UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA DE CIENCIAS Y TECNOLOGÍA

PROGRAMA DE INGENIERIA INFORMATICA

PROYECTO DE GRADO

IMPLEMENTACIÓN DE UN SERVIDOR DE ADMINISTRACIÓN DE RED DE DATOS PARA EL PREDIO CENTRAL DE LA PREFECTURA DE PANDO

Postulante: Univ. Rolando Arce Balderrama.

Asesor: Ing. Jhonny Mamani Y.

Tutor: Lic. Milton Ramírez L.

Cobija - Pando - Bolivia

2010

AGRADECIMIENTO

Al finalizar un trabajo tan arduo y lleno de dificultades como el desarrollo del proyecto de grado, es inevitable ocultar lo agradecido que estoy por las personas, que me rodean y me apoyaron en los momentos del desarrollo del proyecto y a la instituciones que han facilitado las cosas para que este trabajo llegue a un feliz término. Por ello, es para mí un verdadero placer utilizar este espacio para ser justo y consecuente con ellas, expresándoles mis agradecimientos.

En primer lugar agradecer al señor Jesucristo que incondicionalmente me ha apoyado, desde el inicio hasta la culminación de este proyecto me seguirá apoyando hasta los últimos días de mi vida.

También agradecer a mis padres que desde el inicio de mi formación académica en la carrera me han apoyado, de forma cotidiana y aguantando mi mal humor en mis días malos de estudios, como también el los buenos momentos que con sus consejos me levanta las ganas de estudiar.

También es grato agradecer a mi tutor el Lic. Juan carlós H. que corrigió mis errores de mi proyecto, teniendo esa paciencia que le caracteriza.

También agradezco a mi asesor que me oriento y ayudo para el desarrollo del proyecto como para la paciencia que a ojos cerrados aceptaba mis opiniones.

Como dejar de agradecer a todos los compañeros y docentes que conforma el plantel del área de ciencias y tecnología, que en conversas de pacillo siempre, fortalecían mis ganas de seguir estudiando y también esos consejos que de docentes en particular nos dan cada vez que me miraban.

Por último agradezco a mi querida novia eloyza, que en momentos yo no tenía tiempo para ella y sacarle a pasear y ella comprendía que tenía que a ser mi proyecto de grado.

Dedicatoria:

A mis padres Alfredo y Matilde.

Atte. Rolando su Hijo.

RESUMEN

Uno de los métodos para la administración de redes, es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada, la característica fundamental de un sistema de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red, esto quiere decir: soporte para los protocolos de red más importantes, una vez seleccionando la herramienta adecuada para implementación, se trabajó bajo la metodología basada en modelos funcionales estándar de la ITU y de la ISO, teniendo las ventajas y desventajas, se obtiene una análisis de uso del internet, de acuerdo a dicho al estudio obtenido, uno de los primeros pasos a realizar, fue los diseños del edifico como de la parte lógica de la red de datos, luego se procede a la instalación del software bajo las características y requerimientos propuestos, una vez activo el servidor, asigno IP de acuerdo a sus sitios de trabajo, conjuntamente con las políticas de uso planteadas por la dirección de sistemas, teniendo en cuenta que las políticas están configuradas bajo el filtro del servidor, la administración de aquí en adelante la realiza el encargado del área, brindando reportes de acuerdo a cada usuario con todo los contenidos visitados y del tráfico de ancho consumido.

INDICE

Capítulo I

Introducción

CAPITULO I INTRODUCCIÓN

Con el avance tecnológico de la comunicación, también creció la inseguridad en navegación a sitios web, en la actualidad el internet es muy utilizado por los cibernautas, sin un control de acceso a sitios web peligrosos e restringidos. En las redes de datos son importantes los mecanismos de prevención, por ello es necesario hacer uso de una serie de herramientas de tipo software y/o hardware, así como políticas de seguridad a fin de asegurar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta que hoy en día los datos viajan a través del internet de manera insegura, debido a los ataques de los hackers, spyware y virus, que hacen que la información se a vulnerable, cambios, modificaciones o uso indebido.

Los problemas que se percibió en el predio central de la prefectura de Pando, sobre las visitas a páginas web prohibidas y descargas de archivos no debidos, ponen en saturación el ancho de banda de la red de datos, molestia a usuarios que trabajan con este recurso, viendo estos problemas se ha optado por implementar un servidor de administración y seguridad de red de datos, basado en sistema operativo Linux el cual es software libre con licencia GPL. Se realizaran las políticas de uso según al entorno de la institución. El presente trabajo ayudara a regularizar el tráfico de ancho de banda y restringirá el acceso a sitios web prohibidos, tomando en cuenta el control a cada equipo de manera individual, con el fin de tener una red de datos más óptima y con una mejor administración de todo los recursos que interactúan entre usuarios.

1.1.ANTECEDENTES Y MOTIVACIÓN

En la década de los 90's empezó un continuo crecimiento de la industria de redes datos, así como el surgimiento de más tecnologías de conectividad, independientes de protocolos y de equipos, en un principio de las redes de computadoras se formaban por simples conexiones que permitían a un usuario, acezar recursos compartidos en otro computadoras.

En los últimos años las instituciones tanto gubernamentales como privadas, han optado en tener redes estructuradas para satisfacer las necesidades básicas como el compartimiento de

recursos y conexiones a internet, usando herramientas de comunicación que consume mayor ancho de banda, como video conferencias o videos informativos ya que es necesario tener mayor velocidad de conexión, esta tendencia de uso compartido de archivos ha evolucionado en dos frentes: el uso de aplicaciones P2P de distribución de archivos con fines recreativos para la descarga (con frecuencia ilegal) de películas, música, videojuegos y aplicaciones digitales y el uso de herramientas P2P para la descarga de contenidos académicos legítimos y proyectos de colaboración en investigación.

La Prefectura del Departamento de Pando, tiene como misión promover el desarrollo departamental, planificar el desarrollo administrativo de los recursos públicos departamentales, reglamentar las atribuciones delegadas, proporcionar servicios y coordinar con instituciones del departamento, así como a nivel departamental como municipal, con la finalidad de contribuir al mejoramiento de la calidad de vida de la región.

Según los indicios del tiempo y la necesidad institucional, una de las primeras redes de datos que se implementó en la prefectura de Pando, fue aproximadamente una década atrás, su utilidad únicamente era para el intercambio de información, de forma espontánea en la parte financiera, utilizando la herramienta SIFF (Sistema Información Financiera). Teniendo en cuenta que la red solo estaba compartida, en el área de económica y no así en todo el predio central, hoy en día la red esta ampliada en todas sus direcciones ya que es una necesidad latente, que es de gran ayuda para el intercambio de información y compartir recursos.

Con la llegada del servicio de internet a pando por el año 2000, la prefectura fue una de las primeras instituciones en adquirir esta TIC, no todos fueron los beneficiado ya que el servicio solo era DIAL-UP, que solo tenía un a velocidad 56kbps y se adquiero solo para los directores de cada secretaria de manera individual, pero con la gran necesidad del servicio internet el 2006, se realiza la instalación de la conexión ADLS vía modem de 512kbps. La cual se realiza una pequeña red de datos, para la distribución del internet, al personal que trabaje con esta TIC.

1.2.DESCRIPCIÓN DEL PROBLEMA

En la actualidad el predio central de la prefectura de Pando, se encuentra descuidado en la administración de la red de datos. Las causas que se percutan en la institución son, el mal manejo del internet por los usuarios, descarga desde un gestor p2p, como videos, músicas, otros. Esto nos conlleva a la formulación del siguiente problema:

"Deficiencia en la administración de la red de datos de la prefectura".

Los efectos del problema nos llevan a distracción en el trabajo, saturación del ancho de banda, molestias de los usuarios por la lentitud del internet y conflicto de IP.

1.3. SOLUCIÓN PROPUESTA

Es de implementar el servidor de administración de red de datos, para tener mejor funcionamiento de la red, en la que todos los usuarios estarán gestionados por el administrador, de acuerdo a su registro y prioridad asignada, así evitando disconformidad en la velocidad y seguridad de la red, también se contara con un monitoreo continuo de todos los sitios visitados por los usuarios registrados.

1.4. OBJETIVOS Y ALCANCES DEL PROYECTO

1.4.1. Objetivo general

Implementar un servidor de administración de red de datos para el predio central de la prefectura de Pando bajo la metodología funcional para la administración de redes.

1.4.2. Objetivos específicos

- Realizar un diagnóstico de todo el funcionamiento de la red de datos actual.

- Elaborar el rediseño de la estructura de la red de datos actual.
- Configurar e implementar el servidor para administración de red datos, bajo la distribución del Sistema Operativo Linux (BarzilFW).
- Realizar pruebas de funcionamiento adecuado del servidor.

1.4.3. Alcances

Con la implementación del servidor de administración de red de datos, se resolver los problemas propuestos, tanto en la administración de la red como en la seguridad que mediante Firewall (IDS), ya que se trabajara constantemente con la institución, teniendo en cuenta que se realizara lo previsto.

- Balanceo de carga.
- Administración del ancho de banda.
- Filtrado de servicios externos
- Administración de control de accesos bajo filtrado.
- Administración de usuarios bajo control IP x MAC.
- Administración de los registros de usuarios de bajada y subida.
- Implementación servidor nativo DNS del BFW 3.0 = Bind.

1.5. METODOLOGÍA Y HERRAMIENTA UTILIZADA

1.5.1. Metodología

Se utilizara es la metodología funcional para la administración de redes, en la que se describe una metodología basada en modelos funcionales estándar de la ITU y de la ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes, se refiere a la asignación de tareas de administración por medio de áreas funcionales.

1.5.2. Herramientas utilizada

La herramienta a utilizarse es BrazilFW Firewall & Router es una distribución del sistema operativo Linux que implementa un cortafuegos (o firewall) y puede realizar tareas avanzadas de ruteo y QoS, proporciona una interfaz web para administración, cuenta con agregados o funcionalidades extra llamados addons de fácil instalación. BrazilFW tiene como objetivo ser un potente enrutador cortafuegos con altas funcionalidades extra, sin dejar de lado la simplicidad tanto en administración como en requerimientos de hardware.

Capítulo II

Marco teórico

CAPITULO II MARCO TEORICO

2.1. DESCRIPCIÓN DEL CONTEXTO DE LA RED DE DATOS DE LA PREFECTURA DE PANDO

La prefectura de Pando se encuentra ubicado en la ciudad de Cobija, capital del Departamento Pando, con la llegada del servicio de internet a Pando por el año 2000, la prefectura fue una de las primeras instituciones en adquirir esta tecnología, no todos fueron los beneficiado ya que el servicio solo era DIAL-UP, que solo tenía un a velocidad 56kbps y se adquiero solo para los directores de cada secretaria de manera individual, pero con la gran necesidad del servicio internet el 2006, se realiza la instalación de la conexión ADLS vía modem de 512kbps. La cual se estructuro una pequeña red de datos, para la distribución del internet, al personal que trabaja con sistemas en línea.

Actualmente la prefectura cuenta con diferentes unidades y secretarias en toda la capital de cobija, en cada unida cuenta con una estructura de red de datos ya que el servicio de internet es muy necesario, el proyecto estará dirigido al predio central de la prefectura ya que es el edificio con más cantidad de equipos conectados a una red, la unida en cargada de mantener los dispositivos de computación y las estructuras de red es la unidad de sistemas.

2.1.1. Unidad de Sistemas

La unidad de sistemas de la prefectura de Pando tiene como objetivo de brindar apoyo técnico en las ramas de sistemas, redes y hardware, a todas las unidades dependientes de la institución, en la división de redes tiene como objetivo promover el uso de los sistemas de comunicación dentro de la prefectura de Pando, además de implementar políticas de uso de todos los sistemas de comunicación al interior de la institución, que permitan un buen uso de todos estos servicios, coordinando y planificando todas las tareas de cada una de las unidades de la estructura.

2.1.2. La red de datos del predio central de la Prefectura de Pando

La red de datos del predio central de la prefectura de Pando, se encuentra constituidos por, por una serie de interconexiones entre unidades de manera libremente, en la que se cuenta con el servicio de internet que brinda la cooperativa de coteco con una velocidad de 1Mbps.

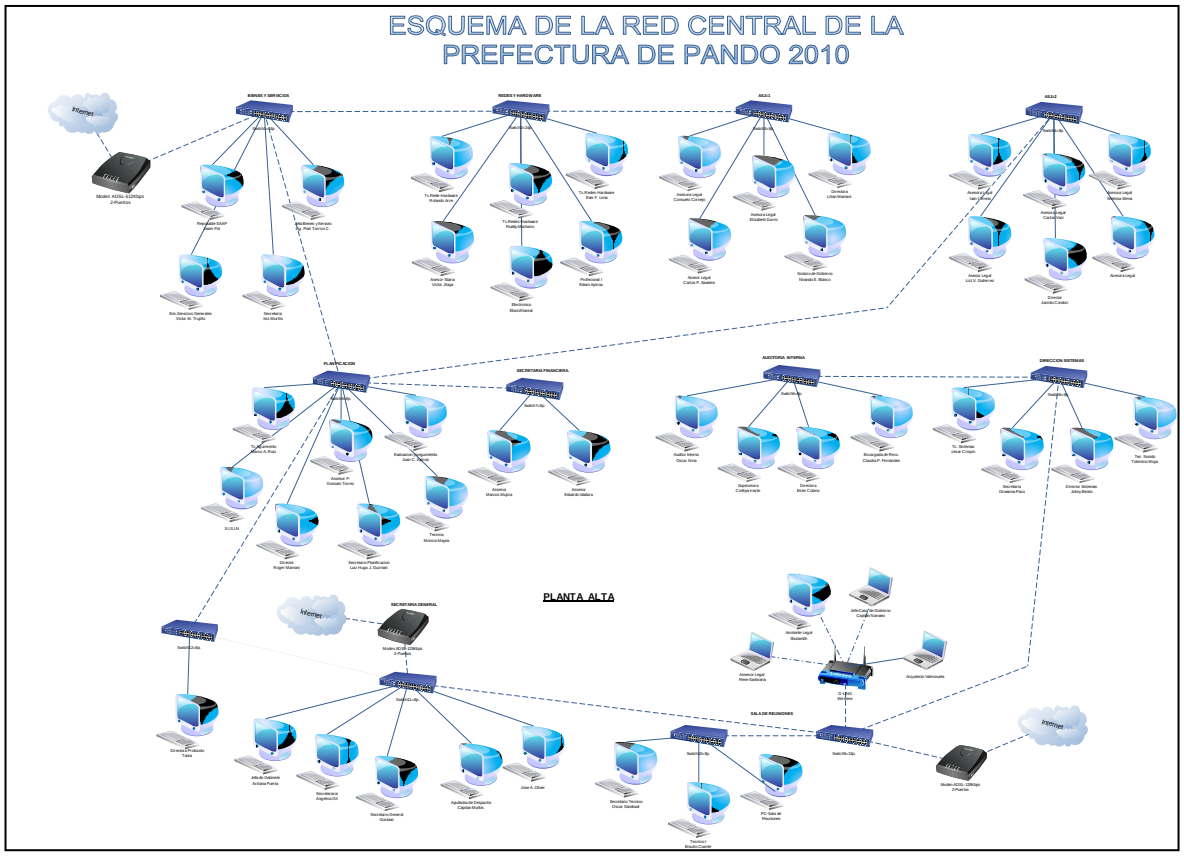


Figura 2.1: *Esquema de la red de datos*

Fuente: *Propia*

2.2. LA ADMINISTRACIÓN DE REDES DE DATOS

Según (Dumrauf, 2002) Con el crecimiento de los ciberespacios también crecieron las redes locales, es así que la administración de redes se ha convertido en un aspecto crítico, especialmente en redes de computadores de varios vendedores heterogéneos. El modelo

Cliente – Servidor con una gran cantidad de estaciones de trabajo necesita de la administración de redes para manejar y controlar las redes y los componentes asociados al hardware y al software.

2.2.1. Cambios en la Administración de Redes

Las computadoras hoy en día se conectan de forma distintas y no como lo hacían al principio, en que un gran computadora central estaba conectada con todas las estaciones de trabajo homogéneas, con la llegada de las LAN (Local Área Network) existen dos escenarios de redes de computadoras.

- **Modelo Cliente – Servidor:** Un cliente requiere un servicio de un servidor que está preparado para proporcionar dichos servicios a los clientes que lo necesitan.
- **Modelo peer – to – peer:** No existen roles fijos como cliente y servidor, cualquier computadora puede, en un determinado momento, ser un cliente o un servidor.

La evolución de una red de computadoras host céntricas a redes de tipo LAN heterogéneas fue gradual. La transformación al ambiente LAN es más complicado por la existencia de aplicaciones y protocolos de diferentes grupos de estándares y fabricantes. Sin embargo, las limitaciones de la tecnología, protocolos y topologías imponen restricciones acerca del número de computadores que se pueden conectar a la LAN. Por todos estos aspectos, la conexión y administración de redes, así como también de sus componentes, se está volviendo más y más importante.

2.3. LOS PROTOCOLO TCP/IP

Protocolos TCP/IP son importantes en las redes de datos, de ese modo se realizara un estudio profundo de los protocolos básicos que permiten el funcionamiento de Internet. La familia de protocolos TCP/IP es la piedra angular sobre la que se sustentan el resto de

servicios (WWW, FTP, SSH...) que actualmente podemos encontrar en Internet, y por tanto su estudio es parte fundamental para el resto del trabajo. Se introducirá el sistema de direccionamiento, el formato utilizado en sus cabeceras y el modo de funcionamiento de los protocolos más importantes de esta familia:

- El protocolo de control de flujo (**ICMP**).
- El protocolo no fiable de transmisión de datos sin conexión (**UDP**).
- El protocolo fiable de transmisión de datos con conexión (**TCP**).

Finalmente se explicará el proceso de ruteado (*routing*) de los datagramas IP así como su tránsito por la red local hasta el ordenador destinatario, este estudio se centrará únicamente en la versión 4 del protocolo IP, ya que aunque actualmente se está trabajando en la versión 6 esta es aún experimental. (Verdejo, 2003).

2.3.1. Redes IP

Las redes IP y internet se ha convertido en el factor más potente que guía el proceso de convergencia es debido principalmente al hecho de que la suite del protocolo Internet se ha erigido como un estándar utilizado en casi cualquier servicio, la suite del protocolo Internet está compuesto principalmente por el protocolo Internet (IP), y el protocolo de control del transporte (TCP); consecuentemente el término TCP/IP refiere a la familia del protocolo al completo.

Las redes basadas en IP tienen una gran importancia en la sociedad de la información actual. A primera vista esta tecnología puede parecer un poco confusa y abrumadora pero empezaremos por presentar los componentes de red subyacentes sobre los que está construida esta tecnología. (Paper, 2002).

2.3.2. El Modelo OSI

Según (Marín, 2009) El modelo OSI es una organización internacional para la normalización ISO creado en 1984, el modelo de referencia OSI (Open Systems Interconnected), en la que estudia la forma en que viajan los datos atreves de las capas subdivididas, este modelo surge de la necesidad imperante de interconectar sistemas de procedencia diversa de distintos fabricantes, cada uno de los cuales empleaban sus propios protocolos para el intercambio de señales. El término "abierto" se seleccionó con la idea de realizar la facilidad básica del modelo que dio origen al mismo, frente a otros modelos "propietarios" y por tanto cerrados en la que se dividieron en capas.

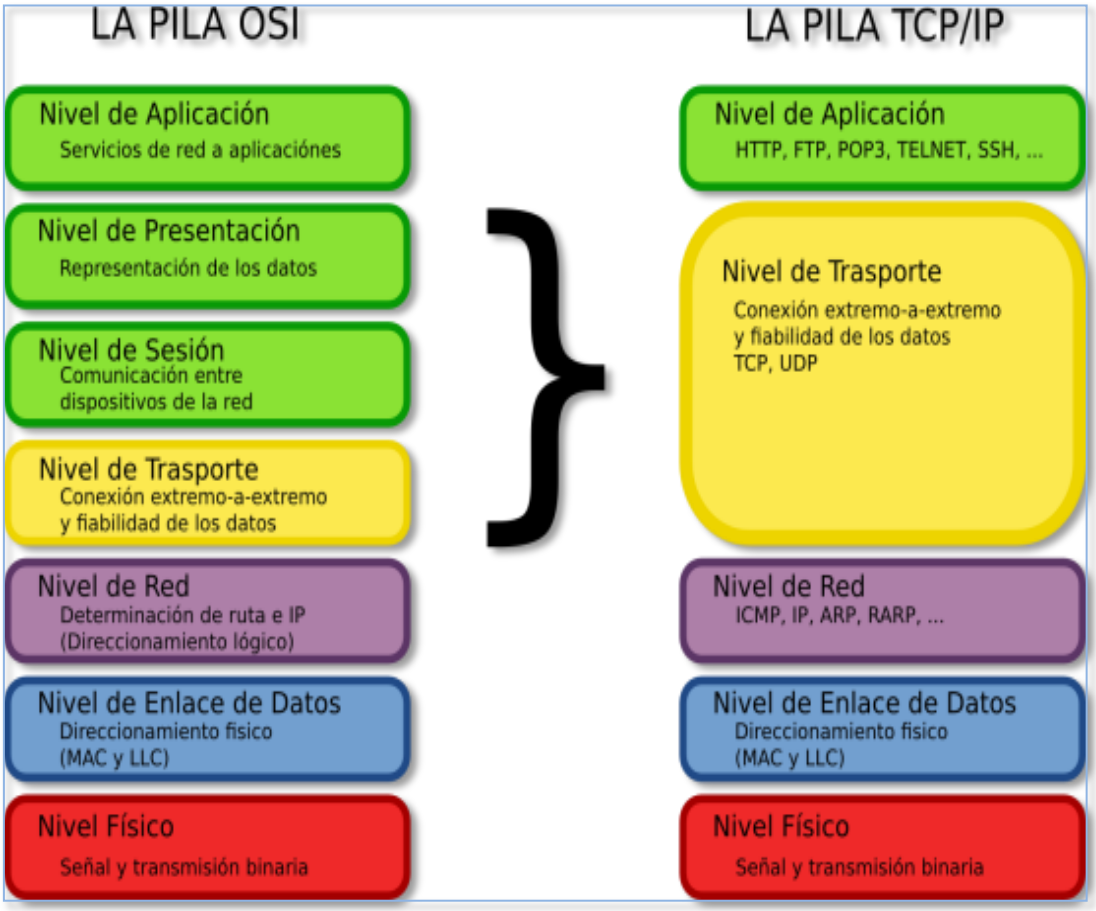


Figura 2.2 Pila OSI Vs Pila TCP/IP

Fuente: Propia

a) **Capa 7 Aplicación:** Proporciona servicios de red a procesos de aplicación como correo electrónico, transferencia de archivos y emulación de terminales.

b) **Capa 6 Presentación:** Garantiza que los datos sean legibles para el sistema receptor, formato de los datos, estructura de los datos, negocia la sintaxis de transferencia de datos para la capa de aplicación.

c) **Capa 5 Sesión:** Establece, administra y termina sesiones entre aplicaciones.

d) **Capa 4 Trasporte:** Se ocupa de aspectos de trasportes entre host, confiabilidad del transporte de datos, establecer mantener y terminar circuitos virtuales, detección y recuperación de fallas y control del flujo de información.

e) **Capa 3 Red:** proporciona conectividad y selección de ruta entre dos sistemas finales y dominio de enrutamiento.

f) **Capa 2 Enlace de Datos:** Permite la transferencia confiable de los datos atreves de los medios, direccionamiento físico, topología de red, notificación de errores y control de flujo.

g) **Capa 1 Física:** Cables, conectores, voltaje y velocidad de datos.

2.3.3. El protocolo IP versión 4

El protocolo IP (*Internet Protocol*) es la pieza fundamental en la que se sustenta el sistema TCP/IP y por tanto todo el funcionamiento de Internet, la unidad de datos del protocolo IP es el *datagrama*, cuyo tamaño máximo es de 65535 bytes (64K). El protocolo IP facilita un sistema **sin conexión** (*connectionless*) y **no fiable** (*unreliable*) de entrega de datagramas entre dos ordenadores cualesquiera conectados a Internet.

IP da un servicio de entrega basado en el mejor intento (*best effort*), esto implica que cuando hay algún funcionamiento anómalo de Internet, como podría ser un *router* colapsado, se contempla un sistema muy simple de tratamiento de errores. Este mecanismo de control de errores viene regulado por el protocolo ICMP (*Internet Control Message Protocol*).

