay muchos programas y el acceso al hardware es limitado, también se encarga de decidir qué programa podrá hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado. Acceder al hardware directamente puede ser realmente complejo, por lo que los núcleos suelen implementar una serie de abstracciones del hardware. Esto permite esconder la complejidad, y proporciona una interfaz limpia y uniforme al hardware subyacente, lo que facilita su uso al programador.

10.- Red Hat

Red Hat es la compañía responsable de la creación y mantenimiento de una distribución del sistema operativo GNU/Linux que lleva el mismo nombre: Red Hat Enterprise Linux, y de otra más, Fedora. Así mismo, en el mundo del middleware patrocina JBoss.org, y distribuye la versión profesional bajo la marca JBoss Enterprise.

Red Hat es famoso en todo el mundo por los diferentes esfuerzos orientados a apoyar el movimiento del software libre. No sólo trabajan en el desarrollo de una de las distribuciones más populares de Linux, sino también en la comercialización de diferentes productos y servicios basados en software de código abierto. Así mismo, poseen una amplia infraestructura en la que se cuentan más de 2.000 empleados en 28 lugares del mundo.

Programadores empleados de Red Hat han desarrollado múltiples paquetes de software libre, los cuales han beneficiado a toda la comunidad. Algunas de las contribuciones más notables han sido la creación de un sistema de empaquetación de software (RPM), y varias utilidades para la administración y configuración de equipos, como sndconfig o mouseconfig.

Algunas de las distribuciones basadas en Red Hat Linux más importantes son:

- Mandriva Linux
- Yellow Dog Linux (sólo para PowerPC)
- CentOS (compilada a partir de las fuentes de Red Hat, mantenida por los laboratorios de física CERN y Fermilab y usada en los ordenadores que controlan el LHC).

11.- CentOS

CentOS (Community ENTerprise Operating System) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat. Los desarrolladores de CentOS usan este código fuente para crear un producto final que es muy similar al Red Hat Enterprise

Linux y está disponible libremente para ser bajado y utilizado por el público, pero no es mantenido ni asistido por Red Hat. También existen otras distribuciones derivadas de las fuentes de Red Hat.

Licencia Pública General de GNU

La Licencia Pública General de GNU o más conocida por su nombre en inglés GNU (General Public License) o simplemente mediante sus siglas del inglés GNU GPL, es una licencia creada por la Free Software Foundation en 1989 (la primera versión), y está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y así protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios a nivel mundial.

12.- Mac

En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (3 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el organizationally unique identifier. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. Debido a esto, las direcciones MAC son a veces llamadas burned-in addresses, en inglés.

Si nos fijamos en la definición como cada bloque hexadecimal son 8 dígitos binarios (bits), tendríamos:

6 * 8 = 48 bits únicos

En la mayoría de los casos no es necesario conocer la dirección MAC, ni para montar una red doméstica, ni para configurar la conexión a internet, usándose esta sólo a niveles internos de la red. Sin embargo, es posible añadir un control de hardware en un conmutador o un punto de acceso inalámbrico, para permitir sólo a unas MAC concretas el acceso a la red. En este caso, deberá saberse la MAC de los dispositivos para añadirlos a la lista. Dicho medio de seguridad se puede considerar un refuerzo de otros sistemas de seguridad, ya que teóricamente se trata de una dirección única y permanente, aunque en todos los sistemas operativos hay métodos que permiten a las tarjetas de red identificarse con direcciones MAC distintas de la real.

La dirección MAC es utilizada en varias tecnologías entre las que se incluyen:

- Ethernet
- 802.3 CSMA/CD
- 802.5 o redes en anillo a 4 Mbps o 16 Mbps
- 802.11 redes inalámbricas (Wi-Fi).
- Asynchronous Transfer Mode

2.4 Marco Legal

Se considera el marco legal a todo aquello que se refiere normativas y leyes por las que tiene que regirse nuestro proyecto; este marco legal se circunscribe a estas leyes:

- **La Ley de Educación Superior.**

  CAPITULO I DE LA NATURALEZA, FINES Y ÁMBITO DEL REGLAMENTO

  Art. 1.- Como determina la Constitución, la educación es derecho irrenunciable de las personas y deber inexcusable del Estado. La educación superior se imparte a través de instituciones integradas en su sistema nacional y se rigen por la Ley de Educación Superior. Las instituciones de este sistema, son públicas; particulares cofinanciadas por el presupuesto del Estado; y, particulares autofinanciadas que coadyuvan en la atención de este deber estatal. Las universidades y escuelas politécnicas serán entidades sin fines de lucro.

  Art. 2.- El presente reglamento establece los procedimientos para la aplicación de la Ley de Educación Superior y sus prescripciones son de cumplimiento obligatorio para las instituciones que integran el Sistema Nacional de Educación Superior".[4]

- [5]La Ley de Derecho de Autor:

  "Art.1**.** El Estado reconoce, regula y garantiza la propiedad intelectual adquirida de conformidad con la ley, las Decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador."[6]

[4] http://190.15.138.2/titulo1.php

[5] www.wikipedia.org

- La Ley del Uso de Software Libre

  Decreto 1014., Art. 1: **"**Establecer como política pública para las entidades de la Administración Pública Central la utilización del software libre en sus sistemas y equipamientos informáticos".

  - Utilización de programas con cualquier propósito de uso común.
  - Distribución de copias sin restricción alguna
  - Estudio y modificación de programas (Requisito: código fuente disponible).
  - Publicación del programa mejorado (Requisito: código fuente disponible)".

  "Art. 3: Las entidades de la Administración Pública Central, previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para este tipo de software".

  "Art. 4: Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo de seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

- Las leyes internas de COONECTA.

  Estos reglamentos se encuentran en trámite de aprobación del directorio.

[6] www.wikipedia.org

Capítulo III

3. Investigación Científica

3.1 Tipos de Investigación

- Investigación Cuantitativa

  Este tipo de investigación científica es muy aplicable al proyecto que aquí presentamos, ya que este tipo de investigación permite un análisis y una síntesis de la información que podemos obtener a través de libros, escritos, documentos, manuales técnicos e, inclusive, en el Internet. Este proceso analítico- sintético que realizamos a la información nos permitirá poner en práctica los conceptos doctrinarios adquiridos durante nuestra etapa de estudio.

  Todo este ejercicio investigativo tiene como fin primordial obtener de una manera práctica, conclusiones y recomendaciones que identifiquen en la formulación de hipótesis sobre hechos reales obtenidos a través de la implementación de un servidor de frontera.

- Investigación descriptiva

Este tipo de investigación es plenamente aplicable a nuestro proyecto, debido a que una vez determinado, analizado, interpretado y estudiado todos los factores, causas, fenómenos y efectos que producen el objeto de la investigación que se ha determinado para dicha problemática, y haciendo uso de las herramientas que se tiene a disposición para llevar a cabo la culminación exitosa del proyecto.

La investigación descriptiva consiste en categorizar exhaustivamente todas las características de un hecho o fenómeno. Esta investigación pretende delinear, dibujar de tal manera lo que se investiga para representarlo de manera cabal y ser comprendido perfectamente en todos sus matices.

- Investigación explicativa

Este tipo de la investigación científica se aplica desde el punto de vista de análisis de la problemática que se desarrolla con aristas predominantes en interrogantes que tenemos que resolver, previo al desglose analítico y sintético del mismo. Emplea la destreza de relacionar mediante preguntas por qué ocurrió un hecho y en qué condiciones se encuentra el mismo.

Surgen así las respuestas para lo cual siempre será necesario verificar la causa que la produjo, las circunstancias, el entorno con el que se lo relacionó y los efectos, Así podremos entender cómo o qué puede causar impactos hacia la población que va a utilizar o va a dirigir el servidor en mención.

- Investigación Bibliográfica-Documental

Este tipo de investigación se aplica al proyecto, ya que mediante el mismo nos permite realizar un tipo de investigación analítica y sintética de fuentes de información contenidas en libros, manuales técnicos y otros tipos de documentación escrita.

Esta información nos permite conocer, interpretar, comparar y compartir criterios, opiniones en el manejo e implementación en la seguridad.

Este tipo de investigación también nos ayuda a materializar los conceptos obtenidos en las fuentes y los documentos anteriormente mencionados y esquematizarlos en un levantamiento de un servidor de frontera para la estructuración del modelo de negocios que tenga que construirse para posteriormente implementarlo y obtener un servidor de frontera libre de amenazas en la información que se obtenga a través del Internet, pudiendo así concentrar todo el énfasis en las conceptualizaciones que nos permitirán construir conclusiones y recomendaciones.

Cabe recalcar que todo este proceso investigativo tiene como finalidad orientar e integrar de la mejor manera el proceso de la teoría con la práctica a través de la implementación del servidor.

3.2 Métodos de Investigación

- Método Inductivo

Este tipo de método me ayuda en el desarrollo del plan de proyecto inicialmente en poder disminuir los registros de amenazas mediante la utilización de herramientas propias de la investigación científica como la observación, determinación, análisis y aplicación pudiendo llegar a identificar claramente las reglas del negocio con procesos que quiera llegar a materializar el esquema en una estructura lógica y funcional que nos permita darnos cuenta cual es la necesidad real de COONECTA; posteriormente me ayudará en el desarrollo mismo utilizando la informática para obtener un servidor capaz de poder soportar todo tipo de exigencia y necesidad de la empresa que hasta el momento no ha habido una solución permanente y automatizada.

- Método Deductivo

Este tipo de método se enfoca en el desarrollo de mi proyecto a la inducción de hechos singulares o particulares para llegar a lo universal o general a la formulación de la ley o principio.

La deducción es el proceso inverso, va de los principios o leyes generales hacia lo particular o singular, de verdades generales ya establecidas a otras particulares,

sin llegar a la contradicción, estos métodos deben ser considerados en su interacción dialéctica en el tránsito de lo empírico a lo teórico y viceversa.

Basándose en la información recolectada y brindada por las Autoridades de la misma, con lo cual se cuenta para realizar un previo análisis el mismo que nos servirá como guía para el diseño, desarrollo, implementación y ejecución del proyecto.

- Método Hipotético-Deductivo

Este método es de mucha aplicación en el ambiente de networking para el surgimiento de apuntes a equipos por parte de virus y personal mal intencionado los mismo que me permita ejecutar tácticas y estrategias que de protección y seguridad.

- Histórico lógico

Este método histórico lógico se enfoca al proyecto permitido validar todos los procesos y procedimientos que se encuentran materializados en un plan y que me ayuda a reproducir cronológicamente toda la sucesión de tareas que se tiene que ejecutar en un macro proceso al mismo tiempo me ayuada a definir claramente el comportamiento de cada uno de los procesos, es decir verificando el alcance que tiene cada uno de ellos en la realización de determinada tarea en un tiempo de ejecución.

Por consiguiente este método me ayuda a delimitar las aéreas automatizables y al mismo tiempo las actividades que tiene que cumplir cada uno de los actores involucrados.

- Método analítico sintético

Esta metodología me ayuda a realizar un análisis a profundidad de cada uno de los elementos que intervienen en el desarrollo de una metodología, permitiendo la sistematización en la organización; por otro lado al realizar una síntesis de la información teórica y conceptual nos ayuda a reunir todos los argumentos validos a fin de poder estructurar toda la lógica didáctica y conceptual de todo elemento que interviene en la implementación , pudiendo concentrar el mayor esfuerzo en la búsqueda de información y análisis de la misma pero únicamente con la salvedad de que sea aplicable estrictamente al tema en ejecución. Por consiguiente el método analítico y sintético tiene su fundamentación de aplicación en cómo vamos a tratar la información teórica necesaria para la estructuración del capítulo segundo de este tema de proyecto.

3.3 Técnicas de Recolección de la información

Después de haber realizado la investigación de campo del lugar objeto de estudio (Diálogos con las autoridades de la Empresa, convenios, investigación, etc.), se procedió a realizar:

- **Observación**

Esta técnica de recolección de información se aplica al proyecto con la finalidad de obtener datos primarios de acercamiento a la empresa a quien va dirigido el proyecto, los mismos que nos permitirán realizar una observación de su infraestructura, su capacidad física, el ambiente de trabajo, la camaradería, en fin, una serie de datos importantes que determinan el tipo de organización y la tecnología en la que nos vamos a desenvolver.

También es necesario aclarar que con la información obtenida mediante esta técnica de recolección, es necesario estar presentes en el lugar donde se va a efectuar el levantamiento de la información; por consiguiente, se tendrá que hacer un análisis visual, tanto del área administrativa como del área técnica, con el fin de construir criterios de manejo de datos y relaciones que existan entre todas las dependencias. Un caso especial será la información del lugar en el que enfocaremos nuestra atención para efectuar todos los ambientes computacionales que posean las instalaciones de la empresa, es decir, los pisos, las paredes, la ventilación, la iluminación, las seguridades, etc. Este análisis visual en la empresa podrá corroborar las ideas iníciales de la concepción de una infraestructura tecnológica adecuada.

- **Entrevista**

Esta técnica de recolección de información consiste en que una persona (el entrevistador) solicita información a otra (entrevistado), para obtener datos sobre un problema determinado del departamento de sistemas.

Hemos aplicado la técnica de la entrevista para recolectar información en la empresa Coonecta objeto de este proyecto. A continuación presentamos sus resultados:

- **¿La institución cuenta con control de frontera en el área de seguridad?**

  Respuesta: Actualmente, la empresa no cuenta con un control de frontera, y por lo tanto puede ser fácilmente vulnerable; esta carencia puede reflejarse en posibles daños en los equipos de los usuarios.

  Con la implementación de un servidor de frontera se reforzaría la seguridad a los usuarios, evitando posibles intrusos.

- **¿Estaría interesada la empresa en implementar algún tipo de seguridad para los usuarios que navegan por internet?**

  R/: Sí, y para ello se está buscando un software o un hardware que refuerce la seguridad de la información que maneja la empresa.

  Con la implementación de un servidor de frontera con software libre potente como es Linux y con cero costos de licenciamiento se puede dar seguridad a nuestra información.

- **¿Le interesa dar restricciones a usuarios por niveles de aéreas?**

  R/: Sí, con el fin de poder dar estándares y jerarquizar a los usuarios por aéreas.

Tenemos información que Linux cuenta con poderosas herramientas código abierto para dar niveles a usuarios.

- **¿Al navegar por páginas frecuentemente visitadas, desearía que su ejecución sea más rápida?**

  R/ Si, para optimizar el tiempo y poder desplegar con mayor rapidez las páginas más utilizadas del día a día.

Utilizaremos Squid; es un programa que sirve de Proxy-Cache de Internet, lo que significa que si accedes más de una vez a una página, esta página se almacena en el disco duro, y si no la encuentra, la buscara en Internet. Esto acelera la navegación con internet y normalmente se usa en servidores que se conectan a Internet para que naveguen unos cuantos ordenadores a través de una conexión.

- **¿Le interesaría un reporte de las páginas más visitadas en el internet?**

  R/ Sí, para así saber qué información de la web les interesa a los usuarios y llevar un control de esta actividad.

De esta manera podremos obtener un reporte diario, semanal o mensual, como lo disponga el filtrado.

- **¿Habría intención en el área seguridad de la empresa adquirir un servidor con software libre?**

  R/ Por supuesto que sí, por sus potentes herramientas y por la relación costo-beneficio.

  Sabemos que Linux no requiere licenciamiento, evitando así a la empresa el tener que realizar un gasto muy elevado por la adquisición de un software con licencia.

- **¿Le interesaría saber cuál es el uso que sus usuarios dan al internet?**

  R/ Si, pues nos interesa saber qué tipo de información están buscando los usuarios.

  Con la implementación del servidor nos podemos dar cuenta del tipo de información que se está obteniendo por cada usuario y saber si utiliza Internet para fines personales o de la empresa.

- **¿Tiene políticas de QoS?**

  R/ No empleamos esa política y tenemos problemas cuando un usuario ingresa a páginas de alto tráfico, quitando recursos a procesos más importantes.

Configurando políticas de QoS, nos aseguramos que las aplicaciones que requieran un tiempo de latencia bajo o un mayor consumo de ancho de banda, realmente dispongan de los recursos suficientes cuando los soliciten.

- **¿Conoce sobre servidores Linux?**

R/ Sí, sabemos que es un software que no necesita licenciamiento. Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre.

Su desarrollo es uno de los ejemplos más prominentes de software libre. Creemos que la empresa no tendrá que preocuparse por pagar rubros por la implementación de este sistema ya que es libre.

Procedimientos

Esta entrevista ha sido elaborada con anticipación, revisada y aprobada por el Tutor, con un máximo de 10 preguntas para identificar los problemas y posibles soluciones al asunto planteado.

CAPÍTULO IV

4. Desarrollo de la Propuesta

4.1 Diagnóstico Situacional

La Institución cuenta con estaciones de trabajo, para un uso básico, en un 90% son HP, de arquitectura CISC, con Procesadores Intel / PV 4 Dual Core I3 y I5 de 32 Bits y 64 Bits.

Respecto a software se maneja paquetes de Office 2007, para el proceso diario de trabajo. Para navegar por la web se utiliza en un 80% Mozilla Firefox 3.6, el restante utiliza Internet Explorer.

Actualmente se cuenta con una red LAN, la topología es en forma de estrella. El servicio de Internet se lo comparte mediante configuraciones específicas de un router (en caminador), conectado hacia un switch (repartidor) y este distribuye a todas las estaciones de trabajo. El proveedor de servicios es Telconet.

No existen seguridades periféricas estrictas para la DMZ. El Firewall utilizado es el propio de Windows, Antivirus kaspersky, y el acceso a páginas web no existe control.

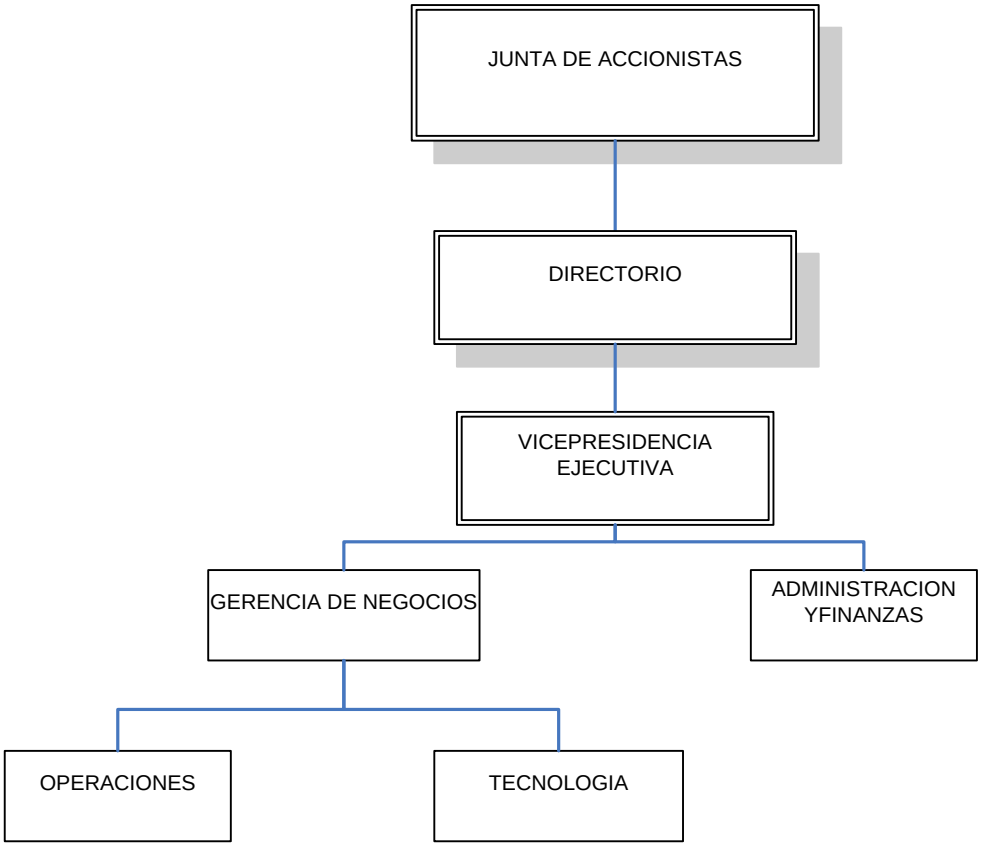
Se está elaborando un plan informático, que asegure o preserve la información generada, por lo diferentes procesos desarrollados.

4.2 Estructura Organizacional

Toda empresa cuenta con una representación gráfica con cierto juego de jerarquías y atribuciones asignadas a los miembros o componentes de la empresa. En consecuencia se puede establecer que la estructura organizativa de COONECTA es el esquema de jerarquización de la organización.

Se detalla la Organización Institucional

4.2.1 Estructura Orgánica



4.3 Infraestructura Informática

4.3.1 Hardware

Características	Ubicación	Arquitectura
Intel Quad Core	DT	CISC
Intel Dual Core	Secretaria	CISC
XEON QUAD CORE	Servidores	CISC
Intel Pentium IV	Monitoreo	CISC

FUENTE: Inventario de Hardware y Software

Tabla N° 1 Hardware existente

4.3.2 Software

Software	Ubicación
Office 2007	Estaciones de Trabajo, gerencia, sistemas y operaciones.
Windows 7	Estaciones de Trabajo, gerencia

Windows 7	Estaciones de Trabajo, sistemas
Windows server 2003	Monitoreo
Windows server 2008	Servidores
Windows server 2008	Estaciones de Trabajo, Contabilidad
Mozilla Firefox	Secretaria, Dirección

FUENTE: Inventario de Hardware y Software

Tabla N° 2 Software existente

4.3.3 Comunicaciones

Equipo	**Ubicación**
Router	Redes
Switch	Redes
Cable UTP Cat 5	Redes
Conectores RJ45	Redes
Tarjetas de Red	Redes

FUENTE: Inventario de Hardware y Software

Tabla N°3: Comunicaciones existentes.

4.3.4 Recurso Humano

Nombre	Descripción
Ing. Jaime Padilla	Tutor de Tesis
Jhon Molina	Autor de Tesis
Ing. Robert Enríquez	Director Escuela de Sistemas ITSCO
Ing. Jaime Basantes	Director de Proyectos de Grado del ITSCO
Ing. José Luis Rodríguez	Administrador de Proyecto Coonecta.
Eco. Hugo Reyes	Vicepresidente Coonecta.

Fuente: Propia

Tabla N°4: Recurso Humano

4.4 Descripción de las Alternativas de Solución

Se realiza la respectiva descripción de cada una de las alternativas propuestas para este proyecto.

4.4.1 Alternativa # 1

Enviada por la Empresa telconet.

El equipo sugerido para la seguridad gestionada en red es el FortiGate 80C , pertenece a la marca FORTINET, de la cual somos Partnet-Reseller. Este equipo va acorde la cantidad de usuarios mencionados (200) para el filtrado web y seria colocado en las instalaciones del cliente.

ITEM	CUMPLE	NO CUMPLE
Manual de Usuario		x
Políticas de seguridad	x	
Firewall	X	
Antivirus	X	
Antispam	X	
Antispyware	x	
Antimalware	X	
Prevención de intrusos	X	
Filtrado Web	X	
Control de Aplicaciones	x	

Políticas de seguridad	X	
Garantía Técnica	x	
Data Loss Preventions	x	
Manual Digital	x	
Soporte Técnico	x	

FUENTE: Proforma Empresa Punto Net.

Tabla N°5: Alternativa 1

Proforma:

- Costo: USD. $ 342.00 + IVA (mensuales).

Inversión

Producto/ Servicio	Descripción	Cant.	Precio Total
Seguridad Gestionada en red FortiGate 80C	Cobertura de servicio 8x5, incluye Fortiguard y Forticare hasta dos horas de soporte mensuales	1	**$342,00**
Seguridad Gestionada sobre correo electrónico: FortiMail	Cobertura de servicio 8x5, incluye Fortiguard y Forticare, hasta dos horas de soporte	1	
Configuración inicial e inducción	Cubriendo hasta 2 horas en cada servicio contratado para la configuración y una hora de inducción	-	-

Nota:
Precios no incluven IVA.

- Tiempo: 12 meses mínimo de servicio
- Entregables:

1. 1 Equipo FortiGate 60C ubicado en Quito
2. Configuración Inicial de IPS/IDS, Firewall, AntiX, cubierta hasta 2 horas
3. Usuario de Administración Limitada para tareas básicas y repetitivas y con capacidad para observar todo el trafico de red y de emitir reportes
4. Manuales Digitales

4.4.2 Alternativa # 2

Enviada por la Empresa Golden Sistemas.

