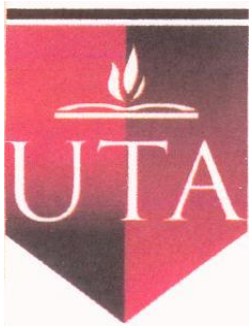


UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

TEMA:

"Esquemas de seguridad en la red para la comunicación interna y hacia el Internet de la Dirección Provincial de Salud de Tungurahua"

Trabajo de Graduación modalidad TEMI presentada como requisito previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

Autor: Diego Olivo Silva Lascano

Director: Ing. David Guevara

AMBATO - ECUADOR

Enero - 2011

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Investigación sobre el tema:

"ESQUEMAS DE SEGURIDAD EN LA RED PARA LA COMUNICACIÓN INTERNA Y HACIA EL INTERNET DE LA DIRECCIÓN PROVINCIAL DE SALUD DE TUNGURAHUA", del señor Diego Olivo Silva Lascano, egresado de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato.

Ambato, enero 2011

_____

Ing. David Guevara

AUTORÍA

El presente trabajo de investigación titulado: "ESQUEMAS DE SEGURIDAD EN LA RED PARA LA COMUNICACIÓN INTERNA Y HACIA EL INTERNET DE LA DIRECCIÓN PROVINCIAL DE SALUD DE TUNGURAHUA". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato enero 21, 2011

_____

Diego Olivo Silva Lascano

C.C.: 1804153649

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes: Ing. Oswaldo Paredes, Ing. Edison Álvarez, e Ing. Eduardo Chaso, revisó y aprobó el Informe Final del trabajo de graduación titulado "ESQUEMAS DE SEGURIDAD EN LA RED PARA LA COMUNICACIÓN INTERNA Y HACIA EL INTERNET DE LA DIRECCIÓN PROVINCIAL DE SALUD DE TUNGURAHUA",, presentado por el señor Diego Olivo Silva Lascano de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato.

_____

Ing. Oswaldo Paredes

PRESIDENTE DEL TRIBUNAL

_____ _____

Ing. Edison Álvarez

DOCENTE CALIFICADOR

Ing. Eduardo Chaso

DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo está dedicado a mis hijos quienes han sido la razón por la cual he sentido la necesidad de seguir adelante, a mis padres y la mujer que amo quienes me han brindado el apoyo incondicional en mis actos, y a toda mi familia que siempre han confiado en mí y me han dado la fortaleza y los valores para ser una persona de bien.

Diego Olivo Silva Lascano

AGRADECIMIENTO

A Dios por brindarme la vida, a mis Padres, hermana y abuelitos; quienes han sabido guiarme y llevarme a ser quien soy, a la mujer que amo por comprenderme y apoyarme, a quienes fueron mis profesores en especial al Ing. David Guevara quienes han sabido formarme profesionalmente, al Ing. Oscar Llerena y la Dirección Provincial de Salud de Tungurahua por abrirme las puertas para el desarrollo de la presente investigación, a mis amigos de corazón quienes de una u otra manera me han apoyado.

Diego Olivo Silva Lascano

Resumen Ejecutivo

El tema del presente trabajo trata sobre los Esquemas de seguridad en la red para la comunicación interna y hacia el Internet de la Dirección Provincial de Salud de Tungurahua, por lo cual en el Capítulo I, trata acerca de la identificación del problema, contextualización, justificación, análisis y planteamiento de objetivos; lo cual define al problema y es lo fundamental para continuar con la investigación.

En el Capítulo II se establece el marco teórico sobre el cual se va a trabajar, la fundamentación legal para la realización del proyecto; y también ya brinda un acercamiento y familiarización con el problema. Se identifican las variables y se formula la hipótesis que posteriormente será comprobada.

El cómo se realizara el proyecto se encuentra en el Capítulo III, donde se define con qué población se va a trabajar y cómo se manejaran las variables, la recolección de datos hasta llegar al análisis e interpretación de la recopilación de datos.

El Capítulo IV muestra la recopilación de los datos con su correspondiente análisis e interpretación, así como también la comprobación de la hipótesis en base a los datos recopilados de las encuestas realizadas a los usuarios de la institución.

Con el Capítulo V se llegan a las conclusiones y se brindan recomendaciones sobre el problema de comunicación de la red Institucional.

En el Capítulo VI se ofrece una propuesta alternativa para solucionar el problema planteado y analizado con respaldo teórico.

Introducción

Gracias a los avances tecnológicos, en día podemos establecer conexiones con cualquier parte del mundo a través del internet, que no es más que una red que abarca millones de equipos. A nivel de Empresas, Entidades educativas, o en cada hogar se cuenta con varios equipos conectados a una intranet, y la Dirección Provincial de Salud de Tungurahua no es la excepción.

La intranet de la Institución nace con la necesidad de conectar un equipo con otro para poder manejar una aplicación financiera, esta primera conexión se la hizo con cable coaxial que hoy se encuentra en desuso, los equipos fueron creciendo, al igual que las necesidades de comunicación entre los mismos. Es entonces cuando se implanta una intranet, con una conexión a internet compartida por un equipo que actuaba como puerta de enlace.

Con el incremento de los equipos, se tuvo que adquirir Acces Points y brindar acceso inalámbrico para evitar una nueva conexión cableada. La administración y el control de acceso a internet era limitada o nula, y empezaron a generarse problemas en la conexión que llevaban al colapso de la red juntamente con el equipo servidor que se encontraba con Windows XP.

Se efectuó un decreto presidencial para las instituciones públicas, de no utilizar más software que necesite la adquisición o desembolso por una licencia, por lo cual es necesario el cambio del servidor, con la adquisición de un nuevo equipo para la administración de la red que funcione sobre un sistema operativo libre, así como la implantación lógica de una nueva estructura de red, para optimizar el servicio.

El presente trabajo contribuye a la solución del problema, además con el cumplimiento de políticas a nivel de instituciones públicas.

CAPITULO I

EL PROBLEMA

1.1 Tema

"ESQUEMAS DE SEGURIDAD EN LA RED PARA LA COMUNICACIÓN INTERNA Y HACIA EL INTERNET DE LA DIRECCIÓN PROVINCIAL DE SALUD DE TUNGURAHUA"

1.2 Planteamiento del Problema

1.2.1 Contextualización

El ministerio de Salud Pública del Ecuador en su estructura jerárquica que se extiende hacia todas las Direcciones Provinciales del País ha considerado al área de informática como un subproceso del Proceso de Servicios Institucionales siendo completamente dependiente de este. Razón por la cual ha tenido que adecuarse con el presupuesto asignado para desempeñar sus funciones en el tratamiento de la información.

En el año 2000 la institución ya contaba con 5 equipos que necesitaban compartir información, para lo cual se crea una red con cable coaxial con conexión tipo bus. Para el Internet se utilizaba una cuenta Dial Up a 54 Mbps compartiendo mediante Windows esta conexión para el Internet en los equipos.

Con el pasar de los años la tecnología ha sido más necesaria cada vez para el tratamiento de la información dentro de la institución; es así que se han ido adquiriendo más equipos hasta ubicarse actualmente en un número de 60; que se encuentran conectadas a una red en su mayoría. Adicionalmente se cuenta con una conexión a Internet de banda ancha tipo ADSL de 1024x512.

Se mantenía un servidor con Windows 2003 Server que distribuía a los equipos por grupos de trabajo siendo además un servidor DNS y ayudaba a la compartición y acceso a la información. Este a su vez

se aprovechaba como servidor de Base de Datos para una aplicación financiera del ministerio de Salud.

En los últimos gobiernos se ha venido actualizando los sistemas de información y ahora en su mayoría son manejados con aplicaciones web; por lo cual las bases de datos en el presente son utilizadas como repositorios para consulta y respaldo de las actividades financieras realizadas en años anteriores.

El crecimiento de la necesidad de servicio de interconexión interna y hacia Internet obligo a implementar un acceso compartido utilizando servidores proxy y firewall gratuitos sobre XP que no brindaban la seguridad necesaria para el acceso seguro a la red global. La estructura de la red está conformada por una sola red clase A sin división permitiendo la libre comunicación de todos los equipos sin distinción.

Los equipos adquiridos luego de la implantación de este servidor intermediario y el de base de datos han sido utilizados inmediatamente muchas de las veces sin pasar por el departamento de informática. Por lo que no han sido configurados correctamente para su uso en la red, solo se les ha dado acceso para salir hacia el Internet.

En la actualidad se cuenta con un Switch DLINK de 24 puertos y otro Switch CNET de 16 puertos; pero el rápido crecimiento del número de equipos y la necesidad de estar interconectados y con servicio de Internet obligo a que en el año 2008 se implemente una red inalámbrica que consta de tres Access Points para cubrir toda la extensión del edificio, la misma que presenta problemas de conectividad por diversas circunstancias que deben ser corregidas.

El espacio físico del subproceso de informática está ubicado en una división dentro de la oficina del proceso de Educación para la Salud. Aquí se encuentran ubicados los servidores anteriormente descritos junto con los equipos de red y la portátil asignada para informática; además se realizan los trabajos de mantenimiento y reparación de equipos resultando insuficiente el área de trabajo.

1.2.2 Análisis critico

Los equipos de la institución se encuentran interconectados entre sí mediante cableado o inalámbricamente con una administración mínima; que permite el libre acceso a información confidencial y exclusiva para los usuarios de determinado proceso que a veces es compartida sin tomar en cuenta los riesgos existentes como el acceso desde cualquier equipo conectado a la red local.

El servidor intermediario para Internet actúa como Gateway o conexión compartida hacia el Internet, y tiene una aplicación proxy y un antivirus con un firewall de configuraciones muy generales. Las cuales dejan propenso al servidor y a la Intranet de infecciones de virus informáticos e incluso infiltraciones externas que ponen en riesgo la información institucional.

La estructura física del edificio limita la intensidad de la señal inalámbrica y a pesar de contar con tres Access Points existen lugares que no son cubiertos por la red. Esto nos da como resultado problemas de conectividad tales como velocidades muy bajas de interconexión, tiempos de espera agotados que traen pérdida de tiempo en el trabajo designado.

Las características de hardware del servidor proxy no son las adecuadas, es un equipo designado para labores de oficina que trabaja sobre la plataforma Windows XP Profesional que tampoco es destinada para ser un servidor. Los usuarios tienen restricciones mínimas para el acceso a Internet que permiten dedicar el tiempo de trabajo en otras actividades.

No se cuenta con herramientas de monitoreo de la red ni control en el ancho de banda sobre el cual trabajan los usuarios, dejando abierta la posibilidad de realizar actividades en la web que ocupen todo el ancho de banda disponible dejando con conexiones lentas a otros usuarios que necesitan mayor prioridad de uso del Internet.

1.2.3 Prognosis

Es imprescindible que se tomen decisiones al respecto, porque los equipos se encuentran expuestos con seguridades mínimas hacia el Internet lo que podría ocasionar robo o alteración de la información, así como pérdida parcial o total de los datos por infecciones de virus. Esto llevaría a perder incluso años de trabajo almacenados ya que pocas son las personas que realizan algún tipo de respaldo.

Es necesario garantizar la conectividad tanto en la Intranet como hacia el Internet, porque tareas que llevan mucho tiempo incluso horas para su conclusión a veces deben ser repetidas en todo su proceso por perdida de conexión a la red. Esto se dará más a menudo y habrá mucha pérdida de tiempo y acumulación de trabajo.

1.3 Formulación del Problema

¿La falta de esquemas de seguridad en la red ocasiona problemas de comunicación interna y hacia el Internet en la Dirección Provincial de Salud de Tungurahua?

1.4 Preguntas Directrices

¿De qué manera podemos limitar y proteger el acceso a la red únicamente de los usuarios de la organización?

¿Cómo se puede conseguir que los usuarios de un proceso no tengan acceso a la información disponible en la red de los usuarios de un proceso distinto?

¿Podemos administrar el acceso hacia Internet?

¿Cómo se limita el ancho de banda de la conexión a Intranet?

¿Qué medidas podemos tomas para protección de virus?

¿Podemos monitorear los sucesos de las actividades de la red local?

¿Se puede administrar los equipos utilizados para la interconexión?

1.5 Delimitación

Campo:	Comunicaciones
Área:	Intranets
Aspecto:	Seguridad
Lugar:	Procesos del edificio de la Dirección Provincial de Salud de Tungurahua ubicada en la ciudad de Ambato.
Tiempo:	Determinado para un tiempo de 4 meses

1.6 Justificación

Es un requisito indispensable en la Dirección de Salud de Tungurahua que sus empleados se encuentren conectados a Internet durante el desarrollo de sus actividades; es por esta razón que es imprescindible garantizar la estabilidad de la conexión de la red. De esta manera los funcionarios de la institución tendrán acceso permanente e ininterrumpido hacia el servicio, evitando la repetición de tareas y desarrollando a tiempo las mismas.

Al aplicar esquemas de seguridad, con control de acceso, políticas que permitan administrar el uso de la red, se tiene la capacidad de limitar quién accede y a donde, se solucionaran problemas de confidencialidad de datos; además de controlar servicios que se pueden ejecutar en segundo plano y establecer comunicación entre los equipos que podrían generar un hueco de seguridad. Con esto se disminuye el acceso libre de cualquier usuario a la información de todos los equipos como se lo hace actualmente.

También disminuirá la propagación de virus informáticos y posibles ataques que actualmente hacen que los equipos se vuelvan lentos, se cuelguen, y en el peor de los casos la perdida de archivos importantes almacenados. De esta manera los equipos se mantendrán funcionando estables y la información almacenada va estar disponible en cualquier momento en que nos puede ser útil por ejemplo frente a una auditoria.

Con la instalación y configuración de un servidor para la administración de la red, se tendrá un acceso más rápido hacia el Internet por la interacción con la cache en el mismo. Podremos limitar el ancho de banda de tal forma que las aplicaciones en línea tendrán prioridad logrando un mejor desempeño. Se podrá controlar el acceso a sitios web que desvían la atención de los empleados y permiten que pierdan tiempo. Incluso con la configuración del firewall tendremos un control preciso del tránsito de la red y hacia el Internet evitando propagación de virus y accesos no deseados.

Es importante conocer lo que está sucediendo en la red, por lo cual se implementaran aplicaciones que permitan monitorear estas actividades y obtendremos informes que nos permitirán tomar decisiones oportunas y a tiempo, lo cual nos lleva a mejorar constantemente el desempeño de la red.

El estado ecuatoriano ha dispuesto que en todas las entidades públicas se utilice software libre. El presente trabajo se lo realizará sobre una plataforma Linux y con la explotación y utilización de herramientas libres ofreciendo igual e incluso mayor rendimiento que las pagadas utilizadas actualmente.

Este proyecto es factible de realizar porque dentro del ámbito de software libre existen varias herramientas que ayudan al desarrollo de la resolución del problema. El equipo para la conexión de la red con que se cuenta es completamente configurable por lo cual la seguridad puede ser implementada.

1.7 Objetivos

1.7.1 Objetivo General

- Implementar Esquemas de seguridad en la red para la comunicación interna y hacia el Internet de la Dirección Provincial de Salud de Tungurahua

1.7.2 Objetivos específicos

- Realizar un estudio estructural de la red para descubrir y solucionar de mejor manera los inconvenientes encontrados
- Establecer políticas de control de acceso para administrar el acceso a la red de los usuarios
- Implementar una nueva estructura lógica en la Intranet
- Instalar un nuevo servidor para la administración de la red con servidores lógicos para Proxy, Firewall, Monitoreo de red
- Validar la propuesta

CAPITULO II

MARCO TEORICO

2.1 Antecedentes Investigativos

En la Universidad Técnica de Ambato, en la Facultad de Ingeniería en Sistema Electrónica e Industrial en el año 2007 el Ing. Geovanny Mauricio Iturralde Ruiz realizo el tema "Diseño e Implantación de una Intranet Informativa bajo el Sistema Operativo Linux para el Centro Educativo Nuevo Mundo". Este tema se ha desarrollado bajo la misma plataforma y en la misma área de Intranets por lo cual tomare las conclusiones de los mismos como referencia.

2.2 Fundamentación

2.2.1 Fundamentación Legal

En el Registro Oficial No. 322 publicado el miércoles 23 de abril del 2008 el actual Presidente de la República Rafael Correa establece como política de estado para las entidades de la Administración Pública Central la utilización del software libre en sus sistemas y equipamientos informáticos. (Adjunto al final el decreto completo)

2.2.2 Fundamentación Teórica

2.2.2.1 Acceso a la Intranet

En el aspecto lógico del diseño de la red una forma de administrar el acceso hacia la misma es haciendo un subneteo. Para la administración de la red es necesaria la implementación de un servidor. Además podemos controlar el acceso a cada equipo por medio de un firewall instalado localmente.

2.2.2.1.1 Subnetting

A medida que las redes crecen aumentando el número de segmentos, mas direcciones de red (IP) son necesarios ya que cada segmento requiere un número propio. La InterNIC (Network Information Centers Cooperation), sin embargo, no puede manejar un número ilimitado de direcciones de red ya que se están acabando rápidamente debido a la alta demanda proveniente de la comunidad de Internet. Es por esto que los administradores de redes deberán trabajar con lo poco que tienen para acomodarse mejor a los requerimientos de la red y la reducida oferta de direcciones.

Una manera de lograrlo es tomar las direcciones que son asignadas a la red y expandir su capacidad con subredes. *Subnetting* permite incrementar el número de redes disponibles sin solicitar otra dirección IP. A medida que se agregan hosts se hace más grande la tabla de direccionamiento (*routing table*), lo que trae como consecuencia un aumento en los costos de los *routers* y una degradación en el performance del *router*.

Una gran solución a este problema es ofrecida por el Subnetting, lo que permite reducir el número total de redes a ser asignadas. La idea es tomar una <parte de red> de una dirección de IP y asignar las direcciones IP de esa <parte de red> a varias redes físicas, que serán ahora referidas como subredes. Pero hay que hacer ciertas cosas para que esto funcione. Primero, las subredes deben de estar cerca unas de otras, debido a que a un punto distante en el Internet todas lucirían igual a una sola red, teniendo solo una <parte de red> en común. Esto significa que un *router* solo estaría habilitado para seleccionar una sola ruta para llegar a cualquiera de las subredes, así que es mejor que se encuentren ubicadas en la misma dirección.

El mecanismo con el cual se puede lograr compartir un numero de red (<parte de red>) entre distintas redes involucra la configuración de todos los nodos en cada subnet con una máscara de red, la misma para todos los nodos dentro de una subred. Con las máscaras de redes se logra jerarquizar aún más la estructura jerárquica de un IP, que como se dijo antes está constituida por <parte de red> + <parte de host>, incluyendo un nuevo nivel de jerarquía que llamaremos <número de subnet>. Como ya se sabe, todo los hosts en una misma red tienen la misma <parte de red>, pero ahora todos los host en la misma red física tendrán el mismo <número de subnet>, lo que hace que los hosts en la misma red, pero en distintas redes físicas compartan la <parte de red> pero no el <número de subnet>, y esto como se puede notar ayuda notablemente en la transmisión de información, pues se complementa las tablas de direccionamiento con otro campo que ayudara a mejorar la eficiencia de envió de paquetes.

También es importante saber que podemos poner múltiples subredes en una misma red física. El efecto que esto tendría es que se deberá forzar a los hosts en la misma red, pero en diferentes subredes, a hablar a través de *routers*. Esto puede ser útil para razones administrativas como por ejemplo separar distintos departamentos en una misma LAN.

VLSM

Las máscaras de subred de tamaño variable (variable length subnet mask, VLSM) representan otra de las tantas soluciones que se implementaron para el agotamiento de direcciones ip (1987) y otras como la división en subredes (1985), el enrutamiento de interdominio CIDR (1993), NAT y las direcciones ip privadas.

Planificación de subredes de tamaño variable.- Recordemos que una subred es un conjunto de direcciones IP y con ella podemos hacer dos cosas: asignar direcciones IP a los equipos o dividirlo nuevamente en subredes más pequeñas. En cada división, las subredes primera y última no se usan (Actualmente la mayoría del hardware ya soporta el poder trabajar con ambas, primera y última pero deberemos de comprobarlo antes de hacer uso de estas, estas tenían una aplicación parecida al direccionamiento Ip donde la primera identificaba la red y la última es de broadcast, en este caso la primera identificaba la subred y la última se aplicaba al broadcast de subred), cabe aclarar que no se usan para asignar direcciones IP a los equipos pero si se pueden usar para dividirlas en subredes más pequeñas.
El concepto básico de VLSM es muy simple: Se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir tomando bits "prestados" de la porción de hosts, ajustándose a la cantidad de hosts requeridos por cada segmento de nuestra red.

2.2.2.1.2 Servidor

El sistema operativo a instalarse debe ser de Software Libre por el decreto presidencial anteriormente enunciado, por lo cual se ha elegido GNU/Linux.

GNU/Linux

Linux Is Not UniX. Linux es una implementación totalmente independiente del núcleo (Kernel) de Unix. Es un sistema operativo completo, multitarea y multiusuario al igual que cualquier otra versión de Unix que es sobre el que se basa. Este ofrece todo lo necesario para trabajar en red con TCP/IP.

El sistema operativo se complementa con varias aplicaciones desarrolladas por el grupo GNU. Tanto las aplicaciones como el núcleo son de software libre y podemos tener las mismas utilidades y prestaciones que en un Windows.

Al igual que Windows existen distintas distribuciones y distintas versiones de Sistema Operativo orientado tanto para ser servidor como para ser utilizado en un escritorio. Cada versión agrupa diferentes aplicaciones que se ejecutan de distinta manera según las necesidades de los usuarios.

CentOS

CentOS (**C**ommunity **ENT**erprise **O**perating **S**ystem) 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.

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

CentOS al igual que el resto de distribuciones Linux, posee varias herramientas administrativas para servicios de red, como firewalls, limitadores de ancho de banda, monitores de actividades, servidores intermediarios, puede actuar como Gateway, redireccionar paquetes etc. Debemos tratar de explotar estos servicios de mejor manera para obtener un mejor rendimiento.

Iptables

Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de paquetes en diferentes estados del procesamiento. Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.

El componente más popular construido sobre *Netfilter* es iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log. El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías.

iptables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. El nombre *iptables* se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto Netfilter. Sin embargo, el proyecto ofrece otros subsistemas independientes de iptables tales como el *connection tracking system* o sistema de seguimiento de conexiones, que permite encolar paquetes para que sean tratados desde espacio de usuario. *iptables* es un software disponible en prácticamente todas las distribuciones de Linux actuales.

Funcionamiento.- iptables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en *cadenas*: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en *tablas*: cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

Cada regla especifica qué paquetes la cumplen (*match*) y un *destino* que indica qué hacer con el paquete si éste cumple la regla. Cada paquete de red que llega a una computadora o que se envía desde una computadora recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete. Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el fin de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena, la *política* de destino de la cadena dicta qué hacer con el paquete. Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido ninguna regla de la cadena o si la cadena definida por el usuario está vacía, el recorrido continúa en la cadena que hizo la llamada (lo que se denomina *implicit target RETURN* o RETORNO de destino implícito). Solo las cadenas predefinidas tienen políticas.

2.2.2.1.3 Firewall Local

A más de la protección del acceso de entrada y salida de paquetes de Internet mediante el servidor con iptables; tenemos otras herramientas firewall que podemos instalarlas en cada equipo para su propia protección.

Existe variedad de estas herramientas, muchas de estas pagadas y otras de software de libre distribución. COMODO es una empresa dedicada al desarrollo de herramientas de seguridad como son antivirus, firewall, servicio de DNS seguros, etc. Esta misma empresa ofrece un paquete denominado Internet security, el cual contiene el firewall y un antivirus ambos básicos totalmente gratuitos. También ofrece estas y otras herramientas en una versión pagada que son mucho más completas.

Para motivos de protección de los equipos es suficiente adquirir la versión gratuita, la cual nos ofrece el filtrado de acceso de nuestro equipo desde y hacia la red e Internet, ofreciéndonos un porcentaje extra de seguridad, además del antivirus que nos ayuda con la eliminación de virus conocidos eliminándolos antes que estos puedan ser ejecutados previniendo daños en el sistema operativo.

2.2.2.2 Compartición de Archivos

Un punto muy importante dentro de una Intranet es la compartición de archivos, que archivos se comparte y a que archivos se tiene acceso y más aun quien tiene acceso a estos archivos q se encuentran compartidos. Y no solo pueden ser archivos sino también otros recursos los que se encuentren disponibles en la red. Por este motivo es muy importante la configuración de un servidor que ayude con la administración del acceso de estos archivos.

Al momento de realizar el subneteo protegemos el acceso a la información de tal manera que solamente los miembros de una misma subnet tengan acceso a sus equipos, esto se refleja en los procesos donde por ejemplo solamente los empleados de financiero pueden acceder a equipos de financiero y a ningún otro más de la institución aparte del servidor.

2.2.2.2.1 Servidor Samba

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios

haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autentificar con su propio archivo de usuarios.

Entre los sistemas tipo Unix en los que se puede ejecutar Samba, están las distribuciones GNU/Linux, Solaris y las diferentes variantes BSD entre las que podemos encontrar el Mac OS X Server de Apple.

Samba configura directorios Unix y GNU/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de GNU/Linux pueden montar en sus sistemas de archivos estas unidades de red como si fueran dispositivos locales, o utilizar la orden smbclient para conectarse a ellas muy al estilo del cliente de la línea de órdenes ftp. Cada directorio puede tener diferentes permisos de acceso sobrepuestos a las protecciones del sistema de archivos que se esté usando en GNU/Linux. Por ejemplo, las carpetas *home* pueden tener permisos de lectura y escritura para cada usuario, permitiendo que cada uno acceda a sus propios archivos; sin embargo, deberemos cambiar los permisos de los archivos localmente para dejar al resto ver nuestros archivos, ya que con dar permisos de escritura en el recurso no será suficiente.

2.2.2.3 Acceso a Internet

Como es conocido es suficiente tener un equipo que tenga conexión a Internet para poder compartir ese acceso y aprovechar el ancho de banda en su máximo posible de una manera correcta. Pues de la manera como se administre la conexión depende la satisfacción del servicio en cada cliente.

2.2.2.3.1 Servidor Proxy

Se suele interpretar como intermediario o delegado; y es aquel que ofrece un servicio de red a varios clientes para realizar conexiones con otros servicios de red.

Trabaja de la siguiente manera:

- Cliente se conecta al servidor proxy
- Cliente solicita un servicio de otro servidor
- El servidor proxy proporciona el recurso ya sea conectándose al servidor especificado o sirviéndose de su memoria cache
- El servidor proxy puede alterar la solicitud o la respuesta para diversos propósitos.

Pueden trabajar también como muros cortafuegos actuando como filtro de paquetes en el nivel de red o en el nivel de aplicación controlando diferentes servicios.

Una aplicación común de los servidores proxy es actuando como cache de contenido de red, generalmente HTTP. Al momento de realizar una petición de un URL el servidor primero consulta en su cache, si lo tiene envía la respuesta inmediatamente caso contrario lo traerá del servidor remoto y envía la respuesta al cliente. De esta manera se tiene un acceso más rápido y confiable.

SQUID

Es un servidor intermediario proxy de alto desempeño que se ha venido desarrollando desde hace varios años y que hoy en día es muy popular y usado ampliamente en servidores Linux y Unix; es confiable robusto y versátil distribuido bajo licencia GNU/GPL. Squid funciona como servidor intermediario y cache de contenido de red para protocolos HTTP, FTP, GOPHER y WAIS, entre otros.

Permite el acceso mediante reglas pudiendo entre otras cosas filtrar sitios web, extensiones, palabras; controlar quien puede acceder hacia los servicios, administrar un horario.

2.2.2.4 Ancho de Banda

Se refiere a la velocidad binaria, tasa de bits o flujo de bits que se transmiten por segundo a través de un sistema de transmisión digital o entre dos dispositivos digitales; en otras palabras es la velocidad de transferencia de datos.

Se lo expresa en bits por segundo y generalmente se lo representa como bps, bit/s, b/s donde la b siempre se debe escribir en minúscula para impedir la confusión con byte.

2.2.2.4.1 CBQ

Class Based Queueing o Encolamiento Basado sobre Clases, es un guión escrito en BASH utilizado para la gestión y control del uso de ancho de banda en GNU/Linux. Fue originalmente creado en 1999 por Pavel Golubev y posteriormente mantenido de 2001 a 2004 por Lubomir Bulej. Utiliza de una forma simplificada los mandatos ip y tc para su funcionamiento, y forma parte del paquete iproute, el cual se incluye en las instalaciones básicas de la mayor parte de las distribuciones de GNU/Linux.

2.2.2.5 Antivirus

Los antivirus nacieron como una herramienta simple cuyo objetivo era detectar y eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectar y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de *malware*, como *spyware*, *rootkits*, etc.

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.

Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el ordenador, con técnicas como heurística, HIPS, etc.

Usualmente, un antivirus tiene un (o varios) componente residente en memoria que se encarga de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso.

Asimismo, cuentan con un componente de análisis bajo demanda (los conocidos *scanners*, exploradores, etc.) y módulos de protección de correo electrónico, Internet, etc.

El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

2.2.2.5.1 ClamAV (Servidor)

Es un servicio muy útil implementado sobre el servicio clamd que permite utilizar con mejor desempeño la base de datos de firmas digitales.

ClamAV tiene las siguientes características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Cumple con las especificaciones de familia de estándares POSIX (Portable Operating System Interface for UNIX o interfaz portable de sistema operativo para Unix).

- Exploración rápida.
- Detecta más de 44 mil virus, gusanos y troyanos, incluyendo virus para MS Office.
- Capacidad para examinar contenido de ficheros ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Soporte para explorar ficheros comprimidos con UPX, FSG y Petite.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.