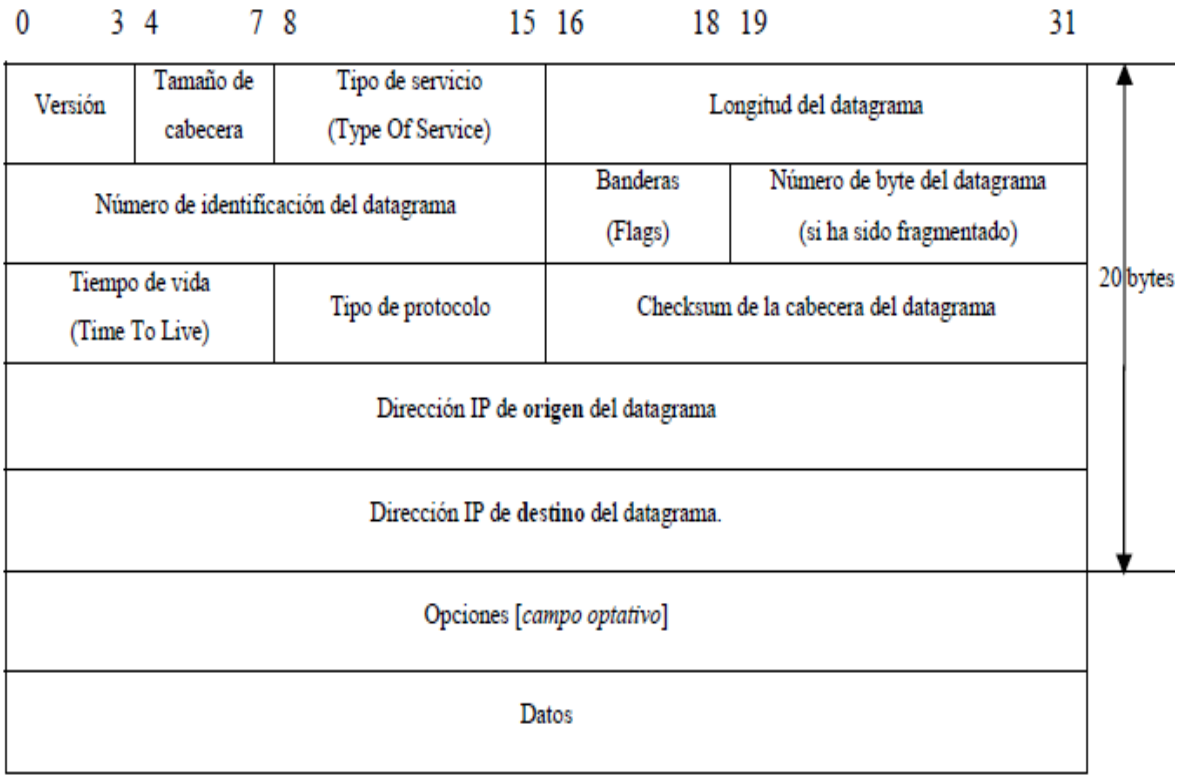


Figura 2.3: *estructura de un data grama*

Fuente: *verdejo, 2003*

La versión (4 bits), sirve para identificar a que versión específica (RFC) hace referencia el formato del datagrama. Esta información sólo es utilizada por los routers y capa IP de origen y final del datagrama. Esto permite la coexistencia de diferentes versiones del protocolo IP de una forma transparente al usuario. La versión actual es la 4 (conocida también cómo IPv4). (Verdejo, 2003).

2.3.4. TCP/IP y Linux

TCP/IP, Unix e internet están profundamente relacionados, con énfasis adicional en Linux, esto podría parecer más como una con dependencia, de hecho los protocolos TCP/IP se han implementado en muchas plataformas y funcionan como una especie de pegamento, uniéndolos en la red. Esto no quiere decir que algunos distribuidores no abusen del protocolo, implementado extensiones patentadas y ocasionalmente no interoperables de los estándares, a largo plazo este tipo de comportamiento puede ser bastante perjudicial. (pat, 2001)

2.4. SERVIDORES EN LINUX

Los servidores bajo el sistema operativo Linux es del presente y del futuro, su permanencia está garantizada por cientos de programadores de todo el mundo que, en un esfuerzo sin precedentes se han dedicado a construir una plataforma de trabajo estable, libre y completa. Ese futuro está garantizado por su licencia GNU que asegura que el programa binario venga acompañado de sus fuentes; de esta forma, los programas nunca quedarían en el olvido y siempre habría alguien en el mundo que los pueda corregir, ampliar o darles mantenimiento.

2.4.1. Tipos de servidores

Según (Master, 2007) con el pasar del tipo fueron apareciendo diferentes tipos de de servidor, cada uno cumpliendo tareas diferentes, ya sea en red local o una re WAN, a continuación se nombrara algunos de los servidores existentes:

a) **Plataformas de Servidor (*Server Platforms*):** Un término usado a menudo como sinónimo de sistema operativo, la plataforma es el hardware o software subyacentes para un sistema, es decir, el motor que dirige el servidor.

b) **Servidores de Aplicaciones (*Application Servers*):** Designados a veces como un tipo de *middleware* (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.

c) **Servidores de Audio/Video (*Audio/Video Servers*):** Los servidores de Audio/Video añaden capacidades multimedia a los sitios web permitiéndoles mostrar contenido multimedia en forma de flujo continuo (*streaming*) desde el servidor.

d) **Servidores de Chat (*Chat Servers*):** Los servidores de chat permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo discusiones en tiempo real.

e) **Servidores de Fax (*Fax Servers*):** Un servidor de fax es una solución ideal para organizaciones que tratan de reducir el uso del teléfono pero necesitan enviar documentos por fax.

f) **Servidores FTP (*FTP Servers*):** Uno de los servicios más antiguos de Internet, File Transfer Protocol permite mover uno o más archivos.

g) **Servidores Groupware (*Groupware Servers*):** Un servidor groupware es un software diseñado para permitir colaborar a los usuarios, sin importar la localización, vía Internet o vía Intranet corporativo y trabajar juntos en una atmósfera virtual.

h) **Servidores IRC (*IRC Servers*):** Otra opción para usuarios que buscan la discusión en tiempo real, Internet Relay Chat consiste en varias redes de servidores separadas que permiten que los usuarios conecten el uno al otro vía una red IRC.

i) **Servidores de Listas (*List Servers*):** Los servidores de listas ofrecen una manera mejor de manejar listas de correo electrónico, bien sean discusiones interactivas abiertas al público o listas unidireccionales de anuncios, boletines de noticias o publicidad.

j) **Servidores de Correo (*Mail Servers*):** Casi tan ubicuos y cruciales como los servidores web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.

k) **Servidores de Noticias (*News Servers*):** Los servidores de noticias actúan como fuente de distribución y entrega para los millares de grupos de noticias públicos actualmente accesibles a través de la red de noticias USENET.

l) **Servidores Proxy (*Proxy Servers*):** Los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

m) **Servidores Telnet (*Telnet Servers*):** Un servidor telnet permite a los usuarios entrar en un ordenador huésped y realizar tareas como si estuviera trabajando directamente en ese ordenador.

n) **Servidores Web (*Web Servers*):** Básicamente, un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red.

2.5. METODOLOGÍA DEL MODELO FUNCIONAL PARA LA ADMINISTRACIÓN DE REDES

Según (Untiveros, 2004) se describe una metodología de redes de datos basada en modelos funcionales estándar de la ITU y de la ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

2.5.1. Administración de redes.

El término *administración de redes* es definido como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

Tres dimensiones de la administración de redes.

a) **Dimensión Funcional.** Se refiere a la asignación de tareas de administración por medio de áreas funcionales.

b) **Dimensión Temporal.** Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.

c) **Dimensión del escenario.** Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

a) Dimensión Funcional

Existen diversas modelos sobre arquitecturas de administración de redes. Tanto el modelo TMN de la ITU como el modelo OSI-NM (Network Management) son modelos funcionales

que dividen la administración de una red en áreas funcionales (configuración, fallas, desempeño, contabilidad y seguridad), definiendo de ésta forma una estructura organizacional con funciones bien definidas. De esto se deriva el nombre de modelos funcionales. El presente trabajo se basa únicamente a lo que proponen los modelos funcionales mencionados.

2.5.2. Desarrollo De La Metodología

Se sugiere la creación de las siguientes áreas funcionales para ser aplicadas en la administración de redes.

2.5.2.1. Administración de la configuración

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

a) Planeación y diseño de la red.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación. El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

- Reunir las necesidades de la red**.** Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológico de una red pueden ser:

    - Multicast,

- Voz sobre IP (VoIP),
- Calidad de servicio (QoS), etc.

Algunas necesidades cuantitativas pueden ser:

- Cantidad de nodos en un edificio
- Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la implementación de nuevas tecnologías de red como el cambiar de ATM a GigabitEthernet, o cambiar los protocolos de ruteo interno.

- Diseñar la topología de la red

- Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.

- Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.

- Si el diseño y equipo propuesto satisfacen la necesidades, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

b) Selección de la infraestructura de red.

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la

mayoría de las necesidades técnicas de la red. Lo más recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

c) Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

- **Instalaciones de hardware,** Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

    - Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
    - Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
    - Notificar anticipadamente a los usuarios sobre algún cambio en la red.
    - Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
    - Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.
    - Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.
    - Documentar el cambio para futuras referencias.

- **Administración del software, e**s la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son

creados para obtener información específica en los dispositivos. Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.
- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requiere especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de ftp.

d) Provisionamiento

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

- Algunos elementos de hardware más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

e) Políticas y procedimientos relacionados

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

2.5.2.2. Administración del rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado. La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

a) Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) *Utilización de enlaces,* Se refiere a las cantidades ancho de banda utilizado por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.

b) *Caracterización de tráfico, e*s la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) *Porcentaje de transmisión y recepción de información,* encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) *Utilización de procesamiento,* es importante conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

b) Análisis.

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño. En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

- *Utilización elevada,* si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

- *Tráfico inusual,* el haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

- *Elementos principales de la red,* un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con mas actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

- *Calidad de servicio,* otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

- *Control de tráfico,* el tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

2.5.3. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

2.5.3.1.Monitoreo de alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red. También conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red.

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla.
Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

a) Tipo de las alarmas

- *Alarmas en las comunicaciones.* Son las asociadas con el transporte de la información, como las pérdidas de señal.

- *Alarmas de procesos.* Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.

- *Alarmas de equipos.* Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.

- *Alarmas ambientales.* Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.

- *Alarmas en el servicio.* Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

b) Severidad de las alarmas.

- *Crítica.* Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.

- *Mayor.* Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.

- *Menor.* Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.

- *Indefinida.* Cuando el nivel de severidad no ha sido determinado por alguna razón.

2.5.3.2.Localización de fallas.

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

a) Pruebas de diagnóstico

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

- *Pruebas de conectividad física, s*on pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

- *Pruebas de conectividad lógica,* son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son "ping" y "traceroute".

- *Pruebas de medición, e*sta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

2.5.3.3.Corrección de fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.

- *Reemplazo de recursos dañados. Hay equipos de red* que permiten cambiar módulos en lugar de cambiarlo totalmente.

- *Aislamiento del problema.* Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.

- *Redundancia.* Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.

- *Recarga del sistema.* Muchos sistemas se estabilizan si son reiniciados.

- *Instalación de software.* Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.

- *Cambios en la configuración.* También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

2.5.3.4.Administración de reportes

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T.

a) Creación de reportes

Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte debe contener al menos la siguiente información:

- El nombre de la persona que reportó el problema
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema
- Comentarios acerca de la problemática.
- Fecha y hora del reporte

b) Seguimiento a reportes

La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc, y esta debe poder ser consultada en cualquier momento por el administrador.

c) Manejo de reportes

El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

d) Finalización de reportes

Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

2.5.4. Administración de la seguridad

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

2.5.4.1.Prevención de ataques

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

2.5.4.2. Detección de intrusos

El objetivo es detectar el momento en que un ataque se esta llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

2.5.4.3. Respuesta a incidentes

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

2.5.4.4. Políticas de Seguridad

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información

ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad. Entre otras, algunas políticas necesarias son:

- Políticas de uso aceptable
- Políticas de cuentas de usuario
- Políticas de configuración de ruteadores
- Políticas de listas de acceso
- Políticas de acceso remoto.
- Políticas de contraseñas.
- Políticas de respaldos.

2.5.4.5. Servicios de seguridad

Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de *mecanismos de seguridad.* Identifica el "*que".*

De acuerdo a la Arquitectura de Seguridad OSI, un *servicio de seguridad* es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad :

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de las políticas de seguridad.

2.5.4.6.Mecanismos de seguridad

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso, cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure shell o IPSec; Mecanismos de integridad como MD5, entre otras.

Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

2.5.4.7.Proceso.

Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones:

- Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.
- Definir, de acuerdo a las políticas de seguridad, los servicios de necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.
- Implementar la política de seguridad mediante los mecanismos adecuados.

2.5.5. Conclusiones

La administración de redes es la suma de todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, la seguridad, entre otras. Esto nos lleva a reconocer que

una red debe contar con un sistema de administración aun cuando se crea que es pequeña, aunque es cierto que entre mayor sea su tamaño mas énfasis se debe poner en esta tarea.

En los puntos anteriores se describió una propuesta de administración para redes de datos. La propuesta se basó en la recomendación de la ITU-T, el modelo TMN y en el modelo OSI-NM de ISO. Se presentó una propuesta global que enfatiza en todos los aspectos relacionados a la buena operación de una red, como lo son el control sobre los sucesos en la red, la visualización de los tipos de tráfico, la detección y atención oportuna de problemas, aspectos de seguridad, etc.

La metodología presentada se basa en un modelo con tareas bien definidas y complementarias. Esta modularidad permite su mejor entendimiento y facilita su implementación y actualización.

Capítulo III

Desarrollo Del Proyecto

CAPITULO III DESARROLLO DEL PROYECTO

Para llevar a cabo la implementación del servidor de administración de redes de datos, y la realización del esquema estructural de todo el cableado de la red de la prefectura de Pando, se está haciendo seguimiento a la metodología funcional para la administración de redes, el cual se describió de manera detallada en el capítulo anterior, para el análisis implementaciones utilizo las herramientas como encuestas, observación y Edraw Max para el diseño lógico de la red.

3.1. FASE DE ANÁLISIS Y DIAGNOSTICO

En esta fase se realizara el análisis anterior y diagnóstico, ya que por el aumento de equipos y peticiones de conexiones a internet, también creció la dificulta para esquematizar la red LAN, en la que se optó, realizar el diseño del esquema de la red, utilizando la metodología funcional para la administración de redes, también las encuestas, para así hacer el estudio del uso de internet, con los datos adquiridos describir el funcionamiento debido de la red y la descripción de cada usuario que este en la red LAN.

3.1.1. Diagnóstico del uso de internet

Se realizó el levantamiento de datos vía encuesta para diagnosticar el uso actual del internet, fueron encuestados los funcionarios que tienen accesos a la red de datos, para así poner tener un diagnostico actual de las problemáticas e inquietudes de cada usuario que gozan de este servicio.

Es así que obteniendo los resultados de dicha encuesta, se realizó el dicho estudio del análisis elaborado, dividiéndolos así en dos partes, en el análisis resultante actual y análisis provisional, en la que a continuación se explicara de forma narrativa.

a) **Análisis resultante actual:** Es logrado en la encuesta obtenida a los usuarios, que usan el internet de la prefectura de Pando, ya que fueron datos cuantitativos se deduce de esta manera:

   En el parámetro de tiempo se observó que los usuarios usan el internet, en un promedio mayor a una hora diaria, aun teniendo en cuenta que el internet no es constante, en la que la mayoría de los usuarios usan paginas informativas de acorde a su labor de trabajo, pero se obtuvo un porcentaje considerado de las personas que usan y conocen los programas de descargar P2P en la que es desventajoso para el tráfico de ancho de banda.

   Obteniendo la información de dicha encuesta, se puede predecir que es necesaria la implementación del servidor para la administración de la red de datos, de acuerdo esta conclusión obtenida:

   Tomando en cuenta que el uso del internet es necesario en el ámbito laboral de la institución y que internet no es constante debido al mal uso y malas conexiones físicas de la red de datos, es necesario dicha implementación del servidor, ya que los usuarios hacen las visitas a páginas informativas y de sistemas en líneas, es por eso que se debe evitar las descargaras de diferentes tipos como por ejemplo de los P2P.

El estudio realizado también se puede observar de acuerdo a cada pregunta así se tendrá un vistazo aproximado de los resultados generales ya que se encuesto al 52% de toda la población, es así que se tiene los resultados según a las preguntas propuestas, en la encuesta que se realizó **(VER ANEXO A).**

Así como se tiene los resultados obtenidos de cada pregunta, podemos mostrar un gráfico representativo de la pregunta 1 de la encuesta realizada:

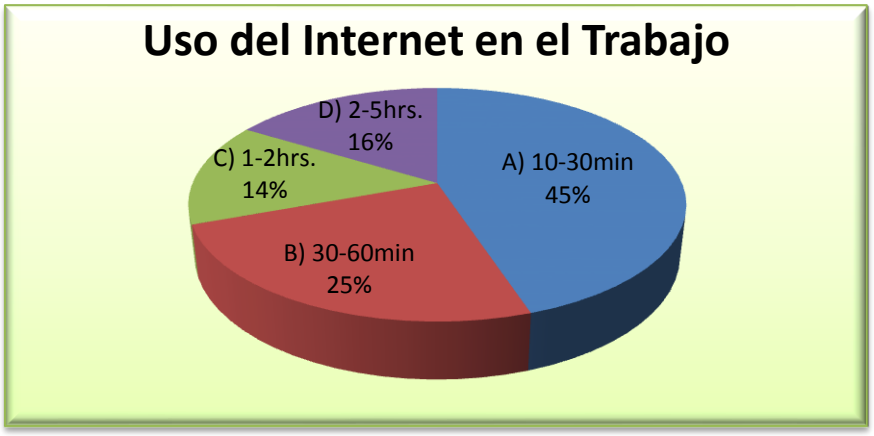


Figura 3.1: *Torta de uso del internet en el trabajo*
Fuente: *Elaboración Propia.*

3.1.2. Diagnóstico de la red estructural vía observaciones

Se realizó el diagnóstico de la red estructural mediante la observación, en la que se pudo observar el estado físico de la red, como también de los dispositivos que se interconectan entre sí de igual forma el cableado estructurado que su mayor parte no estaba bajo las normas adecuadas, y no se encuentra en buenas condiciones, ya que para la implementación del servidor no se debe tener roturas de conexión ni fugas de paquetes, por eso es necesario contar con un cableado regular para una buena comunicación entre dispositivos de red.

Figura 3.2: *Fotografía de una de las estaciones de trabajo*
Fuente: *Elaboración Propia*

Los equipos de computación carecían de IP asignadas adecuadamente, esto ocasionaba conflictos de IPs en cada configuración individual, también no se contaban con grupos de trabajos según sus unidades, para una mejor orientación y compartimiento de recursos como archivos e impresoras, cada equipo no contaba con el nombre del usuario para su debida identificación, observado todos estos detalles nos conlleva a realizar una mejor organización de la red tanto en la parte física con en la lógica para así tener un mejor

Figura 3.3: *Grupos de trabajo desorganizados*
Fuente: *Elaboración Propia*

3.2. FASE DE ADMINISTRACIÓN DE LA CONFIGURACIÓN

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

3.2.1. Planeación y diseño de la red

La meta de esta fase para implementación del servidor de administración de red de datos, es de tener los requerimientos para su ejecución, tales como el diseño estructural de la red tanto lógica como física, también la ubicación de los dispositivos de conectividad que interactúan con el servidor y así tener las necesidades para la red**(VER ANEXO B).**

Duran el diagnostico obtenido por medio de la observación, en la red anterior se percibieron muchas falencias, como repetidas conexiones entre switch vecinos a pocas distancia, ya que el objetivo es de tener una red de datos compactas y sin coaliciones ni perdidas de datos, así teniendo un diagnóstico del presente estudio se realizó un diagrama de red en base a los switch que interactúan en el entorno del cableado estructurado.

Figura 3.4: *Diagrama de red en base a Switch*
Fuente: *Elaboración Propia*

Al realizar el diseño del diagrama de la red en base a Switch, se obtuvo una mejor orientación, en cuanto al tamaño y expansión de la red actual, como también la cantidad de los dispositivos de comunicación existentes, en la que podemos describirlos según sus características de soportes de puertos de enlaces:

Unidad	Dispositivo	Características
4	Switch	D-LINK 24 puertos.
11	Switch	D-LINK 8 puertos.
2	Wireless	D-LINK 4 puertos.
1	Modem	ADLS 1 Mbps.
1	Servidor	Administración de redes de datos.
1	UPS	Capacidad de 1500 Wats.

Tabla 1: *Dispositivos de todo el cableado de red de datos*
Fuente: *Elaboración Propia*

Es así en la que se plantea la realización del esquema estructural, de toda la red de datos del predio central de la prefectura de pando, en este caso relacionando los equipos de forma espontánea y descriptiva, para así tener un idea de la red organizada global, las líneas segmentadas es la descripción de una conexión entre dos dispositivos y las llenas en de un dispositivo a un ordenador, cada switch esta etiquetado de acuerdo al área donde reside, de esta manera se tiene el esquema detallado de la red de datos.

Tomando en cuenta que un esquema estructural de toda la red de datos, es de gran ayuda ya que se tiene la ventaja, a la hora de reparar un cable dañado o una soltura de un conector Rj45. así se puede tener una idea de donde se tiene en corte, estas descripciones son de gran ayuda, ya que sin un esquema estructural sería muy difícil saber dónde se tiene un corte se tendría que testear la mayoría de los Switch.

La cual tomaría más tiempo la reparación del cableado, por lo tanto se diseña el esquema estructural de la red de datos de la prefectura de Pando, tanto planta alta como baja describiendo las áreas de trabajo.

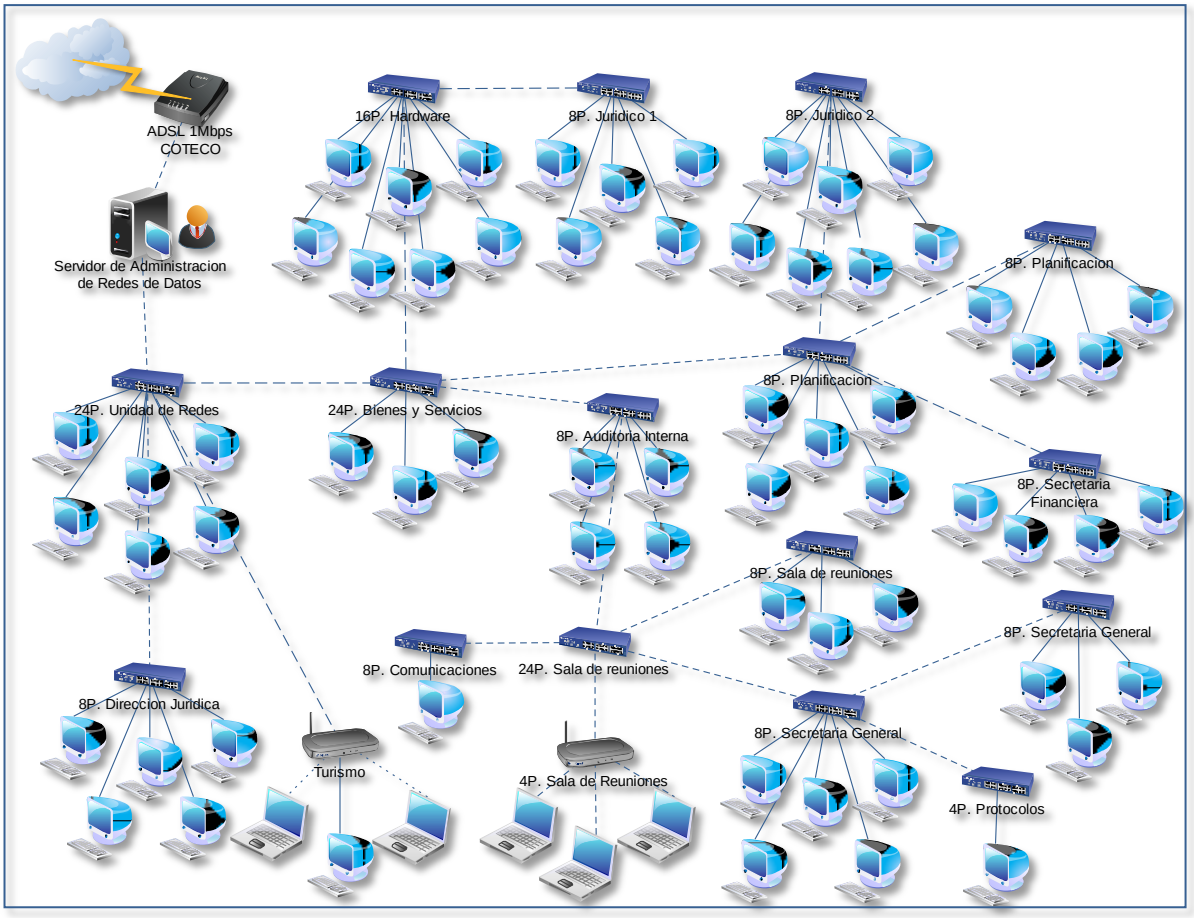


Figura 3.5: *Diagrama de red estructural descriptiva*
Fuente: *Elaboración Propia*

El siguiente diseño fue la implantación del croquis de la institución, relacionado con las conexiones del cableado estructurado de la red de datos, de esta forma se obtuvo los datos mediante la observación, ya que es la esquematización más importante para el entendimiento y ubicaciones de los dispositivos de comunicación, como del medio de trasmisión o cable UTP, de esta manera se tiene una descripción exacta del diseño final del cableado **(VER ANEXO B).**

El cual se trabajó con un cableado ya existente, en la que reestructuro la mayor parte, de manera más óptima para así tener un aproximamiento a las normas OSI, el centro donde se encuentra implantado el servidor de administración de redes de datos, está en la Unidad de Sistemas de acuerdo al croquis que se describe a continuación.