Implementación de un servidor sistema Linux para brindar diferentes soluciones en el

uso del Internet

ITEM	CUMPLE	NO CUMPLE
Manual de Usuario		x
Políticas de seguridad	x	
Firewall	X	
Antivirus	X	
Proxy	X	
Antispyware	x	
IDS		x
Prevención de intrusos		X
Filtrado Web	X	
Control de Aplicaciones		x
Políticas de seguridad	X	
Garantía Técnica	x	
Data Loss Preventions		x
Manual Digital	x	
Soporte Técnico	x	

FUENTE: Proforma Empresa Golden Sistemas.

Tabla N°6: Alternativa 2

Proforma:

- **Costo:** USD. $ 500.00
- **Tiempo:** 2 semanas con Cobertura de servicio 8x5.
- **Garantía:** 1 año
- **Entregables:**

1. Manual de Usuario
2. Reportes
3. Configuración Inicial de IPS/IDS, Firewall, cubierta hasta 4 horas

4.4.3 Alternativa # 3

Enviada por el Ejecutor del Proyecto Jhon Molina

Implementación de un servidor de frontera con sistema Linux para brindar diferentes soluciones en el uso del Internet como Filtro de Contenidos, Proxy, Firewall, QoS (calidad del servicio).

ITEM	CUMPLE	NO CUMPLE
Manual de Usuario	x	

Políticas de seguridad	x	
Firewall	X	
Antivirus	X	
Antispam	X	
Antispyware	x	
QoS	X	
Filtro de Contenidos	X	
Filtrado Web	X	
Control de Aplicaciones	x	
Políticas de seguridad	X	
Garantía Técnica	x	
Data Loss Preventions		x
Manual Digital		x
Soporte Técnico	x	
Proxy	x	

FUENTE: Propia.

Tabla N°7: Alternativa 3

Proforma:

- Costo: USD. $ 0.00
- Tiempo: 2 semanas Configuración inicial, con Cobertura de servicio 8x5.
- Garantía: 6 meses.
- Entregables:

  1 Manual de Usuario

  2 Reportes

  3 Servidor Linux.

4.5 Evaluación de la Alternativa de Solución

Con la finalidad de poder determinar la alternativa que ofrece mayores beneficios para la Institución se ha definido un sistema de calificación con coeficientes matemáticos que están determinados de la siguiente manera:

Técnico 70%

Económico 20%

Soporte Técnico 5%

ITEM TÉCNICO	PESOS	EMPRESA 1	EMPRESA 2	EMPRESA 3

Seguridad	10	X	X	X
Interface				
Estándares	10	X	X	X
Diseño				
Programación				
Bases de datos				
Capacitación Técnica: Charlas	10	X		X
Capacitación Usuario: Charlas, Videos	8			X
Implantación	10	X	X	X
Manuales Técnicos	10	X	X	X
Documentación	2	X		X
Varios				
Soporte Técnico	10	X	X	X

FUENTE: Propia

Tabla N°8: Evaluación Técnico

Realizando la evaluación definitiva de las 3 propuestas presentadas se puede concluir claramente que:

La empresa telconet, alcanzó los siguientes resultados:

En la parte técnica sumo 70 puntos por lo que se le asigna un puntaje de 70%.

La empresa Golden Sistemas, alcanzó los siguientes resultados:

En la parte técnica sumo 60 puntos por lo que se le asigna un puntaje de 60%.

El Proyecto, alcanzó los siguientes resultados:

En la parte técnica sumo 70 puntos por lo que se le asigna un puntaje de 70%.

Costo Económico	**Costo**	**%**
Empresa 1	$ 342 (mensual)	10
Empresa 2	$ 500	15
Propuesta	$ 0.00	20

FUENTE: Propia.

Tabla N°9: Evaluación Económica

Realizando la evaluación definitiva de las 3 propuestas presentadas se puede concluir claramente que:

La empresa telconet, alcanzó los siguientes resultados:

En la parte económica sumo 10 puntos por lo que se le asigna un puntaje de 10%.

La empresa Golden Sistemas alcanzó los siguientes resultados:

En la parte económica sumo 15 puntos por lo que se le asigna un puntaje de 15%.

El Proyecto, alcanzó los siguientes resultados:

En la parte económica sumo 20 puntos por lo que se le asigna un puntaje de 20%.

Empresa	**Garantía/Tiempo**	**%**
Empresa1	6 meses	5
Empresa2	1 meses	3
Propuesta	6 meses	5

Empresa	**# Visitas**	**%**
Empresa1	6	5
Empresa2	2	3
Propuesta	6	5

Realizando la evaluación definitiva de las 3 propuestas presentadas se puede concluir claramente que:

La empresa telconet alcanzó los siguientes resultados:

En la parte de Soporte Técnico y Garantía sumo 10 puntos por lo que se le asigna un puntaje de 10%.

La empresa Golden Sistemas, alcanzó los siguientes resultados:

En la parte de Soporte Técnico y Garantía sumo 8 puntos por lo que se le asigna un puntaje de 4%.

El Proyecto, alcanzó los siguientes resultados:

En la parte de Soporte Técnico y Garantía sumo 10 puntos por lo que se le asigna un puntaje de 10%.

Técnico: Las especificaciones técnicas del software representan la parte más importante de todo el proceso de selección de la alternativa más idónea. Se ha diseñado una matriz que contiene pesos cuantitativos de acuerdo a la importancia de cada uno de los elementos que intervienen en la mencionada alternativa, estos pesos sumarán una totalidad de 70 puntos lo que corresponderá al 70% de la parte técnica.

Económico: Para determinar el puntaje respectivo que le corresponde a la parte económica se define de la siguiente manera: según los criterios analizados con sus respectivos pesos cuantitativos la oferta más económica obtendrá 20 puntos, que corresponde al 20% de la parte económica.

Soporte Técnico: Está determinado por la calidad de técnicos que posea la empresa y además por la lista de clientes que esta tengan, esto se lo realiza para saber el nivel de conocimiento de la empresa y su porcentaje de aceptación en el medio.

4.5.1 Software

Instituto Tecnológico Superior Cordillera

CRITERIO	PESO	ALTERNATIVA 1	ALTERNATIVA 2	ALTERNATIVA 3
Técnico				
- Estándares	10	10	10	10
-Diseño pagina web				
-Implementación	5	5	5	5
-Operatividad	30	30	25	30
Sistema Académico	20	20	15	20
-				
Manuales Técnicos	5	5	5	5
Sub total 1	**70**	**70**	**60**	**70**
Económico				
-Costo Correo	5	5	3	5
-Costo	5	5	7	5
Implementación	10	0	5	10
-Costo Servidor de frontera				
Sub total 2	**20**	**10**	**15**	**20**
Soporte Técnico				

-Periodo de Soporte -Calidad de Soporte - Periodo de Garantía Técnica	4 3 3	4 3 3	4 3 1	4 3 3
Sub total 3	**10**	**10**	**8**	**10**
Total	**100**	**90**	**83**	**100**

FUENTE: Proforma Empresas.

Tabla N°10: Pesos de Alternativas

4.6 Factibilidad Técnica

De lo expuesto anteriormente se desprende que la opción de implementación propuesta como proyecto de grado es la más conveniente en la parte técnica, económica, garantía y soporte técnico.

La misma establece que el aspecto técnico es la principal para poder realizar una calificación coherente y acertada, por otro lado el aspecto económico favorece la ejecución del proyecto, igual tratamiento nos indica lo referente al soporte técnico y garantía técnica.

Por consiguiente es factible la realización del proyecto con la alternativa de desarrollo propio, lo que implica que su soporte y ejecución será estrictamente con apoyo de la institución en todos los géneros que se pueda realizar (técnico, económico).

4.7 Alcance

4.7.1 Antecedentes

El proyecto tiene como propósito optimizar y administrar el uso del internet, brindando diferentes soluciones como: Filtro de Contenidos, Proxy, Firewall. Además de realizar la prueba correspondiente para su correcto funcionamiento.

Habitualmente dentro de la gran parte de empresas no existe una estructura organizativa adecuada, careciendo en muchos casos de la figura del responsable de seguridad, cuyo rol asume la misma persona responsable de Centro de Tecnología (sistemas y/o comunicaciones), lo que unido a la falta de responsabilidad explícita y a las importantes carencias formativas en el área de seguridad de la información, hace que las medidas de seguridad implantadas suelan ser muy básicas y respondan en casi todos los casos, a necesidades puntuales para solventar un problema existente, o a la implantación de una nueva funcionalidad o aplicación dentro de la organización.

La labor cotidiana no permite a sus responsables tomar una visión de conjunto o realizar una planificación y gestión adecuada de la seguridad, lo que a su vez se traduce en una falta de concienciación de la alta dirección en estos temas y por ende, en la atención de unos niveles de riesgo inaceptables para la organización que desafortunadamente, suelen materializarse en el momento de la ocurrencia de un incidente de seguridad o de la necesidad de cumplimiento de una ley o norma, que habitualmente tiene asociado un importante impacto en el negocio. Es en ese momento de forma inmediata, o de forma más planificada, si la organización cuenta

con una persona calificada que logre impulsar una iniciativa previa en ese sentido, cuando se requiere la presencia de los profesionales de la seguridad de la información para por una parte solucionar los problemas existentes en esa materia, y por otra comenzar el camino hacia la disminución del riesgo y la implantación de las medidas de seguridad adecuadas.

4.8 Objetivos de la Metodología de la Especificación de Requerimientos

El método propuesto tiene como uno de sus principales objetivos conocer las expectativas del usuario. Para ello, se identifican los grupos de usuarios reales y posibles con sus áreas de aplicación, se revisa la documentación existente, se analiza el entorno operativo y sus requerimientos de procesado y se realizan entrevistas o cuestionarios a los usuarios.

Para todo este proceso existen técnicas formalizadas de especificación de requerimientos que más o menos concuerdan con las siguientes:

Se identifican las entradas del problema, los resultados deseados o salidas y cualquier requerimiento o restricción adicional en la solución.

• Obtener información acerca de lo que los usuarios desean

Los requerimientos son el punto en que el cliente y el proyecto se unen, esta unión es necesaria para poder configurar un servidor que satisfaga las necesidades del cliente.

Si los requerimientos se enfocan a describir las necesidades del cliente, entonces es lógico que la obtención de esta información sea de primera mano. Esto es, mediante entrevistas con el cliente o buscando documentación que describa la manera que el cliente desea que funcione la solución.

Las necesidades y/o requerimientos del cliente evolucionan con el tiempo y cada cambio involucra un costo. Por eso es necesario tener archivada una copia de la documentación original del cliente, así como cada revisión o cambio que se haga a esta documentación

Como cada necesidad del cliente es tratada de diferente forma, es necesario clasificar estas necesidades para saber cuáles de ellas serán satisfechas por el proyecto y cuales por algún otro producto del sistema.

Una de las bases para conseguir los objetivos mencionados será no sólo considerar la seguridad como algo abstracto y general, sino evaluar, y por tanto analizar y proponer en detalle, las medidas técnicas y organizativas correspondientes. Aspectos organizativos como la estructura de la organización, roles existentes, responsabilidades definidas o flujos de información, entre otros, serán estudiados a la vez que otros más técnicos como arquitectura y topología de servicios, redes, sistemas y comunicaciones, dispositivos de seguridad existentes o análisis de vulnerabilidades, etc.

4.9 Metodología de la Implantación

Esta metodología de manera general comienza evaluando la seguridad de la organización mediante la recolección de información a través de entrevistas con personal de la institución, realizando pruebas de campo y análisis técnicos, para a continuación, presentado un informe del estado de implantación.

Siguiendo el esquema con las siguientes fases secuenciales bien definidas.

4.9.1 Identificación de Interlocutores

Objetivo: Identificar el participante (o interlocutores) válidos en la organización y planificación de su disponibilidad por parte de la organización.

La fase de recolección de información tiene una gran importancia en el desarrollo del método puesto que la información obtenida en la misma será la fuente del análisis y desarrollo del estado en seguridad de la información de la organización y del posterior plan de acción. Por ello, para el desarrollo de esa fase deberá contarse con la colaboración total de la organización para la obtención de la información correspondiente.

Habitualmente la organización deberá nombrar una persona (o varias de ser necesario) que ejercerá como interlocutor entre el equipo de trabajo que esté desarrollando el estudio y la organización, de forma que se realizarán las correspondientes consultas al interlocutor y éste las trasladará a las personas que corresponda dentro de la organización. Será importante que la organización prevea su disponibilidad durante el periodo de recolección de datos.

Adicionalmente, para determinadas tareas que serán claramente identificadas previamente por el equipo de trabajo, podrá ser necesario el acceso directo a determinados dispositivos y sistemas de la compañía para realizar comprobaciones de configuración, de seguridad, etc. Este acceso deberá ser proporcionado por la organización con los requisitos que ésta estime oportunos: bajo supervisión de personal propio, con diario de operaciones efectuadas, o cualquier mecanismo que ofrezca unas funcionalidades similares y salvaguarde la integridad de la información. El equipo de trabajo firmará un acuerdo de confidencialidad constituyendo una garantía hacia la organización de no difusión ni utilización de la información tratada. Así mismo la organización deberá firmar por escrito una autorización para realizar las pruebas que el equipo de trabajo indique y estime oportunas para obtener la información necesaria para la realización de las tareas encomendadas.

4.9.2 Recolección Técnica de Información

Objetivo: Obtener información mediante diversos métodos técnicos y empíricos en una muestra representativa de los sistemas y dispositivos de la organización.

Partiendo de la información recolectada en la fase anterior, se procederá a identificar los sistemas objeto de estudio para a continuación realizar una serie de análisis técnicos con el fin de conocer de forma precisa cual es su estado real desde un punto de vista de seguridad técnica. Mediante estos análisis seremos capaces de detectar problemas de seguridad, existentes o potenciales, que puedan afectar a la integridad de los sistemas de la organización, además de su funcionamiento o rendimiento.

En esta parte se puede reunir información muy importante como cuáles son los servicios que los usuarios de la empresa requieren para la navegación por internet, por ejemplo.

A continuación se enumeran los distintos puntos que deberán ser abordados durante la recolección técnica de información.

4.9.3 Enumeración y Caracterización

Tomando como base la información general recopilada en la fase "Recolección General de Información", se identificarán los sistemas, dispositivos y aplicaciones sobre los que se realizará el estudio técnico, llevando a cabo una caracterización lo más exhaustiva posible de cada elemento puesto que esta información resultará de mucha utilidad a la hora de realizar los análisis técnicos y la interpretación de los resultados.

La información mínima que deberá recopilarse será la siguiente (aunque podrá ser ampliada con aquellos datos que el equipo de trabajo pueda considerar de interés):

Caracterización de Sistemas

- Sistema (nombre, tipo, fabricante)
- Ubicación
- Responsable
- Versiones software (SSOO, aplicaciones que corren en él)

Caracterización de Aplicaciones

- Aplicación (nombre, fabricante, versión)

- Subsistemas asociados (sistemas en que corre)
- Interrelación con otras aplicaciones
- Responsable

4.9.4 Análisis de Tráfico

Mediante el análisis de tráfico se intentará caracterizar el tipo de tráfico que circula habitualmente por las redes de la organización, así como detectar posibles puntos de fallo o cuellos de botella en dichas redes.

Para un óptimo resultado del análisis, deberán identificarse cuales son los puntos sensibles en los que deberán realizarse las medidas, entendiendo por *sensibles* aquellos puntos con representatividad en su tráfico.

Dichos puntos, típicamente podrán ser:

- Interconexiones entre segmentos
- Segmentos de servidores/aplicaciones críticas
- Segmentos de usuarios
- Otros puntos de interés

Cada medida deberá realizarse durante un periodo de tiempo significativo de forma que se capture una cantidad de tráfico suficiente para su posterior análisis. El tiempo de medida dependerá de la cantidad de tráfico que habitualmente soporte la red. En algunos entornos será suficiente mantener la medida durante unos pocos minutos, mientras que en otros será necesario realizar la medida a lo largo de un día completo o incluso, periodos más prolongados de tiempo.

También será necesario tener en cuenta las franjas temporales de utilización de la red. Por ejemplo, no será lo mismo la captura de tráfico en una red de oficina, que en una red de una fábrica en la que se realizan trabajos 24 horas al día.

Por tanto, será importante conocer las pautas de utilización de la red con el fin de seleccionar los momentos de medida adecuados.

Las capturas, por norma general, se realizarán sin ningún tipo de filtrado, y se almacenarán en disco de forma que puedan ser reproducidas y tratadas en laboratorio con el fin de generar informes y estadísticas de uso. Para su realización se utilizará cualquier analizador de protocolos que permita la realización de las tareas anteriormente comentadas.

4.9.5 Análisis de Vulnerabilidades y Aplicaciones

El análisis de vulnerabilidades de sistemas y aplicaciones tiene como objeto detectar puntos débiles en la seguridad de los sistemas y aplicaciones que éstos soportan. Se entiende por puntos débiles, errores de programación o de configuración en las aplicaciones y sistemas operativos que puedan ser causa de vulnerabilidades susceptibles de ser explotadas por potenciales atacantes. Por tanto, será importante conocer cuáles son estos puntos débiles con el fin de implantar los controles adecuados para eliminarlos o evitar su explotación.

No todos los sistemas tienen la misma importancia dentro de la organización. Por esto, y porque el análisis de vulnerabilidades es una tarea que puede consumir mucho tiempo, deberá realizarse una selección de cuáles son los sistemas sobre los que se realizará el análisis. Objetivos típicos de este tipo de análisis serán los sistemas cuyo mal funcionamiento pueda causar un impacto importante en los procesos de la

organización (e.g. Servidores principales) o aquellos que por su visibilidad están más expuestos a posibles ataques (e.g. Servidores con acceso público desde Internet). Deberá ser la organización objeto del análisis quien, con el asesoramiento del equipo de trabajo que efectúe el análisis, decida cuales son los sistemas que deben ser analizados.

En el caso de los servidores de internet la política que se usa es desactivar todos los puertos a excepción de los que se van a utilizar tanto por los usuarios como por las aplicaciones que usa la empresa. Y de esta manera no se deja un agujero de seguridad el cual puede ser explotado por intrusos.

4.9.6 Análisis Remoto

Se prestará especial atención a las vulnerabilidades que pueden ser explotadas remotamente, ya que éstas pueden suponer un mayor riesgo al no requerir de presencia física para su explotación. Dichas vulnerabilidades, habitualmente estarán asociadas a puertos de aplicación que esperan recibir conexiones remotas. El primer paso del análisis de vulnerabilidades, por tanto, será identificar cuáles son los puertos de los sistemas que son accesibles de forma remota. Un método para conseguir esta información será la realización de un escaneo de puertos.

El objetivo del escaneo de puertos será averiguar que puertos (típicamente TCP o UDP) están a la escucha en un sistema determinado, y por tanto, pueden recibir conexiones remotas. Es esta una información de suma importancia, ya que una gran parte de las vulnerabilidades asociadas a aplicaciones, tienen que ver con las

posibilidades de conexión remota de las mismas. La técnica básica para saber el estado de un puerto es tratar de realizar una conexión contra el mismo y analizar el resultado, pudiendo obtenerse tres valores para el estado de un puerto:

- Abierto: El puerto está a la escucha y listo para recibir conexiones.
- Cerrado: El puerto no está a la escucha
- Filtrado: Existe algún dispositivo (típicamente un cortafuegos/firewall) que no permite realizar conexiones contra el puerto.

Existen diferentes técnicas de escaneo de puertos, muchas de ellas orientadas a tratar de evitar métodos de detección y seguridad de los sistemas objetivo, pero en el caso que ocupa pueden no ser relevantes, ya que deberá contarse con la aprobación y el permiso por escrito del propietario de los sistemas para realizar el escaneo y las acciones correspondientes, pudiendo realizar los escaneos y análisis sin necesidad de utilizar técnicas de camuflaje (*stealth*), salvo en el caso en que existan dispositivos de seguridad (como sistemas de prevención de intrusiones IDS) que puedan invalidar los resultados de dichas pruebas.

Una vez establecido el alcance de los sistemas sobre los que se realizará el análisis, se deberá elegir la profundidad del mismo, es decir, deberá decidirse sobre que puertos se realizarán las posteriores comprobaciones. Evidentemente, para que el análisis sea completo, debería comprobarse el estado de todos los puertos (tanto TCP como UDP1), pero dado que en ocasiones esto puede llevar más tiempo del que se tendrá disponible, en ciertos casos será posible reducir el número de puertos a analizar, bien porque se tenga la certeza de que el sistema sólo escucha en ciertos puertos, o porque existan dispositivos de filtrado que sólo permitan la conexión a puertos determinados. De esta forma, la complejidad del escaneo de puertos y el consiguiente análisis de vulnerabilidades se reducirá haciéndose mucho más manejable.

Tras realizar el escaneo de puertos, se dispone de la información referente a que puertos tiene disponibles cada sistema para aceptar conexiones remotas. Cada uno de estos puertos estará asociado a un servicio y por tanto a una aplicación. El siguiente paso será averiguar cuáles son dichas aplicaciones y, si es posible, la versión de las mismas.

Conocer el software específico que está instalado en un sistema es una de las primeras labores que intentará abordar un potencial atacante, ya que con esta información, se pueden conocer cuáles son las vulnerabilidades que presentan las aplicaciones remotamente accesibles, y de esta forma acceder a los métodos de explotación de la vulnerabilidad (o *exploits*). El resultado de la ejecución de un *exploit* se materializa habitualmente en un compromiso del sistema, que puede ir desde la eventual destrucción de sus datos al acceso no lícito de sus recursos.

La identificación de software a partir de los puertos por los que escucha puede realizarse mediante las respuestas (*banners*) que proporciona el servicio ante una conexión entrante. No obstante, dado que los *banners* pueden (y deben) ser modificados por motivos de seguridad, esta no es una manera adecuada de realizar esta tarea. Existen multitud de aplicaciones, muchas de ellas de código libre (*open source*), que automatizan la tarea de identificar las aplicaciones asociadas a un puerto. Estas aplicaciones no se limitan a reconocer los *banners* de respuesta, sino que analizan las respuestas de la aplicación ante ciertas entradas, y en base a diferencias de implementación conocidas, son capaces de deducir, eso sí, con un grado de precisión variable, la aplicación y versión que está proporcionando el servicio en cuestión

Este proceso (escaneo + identificación), es la forma en la que un posible atacante trabajaría, y es importante llevarlo a cabo con el fin de crear consciencia de qué información podría ser obtenida con estos medios. No obstante, desde el punto de vista del análisis de seguridad, y con el fin de tener certeza sobre la veracidad de los resultados obtenidos, la identificación de aplicaciones y sus versiones debería ser abordada adicionalmente mediante el análisis local de los sistemas en cuestión.

En este punto, a un posible atacante le bastaría consultar alguno de los múltiples servicios disponibles en Internet que permiten conocer las vulnerabilidades (y los *exploits*) de una versión de aplicativo determinada. Por el contrario, la labor del equipo de trabajo será averiguar cuáles son los parches o actualizaciones adecuadas para solucionar los problemas de dicho aplicativo. En caso de que no existiesen o no se pudiesen aplicar dichos parches o actualizaciones, deberán buscarse alternativas que disminuyan el nivel de riesgo de exposición de estas aplicaciones.

Actualmente, las redes de comunicaciones en las que se ubican los sistemas analizados, son rara vez planas. Es habitual la existencia de diferentes segmentos, separados por diferentes dispositivos y con distintas políticas de acceso. Por tanto, el análisis de vulnerabilidades ofrecerá diferentes resultados dependiendo desde que origen se realice. Teniendo esto en cuenta, para que los resultados de los análisis sean válidos, éstos deberán ser realizados desde todas las posibles ubicaciones que puedan ocupar los potenciales atacantes, ofreciendo así distintos perfiles de visibilidad (y de exposición al riesgo) del sistema analizado.

De forma típica, se realizarán análisis desde las siguientes ubicaciones:

• **Internet:** Desde Internet se tendrá acceso a los servicios públicamente accesibles de la organización. Mediante este análisis se verificará que sólo estos servicios son accesibles de forma pública.

• **DMZ:** Si en la organización existen segmentos de DMZ, deberán realizarse los escaneos hacia los servidores internos desde esta ubicación, ya que es un punto de entrada habitual una vez que ha sido comprometido alguno de los servidores públicos. De esta forma podrá conocerse que grado de visibilidad tendrán los servidores internos para un atacante que ya ha conseguido comprometer algún sistema de la organización.