2.2.2.6 Monitoreo de Actividades

Una vez implementados todos estos servicios que nos permiten administrar la red, es necesario saber y conocer cómo están trabajando los mismos, para poder tomar medidas en beneficio del desempeño de la red.

2.2.2.6.1 Monitoreo del servidor Proxy

SARG

Squid Analysis Report Generator es la más completa y fácil de utilizar herramienta para la generación de reportes a partir de las bitácoras de Squid. Permite ver con detalle la actividad de todos los equipos y/o usuarios dentro de la red de área local, registrada en la bitácora de Squid.

2.2.2.6.2 Monitoreo de uso de la red y ancho de banda

MRTG

MRTG (Multi Router Traffic Grapher) es una herramienta, escrita en C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera los resultados en ficheros HTML con gráficos, que proveen una representación visual de este tráfico.

MRTG utiliza SNMP (Simple Network Management Protocol o Protocolo Simple de administración de red) para recolectar los datos de tráfico de un determinado dispositivo (dispositivos encaminamiento o servidores), por tanto es requisito contar con al menos un sistema a supervisar con SNMP funcionando, y con dicho servicio correctamente configurado.

2.2.2.7 Administración de Equipos

Además de la instalación, configuración, y administración del servidor, también debemos recordar el resto de dispositivos utilizados para la interconexión de la Intranet. Estos son el ADSL mediante el cual obtenemos el acceso hacia Internet, el Switch D-Link utilizado para la red cableada y los tres AP para la cobertura inalámbrica.

2.2.2.7.1 ADSL/Router

El router ADSL es un dispositivo que permite conectar uno o varios equipos o incluso una red de área local (LAN)

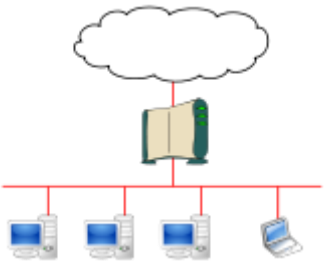


Fig. 2-1. ADSL/Router
Fuente: Internet

Realmente se trata de varios componentes en uno. Realiza las funciones de:

- Puerta de enlace, ya que proporciona salida hacia el exterior a una red local.
- Router: cuando le llega un paquete procedente de Internet, lo dirige hacia la interfaz destino por el camino correspondiente, es decir, es capaz de encaminar paquetes IP.
- Módem ADSL: modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y demodula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos. De hecho, existen configuraciones formadas por un módem ADSL y un router que hacen la misma función que un router ADSL.
- Punto de acceso wireless: algunos router ADSL permiten la comunicación vía Wireless (sin cables) con los equipos de la red local.

Como se puede ver, los avances tecnológicos han conseguido introducir la funcionalidad de cuatro equipos en uno sólo.

2.2.2.7.2 Switch D-Link

Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red,

de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Fig. 2-2.Switch D-Link
Fuente: Internet

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un *filtro* en la red, mejoran el rendimiento y la seguridad de las LANs.

Los puentes (bridges) y conmutadores (switches) pueden conectarse unos a los otros pero siempre hay que hacerlo de forma que exista un único camino entre dos puntos de la red . En caso de no seguir esta regla , se forma un bucle o loop en la red, que produce la transmisión infinita de tramas de un segmento al otro . Generalmente estos dispositivos utilizan el algoritmo de spanning tree para evitar bucles , haciendo la transmisión de datos de forma segura.

2.2.2.7.3 Access Points DWL-520

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Por otro lado, una red donde los dispositivos cliente se administran a sí mismos -sin la necesidad de un punto de acceso- se convierten en una red ad-hoc. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente y las ondas, mediante una antena inalámbrica.

2.3 Hipótesis

La implementación de esquemas de seguridad solucionará los problemas de comunicación interna y hacia el Internet en la red de la Dirección Provincial de Salud de Tungurahua

2.4 Variables

2.4.1 Variable independiente

Esquemas de seguridad en la red

2.4.2 Variable dependiente

Problemas de comunicación interna y hacia el Internet

CAPITULO III

METODOLOGIA

3.1 Enfoque

El tema de investigación del presente proyecto tiene un enfoque cualitativo, porque a través de la recolección de datos se llegó a determinar los problemas de comunicación que se presentan en la red de la Dirección Provincial de Salud de Tungurahua. Todos los usuarios de la red son beneficiados y el informático provincial fue quien apruebe la aplicación de las medidas y su administración.

3.2 Modalidad básica de la investigación

3.2.1 Investigación de Campo

La investigación se realizó en las instalaciones de la institución para obtener información de primera mano que permitió conocer a fondo como se genera el problema lo cual ayudó a tomar soluciones efectivas y cumplir con los objetivos del proyecto.

3.2.2 Investigación Documental – Bibliográfica

La mejor manera de recopilar información es la investigación bibliográfica y documental, pues los libros y el internet son la mayor fuente de información; se obtienen varios puntos de vista sobre un mismo tema para llegar a conclusiones propias, se familiariza mejor con el tema, se enriquece los conocimientos y se puede resolver de mejor manera cualquier problema planteado.

3.3 Nivel o tipo de Investigación

Para el desarrollo del proyecto se utilizó la investigación exploratoria, descriptiva y explicativa; porque fue necesario indagar y determinar el problema en términos generales. También se describió

tal cual se presenta el problema en la organización, sus causas y efectos con el fin de disminuirlos a través de la administración y la implantación de esquemas de seguridad; posteriormente se alcanzó al nivel explicativo con la comprobación de la hipótesis.

3.4 Población y Muestra

3.4.1 Población

A continuación se detalla la lista de funcionarios de la Dirección Provincial de Salud de Tungurahua que utilizan el servicio de red, clasificada por procesos. No se toma en cuenta la muestra por ser una población reducida

Procesos	Funcionarios
Informática	4
Implantación de la Norma	14
Gestión Financiera	7
Aseguramiento de la Calidad	4
Servicios Institucionales	5
Recursos Humanos	4
Vigilancia Sanitaria	4
Gobernante	2
Oferta y Demanda	3
Epidemiología	3
Comisaria de la Salud	2
Asesoría Jurídica	2
TOTAL	**54**

Tabla. 3-1. Número de Funcionarios por proceso de la DPST
Fuente: Distributivo de empleados de la DPST
Elaborado por: Diego Silva

3.5 Operacionalización de variables

Conceptualización	Dimensión	Indicadores	Ítems	Tec. Inst.
Esquemas de seguridad de red: Implementación de seguridad en un servidor que controla tanto la conexión como los dispositivos, para tener acceso a la información.	Conexión hacia Internet	Manera de conectarse	¿Mediante Que Dispositivo Se Tiene La Conexión A Internet?	Encuesta a informático
		Velocidad de conexión	¿Cuál Es La Velocidad De Bajada? ¿Cuál Es La Velocidad De Subida?	
	Servidor	Características del equipo	Procesador, Memoria, Disco Duro	
		Software	¿Existen inconvenientes en reemplazar el sistema operativo actual por una distribución Linux?	
	Dispositivos de conexión	Administración de dispositivos	¿Se pueden configurar libremente los dispositivos?	
	información	Nivel de acceso	¿Puede acceder a información de cualquier equipo de la red? ¿Qué directorios comparte?	
Problemas de comunicación interna y hacia el Internet: Estos problemas son	Infecciones de virus	Uso del flash USB	¿Revisa el flash antes de abrirlo?	Encuesta a usuarios
		Restricción de acceso en	¿Qué paginas visita? ¿Abre correos	

causados principalmente por las infecciones de virus y generalmente afectan a la información contenida	Respaldo de información	Internet Frecuencia de respaldo	electrónicos de remitentes desconocidos? ¿Con que frecuencia respalda sus archivos?	

Tabla. 3-2. Operacionalización de variables
Elaborado por: Diego Silva

3.6 Recopilación de la información

Se realizó la recopilación de la información de las encuestas propuestas; no se detectó ningún tipo de inconveniente con respecto a información contradictoria o no pertinente.

3.6.1 Plan de recolección de la información.

Para la recolección eficaz de la información se recurrió a la siguiente estrategia:

- Elaboración de las encuestas
- Aplicación de la encuesta tanto al informático provincial y a los usuarios
- Recopilación de la información.

3.6.2 Plan de procesamiento de la información.

Luego de haber realizado la entrevista se procedió a realizar el siguiente proceso:

- Revisión crítica de la información.
- Realización de Tabulaciones.
- Organización de la información.
- Graficar.
- Registrar la información

3.7 Plan de análisis e interpretación de resultados

Se utilizaron recursos estadísticos para interpretar los resultados basados siempre en el marco teórico. El análisis de los resultados permitió establecer la comprobación de la hipótesis y formular conclusiones y recomendaciones.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de Resultados

4.1.1 Informático Provincial

Resultados de la encuesta realizada al Informático de la Dirección Provincial de Salud de Tungurahua:

La conexión a internet en la institución se realiza a través de un ADSL/Router, con una velocidad de 1024x512 kbps. El equipo utilizado como servidor de red tiene: procesador intel Pentium IV de 2.4 Ghz, 768 Mb de Memoria RAM y un disco duro de 80 Gb. No existe problema en cambiar el sistema operativo Windows XP por una distribución Linux. Existe total apertura para configurar tanto el servidor como los equipos utilizados para la conexión.

4.1.2 Funcionarios de la Institución

A continuación se presentan los resultados de la encuesta realizada a todos los funcionarios de la Dirección Provincial de Salud de Tungurahua:

¿Puede acceder a información de cualquier equipo de la red?

SI	NO
41	12

Tabla. 4-1. Tabulación de la Encuesta – Pregunta 1
Fuente: Investigación de campo
Elaborado por: Diego Silva

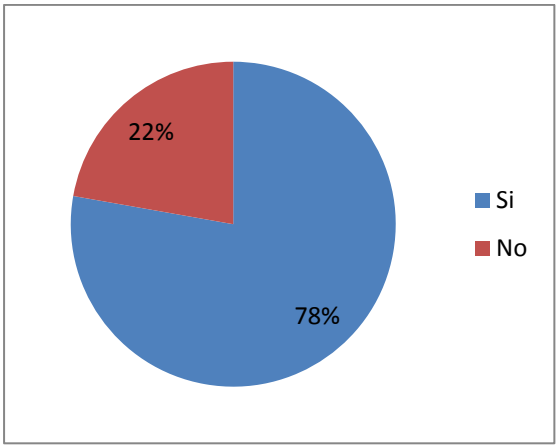


Fig. 4-1. Tabulación de la Encuesta – Pregunta 1
Fuente: Investigación de campo
Elaborado por: Diego Silva

El 78% de usuarios de la Institución tiene libre acceso a la información compartida de cualquier equipo de la red, lo que significa que todos los equipos son accesibles y están expuestos sin ningún tipo de protección tornándolos vulnerables.

¿Qué directorios comparte?

MIS DOCUMENTOS	C	D	OTROS
12	39	17	4

Tabla. 4-2. Tabulación de la Encuesta – Pregunta 2
Fuente: Investigación de campo
Elaborado por: Diego Silva

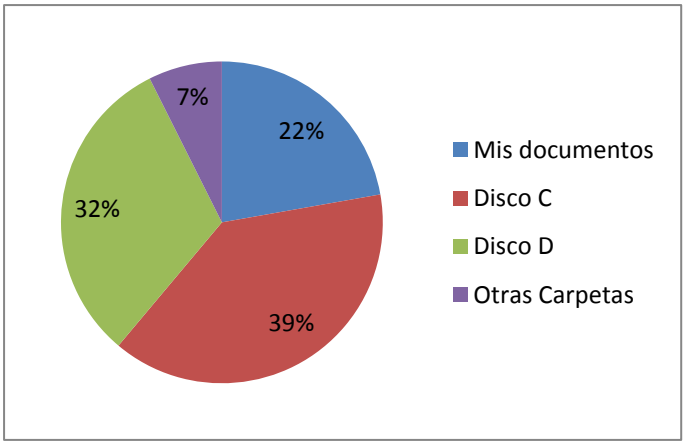


Fig. 4-2. Tabulación de la Encuesta – Pregunta 2
Fuente: Investigación de campo
Elaborado por: Diego Silva

Se puede observar que el 71% de usuarios comparten la raíz del disco duro, lo cual puede ocasionar daño o pérdida de datos, inestabilidad en el sistema operativo, fácil propagación de virus informáticos, también compromete la integridad de archivos al no destinar una sola carpeta para la compartición de los mismos.

¿Revisa el flash antes de abrirlo?

SI	NO
5	48

Tabla. 4-3. Tabulación de la Encuesta – Pregunta 3
Fuente: Investigación de campo
Elaborado por:Diego Silva

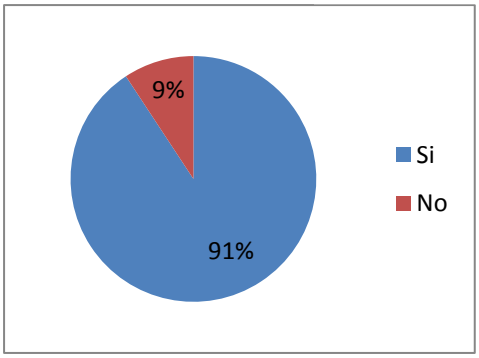


Fig. 4-3. Tabulación de la Encuesta – Pregunta 3
Fuente: Investigación de campo
Elaborado por: Diego Silva

Solamente el 9% de usuarios revisa el flash antes de abrirlo, por lo cual se torna fácil la propagación de virus informáticos.

¿Qué paginas visita?

GOBIERNO	PRENSA	CORREO	DESCARGAS	JUEGOS	REDES SOCIALES	PORNOGRAFIA
7	5	29	8	3	15	3

Tabla. 4-4. Tabulación de la Encuesta – Pregunta 4
Fuente: Investigación de campo
Elaborado por: Diego Silva

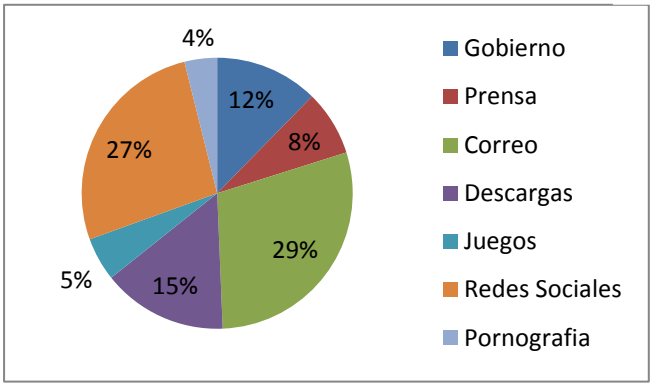


Fig. 4-4. Tabulación de la Encuesta – Pregunta 4
Fuente: Investigación de campo
Elaborado por: Diego Silva

La gráfica demuestra que la mayor parte de usuarios visitan su correo y las redes sociales, también se puede observar que se realizan descargas y se juega en línea, aunque en pequeño porcentaje se visitan sitios pornográficos a pesar que todo lo anterior no está permitido y no es parte del desempeño del trabajo de los funcionarios.

¿Abre correos electrónicos de remitentes desconocidos?

SI	NO
37	16

Tabla. 4-5. Tabulación de la Encuesta – Pregunta 5
Fuente: Investigación de campo
Elaborado por: Diego Silva

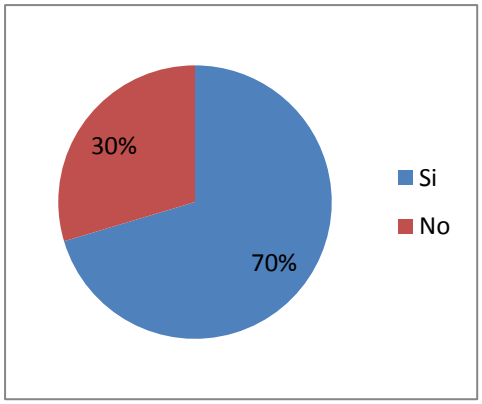


Fig. 4-5. Tabulación de la Encuesta – Pregunta 5
Fuente: Investigación de campo
Elaborado por: Diego Silva

La mayor parte de usuarios abren correos de remitentes desconocidos; esto conlleva a la posible descarga de virus e infección de los equipos al igual que las descargas de sitios desconocidos.

¿Con que frecuencia respalda sus archivos?

DIARIO	SEMANAL	MENSUAL	ANUAL	NUNCA
0	0	8	12	33

Tabla. 4-6. Tabulación de la Encuesta – Pregunta 6
Fuente: Investigación de campo
Elaborado por: Diego Silva

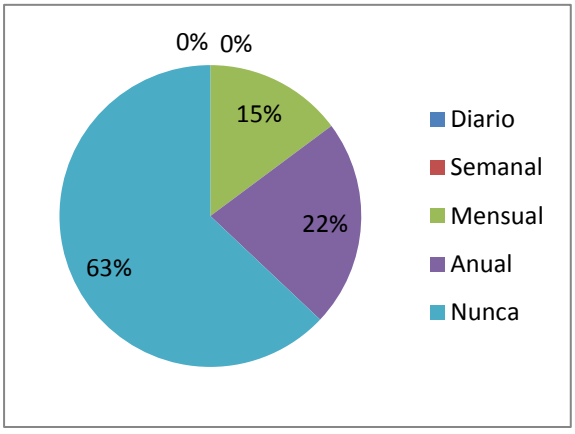


Tabla. 4-6. Tabulación de la Encuesta – Pregunta 6
Fuente: Investigación de campo
Elaborado por: Diego Silva

El 63% de los usuarios nunca realizan respaldos de sus archivos, por lo cual durante una infección o ataque de virus además de los daños causados al sistema pierden sus datos.

4.2 Verificación de la Hipótesis

En la presente investigación se utilizará para la verificación de hipótesis el estimador estadístico Chi-cuadrado que se maneja generalmente para determinar la relación entre variables cualitativas. En este trabajo se tienen variables netamente cualitativas por lo que se justifica la aplicación de éste estimador.

Chi-cuadrado se maneja como un estadígrafo de distribución libre que permite establecer la correspondencia de valores observados y esperados, permitiendo la comparación global del grupo de frecuencias a partir de la hipótesis que se quiere verificar. Además se pretende comprobar si los valores de las frecuencias obtenidos en las encuestas y registrados en la tabla de doble entrada son representativos.

4.2.1. HIPOTESIS.

Paso 1. Establecer la hipótesis nula y alterna

Luego de determinar el problema y realizada la investigación de campo, se procede a plantear la hipótesis con sus correspondientes variables que en este caso es:

La implementación de esquemas de seguridad solucionará los problemas de comunicación interna y hacia el Internet en la red de la Dirección Provincial de Salud de Tungurahua.

Variables

Para el cálculo de la verificación, se toma en cuenta dos variables de la hipótesis ya planteada:

Independiente: Esquemas de seguridad en la red

Dependiente: Problemas de comunicación interna y hacia el Internet

Determinación de Hipótesis

$\boldsymbol{H_O}$: La implementación de esquemas de seguridad **NO** solucionará los problemas de comunicación interna y hacia el Internet en la red de la Dirección Provincial de Salud de Tungurahua.

$\boldsymbol{H_a}$: La implementación de esquemas de seguridad solucionará los problemas de comunicación interna y hacia el Internet en la red de la Dirección Provincial de Salud de Tungurahua.

Paso 2. Nivel de Significancia y grados de libertad

Nivel de Significancia

El nivel de significancia con el que se trabajara es el 0.05 α = 5%

Dónde: α = nivel de significancia

Grados de Libertad

$$gl = (n-1)(m-1)$$
$$gl = (3-1)(3-1)$$
$$gl = (2)(2)$$
$$gl = 4$$

Dónde:

n = columnas

m = filas

gl = grados de libertad

$X_{\alpha}^{2} = 9{,}5$

El valor 9,5 que se refleja en la fila 4 columna 0,05 de la tabla de Distribución Chi cuadrada (X^2)

Paso 3. Determinar las frecuencias observadas y esperadas

A continuación se presenta la tabla de frecuencias observadas con los datos extraídos de las encuestas y agrupados por categorías; aplicadas a los usuarios de la red de la Dirección Provincial de Salud de Tungurahua, y en función de estas se calculó las frecuencias esperadas y por último Chi cuadrado (X^2).

Cuadro de frecuencias observadas

Las frecuencias observadas se detallan en la siguiente tabla:

PROBLEMAS DE COMUNICACIÓN INTERNA Y HACIA EL INTERNET	**APLICACIÓN DE ESQUEMAS DE SEGURIDAD**			
	¿El esquema de seguridad actual en la red ha sido?			
¿Cuáles han sido los aspectos más vulnerables y que han ocasionado problemas?	MUY BUENO	BUENO	REGULAR	**TOTAL**

Conexión a internet	3	14	37	54
Archivos	8	12	34	54
Infecciones de virus	1	6	47	54
TOTAL	12	32	118	162

Tabla. 4-7. Frecuencias Observadas
Fuente: Investigación de campo
Elaborado por: Diego Silva

Cuadro de frecuencias esperadas

Las frecuencias esperadas se detallan en la siguiente tabla:

PROBLEMAS DE COMUNICACIÓN INTERNA Y HACIA EL INTERNET	**APLICACIÓN DE ESQUEMAS DE SEGURIDAD**			
	¿El esquema de seguridad actual en la red ha sido?			
¿Cuáles han sido los aspectos más vulnerables y que han ocasionado problemas?	MUY BUENO	BUENO	REGULAR	**TOTAL**
Conexión a internet	4	10,67	39,33	**54,00**
Archivos	4	10,67	39,33	**54,00**
Infecciones de virus	4	10,67	39,33	**54,00**
TOTAL	**12**	**32**	**118**	**162,00**

Tabla. 4-8. Frecuencias Esperadas
Fuente: Investigación de campo
Elaborado por: Diego Silva

Paso 4. Calcular el estadístico de prueba

$$X^2 = \sum \frac{(f_e - f_o)^2}{f_e}$$

En donde:

X^2 = Chi cuadrado
Σ = Sumatoria
f_e = Frecuencias esperadas
f_o = Frecuencias observadas

Chi – cuadrado calculado X^2

Matriz de datos

PROBLEMAS DE COMUNICACIÓN INTERNA Y HACIA EL INTERNET	**APLICACIÓN DE ESQUEMAS DE SEGURIDAD**				
	¿El esquema de seguridad actual en la red ha sido?				
	VARIABLES		MUY BUENO	BUENO	REGULAR
	Conexión a internet	fo	3	14	37
		fe	4	10,67	39,33
¿Cuáles han sido los aspectos más vulnerables y que han ocasionado problemas?	Archivos	fo	8	12	34
		fe	4	10,67	39,33
	Infecciones de virus	fo	1	6	47
		fe	4	10,67	39,33

Tabla. 4-9. Matriz de Frecuencias
Fuente: Investigación de campo
Elaborado por: Diego Silva

Cálculo de X^2

Fo	Fe	fo-fe	(fo-fe)^2	x= (fo-fe)^2/fe
3	4,00	-1,00	1,00	0,25
14	10,67	3,33	11,11	1,04
37	39,33	-2,33	5,44	0,14
8	4,00	4,00	16,00	4,00
12	10,67	1,33	1,78	0,17
34	39,33	-5,33	28,44	0,72
1	4,00	-3,00	9,00	2,25
6	10,67	-4,67	21,78	2,04
47	39,33	7,67	58,78	1,49
			SUMA	12,11

Tabla. 4-10. Cálculo de chi cuadrado
Fuente: Investigación de campo
Elaborado por: Diego Silva

Dónde: fo = Frecuencias observadas

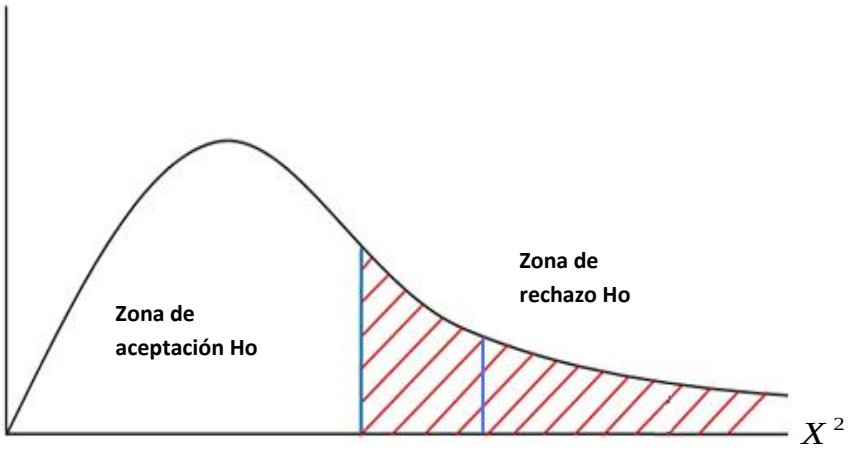
fe = Frecuencias esperadas

Paso 5. Tomar decisiones y concluir.

Regla de rechazo

Si $X^2 \geq X_\alpha^2$ se rechaza la hipótesis nula (Ho); es decir si el valor de Chi-cuadrado calculado es mayor que el valor crítico se rechaza la hipótesis nula.

Representación Estadística



$X_\alpha^2 = 9{,}5$ $X^2 = 12{,}11$

Fig. 4-7. Representación estadística de chi cuadrado
Fuente: Investigación de campo
Elaborado por: Diego Silva

Análisis e Interpretación

Una vez realizados los cálculos podemos notar que la regla de rechazo señala que se rechaza Ho si $X^2 \geq X_\alpha^2$, luego $12{,}11 \geq 9{,}5$; si cumple la condición por lo tanto se rechaza Ho.

4.2.2 Conclusión

Con el 95% de certeza, al 5% de error y con 4 grados de libertad se cumple la condición si $X^2 \geq X_\alpha^2$ entonces $12{,}11 \geq 9{,}5$ se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), por lo que "La implementación de esquemas de seguridad solucionará los problemas de comunicación interna y hacia el Internet en la red de la Dirección Provincial de Salud de Tungurahua."

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La estructura lógica de la red no es la adecuada, porque permite un libre acceso entre los equipos de los usuarios.
- El acceso a internet tiene un control muy básico, razón por la cual se pueden burlar fácilmente las reglas de control de acceso**.**
- El firewall de Windows que se maneja en el servidor de red, lo torna altamente vulnerable a ataques e infecciones de virus.
- No cuenta con un servidor de archivos, y los usuarios realizan la compartición de los mismos de forma incorrecta ocasionando problemas con pérdida de archivos, y también difusión de virus.
- El equipo servidor, no cuenta con las características necesarias para su desempeño óptimo, se encuentra obsoleto y además se lo utiliza para tareas extras tornándolo muy sobrecargado y lento.
- Al realizar descargas o actualización de antivirus el internet se torna muy lento, porque no existe un control en el consumo de ancho de banda.
- Se pueden realizar libremente descargas de cualquier tipo de archivo y realizar tareas como jugar y escuchar música en línea lo que provoca el consumo de todo el ancho de banda y por lo tanto una navegación lenta.
- No se cuenta con informes detallados sobre el consumo de ancho de banda y la navegación de los usuarios, lo que torna difícil la administración y la toma de decisiones.
- El servidor funciona sobre la plataforma Windows, a pesar que existe un decreto presidencial para la utilización de software libre en todas las instituciones públicas.

- Los equipos utilizados para la conexión en la red no cuentan con la seguridad necesaria, por lo cual resulta fácil burlarlo e ingresar a la red para navegar por internet.

5.2 Recomendaciones.

- Se recomienda implementar una nueva estructura lógica de la intranet.
- Es necesario adquirir un equipo que soporte la carga de servidor de red.
- Implementar un sistema operativo de software libre para cumplir con el decreto presidencial.
- Manejar un firewall que permita cumplir con las políticas de seguridad
- Configurar un servicio intermediario para la compartición de internet que permita implementar reglas de control de acceso para cumplir con las políticas de seguridad.
- Configurar un servidor de archivos para la compartición de los mismos en cada proceso de la institución.
- Administrar el ancho de banda para evitar una navegación lenta
- Limitar las descargas únicamente de archivos que realmente son necesarios.
- Presentar informes sobre las actividades realizadas en la red.
- Administrar y asegurar los equipos utilizados para la conexión de la intranet.
- Instalar un firewall en cada equipo de la institución para evitar conexiones no deseadas.

CAPITULO VI

PROPUESTA

6.1 Marco Teórico

6.1.1 Esquema de seguridad

Se conoce que el 70% de ataques de intrusiones o ataques en una red son del personal interno debido a que conoce los procesos y tiene acceso a la información sensible de la empresa, a todos aquellos datos cuya pérdida puede afectar al buen funcionamiento de la organización. Esta situación se presenta a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas. Esto se debe a que cada empresa es un mundo distinto, con diferentes requerimientos, usuarios, arquitectura de red, velocidad de conexión, equipos de conexión y otros que se pueden seguir nombrando.

En la exposición latente del área de informática al internet, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Específicamente, en los ataques de negación de servicio, los equipos ya no son un blanco, es el medio a través del cual es posible afectar todo “El entorno de red”; es decir, anular los servicios de la red, inundar el ancho de banda o alterar los sitios Web de la empresa, así que es evidente que los riesgos están en la red, no en las estaciones de trabajo.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

6.1.2 Políticas de Seguridad

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

6.1.3 Subneting

Se eligió realizar el subneting con VLSM (Máscara de subred de tamaño variable), los procesos tienen un número de equipos irregular, por lo cual existiría exceso de desperdicio de direcciones IP al utilizar un subneteo de mascara fija. Con VLSM se optimiza el subneteo, asignando las direcciones IP necesarias con una holgura para proyección de crecimiento de equipos por cada proceso.