Figura 3.6: *Croquis estructural de la unidad de redes*
Fuente: *Elaboración Propia*

3.2.2. Selección de la infraestructura de red

La infraestructura que se optó para los diseños de implementación fue la topología en estrella, ya que los segmentos de cable de cada equipo en la red están conectados a un componente centralizado, como el Switches un dispositivo que conecta varios equipos juntos. En una topología en estrella, las señales se transmiten desde el equipo, a través del concentrador, a todos los equipos de la red, a mayor escala, múltiples LANs pueden estar conectadas entre sí en una topología en estrella.

Una ventaja de la topología en estrella es que si uno de sus equipos falla, únicamente ese equipo es incapaz de enviar o recibir datos y no afectaría a los demás, es por eso es una de las topologías más buenas eficaces.

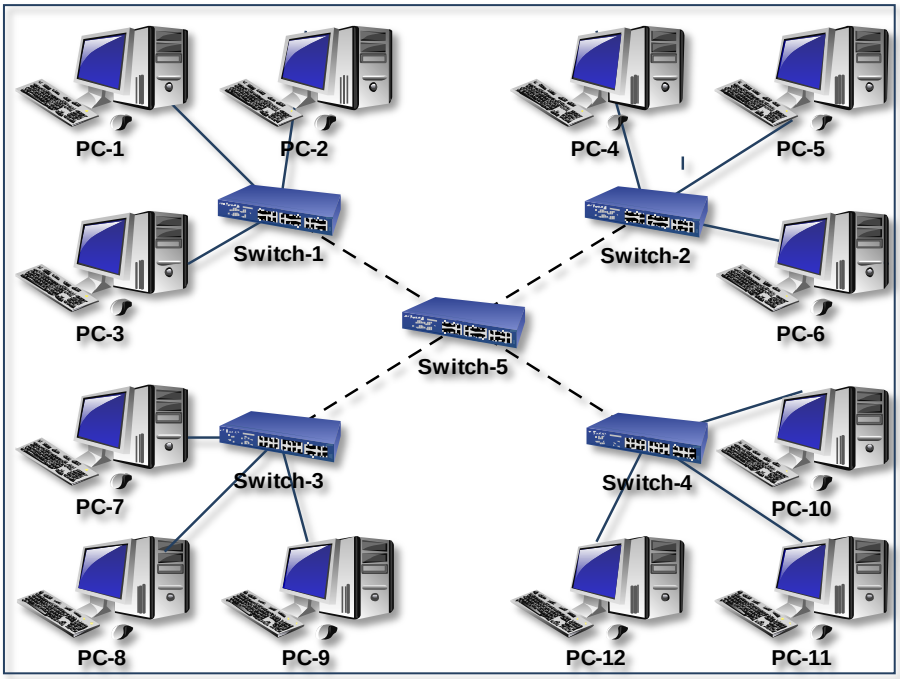


Figura 3.7: *Diagrama de topología estrella expandida*
Fuente: *Elaboración Propia*

La única desventaja de la topología en estrella, es que si realiza un circuito cerrado entre Switch de diferentes marcas, se tiene una pérdida de paquetes leve y a la larga es perjudicial para una red de datos.

3.2.3. Instalaciones y administración del software

En esta etapa se divide en dos partes la administración del hardware y el software en la que se describirá de manera resumida los dispositivos a usar de acuerdo a sus instalaciones:

A) ***Instalación del Hardware.-*** Para la implementación del servidor de red de datos y restructuración de la red, los dispositivos que se instalan son de acuerdos a las necesidades requeridas, como conexiones de equipos nuevos en la que se tiene que agregar una tarjeta de red en caso que no tenga una integrada o incorporación de un Switch si no ay puertos disponibles estas son algunas de las instalaciones de hardware.

El servidor de administración de redes de datos fue armado de acuerdo a las funciones que realizara y estas son sus características:

Unidad	Dispositivos	Descripción
2	Tarjetas de Red.	PCI con puerto RJ45-10/100.
1	Placa Madre.	Intel Gateguay.
1	Procesador.	Intel Pentium IV 3,06Ghz.
2	Memoria RAM.	Capacidad 1 Gb.
1	Disco Duro.	Capacidad de 160 Gb.
1	Lector de CD.	Marca LG.
1	Case Compag.	Color Blanca 40 x 40cm.

Tabla 2: *Características del servidor de red de datos*
Fuente: *Elaboración Propia*

De acuerdo a las características mencionadas el servidor de administración de redes, está en un estado bueno de acuerdo a sus dispositivos integrados, ya que teniendo los hardware idóneos sería mejor tomando en cuenta que subiría el nivel de rendimiento tanto del flujo de la red como el filtrado y monitoreo interno que realiza el servidor. Los hardware más importantes para la implementación del servidor fueron, los concentradores o switch ya que sin ellos no se pudiera interconectar grupos numerosos de equipos que se tiene en la prefectura a continuación se mencionaran los dispositivos que interactúan en la red de datos **(VER ANEXO C).**

Nº	Estado	Descripción	Oficina
1	Bueno	Switch marca d-link de 24 puertos	Unidad de redes
2	Bueno	Switch marca d-link de 24 puertos	Unidad de bienes y servicios
3	Bueno	Switch marca d-link des-1016d de 16 puertos	Unidad de Hardware
4	Bueno	Switch marca d-link de 8 puertos	Unidad de Asuntos Jurídicos 1
5	Bueno	Switch marca d-link de 8 puertos	Unidad de Asuntos Jurídicos 1
6	Bueno	Switch marca d-link de 16 puertos	Unidad de planificación
7	Bueno	Switch marca advantek ams-08p de 8 puertos	Unidad de planificación
8	Bueno	Switch marca advantek ams-08p de 8 puertos	Secretaria Financiera
9	Bueno	Switch marca d-link de 8 puertos	Unidad de Auditoría Interna
10	Bueno	Switch marca d-link de 8 puertos	Unidad de comunicación

11	Bueno	Switch marca advantek ams-08p de 8 puertos	Unidad de Jurídico
12	Bueno	Switch marca d-link de 16 puertos	Sala de reuniones
13	Bueno	*router marca d-link dir-400, wireless 108g*	Sala de reuniones
14	Bueno	Switch marca advantek ams-08p de 8 puertos	Sala de reuniones
15	Bueno	Switch marca d-link de 8 puertos	Unidad de Despacho
16	Bueno	Switch marca d-link de 8 puertos	Unida de secretaria General
17	Bueno	Switch marca d-link de 4 puertos	Unidad de Protocolos

Tabla 3: *Dispositivos Switch de toda la red de datos*
Fuente: *Elaboración Propia*

B) ***Administración del software.***-Para una buena administración del software se debe tener conocimiento experimental de softwareque se usara, en este caso se instalara él una versión estable de BRAZILFW 3.031 Firewall y Router que es una distribución del sistema operativo Linux que implementa un cortafuego y puede realizar tares avanzadas de ruteo y QoS, en la cual proporciona un interfaz gráfica para el fácil monitoreo y administración, y también cuenta con los agregados o funcionalidades extras llamados add-ons que se puede instalar de acuerdo a las necesidades requeridas.

Figura 3.8: *Logo de presentación de BRZILFW*
Fuente: *Elaboración Propia*

El software BRAZILFW, puede ser instaladas en las mínimas características de un equipo informático Pentium III, y soporta tres idioma el portugués, español y ingles, Pero para tener un mejor rendimiento, se opta armar en un equipo de características mayores y así optimizar cada una de sus servicios que nos proporciona este software a continuación observares sus características técnicas;

Especificaciones técnicas :	**Libs:**
Kernel: 2.6.25.4	ld-2.7.so*
Beep: 1.2.2	ld-linux.so.2@
Bind: 9.6.1rc1	libc-2.7.so*
Bridge-utils: 1.4	libcom_err.so.2@
Busybox-1.13.4	libcom_err.so.2.1*
Dialog: 1.1.20080316	libcrypt-2.7.so*
Dhcpd-4.1.1b1	libcrypt.so.1@
Dosfstools: 2.11	libc.so.6@
Dropbear: 0.50	libdl-2.7.so*
E2fsprogs 1.41.1	libdl.so.2@
E3 (edit) 2.7.1 incluye archivo de respaldo con ~	libe2p.so.2@
Ebtables: 2.0.8-2	libe2p.so.2.3*
Hdparm: 8.9 (con soporte para S.A.T.A.)	libgcc_s.so@
Iproute2: 2.6.25	libgcc_s.so.1*
Iptables: 1.4.0	libm-2.7.so*
Iputils: 20071127	libm.so.6@
Ipwatchd: 1.1 (stop ip crash when other person clone the brazilfwip)	libncursesw.so.5@
lshw B.02.13	libncursesw.so.5.6*
l7filter	libnsl-2.7.so*
Init-tools: 3.3	libnsl.so.1@
Madwifi: 0.9.4 (Drivers/Controladores para atheros)	libnss_compat-2.7.so*
Mtools: 3.9.11 (Soporteparasyslinux)	libnss_compat.so.2@
Ndiswrapper: 1.52 (Drivers/Controladores Windows XP)	libnss_dns-2.7.so*
	libnss_dns.so.2@

Pppd 2.4.4	libnss_files-2.7.so*
Rp-pppoe: 3.8	libnss_files.so.2@
Stunnel: 4.23 (soporte SSL)	libnss_hesiod-2.7.so*
Syslinux 3.71	libnss_hesiod.so.2@
Thttpd: 2.25b (servidor http)	libnss_nis-2.7.so*
Util-linux-ng 2.14.1	libnss_nisplus-2.7.so*
Wireless_tools: 0.29	libnss_nisplus.so.2@
Wpa_supplicant: 0.5.10 (wpawireless)	libnss_nis.so.2@

Tabla 4: *Especificaciones técnicas del BRZILFW*
Fuente: *Elaboración Propia*

El software BrazilFW, es una aplicación completamente gratuita y se la puede descargar de cualquier sitio web que distribuya esta aplicación de su página oficial del software http://brazilfw.com.br/users/woshman/bt/brazilfw.isoya que un software dedicado para la administración de redes basado en routeadores y firewall, y que tiene la capacidad de actualizarse de acuerdo a su necesidad y cuenta con los siguientes servicios:

Servicios Existentes	Descripción
Modo de Conexión	Los modos que soporta son:STATIC(IP fijo), DHCP, Dinámico (PPPoE), edge.
WebAdmin	Es la parte grafica del servidor por medio de protocolo SSL.
Servidor Bind	Que es un servidor DNS.
Squid-3.0.	Es un proxy basado en STABLE15.
QOS	Este servicio sirve para el control del ancho de banda y calidad de conexiones.
Sub-Redes	Este servicio se recomienda con tarjetas individuales para tener un mejor rendimiento en enrutamiento.
Load Balance	Este servicio es el balanceo integrado, que se puede realizar con cualquier tipo de Conexión (STATIC, PPPOE, DHCP e edge).

DHCP	Servicio de Server para red y Sub-Redes.
GSM	Este servicio solo seria utilizado si tendríamos un código de telefónico o tarjetas satelitales.
Cálculo de conntrack	Con el nuevo cálculo, ahora son posibles 1.652 conexiones aproximadamente por 1 MB de memoria RAM instalada.
Ipupdate 2.0	Este servicio es para conexiones por link independiente.
wireless	Servicio para soporte de wireless en modo cliente.
Email	con suporte para ssl (gmail).
Port Forwarding	Servicio para el direccionamiento de puertos.
Smart Route	Es ruter lógico en la cual se trabaja con tablas de enrutamiento.
IP X MAC	Es para la seguridad tanto física como lógica de la red de datos se domina amarre de IPx MAC.
DansGuardian	Ideal para uso en redes empresariales en realidad es un filtro de contenidos.
Sarg	Es una herramienta que sirve para sacar reportes diarios de acuerdo a las IP registradas bajo su Log.
WebAlizer	Este servicio es para uso en Proveedores.

Tabla 5: *Servicios que brinda el servidor BrazilFW*
Fuente: *Elaboración Propia*

Muchos de estos servicios funcionan de manera predeterminada o por defecto, otros servicios se tienen que configurar de acuerdo a las necesidades, también es importante saber las características mínimas para la instalación del servidor BrazilFW, continuación mostraremos las características más primordiales para una instalación:

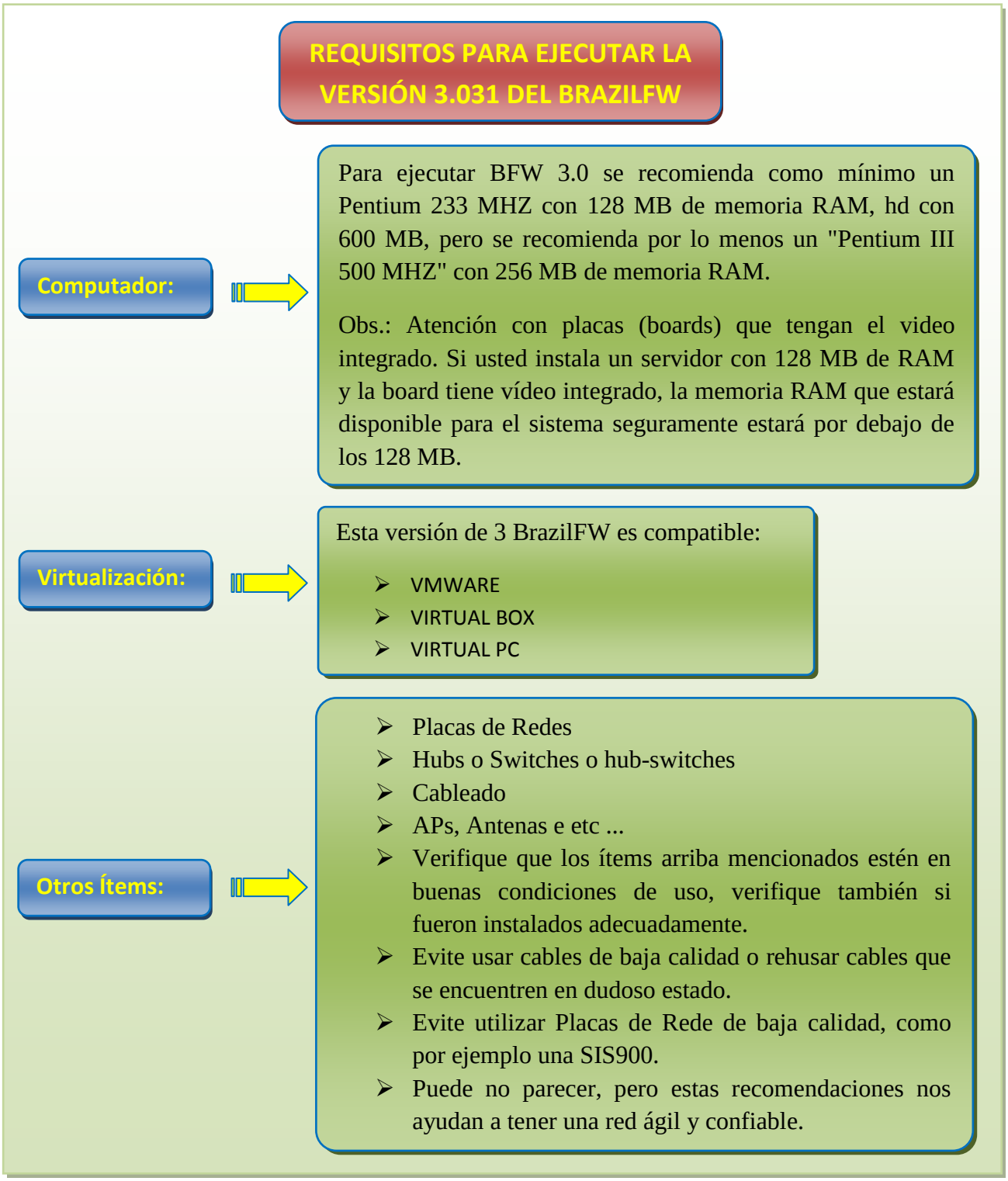


Figura 3.9: *Diagrama de requisitos para la instalación de BrazilFW*
Fuente: *Elaboración Propia*

Para las instalaciones prácticas estará ajuntada una breve instalación del BrazilFW, de manera detallada y entendible **(VER ANEXO D).**

Una vez realizado la instalación satisfactoriamente, se procede la configuración de una serie de archivos, en este caso se mostrara la configuración de los archivos más importantes y primordiales del servidor, en que mostraremos como se configura y para qué beneficios o funciones nos traerá en la implementación, con las configuraciones más importantes:

1) La configuración más importantes es la del archivo maestro *brazilfw.cfg* que se encuentra predeterminado en la ruta, "***/etc/brazilfw/brazilfw.cfg***" y se configuro de acuerdo a los requerimientos.

Código: *brazilfw.cfg*

```
WEBADMIN_PORT='8181'
SSH_PORT='22'
ADMIN_AUTH='xxxxxxxxxxxxxx'
DNSSERVER='yes'
DNS1=''
DNS2=''
DHCP_DNS1=''
DHCP_DNS2=''
NAMESERVER='ns'
DOMAIN='scainet'
LOCALDOMAIN='sis'
PERSIST_LOG='no'
USE_SWAP='no'
SWAP_MEM=''
PARTITION=''
TIMEZONE='EST3'
CACHE_DISK='yes'
USE_QOS='no'
QOS_DEFAULT_GUARANTEE='10'
DHCP_SERVER='no'
DHCP_DEFAULT_LEASE='7200'
IPUPDATE='no'
IPUPDATE_REFRESH='600'
USE_MAC_CONTROL='yes'
DISABLE_NAT='no'
DISABLE_CONNLIMIT='no'
CERTIFICATE_ISSUED_TO=''
EXTERNAL_PING='yes'
```

Siendo así uno de los archivos más importantes, se explicara cada línea de configuración y la importancia que se tiene de la siguiente manera.

Ahora veamos las variables y sus definiciones:

Variable	Descripción
WEBADMIN_PORT='8181'	Puerto de acceso al WebAdmin. Puerto por defecto = 8181.
SSH_PORT='22'	Puerto de acceso al ssh. Puerto por defecto = 22.
ADMIN_AUTH='xxxxxxxxx'	Contraseña de root encriptado.
DNSSERVER='yes'	Servidor DNS nativo del 3.x (Bind). Por defecto está habilitado ='yes'. Estado del Bind habilitado las variables DNS1; DNS2; DHCP_DNS1 e DHCP_DNS NO deben ser llenadas.
DNS1=''	Sólo deben ser llenadas si el elBind (DNSSERVER) está en 'no'.
DNS2=''	Sólo deben ser llenadas si el elBind (DNSSERVER) está en 'no'.
DHCP_DNS1=''	Sólo deben ser llenadas si el elBind (DNSSERVER) está en 'no'
DHCP_DNS2=''	Sólo deben ser llenadas si el elBind (DNSSERVER) está en 'no'.
NAMESERVER='ns'	Nombre del Servidor DNS. Por defecto viene como 'ns'.
DOMAIN='scainet'	Nombre del Dominio. Puede ser cambiando de acuerdo al lugar de trabajo.
LOCALDOMAIN='sis'	Extensión del Dominio. Puede ser cambiando de acuerdo al lugar de trabajo.
PERSIST_LOG='no'	Graba el log en disco. Por defecto viene deshabilitado = 'no'.
USE_SWAP='no'	Activa Memoria virtual en disco. Por defecto viene deshabilitado = 'no.'
SWAP_MEM=''	Establece el valor de la Memoria Virtual en disco. Ejemplo: *SWAP_MEM='1024'* - Será creada una memoria virtual de 1024 MB que será tomada de la memoria RAM del Server.
PARTITION=''	Define manualmente donde está la partición, en caso de usar otro HD. Aún se está testeando.
TIMEZONE='EST4'	Región de los huso horario
CACHE_DISK='yes'	Servidor Proxy nativo del 3.X (Squid). Por defecto

	viene deshabilitado = 'no'.
USE_QOS='no'	Control de Ancho de Banda del 3.X Por defecto viene deshabilitado = 'no'.
QOS_DEFAULT_GUARANTEE='10'	Valor por defecto que garantiza para QoS.
DHCP_SERVER='no'	Servidor DHCP. Por defecto viene deshabilitado = 'no'.
DHCP_DEFAULT_LEASE='7200'	Tiempo de concesión para DHCP Server. Por defecto viene '7200' = 2 Horas.
IPUPDATE='no'	Viene deshabilitado por defecto.
IPUPDATE_REFRESH='600'	IpUpdate y tiempo de actualización. Por defecto viene deshabilitado = 'no' y con el tiempo '600' = 10 Minutos.
USE_MAC_CONTROL='yes'	Control de MAC X IP. Por defecto viene deshabilitado = 'no'.
DISABLE_NAT='no'	Deshabilita el Enmascaramiento de IP (Compartido). El valor predeterminado es = 'no'.
DISABLE_CONNLIMIT='no'	Deshabilita el Connlimit automático del QOS. El valor predeterminado es = 'no'
CERTIFICATE_ISSUED_TO=''	Para personalizar el certificado de (https).
EXTERNAL_PING='yes'	Activa o Desactiva el Ping Externo. Por defecto está Activado = 'yes'

Tabla 5: *Variables maestras del BrazilFW*
Fuente: *Elaboración Propia*

2) El siguiente archivo a configurar es **accept.cfg** que son los puertos predeterminados del servidor, en la que se abre los accesos externos a los siguientes servicios que por defecto bien bloqueados, el archivo se encuentra en la ruta**"/etc/brazilfw/ports/accept.cfg",** la configuración se realiza de acuerdo a los servicios que se estén usando en este caso se tiene 5 servicios habilitados en este momento pueden ser más o menos de acuerdo a la necesidad:

Código: *accept.cfg*

```
yes 22 tcp # Acceso externo a SSH
yes 53 all # Acceso externo a DNS
yes 3128 tcp # Acceso externo a Squid
yes 8080 tcp # Acceso externo a Dansguardian
yes 8181 tcp # Acceso externo a Webadmin
```

En este código habilitamos los servicios más importantes que tiene el servidor como, SSH que nos servirá para el acceso remoto al servidor, DNS que nos servirá para registrar a los equipos que estarán en la red, SQUID que hará un papel importante como proxy de cacheo y de reporte con sarg, DANSGUARDIAN que será el filtro de contenido para internet, WEBADMIN que será el entorno grafico del servidor en la que podremos hacer operaciones básicas de registro y bloqueo.

3) El siguiente archivo que se configurara, es para red local que se distribuirá con la IP 192.168.7.1/24, en la que de manera predeterminada el BrazilFW apunta a eth0 para la red local y la eth1 para internet, de acuerdo a estos parámetros primero se configurara la red local que se encuentra en la ruta **"/etc/brazilfw/logical/local"**se edita el archivo local que nos presentara de la siguiente manera:

Código: *local*

```
LINK_ALIAS="local"
LINK_CONNECTION="local"
LINK_TYPE="static"
LINK_IP="192.168.7.1"
LINK_NETMASK="255.255.255.0"
```

Tomando en cuenta que se trabajara en la tarjeta de red **eth0**, que es la predeterminada para la red local, con IP 192.168.7.1 que es del servidor de acurdo a estos parámetros ya se pueden configurar equipos bajo el rango del servidor 192.168.7.2 a 192.168.7.254 si encaso se requiere de otra sub-red se recomienda otra tarjeta, pero la configuración es de la misma manera solo cambiaría el nombre del archivo ej.: local2 y el rango de IP.

4) Luego de tener configura la red local, procedemos a la configuración de la conexión a internet, la cual de pende mucho el tipo de servicio de dicho proveedor, en este caso se configuro una conexión estática vía modem de coteco, las modificaciones se realizan en el archivo internet que se encuentra en la ruta **"/etc/brazilfw/logical/internet"** se

edita el archivo internet y se configura de acuerdo a las IP que se asigna el proveedor en este caso es 192.168.40.11 que es de una sub-red entrante por el modem.