• **Mismo segmento:** El escaneo desde el mismo segmento de red permite conocer sin acceder físicamente al sistema cuales son los servicios que tiene configurados, tanto los que se están utilizando como los que están en funcionamiento sin ser utilizados debido a malas prácticas de administración o instalaciones por defecto.

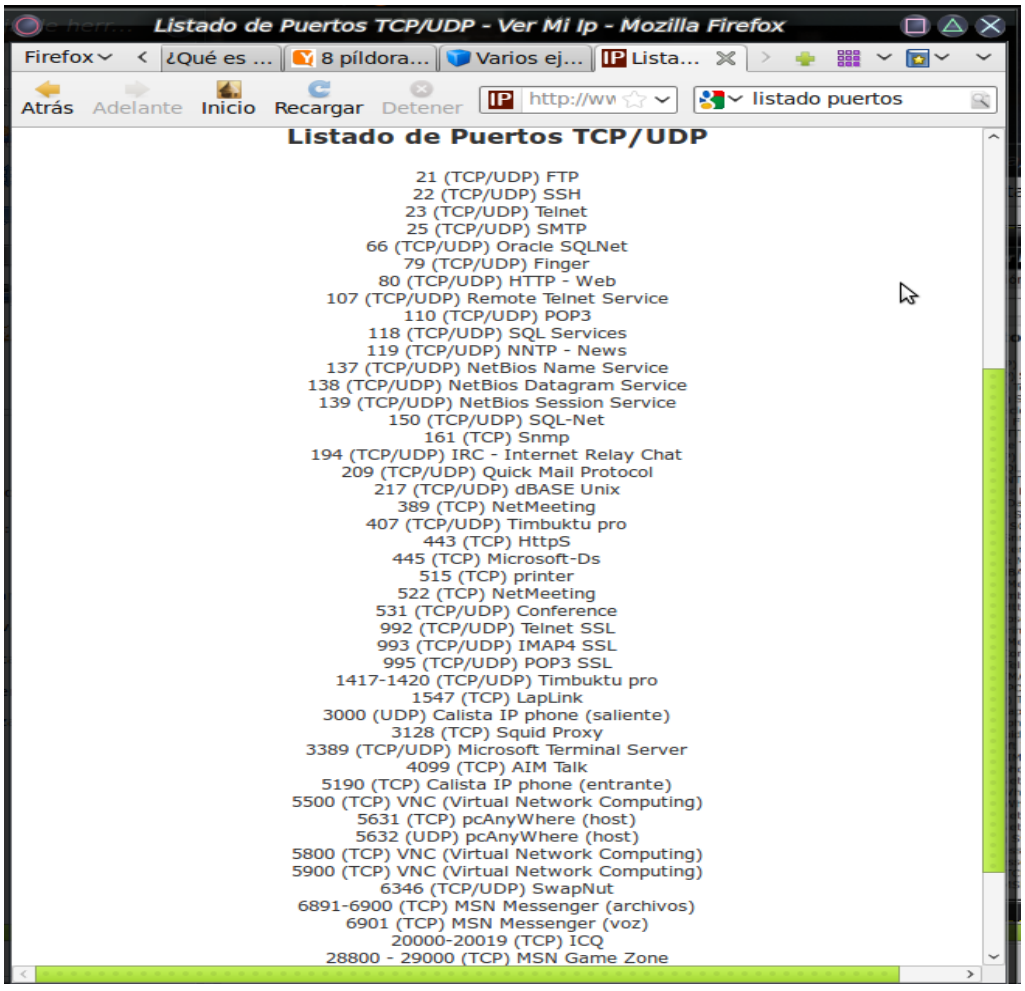
• **Red Interna:** Dado que una gran parte de los incidentes de seguridad en los sistemas de las organizaciones proviene de la propia organización, es importante conocer que servicios son accesibles (y por tanto posibles causas de vulnerabilidad) desde las redes de usuarios internos.

En el caso del servidor Linux se puede trabajar con ssh (Secure Shell) esta es una herramienta que permite modificar configuraciones del servidor y poder acceder de manera remota desde cualquier lugar usando internet.

Como se puede ver en el siguiente gráfico, hay una lista de puertos que son usados para las diferentes funcionalidades de usuarios y aplicaciones, dependiendo de los requerimientos de la empresa estos puertos se pueden dejar abiertos, según sea conveniente. La política de seguridad de Linux es todos los puertos son cerrados a menos que se necesite usarlos.

Algo importante que se requiere realizar en el área de seguridad es capacitar a los usuarios que son el eslabón más débil de la cadena, ya que hay maneras de sacar información valiosa estas técnicas las conocen como ingeniería social.

El uso y cambio regular de claves de acceso así como también el usar claves que contengan números, letras mayúsculas y minúsculas, símbolos. Estas políticas de contraseñas también son aplicables a los administradores informáticos.



Nombre: Lista de puertos

Fuente: Lista de puertos TCP / UDP

Elaborado: JHON MOLINA

Figura: 2 Lista de puertos

4.9.7 Revisión y Configuración

Durante la recolección técnica de información se revisarán también las configuraciones de elementos clave de la red de la organización. Muchas veces, debido al volumen de elementos de red no será posible realizar una revisión exhaustiva, sin embargo, será necesario en este caso decidir de acuerdo con el interlocutor de la organización cuales serán los dispositivos sobre los que se realizará el análisis.

Para la revisión de las configuraciones será necesaria la participación de expertos en los distintos dispositivos analizados que puedan identificar fallos en las mismas, formas más eficientes de implementar una determinada funcionalidad o mecanismos alternativos que mejoren la seguridad y eficiencia del dispositivo.

Típicamente deberán revisarse al menos dispositivos de electrónica de red (routers, switches, bridges, etc.), dispositivos de seguridad (cortafuegos / firewalls, etc.), aplicaciones (servidores Web, ftp, de correo, etc.) y en general cualquier dispositivo con una funcionalidad necesaria dentro de la organización que pueda suponer una posible fuente de vulnerabilidades y por tanto de elevación del nivel de riesgo asumido por la organización.

4.9.8 Visualización Externa

Existe una gran cantidad de información relativa a las organizaciones accesible de forma pública desde Internet. Esta información puede ser una pieza clave para el diseño de un eventual plan de ataque contra la organización, porque puede revelar interesantes detalles, tanto técnicos como organizativos, que utilizados de forma adecuada facilitan la tarea de potenciales atacantes. Es importante, por tanto, que la organización sea consciente de la existencia de esta información, por lo que deberá prestarse especial atención a los siguientes puntos.

4.9.8.1 Direccionamiento Público

Mediante los servicios de los registradores regionales de Internet (ej. RIPE en Europa, ARIN en Norteamérica) se conoce los rangos de direcciones públicas asignados a la organización, direcciones postales, de correo electrónico y números de teléfono, nombres de responsables y contactos dentro de la organización.

La organización deberá tener un conocimiento preciso de esta información con el fin de asegurarse que los datos son correctos y no proporciona más información de la debida.

4.9.8.2 Nombres de Dominio y DNS

Deberán recopilarse todos los nombres de dominio pertenecientes a la organización, puesto que mediante las herramientas de consulta ofrecidas por los agentes registradores de dominio se pueden obtener datos de contactos técnicos, administrativos y de facturación.

Para cada dominio de la organización deberán realizarse búsquedas en el servicio DNS, prestando especial atención a:

- Servidores de Nombres (NS)
- Intercambiadores de correo (MX)
- Nombres conocidos (ej. www, ftp)

Estos nombres, corresponderán a servidores susceptibles de ser atacados y por tanto deberán ser objeto de un cuidadoso proceso de asegurado.

En el caso del servicio whois y DNS los registradores tienen un servicio que pone datos ficticios para proteger a los dueños del dominio de posibles búsquedas de información importante por parte de intrusos.

4.9.8.3 Filtrado de Documentación

Una mala configuración de los servidores Web puede permitir la publicación en Internet de documentos que no deberían ser vistos fuera de la organización. Los actuales buscadores Web (ej. Google) permiten realizar sofisticadas búsquedas, por ejemplo restringidas por dominio y por tipo de fichero.

Siempre resulta sorprendente la cantidad de información que puede ser hallada mediante estas búsquedas. Por tanto, dentro de la recolección técnica de información de la organización, deberán realizarse búsquedas de este tipo con el fin de conocer si la organización es vulnerable a este tipo de ataques e identificar cual es la causa de esta publicación no autorizada.

Para evitar este tipo de actividades por parte de atacantes, se puede realizar cada cierto tiempo tests de vulnerabilidad estos consisten en simular ataques externos e internos para comprobar si las políticas de seguridad son las adecuadas.

4.10 Seguridad de Frontera

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aun, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo.

De lo anterior, los administradores de red han tenido la necesidad de crear políticas de seguridad consistentes en realizar conexiones seguras, enviar y recibir información encriptada, filtrar accesos e información, etc. No obstante lo anterior, el interés y la demanda por Internet crece y crece y el uso de servicios como World Wide Web (WWW), Internet Mail, Telnet y el File Transfer Protocol (FTP) es cada vez más popular.
El presente trabajo piensa dar una visión global acerca de los problemas de seguridad generados por la popularización de Internet, como las transacciones comerciales y

financieras seguras, el ataque externo a redes privadas, etc. Se conceptualizarán temas como el uso de firewalls, de llaves públicas (criptografía) y los niveles de seguridad establecidos en la actualidad.

4.11 Firewalls

Es conveniente que para iniciar este documento hay que definir primeramente las partes elementales que más interesan en esta tesis. En primer lugar la WAN (World Area Network) es una gran red de cómputo de cobertura mundial y una de las más comunes es Internet. En segundo lugar, está la red LAN (Local Area Network) que es una red mediana denominada local ya que está limitada a una pequeña área geográfica y normalmente es utilizada por empresas privadas, públicas, educativas, etc. Estas dos redes llegan a interactuar utilizando un conjunto de protocolos de comunicación de datos.

TCP/IP es de los protocolos más comunes. Y en sus siglas encontramos Protocolo de Control de Transmisión y Protocolo de Internet (Transmisión Control Protocol / Internet Protocol). Estos protocolos permiten el enrutamiento de información de una máquina a otra, la entrega de correo electrónico y noticias, e incluso la conexión remota.

Dado que esta investigación se enfoca en la seguridad que le proporciona un dispositivo Firewall a la información, se define para su entendimiento. Un Firewall es un sistema que se encarga de fortalecer las políticas de acceso entre redes de trabajo; por desgracia, en el mundo se tiene que someter a una constante precaución por diferentes ataques que pueden dañar incluso la información que se guarda en los computadores.

El propósito de un firewall es, entonces, proteger datos almacenados contra cualquier tipo de persona que busque afectar la máquina y a la vez permite llevar a cabo el trabajo de una forma más cómoda y eficiente.

Es importante tener una política de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de su compañía.

La mayoría de los diseñadores de redes por lo general empiezan a implementar soluciones de Firewall antes de que se haya identificado un problema particular de seguridad de red. Una organización puede tener muchos sitios, y cada uno contar con sus propias redes.

Si la organización es grande, es muy probable que los sitios tengan diferente administración de red, con metas y objetos diferentes. Si estos sitios no están conectados a través de una red interna, cada uno de ellos puede tener sus propias políticas de seguridad de red. La política de seguridad del sitio debe tomar en cuenta las necesidades y requerimientos de seguridad de todas las redes interconectadas.

En general, un sitio es cualquier parte de una organización que posee computadoras y recursos relacionados con redes. Algunos, no todos, de esos recursos son los siguientes:

- Estaciones de trabajo
- Computadoras hosts y servidores
- Dispositivos de interconexión: gateway, routers, bridges, repetidores
- Servidores de terminal

- Software para conexión de red y de aplicaciones
- Cables de red

4.11.1 Decisiones Básicas al Adquirir una Red Firewall

La primera decisión y la más básica, es reflejar la política con que la compañía u organización quiere trabajar con el sistema: ¿Se destina el Firewall para denegar todos los servicios excepto aquellos críticos para la misión de conectarse a red? ó ¿Se destina el Firewall para proporcionar un método de medición y auditoría de los accesos no autorizados de la red? El segundo es: ¿Qué nivel de vigilancia, redundancia y control queremos? Hay que establecer un nivel de riesgo aceptable para resolver el primer asunto tratado, para ello se pueden establecer una lista de comprobación de los que debería de ser vigilados, permitido y denegado. El tercer asunto es financiero: Es importante intentar cuantificar y proponer soluciones en términos de cuánto cuesta comprar o implementar tal cosa o tal otra. En cuanto al asunto técnico, se debe tomar la decisión de colocar una máquina desprotegida en el exterior de la red para correr servicios Proxy tales como telnet, ftp, news, etc. o bien colocar un router cribador a modo de filtro, que permita comunicaciones con una o más máquinas internas.

4.11.2 Características de los Firewalls

Para que un firewall trabaje apropiadamente y cumpla con su función, éste debe ser parte de una consistente arquitectura de seguridad, por lo tanto debe al menos cumplir las siguientes características:

• **Protección de la Red.** Bloquear el tráfico del exterior hacia el interior a la vez que le permiten el acceso al tráfico interior hacia el exterior.

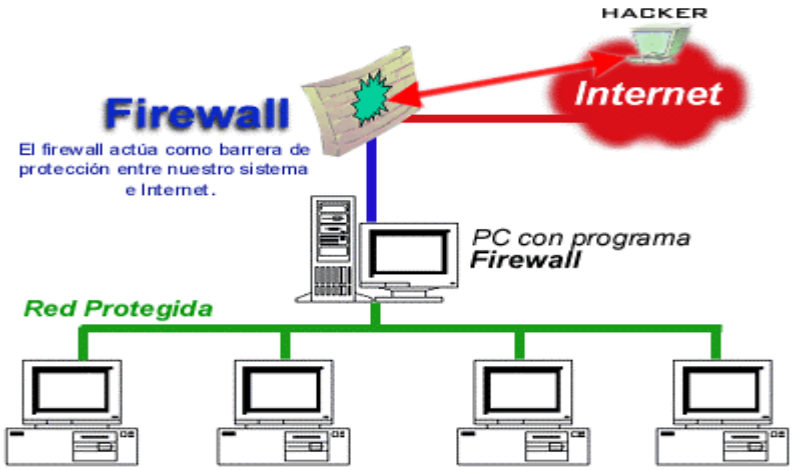
• **Control de acceso a los recursos de la red.** Al encargarse de filtrar, en primer nivel antes que lleguen los paquetes al resto de las computadoras de la red, el firewall debe ser idóneo para implementar controles de acceso.

• **Control de uso de Internet.** Bloquear el material no- adecuado, determinar que sitios que puede visitar el usuario de la red interna y llevar un registro.

• **Concentra la seguridad**. Facilitar la labor a los responsables de seguridad, dado que su máxima preocupación de encarar los ataques externos y vigilar, mantener un monitoreo.

• **Control y estadísticas**. Permitir controlar el uso de Internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.

• **Alarmas de Seguridad**. Generar alarmas para que el administrador del firewall pueda tomar el tiempo para responder una alarma y examina regularmente los registros de base.



Nombre: Firewall

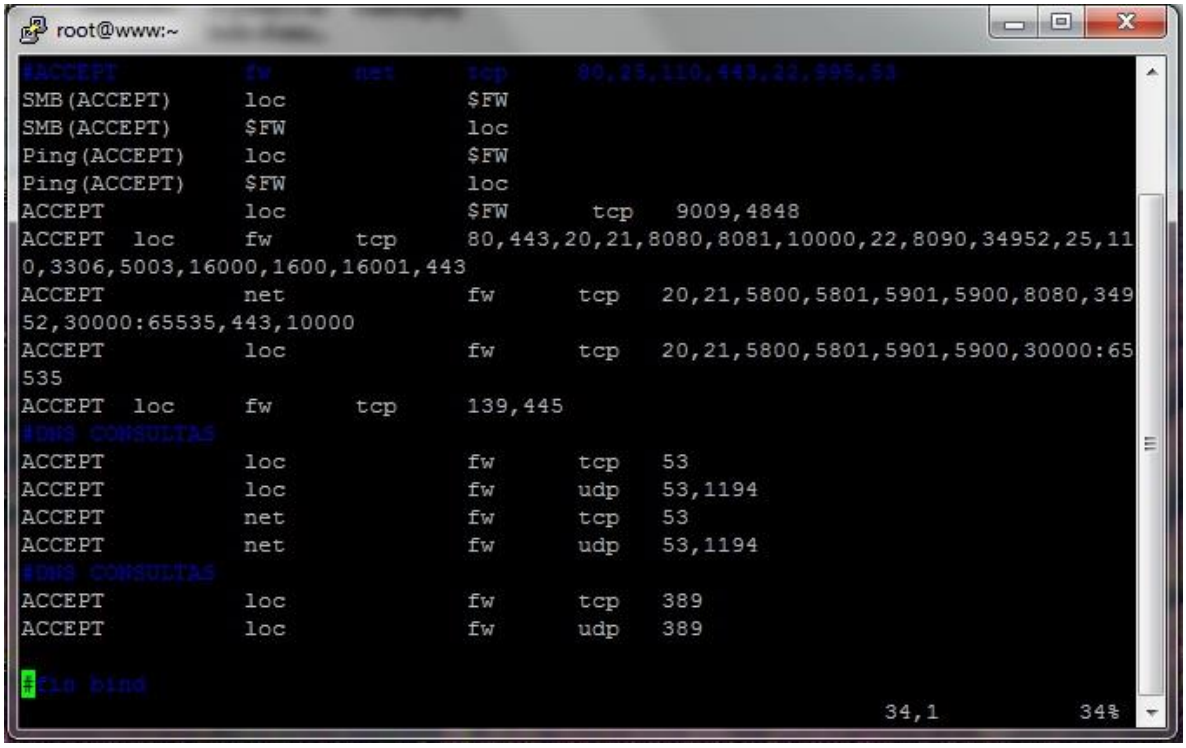
Fuente: Soporte21

Elaborado: JHON MOLINA

Figura: 3 Firewall

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

La configuración del Firewall la realizaremos con la herramienta Shorewall, es un poco más sencilla de usar que Iptables, pero no por eso menos efectiva. Las reglas que se usaron son las que se pueden observar en los 2 gráficos de a continuación:



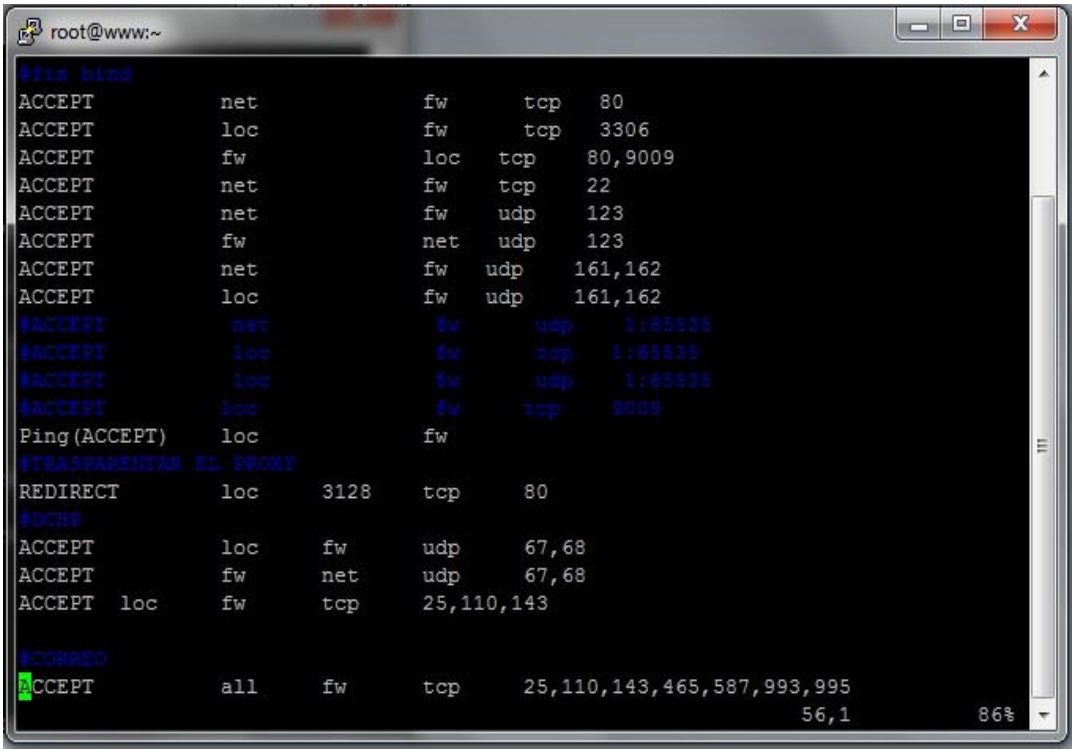
Los símbolos de la configuración significan:

Loc → Red Local

Net → Red Externa

Fw → Reenvío

La política usada es la de restricción, esto quiere decir que todos los puertos están cerrados hacia la comunicación a excepción de los que se define en este archivo, de esta manera solo activaremos los servicios que vamos a utilizar aislando al máximo la cantidad de puertos abiertos innecesariamente.

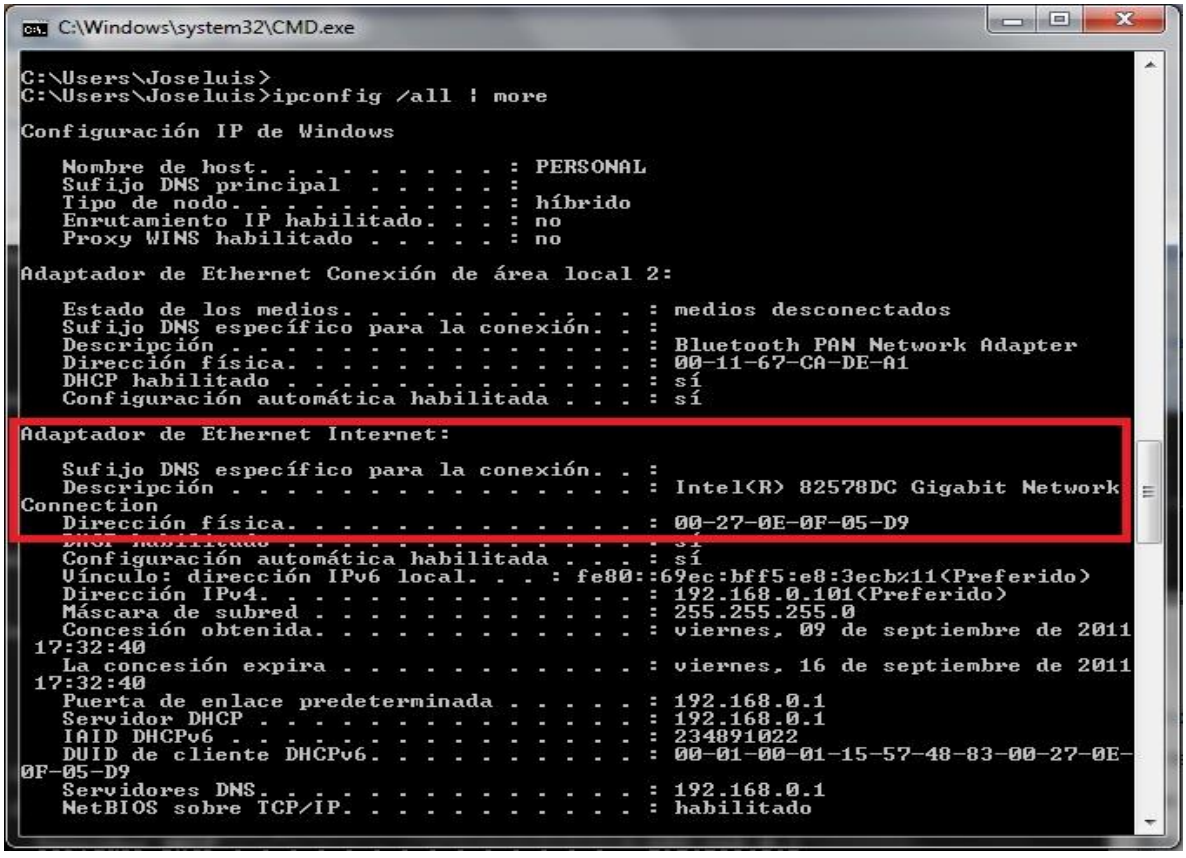


4.12 Niveles de Navegación

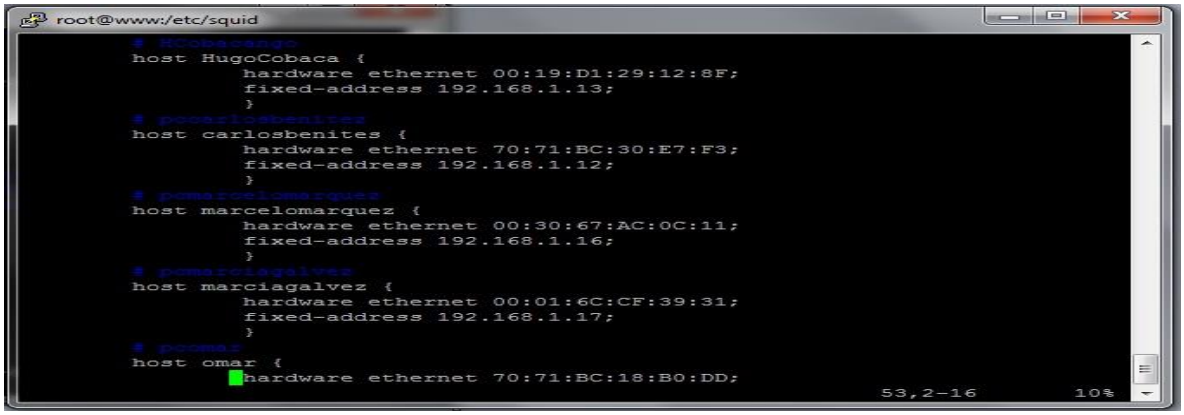
Para trabajar con niveles de navegación que permitan a ciertos usuarios tener acceso total a la red y por otro lado, otros usuarios tengan internet con ciertas restricciones lo que nos permite optimizar y priorizar la red a los servicios específicos del negocio. Esto se lo logra usando un servicio DHCP que filtre a los usuarios por medio de las direcciones MAC.