Es conocido que al realizar un subneting cada subred se ve como una red distinta lo cual nos ayuda a cumplir con una política de seguridad evitando de esta manera que los equipos de distintos procesos puedan verse entre sí.

6.1.4 Servidor

Es un equipo que se encuentra conectado en red y provee de servicios a otros equipos denominados clientes.

6.1.4.1 Sistema Operativo

Un Sistema Operativo es el software encargado de ejercer el control y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de hardware del sistema.

Las funciones básicas del Sistema Operativo son administrar los recursos de la máquina, coordinar el hardware y organizar archivos y directorios en dispositivos de almacenamiento.

Los Sistemas Operativos más conocidos son DOS, Windows, Linux y Mac.

Linux

Linux es un núcleo (también denominado Kernel) de sistema operativo libre tipo Unix. Es uno de los principales ejemplos de software libre y código abierto. Linux está desarrollado por colaboradores de todo el mundo.

Distribuciones

Una distribución Linux es un conjunto de software acompañado del núcleo Linux que se enfoca a satisfacer las necesidades de un grupo específico de usuarios. De este modo hay distribuciones para hogares, empresas y servidores. Cada distribución se distingue por incorporar software y soporte extra.

CentOS

CentOS es una distribución de Linux basada en los fuentes libremente disponibles de Red Hat Enterprise Linux. Cada versión de CentOS es mantenida durante 7 años (por medio de actualizaciones de seguridad). Las versiones nuevas son liberadas cada 2 años y actualizadas regularmente (cada 6 meses) para el soporte de hardware nuevo.

6.1.5 Formas de Protección

Básicamente existen tres maneras de protegerse de los peligros que se corren al conectarse a Internet:

La primera y la más obvia es estar desconectados de internet. Es la más segura, pero se puede encontrar con un problema aún mayor; pues para los usuarios de la institución es indispensable conectarse a internet y van a buscar la manera pudiendo utilizar sus módems y configurar sus propios accesos, dejando abiertos los equipos a ataques de los cuales nunca se va conocer.

La segunda opción que es la más usada y recomendable es configurar una conexión a internet a través de un servidor intermediario que recibe las peticiones de acceso de todos los clientes y se conecta a internet para descargar la solicitud y la regresa al cliente. Este mismo actúa como firewall y filtro permitiendo un mayor control sobre las actividades realizadas en internet.

La última opción es dar a cada cliente acceso ilimitado hacia internet, de esta manera es el cliente quien se preocupa de la protección de su equipo. Esto lo realizan los proveedores de internet, donde los usuarios requieren acceso sin restricción alguna.

6.1.6 Firewall

Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. 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.

Un firewall es la combinación de componentes que implementan y hacen cumplir las políticas de seguridad. Y como cada empresa tiene diferentes políticas de seguridad tendrán también diferente firewall; las políticas de seguridad dictaminan como el firewall debe comportarse. Puede actuar como Router filtrado con zonas desmilitarizadas o protegidas, como servidor de sockets, proxy, puerta de enlace para mail, servidor DNS, dispositivo de túnel, como traslador de direcciones de red o enmascaramiento IP.

Lo que el firewall no puede proteger es: el abuso de conexiones permitidas, usuarios maliciosos, datos en tránsito en internet, conexiones que no pasen por el firewall, conexiones a sistemas que se encuentren fuera del firewall y por ultimo daños o robos físicos.

6.1.7 Iptables

Un firewall puede ser hardware o software con dos o más interfaces de red, protege las conexiones entrantes y salientes, decide si un paquete pasa, se modifica, se convierte o se descarta.

Iptables viene incluido en el núcleo de Linux y básicamente lo que hace es interceptar y manipular paquetes de red, filtra paquetes y también se encarga del NAT (Traducción de Direcciones de Red). Iptables se encuentra cargado en memoria y a través de esta se crean reglas para cada filtrado de paquetes y módulos de NAT.

Se puede implementar el firewall estableciendo políticas por defecto:

- **Aceptar**: Es fácil de implementar pero peligroso en seguridad
- **Denegar**: Difícil de implementar, pero muy seguro

El orden en que se establecen las reglas es determinante; una vez que entra un paquete, es comparado en orden con cada regla hasta que encuentra un match o coincidencia, hace lo que diga la regla y después de eso no se chequearan más reglas.

Al entrar un paquete al firewall cumple con el siguiente diagrama de flujo:

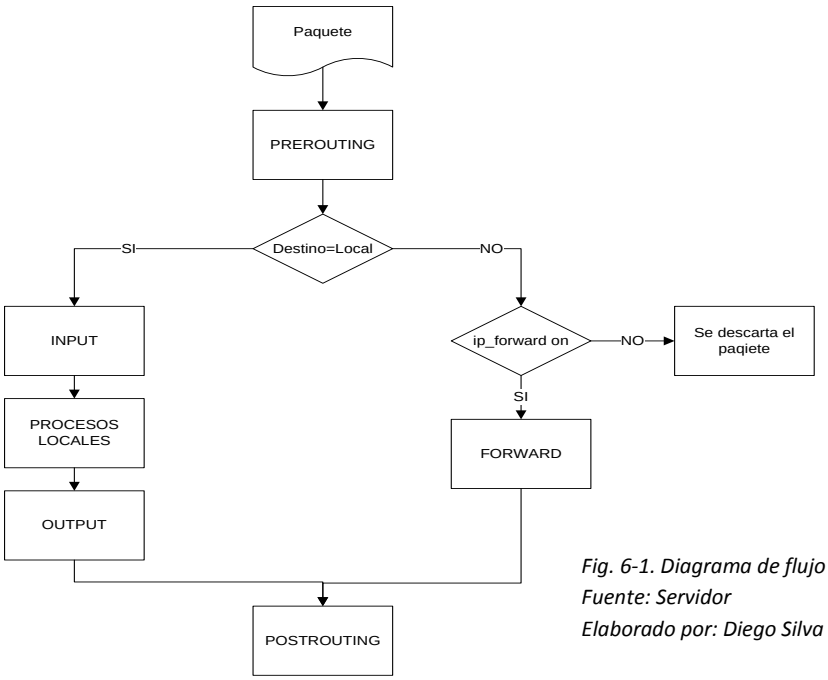


Fig. 6-1. Diagrama de flujo de iptables
Fuente: Servidor
Elaborado por: Diego Silva

Este es uno de los aspectos más importantes en la configuración del servidor, porque de este dependerá el nivel de seguridad y acceso a la red, por esto es imprescindible conocer bien qué servicios se ejecutaran, y que puertos utilizaran para comunicarse.

6.1.8 Servidor Proxy

Para poder brindar el servicio de internet a todos los usuarios de la institución cumpliendo con las políticas establecidas, es necesaria la configuración de un servicio intermediario, de tal manera que se pueda administrar y controlar estos accesos, además de definir reglas que ayuden a cumplir las políticas.

Un servidor intermediario escucha a través de un puerto peticiones de acceso a internet, el servidor proxy se conecta al servidor de internet y descarga la solicitud, finalmente devuelve al cliente lo requerido.

Hay varias alternativas en Linux para configurar este servicio:

Apache: Además de ser un servidor web, también tiene la alternativa de cargar un modulo para proporcionar el servicio intermediario de internet, se puede combinar y hacerlo un servidor web/proxy

Squid: es un exclusivo servidor proxy para http y ftp, que permite además realizar cache tiene una configuración muy amplia.

TIS firewall toolkit: ofrece varios servidores proxy como para telnet, ftp, gopher entre otros

La mejor alternativa es utilizar squid, por su amplia configuración y opciones que cuenta, además que es orientado exclusivamente a ser un servidor intermediario para internet.

6.1.8.1 Squid

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

6.1.8.2 SARG – Reporte de Actividades de Squid

SARG (Squid Analysis Report Generator) es la herramienta más completa y fácil de usar para la generación de reportes a partir de los logs de Squid. Permite ver con detalle la actividad de todos los equipos y/o usuarios dentro de la red de área local, registrada en la bitácora de Squid.

6.1.9 Compartición de archivos

Para el usuario es importante compartir ciertos archivos dentro de sus procesos, y poder utilizarlos posteriormente desde otros clientes. En la institución la mayor parte de equipos utilizan el sistema operativo en la plataforma Windows, aunque existen también a más del servidor equipos con el sistema operativo Linux. Para el cliente no importa el sistema operativo con que se encuentre trabajando debe ser transparente el uso de un recurso de red.

6.1.9.1 Samba

Es una implementación libre del protocolo de archivos compartidos de Microsoft Windows para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio, como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autentificar con su propio archivo de usuarios.

6.1.10 Limitación del ancho de banda con CBQ (Class Based Queueing o Encolamiento Basado Sobre Clases)

Es un guion escrito en bash utilizado para la gestión y control del uso de ancho de banda sobre Linux. Utiliza de una forma simplificada los mandatos ip y tc para su funcionamiento y forma parte del paquete iproute.

6.1.10.1 Velocidad Binaria (BIT RATE)

Es la velocidad de transferencia de datos. Se refiere a la tasa, al flujo o número de bits que se transmiten por segundo a través de un sistema de transmisión digital o entre dos dispositivos digitales. La velocidad con la que se expresa es el bit por segundo y se representa como: bit/s, b/s, bps siempre en minúscula para evitar confusión con Byte.

6.1.10.2 Pasos Previos

Los ficheros con las configuraciones se guardan dentro del directorio /etc/sysconfig/cbq y deben llevar la siguiente nomenclatura:

/etc/sysconfig/cbq/cbq-[numero-ID-Clase].[nombre]

Dónde:

[numero-ID-Clase] → numero hexadecimal entre 0002 y FFFF que es el que identifica a la clase

[nombre] → un nombre asignado para esa clase

6.1.10.3 Parámetros de los ficheros de configuración

Ahora debemos entender los valores para los distintos parámetros necesarios para construir una regla:

Device Es un parámetro obligatorio. Se determina los valores con el nombre de la interfaz, ancho de banda y peso de esta interfaz. Este último valor, que es opcional en este parámetro, se calcula dividiendo el ancho de banda de la interfaz entre diez. Nuestra conexión al ADSL trabaja a 1024 Kbps de bajada conectado a eth0, por lo tanto DEVICE quedaría así:

```
DEVICE=eth0,1024Kbit,102Kbit
```

Rate Es un parámetro obligatorio. Se refiere al ancho de banda a asignar a la clase. El tráfico que pase a través de esta clase será modificado para ajustarse a la proporción definida. Si se desea limitar a 512 kbit/s

```
RATE=512Kbit
```

Weight

Es un parámetro obligatorio. Éste es proporcional al ancho de banda total de la interfaz. Como regla se calcula dividiendo entre diez el ancho de banda total. Para la interfaz de 1024kbps, correspondería un valor de 102Kbit

```
WEIGHT=102Kbit
```

Prio Es un parámetro opcional que se utiliza para especificar que prioridad tendrá sobre otras reglas de control de ancho de banda. Mientras más alto sea el valor, menos prioridad tendrá sobre otras reglas. Se recomienda utilizar el valor 5 que funcionará para la mayoría de los casos

PRIO=5

Parámetros de filtración Son las reglas de filtración que se utilizan para seleccionar tráfico en cada una de las clases. La sintaxis completa es la siguiente, donde todos los valores son opcionales, pero se debe especificar al menos uno:

RULE=IP-origen:puerto-origen,IP-destino:puerto-destino

Por ejemplo si se desea filtrar lo que sale desde la red local al puerto 1494

RULE=192.168.43.0/24,:1494

6.1.11 Monitoreo de actividades con CACTI

CACTI es una completa herramienta de solución grafica de red para aprovechar el poder de almacenamiento de datos y graficas de RRDTool's. Provee un rápido encuestador, plantillas de gráficos avanzadas, múltiples métodos de adquisición de datos, y características de administración avanzadas. Presenta una interfaz sencilla que puede abarcar varias interfaces de grandes redes.

Es un front-end de RRDTool's manejado por php, que almacena toda la información en una base de datos mysql, permite la configuración de presentación de los gráficos, permite manejo de usuarios para configuración y visualización de la información.

Anteriormente, se había propuesto, la utilización de MRTG para visualizar el tráfico de la red, pero esta herramienta ofrece muchas más funcionalidades.

6.1.12 Clamav Antivirus

Los antivirus nacen con la necesidad de eliminar programas que causaban daño tanto en el sistema operativo como en los archivos almacenados. Con el pasar del tiempo y la evolución del internet y los sistemas operativos ha evolucionado también la forma de infección de los virus; así como los programas antivirus que ahora no solo buscan virus sino tratan de bloquearlos, desinfectarlos, evitar su propagación, utilizando varias técnicas de inteligencia artificial.

En día los antivirus no solo buscan en una lista incorporada sino analizan el comportamiento de estos programas o las comunicaciones que pueden causar daño al equipo.

Clamav es uno de estos programas antivirus libre y de código fuente abierto, que tiene la capacidad de detectar más de 720 mil virus, gusanos, troyanos y otros programas maliciosos, pudiendo examinar incluso archivos comprimidos, tiene exploración rápida y su actualización de firmas digitales no es muy pesada.

6.1.13 Firewall y antivirus COMODO

Es una edición libre de un completo firewall, donde podemos establecer las reglas necesarias para el control del tráfico y filtrado de la red, además de la ejecución de procesos en el sistema. Tiene un ambiente muy amigable y fácil de utilizar. Luego de instalado el producto este va aprendiendo en base a preguntas acerca de los procesos y las conexiones que se establecen con el equipo; permitiendo el control y manteniendo al equipo seguro.

Cuenta también con un módulo de antivirus muy eficiente capaz de reconocer y eliminar amenazas, o ponerlas en cuarentena si es necesario, además que trabaja conjuntamente con el firewall y no pone en alerta en caso de que alguna aplicación este tratando de ejecutarse en memoria o cambiar algún registro sin autorización previa.

6.1.14 Access Point

Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena normalmente se colocan en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

6.1.14.1 Access Points DWL-3200AP

Este es un poderoso, robusto y fiable Access Point para operar en entornos de empresas con diversos negocios. Diseñado para instalaciones Indoor, este Access Point provee opciones

avanzadas de seguridad para los administradores de red, permitiendoles desplegar una administración muy robusta en redes wireless. El Access Point DWL-3200AP soporta Power Over Ethernet (PoE) y provee dos antenas de alta ganancia para una óptima cobertura wireless.

Principales Características y Facilidades:

- Soporte de Multiples SSID's
- Soporte 11g, 108Mbps Modo Turbo
- Robusto Access Point para soluciones Indoor
- Soporte de PoE (Power over Ethernet), 802.3af
- Soporte WEP,
- Soporte WPA, AES y 802.11i
- Seguridad Ampliada, con soporte de ACL, 802.1x y MAC Address Filtering
- Administración versátil, vía D-Link D-View, SNMP v3, Web, Telnet y AP Manager.

6.2 Desarrollo

6.2.1 Esquema de Seguridad

Para la institución, se implementará el siguiente esquema:

- Establecimiento de políticas de seguridad
- Subneteo de la red
- Instalación de servidor de red sobre la plataforma Linux
  - » Configuración básica
    - ✓ BIOS
    - ✓ Claves de acceso
    - ✓ Inhabilitación de servicios
    - ✓ Ocultación de información importante
    - ✓ Tiempo de inactividad
  - » Configuración de Firewall
  - » Servidor Proxy
    - ✓ Monitoreo
  - » Servidor Samba
  - » Administración de ancho de banda
  - » Monitoreo de Red

- Antivirus

- Configuración de acceso en los equipos de conexión
- Instalación de Firewall y antivirus en los equipos de la institución

6.2.2 Políticas de Seguridad y acceso a la red

- Todos los usuarios de la Institución tienen acceso a internet con los equipos asignados para su trabajo
- Los usuarios de cada proceso podrán ver sus equipos y compartir archivos entre sí, mas no con los usuarios de otros procesos
- Se implanta subneting en la intranet, con una holgura de crecimiento de equipos por cada proceso
- No está permitido ingresar a sitios web de pornografía, farándula, entretenimiento, redes sociales, y otras que no sean de utilidad para el trabajo en el cargo y proceso designado
- Está prohibido la realización de descargas de música, video y otros tipos de archivo sin antes notificar al subproceso de informática
- El proceso de contabilidad tendrá acceso además por el puerto 1494 que utiliza la aplicación con Citrix
- La actualización de firewall y antivirus será limitada en el ancho de banda
- Se determinará que usuarios y procesos utilizan mayor ancho de banda para su trabajo; pudiendo ser limitados
- Se emitirán informes sobre el acceso a sitios web y el uso de ancho de banda.
- Queda abierta la posibilidad de conectarse a la intranet con equipos que cuenten con conexión inalámbrica con previo aviso al subproceso de informática para su inclusión.
- Los equipos utilizados para la conexión de la intranet, contaran mínimo con una clave WAP para su acceso

6.2.3 Esquema Lógico de la red.

A continuación se detalla en la imagen el esquema lógico de la red, en el cual se puede observar la conexión a internet que será controlada y compartida por el servidor proxy, el mismo que se conecta a la intranet para controlarla a través de un firewall; observamos que a la intranet también se conectan los AP que son utilizados para la conexión en algunos equipos de escritorio y portátiles de la institución.

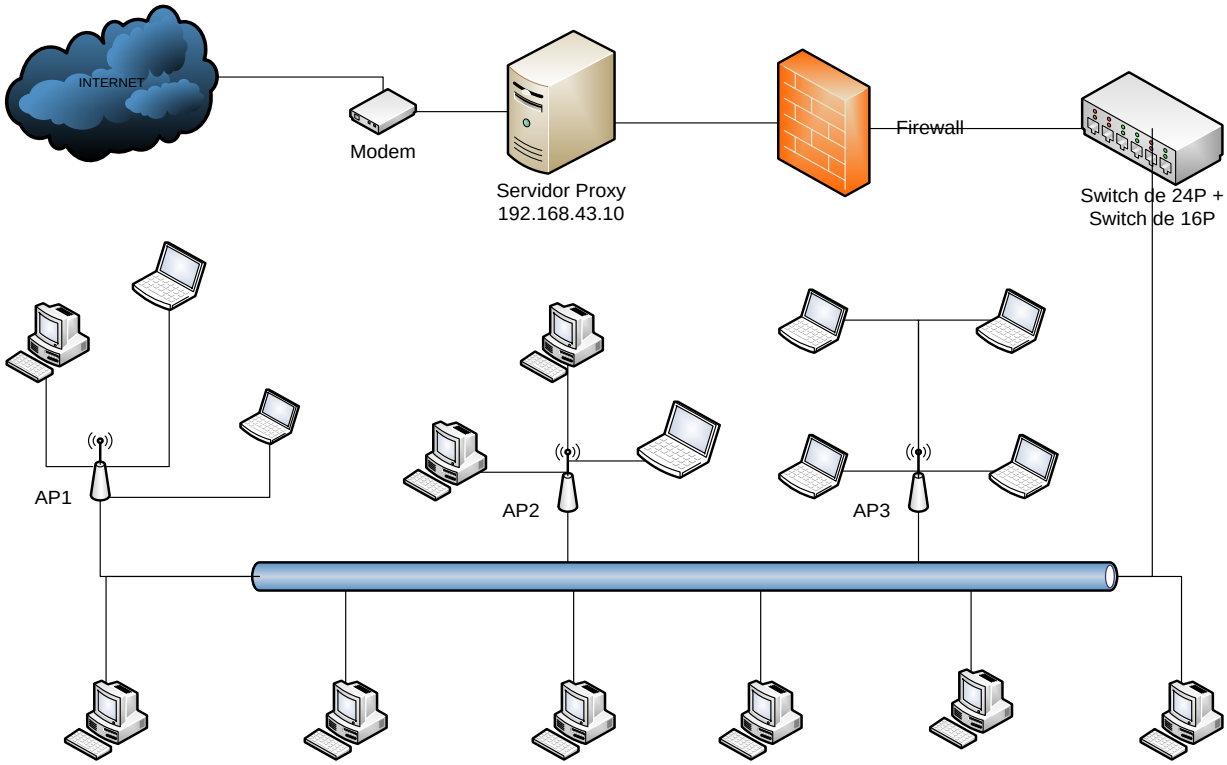


Fig. 6-2. Esquema de la red Institucional
Fuente: Informático Provincial
Elaborado por: Diego Silva

A continuación se presenta el número de equipos por cada subproceso, para determinar las subredes:

No.	PROCESO	No. Equipos	Crecimiento	IPs Requeridas
1	Informática	18	10	28
2	Auditorio (DHCP)	30	0	30
3	Implantación de la Norma	19	10	29
4	Gestión Financiera	8	5	13
5	Aseguramiento de la Calidad	5	5	10
6	Servicios Institucionales	6	5	11
7	Recursos Humanos	6	5	11
8	Vigilancia Sanitaria	5	5	10
9	Gobernante	4	5	9
10	Oferta y Demanda	4	5	9
11	Epidemiología	6	5	11
12	Comisaria de la Salud	2	5	7
13	Asesoría Jurídica	1	5	6

Tabla. 6-1. Equipos por proceso
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

La asignación de la subred junto con el Broadcast, la máscara, su prefijo y las direcciones IP disponibles por cada proceso queda determinada de la siguiente manera:

No.	PROCESOS	Subred	Broadcast	Mascara	Prefijo	Disponibles
1	Informática	192.168.43.0	192.168.43.31	255.255.255.0	24	30
2	Direccionamiento DHCP	192.168.43.32	192.168.43.63	255.255.255.224	27	30
3	Implantación de la Norma	192.168.43.64	192.168.43.95	255.255.255.224	27	30
4	Gestión Financiera	192.168.43.96	192.168.43.111	255.255.255.240	28	14
5	Aseguramiento de la Calidad	192.168.43.112	192.168.43.127	255.255.255.240	28	14
6	Servicios Institucionales	192.168.43.128	192.168.43.143	255.255.255.240	28	14
7	Recursos Humanos	192.168.43.144	192.168.43.159	255.255.255.240	28	14
8	Vigilancia Sanitaria	192.168.43.160	192.168.43.175	255.255.255.240	28	14
9	Gobernante	192.168.43.176	192.168.43.191	255.255.255.240	28	14
10	Oferta y Demanda	192.168.43.192	192.168.43.207	255.255.255.240	28	14
11	Epidemiologia	192.168.43.208	192.168.43.223	255.255.255.240	28	14
12	Comisaria de la Salud	192.168.43.224	192.168.43.239	255.255.255.240	28	14
13	Asesoría Jurídica	192.168.43.240	192.168.43.247	255.255.255.248	29	6

Tabla. 6-2. Asignación de subredes por proceso
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Una vez que han sido asignadas las subredes, se procede a la asignación de IPs para cada equipo dentro de la institución.

Proceso	Informática		
Subred	192.168.43.0 / 24		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Sw Principal (D-Link)	192.168.43.1	Swdlink	
Ap Acces Point 1	192.168.43.2	apdlink 1	
Ap Acces Point 2	192.168.43.3	apdlink 2	
Ap Acces Point 3	192.168.43.4	apdlink 3	
Ap Acces Point 4	192.168.43.5	apdlink 4	
Es Srv Proxy Firewall	192.168.43.10	proxy.dpst	
Es Srv Antivirus	192.168.43.11	Srvantivirus	
Es Respaldo	192.168.43.12	Infdpst3	
Es Srv Proxy Firewall (Anterior)	192.168.43.13	infdpst2	
Es Srv Oracle (Servidor Dell)	192.168.43.14	Srvoracle	
Po HP	192.168.43.15	infdpst1	Ing. Oscar Llerena
Po HP Nueva	192.168.43.16	Infdpst2	Ing. Oscar Llerena
Observaciones: Las direcciones desde la 1 hasta la 9 son designadas para equipos de conexión, a partir de la 10 se designan los equipos, las restantes serán utilizadas para pruebas y mantenimiento de equipos.			

Tabla. 6-3. Asignación de IPs para informática
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Implantación de la Norma		
Subred	192.168.43.64 / 27		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es Coordinación	192.168.43.65	impnorc001	Dra. Lourdes Silva
Es Normalización	192.168.43.66	Impnorc002	
Po Normatización	192.168.43.79	dpstnorpo01	Dra. Lourdes Silva
Subproceso de Estomatología			
Es Estomatología	192.168.43.67	Impest	Dra. Clemencia Bosques
Subproceso de Vacunas			
Es Vacunas 1	192.168.43.68	ImpnorEnf	Lic. Martha Sánchez
Es Vacunas 2	192.168.43.69	IMPNORVAC	Jorge Mora
Es Lupita	192.168.43.80	Impnorvac	Lic. Guadalupe Cuello
Po Hp Compaq PAI	192.168.43.81	Impnorpaipo	Lic. Martha Sánchez
Subproceso de Nutrición			
Es Nutrición 1	192.168.43.70	Nut01	Dr. Fausto Pasochoa
Es Nutrición 2	192.168.43.71	nut02	Ing. Carla Barrionuevo
Subproceso de UMSET			
Es Umset 1	192.168.43.72	UMSET01	Lic. Lorena Gavilánez
Es Umset 2	192.168.43.73	UMSET02	
Es Umset 3	192.168.43.74	UMSET03	
Subproceso de Educación para la Salud			
Es Educación 1	192.168.43.75	impnores01	Dr. Iván Núñez
Es Educación 2	192.168.43.76	Impnores02	Sr. Ramiro Rodríguez
Subproceso de Salud Intercultural			
Es Salud intercultural 3	192.168.43.77	salind03	Dra. Marcia Masaquiza
Es Salud intercultural 4	192.168.43.78	salind04	Dra. Marcia Masaquiza
Es Salud intercultural 1	192.168.43.82	salin01	Dra. Marcia Masaquiza
Es Salud intercultural 2	192.168.43.83	salin02	Lic. Rosa Pucha

Tabla. 6-4. Asignación de IPs para implantación de la Norma
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Gestión Financiera		
Subred	192.168.43.96 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es coordinación	192.168.43.97	Gesfincoor	Dra. Grecia Paredes
Es Secretaria	192.168.43.98	Gesfinsec	Ing. Elizabeth Aguilar
Po Toshiba	192.168.43.99	gesfinpo01	Dra. Grecia Paredes
Administración de Caja			
Es Caja	192.168.43.100	Gesfintes	Dra. Norma Yánez
Gestión de Presupuesto y Contabilidad			
Es contabilidad	192.168.43.101	gesfincon1	Dra. Emma Sánchez
Es Presupuesto	192.168.43.102	gesfincon2	Sra. Gladys Vaca
Es Nomina 02	192.168.43.104	Gesfinnomina	Ing. Fernando Meza
Observaciones: Estos equipos utilizan el Citrix para una aplicación financiera gubernamental			

Tabla. 6-5. Asignación de IPs para Gestión Financiera
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Aseguramiento de la Calidad		
Subred	192.168.43.112 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es Coordinación	192.168.43.113	Asecalcoo	Dra. Myriam Mejía
Es Auxiliar	192.168.43.114	Asecalaux	Ing. Patricio Carrillo
Es Coordinación 2	192.168.43.118	Asecal01	Dra. Pamela Medina
Po HP Pavilion	192.168.43.117	AsecalPo	Dra. Pamela Medina

Tabla. 6-6. Asignación de IPs para Aseguramiento de la Calidad
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Servicios Institucionales		
Subred	192.168.43.128 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es Coordinación	192.168.43.129	Serinscoor	Ing. Paulina Terán
Es Proveeduría	192.168.43.130	Serinspro	Dra. Anita Fiallos
Es Inventarios	192.168.43.131	Serinsinv	Ing. Juan Carrión
Es Bodega	192.168.43.132	Serinsbod	Sr. Nicolás Calle
Es Mantenimiento	192.168.43.133	Serinsman	Sr. José Freire

Tabla. 6-7. Asignación de IPs para Servicios Institucionales
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Recursos Humanos		
Subred	192.168.43.144 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es coordinación	192.168.43.145	Rechumcoor	Ing. Alicia Sánchez
Es Secretaria	192.168.43.146	Rechumsec	Ing. Mónica Estupiñan
Es auxiliar	192.168.43.147	Rechumaux	Ing. Carola Aldaz
Es archivo 1	192.168.43.148	Rechumexp	Ing. Ximena Castro
Es archivo 2	192.168.43.149	Rechumpas	Pasantes
Es Auxiliar	192.168.43.150	rechumaux2	Pasantes

Tabla. 6-8. Asignación de IPs para Recursos Humanos
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Vigilancia Sanitaria		
Subred	192.168.43.160 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es coordinación	192.168.43.161	Cvscoor	Dr. Richard Flores
Es Secretaria	192.168.43.162	Cvssec	Lic. Irma Sánchez
Es CVS 1	192.168.43.163	CVSME	Dr. Mauricio Núñez
Es Permisos	192.168.43.164	CVSPER	Dr. Pliño Peñafiel
Po Dell	192.168.43.165	CVS01	Dr. Francisco Portero

Tabla. 6-9. Asignación de IPs para Vigilancia Sanitaria
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Gobernante		
Subred	192.168.43.176 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es Secretaria	192.168.43.177	GOBSEC	Sra. Margarita Parra
Es Despacho	192.168.43.178	GOBDIR	Dra. María de Lourdes Freire
Po Toshiba	192.168.43.179	GOBPO01	Dra. María de Lourdes Freire
Po HP Pavilion	192.168.43.180	GOBPO02	Dra. María de Lourdes Freire

Tabla. 6-10. Asignación de IPs para Gobernante
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Oferta Demanda		
Subred	192.168.43.192 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Po HP Pavilion Coordinación	192.168.43.193	ofedempor01	Dr. Antonio Orquera
Es Secretaria	192.168.43.194	Ofedemsec	Tlga. Myriam Aguilar
Es Enfermería	192.168.43.195	Ofedemenf	Lic. Gloria Ramírez
Po HP Pavilion	192.168.43.196	ODDPST03	Lic. Gloria Ramírez

Tabla. 6-11. Asignación de IPs para Oferta Demanda
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Epidemiología		
Subred	192.168.43.208 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Po Nueva HP Compaq	192.168.43.214	epipor02	Lic. Liliana Aguirre
Es Coordinación	192.168.43.209	Dpstepicoor	Dr. Francisco Lozada
Es Epidemiología 1	192.168.43.210	Dpstepienf	Lic. Liliana Aguirre
Es Epidemiología 2	192.168.43.211	Dpstepiaux	Lic. Mónica Arias
Es Epidemiología 3	192.168.43.212	Dpstepi04	Dr. Francisco Lozada
Po Epidemiología	192.168.43.213	Epipor01	Dr. Francisco Lozada

Tabla. 6-12. Asignación de IPs para Epidemiologia
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Comisaria de la Salud		
Subred	192.168.43.224 / 28		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es Comisario	192.168.43.224	Comsal01	Dr. Favio Miranda
Es Secretario	192.168.43.225	Comsal02	Dr. Mauricio López

Tabla. 6-13. Asignación de IPs para Comisaria de la Salud
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

Proceso	Asesoría Jurídica		
Subred	192.168.43.240 / 29		
EQUIPOS	**IP**	**NOMBRE DEL EQUIPO**	**USUARIO**
Es Asesor jurídico	192.168.43.242	dpstaj02	Dr. Fernando Galarza

Tabla. 6-14. Asignación de IPs para Asesoría Jurídica
Fuente: Inventario de Equipos
Elaborado por: Diego Silva

6.2.4 Características del Servidor

6.2.4.1 Hardware

Se adquirió un equipo con las siguientes características:

- Mainboard Intel DG35EC
- Procesador Intel CORE 2 QUAD 2.8 Ghz Arquitectura de 64 bits
- Memoria RAM 8 GB (4 memorias de 2 GB)
- Disco Duro sata de 500 GB
- Tarjeta de red incorporada 10/100/1000
- Tarjeta de red 10/100/1000 para arquitectura 64 bits
- DVD/RW
- Lector de Tarjetas

6.2.4.2 Software

Sistema Operativo

Se eligió la distribución de software libre Linux CentOS 5.3 de 64 bits que es una distribución derivada del código liberado por Red Hat la misma que anteriormente era pagada que al igual que otras distribuciones Linux tiene prestaciones muy importantes y útiles que ayudaran al desempeño del trabajo, y que se acopla perfectamente a las características del equipo.