Código: *internet*

```
LINK_ALIAS="internet"
LINK_CONNECTION="internet"
LINK_TYPE="static"
LINK_IP="192.168.40.11"
LINK_NETMASK="255.255.255.0"
LINK_GATEWAY="192.168.40.1"
LINK_DOWNSTREAM="0"
LINK_UPSTREAM="0"
LINK_WEIGHT="2"
```

El nombre de la conexión tiene que ser el mismo nombre del archivo a configurar, si se tiene otra conexión se tendría que colocar internet2 y la configuración seria de la misma manera de acuerdo al código observado.

5) Para el aumento de una tarjeta de red física, en caso que se tengo otra conexión entrante de internet se tiene que configurar los archivos del mismo nombre de la conexión creada, la configuración física se encuentra en la ruta **"/etc/brazilfw/physical/internet2",** no debemos olvidar que este código es para agregar nuevo dispositivo de red de esta forma:

Código: internet2

```
INTERFACE_TYPE="cabled"
INTERFACE_PHYSICAL="eth2"
```

Se crea y edita el archivo, luego se modifica la interface eth2, no olvidemos que esto describe a la tarjeta de red nueva y el nombre guardado en internet2 para poder identificar la el nuevo dispositivo de esta forma ya podemos usar la nueva tarjeta de red.

6) En este paso configuramos el filtrado de IP x MAC, que ya se habilito en el punto uno anterior, la línea de código que habilita es *USE_MAC_CONTROL='yes',* que se

encuentra **"/etc/brazilfw/brazilfw.cfg"** luego de la habilitación se procede al llenado de los IP x MAC, que se encuentra en la ruta **"/etc/brazilfw/reserve.cfg"** el llenado se debe realizar de acuerdo a estos parámetros, el MAC debe estar con dos puntos(:) y no con el guión (-), Ej. 192.168.0.1 2e:00:54:16:a4:66 este formato se debe realizar para todo los registros como a continuación:

Código: *reserve.cfg*

```
192.168.7.2 00:13:8F:A0:20:F8 #CESAR CRISPIN
192.168.7.3 00:08:54:2F:A7:A5 #MARIA ELODIA SUAREZ
192.168.7.4 00:19:D1:F6:F1:BB #LICY CARDOZO
192.168.7.5 00:17:31:87:E9:80 #GIOVANA PACO
192.168.7.6 00:14:2A:CA:0B:A2 #EVER FAVIO LIMA
192.168.7.7 00:08:A1:8A:C2:61 #BIOMETRICO CESAR
192.168.7.10 00:1D:92:54:C7:76 #EFRAIN OPI CONDORI
192.168.7.11 00:19:21:2D:A0:25 #AFUSTIN VELASQUES
192.168.7.12 00:0A:E6:31:8B:92 #RODRIGO COCK
192.168.7.61 00:1C:C0:91:93:03 #ALFREDO APARICION
192.168.7.71 00:15:E9:AA:7E:87 #SINGARA MIAUCHI
192.168.7.72 00:01:29:21:9A:11 #ANGELICA DESPACHO
192.168.7.73 00:19:21:43:7B:1E #TENIENTE OLIVER
192.168.7.74 00:01:6C:F9:06:5B #RICARDO TORRES
192.168.7.75 00:13:CE:92:54:BF #ADA HIELMAU BECERRA
192.168.7.91 00:13:CE:4D:62:19 #JACINTO CONDORI T
192.168.7.92 00:19:5B:D2:45:7E #GUNAR D. ZEBALLOS
192.168.7.101 00:19:D1:39:71:AC #PIALY TORRICO
192.168.7.102 00:25:22:16:A4:6D #JAVIER POL ARAMAYO
192.168.7.103 00:07:E9:82:8B:E6 #VICTOR H TRUJILLO SUAREZ
```

Los beneficios que trae MAC x IP cuando está habilitado en el **brazilfw.cfg,** si el MAC no está en la lista, el cliente no conseguirá hacer nada, ni siquiera podrá conseguir hacer ping al BFW, a través del MAC no registrado sólo se podrá tener acceso al puerto del webadminy al puerto ssh, esto nos brinda seguridad física como lógica ya que personas externas a la institución no podrán acceder a nuestros servicios por qué no estará registrados en nuestra lista base.

7) Ya que el SQUID se ha habilita en el archivo maestro **brazilfw.cfg** en el punto uno, en la línea de código CACHE_DISK='yes' como elDansguardian es un filtro que si integra al SQUID para la filtración del "contenido incorrecto", para habilitar el Dansguardian se debe entrar a la ruta **"/etc/brazilfw/custom/squid.cfg",** y se cambia la línea de código de esta forma, WEB_CONTENT_FILTER='yes' y se ve de esta forma.

Código: *squid.cfg*

```
MAXIMUM_OBJECT_SIZE=''
MAXIMUM_OBJECT_SIZE_MEMORY=''
MAXIMUM_CACHE_SIZE=''
MAXIMUM_RAM_CACHE_SIZE=''
WEB_CONTENT_FILTER='yes'
SQUID_REPORT='sarg'
SARG_LONG_URL='no'
REPORT_DELETE_AFTER_DAYS='30'
RUN_REPORT_PERIODIC='yes'
CACHE_LOG='no'
TPROXY='no'
HIDE_PROXY='no'
SARG_GRAPHS='no'
```

Es muy útil porque se necesita un control riguroso de las páginas visitadas, siendo mucho más completas que las reglas del mismo SQUID. Aunque es riguroso, es extremadamente flexible, en este archivo también se realiza la habilitación de del SARG que especial para el reporte en tiempo real.

8) Después de la habilitación de Dansguardian se procede a la configuración de las diferentes categorías, que se encuentra en la ruta**"/etc/brazilfw/dansguardian/lists/"** la cual ofrece este filtro de contenidos y se nombrara y describirá cada contenido de manera resumida y práctica.

(/etc/brazilfw/dansguardian/lists/)

- **bannedextensionlist** ==> Lista de bloqueo por extensión de archivos. Aquí colocan las extenciones de los archivos que desean bloquear el acceso.
- **bannedsitelist** ==> Lista de sitios bloqueados, coloquen aquí sus listas en archivo blacklist.
- **filtergroupslist**==> aquí se pode atribuir a un usuario a determinado grupo, al principio todos son un solo grupo.
- **bannediplist** ==> Lista de IP's bloqueadas. Las IP's contenidas en este archivo no tendrán ningun tipo de acceso.
- **bannedmimetypelist** ==> Tipo MIME bloqueados (download bloqueado).

- **bannedphraselist** ==> Lista de frases "prohibidas" dentro de página (y no una URL).
- **bannedregexpurllist** ==> Lista de expresiones regulares bloqueadas.
- **bannedurllist** ==> Lista de URLs bloqueadas.
- **banneduserlist** ==> Lista de usuarios bloqueados, usuarios sin acceso a Internet.
- **banneduserlist** ==> Usuarios bloqueados.
- **contentregexplist** ==> Contenido basado en expresiones regulares que serán sustituidos.
- **exceptioniplist** ==> Excepción de IP's filtradas (IP's de la RED que no serán filtrados).
- **exceptionsitelist** ==> Sitios liberados. los sitios contenidos aquí son liberados de todo contenido.
- **exceptionphraselist** ==> Lista frases que las consideramos una excepción.
- **exceptionurllist** ==> Lista de urls que consideramos son una excepción (urls liberadas).
- **exceptionuserlist** ==> Lista de usuarios que consideramos una excepción.
- **greysitelist** ==> Sitios que estan en la lista ¿¿blanca??
- **greyurllist** ==>URLs que están en la lista ¿¿blanca??
- **pics** ==> Definición de PICS Labeling.
- **weightedphraselist** ==> Lista de frases/palabras e seus "pesos" (os pesos podem ser positivos ou negativos)

(/etc/brazilfw/dansguardian/)

- **dansguardian.conf** ==> Archivo de configuración principal.
- **dansguardianf1.conf** ==> Archivo de configuración de grupos de usuarios.

3.2.4. Provisionamiento

Es necesario prevenir con materiales de redes como dispositivos, en el cual atreves de la unidad de sistemas de la prefectura de pando, se realizó un pedido de materiales de red y

también dispositivos de comunicación estos materiales están provisionalmente ostentado para un año de gestión o según las actividades que se realice en la unidad de redes estos son los materiales que están en pedido actualmente bajo proformas realizadas.

Nº	DESCRIPCIÓN DEL DISPOSITIVO	CANTIDAD	COSTO Bs.
1	Caja de cable UTP de 300mts. categoría 5	5	3500
2	Bolsa de RJ45 500 unidades.	2	1000
3	Canaleta de 1 pulgada.	100	1200
4	Rosetas dobles RJ45	50	500
5	Cajita de grapas de ¾ de pulgadas.	10	150
6	Haming de comunicación	6	2000

Tabla 6: *Materiales para la unidad de redes*
Fuente: *Elaboración Propia*

Tomando en cuenta que también se realiza Backup del servidor cada dos días de manera automática para así estar alerta a cualquier imperfecto o caída del servidor.

- **Plan de contingencia:** Es el proceso de determinar qué hacer si una catástrofe sucede en una empresa. la institución debe estar lista a la reanudación de las actividades ante una calamidad, misma que podría ser una de las situaciones más difíciles con las que una organización deba enfrentarse. El plan de contingencia es sujeta a tres acciones importantes:

    1. **Prevención:** Es aquí donde tomamos en cuenta prevenir incidentes futuros es por eso que se tienen como prevención tener un equipo de computación completo por si sucedo algo con el que actualmente está funcionando, este equipo tiene que tener todas las configuraciones actuales y tiene que estar listo para ser usado en cualquier situación.

    2. **Detección:** Existe varias formas detectar los incidentes pero una de las mejores formas es examinar todos los daños tanto naturales como eventuales que todavía no están considerados, tales como cortes de

energía, robos, entre otros, para que a futuro se pueda prevenirlos y llegar a una pronta solución en el caso de que llegasen a suceder.

3. **Recuperación:** Se considera el mantenimiento de los recursos afectados por un desastre que posee la institución ya sea física o lógica, es por eso que se tiene backups diarios para si poder tener una recuperación inmediata y también se cuenta con un equipo ya configurado por si se quema el que está funcionando.

3.3. ADMINISTRACIÓN DEL RENDIMIENTO

Para una buen control del rendimiento, primeramente ay que tener los instrumentos necesarios , ya que el servidor esta implementado bajo la distribución de Linux que es BrazilFW, este software como tal cuenta con las herramienta de testeo ya que está dedicado a la administración de redes de datos. La administración del rendimiento se divide en 2 etapas:

3.3.1. Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red de datos, es importante hacer monitores de diferentes tipo ya que es impredecible los errores o bajadas de conexiones, el servidor de administración de redes, tiene diferentes tipos de monitores para así tener un vistazo resumido de los que pasa en la red en tiempo real las herramientas que cuenta son:

a) IpTraf Monitoriamente de Tráfico de Rede:

IPTrafes un utilitario en Linux basado en consola para estadísticas de rede, funciona recolectando información de las conexiones TCP, como las estadísticas y la

actividad de las interfaces, así como las caídas de tráfico TCP y UDP. Se encuentra disponible en sistemas operativos GNU/Linux.

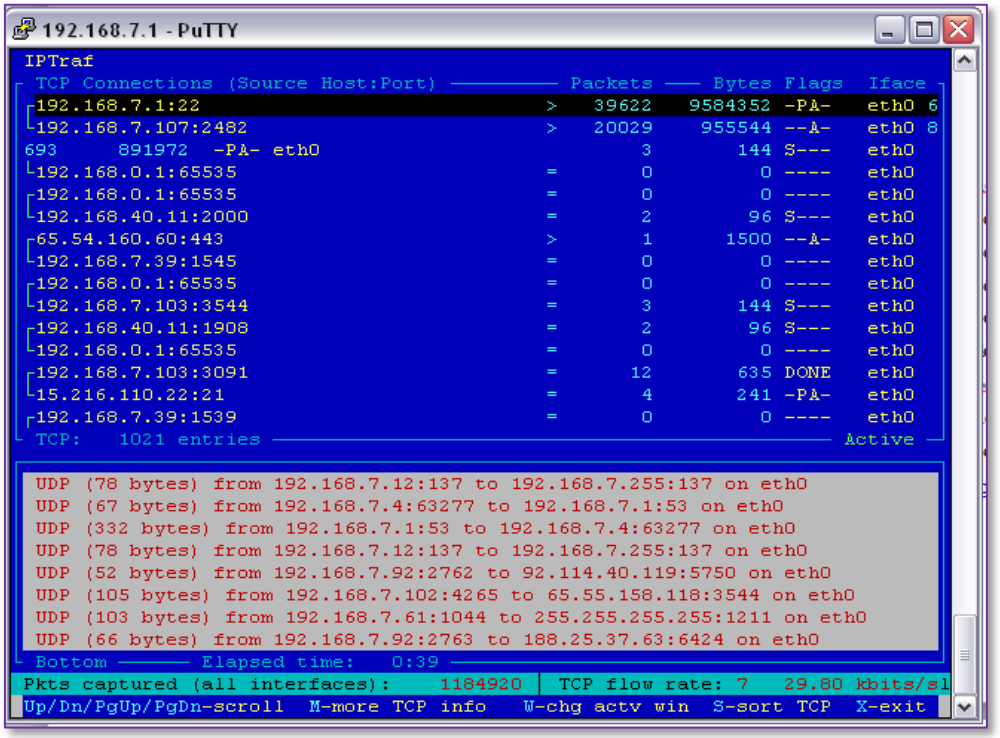


Figura 3.10: *El IPTRAF en acción.*
Fuente: *Elaboración Propia*

La herramienta del iptraf nos proporciona múltiples estadísticas que se pueden medir y muchas funciones como:

- Por protocolo/puerto
- Por tamaño de paquetes
- Genera logs
- Utiliza DNS para traducir direcciones.

Ventajas:

- Simplicidad

- Basado en menús (utiliza “curses”)
- Configuración flexible

IPTtraf admite la audición de múltiples protocolos: IP, TCP, UDP, ICMP, IGP, IGMP, IGRP, OSPF, ARP, RARP. Además de un menú de opciones a pantalla completa, IPTraf posee las siguientes características:

- Monitor de tráfico IP que muestra información del tráfico de la red.
- Estadísticas generales de las Interfaces.
- Módulo de estadísticas de LAN que descubre hosts y muestra datos sobre su actividad.
- Monitor TCP, UDP que muestra la cuenta de los paquetes de red para las conexiones de los puertos de aplicaciones.

Utiliza el "raw socket interface" que lleva el kernel permitiendo ser usado por un amplio rango de "tarjetas de red".

b) Iftop Uso de red por conexión:

El comando top muestra los procesos que están utilizando la mayoría del tiempo de procesamiento y memoria y se muestra el uso iftop interrupción de entrada / salida. El iftop es un poco diferente de estas aplicaciones, que muestra el uso de la red por la conexión. La vista predeterminada muestra los destinos de las conexiones (números de puerto se puede ver con el atributo p), con un volumen de datos transmitidos en un formato numérico y gráfico horizontal. Varias de las funciones encargará del control del video, pulse la tecla? para ver una página con la ayuda de estos controles. El iftop también tiene la opción de la línea de comandos para filtrar el tráfico y la selección de interfaces.

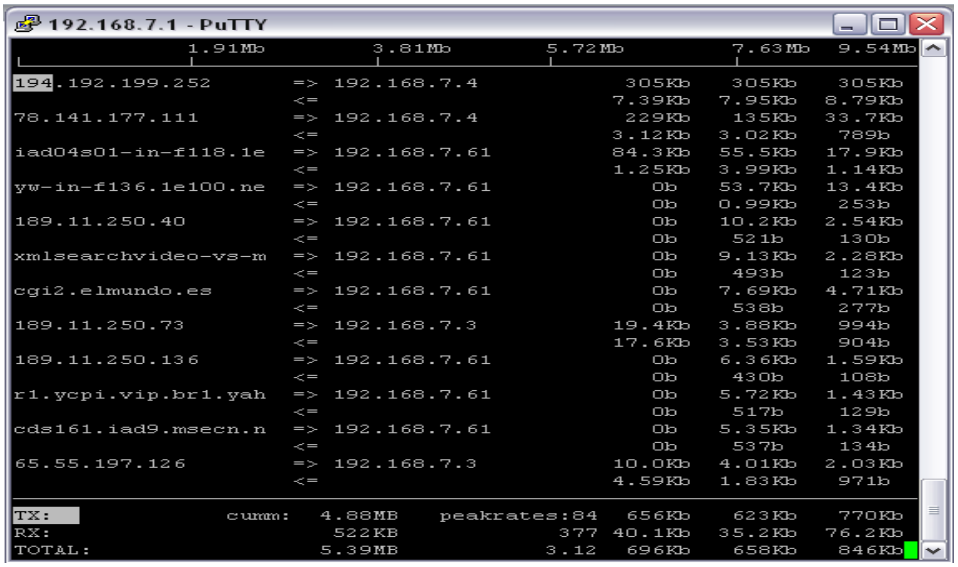


Figura 3.11: *El IFTOP en acción.*
Fuente: *Elaboración Propia*

c) Htop Visualizador de procesos:

El htop es una herramienta similar al principio, pero tiene algunas diferencias que hacen que sea más fácil de usar. La interfaz permite atajos simples se pueden utilizar para alcanzar un precio de F3 F7 y F8 para cambiar la prioridad del proceso, F9 para poner fin a un proceso. También puede desplazarse horizontal y verticalmente, y pueden ver todos los procesos y su línea de comandos completa.

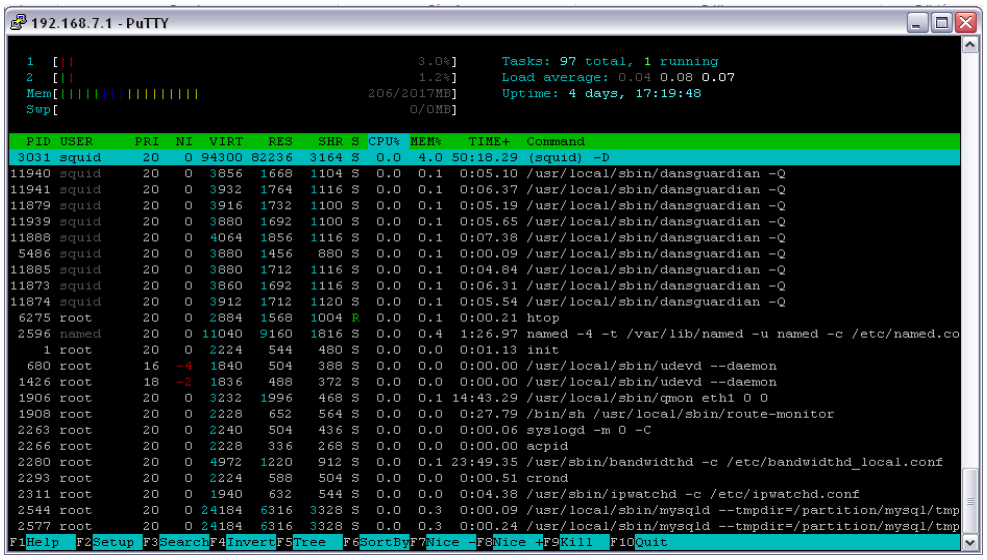


Figura 3.12: *El HTOP en acción.*
Fuente: *Elaboración Propia*

d) Ifstat - Monitor de interfaces de rede:

Muestra el rendimiento de la interfaz seleccionada, mostrando la cantidad de bytes de datos dentro y fuera de la misma.

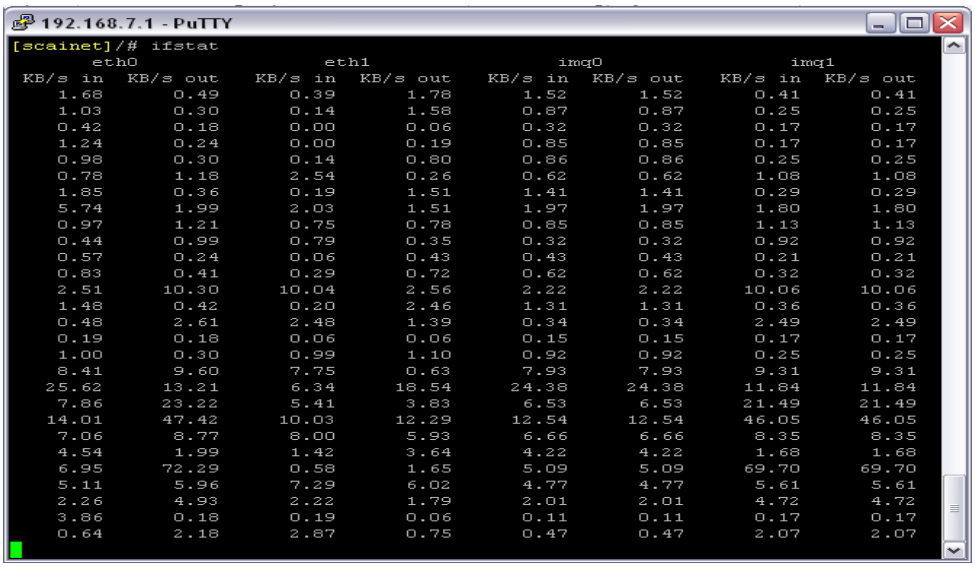


Figura 3.13: *El IFSTAT en acción.*
Fuente: *Elaboración Propia*

El servidor también cuenta con monitores gráficos que en la cual es más amigable al observar, este componente se encarga de mostrar el tráfico de entrada de la red entrante en este caso es el servicio de internet que contamos.

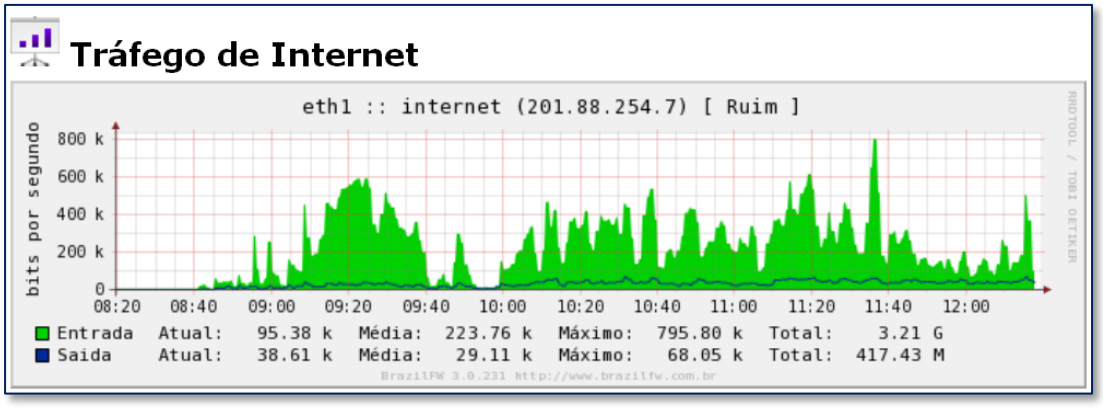


Figura 3.14: *Monitoreo del tráfico de internet.*
Fuente: *Elaboración Propia*

También viene acoplado para monitorear el sistema, este tipo de monitoreo se encarga de ver la cantidad de disco usado, memoria, y procesador ya que muchas veces puede colgarse un servidor por la falta de memoria RAM o disco duro.

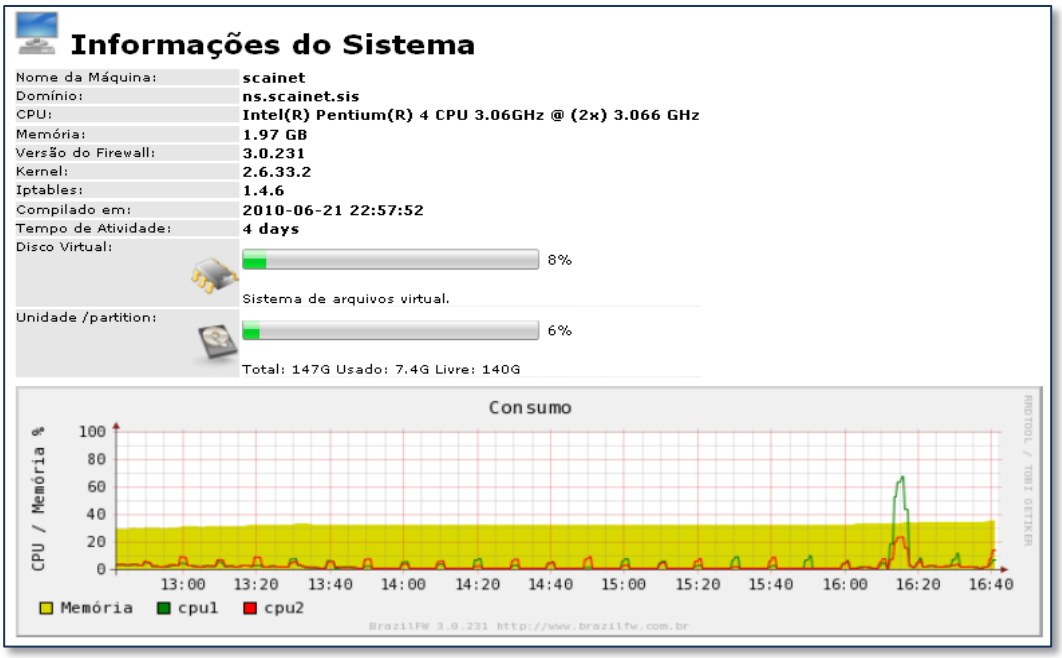


Figura 3.15: *Monitoreo del tráfico del CPU y Memoria RAM*
Fuente: *Elaboración Propia.*

3.3.2. Análisis

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño. En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

- *Utilización elevada.*
- *Tráfico inusual.*
- *Elementos principales de la red.*
- *Calidad de servicio.*
- *Control de tráfico*

Todos estos los puntos se centran en base al monitoreo de acuerdo a los resultados obtenidos se hace el análisis para llegar a un deducción y así tomar decisiones.