De esta manera el servicio DHCP asocia la dirección MAC con una dirección IP, posteriormente se crea archivos que contengan las direcciones de acceso a la red.

Este requerimiento nos obligara a crear una lista de direcciones MAC que se extiende de acuerdo al número de usuarios que tengamos, para obtener estos datos hay que ejecutar el comando ipconfig /all desde la consola de DOS en Windows o usando ifconfig desde Linux de ser el caso. En el siguiente gráfico podemos observar la información sobre la dirección MAC también conocida como dirección física obtenida usando Windows.

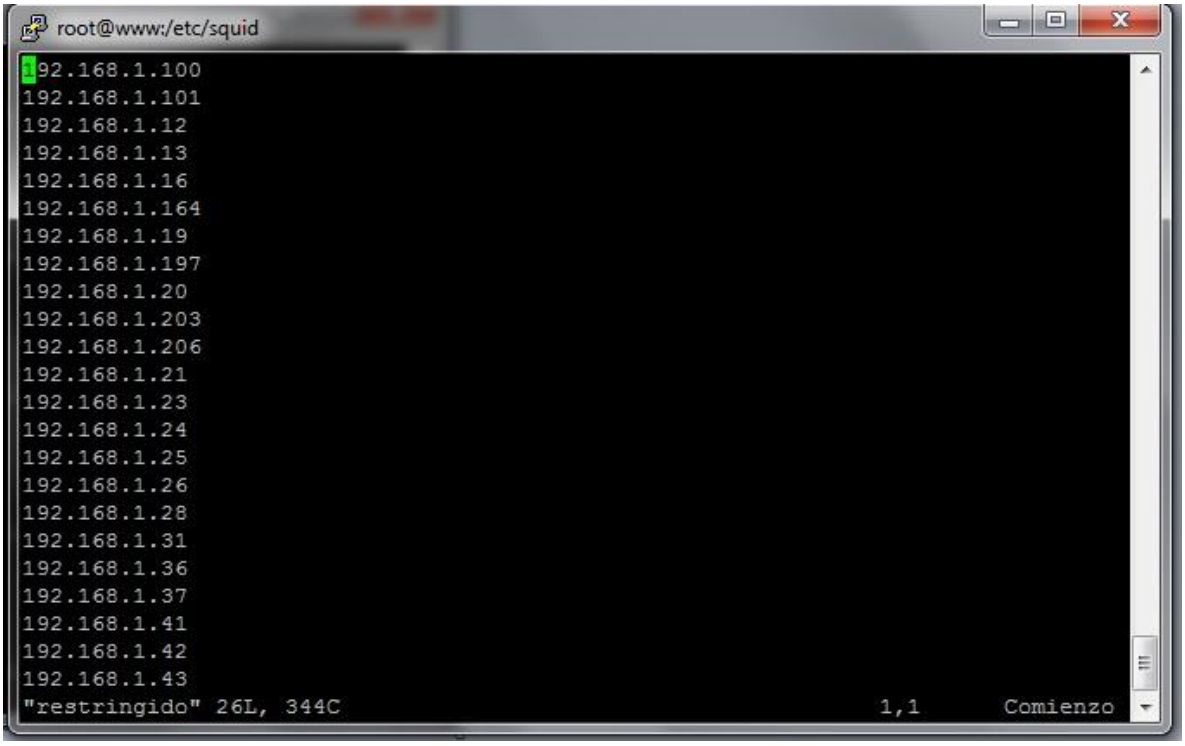


Un ejemplo de la configuración a la que haremos referencia la pueden observar en los siguientes gráficos.



Este servicio DHCP en la práctica genera una IP Fija la cual es asignada de acuerdo a la dirección física la estructura del archivo de configuración sería una similar a la del gráfico.

Con esta configuración ya definida solo bastaría con crear los archivos que permitan el acceso total o restringido al internet según los requerimientos de la institución. La configuración de los archivos sería muy similar al siguiente gráfico.



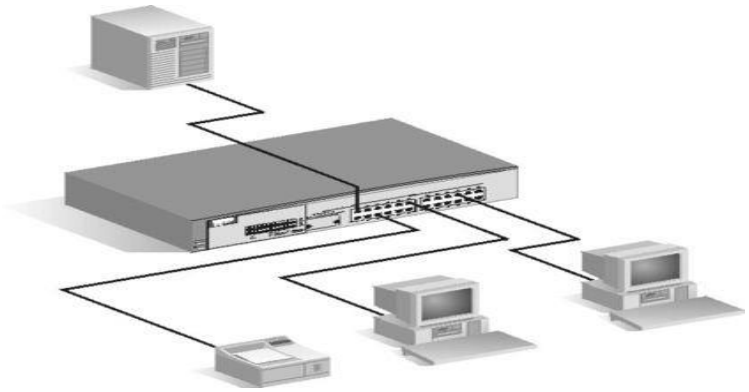
4.13 Switches

Un switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los data gramas en la red.[7]

Un conmutador en el centro de una red en estrella. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola.

[7] http://es.wikipedia.org/wiki/Switch

Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).



Nombre: Conmutador o *Switch*

Fuente: Google imágenes

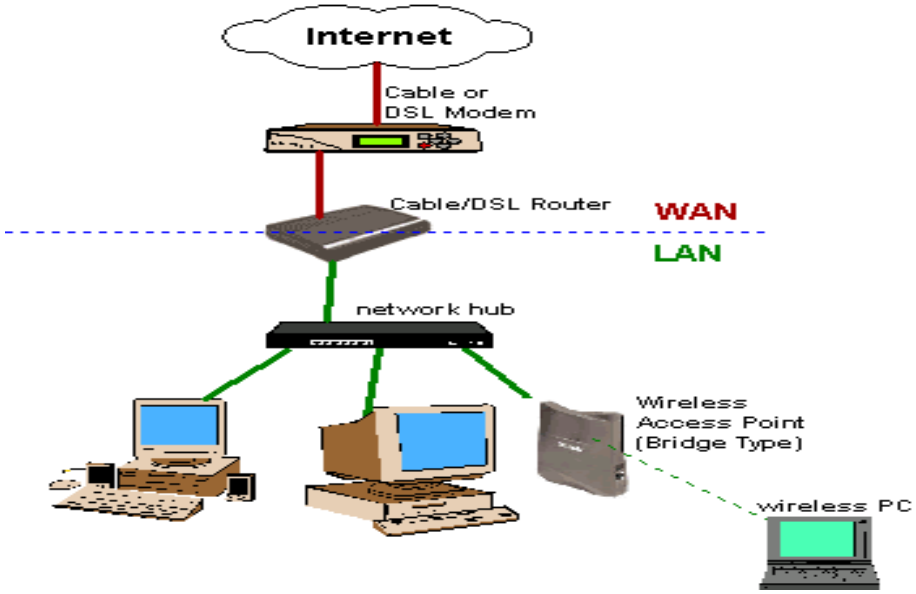
Elaborado: JHON MOLINA

Figura: 4 Conmutador o *Switch*

4.13 Routers

Un router (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.[8]

[8] http://es.wikipedia.org/wiki/Router



Nombre: Router

Fuente: Google imágenes

Elaborado: JHON MOLINA

Figura: 5 Router

Un router es un elemento de una red capaz de dirigir y filtrar el tráfico de una red. Por ejemplo, si un router trabajara en correos sería la persona encargada de decidir hacia dónde va una carta ya que es capaz de leer la dirección y dirigirla al lugar de destino. Por lo tanto, opera dirigiendo el tráfico de la red (paquetes de datos que van y vienen).

4.14 Medios de Comunicación

4.14.1 LAN (Local Area Network)

LAN son las siglas de Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Es la más simple de todas las conexiones que existen, ya que solo enlaza computadoras de un área pequeña como un edificio u oficina, así mismo, una LAN puede estar conectada con otras LAN a cualquier distancia por medio de línea telefónica y ondas de radio.

Su extensión está limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc. Para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

Pueden ser desde 2 computadoras, hasta cientos de ellas. Todas se conectan entre sí por varios medios y topología, a la computadora(s) que se encarga de llevar el control de la red es llamada "servidor" y a las computadoras que dependen del servidor, se les llama "nodos" o "estaciones de trabajo".
Los nodos de una red pueden ser PC´s que cuentan con su propio CPU, disco duro y software y tienen la capacidad de conectarse a la red en un momento dado; o pueden ser PC´s sin CPU o disco duro y son llamadas "terminales tontas", las cuales tienen que estar conectadas a la red para su funcionamiento.

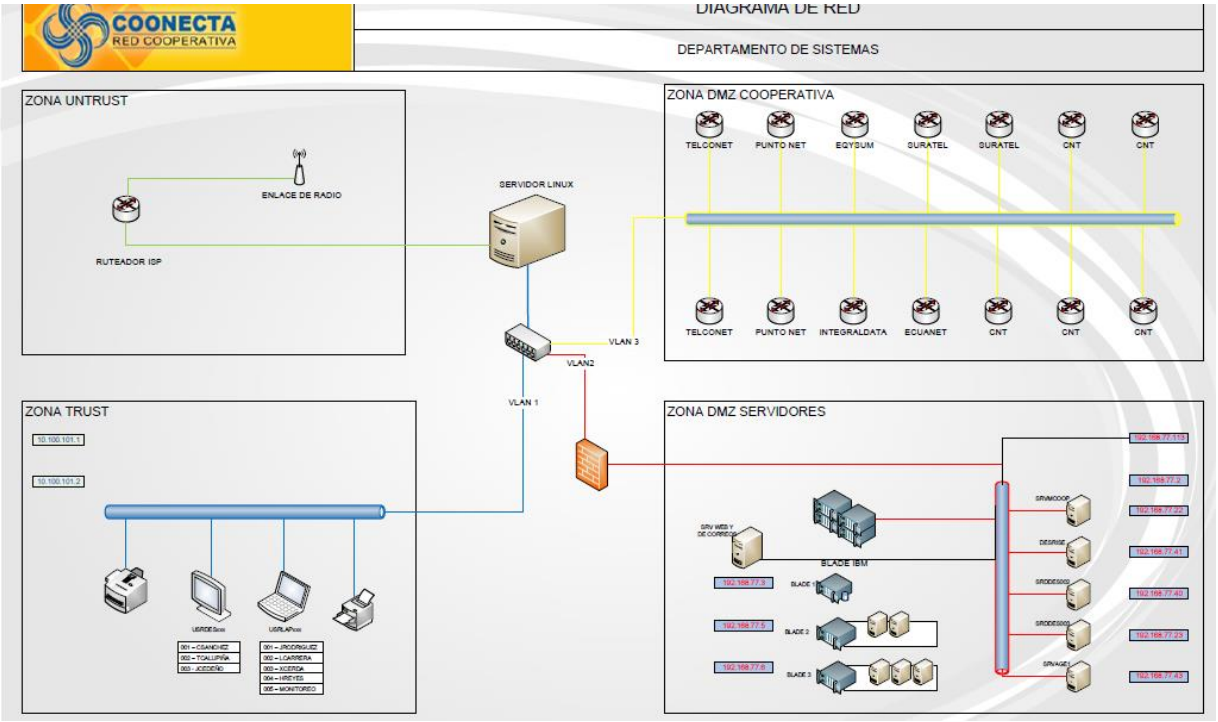
Las LAN son capaces de transmitir datos a velocidades muy rápidas, algunas inclusive más rápido que por línea telefónica; pero las distancias son limitadas.

Asimismo, en este tipo de red, tenemos tres formas en que las computadoras se conectan en red, estas son:

Igual a Igual: Cada estación de trabajo puede compartir alguno, todos o ninguno de sus recursos con las demás estaciones de trabajo.

Recursos Compartidos: Uno o más servidores centralizados envían y reciben ficheros, y contienen los recursos de las estaciones de trabajo en uso. Las estaciones de trabajo no pueden acceder a los recursos de las restantes estaciones, por lo que deben realizar ellas mismas todos los procesos.

Cliente-Servidor: Reparte una aplicación entre el cliente (estaciones de trabajo) y los componentes del servidor. El cliente de la aplicación acepta las entradas del usuario, las prepara para el servidor y le envía una solicitud. El servidor recibe las solicitudes de los clientes, las procesa y facilita el servicio solicitado al cliente. Entonces, el cliente presenta los datos u otros resultados al usuario por medio de su propia interfaz.



Nombre: Lan

Fuente: Coonecta

Elaborado: JHON MOLINA

Figura: 6 Lan

4.14.2 WAN (Wide Area Network)

Una red de área amplia, WAN, acrónimo de la expresión en idioma inglés Wide Area Network, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de

este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

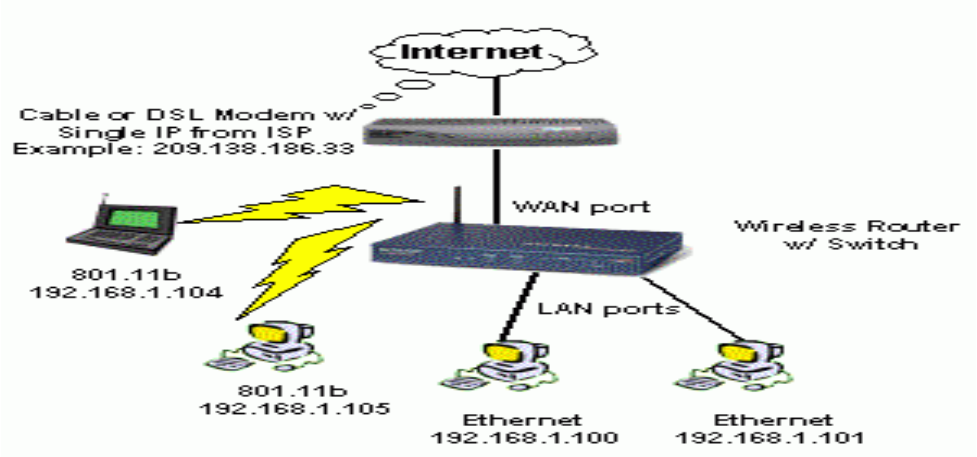
Actualmente Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente mientras que las VPN que utilizan cifrado y otras técnicas para hacer esa red dedicada aumentan continuamente.

Normalmente la WAN es una red punto a punto, es decir, red de paquete conmutado. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio. Fue la aparición de los portátiles y los PDA´s la que trajo el concepto de redes inalámbricas.

A diferencia de las redes LAN (siglas de "local area network", es decir, "red de área local"), la velocidad a la que circulan los datos por las redes WAN suele ser menor que la que se puede alcanzar en las redes LAN. Además, las redes LAN tienen carácter privado, pues su uso está restringido normalmente a los usuarios miembros de una empresa, o institución, para los cuales se diseñó la red.

La infraestructura de redes WAN la componen, además de los nodos de conmutación, líneas de transmisión de grandes prestaciones, caracterizadas por sus grandes velocidades y ancho de banda en la mayoría de los casos. Las líneas de transmisión (también llamadas "circuitos", "canales" o "troncales") mueven información entre los diferentes nodos que componen la red.

Los elementos de conmutación también son dispositivos de altas prestaciones, pues deben ser capaces de manejar la cantidad de tráfico que por ellos circula. De manera general, a estos dispositivos les llegan los datos por una línea de entrada, y este debe encargarse de escoger una línea de salida para reenviarlos. A continuación, en la Figura 7, se muestra un esquema general de los que podría ser la estructura de una WAN. En el mismo, cada host está conectada a una red LAN, que a su vez se conecta a uno de los nodos de conmutación de la red WAN. Este nodo debe encargarse de encaminar la información hacia el destino para la que está dirigida.



Nombre: Wan

Fuente: Google imágenes

Elaborado: JHON MOLINA

Figura: 7 Wan

4.14.3 WLAN (Wireless)

Una WLAN es un sistema flexible de comunicación de datos implementado como una extensión de, o como una alternativa para una LAN cableada.
Usando ondas electromagnéticas, las LAN inalámbricas transmiten y reciben datos sobre el aire, minimizando la necesidad de conexiones cableadas.

Además las LANs inalámbricas combinan la conectividad de los datos con la movilidad del usuario.
A través del despliegue de dispositivos llamados Puntos de Acceso o estaciones Base, la tecnología LAN inalámbrica puede ser usada para extender el alcance de una red cableada. Un Punto de Acceso típicamente tiene un puerto Ethernet para conexión a una red cableada, y una antena para comunicaciones inalámbricas. El software es integrado al "puente" entre lo inalámbrico y las redes cableadas. Comunicando inalámbricamente vía un punto de acceso, usuarios de computador pueden tomar ventajas de servicios de redes cableadas con flexibilidad de lo inalámbrico.

Nombre: WLan
Fuente: Google imágenes

Elaborado: JHON MOLINA

Figura: 8 WLan

4.14.4 BLUETOOTH

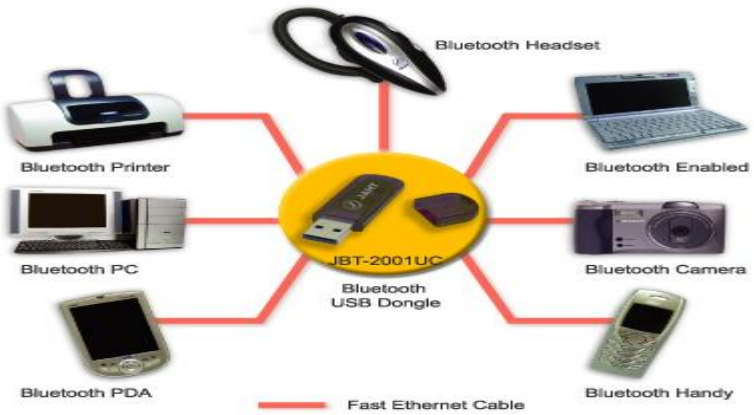
La tecnología Bluetooth es una especificación abierta para la comunicación inalámbrica (WIRELESS) de datos y voz. Está basada en un enlace de radio de bajo coste y corto alcance, implementado en un circuito integrado de 9 x 9 mm, proporcionando conexiones instantáneas para entornos de comunicaciones tanto móviles como estáticas. En definitiva, Bluetooth pretende ser una especificación global para la conectividad inalámbrica.

El principal objetivo de esta tecnología, es la posibilidad de reemplazar los muchos cables propietarios que conectan unos dispositivos con otros por medio de un enlace radio universal de corto alcance. Por ejemplo, la tecnología de radio Bluetooth implementada en el teléfono celular y en el ordenador portátil reemplazaría al molesto cable utilizado para conectar ambos aparatos.

Las impresoras, las agendas electrónicas, los PDA, los faxes, los teclados, los joysticks y prácticamente cualquier otro dispositivo digital son susceptibles de formar parte de un sistema Bluetooth.

Pero más allá de reemplazar, con frecuencia incómodos cables, la tecnología Bluetooth ofrece un puente a las redes de datos existentes, una interfaz con el exterior y un mecanismo para formar en el momento, pequeños grupos de dispositivos conectados entre sí de forma privada fuera de cualquier estructura fija de red.

Integrado en un pequeño transmisor de radiofrecuencia que permite conectar entre sí todo tipo de dispositivos electrónicos (teléfonos, ordenadores, impresoras, faxes, etc.) situados dentro de un radio limitado de 10 metros (ampliable a 100, aunque con mayor distorsión) sin necesidad de utilizar cables.



Nombre: Arquitectura Bluetooth

Fuente: Google imágenes

Elaborado: JHON MOLINA

Figura: 9 Arquitectura Bluetooth

4.15 Seguridad en Internet

La incorporación de las nuevas tecnologías encamina a un nuevo mundo virtual fantástico, pero también plantean nuevas situaciones que se debe conocer y afrontar.

Uno de los temas que se olvida, o se deja un poco de lado, es la seguridad en Internet. Así, los inconvenientes en cuestión de seguridad no son conocidos por todos los usuarios de la red y por ello no saben cómo protegerse de dicha vulnerabilidad que tienen cada vez que se conectan a la red de Internet, por lo tanto en los siguientes puntos explicaremos de manera simplificada los tópicos más comunes en cuanto a seguridades Internet se refiere.

4.16 Servidor Anti Virus

4.16.1 *Clamv Antivius Navegacion*

ClamAV es un software antivirus open source (de licencia GPL) para las plataformas, Linux, que nos ayudara para proteger de virus al internet.

Un virus es un ente que ingresa al organismo y que se reproduce a sí mismo para infectar a otras células del organismo, la misión del virus informático es semejante, sólo que en este caso es un programa o código el cual ingresa a través de diversas vías a otros sistemas y se auto reproduce a si mismo creando varias copias y dañando, modificando e incluso eliminar la información en la memoria, casi la mayoría de las veces sin que el usuario se de cuenta hasta que sea demasiado tarde, cuando los archivos ya están borrados hasta que el computador quede inoperante por el ataque.

El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa

del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo", menos comunes son los no-residentes que no permanecen en la memoria después que el programa-huésped es cerrado.

4.17 Zonas Desmilitarizadas (DMZ) y Zonas Militarizadas (ZM)

Una DMZ (del inglés Demilitarized zone) es una red o parte de una red, separada de otros sistemas por un cortafuegos, que permite que sólo entren o salgan ciertos tipos de tráfico de red.

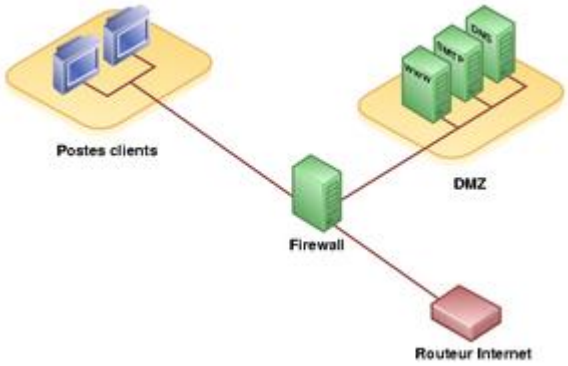
La correcta colocación de los servidores de red es un factor crítico en términos de seguridad. Para crear un acceso al público se puede configurar un firewall de modo que sólo habilite el tráfico que responda a un segmento interno; esto le confiere a la red un grado elevado de protección y es apropiado para usuarios que desean navegar la Web. Sin embargo, para acceder a información interna se deben crear niveles de acceso, que los hackers aprovechan para monitorear el servidor y detectar puntos vulnerables. Si el servidor que reside en la red interna es violado, es posible penetrar el firewall y dejar abierta la puerta para ataques a otros servidores internos.

Para evitar esta situación, se recomienda colocar el servidor público en una "Zona Desmilitarizada", como por ejemplo, una red que se localice entre el enrutador externo (que se encarga de filtrar) y el firewall. Como alternativa, una DMZ puede ser una

interfaz, adicional al firewall, que protege al servidor pero que, en caso de accesos no autorizados, incluye una red aislada.