Instalación de CentOS

Una vez instalado físicamente el equipo, se procede al encendido; insertar el disco de instalación y hacer que el equipo arranque desde el mismo, después de iniciado el instalador identifica los dispositivos del equipo y se presenta una pantalla donde se debe dar un enter para iniciar el proceso de instalación.

Se puede apreciar la pantalla de presentación y dar clic en siguiente

Fig. 6-3. Bienvenida de instalación de Centos
Fuente: Servidor
Elaborado por: Diego Silva

Elegir el idioma que se va a utilizar durante el proceso de instalación y siguiente

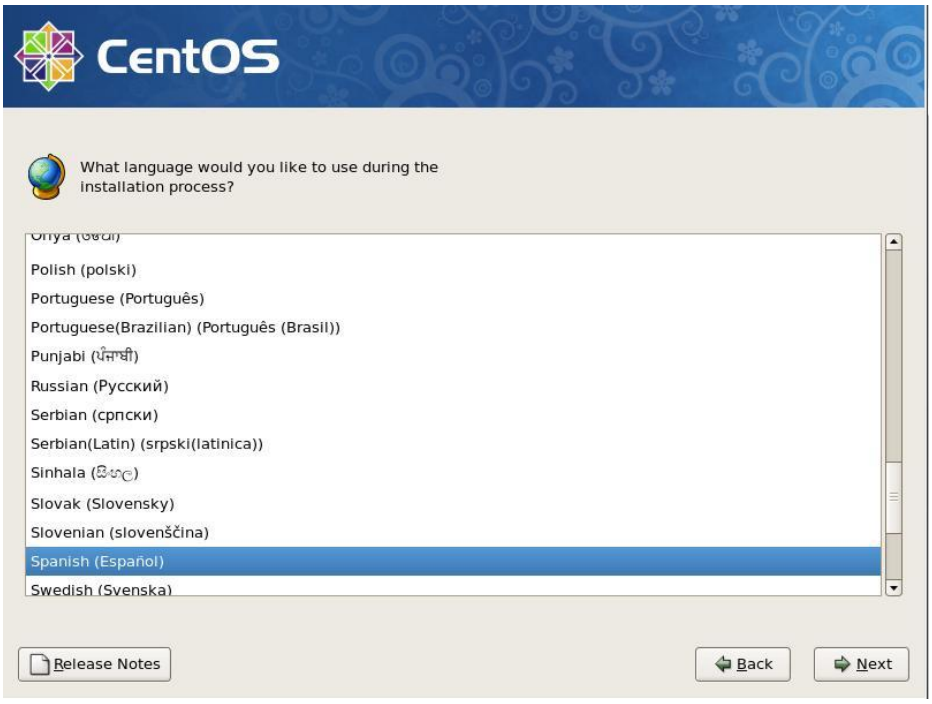


Fig. 6-4. Elegir Idioma de instalación
Fuente: Servidor
Elaborado por: Diego Silva

Elegir el idioma de instalación

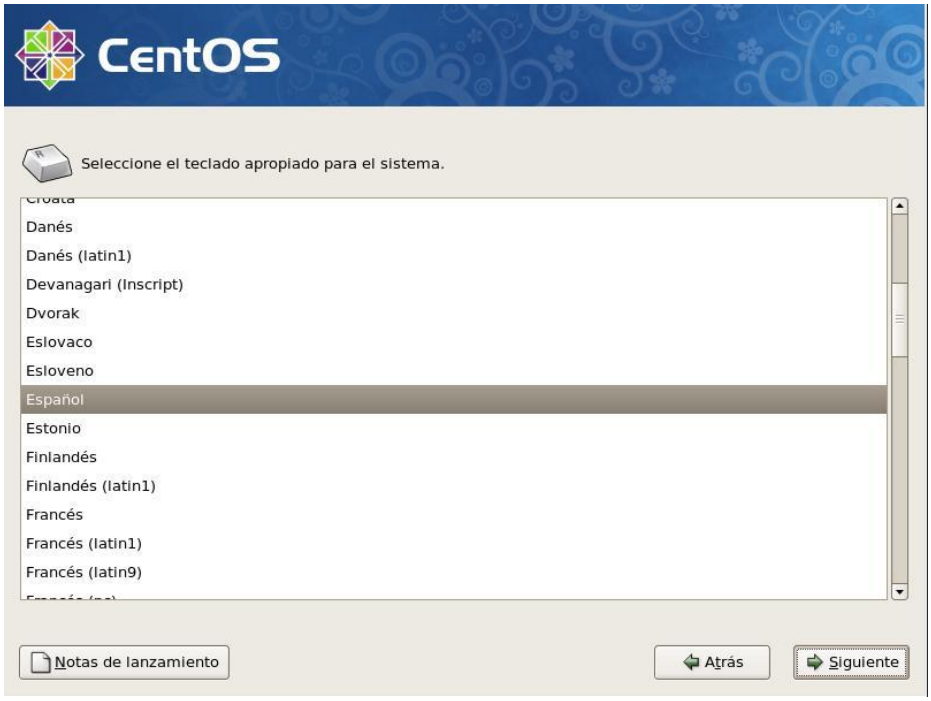


Fig. 6-5. Idioma del sistema
Fuente: Servidor
Elaborado por: Diego Silva

A continuación un punto muy importante que es la elección de la partición del disco, elegir un diseño predeterminado y marcar la casilla de modificación de la capa de particiones

Fig. 6-6. Particionamiento del disco
Fuente: Servidor
Elaborado por: Diego Silva

Se crea una partición swap que es igual al doble de la memoria RAM, una partición de 100 Mb para boot y una partición ext3 en la raíz con el resto de espacio en el disco; siguiente

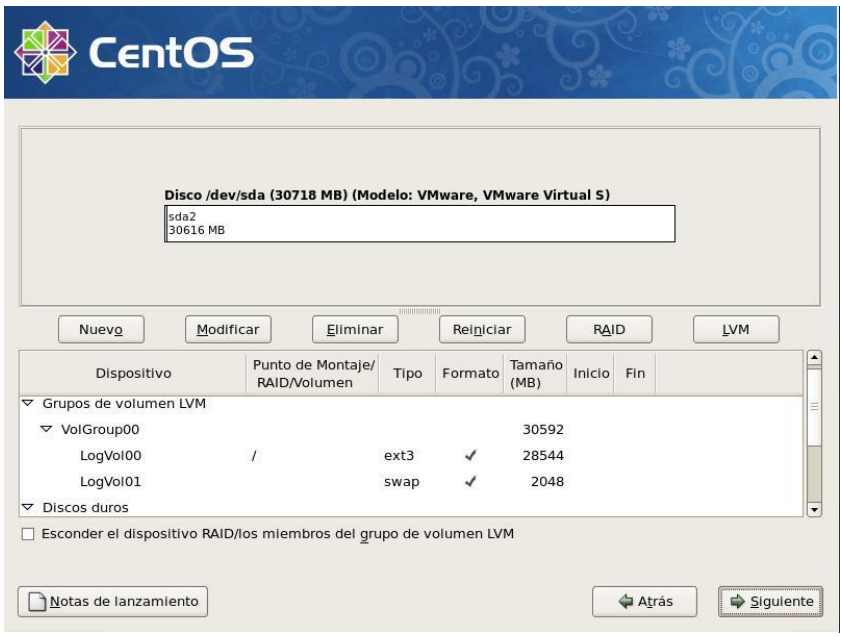


Fig. 6-7. Tabla de particiones
Fuente: Servidor
Elaborado por: Diego Silva

Configuración del gestor de arranque, muestra el sistema operativo que arrancara y es importante añadirle una contraseña para evitar la edición del GRUB que fácilmente dejaría vulnerable el sistema; siguiente

Fig. 6-8. Contraseña de Gestor de arranque
Fuente: Servidor
Elaborado por: Diego Silva

Configurar las direcciones IP para las tarjetas de red, en este caso eth0 se conectará al modem y eth1 a la intranet

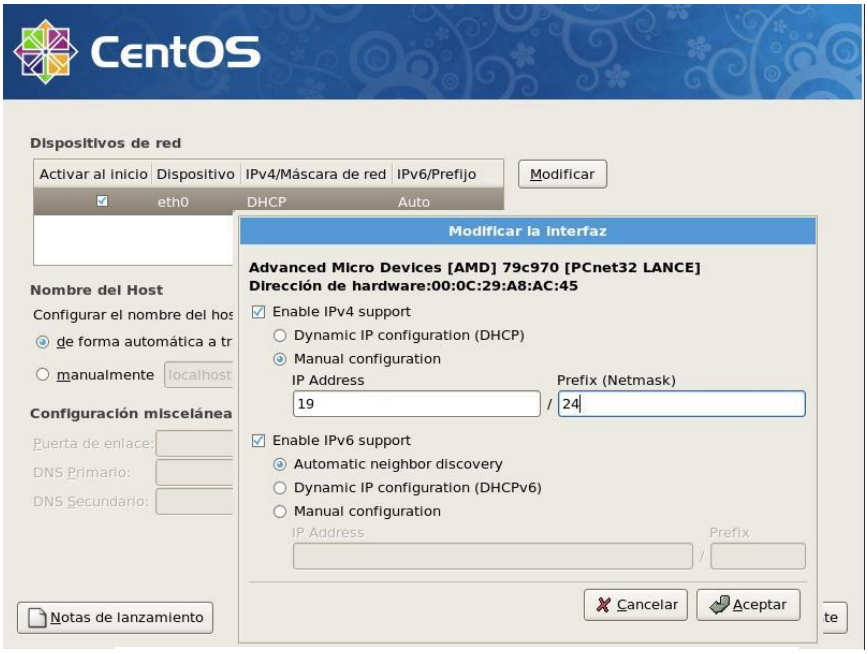


Fig. 6-9. Configuración de red
Fuente: Servidor
Elaborado por: Diego Silva

Elegir la ubicación dando un clic en el mapa o a su vez buscarlo en la lista

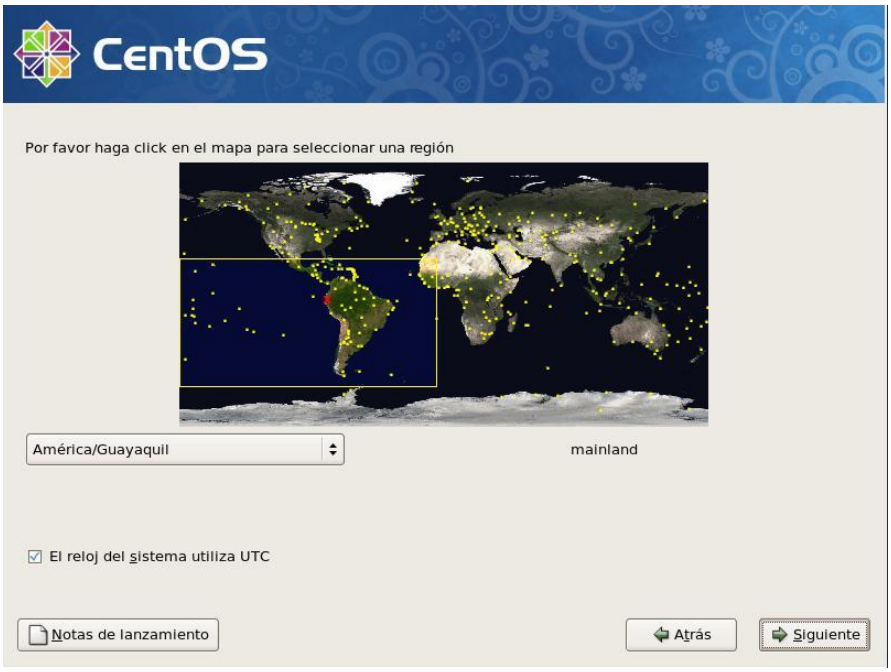


Fig. 6-10. Ubicación Geográfica del servidor
Fuente: Servidor
Elaborado por: Diego Silva

Digitar la contraseña para el usuario root; siguiente

Fig. 6-11. Obteniendo información de la instalación
Fuente: Servidor
Elaborado por: Diego Silva

Elegir de manera general las tareas que va realizar el servidor, lo importante es un entorno gráfico y los paquetes de servidor, en la parte inferior seleccionar "Personalizar ahora" para elegir que paquetes se instalarán

Fig. 6-12. Tipo de servidor
Fuente: Servidor
Elaborado por: Diego Silva

Seleccionar algunas aplicaciones extras que posteriormente serán útiles, entre estas las bibliotecas de desarrollo, java, mysql, verificar la selección de squid, ssh; incluso soporte de idiomas. Aunque posteriormente se puede instalar si alguna hace falta

Fig. 6-13. Selección de paquetes a instalar
Fuente: Servidor
Elaborado por: Diego Silva

Al dar clic en siguiente el instalador va comprobar las dependencias de los paquetes, pues varios servicios dependen de otros para ejecutarse con lo cual el sistema los completara.

Fig. 6-14. Comprobación de dependencias de paquetes
Fuente: Servidor
Elaborado por: Diego Silva

Una vez completado está listo para instalar el sistema operativo con un clic en siguiente, muestra un mensaje indicando donde encontrar una bitácora con las opciones de nuestra instalación.

Fig. 6-15. Aviso de inicio de instalación
Fuente: Servidor
Elaborado por: Diego Silva

Empieza la instalación y va indicando avances en el monitor.

Fig. 6-16. Transferencia de datos para la instalación
Fuente: Servidor
Elaborado por: Diego Silva

Fig. 6-17. Avance de instalación
Fuente: Servidor
Elaborado por: Diego Silva

Una vez que ha concluido con la instalación, clic en reiniciar

Fig. 6-18. Instalación Completada
Fuente: Servidor
Elaborado por: Diego Silva

Una vez reiniciado el servidor aparece el menú del grub donde si se desea cambiar sus opciones será necesario introducir la clave que se puso en la instalación.

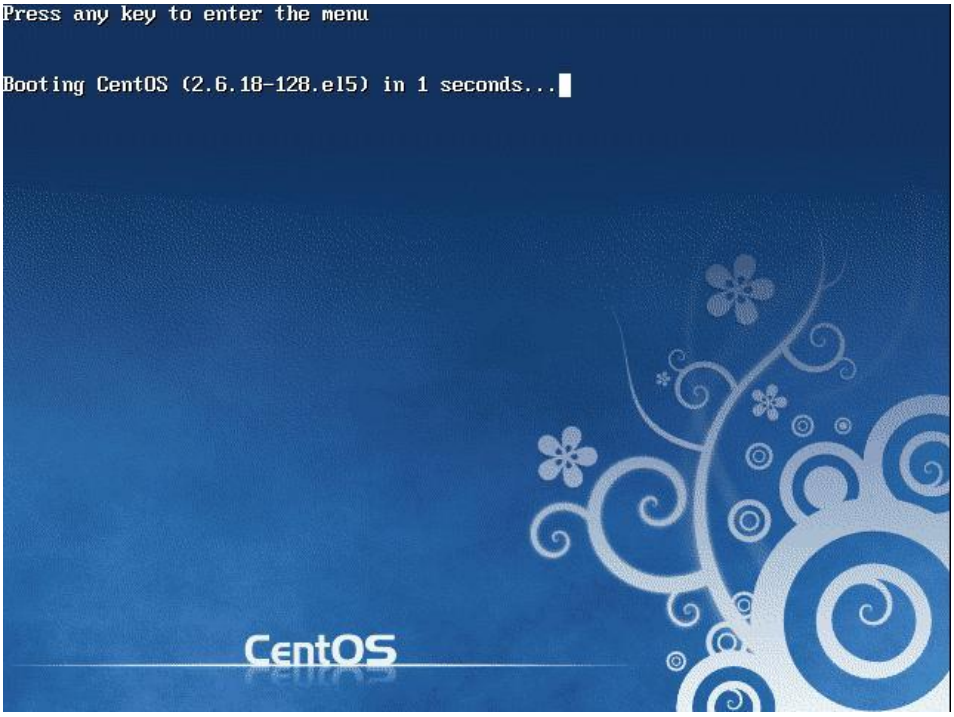


Fig. 6-19. Booteo de Centos
Fuente: Servidor
Elaborado por: Diego Silva

Cuando ya ha booteado el sistema, si se desea, mostrar los detalles para poder ver los servicios que se inician

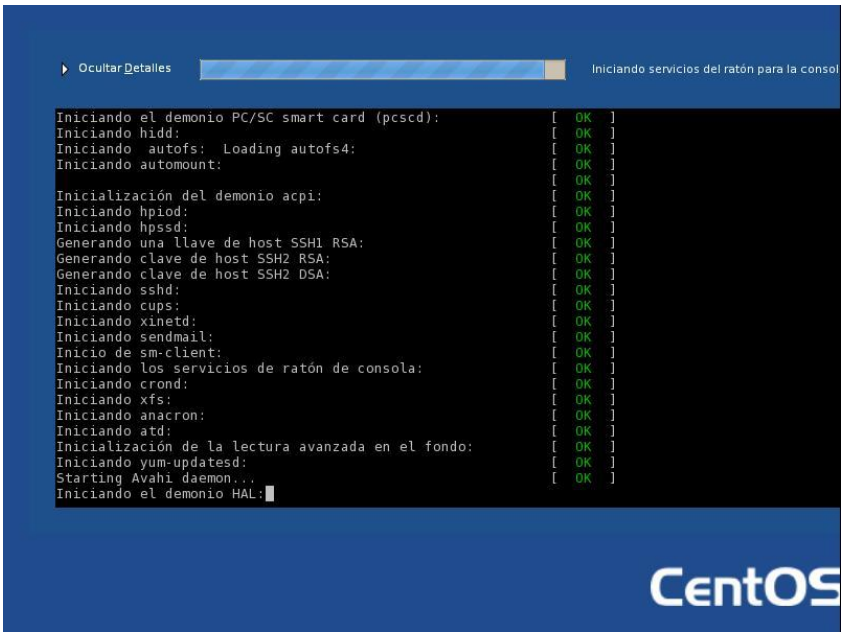


Fig. 6-20. Inicio de Servicios
Fuente: Servidor
Elaborado por: Diego Silva

Como es la primera vez que inicia el sistema es necesario realizar algunas configuraciones; Se aprecia la pantalla de bienvenida

Fig. 6-21. Pantalla de bienvenida
Fuente: Servidor
Elaborado por: Diego Silva

En este paso dejar habilitado el firewall únicamente con los puertos abiertos para HTTP y HTTPS para poder tener acceso a internet, porque posteriormente se realizara una configuración personalizada de firewall

Fig. 6-22. Configuración de Cortafuegos
Fuente: Servidor
Elaborado por: Diego Silva

Muestra un mensaje de advertencia de modificación del cortafuegos. Aceptar

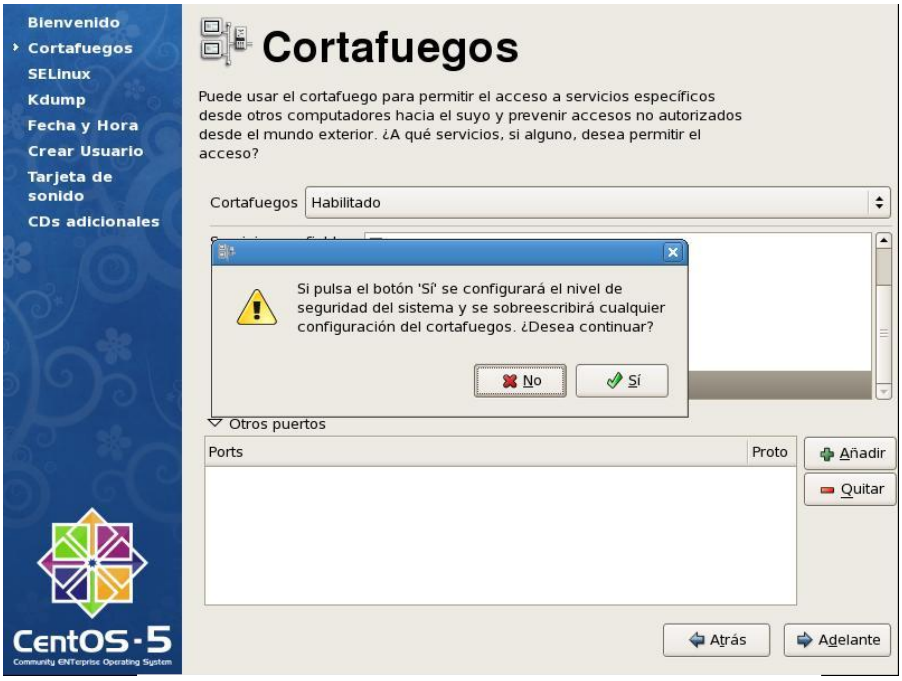


Fig. 6-23. Advertencia de Cortafuegos
Fuente: Servidor
Elaborado por: Diego Silva

En la configuración de SELinux, que es una seguridad extra al sistema dejar deshabilitado porque se va a controlar todo con nuestra configuración firewall; adelante

Fig. 6-24. Configuración SELinux
Fuente: Servidor
Elaborado por: Diego Silva

Deshabilitar Kdump, que es un servicio que determina los fallos en caso de una caída

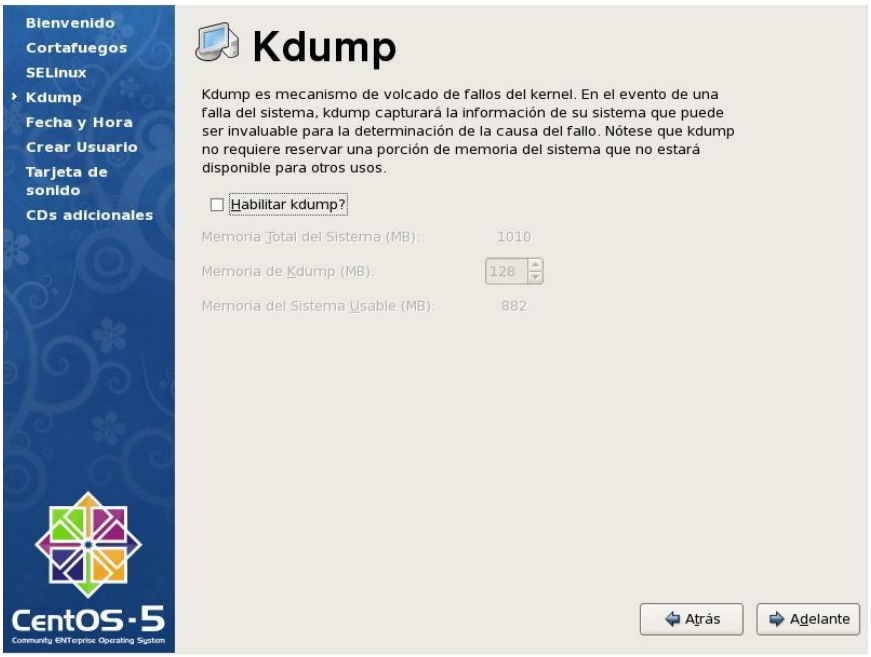


Fig. 6-25. Habilitar Kdump
Fuente: Servidor
Elaborado por: Diego Silva

Igualar la fecha y hora del sistema

Fig. 6-26. Fecha y hora del sistema
Fuente: Servidor
Elaborado por: Diego Silva

Crear un usuario, estableciendo una contraseña de preferencia con una combinación de caracteres alfabéticos, numéricos y símbolos

Fig. 6-27. Creación de usuario
Fuente: Servidor
Elaborado por: Diego Silva

Se realizan pruebas de la tarjeta de sonido

Fig. 6-28. Configuración de sonido
Fuente: Servidor
Elaborado por: Diego Silva

Si se tiene discos de instalación con paquetes adicionales insertarlo e instalar y finalizar

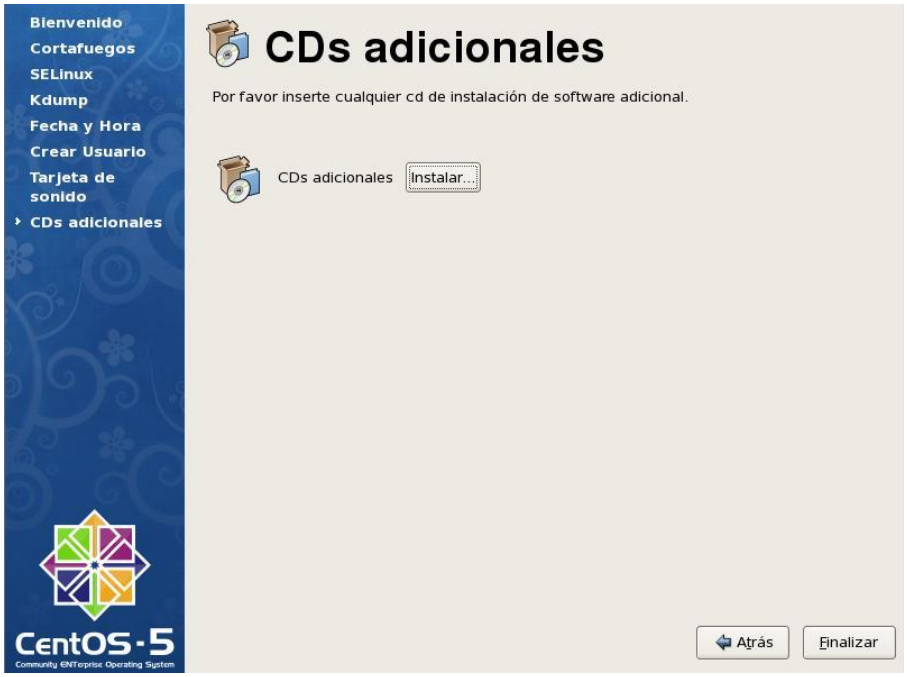


Fig. 6-29. Instalación de CDs Adicionales
Fuente: Servidor
Elaborado por: Diego Silva

Se presenta la pantalla de inicio de sesión, es recomendable siempre ingresar con un usuario con privilegios limitados para evitar ataques y problemas de seguridad