3.4. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

3.5. Administración de seguridad

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad, el servidor de administración tiene un módulo especifico en seguridad, en la que está dedicado a protección bajo su firewall, otra parte es el squid que viene integrado con el dansguardian que es de gran utilidad en la parte de filtrados también se ha agregado el L7-Firewall, que nos sirve para realizar un filtrado más óptimo.

3.5.1. Prevención de ataques

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación del dansguardian que filtra los contenidos y el control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

Figura 3.16: *Monitoreo del tráfico de internet.*
Fuente: *Elaboración Propia.*

3.5.2. Detección de intrusos

La detección de intrusos se puede lograr mediante un sistema de protocolos L7-Ferewall que vigila el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red como también bloquea los puertos débiles y limita herramientas peligrosas.

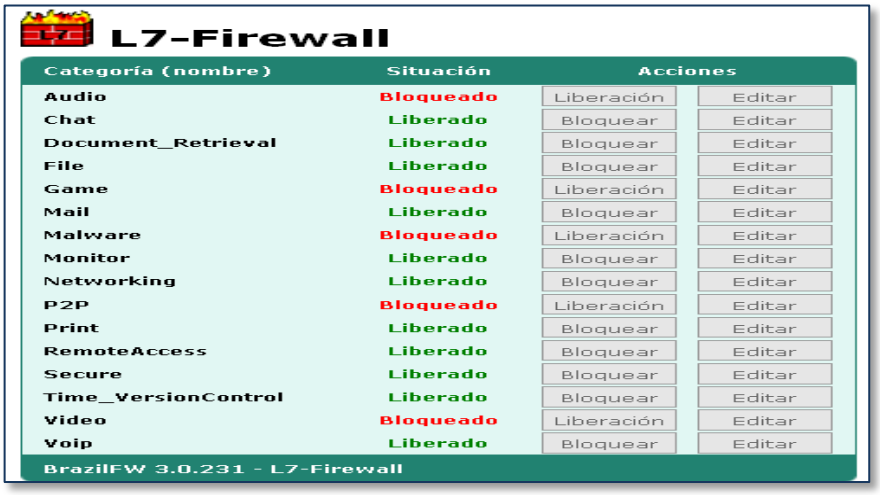


Figura 3.17: *Interfaz gráfica del L7-Ferewall.*
Fuente: *Elaboración Propia.*

CAPÍTULOS IV CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

Como conclusión del presente proyecto, quiero manifestar que se consigo implementar el servidor para la administración de redes de datos para el predio central de la Prefectura Pando, el cual se puede aplicar en cualquier tipo de redes ya que esta bajo implementado bajo la distribución de BrazilFW que es una distribución de Linux con kernel 2.6, de acuerdo a esta distribución se puede añadir más módulos de monitoreo como de seguridad, tomando en cuenta que es un sistema actualizable.

También se concluyó con los planos estructurales de red, de ambas plantas del edificio central, teniendo en cuenta que se finalizó los diseños lógicos y esquema de toda la red de datos, se imprimió y se plasmó en las paredes de la unidad de redes para así poder facilitar las búsquedas a fallas futuras, también se entregó la lista de todos los usuarios registrados en el edificio, de acuerdo a IP xMAC y el cargo que ocupan cada usuario.

Este servidor se implementó de acuerdo al cronograma presentado en el perfil, y se basó bajo las etapas de la metodología funcional, tomando en cuenta que en peso a funcionar hace 7 meses atrás, en la que fue de gran utilidad y se corrigió algunos percances en el proceso de uso, sin mencionar que se tiene una cache bien cargada y ayuda a la exploración de sitios cotidianos como de sistemas de usos que son muy pesados.

El servidor ofrece los servicios de filtrado bajo el Dansguardian, Squid como cache, reportes con sarg de acuerdo a los sitios visitados, monitoreo de ancho de banda, monitoreo del sistema como tal, firewall bajo IPTABLE, un están de herramientas de redes completo y también los addons agregados que tienen múltiples funciones como monitoreo, firewall bajo layer-7, administrador auxiliar, etc.

Finalmente, considero que los objetivos generales y específicos planteados al inicio de este trabajo fueron cumplidos en su totalidad. Quizá algunas aportaciones más significativas de este Proyecto de Grado es que a través del servidor implementado juntamente con los

diseños de los planos y esquemas reducir de forma notable, tiempo y esfuerzo en para un control de falla o rotura de un cable de red o coalición de paquete, que hasta hace poco era realizado de forma morosa ya que se tenía que testear la mayoría de los cables para encontrar el error ahora solo se tendría q mirar el plano estructural y el registro del servidor así se encontraría el sector de corte.

4.2 RECOMENDACIONES

Amanera de optimizar este proyecto, se pueden tomar en cuenta los siguientes puntos, para poder estructurarlos a corto plazo ya es más de la parte económica, y se necesitaría algunas gestiones para poder aplicarlos:

- Implementar un mayor ancho de banda, para una mejor navegación de los usuarios y así no tener molestias de conexiones como también para repartir a otros predios de la institución.

- Comprar un servidor específico de característica mejor, para habilitar la mayoría de los servicios, ya que el que tenemos es de características regulares.

- Realizar la compra de dispositivos de interconexión de alto alcance como SkyPilot para conectar el edificio de excoordepando con el predio central.

Implementar nuevos módulos de monitoreo más específicos, para así tener un completo control de toda la red de datos.

BIBLIOGRAFÍA

- González Dumrauf (2002, 13 de Mayo) Administración De Redes.
  Extraído 13 de Agosto 2010 desde:
  www.chaco.gov.ar/UTN/AdmRedes/Traduccion/cap1.doc

- Gabriel Verdejo Alvarez (2003, septirmbre) Seguridad en Redes IP.
  Extraído 25 de Abril 2010 desde:
  http://archivos.abcdatos.com/tutoriales/O/O149/O149.zip

- White Paper (2002) Las redes IP: Conceptos básicos
  Extraído 14 de agosto 2010 desde:
  http://www.casadomo.com/redirLink.aspx?url=images%5Carchivos%5Caxis_las_redes_ip.pdf&src=/profesionalesDetalle.aspx

- William Marín Moreno (2009, 17 Febrero) Modelo OSI.
  Extraído 10 de Agosto 2010 desde:
  www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip(oficial).pdf

- Pat Eyler, (2001) Redes Linux con TCP&IP.
  Editorial PEARSON EDUCACION S.A Madrid 2001.

- Buen Master (2007, Mayo) Tipos de Servidores.
  Extraído el 18 de Agosto 2010 desde:
  http://buenmaster.com/?a=298

- Sergio Untiveros, (2004, Julio) Metodología Funcional para la administración de redes.
  Extraído el 11 de Agosto 2010 desde:
  www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

- Pramod Karnad (1997, 7 de Agosto). Linux como servidor de Intranet Extraído el 18 de Agosto 2010 desde:

  http://www.google.com.bo/url?sa=t&source=web&cd=3&ved=0CBwQFjAC&url=http%3A%2F%2Fes.tldp.org%2FCOMO-INSFLUG%2Fes%2Fmini%2Fpdf%2FServidor-Intranet-Como.pdf&rct=j&q=servidores%20linux&ei=AEJsTNiiGIWKlwfoi73AAQ&usg=AFQjCNEtp4973tuVNVcPp6BDDthByk01DA&cad=rja

- Isabel González (2006, 25 de Abril). Comunicación interpersonal. Extraído el de 20 de Abril de 2010 desde http://www.coninpyme.org/pdf/ComunicacioninterpersonalyComunicacioninterpersonal.pdf

- Charles L. Hedrick 27 de Julio de 1999 http://es.tldp.org/Manuales-LuCAS/IAR/intro-admon-redes-v1.1.html

- Sergio Untiveros, Julio 2004 www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

- REAL ACADEMIA ESPAÑOLA (2003) Diccionario de la Real Academia Española. 22.ª EDICIÓN,

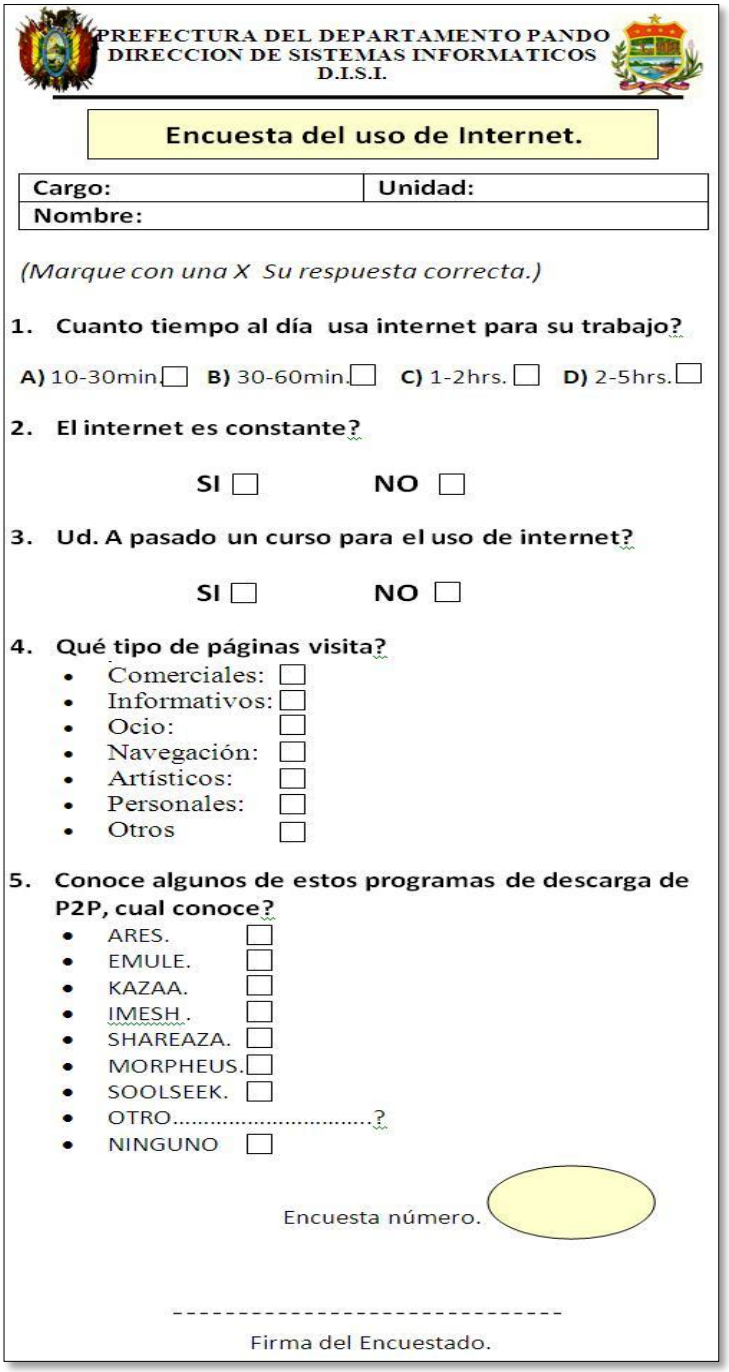
David de Ugarte, El Poder de las Redes, octubre 2007

Anexos

Anexo A

ANEXOS A

DESCRIPCIÓN DEL DIAGNOSTICO Y ANÁLISIS REALIZADO EN BASE A ENCUESTA Y OBSERVACIÓN



PREFECTURA DEL DEPARTAMENTO PANDO
DIRECCION DE SISTEMAS INFORMATICOS
D.I.S.I.

Encuesta del uso de Internet.

Cargo:	Unidad:
Nombre:	

(Marque con una X Su respuesta correcta.)

1. **Cuanto tiempo al día usa internet para su trabajo?**

A) 10-30min. ☐ **B)** 30-60min. ☐ **C)** 1-2hrs. ☐ **D)** 2-5hrs. ☐

2. **El internet es constante?**

SI ☐ **NO** ☐

3. **Ud. A pasado un curso para el uso de internet?**

SI ☐ **NO** ☐

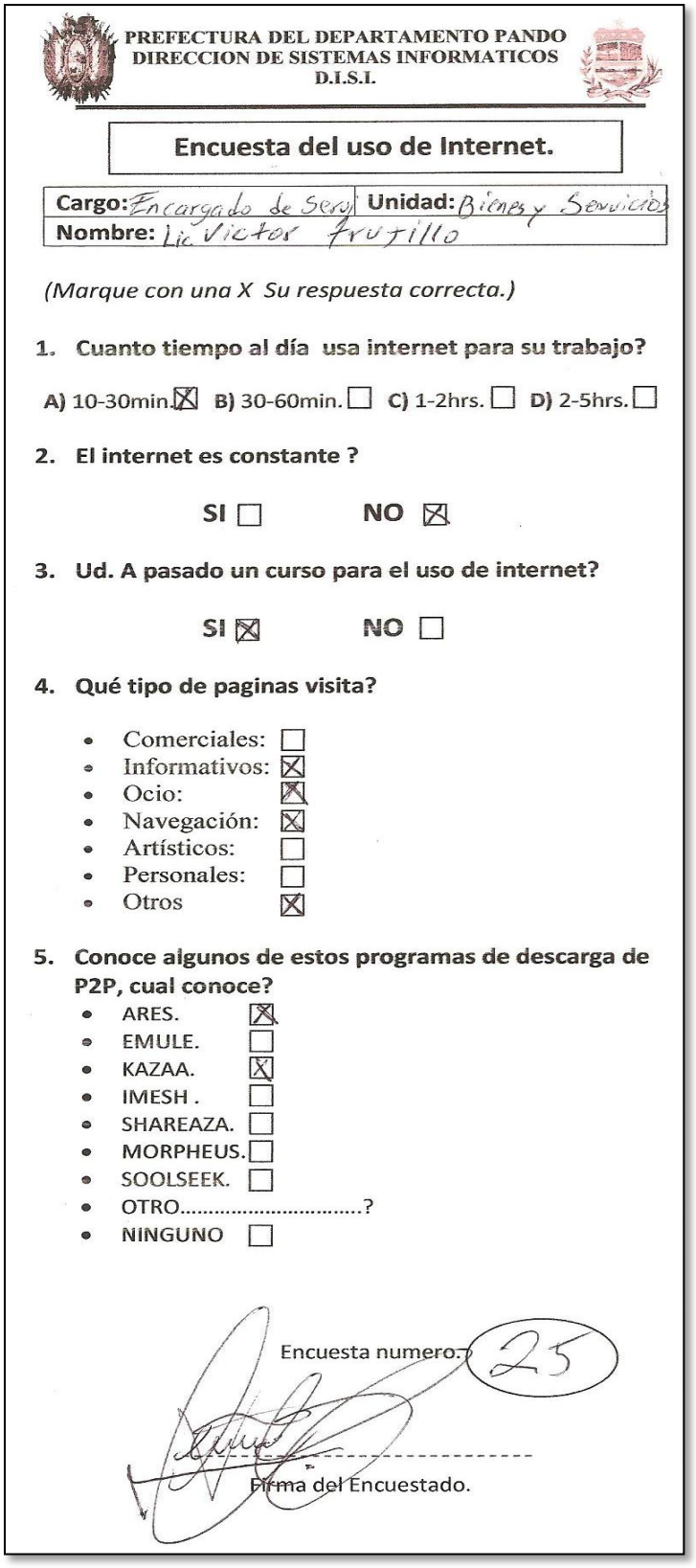
4. **Qué tipo de páginas visita?**
   - Comerciales: ☐
   - Informativos: ☐
   - Ocio: ☐
   - Navegación: ☐
   - Artísticos: ☐
   - Personales: ☐
   - Otros ☐

5. **Conoce algunos de estos programas de descarga de P2P, cual conoce?**
   - ARES. ☐
   - EMULE. ☐
   - KAZAA. ☐
   - IMESH. ☐
   - SHAREAZA. ☐
   - MORPHEUS. ☐
   - SOOLSEEK. ☐
   - OTRO.....?
   - NINGUNO ☐

Encuesta número.

Firma del Encuestado.

Figura 1: *Formato de la encuesta elaborada*
Fuente: *Elaboración Propia*



PREFECTURA DEL DEPARTAMENTO PANDO
DIRECCION DE SISTEMAS INFORMATICOS
D.I.S.I.

Encuesta del uso de Internet.

Cargo: Encargado de Serv	**Unidad:** Bienes y Servicios
Nombre: Lic. Victor Trujillo	

(Marque con una X Su respuesta correcta.)

1. **Cuanto tiempo al día usa internet para su trabajo?**

A) 10-30min. [X] **B)** 30-60min. [ ] **C)** 1-2hrs. [ ] **D)** 2-5hrs. [ ]

2. **El internet es constante ?**

SI [ ] **NO** [X]

3. **Ud. A pasado un curso para el uso de internet?**

SI [X] **NO** [ ]

4. **Qué tipo de paginas visita?**

- Comerciales: [ ]
- Informativos: [X]
- Ocio: [X]
- Navegación: [X]
- Artísticos: [ ]
- Personales: [ ]
- Otros [X]

5. **Conoce algunos de estos programas de descarga de P2P, cual conoce?**

- ARES. [X]
- EMULE. [ ]
- KAZAA. [X]
- IMESH . [ ]
- SHAREAZA. [ ]
- MORPHEUS. [ ]
- SOOLSEEK. [ ]
- OTRO.....?
- NINGUNO [ ]

Encuesta numero: 25

Firma del Encuestado.

Figura 2: *Encuesta Llenada Nº 25*
Fuente: *Elaboración Propia*

ESTADISTICAS DEL USO DE INTERNET

1. Cuanto tiempo al día usa internet para su trabajo?

A) 10-30min	**22**
B) 30-60min	**12**
C) 1-2hrs.	**7**
D) 2-5hrs.	**8**

2. El internet es constante ?

SI	**9**
NO	**40**

3. Ud. A pasado un curso para el uso de internet?

SI	**34**
NO	**15**

4. Qué tipo de paginas visita?

Comerciales:	**7**
Informativos:	**35**
Ocio:	**0**
Navegación:	**7**
Artísticos:	**1**
Personales:	**7**
Otros	**28**

5. Conoce algunos de estos programas de descarga de P2P, cual conoce?

ARES.	**10**
EMULE.	**9**
KAZAA	**6**
IMESH .	**2**
SHAREAZA	**1**
MORPHEUS.	**0**
SOOLSEEK.	**0**
OTRO..?	**1**
NINGUNO	**38**

Numero de De Encuestas Realizadas

TOTAL DE PERSONAS QUE USAN INTERNET	***93***	***100%***
TOTAL DE PERSONAS ENCUESTADAS	***49***	***52%***

Figura 3: *Tabla de resultado cuantitativo de encuestas realizadas*
Fuente: *Elaboración Propia*

RESULTADOS DE LA ENCUESTA SOBRE EL USO DE INTERNET EN LA PREFECTURA DE PANDO

Pregunta 1: Cuanto tiempo al día usa internet para su trabajo?

Ya que la pregunta fue directa a todas las personas que tienen internet, según la encuesta el promedio de uso diario por persona que tiene internet es 1:15 min. Diarios.

Figura 4: *Torta grafica de pregunta 1*

Fuente: *Elaboración Propia*

Pregunta 2: El internet es constante?

El 18% de las personas dijeron que el internet **Si** es constante, pero 82% dijeron que **NO** es constante. En síntesis el servicio que se tiene de internet no es constate se para cortando o la señal llega entre cortada.

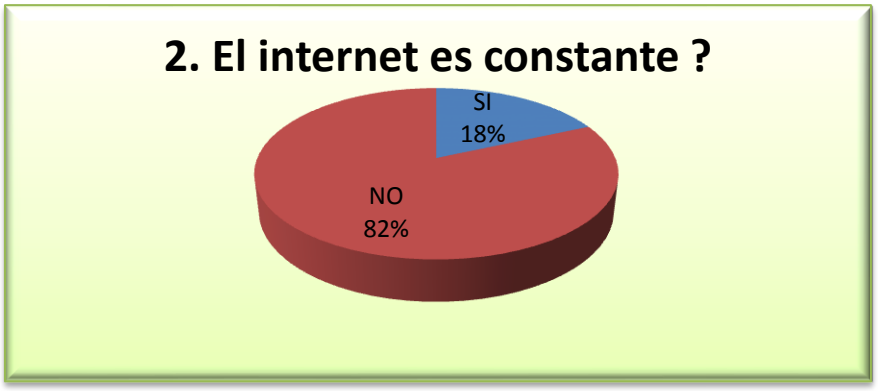


Figura 5: *Torta grafica de pregunta 2*
Fuente: *Elaboración Propia*

Pregunta 3: Ud. A pasado un curso para el uso de internet?

El 69% respondió que sí tuvo un curso del uso de internet y el 39% que no paso ningún curso pero que tiene conocimientos del uso básico del internet.

Figura 6: *Torta grafica de pregunta 3*

Fuente: *Elaboración Propia*

Pregunta 4: Qué tipo de paginas visita?

La mayoría de los Usuarias el 41% visitas páginas informativas, 33% respondieron otro Ej.: SICOES, SISIN, PAGINAS JURIDICAS, etc. El 8% páginas personales y navegación, por lo que se observo que las visitas a sitios web son mas de información.

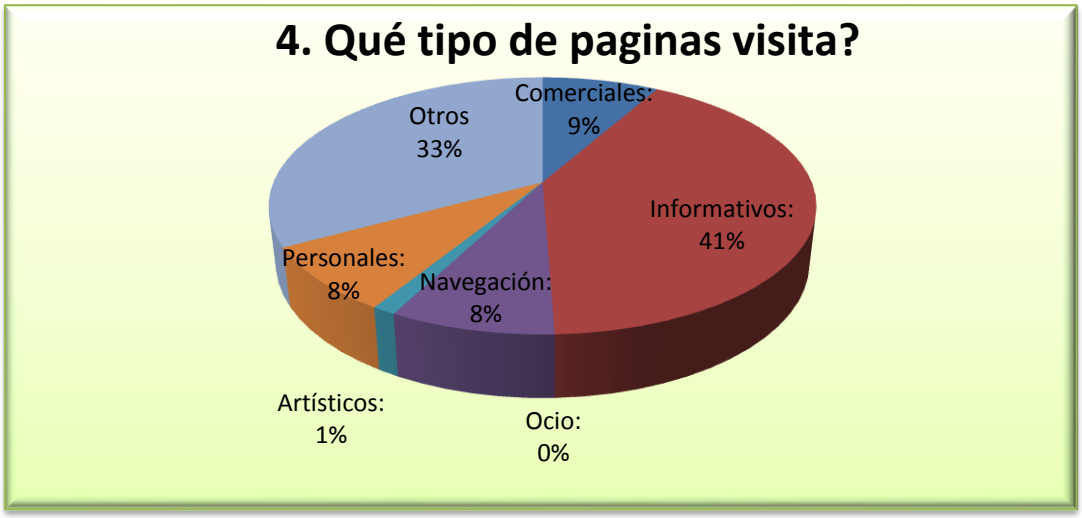


Figura 7: *Torta grafica de pregunta 4*

Fuente: *Elaboración Propia*

Pregunta 5: Conoce algunos de estos programas de descarga de P2P, cual conoce?

Ya que los programas como ares, emule, kazaa, imesh, shareaza, morpheus, soolseek y otros son programas de dicados para descargas de archivos, como video música imágenes, en la que 57% respondió que no conocen, pero 43% que si conoce, por lo tanto se tiene que el 43% de las personas están actas a usar los programas P2P o de descargas de archivos.