Definiciones

Una DMZ es una red adicionada entre una red protegida y una red externa con el fin de proveer un nivel de seguridad adicional



Nombre: Estructura DMZ

Fuente: Wikipedia

Elaborado: JHON MOLINA

Figura: 10 Estructura DMZ[9]

En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la

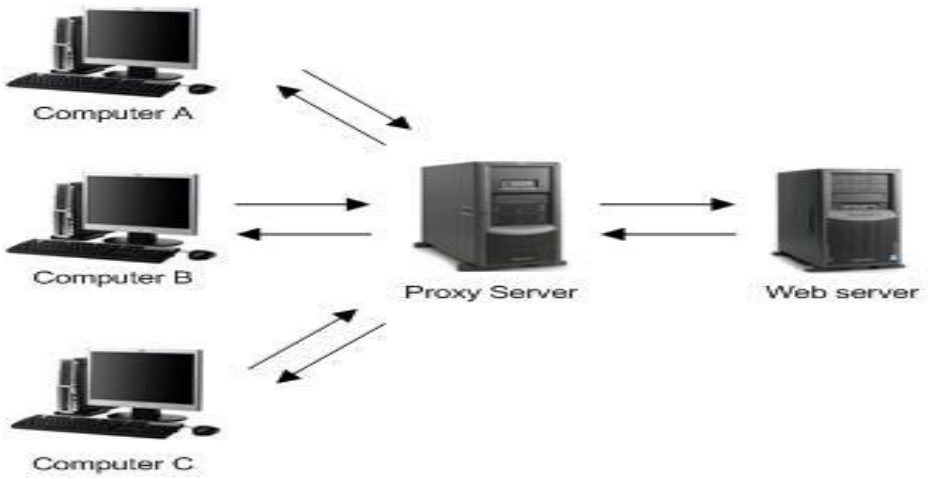
[9] http://es.wikipedia.org/wiki/Zona_desmilitarizada_%28inform%C3%A1tica%29

DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

Por lo general la DMZ se utiliza para ofrecer servicios que necesitan ser accedidos desde el exterior, como ser servidores de e-mail, servidores Web, FTP o DNS.

4.18 Proxy Squid

Un proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina *a* solicita un recurso a una *c*, lo hará mediante una petición a *b*; *C* entonces no sabrá que la petición procedió originalmente de *a*. Su finalidad más habitual es la de servidor proxy, que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.



Nombre: Proxy

Fuente: Wikipedia

Elaborado: JHON MOLINA

Figura: 11 Proxy[10]

- **Proxy de web / Proxy cache de web**

  Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

- **Funcionamiento**

[10] http://linamarcela21.blogspot.com/2011/02/proxy-server.html

1. El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.

- **Ventajas**

  - **Ahorro de Tráfico**: las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
  - **Velocidad en Tiempo de respuesta**: el servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.
  - **Demanda a Usuarios**: puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
  - **Filtrado de contenidos**: el servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.

- **Modificación de contenidos**: basándose en la misma función del filtrado, y llamado Privoxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

- **Desventajas**

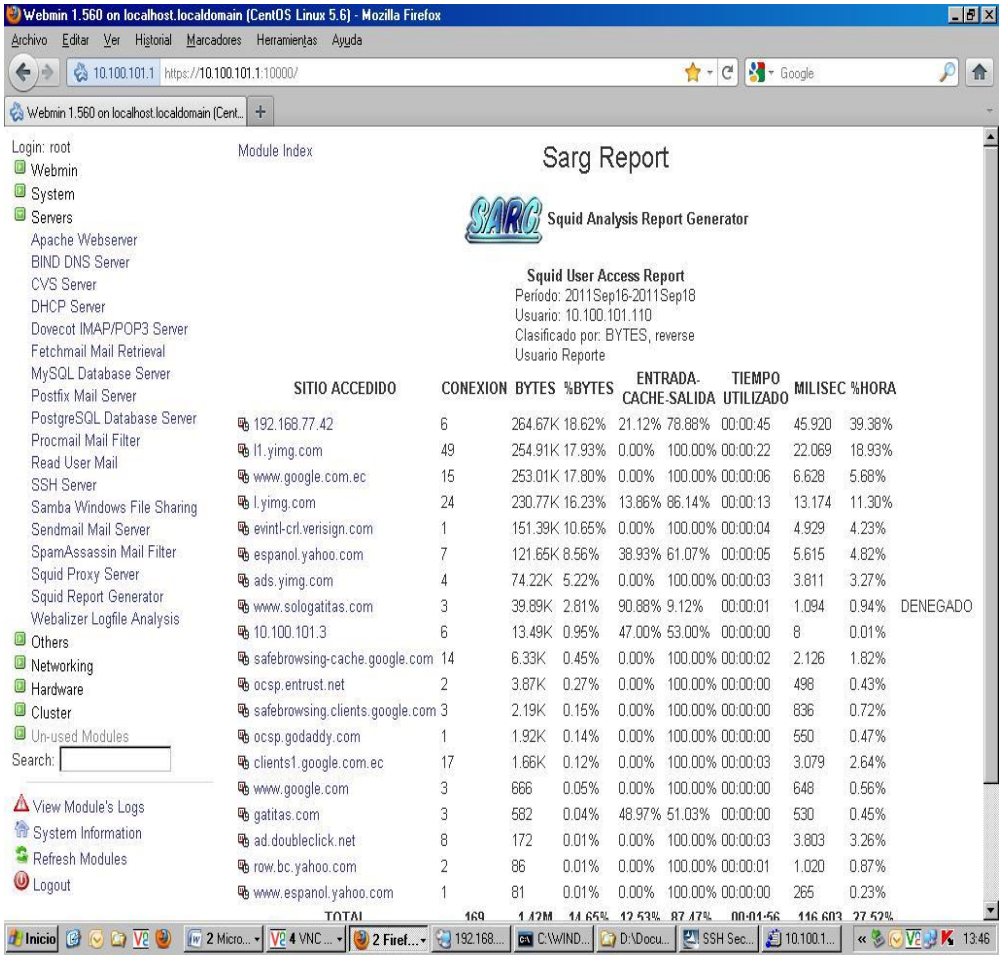
  - Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.
  - Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.

  - El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.

  - Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

4.18.1 Squid Analysis Report Generator (SARG)

Sarg es un programa para ver los informes de uso del Squid de una red. En palabras de su programador: Sarg es un Squid Analysis Report Generator que te permite ver "dónde" están yendo tus usuarios dentro de Internet. Sarg genera informes en html, con muchos campos, como: usuarios, Direcciones IP, bytes transmitidos, sitios web and tiempos.



Nombre: SARG

Fuente: Webmin

Elaborado: JHON MOLINA

Figura 12 (SARG)

4.19 DNS

Domain Name System o DNS (en castellano: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

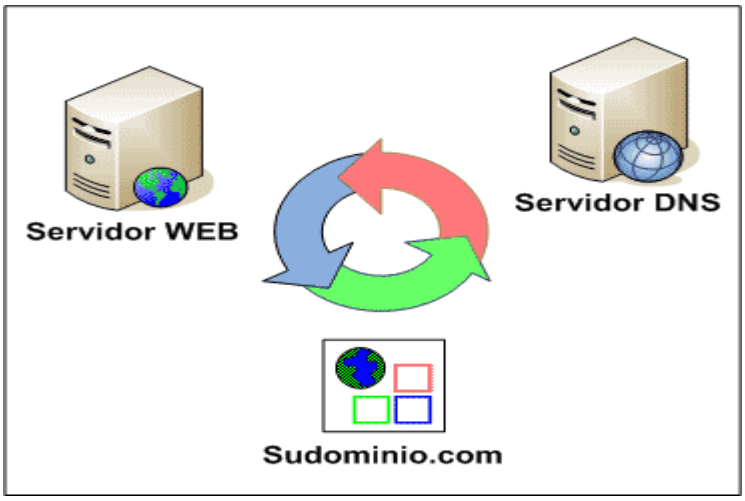
El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Para cada dominio de la organización deberán realizarse búsquedas en el servicio DNS, prestando especial atención a:

- Servidores de Nombres (NS)
- Intercambiadores de correo (MX)
- Nombres conocidos (ej. www, ftp)

Estos nombres, corresponderán a servidores susceptibles de ser atacados y por tanto deberán ser objeto de un cuidadoso proceso de fortalecido.



Nombre: DNS

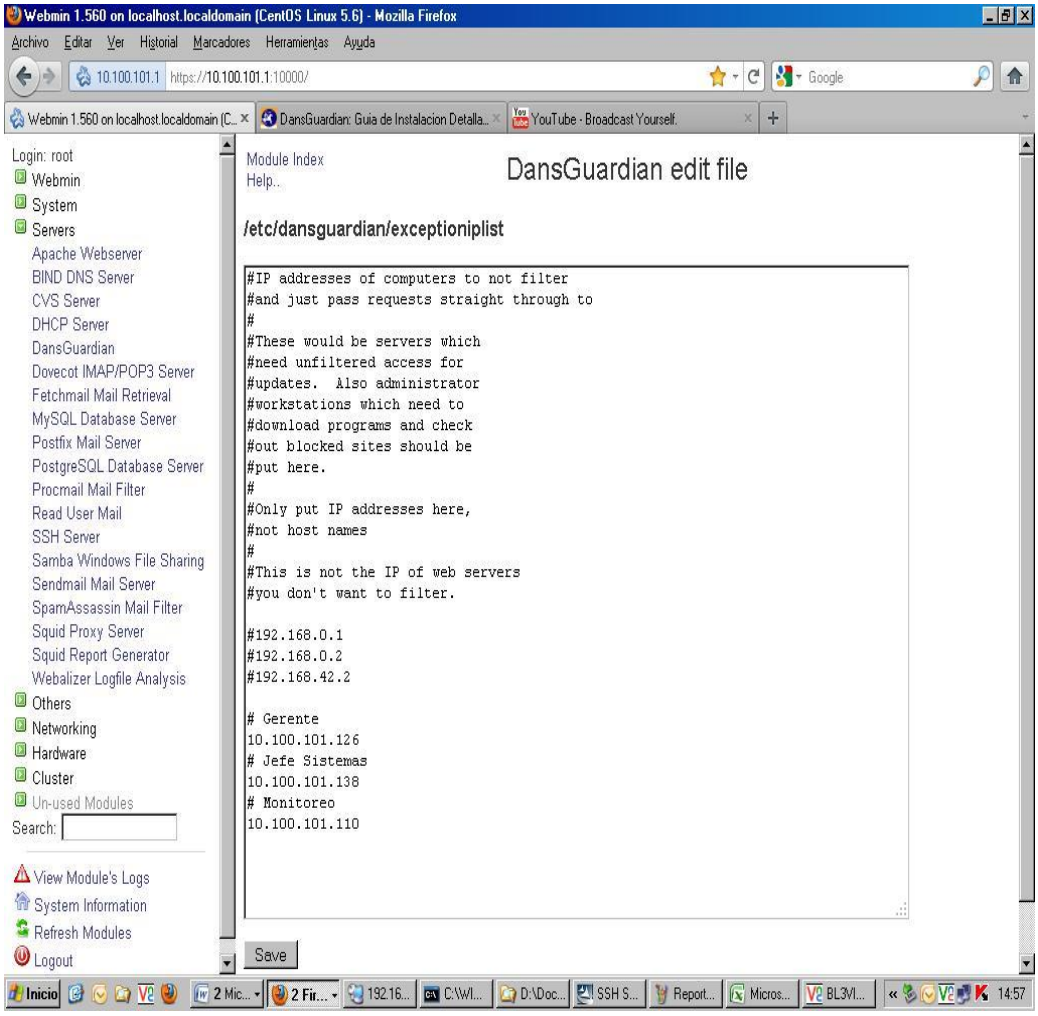
Fuente: Google imágenes

Elaborado: JHON MOLINA

Figura: 13 DNS

4.20 Control de Contenido DAMS GUARDIAN

DansGuardian es un filtro directo que se ubica entre el cliente Web (web browser) y el Servidor Proxy Squid. Dansguardian acepta conexiones en el puerto 8080 y se conecta a squid en el puerto 3128. Por lo tanto, es importante que no haya otro servicio utilizando el puerto 8080. Se da acceso total a 3 usuarios como indica el grafico.



Nombre: DansGuardian

Fuente: Webmin

Elaborado: JHON MOLINA

Figura: 14 DansGuardian

4.21 PLAN DE PRUEBAS

Introducción

Este documento contiene las especificaciones para cumplir las pruebas de funcionalidad y manejo de las herramientas configuradas bajo Linux.

4.21.1 Objetivo y Alcance

Las enumeraciones de prueba de la administración y optimización de los recursos para el proyecto verificaran que la funcionalidad de cada configuración satisfaga los requerimientos de Coonecta.

4.21.2 Estrategia

El encomendado de realizar las pruebas preparará las descripciones y ejecutará las pruebas. La especificación de requerimientos será la base para iniciar la evaluación de cada módulo configurado, combinando con el escenario lógico que corresponde a la secuencia de los procesos requeridos.

4.21.3 Organización del Documento

Este documento define el plan para conducir las pruebas de acuerdo con las especificaciones de la Prueba en las áreas siguientes:

• Objetivos: identifica las categorías de las pruebas que van a ser incluidas o excluidas desde la Especificación de Prueba.

• Las responsabilidades: identifica los recursos disponibles.

• Los procedimientos: describe los procedimientos a seguir en la preparación, desarrollo y verificación de los resultados de la prueba.

• Supuestos: documenta los supuestos hechos en la preparación de la especificación de la prueba.

• Los apéndices: contienen una secuencia de los escenarios de prueba, y una muestra de los documentos que resultan de las pruebas definidas.

4.21.4 Definición General de las Pruebas

Las especificaciones para las pruebas de administración y optimización proveerán una metodología formal para las pruebas de cada configuración. Al identificar los tipos de prueba necesarios para esta aplicación, colocando un (X) en (Si) o (No), si se va a ejecutar o no ese Tipo de prueba (esto si el Tipo de prueba aplica para el proyecto), o (N.A). Si la prueba no aplica para el proyecto.

Probar			Tipo de prueba	Descripción del Prueba	Duración
Si	No	NA			
X			Procesos e Interface de Usuario	Procesamiento Lógico en el servidor: actualización de la configuración, modificaciones y que las configuraciones satisfagan lo descrito en el documento de especificaciones funcionales.	
X			Interface con otras redes.	Respuesta a peticiones de páginas web por las redes remotas	
X			Volumen	Simulación de volúmenes para peticiones de páginas web esperados en ambiente de producción.	
X			Concurrencia	Usuarios simultáneos accediendo a Internet.	
	X		Recuperación	Procedimientos de Backup y recuperación de la configuración.	
X			Seguridad	Especificaciones de Seguridad de acuerdo con las especificaciones	

FUENTE: Propia

Tabla N°11: Tipos de Prueba

4.21.5 Recursos de Hardware o Software.

La siguiente sección define los recursos necesarios, personas, hardware o software.

4.21.6 Responsable del Equipo de Pruebas

El equipo de pruebas es:

Nombre	Tipo de prueba	Responsabilidad
Jhon Molina	Procesos e Interface de Usuario	Hacer uso del Internet, probando así todas las funciones del servidor.
Jhon Molina	Interfase con otras redes.	Hacer uso del Internet en puntos remotos, probando así todas las funciones del servidor con redes remotas.
Jhon Molina	Volúmen	Acceder al Internet de todas las máquinas posibles a nivel de red interna.
Jhon Molina	Concurrencia	Acceder al Internet, desde varios equipos terminales con el fin de verificar que no se bloqueen las configuraciones.

Jhon Molina	Seguridad	Verificar que todas las funciones de seguridad impuestas en la fase

FUENTE: Personal

Tabla N°12: Personal de Pruebas

4.21.7 Procedimiento para Escenario de Pruebas

El siguiente es el procedimiento para la preparación del cumplimiento de los escenarios de las pruebas:

4.21.8 Preparación de Pruebas

Múltiples casos deben ser preparados, uno por cada proceso definido en las especificaciones funcionales.

Los casos serán combinados en los escenarios. A cada escenario corresponde:

- Una o más tareas dentro del proceso.
- Secuencias Lógicas que pueden ser repetidas.
- Excepciones del proceso.

4.21.9 Ambiente de Pruebas

Para las pruebas al servidor se será integrado a la infraestructura de red existente, como dirección IP de la WAN la dirección 10.10.10.2/30 y como dirección IP de la LAN la 10.100.101.1/24.

4.21.10 Ejecución y Evaluación de Pruebas

Los escenarios de prueba serán efectuados en la secuencia enumerados en el Apéndice A.

El encargado de ejecutar un escenario de prueba, evaluará y escribirá los resultados de la prueba. La documentación de apoyo (pantallas e informes) debe conservarse para cada corrida de prueba, al igual que los registros de las pruebas efectuadas y de los problemas encontrados. Una copia del formato para el Registro y Control de estas fallas se encuentra en el Apéndice C.

Las fallas presentadas deberán ser archivadas en el Fólder del Proyecto e informadas en la reunión de control con el personal de Coonecta.

Cada falla debe calificarse de acuerdo con su gravedad y determinar si afecta la secuencia de las pruebas programadas, de acuerdo con la siguiente tabla:

Gravedad	Descripción
1	Error grave que causa la suspensión del trabajo, es un error crítico y su solución debe ser de inmediata.
2	Error medio, es posible continuar con otras pruebas, pero el error corresponde a una funcionalidad esencial. La solución a estas situaciones debe tener prioridad alta.

3	Errores leves de presentación que no afectan la operación de la aplicación.

FUENTE: Personal

Tabla N°13: Descripción gravead de errores.

Cuando la falla se soluciona la prueba debe volverse a correr y todos los escenarios relacionados

4.21.11 Supuestos

Las pruebas están basadas en los siguientes supuestos:

• El ambiente para la prueba va a estar disponible en la fecha de inicio de acuerdo con el cronograma de pruebas.

• La conexión a Internet estará disponible y será probada.

• Los documentos de referencia fueron la base para la elaboración de los casos de prueba y estarán disponibles durante la prueba.

Todos los escenarios tendrán un mecanismo de aprobación que asegure que el caso a probar cumple con los requerimientos, y de no ser así serán modificados hasta que cumplan con los requisitos.

4.21.12 Criterios de Aceptación

El proyecto será aceptado cuando todas las pruebas especificadas en el Apéndice B sean ejecutadas satisfactoriamente y:

a. Los Resultados esperados estén de acuerdo con las especificaciones funcionales.

b. Todos los problemas hayan sido corregidos y los escenarios asociados a estas fallas se hayan ejecutado satisfactoriamente

4.21.13 Apéndices

4.21.13.1 Apéndices A: Secuencias Escenarios

Orden / Sec	Escr No.	Nombre Escenario	Escenarios Previos Requeridos
1	1	Ingreso de usuarios	
2	2	Permisos de navegación.	Ingreso de Usuarios
3	3	Intento de ingreso al servidor por puertos.	Ingreso de Usuarios
4	4	Intento de ataques externos.	
5	5	Pruebas de control de contenido.	Ingreso de Usuarios

FUENTE: Personal

Tabla 8 secuencias escenarios.

4.21.13.2 Apéndices B: Escenarios de Prueba

Escenario de Prueba		
Proyecto:	Administración y Optimización del Internet en COONECTA	
Escenario:	**Ingreso de usuarios.**	**No. 1**
Módulo:	Proxy Server	
Caso de prueba:	Ingreso usuario a Internet.	
Tipo de prueba:	Interface con otras redes	**Pág.** 1
Definido por:	Jhon Molina	**Fecha Creación:** 2011-09-09
Participantes:	Jhon Molina	
Descripción de la prueba:	Ingreso al Internet con un usuario previamente definido.	

FUENTE: Personal

Tabla 9 Escenario ingreso de usuarios

Apéndices B: Escenarios de prueba

4.21.13.3 Apéndices C: Resumen de la Ejecución de las Pruebas

No.	Escr	Usuarios	Resultado	Fecha	Grav
1	1	Jhon Molina	La prueba de ingreso de usuarios registrados, brindó resultados satisfactorios en cuanto a validación y registro de usuarios en redes remotas.	2011-09-18	Ninguna

FUENTE: Personal

Tabla: 10 Resumen de ejecución de las pruebas

4.21.13.4 Apéndices D: Resultados de las Pruebas

Requisitos		
Procedimiento	**Descripción**	**Ok**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales	Usuarios, personal registrado en el servidor.	Ok
Ambiente Técnico Previo Requerido:	PC Pentium Core 2 Duo à 1Gb RAM Windows XP Internet Explorer 9.x o superior Firefox 3.5	Ok
Comentarios: Las pruebas serán realizadas desde un computador con el navegador Firefox 3.5. La máquina de pruebas estará conectada a la red de Coonecta		
Secuencia de la Prueba		
Procedimientos	**Descripción**	**Ok**
Ingresar al Internet agregando usuario y contraseña.	Ingresar a página principal www.coonecta.com.ec	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Comentarios de la prueba:		

La prueba de ingreso de un usuario registrado, brindo resultados satisfactorios en cuanto a validación y registro del navegador.
Nombre Ejecutor de la Prueba: Jhon Molina _____ Firma Ejecutor de la Prueba

FUENTE: Personal

Tabla: 11 Resultados del Escenario

CAPITULO V

5. Impactos Esperados del Proyecto

Entre los impactos que deseamos generar en este proyecto hay varios ámbitos, pero en general lo que se busca es mejorar la situación de la empresa en el área operativa, de seguridad, de eficiencia, en la optimización de recursos tanto tecnológicos, económicos como los de la fuerza de trabajo, para que los usuarios no tengan que preocuparse de aspectos técnicos y se enfoquen únicamente a satisfacer las necesidades de sus clientes.

5.1 Científico

Dentro de los beneficios que producirá el proyecto está la documentación de apoyo que recibirán tanto profesores como alumnos los cuales se podrán basarse en esta para futuros proyectos. Igualmente se lleva a la práctica muchos de los conocimientos que a lo largo de los años he adquirido en esta institución, más el valor agregado de la experiencia en un caso real donde se puede ampliar el conocimiento de diversos temas que en el desarrollo del proyecto van apareciendo.

5.2 Educativo

En el aspecto educativo esta experiencia complementa los aspectos teóricos que se adquiere al estudiar. Las dudas que van surgiendo dentro del proyecto y que mediante

investigación se van aclarando se pueden convertir en la retroalimentación que necesita el maestro por parte del alumno para ampliar y mejorar la calidad de la enseñanza, a la par, el alumno puede recibir el estímulo que necesita para encontrar el área de especialización de su carrera.

5.3 Técnico

En este aspecto se conocieron diversas herramientas para el desarrollo del proyecto básicamente fueron herramientas de código abierto, dentro de las principales características de éstas son la versatilidad, el potencial uso del código fuente para mejorar tareas, el software libre también permite en ciertos casos ahorrar el costo de las licencias, la seguridad que nos brinda.

Dentro de las herramientas se usó como sistema base Linux Centos 5.6 32 bits, de acuerdo a las necesidades de la empresa se utilizó:

Firewall → Cortafuegos (Iptables)
Proxy → Squid

Reportes de navegación →SARG

Monitoreo de Red → Iptraf

5.4 Tecnológico

En la actualidad y dado el tremendo grado de intercomunicación e interoperatividad de las computadoras es necesario la aplicación de políticas de seguridad tanto de los usuarios que usan nuestros servicios como de los datos que se generan y comparten en

los mismos, por este motivo se debió implementar 4 fases con las cuales se pudo determinar la siguiente metodología:

FASE I Determinación de la situación actual

FASE II Determinación de necesidades

FASE III Análisis

FASE IV Pruebas e implementación

5.5 Empresarial

Los procedimientos aplicados para recoger la información necesaria se realizaron en 3 pasos:

- Observación
- Levantamiento de requerimientos
- Entrevista

Estos pasos son fundamentales para reconocer la amplitud del proyecto y los alcances que debe tener a futuro de modo que puede ampliar su campo de acción de manera acorde al crecimiento de las necesidades de la institución.

5.6 Social

Este proyecto permite en mi caso generar una matriz de conocimiento importante para la empresa donde laboro tanto en aspectos de funcionamiento interno de los procesos de la misma como por la optimización de recursos tanto económicos como logísticos y operativos.

El uso de esta tecnología genera empleo desde la instalación e implementación de los servicios, como también puede generar puestos de trabajo en el mantenimiento y administración del sistema operativo.