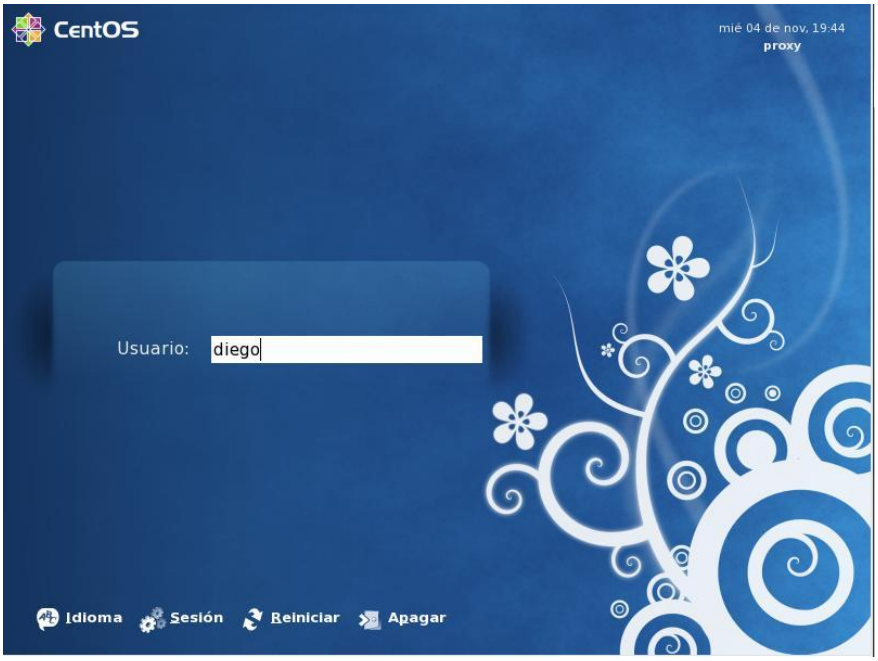


Fig. 6-30. Inicio de Sesión
Fuente: Servidor
Elaborado por: Diego Silva

Si se loguea correctamente se muestra el inicio de los servicios

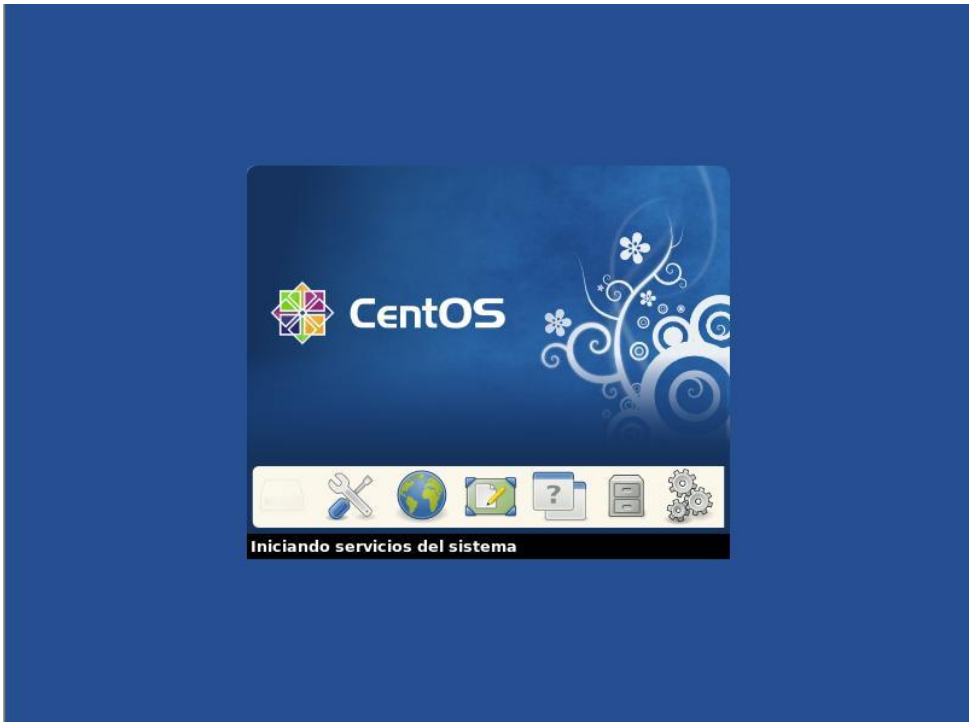


Fig. 6-31. Carga de servicios del sistema
Fuente: Servidor
Elaborado por: Diego Silva

Se puede observar el ambiente del servidor

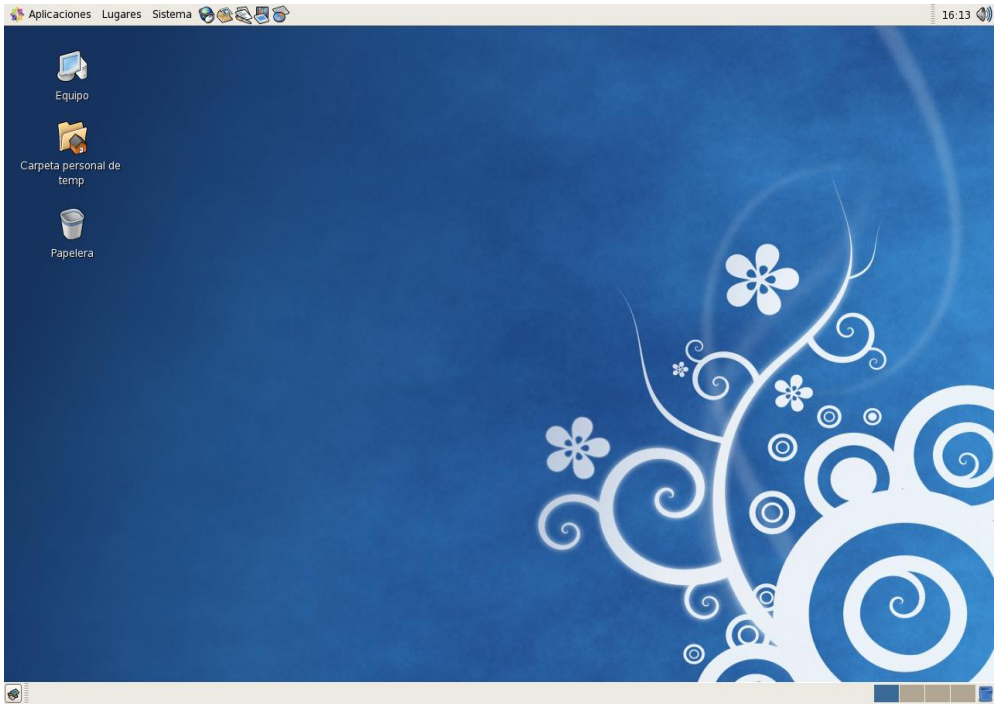


Fig. 6-32. Ambiente del servidor
Fuente: Servidor
Elaborado por: Diego Silva

6.2.5 Seguridad en el Servidor

6.2.5.1 Seguridad Física

Físicamente tienen acceso al servidor los integrantes del Subproceso de Informática: Ing. Oscar Llerena, Diego Silva y pasante o practicante, además del personal de servicio de limpieza quienes en su respectivo horario serán responsables de la integridad y acceso hacia el servidor.

Para evitar problemas durante los cortes eléctricos cuenta también con un UPS, y se encuentra protegido del calor y la humedad por su ubicación dentro del APD. Lastimosamente, dentro de toda el área de la Institución no se cuenta con los recursos necesarios para la protección en caso de incendios.

En caso de desperfecto o daño en el equipo o alguno de sus componentes, se cuenta con un servidor alterno de respaldo con capacidades de procesamiento y memoria inferiores; pero con las mismas configuraciones establecidas en el servidor principal. Este servidor alterno puede entrar inmediatamente en funcionamiento mientras se solucionan los problemas con el servidor, evitando de esta manera los cortes en el servicio.

6.2.5.2 Autenticación y autorización

Para la aplicación es suficiente una autenticación con usuario y contraseña, la misma que será siempre con una cuenta de privilegios y autorización limitada; para realizar la configuración del equipo es recomendable nunca acceder con usuario root o súper-usuario, más bien se deberá escalar privilegios a súper-usuario cuando sea necesario.

Además de un único usuario root, con el cual se accederá a la configuración del equipo, se crean dos usuarios para las únicas personas permitidas en administrar el servidor y se describen a continuación.

Nombre del Usuario	Usuario	Tipo de Cuenta
Ing. Oscar Llerena	Oscar	Limitada
Diego Silva	Diego	Limitada
Administrador	Root	Administrador

Tabla 6-15. Usuarios del servidor
Fuente: Informático Provincial
Elaborado por: Diego Silva

6.2.5.3 Primeras medidas de seguridad en el equipo

- **Configurando el BIOS:** es necesario iniciar configurando el BIOS, de tal manera que un hacker que este frente a nuestro equipo no pueda ingresar fácilmente; seguir estos sencillos pasos:
    a) Establecer en la prioridad de arranque primero al disco duro, para evitar que arranquen desde un CD o un disquete en modo de rescate
    b) Establecer una contraseña en el BIOS para evitar que se realicen cambios, sin embargo esta puede ser vulnerada al sacarle la pila del mainboard o con programas para crackearla
- **Password del gestor de arranque:** a pesar de haber establecido un password durante la instalación, se puede cambiarla de la siguiente manera:

```
[diego@proxy ~]$ su -
Contraseña:
[root@proxy ~]# grub
grub> md5crypt
Password: **********
Encrypted: $1$5IFLp/$D7qh7.2L4vVwg6yi72lN61
grub> quit
[root@proxy ~]# vi /boot/grub/menu.lst
…
password --md5 $1$5IFLp/$D7qh7.2L4vVwg6yi72lNh61
…
[root@proxy ~]# chmod 600 /boot/grub/menu.lst
```

Primero escalar privilegios a súper-usuario y escribir la contraseña de root; con el comando grub se ingresa a la edición del mismo, digitar md5crypt y presionar enter, escribir la nueva contraseña y al presionar enter devuelve una combinación de caracteres que representan a la contraseña encriptada; copiar estos caracteres y salir con quit. Editar el archivo /boot/grub/menu.lst, ubicar la línea que dice password --md5 y reemplazar todo el resto de la línea pegando lo que se generó con el comando grub, salir guardando (Esc : wq enter) y cambiar los privilegios con chmod 600 al archivo, para de esta manera permitir que solamente root tenga permisos de lectura y escritura.

- **Deshabilitar servicios:** Los servicios pueden ser iniciados automáticamente, o a través de xinetd. Son iniciados automáticamente en un script por cada servicio que se

encuentra en el directorio /etc/rc.d/init.d y los que se inician a través de xinetd pueden ser configurados en el archivo /etc/xinetd.conf. Podemos ver los servicios que se inician con el comando: **ps aux**, y con el comando chkconfig habilitar o deshabilitar el inicio de los servicios que se consideren innecesarios. Se realiza esta acción, porque cada servicio en ejecución significa un posible hueco de seguridad.

Sintaxis chkconfig:

chkconfig [--level <levels>] <nombre> <on|off|reset|resetpriorities>

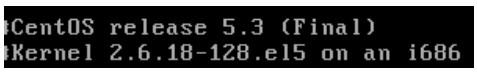
En la línea de comando digitar:

chkconfig bluetooth off

chkconfig firstboot off

Y se deshabilita el inicio automático del servicio bluetooth porque no se cuenta con un dispositivo y firstboot que se ejecuta solamente luego de la instalación.

» **Ocultar información importante:** Al loguerse en el servidor se presenta información del sistema operativo como la distribución y la versión del mismo así como el kernel con su versión



Estos datos son muy importantes para un hacker pues sabiendo el tipo de sistema y versión empiezan a buscar las vulnerabilidades conocidas. Es recomendable mostrar aquí la menor información posible; para modificar dirigirse al archivo /etc/issue y /etc/issue.net. Antes de la modificación se saca una copia y se procede a dejar el archivo de la siguiente manera:

cd /etc

cp issue issue.respaldo

cp issue.net issue.net.respaldo

nano issue

Servidor proxy de la Dirección Provincial de Salud de Tungurahua

El uso es solamente para usuarios autorizados, si no lo es

desconectese ahora!

nano issue.net

Servidor proxy de la Dirección Provincial de Salud de Tungurahua

El uso es solamente para usuarios autorizados, si no lo es

desconectese ahora!

Además se puede agregar un aviso que se presenta cuando un usuario se loguea en el sistema, de este modo se advierte a los usuarios no autorizados que su uso no está permitido. Editamos el archivo /etc/motd y escribimos un aviso

```
# nano /etc/motd
**************************AVISO**********************************
Este equipo es para usuarios autorizados solamente, si no lo
es puede afrontar acciones disciplinarias administrativas o
cargos legales.

El uso de este sistema es monitoreado por razones de seguri_
dad; todas sus acciones son registradas y pueden ser usadas
en su contra. Su privacidad aqui no esta garantizada.

Para continuar usando este sistema debe estar de acuerdo con
los terminos descritos anteriormente. Caso contrario debe
DESCONECTARSE INMEDIATAMENTE
*************************************************************
```

- **Tiempo de Inactividad:** Se refiere al tiempo en que un usuario mantiene al equipo de ocioso, se puede configurar el tiempo que puede estar así para que posteriormente pasado éste, la sesión se cierre automáticamente. Para el servidor se le fija en 5 minutos (300 segundos). Editamos el archivo /etc/profile y añadimos la siguiente variable, puede ser al inicio del resto de instrucciones de este script.

```
# nano /etc/profile
TMOUT=300
```

6.2.6 Configuración de Firewall

A continuación se describen los servicios y el puerto utilizado para comunicarse

Servicio	Puerto
http	80
https	443
DNS	53

Ssh	222
Squid	8080
Citrix para equipos de contabilidad	1494

Tabla. 6-16. Servicios a configurar en el iptables
Fuente: Servidor
Elaborado por: Diego Silva

6.2.6.1 Definición de Reglas

- Hacer un flush de las reglas (limpiarlas)
- Establecer la política por defecto DROP
- Permitir entrada y salida a todo a localhost
- Permitir toda conexión de entrada y salida en la IP de la intranet
- En la IP de salida a internet permitir las conexiones salientes a través de los puertos 80, 443
- Permitir la consulta de DNS
- Abrir el puerto para administración a través de ssh
- Recibir paquetes para el servicio proxy a través del puerto 8080 en la interfaz de red local
- Permitir conexión hacia el servidor citrix para el área de contabilidad a través del puerto 1494
- Establecer una barrera de Backup en caso se cambie la política de seguridad a ACCEPT temporalmente cerrando todos los puertos confiables y otros conocidos
- Activar el bit de reenvío

Nota: Posteriormente a medida que se van configurando los servicios será necesario añadir más reglas, y al final se añadirá como anexo el script completo de la configuración de Iptables.

Es necesario realizar ciertos cambios para lograr que la configuración de Iptables se restaure cada vez que se pare o se reinicie el servicio. El archivo de configuración de Iptables está en el directorio /etc/sysconfig/iptables-config editar y cambiar los siguientes parámetros:

```
# nano /etc/sysconfig/iptables-config
IPTABLES_SAVE_ON_STOP="yes"
IPTABLES_SAVE_ON_RESTART="yes"
```

6.2.7 Configuración de SQUID

Verificar si squid está instalado

```
# rpm -q squid
squid-2.6.STABLE21-3.el5
```

Si no lo está descargarlo e instalarlo a través de yum

```
# yum –y install squid
```

Entrar como super usuario con el comando su – el cual pedirá la clave de root.

```
[diego@proxy ~]$ su -
Contraseña:
[root@proxy ~]#
```

Antes de realizar cualquier cambio en los archivos de configuración es recomendable sacar una copia de respaldo

```
#cp /etc/squid/squid.conf /etc/squid/squid.conf.respaldo
```

Ahora editar el archivo de configuración principal squid.conf que se encuentra en el directorio /etc/squid/

```
# nano /etc/squid/squid.conf
```

Este archivo es muy extenso y contiene la descripción de cada una de las opciones posibles a configurar, por lo cual se debe centrar en buscar las opciones necesarias para que arranque y funcione el servidor proxy.

6.2.7.1 Parámetro http_port

Buscar la sección del puerto por el cual se va a hacer que el servidor intermediario escuche las peticiones de salida a internet. En este caso con el editor de texto usado presionar ctrl+w, digitar el texto http_port hasta encontrar la siguiente línea

```
http_port 3128
```

En esta sección registrar el puerto del squid. Además es posible indicar la IP por la cual va escuchar para evitar accesos de petición al servidor proxy desde la IP mediante la cual se accede al proveedor de internet. Se utilizaran tres puertos, pensados con la limitación de ancho de banda, dos puertos para acceso a internet y un tercero para actualización de antivirus

```
http_port 192.168.43.10:8080
http_port 192.168.43.10:3128
http_port 192.168.43.10:8181
```

6.2.7.2 Parámetro cache_mem

El parámetro cache_mem establece la cantidad ideal de memoria para lo siguiente:

- Objetos en tránsito.
- Objetos frecuentemente utilizados (Hot).
- Objetos negativamente almacenados en el caché.

De modo predefinido se establecen 8 MB. Se recomienda asignar 10 MB por cada Giga asignado en el parámetro cache_dir mas 20 MB extras; por lo tanto serían 90 MB para este parámetro pero se lo establece en 128 MB que no afectan a los 8 GB de RAM del equipo.

```
cache_mem 128 MB
```

6.2.7.3 Parámetro cache_dir

Define cuanto se desea almacenar de internet en el disco duro; de modo predefinido squid almacena 100 MB. Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. Se recomienda asignar 14 MB por cada Giga de Disco Duro; por lo tanto para el disco de 500 GB se recomienda asignar 7000 MB.

```
cache_dir ufs /var/spool/squid 7000 16 256
```

Los números 16 y 256 significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno. No hay necesidad de modificarlos. Es muy importante considerar que si se especifica un determinado tamaño de caché y éste excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente.

6.2.7.4 Listas de control de acceso

Es necesario definir listas de control de acceso, para establecer las reglas de acceso o denegación ya sea de una red o determinados equipos, de sitios, de horarios, de extensiones, el acceso a través de claves.

Para cumplir con las políticas de seguridad se definirán las siguientes reglas:

- Denegar acceso a las IPs que no están en uso
- Acceso total para el proceso de informática
- Acceso a internet de toda la red con:
  - ✓ Limitación del horario de Lunes a Viernes de 8:00 a 18:00
  - ✓ Permitir los sitios que pueden contener palabras no deseadas pero que son inocentes
  - ✓ Denegación de sitios pornográficos, farándula, descargas, entretenimiento, redes sociales, túneles o proxys. Y también de palabras no deseadas relacionadas con pornografía, ocio, descargas, telefonía móvil
  - ✓ Denegación de extensiones de descargas de música, video, archivos comprimidos y otros que pueden implicar riesgo o consumo de ancho de banda
- Denegar todo el resto de conexiones que no hayan pasado por las reglas establecidas

En el mismo archivo de configuración, ubicarse en las líneas donde se deben insertar reglas propias

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
acl redLocal src 192.168.43.0/24
acl ipsBloqueadas src "/etc/squid/listas/ipsBloqueadas"
acl sitiosNegados url_regex "/etc/squid/listas/sitiosNegados"
acl inocentes url_regex "/etc/squid/listas/inocentes"
acl extensiones urlpath_regex "/etc/squid/listas/extensiones"
acl informatica src "/etc/squid/listas/informatica"
acl horario time MTWHF 8:00-18:00
# And finally deny all other access to this proxy
http_access allow localhost
http_access deny ipsBloqueadas
http_access allow informatica
http_access allow horario redlocal !sitiosNegados !extensiones
http_access allow inocentes
http_access deny all
```

Los archivos descritos se adjuntan al final:

- ipsBloqueadas: contiene una lista de IPs
- sitiosNegados: palabras y sitios
- inocentes: palabras y sitios

- extensiones: extensiones en este formato \.mp3$
- informática otra lista de IPs.

6.2.7.5 Parámetro error_directory

Define el directorio donde squid buscará el error para presentarlo al usuario, por default se encuentra en inglés. Cambiar esta línea para nuestro idioma

```
error_directory /usr/share/squid/errors/Spanish
```

Posteriormente eliminar el enlace simbólico del idioma inglés y añadir el enlace a español

```
rm -f /etc/squid/errors
ln -s /usr/share/squid/errors/Spanish /etc/squid/errors
```

Este enlace debe regenerarse después de actualizar squid

6.2.7.6 Iniciar, reiniciar y añadir el servicio al arranque del sistema

Una vez terminada la configuración, ejecutar el siguiente mandato para iniciar por primera vez Squid:

```
service squid start
```

Si se necesita reiniciar para probar cambios hechos en la configuración:

```
service squid restart
```

Para que Squid inicie de manera automática la próxima vez que inicie el sistema:

```
chkconfig squid on
```

Lo anterior habilitará a Squid en todos los niveles de corrida.

6.2.7.7 Depuración de errores

Cualquier error al inicio de Squid solo significa que hubo errores de sintaxis, o bien se están citando incorrectamente las rutas hacia los ficheros de las Listas de Control de Acceso.

Se puede realizar diagnóstico de problemas indicándole a Squid que vuelva a leer la configuración, lo cual devolverá los errores que existan en el fichero /etc/squid/squid.conf.

```
service squid reload
```

Cuando se trata de errores graves que no permiten iniciar el servicio, puede examinarse el contenido del fichero /var/log/squid/squid.out con el mandato less, more o cualquier otro visor de texto:

```
less /var/log/squid/squid.out
```

6.2.7.8 SARG - Reporte de actividades de SQUID

SARG (Squid Analysis Report Generator) es la herramienta más completa y fácil de usar para la generación de reportes a partir de los logs de Squid. Permite ver con detalle la actividad de todos los equipos y/o usuarios dentro de la red de área local, registrada en la bitácora de Squid.

Configuración

Agregar un repositorio del sitio Alcance Libre de donde posteriormente se realizara la descarga

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd -
```

Instalar SARG utilizando el siguiente mandato

```
yum -y install sarg
```

Editar el archivo de configuración de SARG

```
nano /etc/sarg/sarg.conf
```

Localizar la línea del idioma para adaptarlo a español y salir guardando

```
language Spanish
```

Editar el archivo de configuración del servidor apache

```
nano /etc/httpd/conf.d/sarg.conf
```

Localizar la línea `allow from 127.0.0.1` que define una red o redes o IP o conjunto de IPs que pueden acceder hacia el servidor para visualizar los reportes a través de SARG. Incluir además luego de esta línea las siguientes que definen el acceso solamente a usuarios autorizados autenticándolos mediante una clave

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
  DirectoryIndex index.html
  order deny,allow
  deny from all
  allow from 127.0.0.1 192.168.43.10/24 192.168.43.30/24
  AuthName "Solo usuarios autorizados."
  AuthType Basic
  require valid-user
  AuthUserFile /var/www/claves-sarg
</Directory>
```

Salir guardando y crear el fichero de claves donde se autenticará SARG

```
# touch /var/www/claves-sarg
```

Otorgar permiso de lectura y escritura para la clase de usuario y definir que el fichero pertenece al usuario y grupo apache

```
# chmod 0600 /var/www/claves-sarg
# chown apache:apache /var/www/claves-sarg
```

Utilizar el mandato htpasswd sobre el fichero /var/www/claves-sarg para crear el usuario virtual administrador y asignarle una clave de acceso

```
# htpasswd /var/www/claves-sarg administrador
```

Iniciar el servicio httpd y agregarlo al arranque

```
# service httpd start
# chkconfig httpd on
```

Digitar el comando sarg para generar un reporte de squid

```
# sarg
```

Para ver el reporte generado desde el servidor o desde las IPs permitidas en el navegador digitar http://proxy.dpst/sarg/ONE-SHOT o reemplazar proxy.dpst por la IP del servidor 192.168.43.10. A continuación algunas vistas de la navegación en el reporte:

Índice de los reportes generados

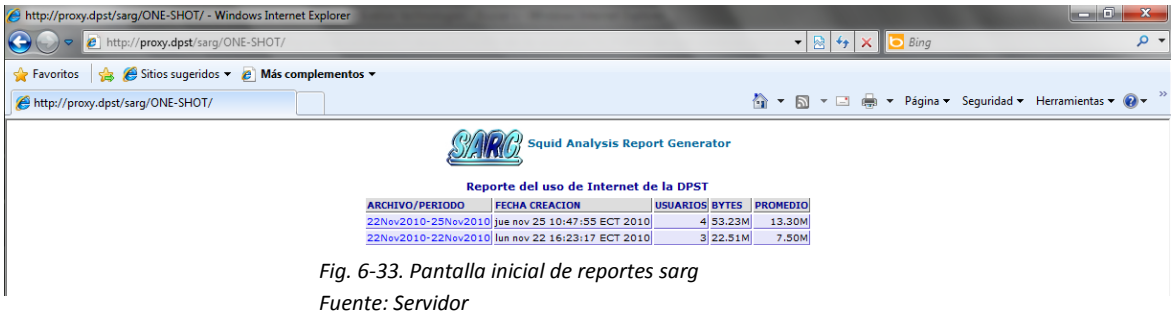


Fig. 6-33. Pantalla inicial de reportes sarg
Fuente: Servidor
Elaborado por: Diego Silva

Índice de uno de los reportes generados se puede observar que hay la posibilidad de mostrar un gráfico por cada IP

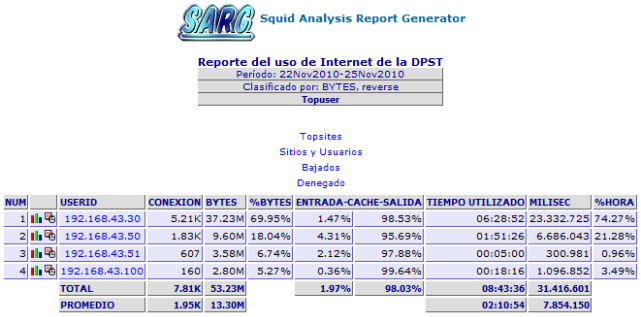


Fig. 6-34. Visualización del reporte generado
Fuente: Servidor
Elaborado por: Diego Silva

Gráfico de uso de MB por cliente

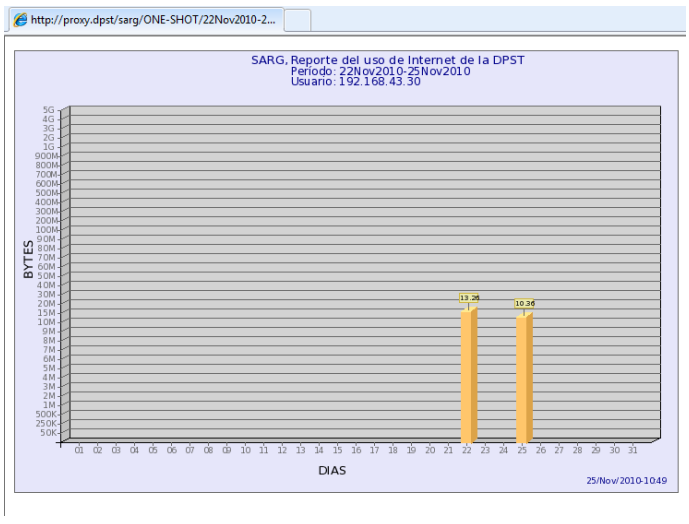
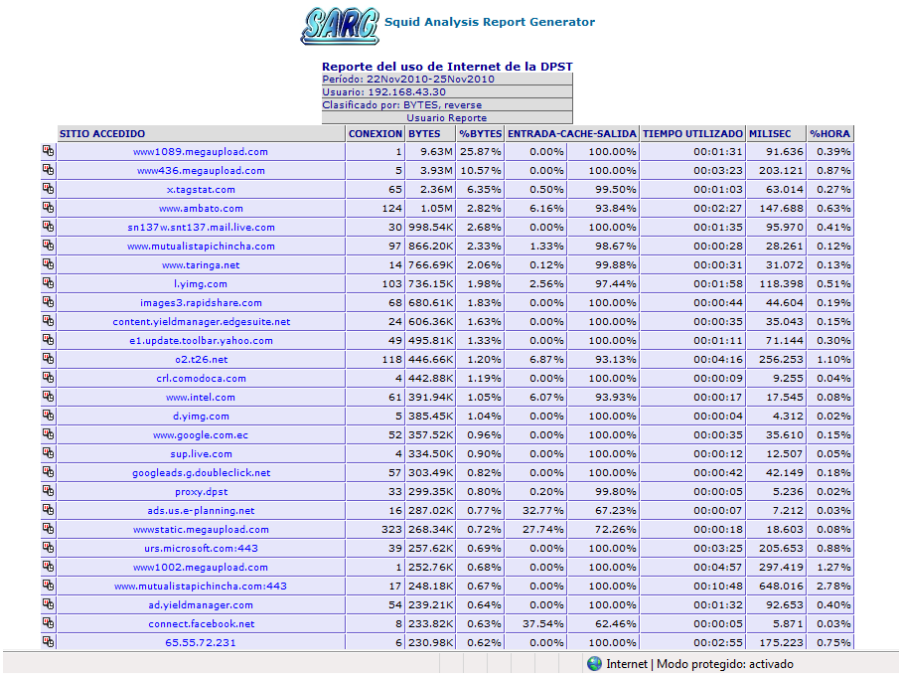


Fig. 6-35. Gráficos por cliente
Fuente: Servidor
Elaborado por: Diego Silva

Reporte de sitios accedidos por IP



Squid Analysis Report Generator

Reporte del uso de Internet de la DPST

Periodo: 22Nov2010-25Nov2010
Usuario: 192.168.43.30
Clasificado por: BYTES, reverse
Usuario Reporte

SITIO ACCEDIDO	CONEXION	BYTES	%BYTES	ENTRADA-CACHE-SALIDA		TIEMPO UTILIZADO	MILISEC	%HORA
www1089.megaupload.com	1	9.63M	25.87%	0.00%	100.00%	00:01:31	91.636	0.39%
www436.megaupload.com	5	3.93M	10.57%	0.00%	100.00%	00:03:23	203.121	0.87%
x.tagstat.com	65	2.36M	6.35%	0.50%	99.50%	00:01:03	63.014	0.27%
www.ambato.com	124	1.05M	2.82%	6.16%	93.84%	00:02:27	147.688	0.63%
sn137w.snt137.mail.live.com	30	998.54K	2.68%	0.00%	100.00%	00:01:35	95.970	0.41%
www.mutualistapichincha.com	97	866.20K	2.33%	1.33%	98.67%	00:00:28	28.261	0.12%
www.taringa.net	14	766.69K	2.06%	0.12%	99.88%	00:00:31	31.072	0.13%
l.yimg.com	103	736.15K	1.98%	2.56%	97.44%	00:01:58	118.398	0.51%
images3.rapidshare.com	68	680.61K	1.83%	0.00%	100.00%	00:00:44	44.604	0.19%
content.yieldmanager.edgesuite.net	24	606.36K	1.63%	0.00%	100.00%	00:00:35	35.043	0.15%
e1.update.toolbar.yahoo.com	49	495.81K	1.33%	0.00%	100.00%	00:01:11	71.144	0.30%
o2.t26.net	118	446.66K	1.20%	6.87%	93.13%	00:04:16	256.253	1.10%
crl.comodoca.com	4	442.88K	1.19%	0.00%	100.00%	00:00:09	9.255	0.04%
www.intel.com	61	391.94K	1.05%	6.07%	93.93%	00:00:17	17.545	0.08%
d.yimg.com	5	385.45K	1.04%	0.00%	100.00%	00:00:04	4.312	0.02%
www.google.com.ec	52	357.52K	0.96%	0.00%	100.00%	00:00:35	35.610	0.15%
sup.live.com	4	334.50K	0.90%	0.00%	100.00%	00:00:12	12.507	0.05%
googleads.g.doubleclick.net	57	303.49K	0.82%	0.00%	100.00%	00:00:42	42.149	0.18%
proxy.dpst	33	299.35K	0.80%	0.20%	99.80%	00:00:05	5.236	0.02%
ads.us.e-planning.net	16	287.02K	0.77%	32.77%	67.23%	00:00:07	7.212	0.03%
wwwstatic.megaupload.com	323	268.34K	0.72%	27.74%	72.26%	00:00:18	18.603	0.08%
urs.microsoft.com:443	39	257.62K	0.69%	0.00%	100.00%	00:03:25	205.653	0.88%
www1002.megaupload.com	1	252.76K	0.68%	0.00%	100.00%	00:04:57	297.419	1.27%
www.mutualistapichincha.com:443	17	248.18K	0.67%	0.00%	100.00%	00:10:48	648.016	2.78%
ad.yieldmanager.com	54	239.21K	0.64%	0.00%	100.00%	00:01:32	92.653	0.40%
connect.facebook.net	8	233.82K	0.63%	37.54%	62.46%	00:00:05	5.871	0.03%
65.55.72.231	6	230.98K	0.62%	0.00%	100.00%	00:02:55	175.223	0.75%

Internet | Modo protegido: activado

Fig. 6-36. Pantalla inicial de reportes sarg
Fuente: Servidor
Elaborado por: Diego Silva

Generación automática de informes

Se puede generar informes de acuerdo a necesidades propias con la herramienta crontab

Para poder configurar un crond:

1) Ejecutar el siguiente comando que permite editar el crond. crontab –e
2) La configuración del crond es la siguiente:

Los valores del crond:

- Minuto (0- 60)
- Hora (0-23)
- Mesdia (1-31)
- Mes (1-12)
- Diasemana (0-7)

Los valores van por columnas

min. horas dia-mes mes diasemana comando

Para el servidor se desea crear a las 18:30 todos los días viernes para poder chequear el informe los días lunes

30 18 * * 5 sarg

Salimos guardando con ESC:wq

6.2.8 Configuración del servidor Samba

Para la institución se crea un directorio para cada proceso el mismo que podrá ser accedido únicamente por los usuarios de dicho proceso, además se crea un directorio al cual podrán acceder todos los usuarios de la institución. Se crea un usuario por cada proceso para acceder al servidor de archivos; los usuarios del subproceso de informática pueden acceder a cualquier directorio.

Además se comparte la impresora solamente para los equipos del subproceso de informática.

Proceso	Directorio	Usuario
General	/general	Todos los usuarios
Informática	/home/informatica	Informática
Implantación de la Norma	/home/impnorma	Impnorma
Gestión Financiera	/home/gesfinanciera	Gesfinanciera
Aseguramiento de la Calidad	/home/asecalidad	Asecalidad
Servicios Institucionales	/home/serinstituc	Serinstituc
Recursos Humanos	/home/rechumanos	Rechumanos
Vigilancia Sanitaria	/home/vigsanitaria	Vigsanitaria
Gobernante	/home/gobernante	Gobernante
Oferta y Demanda	/home/ofertademanda	Ofertademanda
Epidemiología	/home/epidemiologia	Epidemiologia
Comisaría de la Salud	/home/comsalud	Comsalud
Asesoría Jurídica	/home/asejuridica	Asejuridica

Tabla. 6-17. Usuarios de samba
Fuente: Investigación
Elaborado por: Diego Silva

Verificar la existencia de los siguientes paquetes con el comando rpm -q:

Samba

Samba-client

Samba-common

Si no los tenemos realizamos la instalación con el siguiente mandato:

```
yum -y install samba samba-client samba-common
```

El siguiente paso es la creación de usuarios con el mandato

```
useradd -s /sbin/nologin usuario_nuevo
smpbpasswd –a usuario_nuevo
```

Se procede a definir los parámetros principales de samba en el archivo de configuración /etc/samba/smb.conf:

- workgroup: Establece el grupo de trabajo del equipo

```
workgroup = informática
```

- server string: Define en un comentario la descripción del servidor

```
server string = Servidor de Archivos de la DPST
```

- netbios name: Se establece el nombre del servidor, debe coincidir con el archivo lmhosts en caso se lo hay modificado

```
netbios name = Servidor
```

- interfaces: Define las interfaces por donde escuchara las peticiones el servidor

```
interfaces = lo eth1 192.168.43.10/24
```

- La seguridad es importante y esta se puede establecer primeramente estableciendo la lista de control de acceso que definirá que máquinas o redes podrán acceder hacia el servidor. El parámetro hosts allow sirve para determinar esto. Para definir una IP se asigna la misma y para una red se asigna la parte de los octetos de red 192.168.43.0/24 se define 192.168.43.

```
hosts allow = 127. 192.168.43.
```

» A continuación ubicar la sección HOMES donde se establece el acceso hacia cada directorio de los usuarios definidos en samba, y dar acceso de escritura, que no pueda ser visto por otros usuarios, ocultar archivos de configuración que inician con punto, y evitar que sobrecarguen de archivos pesados como música y videos que además está prohibido su uso en la institución

```
[homes]
      comment = Archivos del Proceso
      browseable = no
      writable = yes
;     valid users = %S
;     valid users = MYDOMAIN\%S
      hide dot files = yes
      veto files = /*.mp3/*.mp4/*.mpg/*.avi/*.tmp/
```

» Se comparte también la impresora del proceso de informática poniendo como administrador al mismo usuario informática

```
[printers]
      comment = Impresoras Informatica
      path = /var/spool/samba
      browseable = no
      guest ok = no
      writable = no
      printable = yes
      printer admin = informatica
```

» Por último configurar un directorio para que pueda acceder cualquier usuario de la institución logueado en el servidor. A este directorio cualquier usuario puede acceder y modificar los archivos. Antes se debe haber creado el directorio a compartir con el mandato

```
mkdir –p /general
```

```
#Comparticion para cualquier usuario
[general]
      comment = Archivos compartidos de la DPST
      path = /general
      guest ok = yes
      read only = no
      writable = yes
      hide dot files = yes
      admin users = informatica impnorma gesfinanciera
      asecalidad serinstituc rechumanos vigsanitaria gobernante
      ofertademanda epidemiologia comsalud asejuridica
      directory mask = 0755
      create mask = 0644
      veto files = /*.mp3/*.mp4/*.mpg/*.avi/*.tmp/
```

» Iniciar, reiniciar y añadir el servicio al arranque

```
service smb start
service smb restart
chkconfig smb on
```

» Como la política por defecto en el firewall es denegar todo, es necesario abrir los siguientes puertos: 137, 138, 139 y 445 incluyendo en el script y ejecutándolo nuevamente

Para conectarse al servidor en el explorador de windows digitar en la barra de dirección \\192.168.43.10 y dar enter lo cual lleva a una pantalla de inicio de sesión como se aprecia en la Fig. 6-37 y digitar el usuario y contraseña

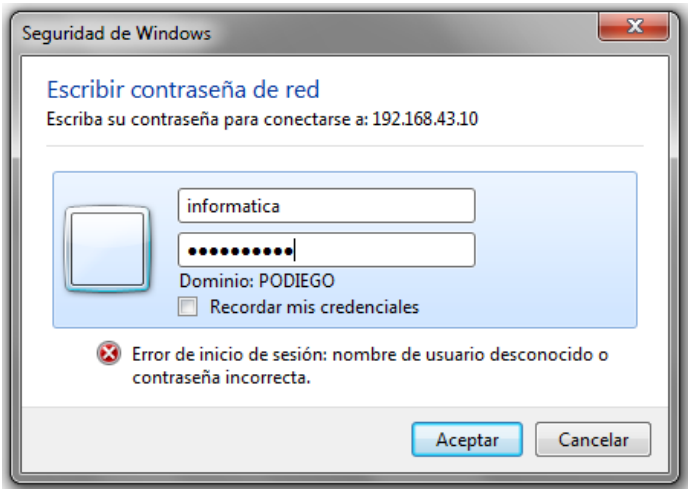


Fig. 6-37. Autenticación en samba desde windows
Fuente: Servidor
Elaborado por: Diego Silva

Una vez logueados se puede apreciar el directorio del usuario que es el de `/home` en el servidor y también el directorio general que es visible a todos los usuarios

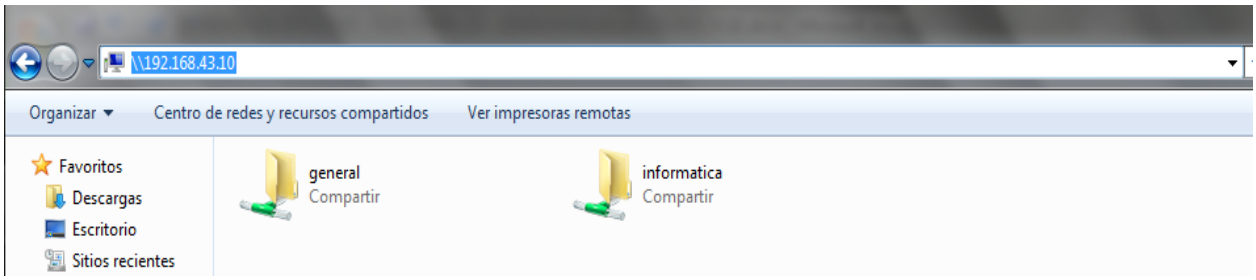


Fig. 6-38. Archivos en samba desde windows
Fuente: Servidor
Elaborado por: Diego Silva

Desde el entorno Linux en el menú Lugares elegir Conectar con el Servidor

Fig. 6-39. Explorar archivos desde linux
Fuente: Servidor
Elaborado por: Diego Silva

En la siguiente ventana en servidor elegir Compartido por Windows

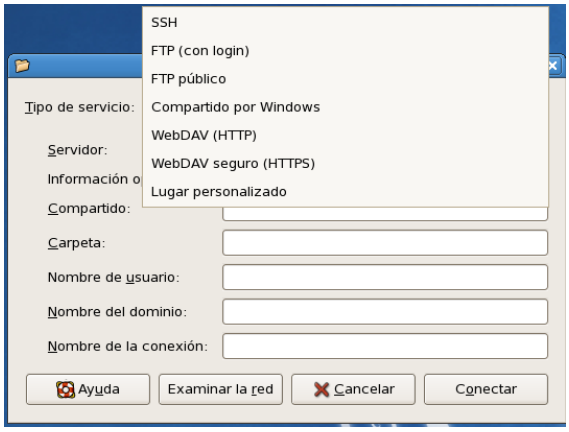


Fig. 6-40. Datos de autenticación
Fuente: Servidor
Elaborado por: Diego Silva

En servidor digitar la IP del mismo en nombre de usuario informática y nombre de dominio informática, clic en conectar

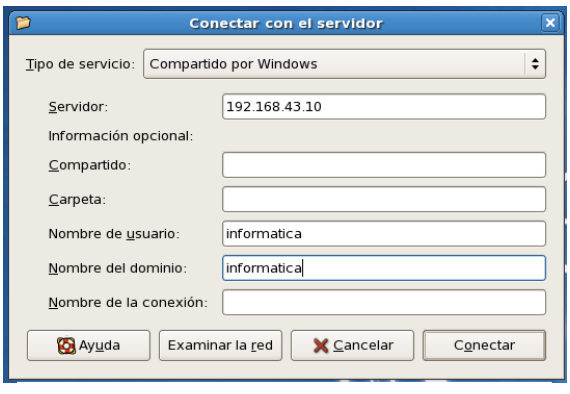


Fig. 6-41. Nombre de usuario y dominio
Fuente: Servidor
Elaborado por: Diego Silva

El servidor pide la clave para autenticarse digitar y conectar

Fig. 6-42. Clave de usuario samba
Fuente: Servidor
Elaborado por: Diego Silva

Al igual que el entorno Windows se observa los dos directorios disponibles para el usuario

Fig. 6-43. Directorios desde linux
Fuente: Servidor
Elaborado por: Diego Silva

6.2.9 Administración de ancho de banda

6.2.9.1 Escenario

El servidor está conectado al ADSL que tiene un ancho de banda de 1024Kbps de bajada por 512Kbps de subida mediante una tarjeta de red eth0 a 10/100/1000 Mbps; a la red local se conecta con otra interfaz eth1 a una velocidad de 10/100/1000Mbps. El internet se encuentra compartido mediante el servicio Proxy con squid por el puerto 8080, además se desea que un grupo de equipos de todas las subredes ocupen menor ancho de banda porque acceden únicamente al correo por el puerto 3128; los equipos de contabilidad se conectan a un servidor citrix por el puerto 1494; se utilizan 2 equipos que se conectan a un servidor mail para descargar y enviar el correo institucional, otros servicios como el ftp y el ssh son utilizados rara vez y únicamente por el personal de informática. Se desea también que las actualizaciones de antivirus ocupen un ancho de banda menor, por lo cual se realizara por el puerto 8181.

6.2.9.2 Instalación

Verificar si tenemos instalado el paquete iproute que se instala en la mayoría de servidores Linux

```
rpm –q iproute
```

Sino lo tenemos instalado lo hacemos con el siguiente comando

```
yum –y install iproute
```

6.2.9.3 Definición de Reglas

Se deben crear las reglas de limitación de ancho de banda, tanto para entrada como para salida para los servicios deseados, a continuación se incluyen los archivos y la descripción de cada archivo para la limitación de ancho de banda; los mismos que se crean en el directorio /etc/sysconfig/cbq/

Fichero:	**cbq-0002.internet-out**	**cbq-0007.internet.in**
Descripción:	Limita el ancho de banda de la interfaz eth0 para los equipos que ingresan a internet a través de sus puertos incluyendo el proxy	Limita el ancho de banda de las conexiones entrantes a los equipos de la red local a través de los puertos de internet
Contenido:	DEVICE=eth0,1024Kbit RATE=304Kbit WEIGHT=102Kbit PRIO=5 RULE=192.168.43.0/24,:80 RULE=192.168.43.0/24,:443 RULE=192.168.43.0/24,:8080	DEVICE=eth0,1024Kbit RATE=712Kbit WEIGHT=102Kbit PRIO=5 RULE=:80,192.168.43.0/24 RULE=:443,192.168.43.0/24 RULE=:8080,192.168.43.0/24
Fichero:	**cbq-0004.citrix-out**	**cbq-0003.citrix-in**
Descripción:	Limita el ancho de banda de la interfaz eth0 para los equipos que ingresan a la aplicación financiera del citrix	Limita el ancho de banda de las conexiones entrantes a los equipos de de la red local para conectarse al citrix

Contenido:	DEVICE=eth0,1024Kbit RATE=54Kbit WEIGHT=102Kbit PRIO=5 RULE=192.168.43.0/24,:1494 RULE=192.168.43.0/24,:1604	DEVICE=eth0,1024Kbit RATE=56Kbit WEIGHT=102Kbit PRIO=5 RULE=:1494,192.168.43.0/24 RULE=:1604,192.168.43.0/24
Fichero:	**cbq-0009.comodo-out**	**cbq-0008.comodo-in**
Descripción:	Limita el ancho de banda de la interfaz eth0 para actualización de los antivirus	Limita el ancho de banda de las conexiones entrantes para actualización de antivirus
Contenido:	DEVICE=eth0,1024Kbit RATE=34Kbit WEIGHT=102Kbit PRIO=5 RULE=192.168.43.0/24,8181:	DEVICE=eth0,1024Kbit RATE=50Kbit WEIGHT=102Kbit PRIO=5 RULE=:8181
Fichero:	**cbq-0006.otros-out**	**cbq-0005.otros-in**
Descripción:	Limita el ancho de banda de la interfaz eth0 de las conexiones salientes hacia los puertos conocidos incluido el servicio de internet por el puerto 3128 para usuarios que no utilizan mucho el internet	Limita el ancho de banda de las conexiones entrantes de algunos puertos conocidos, incluyendo a usuarios que no utilizan el internet comúnmente
Contenido:	DEVICE=eth0,1024Kbit RATE=120Kbit WEIGHT=102Kbit PRIO=5 RULE=192.168.43.0/24,:20 RULE=192.168.43.0/24,:21 RULE=192.168.43.0/24,:22 RULE=192.168.43.0/24,:25 RULE=192.168.43.0/24,:465	DEVICE=eth0,1024Kbit RATE=206Kbit WEIGHT=102Kbit PRIO=5 RULE=:20,192.168.43.0/24 RULE=:21,192.168.43.0/24 RULE=:22,192.168.43.0/24 RULE=:25,192.168.43.0/24 RULE=:465,192.168.43.0/24

	RULE=192.168.43.0/24,:587 RULE=192.168.43.0/24,:110 RULE=192.168.43.0/24,:143 RULE=192.168.43.0/24,:993 RULE=192.168.43.0/24,:995 RULE=192.168.43.0/24,:3128	RULE=:587,192.168.43.0/24 RULE=:110,192.168.43.0/24 RULE=:143,192.168.43.0/24 RULE=:993,192.168.43.0/24 RULE=:995,192.168.43.0/24 RULE=:3128,192.168.43.0/24

Tabla 6-18. Archivos de configuración de cbq
Fuente: Servidor
Elaborado por: Diego Silva

6.2.9.4 Iniciar, detener y reiniciar el servicio

El guión de inicio de cbq está instalado como /sbin/cbq. Es necesario copiar este fichero dentro de /etc/init.d/ y tratarlo igual que cualquier otro servicio del sistema.

```
cp -a /sbin/cbq /etc/init.d
```

Para probar que las clases están correctas antes de utilizar éstas, se debe primero compilar:

```
service cbq compile
```

Para la ejecución, reinicio y parada del sistema al igual que los otros servicios con start, restart y stop.

Para supervisar las estadísticas del trafico utilizar:

```
service cbq stats
```

Por último hacer que arranque con el sistema

```
chkconfig cbq on
```

6.2.10 Configuración de Monitoreo de red con Cacti

Requiere tener instalados los siguientes paquetes:

- httpd
- php
- php-mysql
- php-snmp
- mysql

- mysql-serve
- net-snmp

6.2.10.1 Instalación:

Se puede realizar de forma manual descargando cada uno de los paquetes, o a su vez se puede realizar la instalación desde un repositorio de paquetes, la ventaja de la descarga e instalación directa de un repositorio es que analiza e instala también las dependencias de los paquetes.

Obtener el repositorio

```
#  wget  http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm
```

Instalar el repositorio

```
# rpm -Uvh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
```

Instalar la herramienta RRDTool

```
# yum –y install rrdtool
```

Instalar CACTI

```
# yum –y install cacti
```

6.2.10.2 Configuración PHP

Verificar que PHP tenga integrado o instalado los siguientes módulos de extensión PHP: mysql, SNMP, XML, Session, Sockets. Con el comando

```
php –m
```

Activar mysql en el fichero /etc/php.d/mysql.ini

```
; Enable mysql extension module
extension=mysql.so
```

Activar SNMP en el fichero /etc/php.d/snmp.ini

```
; Enable snmp extension module
extension=snmp.so
```

6.2.10.3 Configuración Apache

Localizar el archivo de configuración y editar /etc/httpd/conf/httpd.conf y verificar la siguiente línea o incluirla

```
# Load config files from the config directory # "/et
/httpd/conf.d".
Include conf.d/*.conf
```

Ahora editar el archivo /etc/httpd/conf.d/php.conf y verificar o añadir las siguientes líneas

```
LoadModule php5_module modules/libphp5.so
AddHandler php5-script .php
AddType text/html .php
DirectoryIndex index.php
```

6.2.10.4 Configuración MySQL

Como es la primera vez que utilizamos MySQL; iniciar el servicio, agregar el servicio al arranque del sistema y establecer un password para acceder

```
service mysqld start
chkconfig mysqld on
mysqladmin --user=root password somepassword
mysqladmin --user=root --password reload
```

Crear la base de datos

```
mysqladmin --user=root -p create cacti
```

Importar la base de datos, se debe estar ubicado en el directorio cacti /var/www/cacti

```
mysql cacti < cacti.sql
```

Crear un usuario con su password para MySQL

```
mysql --user=root -p mysql
> GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY
'password';
> flush privileges;
```

Editar el archivo `/var/www/cacti/include/config.php` y añadir el nombre del usuario creado con su password para que pueda acceder a la base de datos

```
$database_type = "mysql";
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cactiuser";
$database_password = "dpst711022";
$database_port = "3306";
```

6.2.10.5 Configuración SNMP

Simple Network Management Protocol o Protocolo Simple de administración de red. Está diseñado para facilitar el intercambio de información entre dispositivos de red y es ampliamente utilizado en la administración de redes para supervisar el desempeño, la salud y el bienestar de una red, equipo de cómputo y otros dispositivos.

Sacar una copia de respaldo del archivo de configuración y crear un nuevo vacio

```
# mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.respaldo
# nano snmpd.conf
```

Añadir el siguiente contenido

```
com2sec local 127.0.0.1/32 local711022
com2sec miredlocal 192.168.43.0/24 miredlocal711022
#se asigna local al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
#Se asigna miredlocal al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal
## name incl/excl subtree mask(optional)
view all included .1 80
##group context sec.mod sec.lev prefix read write notif
access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all all all
syslocation Servidor proxy de la DPST
```

```
syscontact Administrador (root@proxy.dpst)
```

Aquí se encuentra definido en la primera sección las listas de control de acceso, una para local y otra para toda la red. A continuación se crean dos grupos uno de lectura escritura y otro de solo lectura, y se asigna a la regla local y a la regla miredlocal respectivamente. Se especifican las ramas permitidas que con la línea escrita es lo mas común para utilizarlo con CACTI. Se asignan los permisos a cada grupo y por ultimo definimos dos parámetros con carácter informativo.

Iniciar, detener, reiniciar el servicio y añadirlo al arranque del sistema.

```
service snmpd start
chkconfig snmpd on
```

Realizar comprobaciones para verificar que el servicio snmp este funcionando correctamente

snmpwalk -v 1 192.168.43.10 -c miredlocal711022 system
snmpwalk -v 1 192.168.43.10 -c miredlocal711022 interfaces

SNMP trabaja en los puertos 161 y 162, los cuales hay que desbloquear. En el script firewall incluir las siguientes líneas y volver a ejecutarlo

```
#Desbloqueo de los puertos para snmp
iptables -A INPUT -i eth1 -p udp -s 192.168.43.0/24 -d 192.168.43.10
--dport 161 -j ACCEPT
iptables -A OUTPUT -o eth1 -p udp -s 192.168.43.10 --sport 161 -d
192.168.43.0/24 -j ACCEPT

iptables -A INPUT -i eth1 -p udp -s 192.168.43.0/24 -d 192.168.43.10
--dport 162 -j ACCEPT
iptables -A OUTPUT -o eth1 -p udp -s 192.168.43.10 --sport 162 -d
192.168.43.0/24 -j ACCEPT
```

6.2.10.6 Configuración CACTI

Dar los permisos apropiados a los directorios de creación de gráficos y log dentro del directorio cacti /var/www/cacti

```
chown -R diego rra/ log/
```

Añadir la siguiente línea en el fichero /etc/crontab para la generación automática de los reportes cada 5 minutos

```
*/5 * * * * diego php /var/www/cacti/poller.php > /dev/null 2>&1
```

Ejecutar los siguientes comandos desde el directorio de Cacti que descargara los parches y los aplicara

```
wget   http://www.cacti.net/downloads/patches/0.8.7g/data_source_deactivate.patch
wget          http://www.cacti.net/downloads/patches/0.8.7g/graph_list_view.patch
wget              http://www.cacti.net/downloads/patches/0.8.7g/html_output.patch
wget
http://www.cacti.net/downloads/patches/0.8.7g/ldap_group_authenication.patch
wget
http://www.cacti.net/downloads/patches/0.8.7g/script_server_command_line_parse.p
atch
wget http://www.cacti.net/downloads/patches/0.8.7g/ping.patch
wget http://www.cacti.net/downloads/patches/0.8.7g/poller_interval.patch