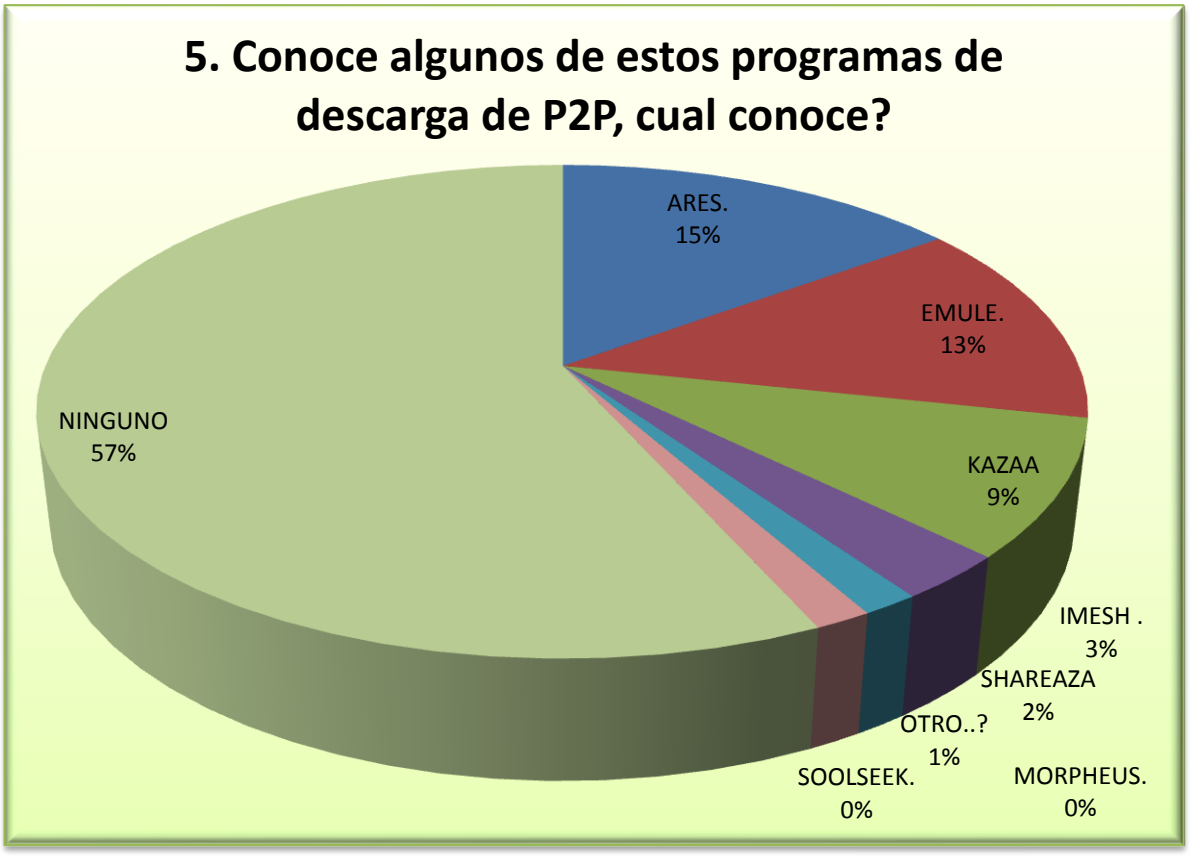


Figura 8: *Torta grafica de pregunta 5*

Fuente: *Elaboración Propia*

Anexo B

ANEXOS B

PLANEACIÓN Y DISEÑO DE LA RED DE DATOS DE LA PREFECTURA DE PANDO VÍA ESQUEMAS Y PLANO A ESCALA PERIMETRAL.

En este anexo B se detalla los diseños realizados para la implementación del servidor, tomando en cuenta también la figura 1 en la que es el esquema de la red antigua, se observa el cambio y el crecimiento de usuarios, como también la unión de los ADSL. Para así tener una mejor administración de todo el entorno de la red, ya que es una realidad la implementación del servidor ay que tomar en cuenta las modificaciones de la red, que de uno u otro motivo cambia de acuerdo a la movilidad de los usuarios y usabilidad.

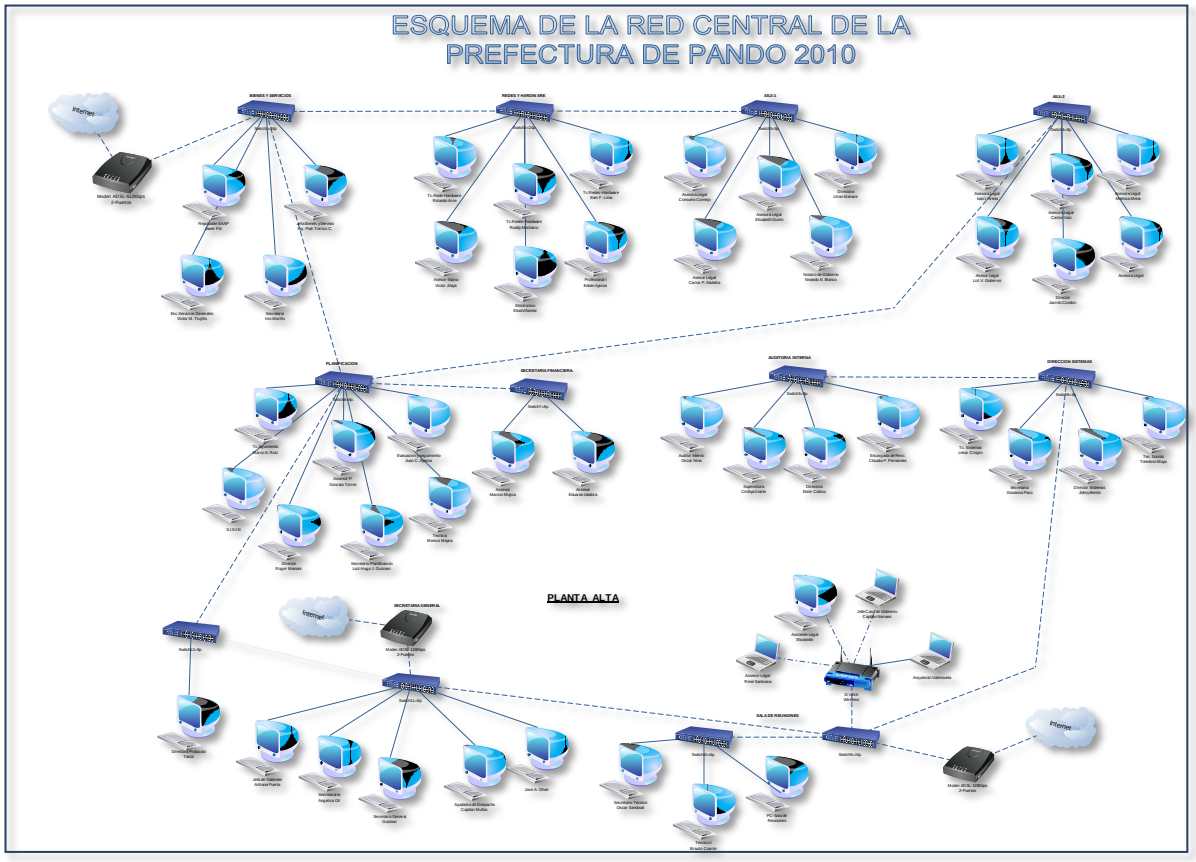


Figura 1: *Esquema de red de datos Prefectural Antigua*
Fuente: *Elaboración Propia.*

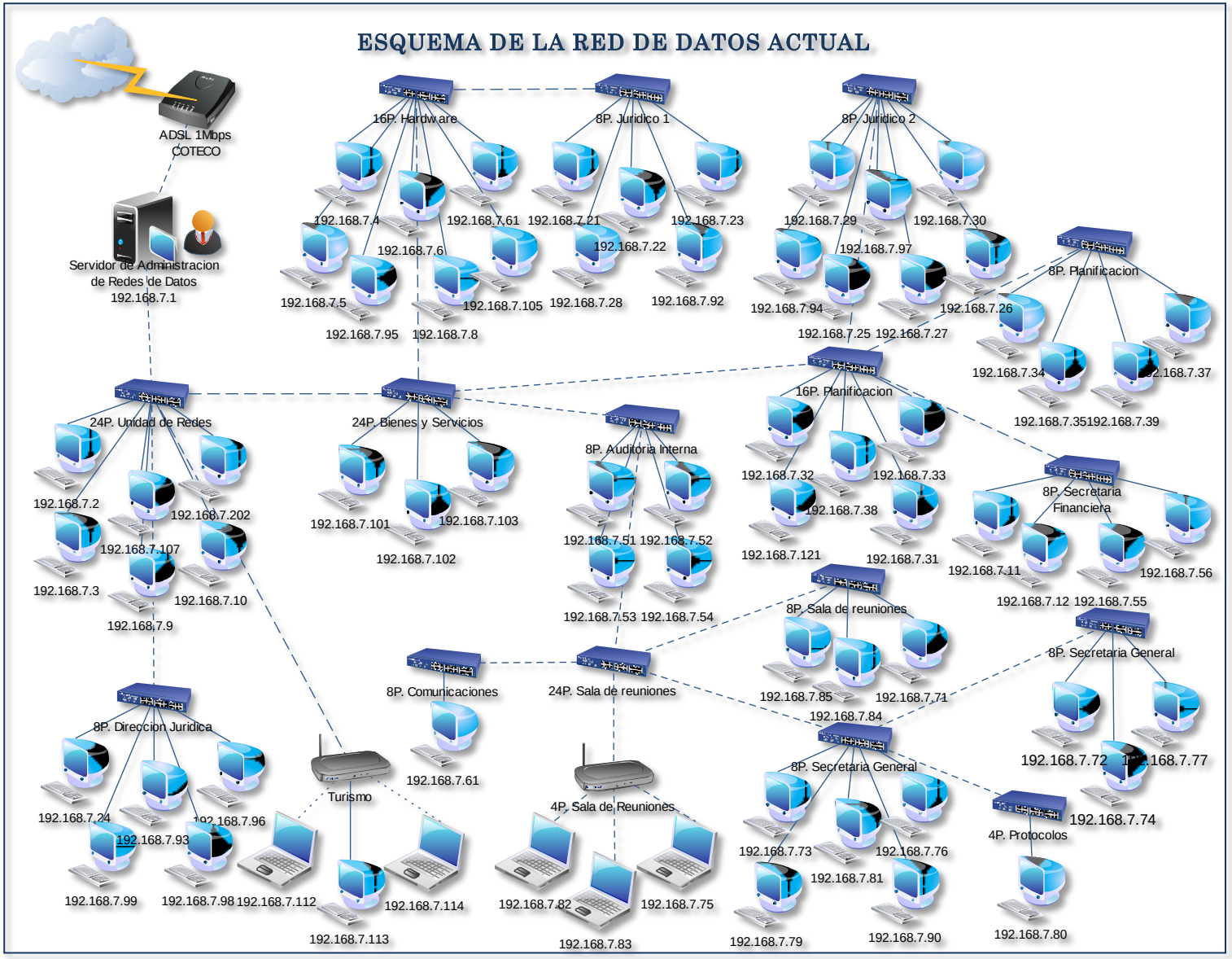


Figura 2: *Esquema de red de datos Prefectural Actual*

Fuente: *Elaboración Propia*

Figura 3: *Plano Informativo de la planta baja*
Fuente: *Elaboración Propia.*

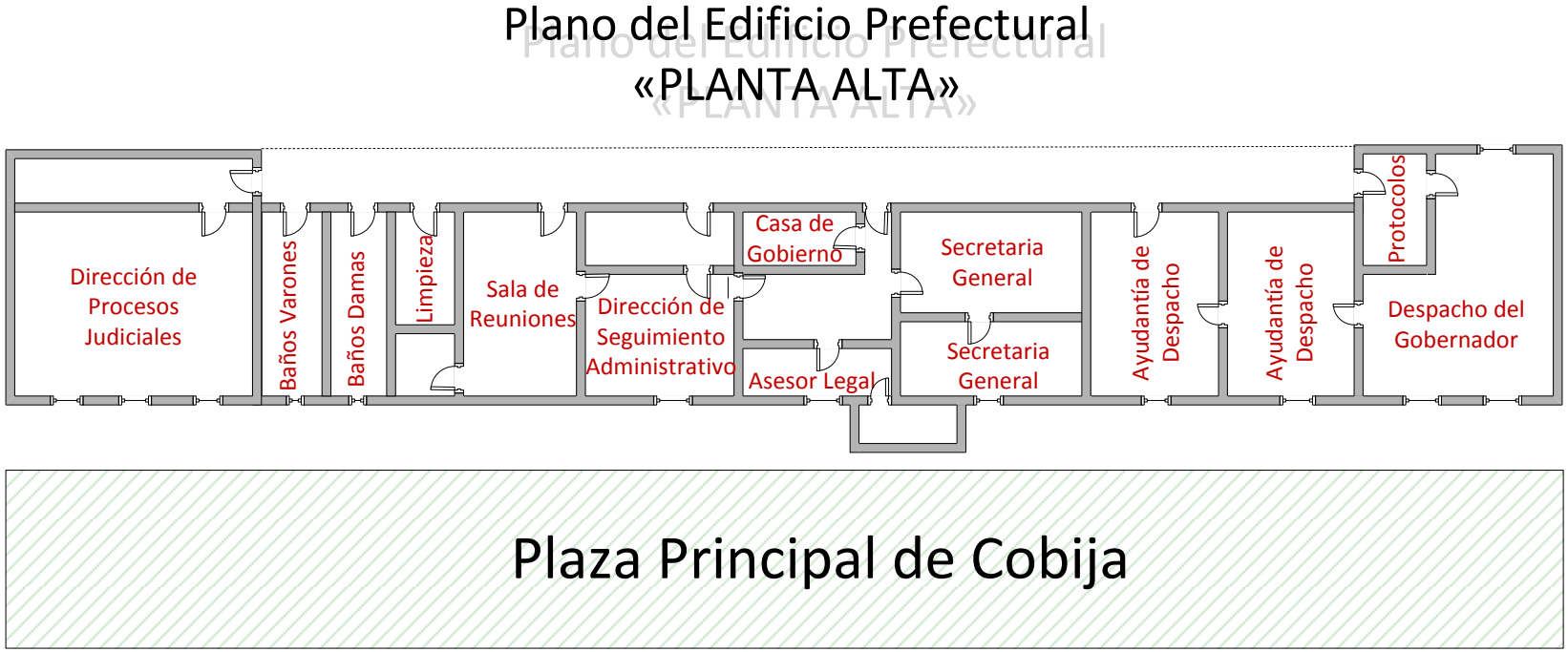


Figura 4: *Plano Informativo de la planta alta*
Fuente: *Elaboración Propia.*

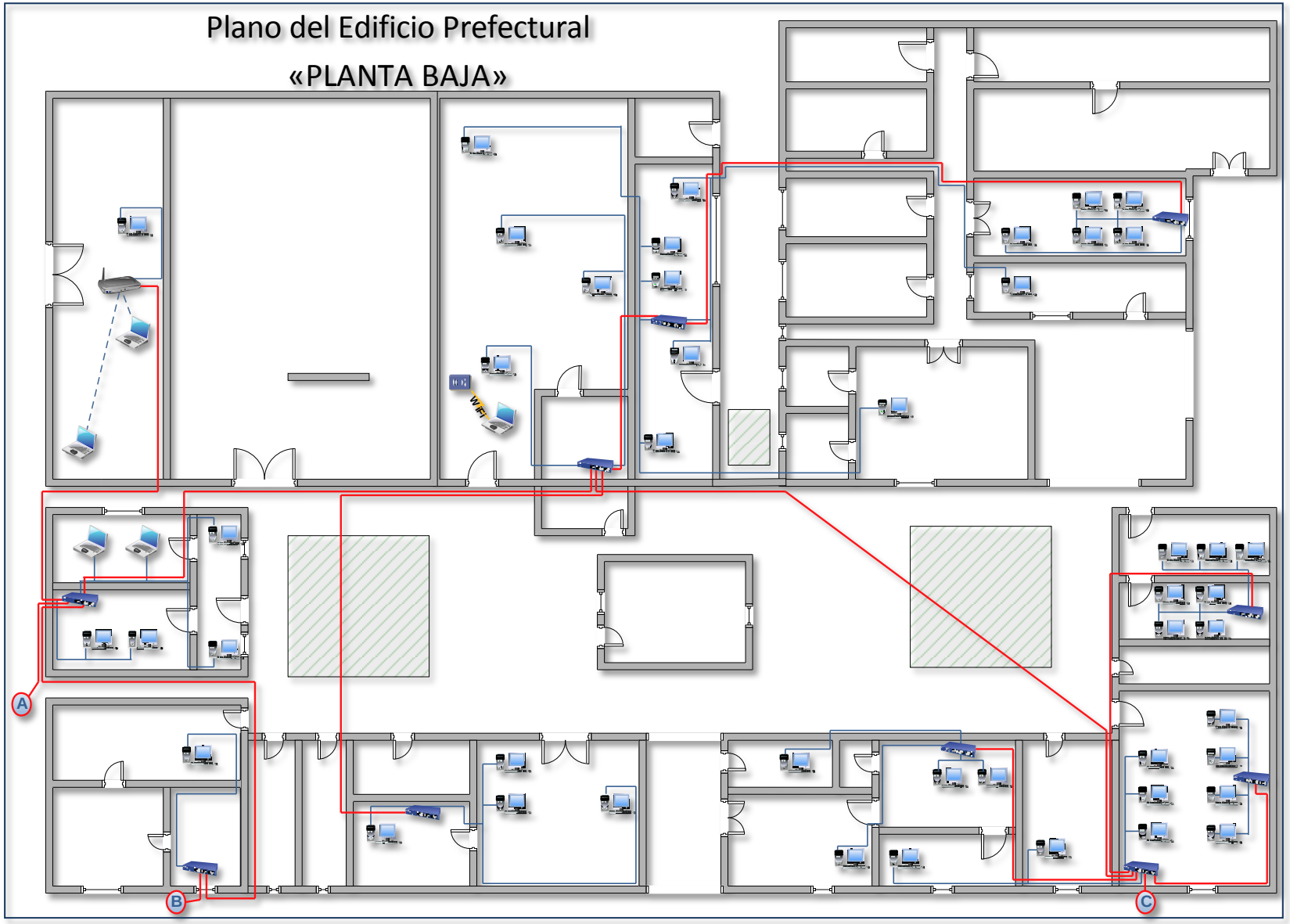


Figura 5: *Plano Del cableado Estructurado planta baja*
Fuente: *Elaboración Propia*

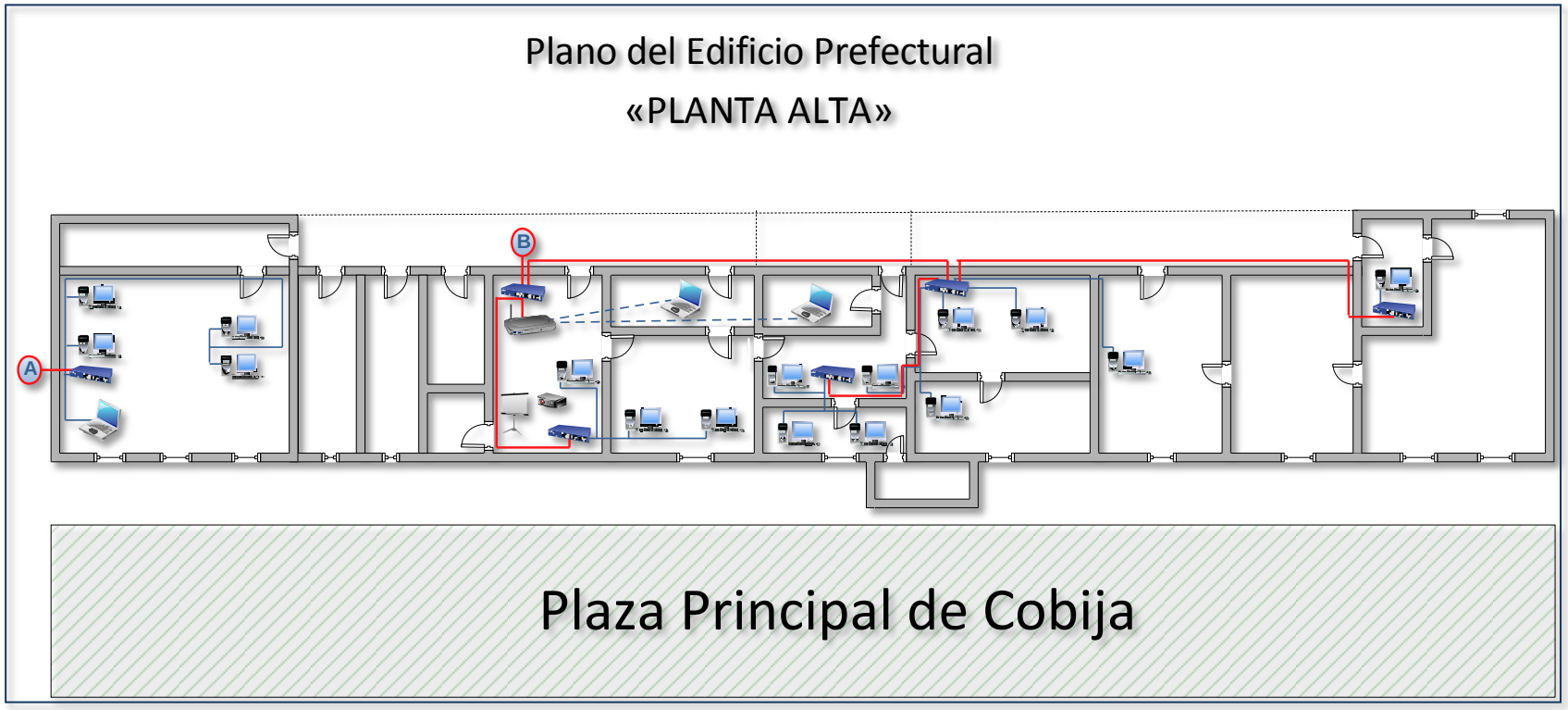


Figura 6: *Plano del cableado estructurado planta alta*
Fuente: *Elaboración Propia.*

Anexo C

ANEXOS C

INSTALACIONES Y ADMINISTRACIÓN HARDWARE, EN BASE A FOTOGRAFÍAS.

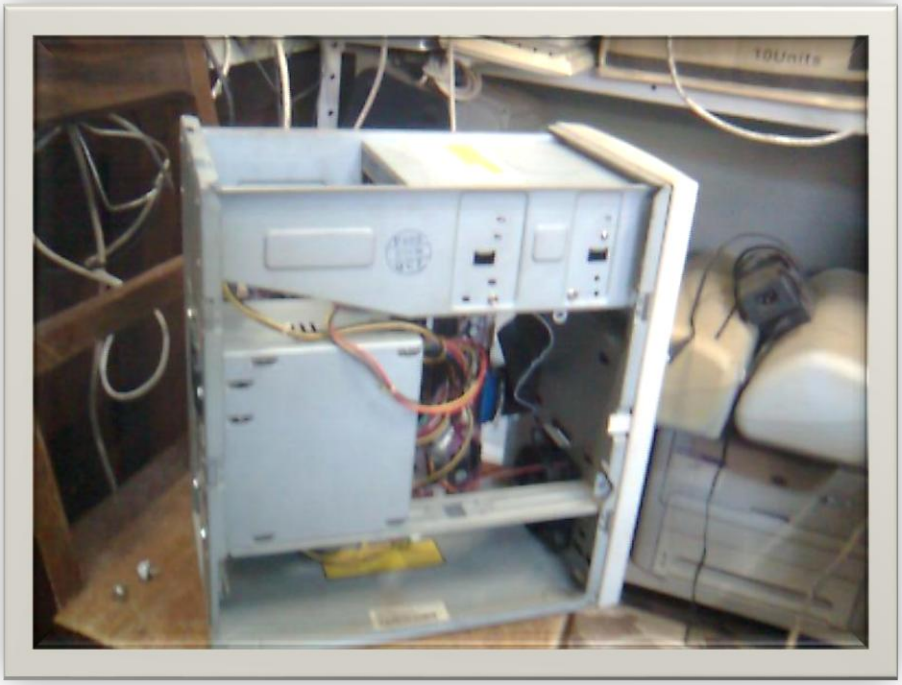


Figura 1: *Fotografía del Armado del Servidor*
Fuente: *Elaboración Propia.*

Figura 2: *Fotografía de los Switch Central Ubicado en la Unidad de Redes*
Fuente: *Elaboración Propia.*

Figura 3: *Fotografía de ejemplo que los Switch están empotrado en la pared*
Fuente: *Elaboración Propia.*

Luego de a ver tenido los diseños de la red, el traslado y instalación de dispositivos se instala el servidor de administración de red de datos, en la unidad de redes así conectado a un UPS, para evitar futuros cortes ya que este servidor será el que reparta el internet a todo el predio central de la Prefectura de Pando.