5.7 Económico

Dentro de la base de las relaciones existen 2 ideas fundamentales para obtener el éxito confianza y cooperación ambas se pueden resumir en el concepto del ganar/ganar en este proyecto todos resultan beneficiados, la empresa encontrará una solución a sus necesidades que le represente un ahorro de recursos, tanto económicos como logísticos, etc., igualmente el ITSCO recibe un caudal de conocimientos puestos en práctica, documentados, comprobados, que pueda complementar su programa de estudios.

Los gastos que genera el proyecto y beneficia a la empresa, son detallados en el cuadro de recursos económicos y son:

CUADRO DE RECURSOS ECÓNOMICOS			
DETALLE	**CANTIDAD**	**C / UNITARIO**	**C / TOTAL**
Estación de Trabajo	1	600	600
Impresora	1	150	150
Material de escritorio	1	130	130
Internet	1	120	120
Servicios básicos	1	50	50
Trasporte	60	1	60
Varios	1	100	100
Dólares			**1210**

Fuente: Personal

Tabla: 12 Recursos económicos

5.8 CONCLUSIONES

1. Se investigo diferentes herramientas de software libre como DansGuardian, que nos ayudo con el control de contenido, con el cual se pudo llegar al objetivo general.

2. La teoría es punto de partida esencial para el desarrollo de la tesis, pero en el momento de la práctica no tiene validez universal, ya que se debe adaptar esa teoría al ambiente en el cual se esté trabajando.

3. El uso de un sistema operativo como Linux permite tener una extensa flexibilidad en las diferentes configuraciones ya que los paquetes utilizados pueden correr bajo cualquier versión de Kernel, esto universaliza la funcionalidad de las configuraciones en cualquier sistema Linux.

4. El uso de un sistema ya programado como Linux facilita la intervención del administrador de la red, mucho más, si este no tiene experiencia en sistemas Linux; sin embargo, en el proceso inicial de configuración se dificultó el hecho de unificar los parámetros con el formato de reportes y configuración simple ya establecidos por Linux.

5. Siempre es necesario utilizar tecnología de punta para salvaguardar la seguridad de la información y proteger de posibles ataques de piratas de la información es muy importante proteger la Zona Desmilitarizada (DMZ) en donde se encuentran los servidores y evitar cualquier daño en los equipos informáticos.

5.9 RECOMENDACIONES

1. Realizar una investigación de campo detallada para saber la factibilidad en el uso de algunas tecnologías y requerimientos específicos del sistema de control.

2. Se debe recopilar una base de datos de los ataques recibidos y del uso del Internet en la institución para tener un reporte histórico, el cual servirá a futuro para analizar el comportamiento del usuario, y sobre todo tener el histórico de los ataques que han tratado de hacer y transformarlos en tablas de prevención de intrusos.

3. Cuando se trabaja dentro de un sistema de alta seguridad se recomienda tomar en cuenta como están configurados los módulos, y la comunicación entre estos.

4. Monitorear continuamente las comunicaciones en los puntos remotos de la red WAN para comprobar que siempre esté activo el enrutamiento hacia la matriz donde se encuentra la conexión global de Internet.

5. Adquirir la alternativa de solución 1 de telconet es muy importante y debe tomarse en cuenta para su implementación ya que garantizara mayor seguridad de la información de Coonecta y ayudara a la separación de los servidores y de la red interna protegiendo la Zona Desmilitarizada (DMZ) y ayudara a la integridad de los servidores.

CAPÍTULO VI

6.1 Bibliografía

- **Autor:** Klimovsky Gregorio (1997) Las desventuras del conocimiento científico. Una introducción a la epistemología, A-Z editora Bs.As. Páginas: 950-534-275-6.

- **Autor:** Murhammer, Martín W; Bourne, Tim A.; GAIDOSH, (1998) A guide to virtual private networks. Configuración de Redes LAN. Primera edición.

- **Autor:** Tamayo y Tamayo Mario, El Proceso de la Investigación, Editorial: Limusa Noriega Editores, Número de Edición: Tercera Edición

- **Autor:** ARMSTRONG, Bruce; BROWN, Julio 25, 2002, Obra: Linux clustering, Editorial: USA. SAMS, Número de Edición: Primera Edición

6.2 Netgrafía

Tema: Firewall

Subtema: Principios básicos Firewall
Dirección: http://www.desarrolloweb.com/articulos/513.php

Tema: Que es un servidor.

Subtema: Definición de un servidor
Dirección: http://www.masadelante.com/faqs/servidor

Tema: Proxy Cache

Subtema: Squid
Dirección: http://www.bulma.net/body.phtml?nIdNoticia=441

Tema: Niveles de acceso a usuarios

Subtema: Tipos de usuarios

Dirección: http://www.linuxtotal.com.mx/index.php?cont=info_admon_008

Tema: código abierto
Subtema: Código abierto

Dirección: http://es.wikipedia.org/wiki/C%C3%B3digo_abierto

Tema: Implantación de QoS en un entorno Linux.

Subtema: QoS Linux

Dirección: http://usuarios.lycos.es/ccd_illusions/QoS-3.pdf

Tema: Dhcp en Centos Linux

Subtema: Como se instala

Dirección: http://syswarp.wordpress.com/2008/10/18/como-instalar-un-servidor-dhcp-en-centos-linux/

Tema: Instalación modo grafico CentOS

Subtema: Instalación Linux CentOS

Dirección:http://www.linuxparatodos.net/portal/staticpages/index.php?page=instalacion-grafico-centos

ANEXO 1

Cuadro de recursos humanos

Anexo Nº1 (Cuadro de Recursos Humanos)

CUADRO DE RECURSOS HUMANOS		
NOMBRE	**FUNCIÓN**	**RESPONSABILIDAD**
Jhon Molina	Investigador	Desarrollo del Proyecto
Ing. Jaime Padilla	Profesor	Tutor del Proyecto
Ing. Robert Enríquez	Director de Escuela	Aprobación del Plan
Ing. José Luis Rodríguez	Coordinador	Coordinador del Proyecto

ANEXO 2

Cuadro de Recursos Económicos

Anexo Nº2 (Cuadro de Recursos Económicos)

CUADRO DE RECURSOS ECONÓMICOS			
DETALLE	**CANTIDAD**	**C / UNITARIO**	**C / TOTAL**
Estación de Trabajo	1	800	800
Impresora	1	150	150
Material de escritorio	1	130	130
Internet	1	120	120
Servicios básicos	1	50	50
Trasporte	60	1	60
Varios	1	100	100
Dólares			**1410**

ANEXO 3

Legalización de la empresa

Anexo Nº 3 (RUC)

ANEXO 4

Cronograma de Actividades

Anexo Nº4 (Cronograma de Actividades)

ANEXO 5

GLOSARIO DE SIGLAS

Anexo Nº 5

ASN: Autonomous System Number

BSD: Berkeley Software Distribution

CPU: Central Processing Uni

DLL: Dynamic Link Library

FTP: File transfer protocol

FPU: Floating Point Unit

FAT32: File Allocation Table 32

GNU: General Public License

HPFS: High Performance File System

IAB: Internet Architecture Board

IP: Internet Protocol

ISO: International Organization for Standardization

LSB: Linux Standard Base

Minix: Unix Clone

NAT: Network Address Translation

NTFS: NT File System

POSIX: Portable Operating System Interface para UNIX

RFC: Request For Comments

SCO: Unix system intellectual property

SVR: Advanced Compatibility Package

STD: Security Tool Distro

TCP: Transmission Control Protocol

ANEXO 6

Instituto Tecnológico Superior Cordillera

Manual técnico

Servidor Centos 5.6

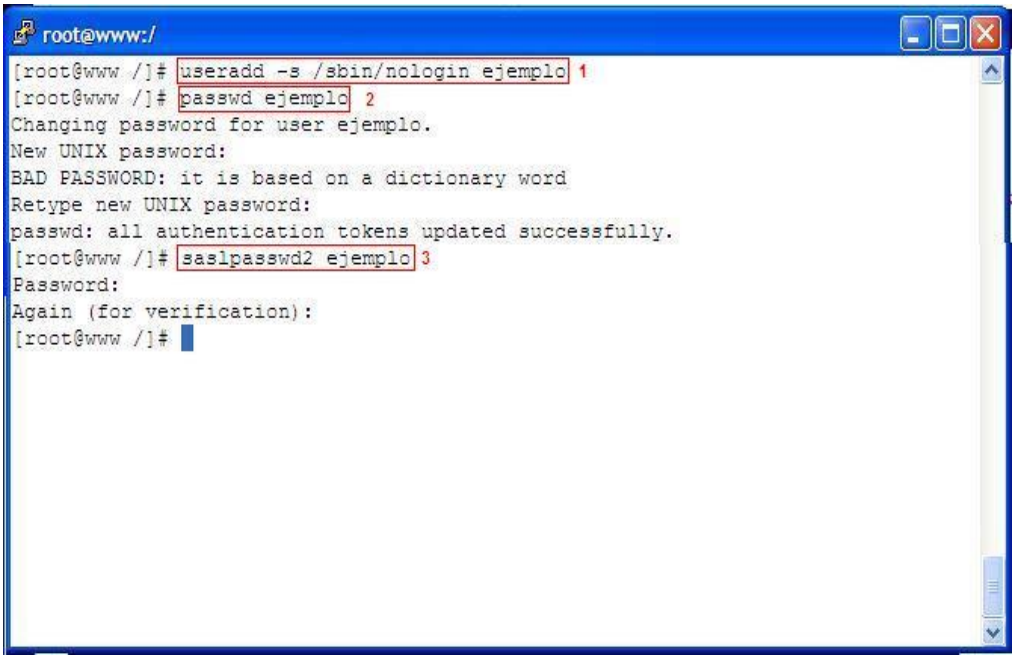
Anexo Nº 6

El presente manual contiene las instrucciones para realizar varias tareas en el servidor Centos desde la consola.

Creación de Usuarios.

Para crear usuarios hay que ejecutar las siguientes órdenes.

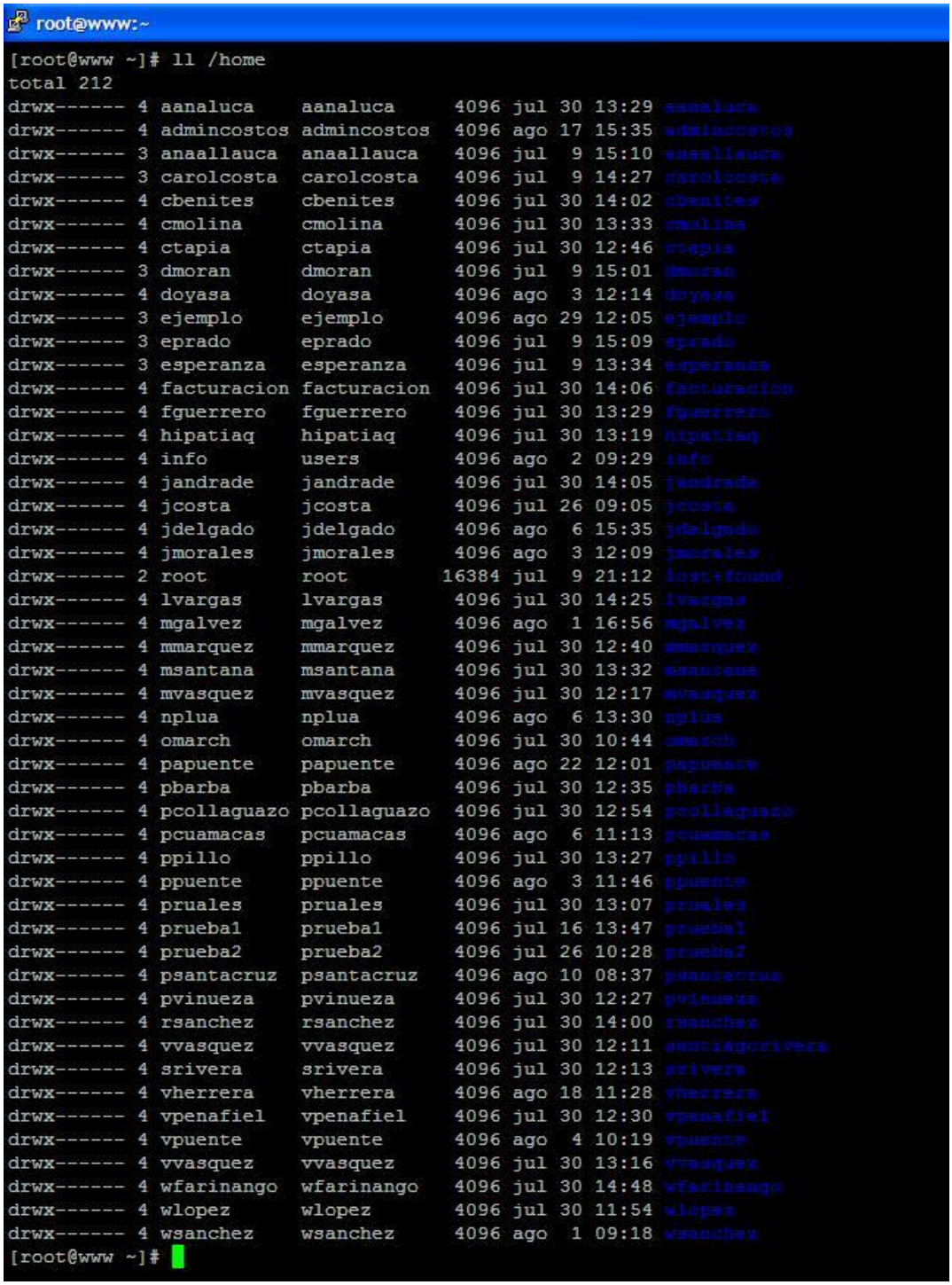
1. useradd –s /sbin/nologin *usuario*
2. passwd usuario
3. saslpasswd2 usuario



Es muy importante recordar que Linux reconoce mayúsculas y minúsculas de manera diferente que Windows, por lo tanto los siguientes usuarios serían diferentes: juanjose Juanjose JuanJose. Igualmente por motivos de seguridad Linux no permite visualizar el cursor al ingresar las contraseñas.

Al crear el usuario del ejemplo que está en el gráfico anterior este ya está habilitado para recibir correo electrónico de la dirección corporativa en este caso la dirección sería ejemplo@coonecta.com.ec

Las carpetas donde se almacenan los datos de los usuarios se ubican en: **/home**


root@www:~
[root@www ~]# ll /home
total 212
drwx------ 4 aanaluca aanaluca 4096 jul 30 13:29 aanaluca
drwx------ 4 admincostos admincostos 4096 ago 17 15:35 admincostos
drwx------ 3 anaallauca anaallauca 4096 jul 9 15:10 anaallauca
drwx------ 3 carolcosta carolcosta 4096 jul 9 14:27 carolcosta
drwx------ 4 cbenites cbenites 4096 jul 30 14:02 cbenites
drwx------ 4 cmolina cmolina 4096 jul 30 13:33 cmolina
drwx------ 4 ctapia ctapia 4096 jul 30 12:46 ctapia
drwx------ 3 dmoran dmoran 4096 jul 9 15:01 dmoran
drwx------ 4 doyasa doyasa 4096 ago 3 12:14 doyasa
drwx------ 3 ejemplo ejemplo 4096 ago 29 12:05 ejemplo
drwx------ 3 eprado eprado 4096 jul 9 15:09 eprado
drwx------ 3 esperanza esperanza 4096 jul 9 13:34 esperanza
drwx------ 4 facturacion facturacion 4096 jul 30 14:06 facturacion
drwx------ 4 fguerrero fguerrero 4096 jul 30 13:29 fguerrero
drwx------ 4 hipatiaq hipatiaq 4096 jul 30 13:19 hipatiaq
drwx------ 4 info users 4096 ago 2 09:29 info
drwx------ 4 jandrade jandrade 4096 jul 30 14:05 jandrade
drwx------ 4 jcosta jcosta 4096 jul 26 09:05 jcosta
drwx------ 4 jdelgado jdelgado 4096 ago 6 15:35 jdelgado
drwx------ 4 jmorales jmorales 4096 ago 3 12:09 jmorales
drwx------ 2 root root 16384 jul 9 21:12 lost+found
drwx------ 4 lvargas lvargas 4096 jul 30 14:25 lvargas
drwx------ 4 mgalvez mgalvez 4096 ago 1 16:56 mgalvez
drwx------ 4 mmarquez mmarquez 4096 jul 30 12:40 mmarquez
drwx------ 4 msantana msantana 4096 jul 30 13:32 msantana
drwx------ 4 mvasquez mvasquez 4096 jul 30 12:17 mvasquez
drwx------ 4 nplua nplua 4096 ago 6 13:30 nplua
drwx------ 4 omarch omarch 4096 jul 30 10:44 omarch
drwx------ 4 papuente papuente 4096 ago 22 12:01 papuente
drwx------ 4 pbarba pbarba 4096 jul 30 12:35 pbarba
drwx------ 4 pcollaguazo pcollaguazo 4096 jul 30 12:54 pcollaguazo
drwx------ 4 pcuamacas pcuamacas 4096 ago 6 11:13 pcuamacas
drwx------ 4 ppillo ppillo 4096 jul 30 13:27 ppillo
drwx------ 4 ppuente ppuente 4096 ago 3 11:46 ppuente
drwx------ 4 pruales pruales 4096 jul 30 13:07 pruales
drwx------ 4 prueba1 prueba1 4096 jul 16 13:47 prueba1
drwx------ 4 prueba2 prueba2 4096 jul 26 10:28 prueba2
drwx------ 4 psantacruz psantacruz 4096 ago 10 08:37 psantacruz
drwx------ 4 pvinueza pvinueza 4096 jul 30 12:27 pvinueza
drwx------ 4 rsanchez rsanchez 4096 jul 30 14:00 rsanchez
drwx------ 4 vvasquez vvasquez 4096 jul 30 12:11 vanessagorivera
drwx------ 4 srivera srivera 4096 jul 30 12:13 srivera
drwx------ 4 vherrera vherrera 4096 ago 18 11:28 vherrera
drwx------ 4 vpenafiel vpenafiel 4096 jul 30 12:30 vpenafiel
drwx------ 4 vpuente vpuente 4096 ago 4 10:19 vpuente
drwx------ 4 vvasquez vvasquez 4096 jul 30 13:16 vvasquez
drwx------ 4 wfarinango wfarinango 4096 jul 30 14:48 wfarinango
drwx------ 4 wlopez wlopez 4096 jul 30 11:54 wlopez
drwx------ 4 wsanchez wsanchez 4096 ago 1 09:18 wsanchez
[root@www ~]#

Es muy importante por seguridad que los permisos de las carpetas se mantengan como están en el siguiente gráfico:

```
drwx------ 4 aanaluca
```

Servidor Squid SARG

El funcionamiento del servicio Squid (Proxy) en el caso que se requiera filtrar usuarios para el uso de Internet requiere de la dirección MAC de la máquina, con esa información se edita el archivo **/etc/dhcpd.conf** en el cual se le asigna una dirección IP.

La configuración debe respetar la estructura del archivo como se observa en el siguiente gráfico:

Acceso o restricción de Usuarios al Internet.

Luego de registrar al usuario en el servidor Squid hay que usar la dirección IP que se le asignó y escribirla al editar los archivos ubicados en la dirección /etc/squid/

En los requerimientos del servidor se necesitaban 3 tipos de usuarios y sus archivos correspondientes son.

1.) Acceso Total → total

2.) Acceso con restricciones → restringido

3.) Sin Acceso → sininter

Solamente ingresando la dirección IP al archivo del grupo correspondiente y reiniciando el servicio es suficiente para que funcione el servicio correctamente.

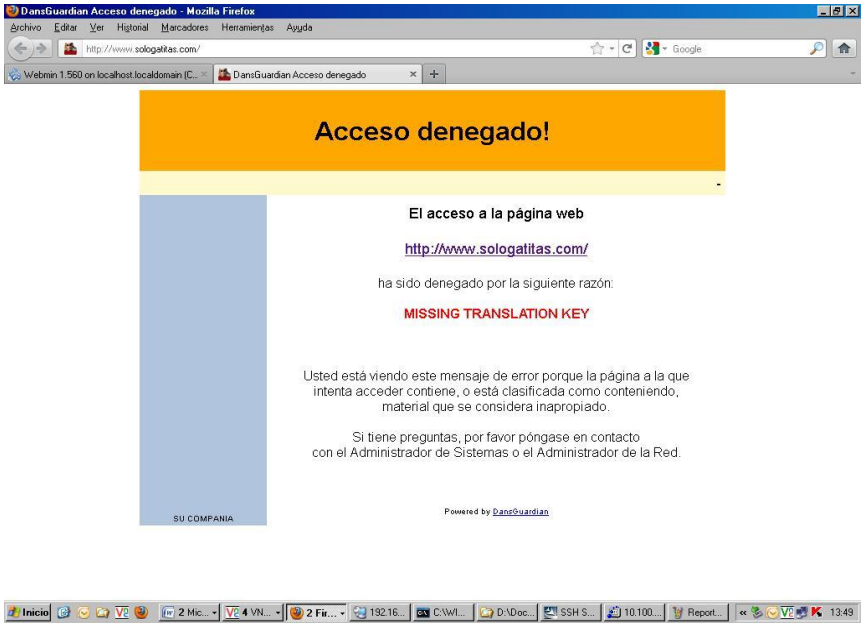
Nota.- *Para que cualquier modificación surta efecto en el servidor Squid hay que ejecutar el siguiente comando:* service squid reload

Bloqueo de páginas a los usuarios con Acceso Restringido.

El grupo más extenso de usuarios es el #2 este grupo tiene bloqueadas algunas páginas web como son redes sociales, pornografía, etc.

Si se desea modificar dichas reglas de navegación solamente hay que editar el archivo /etc/squid/porno se ingresa la palabra clave o página web se reinicia el servicio y entra en funcionamiento.

Para que cualquier modificación surta efecto en el servidor Squid hay que ejecutar el siguiente comando: service squid reload

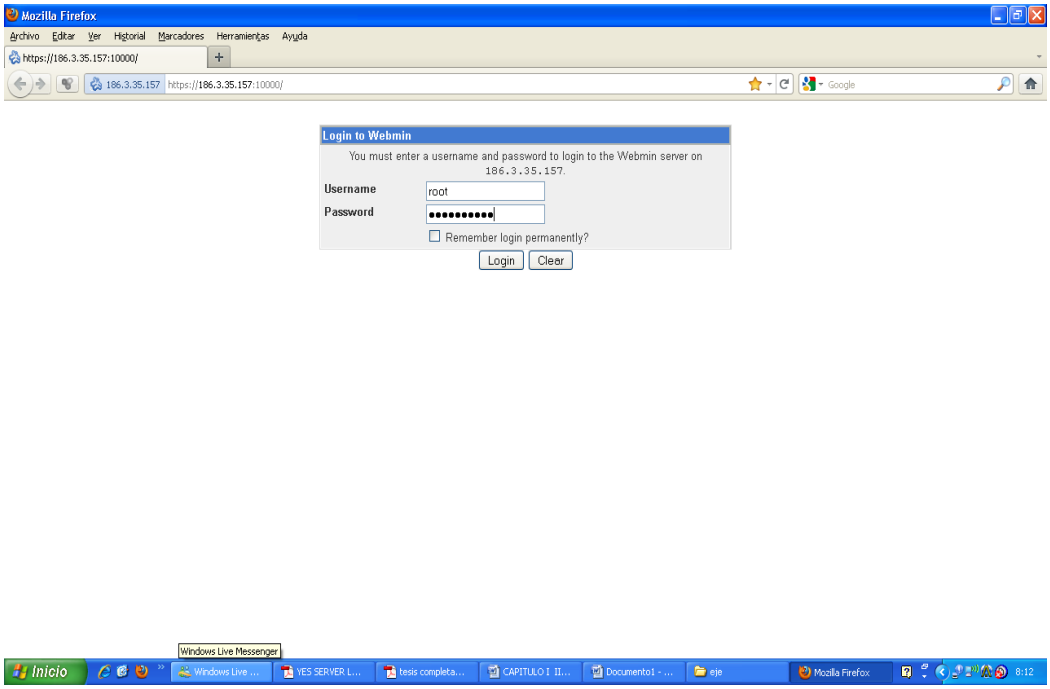


Administración Remota.