patch -p1 -N < data_source_deactivate.patch
patch -p1 -N < graph_list_view.patch
patch -p1 -N < html_output.patch
patch -p1 -N < ldap_group_authenication.patch
patch -p1 -N < script_server_command_line_parse.patch
patch -p1 -N < ping.patch
patch -p1 -N < poller_interval.patch
```

En el navegador de internet digitar http://proxy.dpst/cacti/index.php y se presenta el dialogo de acceso, el usuario y password es admin, ingresar y cambiar el password

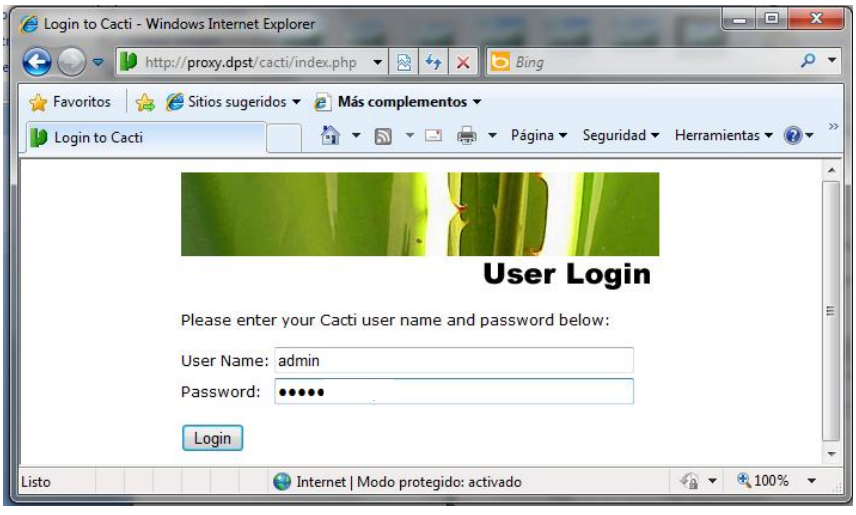


Fig. 6-44. Inicio de sesión cacti
Fuente: Servidor
Elaborado por: Diego Silva

A continuación se presenta el ambiente de Cacti

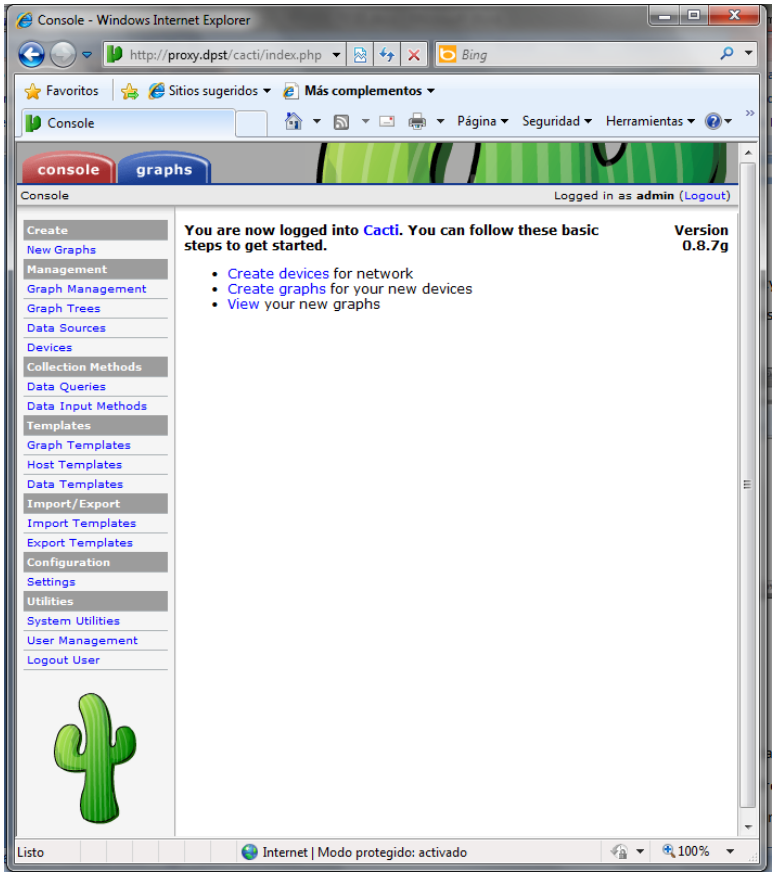


Fig. 6-45. Pantalla de usuario cacti
Fuente: Servidor
Elaborado por: Diego Silva

Como indica en el mismo sitio el primer paso es crear el dispositivo, haciendo clic en Create Device o desde el submenú Management -> Devices y se redirigirá hacia la siguiente página (Fig. 6-46) donde por defecto ya está creado el dispositivo localhost

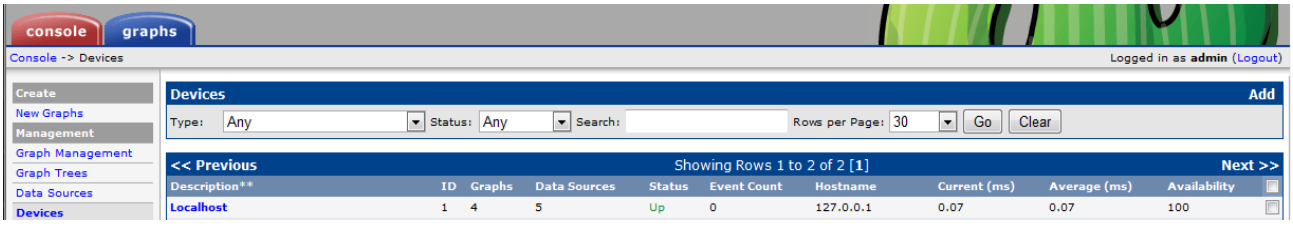


Fig. 6-46. Creación de dispositivos
Fuente: Servidor
Elaborado por: Diego Silva

Damos clic en Add y se envía a la siguiente página donde se debe ingresar los datos del dispositivo que se está creando en este caso el servidor así como la información de SNMP definida anteriormente

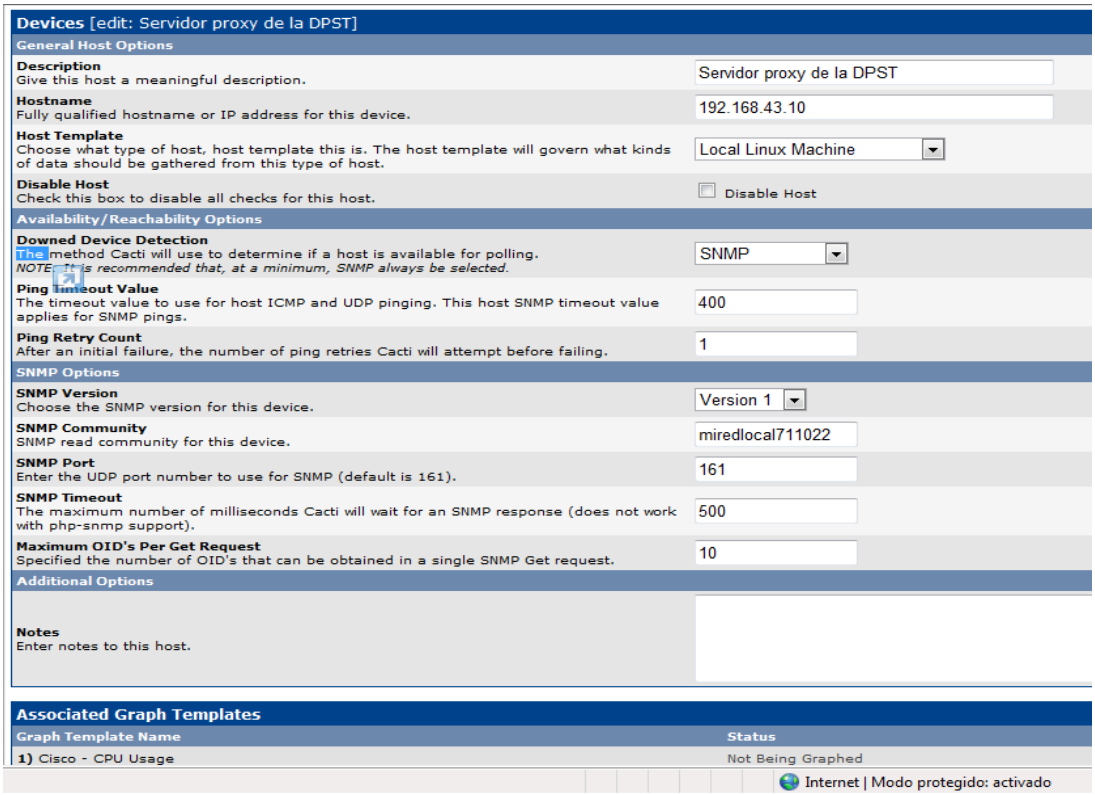


Fig. 6-47. Información nuevo dispositivo
Fuente: Servidor
Elaborado por: Diego Silva

Continuando con la pagina seleccionar los gráficos que se van a crear, dar clic en save y posteriormente en create graphs for this host

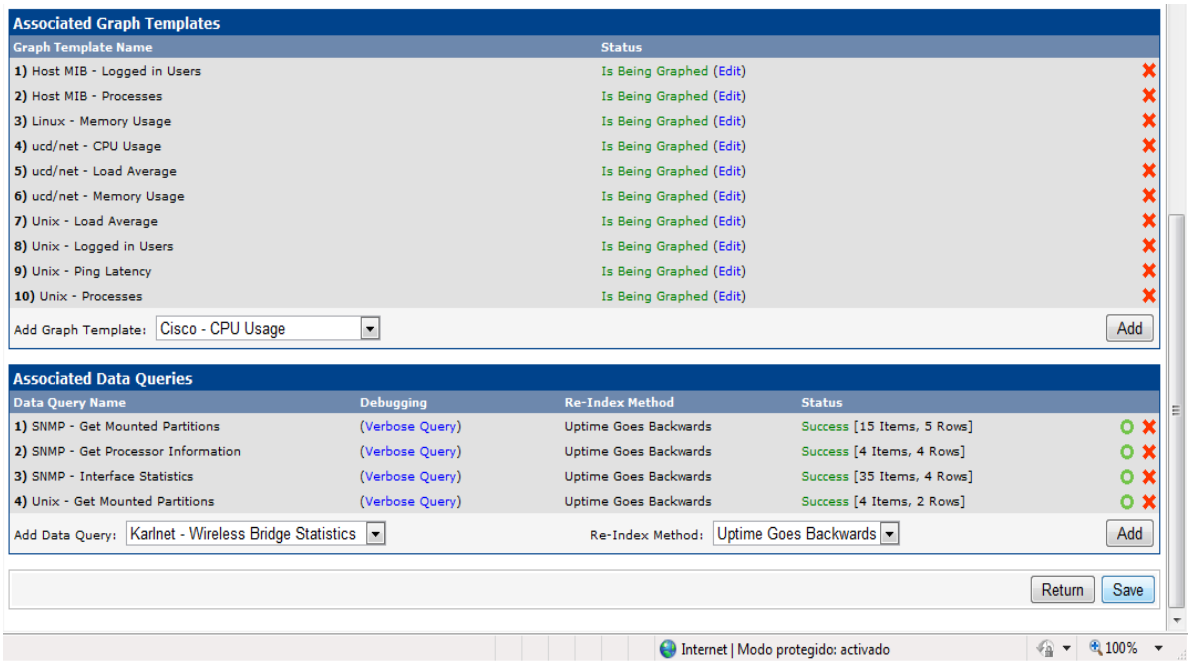


Fig. 6-48. Gráficos a crearse
Fuente: Servidor
Elaborado por: Diego Silva

Se aprecia la lista de gráficos que se crearan el dar clic en create

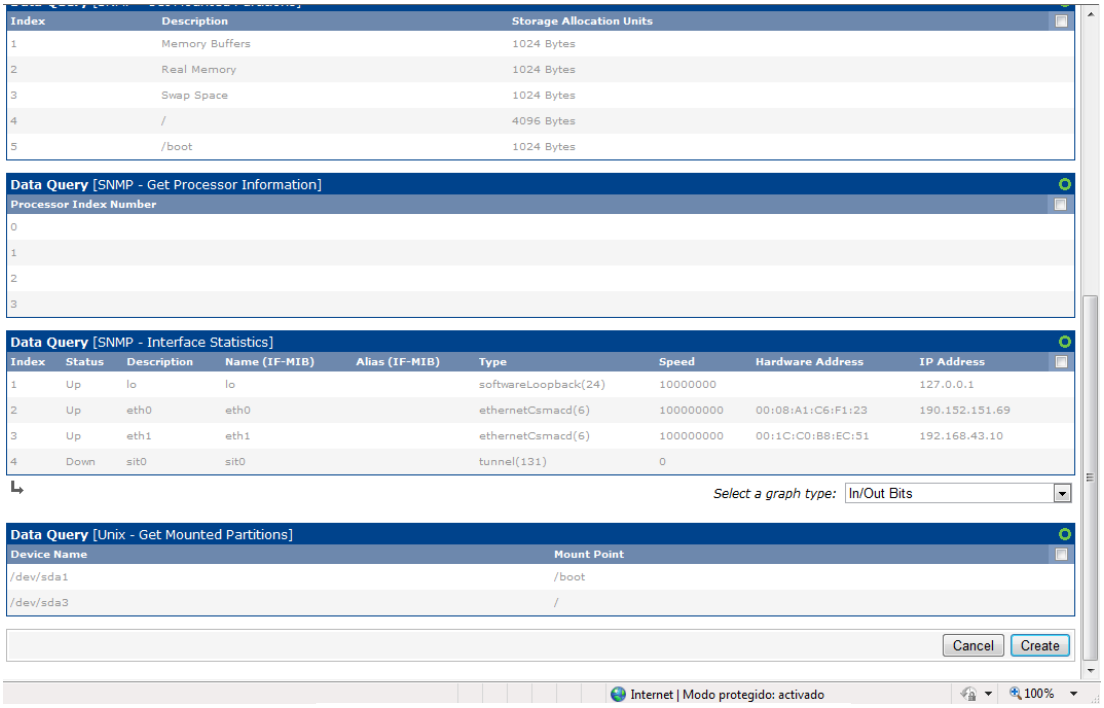


Fig. 6-49. Lista de gráficos
Fuente: Servidor
Elaborado por: Diego Silva

En la pestaña graphs ya se puede ver los gráficos creados y navegar a través de ellos verificando la información requerida como el ancho de banda utilizado, el uso de memoria y CPU, lo cual ayudara posteriormente a tomar decisiones administrativas

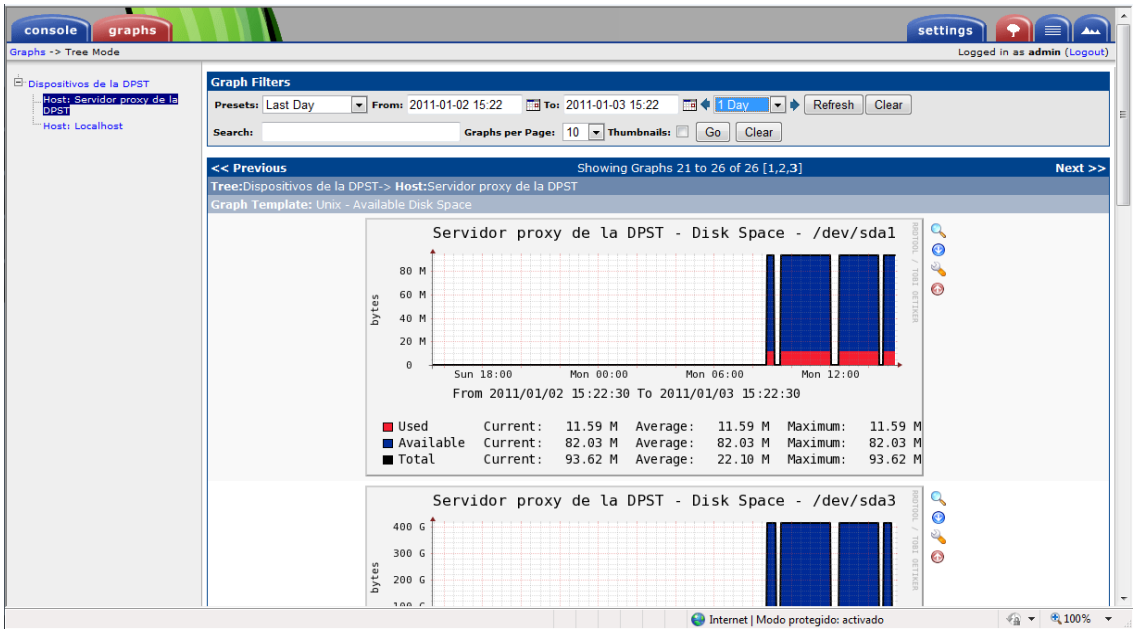


Fig. 6-50. Gráficos Generados
Fuente: Servidor
Elaborado por: Diego Silva

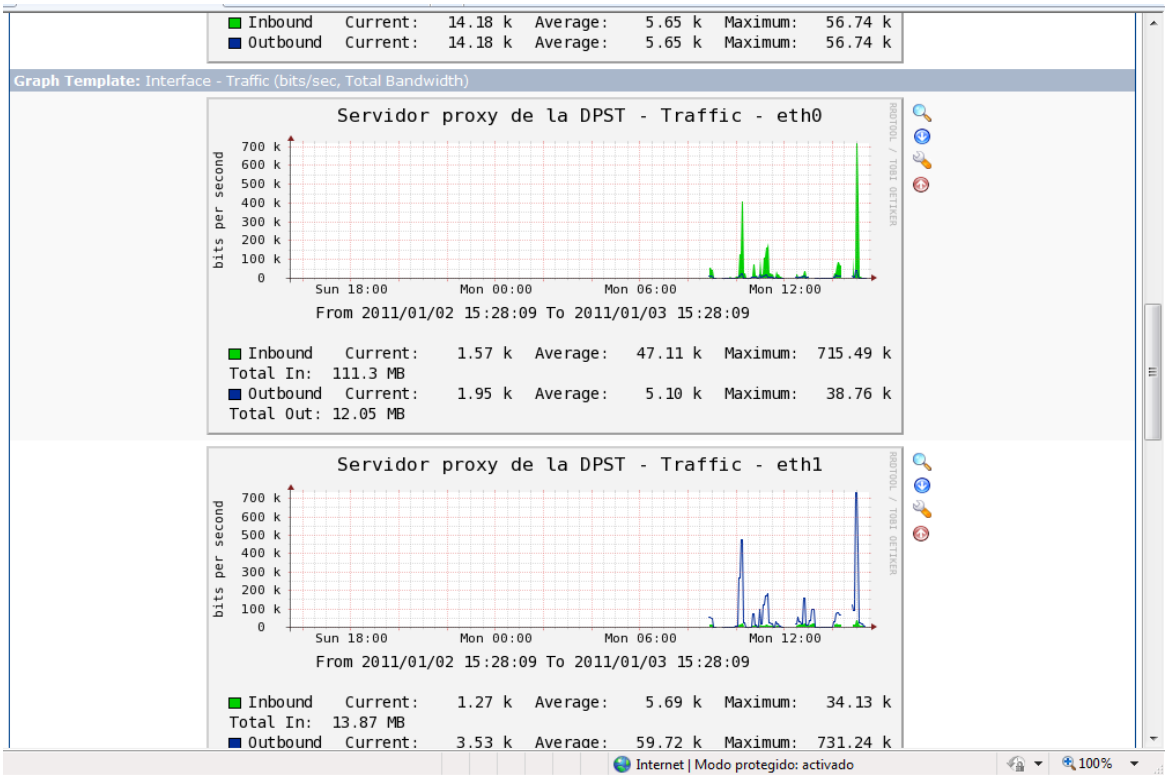


Fig. 6-51. Gráficos Generados
Fuente: Servidor
Elaborado por: Diego Silva

6.2.11 Configuración de Antivirus

Anteriormente para otras aplicaciones ya se instaló el repositorio de paquetes, por lo cual se puede instalar únicamente a través de yum los paquetes necesarios

```
# yum install -y clamav clamav-update
```

Crear un usuario y grupo clamav que será exclusivo para la ejecución del antivirus.

```
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav
```

Instalar a través de yum, con esto se crean los directorios necesarios y la aplicación esta lista para su funcionamiento

```
# yum -y install clamav clamav-update
```

Configurar freshclam para que se puedan realizar las actualizaciones. Editar el archivo /etc/freshclam y comentar la línea 8 que contiene Example

```
# Comment or remove the line below.
```

```
# Example
```

Ahora se puede ejecutar el comando freshclam y se bajaran las actualizaciones de la base de datos del antivirus, se puede agregar un comando en el crontab para que el antivirus se actualice por lo menos una vez al día. Editar el crontab agregar la línea siguiente y salir guardando con Esc:wq

```
# crontab -e
30 22 * * * freshclam
```

Para revisar un archivo sospechoso que puede estar infectado hacerlo de la siguiente manera:

```
# clamscan /ruta/del/fichero
```

Y para revisar todo un directorio y su contenido hacerlo de la siguiente manera:

```
# clamscan –r /ruta/del/directorio
```

Para especificar que los ficheros infectados solo sean movidos a un directorio de cuarentena, se utiliza el mandato clamscan con la opción **--**move especificando un directorio que servirá como cuarentena. El directorio de cuarentena debe de existir previamente.

```
# mkdir /antivirus/cuarentena
#        clamscan        --move=/antivirus/cuarentena        -r
/ruta/del/directorio
```

Se pueden eliminar las infecciones detectadas, pero no es recomendable porque pueden afectar al sistema. Se puede llevar una bitácora del resultado de los análisis para examinarla detenidamente y posteriormente tomar una decisión.