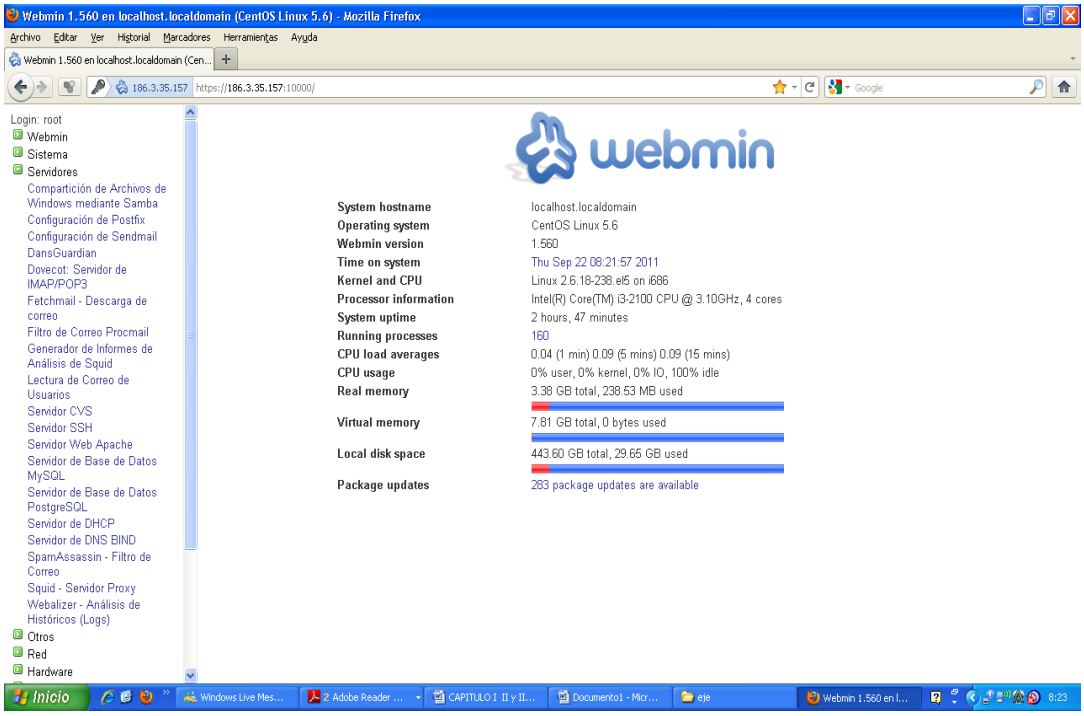
El sistema también contempla la administración remota del mismo tanto de manera gráfica como por consola vía Internet:

Para acceder hay que ingresar a la dirección que se observa en el siguiente gráfico:

https://186.3.35.157:10000/



Igualmente el usuario root con la clave ++++++++++ con 10 dígitos alifa numéricos pueden ingresar a vía Web mail con la siguiente opción:


Webmin 1.560 en localhost.localdomain (CentOS Linux 5.6) - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Webmin 1.560 en localhost.localdomain (Cen...
186.3.35.157 https://186.3.35.157:10000/
Google
Login: root
Webmin
Sistema
Servidores
Compartición de Archivos de Windows mediante Samba
Configuración de Postfix
Configuración de Sendmail
DansGuardian
Dovecot: Servidor de IMAP/POP3
Fetchmail - Descarga de correo
Filtro de Correo Procmail
Generador de Informes de Análisis de Squid
Lectura de Correo de Usuarios
Servidor CVS
Servidor SSH
Servidor Web Apache
Servidor de Base de Datos MySQL
Servidor de Base de Datos PostgreSQL
Servidor de DHCP
Servidor de DNS BIND
SpamAssassin - Filtro de Correo
Squid - Servidor Proxy
Webalizer - Análisis de Históricos (Logs)
Otros
Red
Hardware
webmin
System hostname localhost.localdomain
Operating system CentOS Linux 5.6
Webmin version 1.560
Time on system Thu Sep 22 08:21:57 2011
Kernel and CPU Linux 2.6.18-238.el5 on i686
Processor information Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz, 4 cores
System uptime 2 hours, 47 minutes
Running processes 160
CPU load averages 0.04 (1 min) 0.09 (5 mins) 0.09 (15 mins)
CPU usage 0% user, 0% kernel, 0% IO, 100% idle
Real memory 3.38 GB total, 238.53 MB used
Virtual memory 7.81 GB total, 0 bytes used
Local disk space 443.60 GB total, 29.65 GB used
Package updates 283 package updates are available
Inicio
Windows Live Mes...
2 Adobe Reader ...
CAPITULO I II y II...
Documento1 - Micr...
eje
Webmin 1.560 en l...
8:23

ANEXO 7

Instituto Tecnológico Superior Cordillera

MANUAL DE INSTALACIÓN CentOS 5.6

Anexo Nº 7

Requisitos

Para la instalación del sistema operativo necesario los siguientes requisitos:

- Un equipo servidor con un CPU Dual-Core con 1 GB en RAM y 200Gb de Disco duro.

- Dos tarjetas de red 10/100.

Obtención de los medios.

Descargue la imagen ISO del DVD de CentOS 6, para arquitectura i386, o bien arquitectura x86-64 (solo es necesario el DVD 1, salvo que requiera soporte para algún idioma exótico), desde algunos de los sitios espejo que encontrará en el siguiente URL:

- http://www.alcancelibre.org/staticpages/index.php/como-centos5-grafico

Si descarga la imagen para arquitectura i386, grabe ésta en un disco virgen DVD-R (capacidad de 4,707,319,808 bytes). La imagen de DVD para i386 (4,705,456,128 bytes) es demasiado grande para poder ser grabada en un DVD+R (capacidad de 4,700,372,992 bytes). Las imágenes de los dos DVD para arquitectura x86-64, 4,238,800,896 bytes, y 1,182,699,520 bytes, respectivamente, caben perfectamente en discos DVD+R y DVD-R.

Pasos para la instalación

Instalación del sistema operativo.

Inserte el **disco DVD** de instalación de **CentOS 5.6**, espere 60 segundos para el inicio automático, o bien pulse la tecla **ENTER**, o bien pulse la tecla para ingrese las opciones de instalación deseadas.

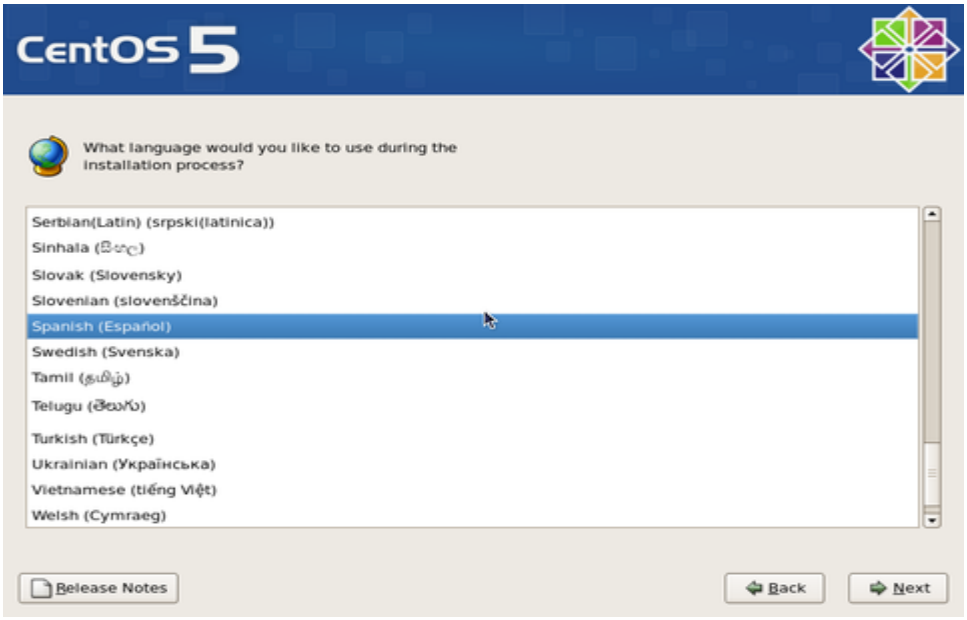
Inserte el **disco DVD** de instalación de **CentOS 5** y en cuanto aparezca el diálogo de inicio (boot:), pulse la tecla **ENTER** o bien ingrese las opciones de instalación deseadas.

Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla **ENTER**, considere que esto puede demorar varios

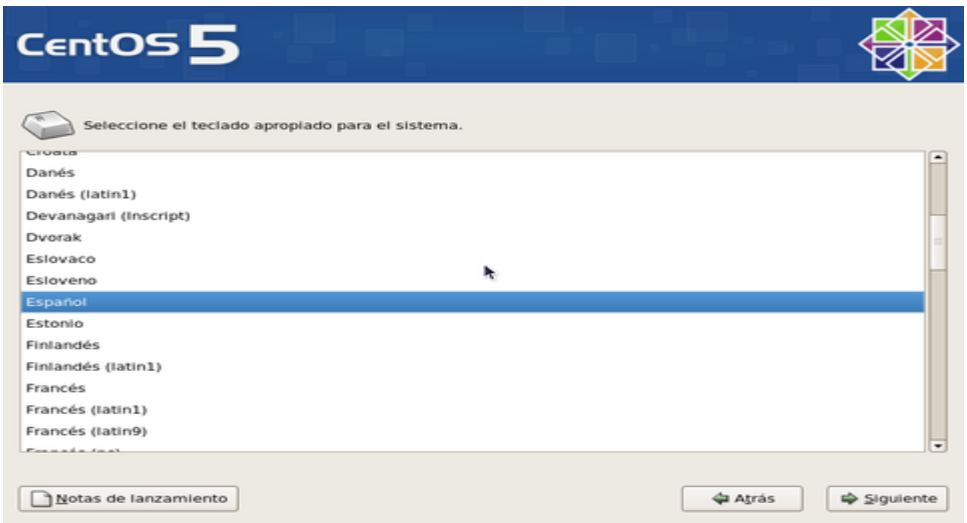
minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione **«Skip»** y pulse la tecla **ENTER**.

Haga clic sobre el botón **«Next»** en cuanto aparezca la pantalla de bienvenida de CentOS.

Seleccione **«Spanish»** como idioma para ser utilizado durante la instalación.



Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«Español»** o bien **«Latinoamericano»** de acuerdo a lo que corresponda. Al terminar, haga clic sobre el botón **«Siguiente»**.



Salvo que exista una instalación previa que se desee actualizar (no recomendado), deje seleccionado **«Instalar CentOS»** y haga clic en el botón **«Siguiente»** a fin de realizar una instalación nueva.

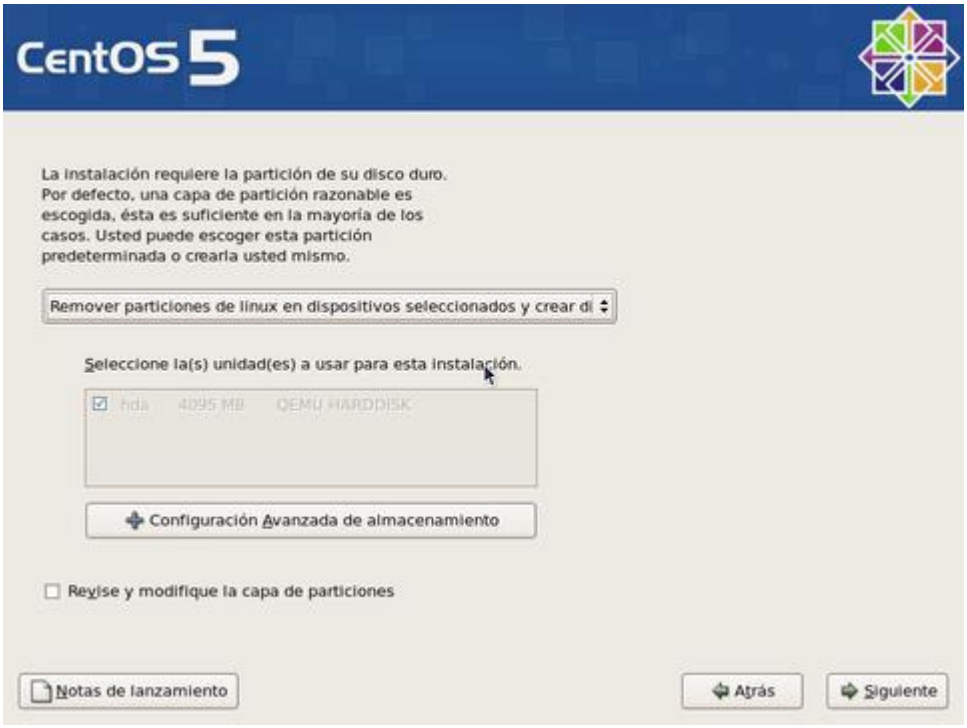
Para crear las particiones de forma automática, lo cual puede funcionar para la mayoría de los usuarios, puede seleccionar:

- «Remover particiones en dispositivos seleccionados y crear disposición», lo cual eliminaría cualquier partición de cualquier otro sistema operativo presente, y creará de forma automática las particiones necesarias.

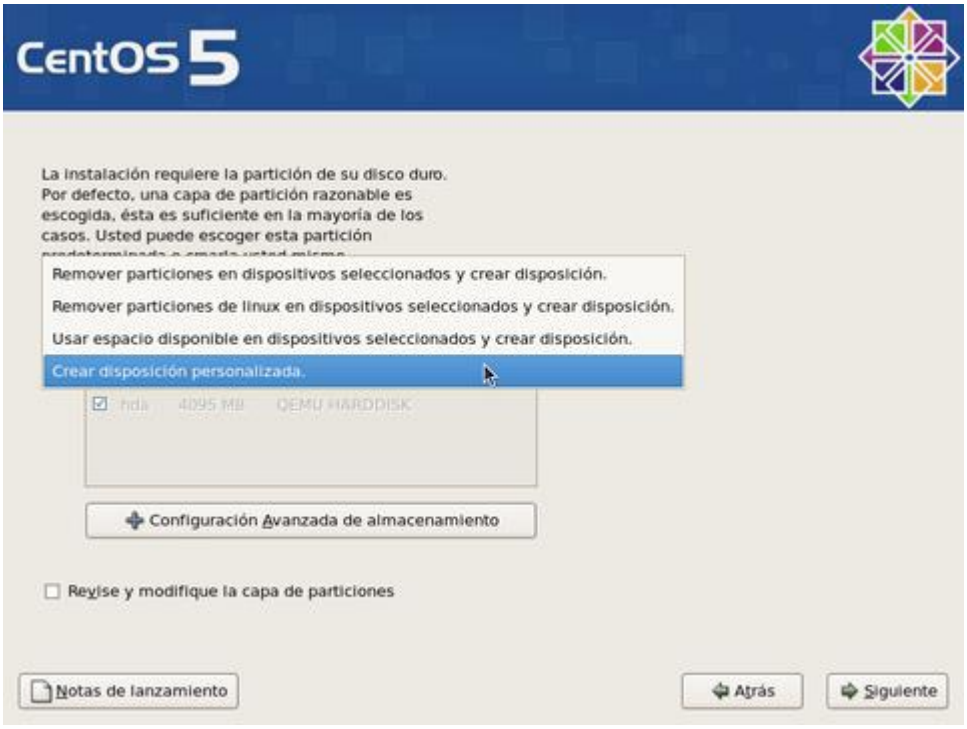
- «Remover particiones de linux en dispositivos seleccionados y crear

disposición», lo cual eliminaría cualquier partición otra instalación de Linux presente, y creará de forma automática las particiones necesarias.

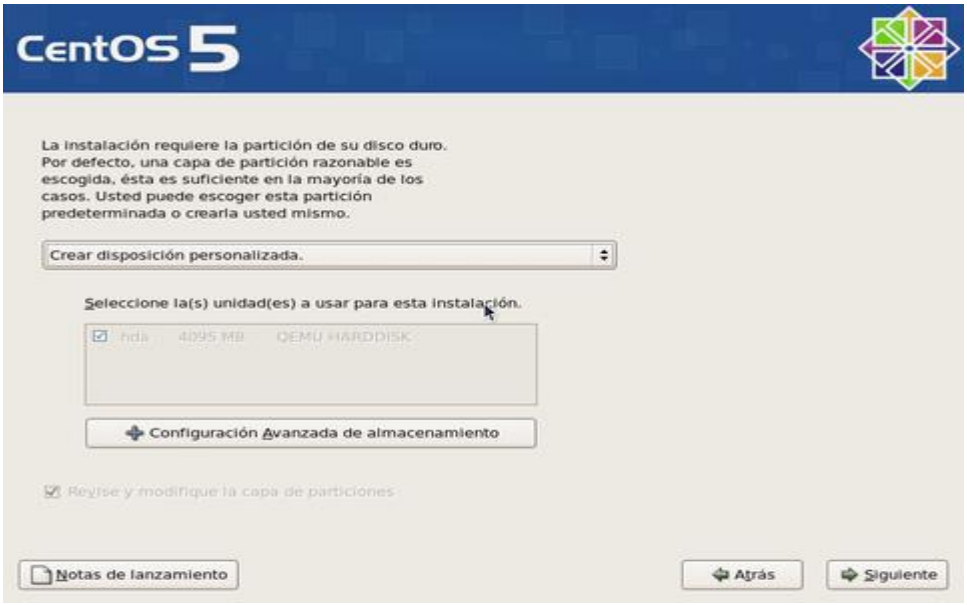
- «Usar espacio disponible en dispositivos seleccionados y crear disposición», lo cual creará de forma automática las particiones necesarias en el espacio disponible.



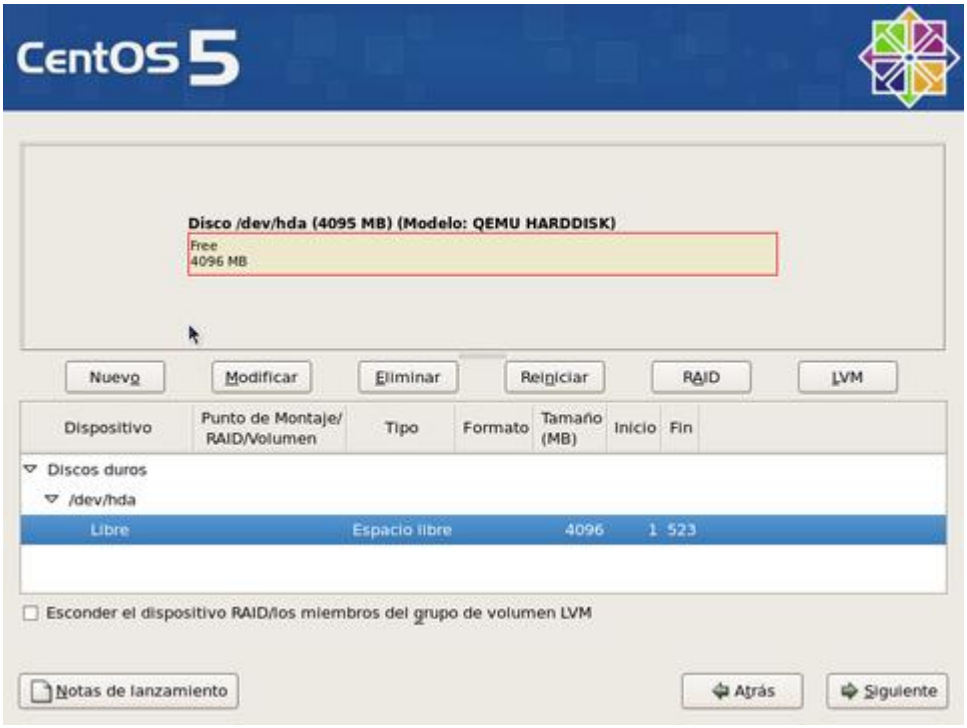
Conviene crear una disposición que permita un mayor control. Seleccione «Crear disposición personalizada».



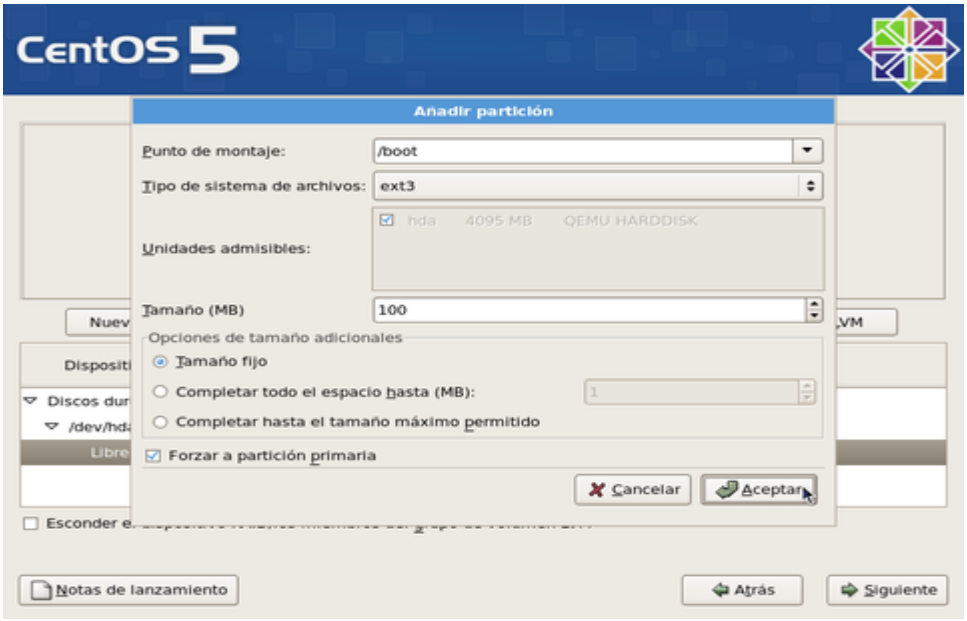
Una vez seleccionado «Crear disposición personalizada», haga clic sobre el botón «Siguiente».



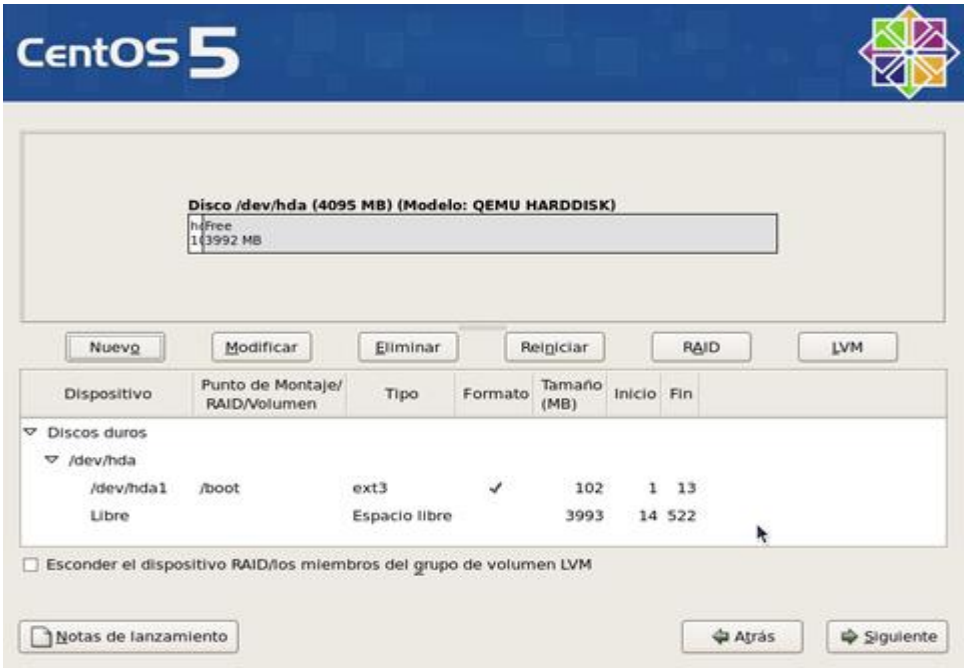
La herramienta de particiones mostrará el espacio disponible. Haga clic en el botón «Nuevo».



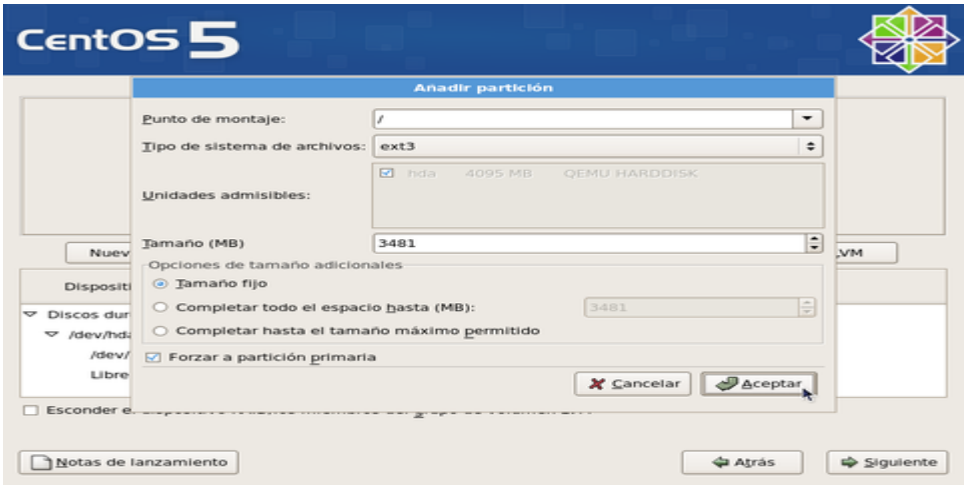
Asigne 100 MB a la partición /boot y defina ésta como partición primaria, siempre que la tabla de particiones lo permita.



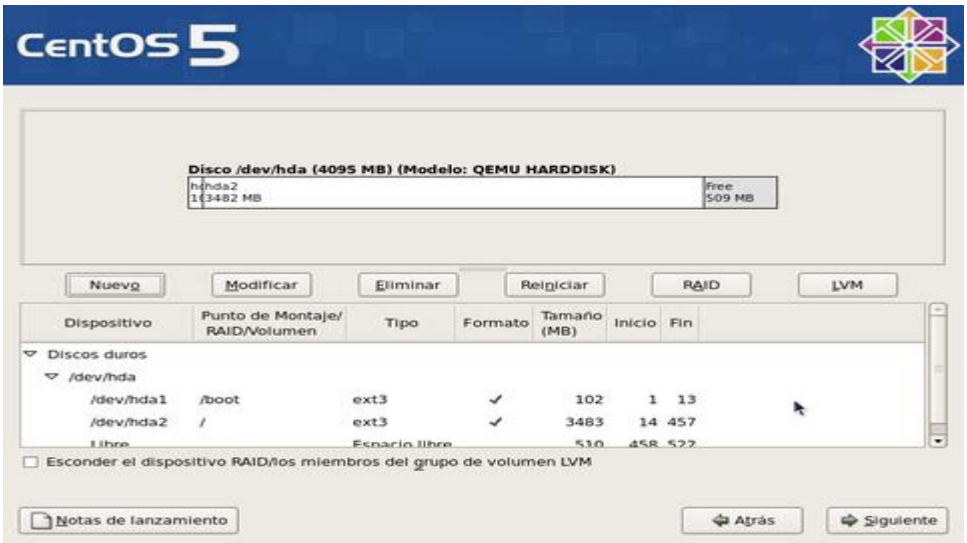
Si está conforme, haga clic otra vez en el botón «Nuevo» y proceda a crear la siguiente partición.



Asigne a la partición / el resto del espacio disponible menos lo que tenga calculado asignar para la partición de intercambio (200% de la memoria física, o cuanto baste para 2 GB). Se recomienda asignar / como partición primaria, siempre que la tabla de particiones lo permita.



Si está conforme, haga clic otra vez en el botón «Nuevo» y proceda a crear la siguiente partición.

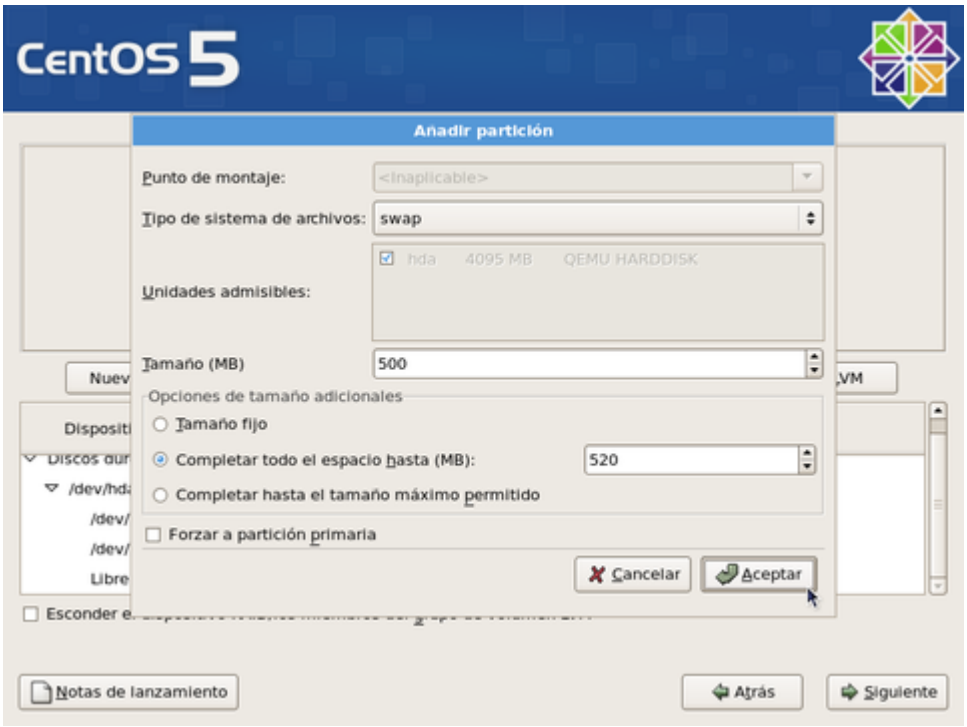


La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de «Tipo de sistema de archivos» la opción «swap». Si tiene menos de 1 GB de RAM, asigne el 200% de la memoria física. Si tiene más de 1GB RAM, asigne una cantidad equivalente al total del RAM más 2 GB. Por tratarse de la última partición de la tabla, es buena idea asignarle el espacio por rango, especificando valores ligeramente por debajo y ligeramente por arriba de lo planeado.

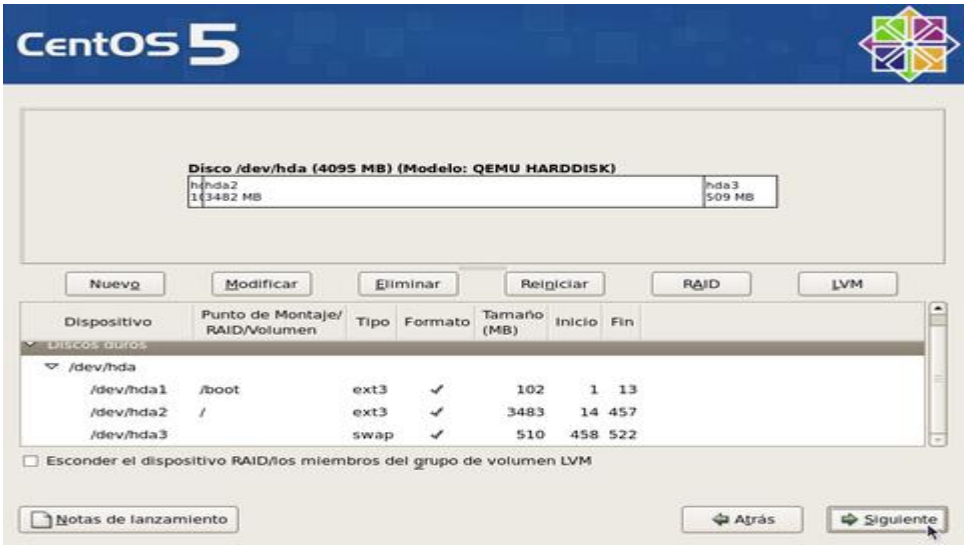
Otras particiones que se recomienda asignar, si se dispone del espacio en disco duro suficiente, son:

/usr	Requiere al menos 1.5 GB en instalaciones básicas. Debe considerarse el sustento lógico a utilizar a futuro. Para uso general, se recomiendan no menos de 5 GB y, de ser posible, considere un tamaño óptimo de hasta 8 GB en instalaciones promedio.
/tmp	Requiere al menos 350 MB y puede asignarse hasta 10240 MB o más dependiendo de la carga de trabajo y tipo de aplicaciones. Si por ejemplo el sistema cuenta con un grabador de DVD, será necesario asignar a /tmp el espacio suficiente para almacenar una imagen de disco DVD, es decir, al menos 4.2 GB.
/var	Requiere **al menos** 512 MB en estaciones de trabajo **sin servicios**. En servidores regularmente se le asigna **al menos la mitad del disco duro**.

/home	En estaciones de trabajo se asigna al menos la mitad del disco duro a esta partición.

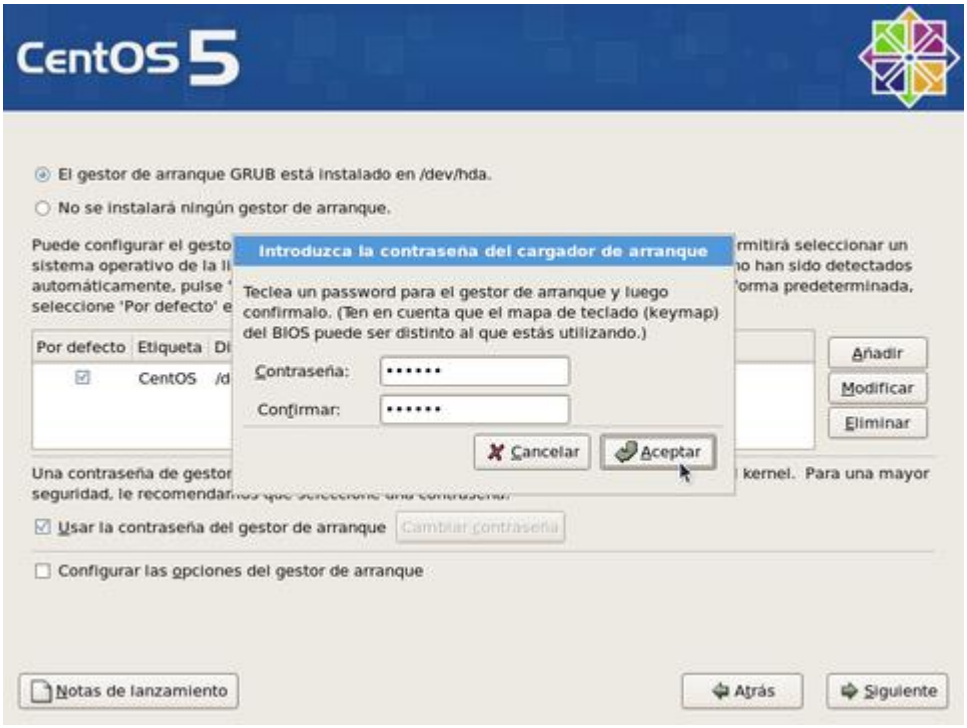


Si está conforme con la tabla de particiones creada, haga clic sobre el botón «siguiente» para pasar a la siguiente pantalla.

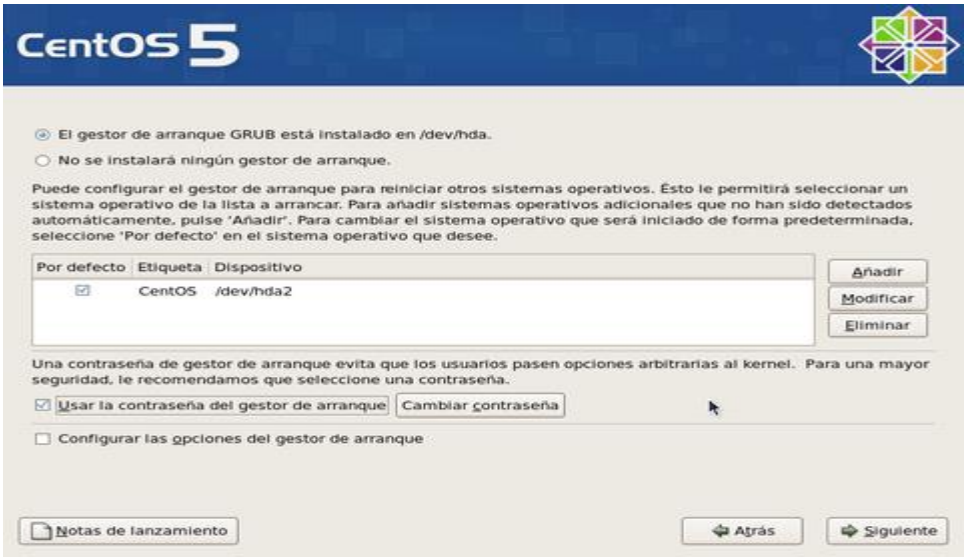


Ingresará a la configuración del gestor de arranque. Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de corrida 1, o cualquiera otro, haga clic en la casilla «Usar la contraseña del gestor de arranque».

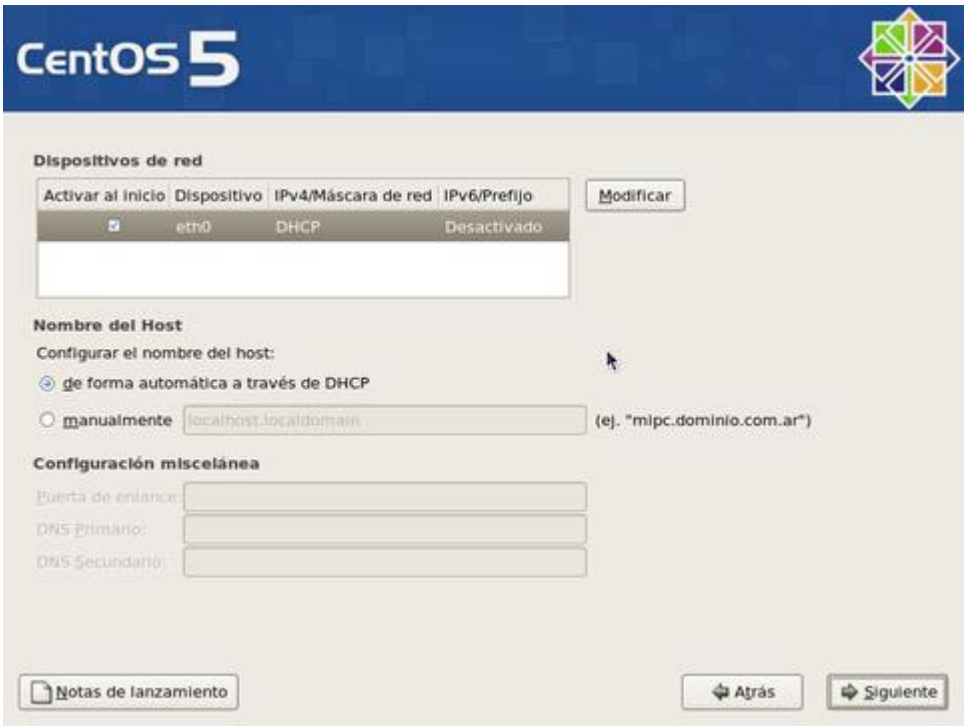
Se abrirá una ventana emergente donde deberá ingresar, con confirmación, la clave de acceso exclusiva para el gestor de arranque. Al terminar, haga clic sobre el botón «Aceptar».



Al terminar, haga clic sobre el botón «Siguiente».



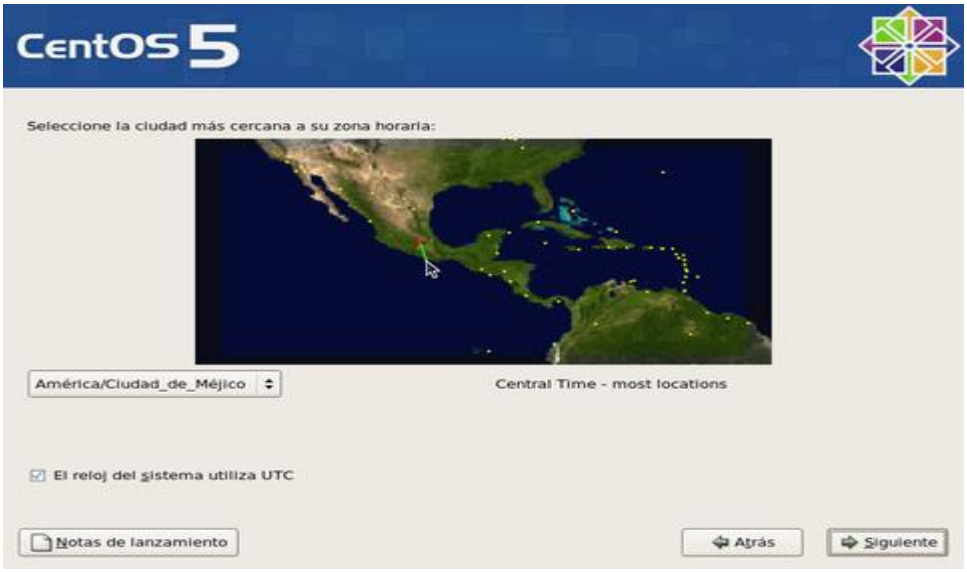
Para configurar los parámetros de red del sistema, haga clic sobre el botón «Modificar» para la interfaz eth0.



En la ventana emergente para modificar la interfaz eth0, desactive la casilla «Configurar usando DHCP» y especifique la dirección IP y máscara de subred que utilizará en adelante el sistema. Si no va a utilizar IPv6, también desactive la casilla. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, haga clic sobre el botón «Aceptar».

Asigne un nombre de anfitrión (HOSTNAME) para el sistema. Se recomienda que dicho nombre sea un FQDN (Fully Qualified Domain Name) resuelto al menos en un DNS local. Defina, además, en esta misma pantalla, la dirección IP de la puerta de enlace y las direcciones IP de los servidores DNS de los que disponga. Si desconoce que dato ingresar, defina éste como localhost.localdomain. Al terminar, haga clic sobre el botón «Siguiente».

Seleccione la casilla «El sistema horario usará UTC», que significa que el reloj del sistema utilizará UTC (Tiempo Universal Coordinado), que es el sucesor de GMT (b>Greenwich Mean Time, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Haga clic con el ratón sobre la región que corresponda en el mapa mundial o seleccione en el siguiente campo la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

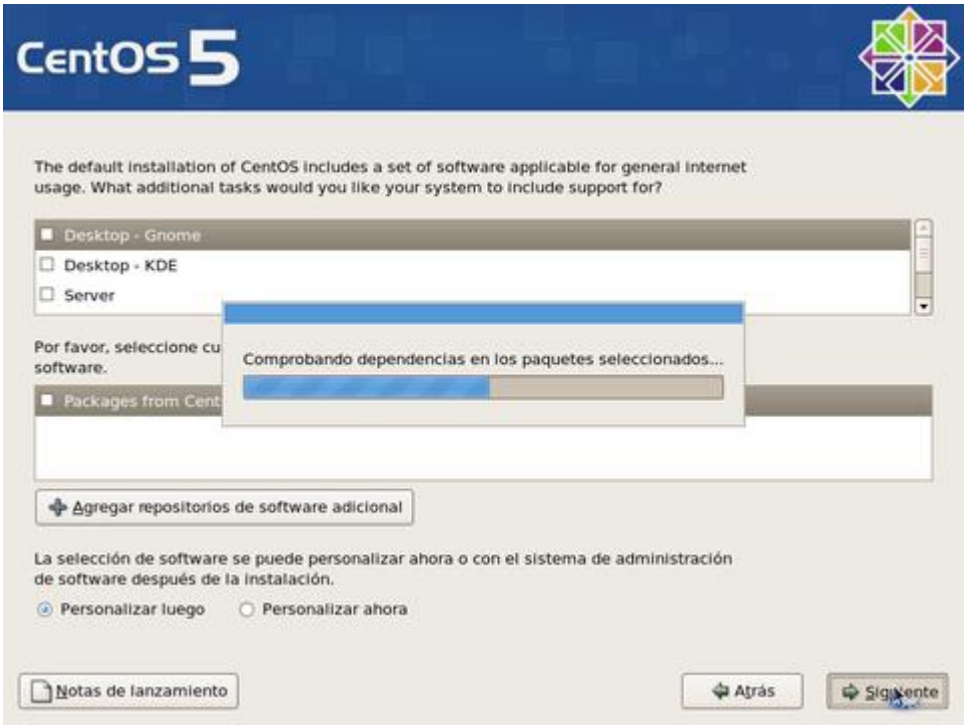


Asigne una clave de acceso al usuario root. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así como cualquier combinación que tenga relación con datos personales.

Al terminar, haga clic sobre el botón «Siguiente», y espere a que el sistema haga la lectura de información de los grupos de paquetes.

En la siguiente pantalla podrá seleccionar los grupos de paquetes que quiera instalar en el sistema. Añada o elimine a su conveniencia. Lo recomendado, sobre todo si se trata de un servidor, es realizar una instalación con el mínimo de paquetes, desactivando todas las casillas para todos los grupos de paquetes. El objeto de esto es solo instalar lo mínimo necesario para el funcionamiento del sistema operativo, y permitir instalar posteriormente solo aquello que realmente se requiera de acuerdo a la finalidad productiva que tendrá el sistema. Al terminar, haga clic sobre el botón «Siguiente».

Se realizará una comprobación de dependencias de los paquetes a instalar. Este procesos puede demorar algunos minutos.



Antes de iniciar la instalación sobre el disco duro, el sistema le informará respecto a que se guardará un registro del proceso en si en el archivo /root/install.log. Para continuar, haga clic sobre el botón «Siguiente».

Si iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo. Dependiendo de la capacidad del disco duro, este proceso puede demorar algunos minutos.

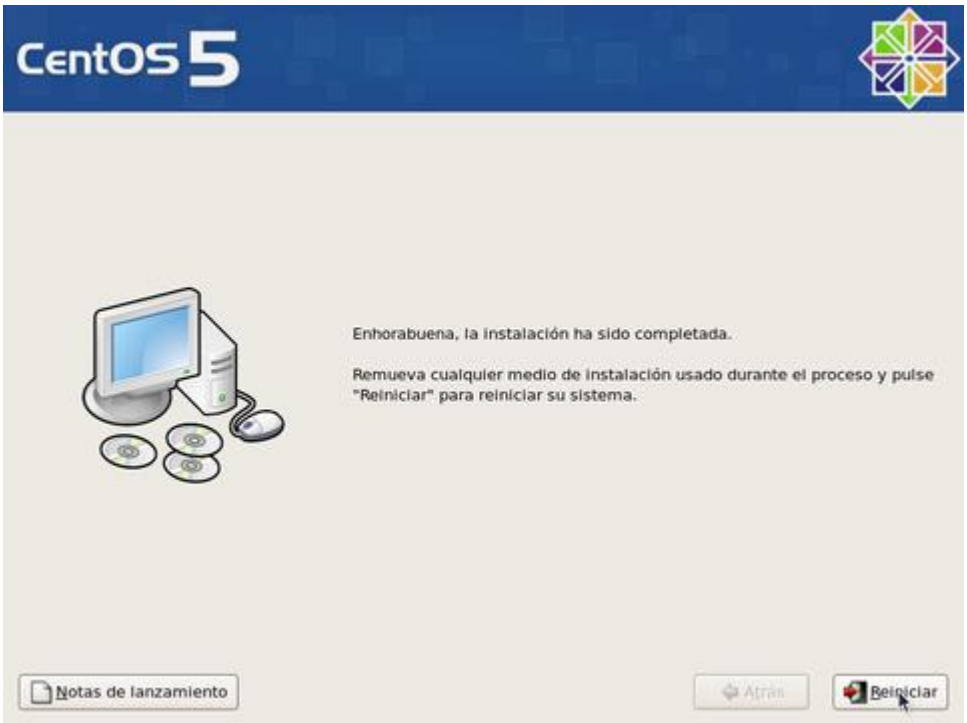
Se realizará automáticamente una copia de la imagen del programa de instalación sobre el disco duro a fin de hacer más eficiente el proceso. Dependiendo de la capacidad del microprocesador y cantidad de memoria disponible en el sistema, este proceso puede demorar algunos minutos.

Espere a que se terminen los preparativos de inicio del proceso de instalación.

Se realizarán preparativos para realizar las transacciones de instalación de paquetes.

Iniciará la instalación de los paquetes necesarios para el funcionamiento del sistema operativo. Espere algunos minutos hasta que concluya el proceso.

Una vez concluida la instalación de los paquetes, haga clic sobre el botón «Reiniciar».



ANEXO 8

Aprobación del Auspiciante

Anexo Nº8 (Aprobación del Auspiciante)