```
# clamscan --log=/antivirus/log/clamscan.log --infected --
remove=yes –r /ruta/del/directorio
```

6.2.12 Firewall Local

Es necesario utilizar un software de libre distribución, y para este aplicativo el mejor encontrado a sido COMODO, el cual podemos instalarlo en cada equipo sobre la plataforma windows, para ofrecer una seguridad extra, además de proteger conexiones entrantes no deseadas ya sea desde internet o

a nivel de la red local por servicios innecesarios que pueden ser virus intentando propagarse o intrusiones en busca de información del equipo.

6.2.12.1 Descarga:

Visitar el sitio www.comodo.com y ubicar la edición de 32 y 64 bits para instalarla en los equipos de acuerdo a las necesidades.

6.2.12.2 Instalación

Al ejecutar la aplicación el primer paso es elegir el lenguaje

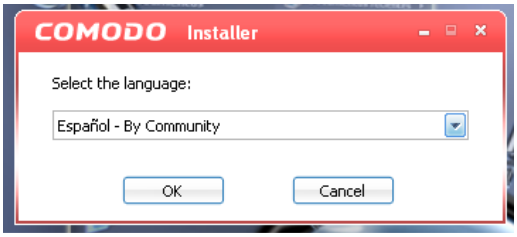


Fig. 6-52. Idioma instalación COMODO
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Aceptar el acuerdo de licencia

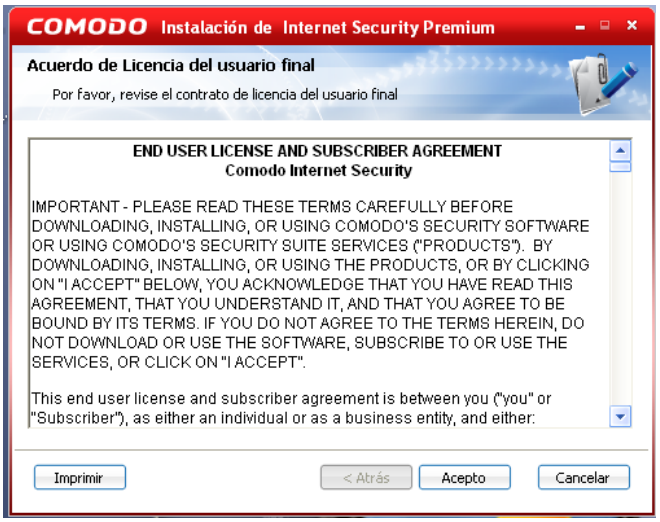


Fig. 6-53. Acuerdo de licencia
Fuente: Equipo Cliente
Elaborado por: Diego Silva

El siguiente es un paso alternativo, introducir la dirección e-mail para posteriormente recibir noticias o actualizaciones de la aplicación.

Fig. 6-54. E-mail (Alternativo)
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Elegir los productos a instalar, puede ser solamente el antivirus o el firewall o los dos a la vez

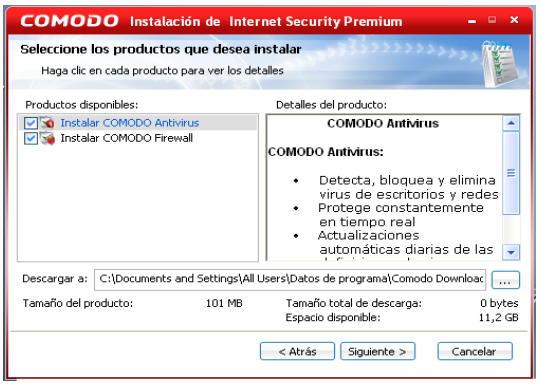


Fig. 6-55. Selección de paquetes
Fuente: Equipo Cliente
Elaborado por: Diego Silva

El instalador extrae los paquetes para su posterior instalación

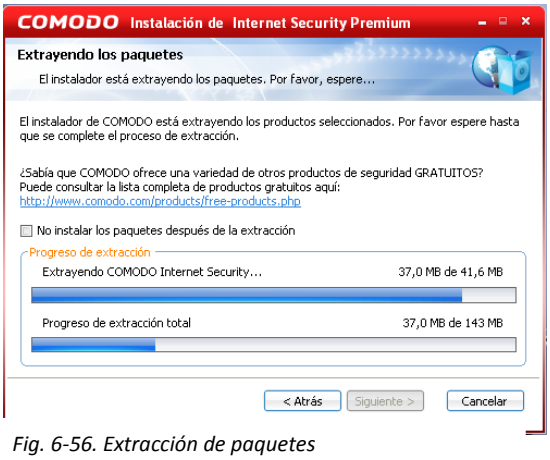


Fig. 6-56. Extracción de paquetes
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Elegir el destino de la instalación

Fig. 6-57. Destino de instalación
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Se puede ingresar a una comunidad para recibir estadísticas sobre infecciones y que decisiones se han tomado

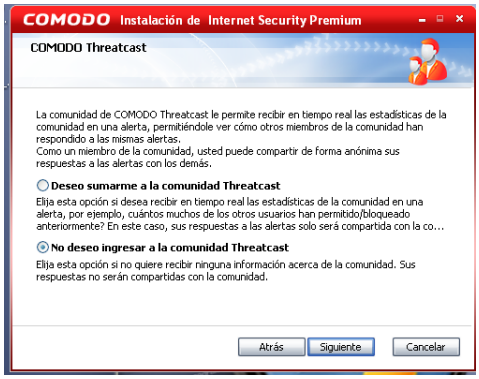


Fig. 6-58. Formar parte de Threadcast
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Alternativamente se puede utilizar los servidores DNS de COMODO, pero para la configuración de la intranet no es necesario

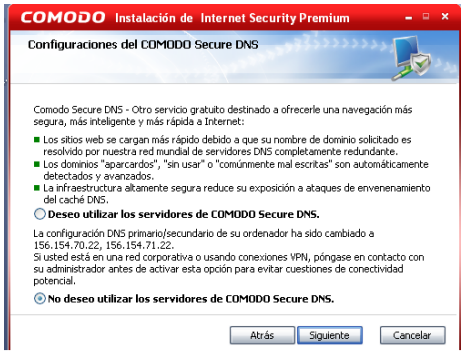


Fig. 6-59. Servicio de DNS seguro
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Se puede iniciar la instalación o cambiar las opciones

Fig. 6-60. Aviso de inicio de instalación
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Se muestra el progreso de la instalación

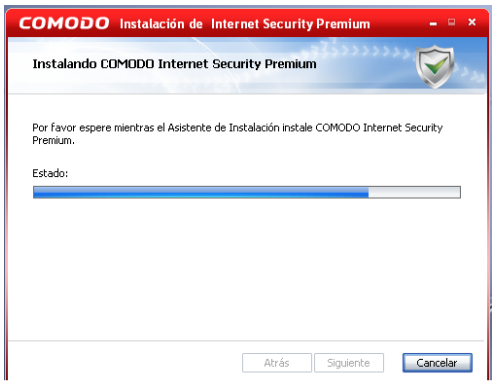


Fig. 6-61. Progreso de instalación
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Muestra la finalización de la instalación y la activación de la licencia gratuita y posteriormente pide el reinicio del esquipo

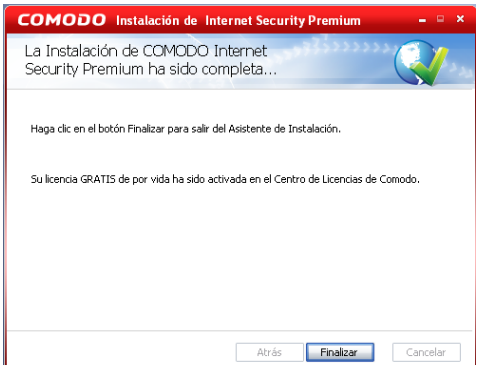


Fig. 6-62. Finalización de instalación
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Al iniciarse por primera vez aparece la ventana donde se dice al firewall que aprenda la dirección de la intranet que es confiable, marcar los otros casilleros para poder ser accesible por el resto de equipos de la red y para no volver a detectar nuevas redes en caso de cambio de IP

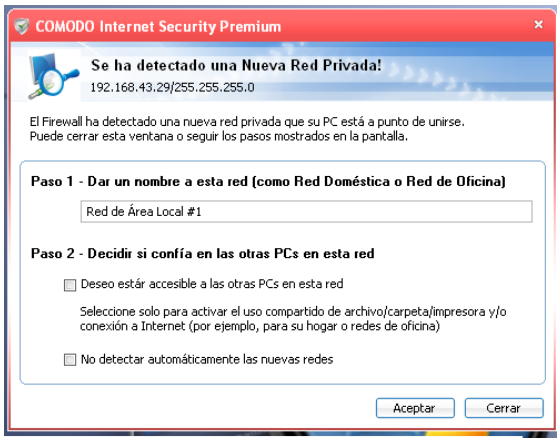


Fig. 6-63. Acuerdo de licencia
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Al ejecutar una aplicación puede ser capturada e inmediatamente denegada a no ser que se enseñe al firewall que es una aplicación seguro permitiendo de esta manera su ejecución

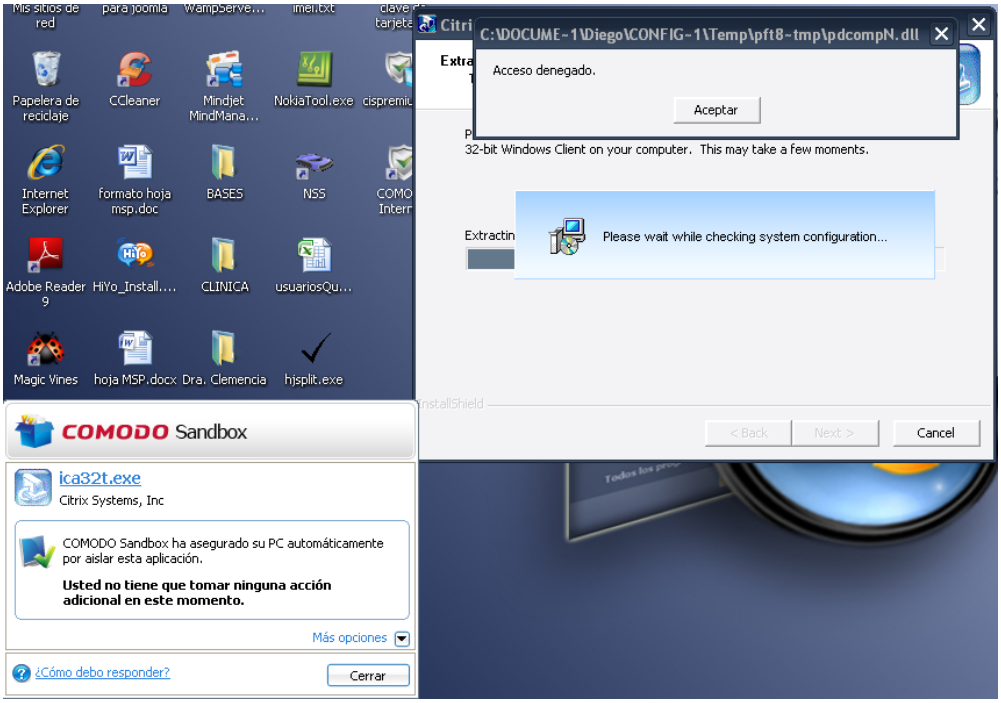


Fig. 6-64. Protección con Sandbox
Fuente: Equipo Cliente
Elaborado por: Diego Silva

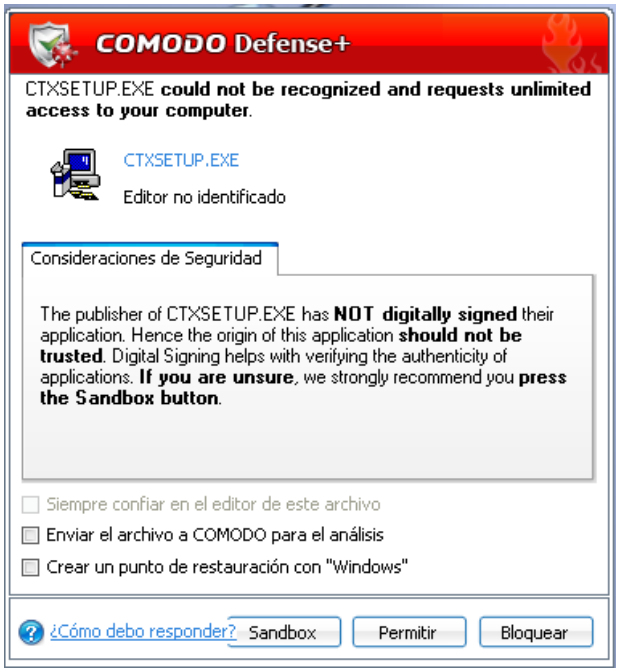


Fig. 6-65. Protección por cambios que desea realizar una aplicación
Fuente: Equipo Cliente
Elaborado por: Diego Silva

Adquiere las mismas funcionalidades que un firewall y un antivirus, se pueden realizar análisis programados y definir reglas en el firewall tanto para aplicaciones como para conexiones por determinados puertos. Ofrece una ayuda importante en el momento que alguien desea acceder al equipo pues primero avisa del intento de conexión y se puede aceptar o rechazarla, evitando de esta manera la propagación de virus y las conexiones no deseadas, así como la ejecución de programas indeseados.

6.2.13 Configuración de Equipos de Conexión

La institución cuenta con 4 Access Points DWL-3200AP. Este es un poderoso, robusto y fiable Access Point para operar en entornos de empresas con diversos negocios. Diseñado para instalaciones Indoor, este Access Point provee opciones avanzadas de seguridad para los administradores de red, permitiendoles desplegar una administración muy robusta en redes wireless. El Access Point DWL-3200AP soporta Power Over Ethernet (PoE) y provee dos antenas de alta ganancia para una óptima cobertura wireless.

6.2.13.1 Principales Características y Facilidades:

- Soporte de Multiples SSID's
- Soporte 11g, 108Mbps Modo Turbo
- Robusto Access Point para soluciones Indoor

- Soporte de PoE (Power over Ethernet), 802.3af
- Soporte WEP,
- Soporte WPA, AES y 802.11i
- Seguridad Ampliada, con soporte de ACL, 802.1x y MAC Address Filtering
- Administración versátil, vía D-Link D-View, SNMP v3, Web, Telnet y AP Manager.

6.2.13.2 Configuración

Para la configuración y administración del AP conectarlo ya sea a la red o con un cable cruzado directamente a un equipo; en el navegador digitar http://192.168.0.50 que es la dirección que viene configurada por defecto en el equipo. El sitio pide autenticarse, el usuario y la clave inicial es admin.

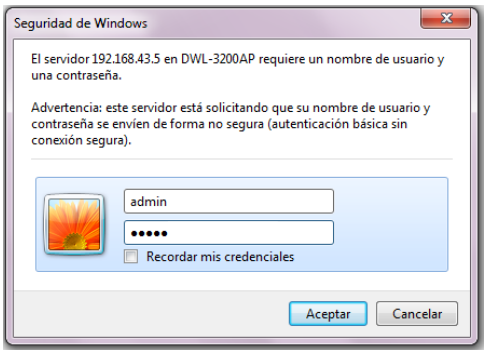


Fig. 6-66. Acceso al AP
Fuente: Access Point
Elaborado por: Diego Silva

La pantalla de inicio del sitio del AP donde muestra información básica como el modelo, el firmware y la IP del equipo que ya está configurada con su IP correspondiente dentro de la intranet.

Fig. 6-67. Ambiente de configuración del AP
Fuente: Access Point
Elaborado por: Diego Silva

En el submenú Wireless establecer el modo de trabajo que será como Access Point, indicar el nombre del equipo que anteriormente se definió, habilitar el SSID Broadcast y una frase de paso o clave. Para guardar estas configuraciones dar clic en Apply

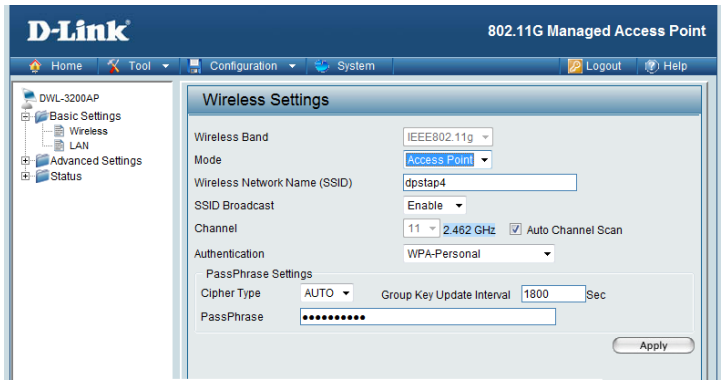


Fig. 6-68. Configuración de acceso como AP
Fuente: Access Point
Elaborado por: Diego Silva

En el submenú LAN establecer la configuración IP

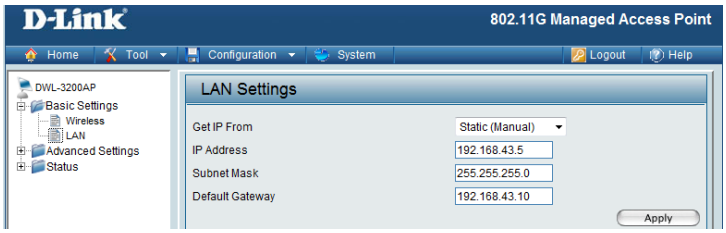


Fig. 6-69. Configuración LAN
Fuente: Access Point
Elaborado por: Diego Silva

Configurar el acceso solamente para el apdlink2 con DHCP para los equipos que se conectaran en el auditorio y necesiten internet, indicar el inicio del direccionamiento dinámico, indicar el rango de IPs a asignar, indicar la máscara para indicar que es una subnet y de esta manera evitar accesos a sitios indeseados a través del squid

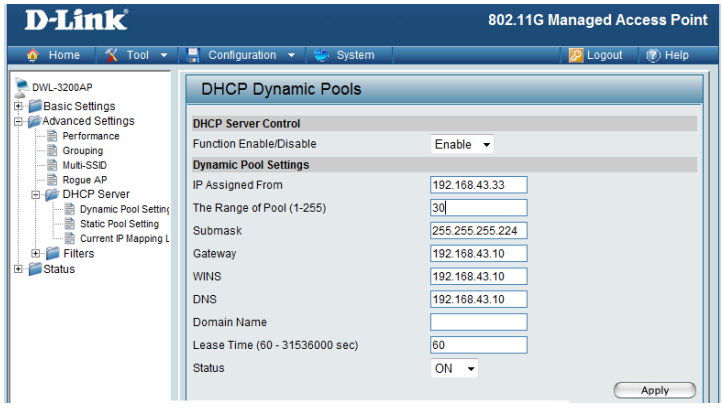


Fig. 6-70. Configuración DHCP
Fuente: Access Point
Elaborado por: Diego Silva

En el menú Tool ubicado en la parte superior elegir “Administrator Settings” para realizar un cambio de clave del administrador del equipo.

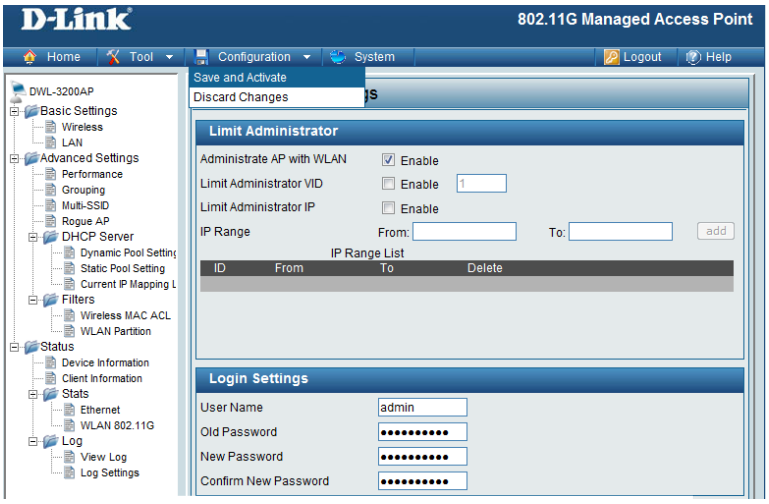


Fig. 6-71. Configuración de Acceso de Administrador
Fuente: Access Point
Elaborado por: Diego Silva

Para que los cambios surtan efecto en el menú Configuration dar clic en “Save and Activate”, se guardaran las configuraciones y el AP se reiniciara poniendo en marcha las configuraciones establecidas.

6.3 Conclusiones

- La implementación de esquemas de seguridad ha optimizado notablemente el desempeño tanto en la intranet como hacia el internet
- Se ha minimizado ataques de virus, así como el robo o pérdida de información gracias a la aplicación de las políticas de seguridad
- Se cumplió eficientemente el decreto presidencial de software libre, eliminando posibles problemas futuros y brindando un servicio de calidad en la red
- Con la compartición de internet a través de Squid y la limitación de ancho de banda con cbq, se ofrece un acceso más dinámico y controlado, evitando problemas y cortes que ocurrían con frecuencia con el servidor Windows.
- La administración de la red ofrece facilidad para la toma de decisiones, gracias a las herramientas de monitoreo e informes
- La protección de la información de los clientes ha sido mejorada, evidencia de ello es la menor frecuencia con la que los equipos presentan fallos en el sistema

6.4 Recomendaciones

- Crear usuarios con cuentas limitadas en los servidores y en todos los equipos de la institución lo cual ayuda a evitar daños en el sistema en los casos de ataques o virus. Y escalar privilegios a administrador solamente cuando sea necesario.
- Monitorear continuamente los informes de estado del equipo y de la red, para evitar una sobrecarga y posible colapso del servidor y tomar decisiones administrativas a tiempo
- Brindar acceso a internet a equipos ajenos a la institución con IPs dinámicas temporales para mantenerlos aislados de los equipos de la institución.
- Mejorar los procesos del plan mantenimiento de equipos incluyendo monitoreo de actividades en tiempo real para brindar asistencia remota
- Chequear periódicamente los directorios compartidos con el antivirus tanto del servidor como de los clientes.
- Adecuar el entorno del APD para un mejor desempeño de las actividades

6.5 Bibliografía

6.5.1 Libros

Samba, Squid, mrtg, ancho de banda, cbq - Barrios, Joel (2009). "Implementación de Servidores con GNU/Linux". Libro electrónico descargado de www.alcancelibre.org

PAZMAY, Galo (2004). "Guía práctica para la elaboración de tesis y trabajos de investigación", Editorial Freire, Riobamba.

Conceptos de Redes, protocolos y servicios – IBM (2004). "Linux Network Administration I: TCP/IP and TCP/IP services"

Seguridad de Redes, Configuración del sistema Linux – IBM (2004). "Linux Network Administration II: Network Security and Firewalls".

6.5.2 Páginas Web

Subneteo VLSM [en línea], Disponible de World Wide Web: http://es.wikipedia.org/wiki/VLSM

CentOS [en línea], Disponible de World Wide Web: http://es.wikipedia.org/wiki/CentOS

CentOS [en línea], Disponible de World Wide Web: www.centos.org

Router ADSL [en línea], Disponible de World Wide Web: http://es.wikipedia.org/wiki/Router_ADSL

Access Point [en línea], Disponible de World Wide Web: http://es.wikipedia.org/wiki/Acces_point

Servicios de red [en línea], Disponible de World Wide Web: http://www.linuxfoundation.org/en/Net:Bonding

Servicios de red [en línea], Disponible de World Wide Web: http://www.kernel.org/pub/linux/kernel/people/marcelo/linux2.4/Documentation/networking/bonding.txt

Configuración de Iptables [en línea], Disponible de World Wide Web: http://oceanpark.com/notes/firewall_example.html

Seguridad en Redes [en línea], Disponible de World Wide Web: www.securytiportal.com

Herramientas hacker [en línea], Disponible de World Wide Web: www.insecure.org

Herramientas firewall para Linux [en línea], Disponible de World Wide Web: www.linux-firewall-tools.com

Blog de Seguridad Informática. [en línea], Disponible de World Wide Web: http://redesysegu.blogspot.com/

Redes de Comunicaciones, Políticas de Seguridad. [en línea], Disponible de World Wide Web:http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-Redes_de_comunicaciones.pdf

Manual de seguridad de Redes. [en línea], Disponible de World Wide Web: http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

Políticas de Seguridad. [en línea], Disponible de World Wide Web: http://www.segu-info.com.ar/politicas/

Seguridad de Redes en Pymes. [en línea], Disponible de World Wide Web: http://www.vdigitalrm.com/archivos/guia_seguridad_pymes.pdf

6.6 Anexos

Anexo 1. Cuestionario 1

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISEMAS ELECTRONICA E INDUSTRIAL

Carrera: Ingeniería en sistemas computacionales e informáticos.

Encuesta dirigida a: Informático Provincial

Nota: La información que se recopile, será de uso exclusivo para el desarrollo de la tesis a efectuarse en la Dirección Provincial de Salud de Tungurahua

Recomendaciones: Por favor marque con una x en un solo ítem por pregunta.

Cuestionario:

¿Mediante que dispositivo se tiene la conexión a Internet?

ADSL/Router ( ) Modem Inalámbrico ( )

¿Cuál es la velocidad de bajada?

2048 ( ) 1024 ( ) 512 ( ) 256 ( ) 128 ( )

¿Cuál es la velocidad de subida?

1024 ( ) 512 ( ) 256 ( ) 128 ( ) 64 ( )

Características:

Procesador: _____

Memoria: _____

Disco duro: _____

¿Existen inconvenientes en reemplazar el sistema operativo actual por una distribución linux?

Si ( ) No ( )

¿Se pueden configurar libremente los dispositivos?

Si ( ) No ( )

Anexo 2. Cuestionario 2

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL

Carrera: Ingeniería en sistemas computacionales e informáticos.

Encuesta dirigida a: Informático Provincial

Nota: La información que se recopile, será de uso exclusivo para el desarrollo de la tesis a efectuarse en la Dirección Provincial de Salud de Tungurahua

Recomendaciones: Por favor marque con una x en un solo ítem por pregunta.

Cuestionario:

¿Puede acceder a información de cualquier equipo de la red?

Si ( ) No ( )

¿Qué directorios comparte?

Mis documentos ( ) Disco C ( ) Disco D ( ) Otras Carpetas ( )

¿Revisa el flash antes de abrirlo?

Si ( ) No ( )

¿Qué paginas visita?

De gobierno ( ) De prensa ( ) Correo ( ) Descarga de programas, música, video, juegos ( )

Música, video, juegos en línea ( ) Redes sociales - hi5, facebook, etc. ( ) Pornografía ( )

¿Abre correos electrónicos de remitentes desconocidos?

Si ( ) No ( )

¿Con que frecuencia respalda sus archivos?

Diario ( ) Semanal ( ) Mensual ( ) Anual ( )

Anexo 3. Decreto Presidencial de uso de Software Libre

Registro oficial 322

No. 1014

Rafael Correa Delgado

PRESIDENTE CONSTITUCIONAL DE LA

REPUBLICA

Considerando:

Que en el apartado g) del numeral 6 de la Carta Iberoamericana de Gobierno Electrónico, aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, realizada en Chile el 1 de junio del 2007, se recomienda el uso de estándares abiertos y software libre, como herramientas informáticas;

Que es el interés del Gobierno alcanzar soberanía y autonomía tecnológica, así como un significativo ahorro de recursos públicos y que el software libre es en muchas instancias un instrumento para alcanzar estos objetivos;

Que el 18 de julio del 2007 se creó e incorporó a la estructura orgánica de la Presidencia de la República la Subsecretaría de Informática, dependiente de la Secretaría General de la Administración, mediante Acuerdo N° 119, publicado en el Registro Oficial No. 139 de 1 de agosto del 2007;

Que el numeral 1 del artículo 6 del Acuerdo N° 119, faculta a la Subsecretaría de Informática a elaborar y ejecutar planes, programas, proyectos, estrategias, políticas, proyectos de leyes y reglamentos para el uso de software libre en las dependencias del Gobierno Central; y,

En ejercicio de la atribución que le confiere el numeral 9 del artículo 171 de la Constitución Política de la República,

Decreta:

Artículo 1.- Establecer como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos.

Artículo 2.- Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Estos programas de computación tienen las siguientes libertades:

a) Utilización del programa con cualquier propósito de uso común;

b) Distribución de copias sin restricción alguna;

c) Estudio y modificación del programa (Requisito: código fuente disponible); y,

d) Publicación del programa mejorado (Requisito: código fuente disponible).

Artículo 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 el uso de este tipo de software.

Artículo 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 la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

Para efectos de este decreto se comprende como seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa de patrimonio nacional.

Para efectos de este decreto se entiende por un punto de no retorno, cuando el sistema o proyecto informático se encuentre en cualquiera de estas condiciones:

a) Sistema en producción funcionando satisfactoriamente y que un análisis de costo beneficio muestre que no es razonable ni conveniente una migración a software libre; y,

b) Proyecto en estado de desarrollo y que un análisis de costo - beneficio muestre que no es conveniente modificar el proyecto y utilizar software libre.

Periódicamente se evaluarán los sistemas informáticos que utilizan software propietario con la finalidad de migrarlos a software libre.

Artículo 5.- Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:

a) Nacionales que permitan autonomía y soberanía tecnológica;

b) Regionales con componente nacional;

c) Regionales con proveedores nacionales;

d) Internacionales con componente nacional;

e) Internacionales con proveedores nacionales; y,

f) Internacionales.

Artículo 6.- La Subsecretaría de Informática como órgano regulador y ejecutor de las políticas y proyectos informáticos en las entidades del Gobierno Central deberá realizar el control y seguimiento de este decreto.

Para todas las evaluaciones constantes en este decreto la Subsecretaría de Informática establecerá los parámetros y metodologías obligatorias.

Artículo 7.- Encárguese de la ejecución de este decreto los señores ministros coordinadores y el señor Secretario General de la Administración Pública y Comunicación.

Dado en el Palacio Nacional, en la ciudad de San Francisco de Quito, Distrito Metropolitano, el día de hoy 10 de abril del 2008.

f.) Rafael Correa Delgado, Presidente Constitucional de la República.

Es fiel copia del original.- Lo certifico.

f.) Pedro Solines Chacón, Subsecretario General de la Administración Pública.

Anexo 4. Archivos de configuración de Squid – ipsBloqueadas

```
192.168.43.66
192.168.43.73
192.168.43.74
192.168.43.91
192.168.43.92
192.168.43.93
192.168.43.94
192.168.43.108
192.168.43.109
192.168.43.110
192.168.43.124
192.168.43.125
192.168.43.126
192.168.43.141
192.168.43.142
192.168.43.157
192.168.43.158
192.168.43.173
192.168.43.174
192.168.43.188
192.168.43.189
192.168.43.190
192.168.43.205
192.168.43.206
192.168.43.220
192.168.43.221
192.168.43.222
192.168.43.236
192.168.43.237
192.168.43.238
192.168.43.241
192.168.43.245
192.168.43.246
192.168.43.248
192.168.43.249
192.168.43.250
192.168.43.251
192.168.43.252
192.168.43.253
192.168.43.254
```

Anexo 5. Archivos de configuración de Squid – sitiosNegados

```
abortion
aborto
acariciar
adult
almeja
amateur
amigos.com
anus
atrapavideox.com
ass
badoo
bestialismo
bestiality
bigamia
bigamist
bigamo
bigamy
bitch
blowjob
blog
cachondasyhumedas
cagada
cagar
caricia
celebri
chica
chingar
chulo
chupar
clit
clitoris
cock
consolador
culo
cum
cybervixen
chatdilandau
divascam.com
ddfcash.com
ejacula
encular
erotic
erotix
eyacula
enfemenino.com
facebook
fetish
follada
follar
fuck
game
```

gang-bang
gay
gifs.com
gigaim.com
gilipollas
girl
gorillaz.com
gravatar.com
guarra
guayaquilcaliente
cabaret
hiyo.com
himem
himen
hi5
hidemyass
homosexual
hustler
hotwords.es
hymen
incest
joder
jodida
juego
ktunnel
ladies
lesbian
lesbic
lesbos
loteria
lovesexy
mamada
mamar
marica
maricon
masturba
mediafire
megaproxy
megaupload
menage
merda
mierda
mija
mimp3
music
myspace
nalga
naughty
napster
netlog
nude
ocio.net
ojete

orgasm
orgia
orgy
pagewash
pecho
pederasta
pederastia
pedofil
pedophilia
peepshow
peido
peito
pelad
peludo
pene
penis
perra
photobucket.com
picha
pipi
follando
playbabe
playboy
polla
porn
proxymafia
prozymafia
pussy
puta
rapidshare
radio
ramera
sadomasochism
sadomasoquismo
sex
shit
slideshare.net
slut
sodomizar
sperm
stripsuck
tarot
tagged
tinypic.com
teen
testicle
testiculo
teta
tiaspilladas.com
tonos
thehotzone
thepiratebay
traseiro

trasero
twitter
tube
.tv
ultrasurf
.ultra*
unik.
unyk.
vagina
velludo
verga
video
video.es.msn.com
videonico
violador
virgen
virgin
warez
whatismyip
www.webcams.cc
webcamclub.com
websimpsons.com
webloader.org
woltermann
wibiya.com
xat.com
xpics
xxx
x-videos
yieldmanager
youtube
zoofilia
zoophilia
zorra
4shared.com
0km

Anexo 6. Archivos de configuración de Squid – inocentes

```
.pichincha.com
.yahoo.
.google.com
etinilestradiol
tribunalconstitucional.gov.ec
.live.com
.gov.ec
vademecum.es
missingheart
documen
button
wirelessexcite
msexchange
msexcel
aids.lv
freetown
geek-girls
scsext
steen
adulteducation
sekst
newshits
glass
georgia
peet
chicag
speech
speed
nomina.mef.gov.ec/Citrix/MetaFrameXP/default/logout.asp?
computa
http://186.42.101.7/Proyectos/ROWAPP.nsf
```

Anexo 7. Archivos de configuración de Squid – extensiones

```
\.mp3$
\.avi$
\.mp4$
\.mpg$
\.mpeg$
\.mov$
\.ra$
\.ram$
\.rm$
\.rpm$
\.vob$
\.wma$
\.wmv$
\.wav$
\.mbd$
\.ace$
\.bat$
\.lnk$
\.pif$
\.scr$
\.sys$
```

Anexo 8. Archivos de configuración de Squid – informatica

```
192.168.43.1
192.168.43.2
192.168.43.3
192.168.43.4
192.168.43.5
192.168.43.6
192.168.43.7
192.168.43.8
192.168.43.9
192.168.43.10
192.168.43.11
192.168.43.12
192.168.43.13
192.168.43.14
192.168.43.15
192.168.43.16
192.168.43.17
192.168.43.18
192.168.43.19
192.168.43.20
192.168.43.21
192.168.43.22
192.168.43.23
192.168.43.24
192.168.43.25
192.168.43.26
192.168.43.27
192.168.43.28
192.168.43.29
192.168.43.30
```

Anexo 9. Script para el firewall Iptables

```
#!/bin/sh
## SCRIPT de IPTABLES
## para proteger el servidor con DROP por defecto
## Diego Olivo Silva Lascano
## DIRECCION PROVINCIAL DE SALUD DE TUNGURAHUA

echo -n Aplicando Reglas de Firewall...

## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

## Establecemos politica por defecto: DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

## Empezamos a abrir puertos porque esta TODO denegado.

# Operar en localhost sin limitaciones
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# A nuestra IP le dejamos todo
iptables -A INPUT -s 192.168.43.10 -j ACCEPT
iptables -A OUTPUT -d 192.168.43.10 -j ACCEPT

# Abrimos los puertos para el servicio de internet
# ese puerto y los salientes vinculados se aceptan.
iptables -A INPUT -i eth1 -p tcp -m tcp --dport 8080 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -m tcp --sport 8080 -m state --state RELATED,ESTABLISHED -j
ACCEPT

iptables -A INPUT -i eth1 -p tcp -m tcp --dport 3128 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -m tcp --sport 3128 -m state --state RELATED,ESTABLISHED -j
ACCEPT

iptables -A INPUT -i eth1 -p tcp -m tcp --dport 8181 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -m tcp --sport 8181 -m state --state RELATED,ESTABLISHED -j
ACCEPT

# Permitimos que la maquina pueda salir a la web
iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

# Y tambien a webs seguras
iptables -A INPUT -p tcp -m tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT

# Permitimos la consulta a un primer DNS
iptables -A INPUT -s 200.107.10.62 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d 200.107.10.62 -p udp -m udp --dport 53 -j ACCEPT

# Permitimos la consulta a un segundo DNS
iptables -A INPUT -s 200.107.60.58 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d 200.107.60.58 -p udp -m udp --dport 53 -j ACCEPT

# Abrir el puerto 80 para las paginas con apache
iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 1024: -d 190.152.151.69 --dport 80 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s 190.152.151.69 --sport 80 -d any/0 --dport 1024: -j
ACCEPT

# Permitimos la administracion del servidor a traves del puerto 222 para ssh
iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 1024: -d 190.152.151.69 --dport 222 -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s 190.152.151.69 --sport 222 -d any/0 --dport 1024: -j
ACCEPT
```

```
iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.10 --dport 222
-j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.10 --sport 222 -d 192.168.43.0/24 --dport
1024: -j ACCEPT

#Abrimos el puerto para la administracion del servidor Zimbra
iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 7071 -d 190.152.151.69 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s 190.152.151.69 -d any/0 --dport 7071 -j ACCEPT

#Puerto de la aplicacion financiera esigef
iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 7778 -d 190.152.151.69 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s 190.152.151.69 -d any/0 --dport 7778 -j ACCEPT

#Puerto del ftp
iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 21 -d 190.152.151.69 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s 190.152.151.69 -d any/0 --dport 21 -j ACCEPT
iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 20 -d 190.152.151.69 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s 190.152.151.69 -d any/0 --dport 20 -j ACCEPT

#Damos acceso para el servidor samba a traves de los siguientes puertos:
iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.10 --dport 137 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.10 --sport 137 -d 192.168.43.0/24 -j ACCEPT

iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.10 --dport 138 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.10 --sport 138 -d 192.168.43.0/24 -j ACCEPT

iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.10 --dport 139 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.10 --sport 139 -d 192.168.43.0/24 -j ACCEPT

iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.10 --dport 445 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.10 --sport 445 -d 192.168.43.0/24 -j ACCEPT

#Abrir los puertos para actualizacion del antivirus corporativo nod32 en la local
iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.11 --dport
2221 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.11 --sport 2221 -d 192.168.43.0/24 --dport
1024: -j ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.11 --dport 2221 -j
ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.11 --sport 2221 -d 192.168.43.0/24 --dport 1024: -j
ACCEPT

iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.0/24 --dport 2222 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.0/24 --sport 2222 -d 192.168.43.0/24 -j ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.11 --dport 2222 -j
ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.11 --sport 2222 -d 192.168.43.0/24 --dport 1024: -j
ACCEPT

iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.0/24 --dport 2223 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.0/24 --sport 2223 -d 192.168.43.0/24 -j ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.11 --dport 2223 -j
ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.11 --sport 2223 -d 192.168.43.0/24 --dport 1024: -j
ACCEPT

iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.0/24 --dport 2224 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.0/24 --sport 2224 -d 192.168.43.0/24 -j ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.11 --dport 2224 -j
ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.11 --sport 2224 -d 192.168.43.0/24 --dport 1024: -j
ACCEPT

iptables -A INPUT -i eth1 -p tcp -s 192.168.43.0/24 -d 192.168.43.0/24 --dport 2846 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp -s 192.168.43.0/24 --sport 2846 -d 192.168.43.0/24 -j ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.11 --dport 2846 -j
ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.11 --sport 2846 -d 192.168.43.0/24 --dport 1024: -j
ACCEPT

#Desbloqueo de los puertos para snmp
iptables -A INPUT -i eth1 -p udp -s 192.168.43.0/24 -d 192.168.43.10 --dport 161 -j ACCEPT
iptables -A OUTPUT -o eth1 -p udp -s 192.168.43.10 --sport 161 -d 192.168.43.0/24 -j ACCEPT
```

```
iptables -A INPUT -i eth1 -p udp -s 192.168.43.0/24 -d 192.168.43.10 --dport 162 -j ACCEPT
iptables -A OUTPUT -o eth1 -p udp -s 192.168.43.10 --sport 162 -d 192.168.43.0/24 -j ACCEPT

#conexion del vnc
iptables -A FORWARD -p tcp -s 192.168.43.0/24 --sport 1024: -d 192.168.43.0/24 --dport 5900 -j
ACCEPT
iptables -A FORWARD -p tcp -s 192.168.43.0/24 --sport 5900 -d 192.168.43.0/24 --dport 1024: -j
ACCEPT

# Permitimos el reenvio de paquetes para contabilidad a traves del puerto 1494
# que se conecta a un servidor citrix
iptables -t nat -A POSTROUTING -o eth0 -p tcp -s 192.168.43.96/28 --sport 1024: -d !
192.168.43.0/24 --dport 1494 -j SNAT --to-source 190.152.151.69
iptables -A FORWARD -i eth1 -o eth0 -p tcp -s 192.168.43.96/28 --sport 1024: -d !
192.168.43.0/24 --dport 1494 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -p tcp -s ! 192.168.43.0/24 --sport 1494 -d
192.168.43.96/28 --dport 1024: -j ACCEPT

#Reenvio de paquetes para administracion de servidores a traves de ssh
iptables -t nat -A POSTROUTING -o eth0 -p tcp -s 192.168.43.0/24 --sport 1024: --dport 222 -j
SNAT --to-source 190.152.151.69
iptables -A FORWARD -i eth1 -o eth0 -p tcp -s 192.168.43.0/24 --sport 1024: -d !
192.168.43.0/24 --dport 222 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -p tcp -s ! 192.168.43.0/24 --sport 222 -d 192.168.43.0/24
--dport 1024: -j ACCEPT

# Barrera de backup por si cambiamos a modo ACCEPT temporalmente
# Con esto protegemos los puertos reservados y otros well-known
iptables -A INPUT -p tcp -m tcp --dport 1:1024 -j DROP
iptables -A INPUT -p udp -m udp --dport 1:1024 -j DROP
iptables -A INPUT -p tcp -m tcp --dport 1723 -j DROP
iptables -A INPUT -p tcp -m tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp -m tcp --dport 5432 -j DROP

# Con esto permitimos hacer forward de paquetes en el firewall, o sea
# que otras maquinas puedan salir a traves del firewall.
echo 1 > /proc/sys/net/ipv4/ip_forward

echo " OK . Verifique que lo que se aplica con: iptables -L -n"

# Fin del script
```