Figura 4: *Fotografía del servidor en funcionamiento diario*
Fuente: *Elaboración Propia.*

Anexo D

ANEXOS D

INSTALACIONES Y ADMINISTRACIÓN DEL SOFTWARE, EN BASE A CAPTURAS DE PANTALLA.

Descarga de la .iso de la versión 3.0 e Instalación/Update de la Build-Tree de 3.0

Descargar de la .iso de BrazilFW 3.0:

http://brazilfw.com.br/users/woshman/bt/brazilfw.iso

Build-tree de BrazilFW 3.0:

build-tree {install/update}

Code: Select all

get-pkg /users/woshman/build-tree

Iniciar desde CD.

El CD de BrazilFW 3.0 trae los siguientes ítems:

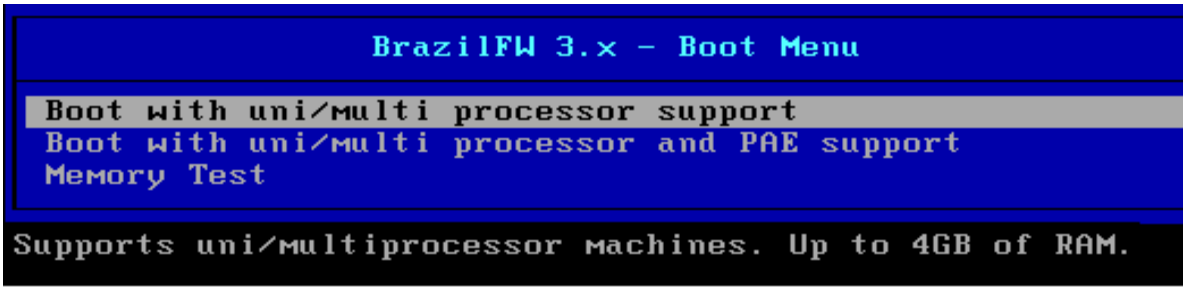
Boot Menú con 2 kernels ambos con soporte para Multiprocesador:

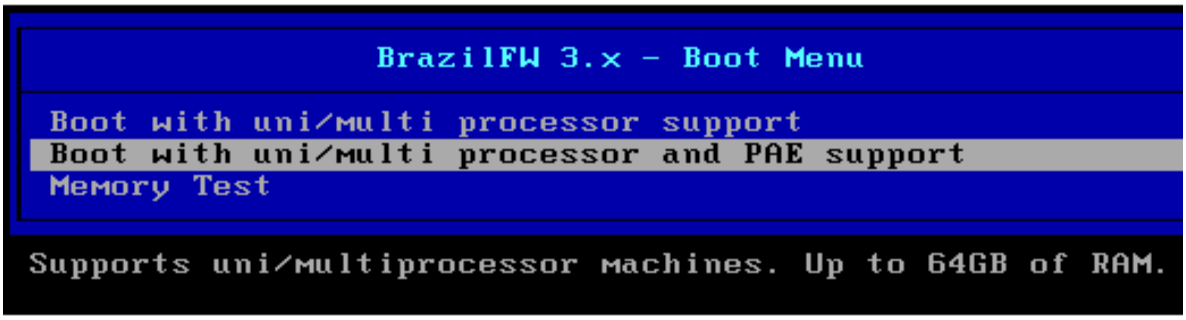
1. El primero es para máquinas que posean hasta 4 GB de memoria RAM.
2. El segundo es para máquinas que posean hasta 64 GB de memoria RAM.
   - En caso de tener un solo procesador, el propio sistema se encargará de hacer los ajustes necesarios.
3. Test de memoria.
   - En esta opción tiene la posibilidad de hacer un test de la Memoria RAM de Server.

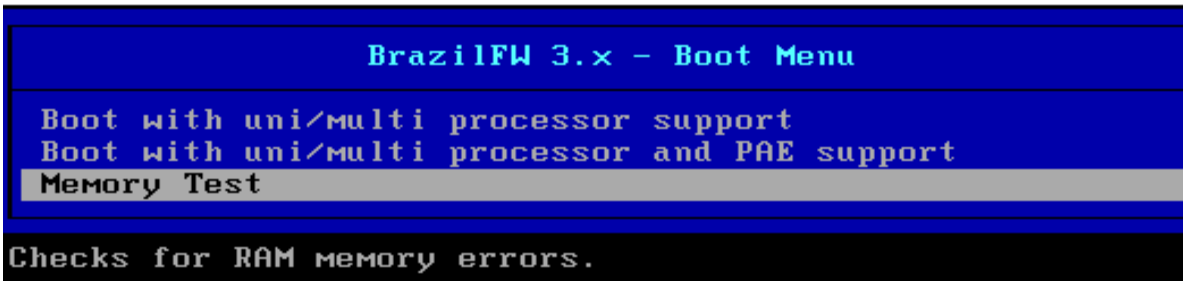
Iniciar desde CD:

Pantalla del Boot Menú poco después de iniciar.

- El Timer es de 15 segundos. Si no selecciona una opción el instalador ingresará de manera automática a la primera opción.





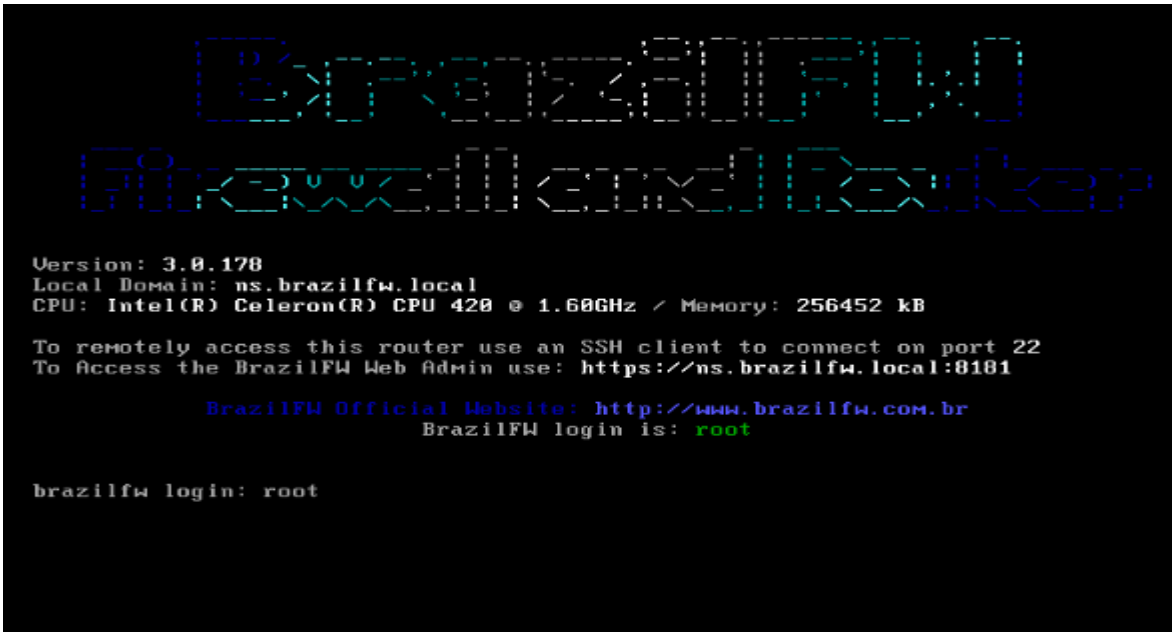


Después de optar por la primera o la segunda opción tendremos la siguiente pantalla:

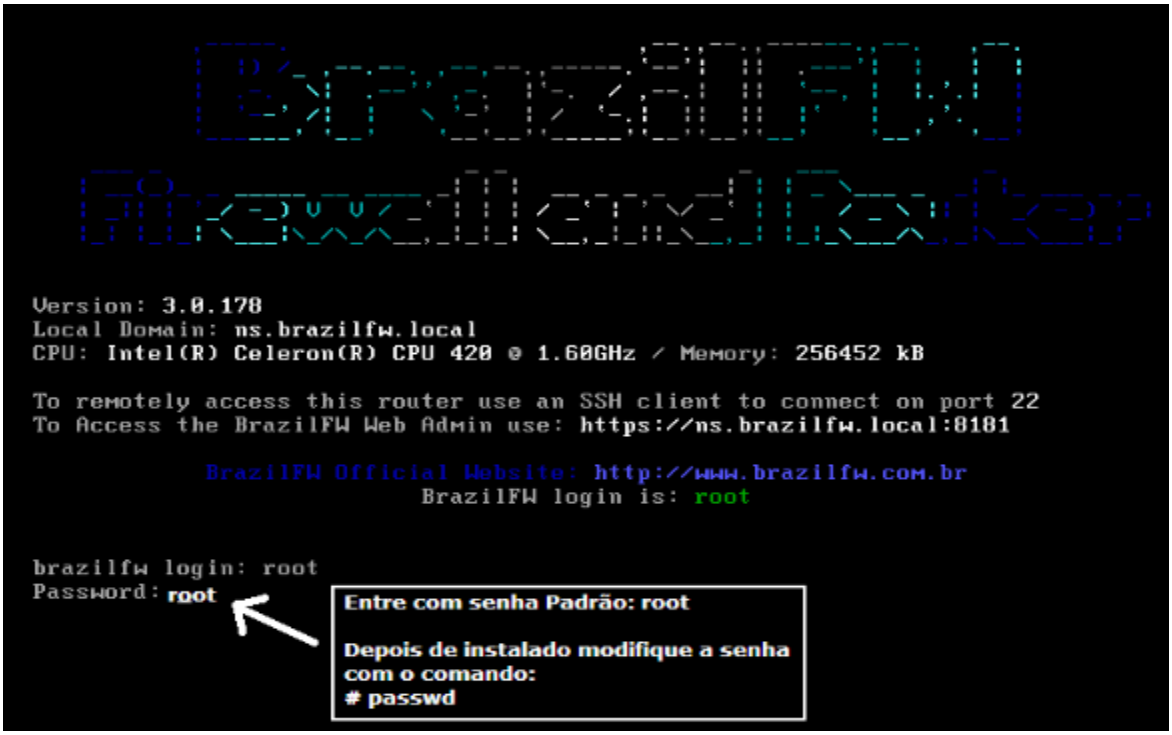
Instalación de BFW 3.0 en un "Disco" de Gran Capacidad:

El instalador crea la primera partición con 100 MB y coloca el espacio restante del HD en la segunda Partición. Para Instalar siga estos pasos:

Ingrese como: # root ==> Enter

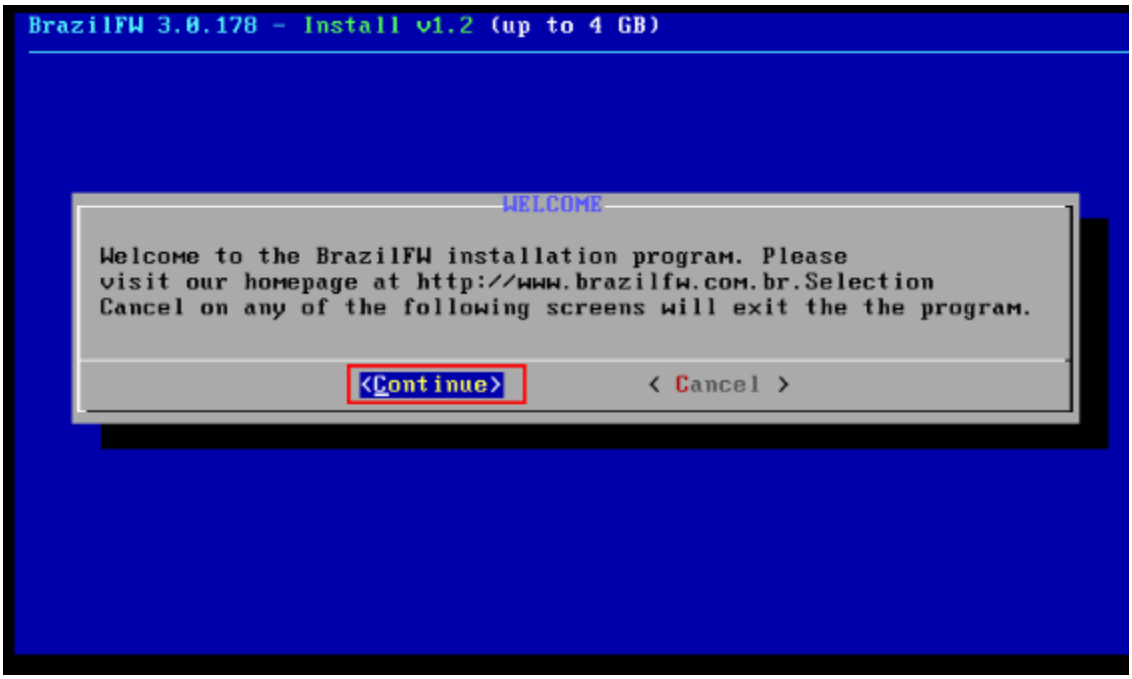


Ingrese con la contraseña predeterminada: # root ==> Enter

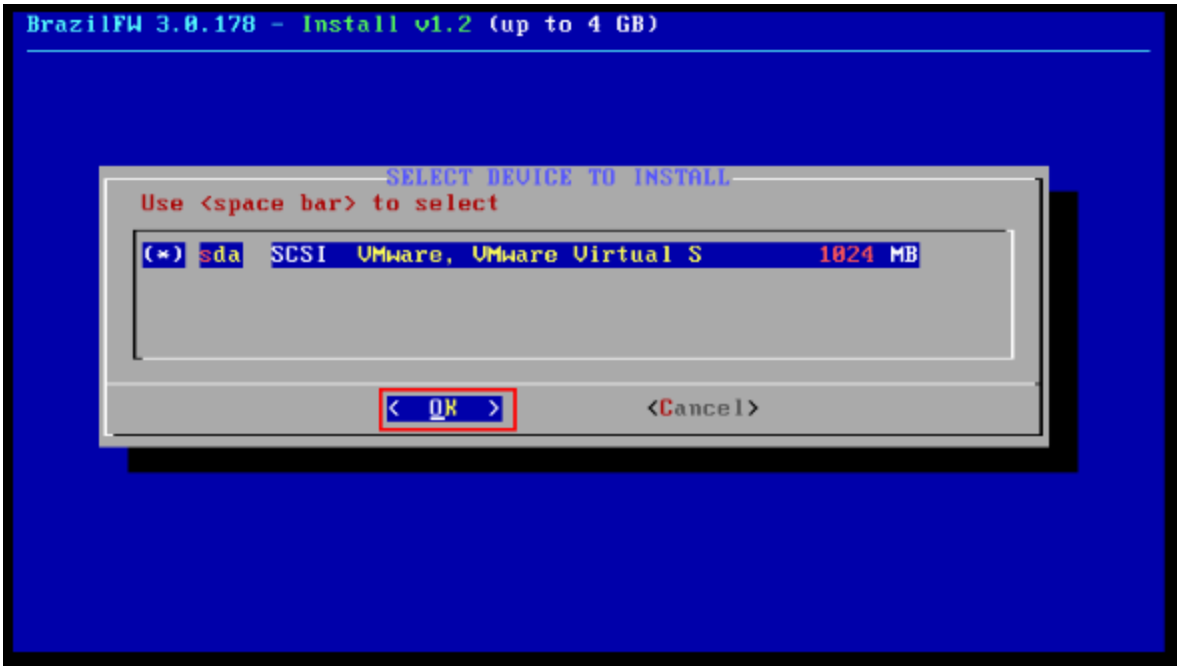


Entre com: # Instalar ==> Enter

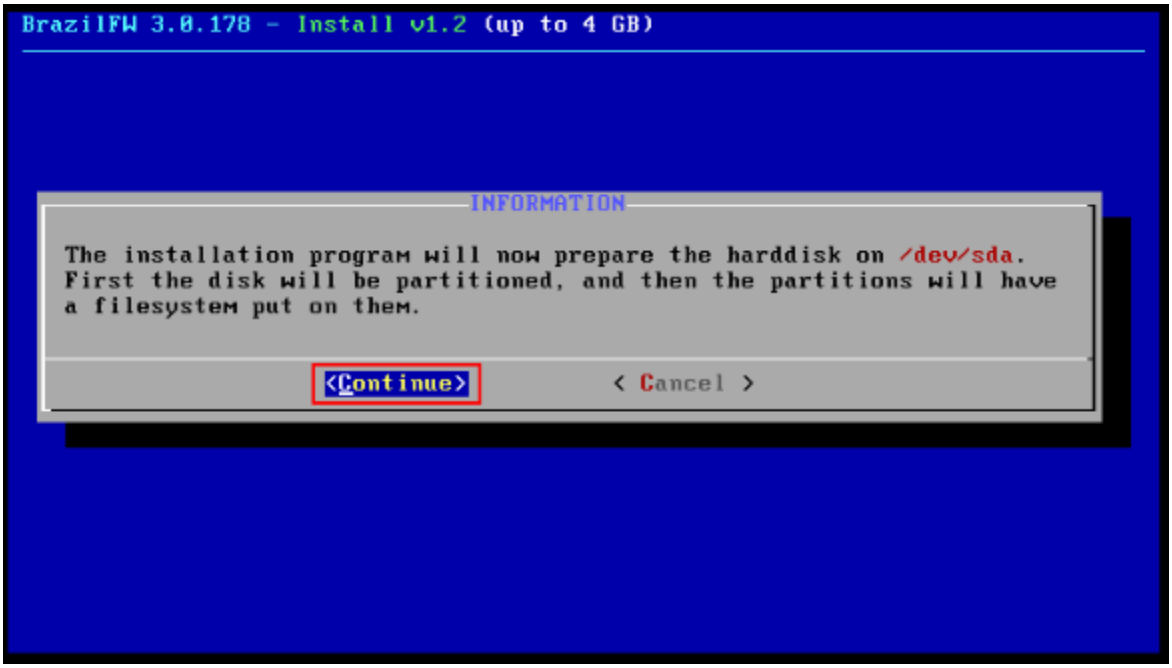
Ahora siga estos pasos



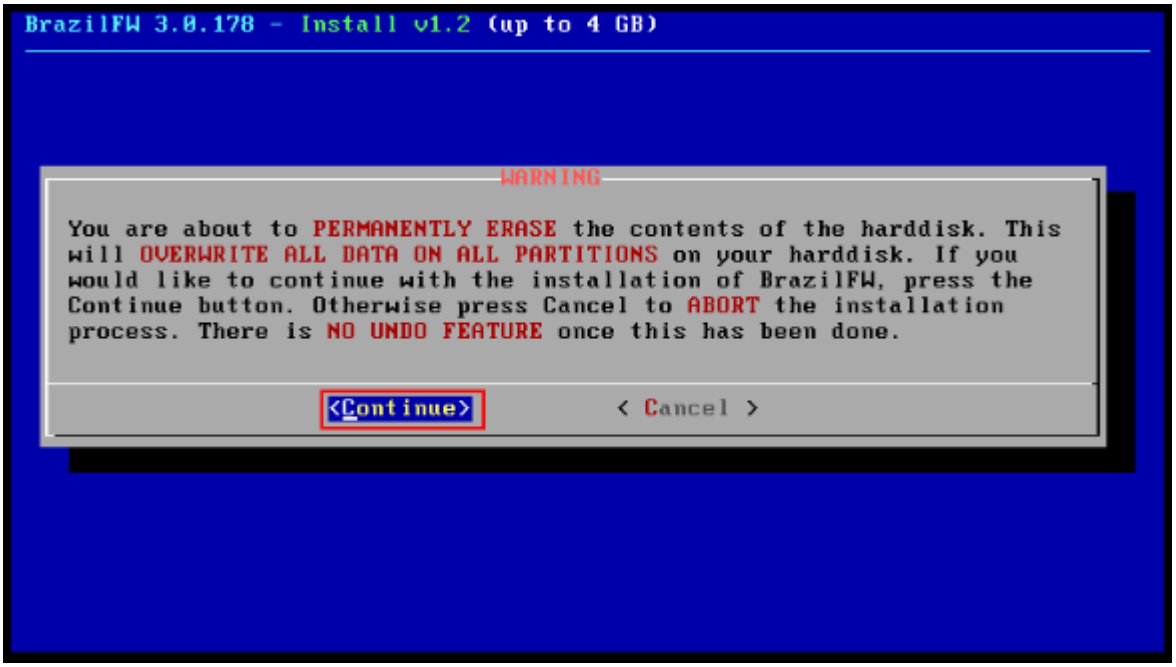
Luego detecta la unida y presionar OK



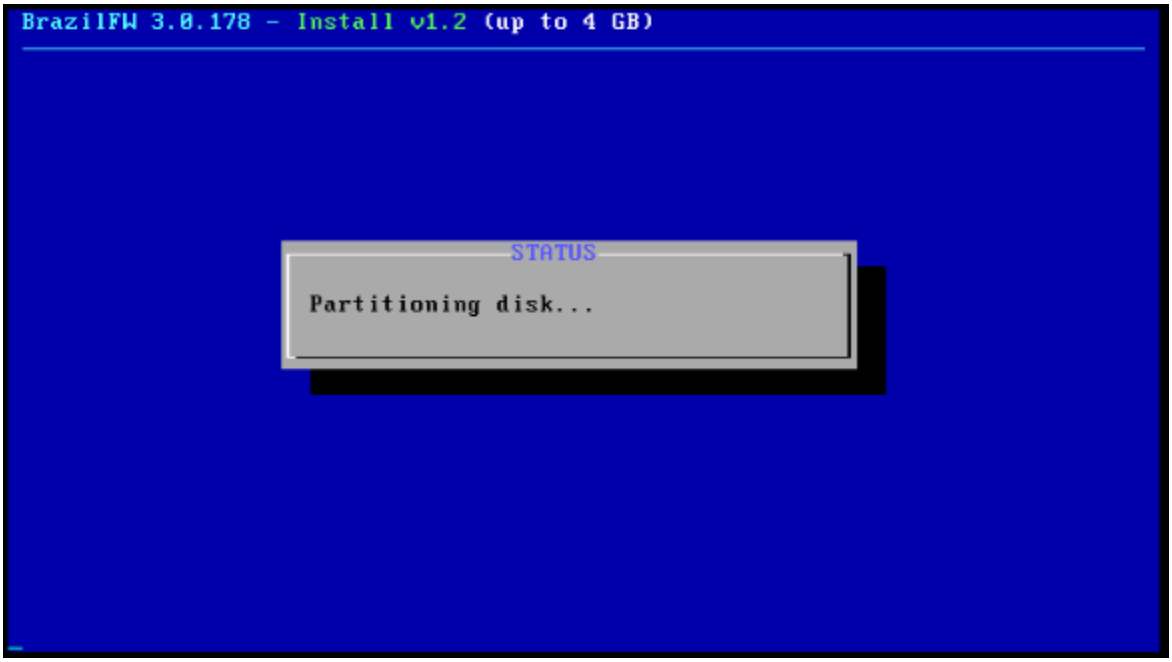
Presionar Continúe:



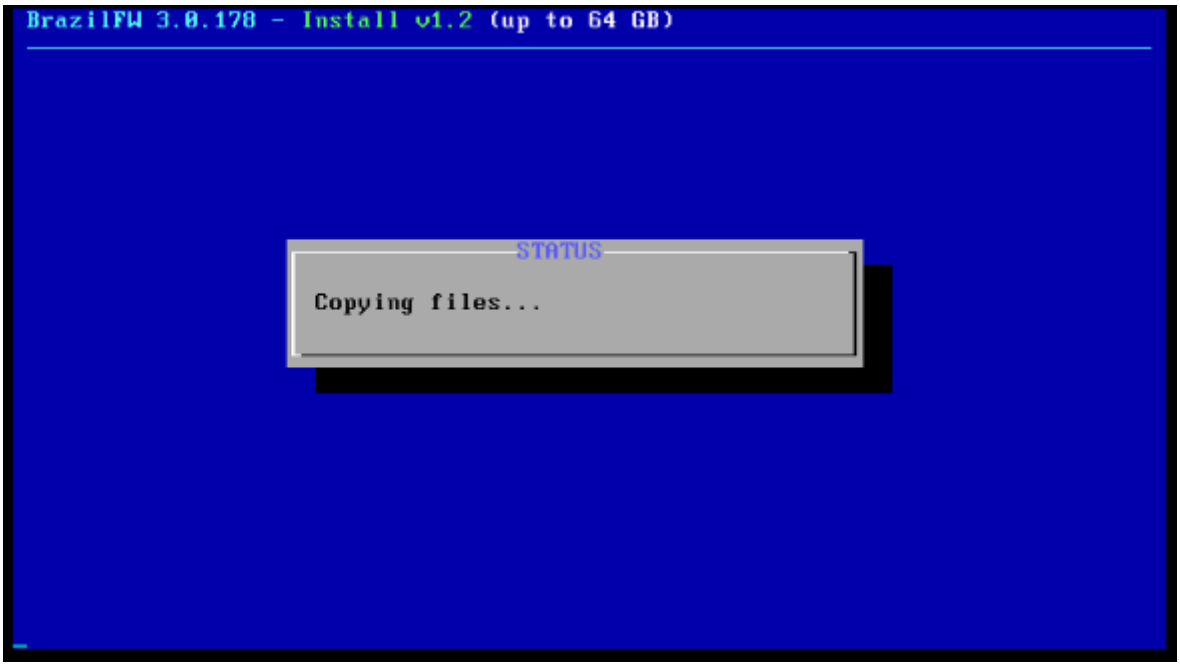
Presionar Continúe:



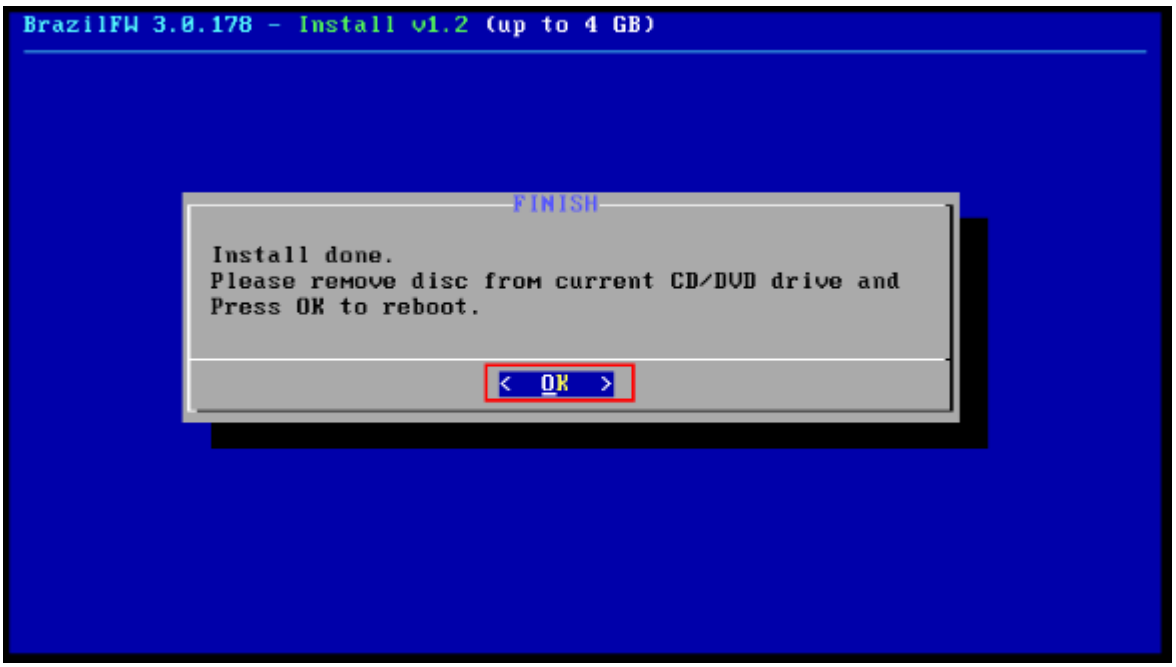
Esperar un par de minutos por que en esta ensena particional el disco duro de forma predeterminada:

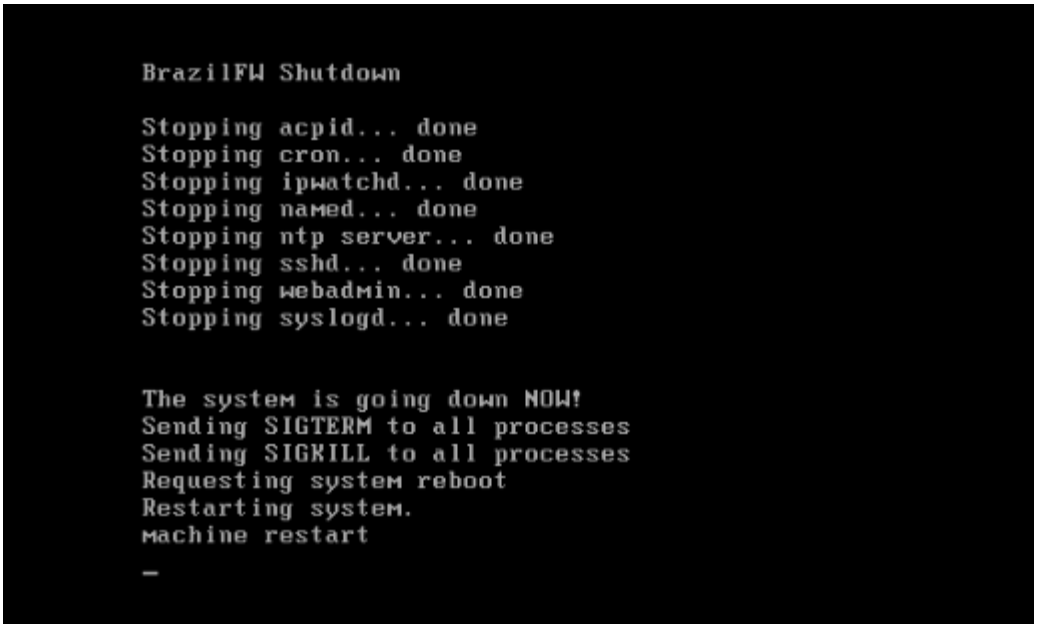


Copiando archivos de programas:



Y finalizo la instalación presione OK:





Después de terminar, haga clic en OK y el server será reiniciado. Deje que el computador bootee desde el HD.

No olvide retirar el CD, ya que incluso dando arranque desde el HD, si el CD se encuentra Todavía en la unidad de CD esto puede generar problema

Anexo E

ANEXOS E

MANUAL DE USUARIO DEL SERVIDOR DE ADMINISTRACIÓN DE RED DE DATOS.

Es un software que nos brinda una interfaz grafica, de los servicios y funciones que se requieren para la administración de de la red de datos, el cual este manual de tallara de una manera práctica y resumida los procesos más importantes del manejo de dicho servidor, bajo pantallas capturadas.

1. ACCEDIENDO AL ENTORNO WEB DEL SERVIDOR BFW3

Una de las primeras instancia es seleccionar un navegador web el BFW soporta la mayoría de los navegadores ya se Firefox, Opera, Safari, etc. En este caso usaremos como navegador predeterminado el Opera, primeramente debemos colocar la dirección en el navegador en este caso es, **https://ns.scainet.sis:8181/** es te dominio esta bajo seguridad de sitios cifrados o certificados digitales ver. (Figura 1).

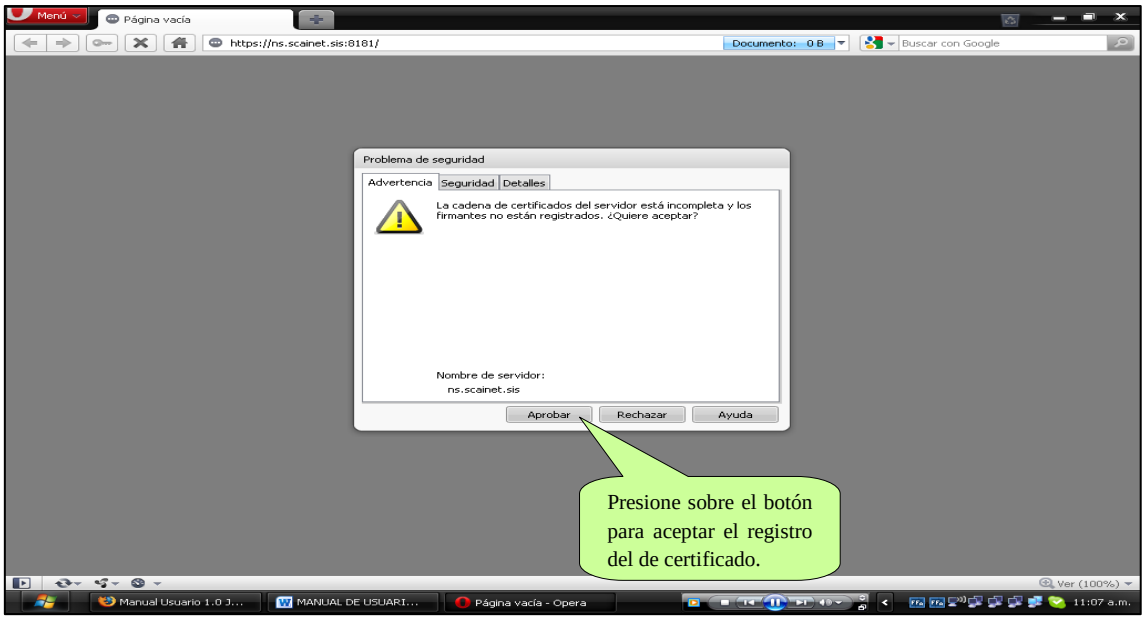


Figura 1.

1.2 Ingresando al servidor BFW: En esta instancia se debe ingresar el nombre de usuario y la contraseña para poder ingresar al sitio web ver. (Figura 2)

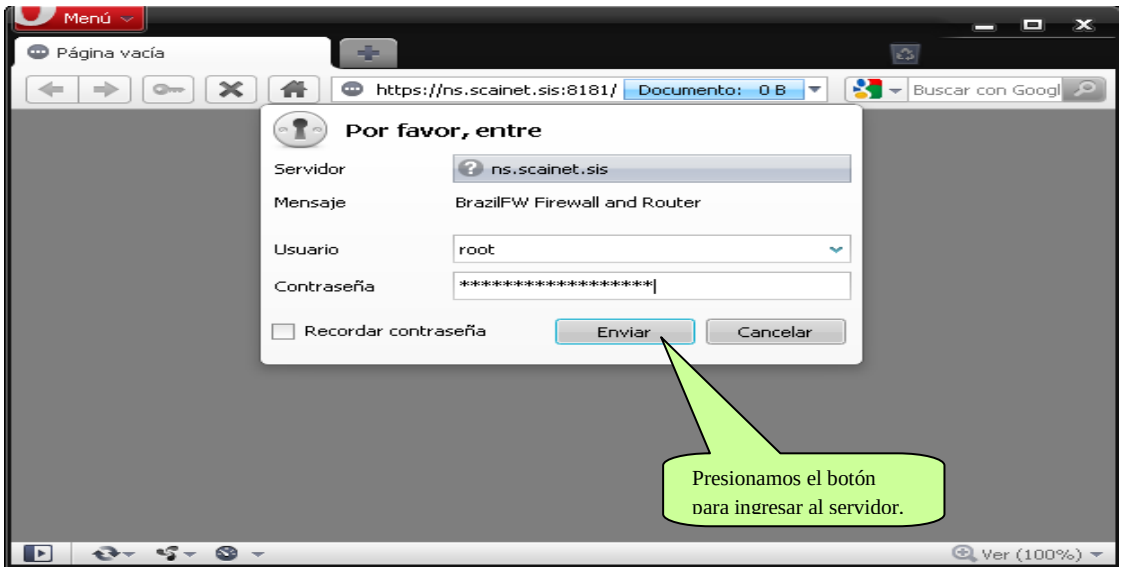


Figura 2.

1.3 Página principal del servidorBFW3: Una vez ingresado al servidor observamos su entorno gráfico y se cuenta con los menús desplegables de cada servicio como de funciones, también se tiene un botón de actualización del servidor ver (Figura 3).

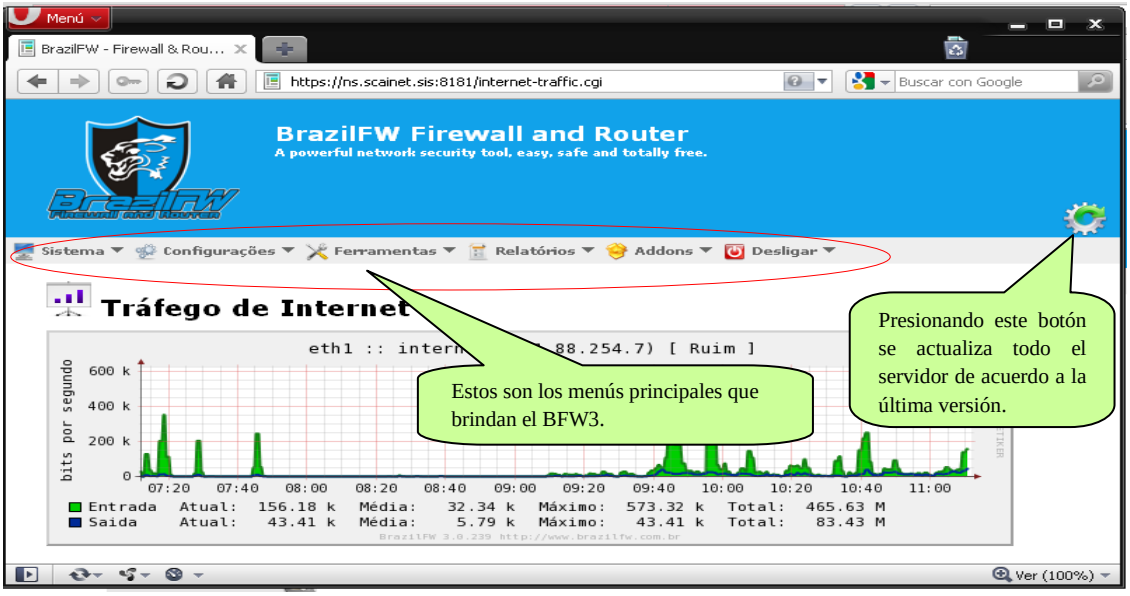


Figura 3.

2. EL MENÚ SISTEMAS

Dentro del menú sistema comprende 1 opción y 3 submenús, en este menú es más de información del sistema como monitoreo de la red ver (Figura 4).

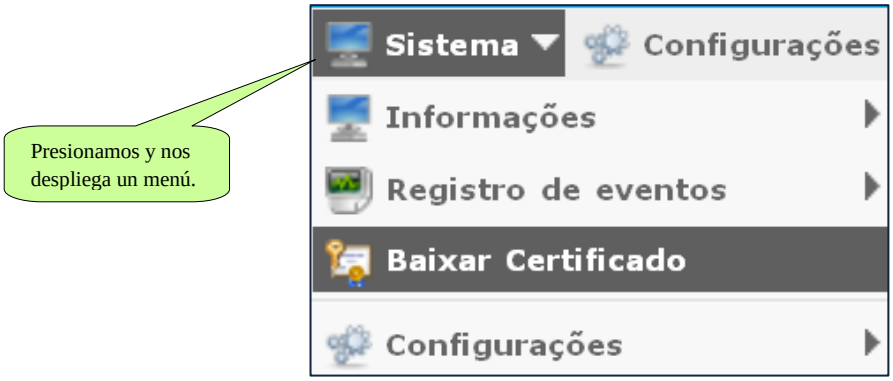


Figura 4.

2.1. Sub-Menú Informaciones: Se divide en dos partes la de información del sistemas y monitoreo del tráfico de internet Ver (Figura 5).

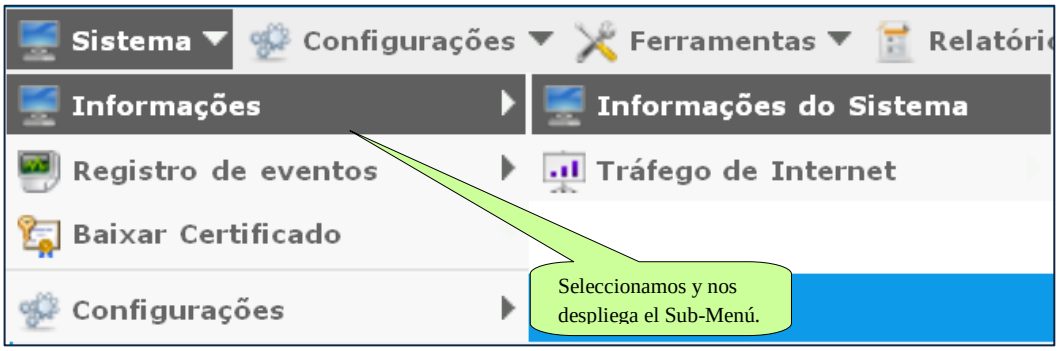


Figura 5.

A continuación mostramos las dos opciones que nos proporciona-el sub-menú Informaciones Ver (Figura 6).

2.1.1. Opción Información de Sistemas: Esta opción es de gran utilidad ya que nos muestra un resumen del estado del sistema tanto el hardware como el software, así podemos saber, la situación que se encuentra nuestro equipo servidor Ver (Figura 6).

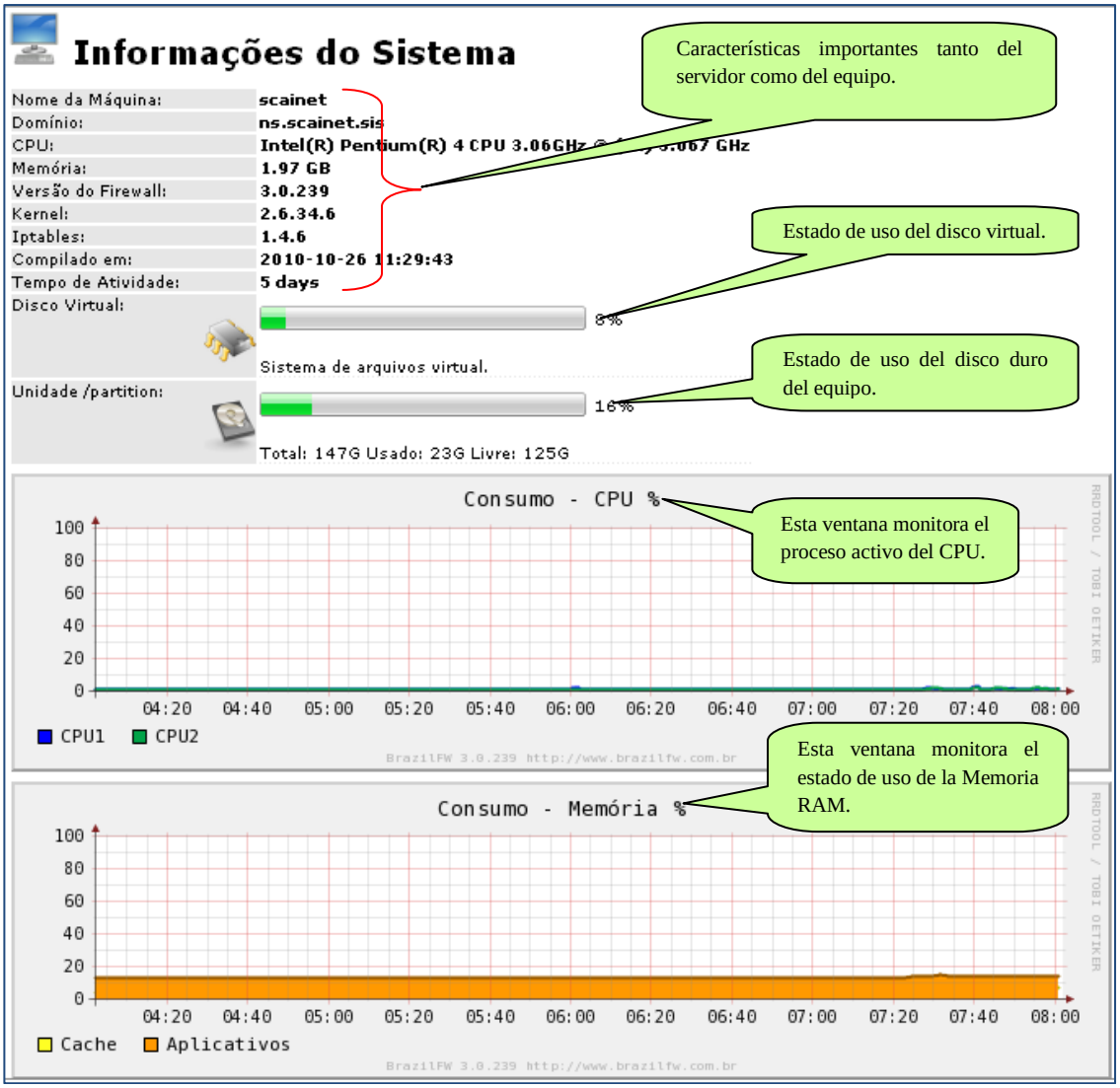


Figura 6.

2.1.2. Opción Tráfico de Internet: Nos muestra el tráfico de internet bajo eth0.

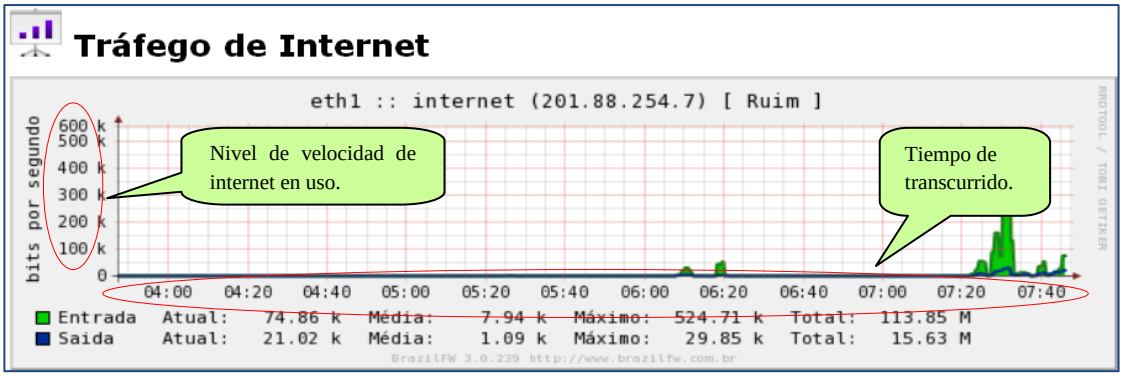


Figura 7.

2.2. Sub-Menú Registro De Eventos: Esta opción nos proporciona los registros adquiridos de los eventos en el sistema, como del kernel, aplicaciones e internet ver (Figura 8).

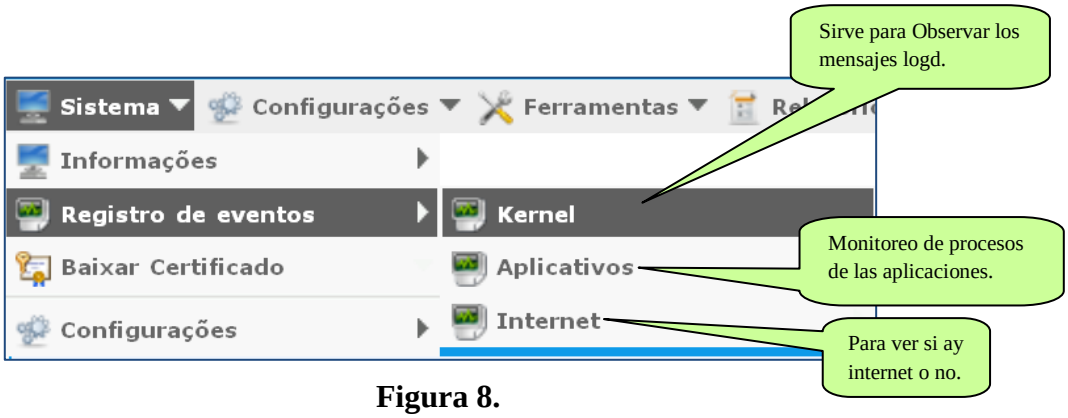


Figura 8.

2.3. Bajar Certificado: Esta opción es únicamente para bajar el certificado digital de seguridad, para la exploración del servidor vía Web ver (Figura 9).

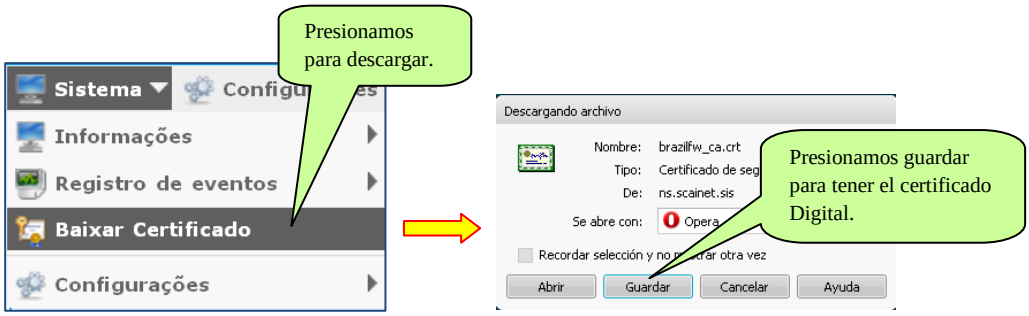


Figura 9.

2.4. Sub-Menú Configuraciones: Esta opción nos permite hacer un Backup de toda la configuración del servidor y guardarlos, como también podemos recuperarlos, comprende de dos opciones de descarga y de subida ver (Figura 10).

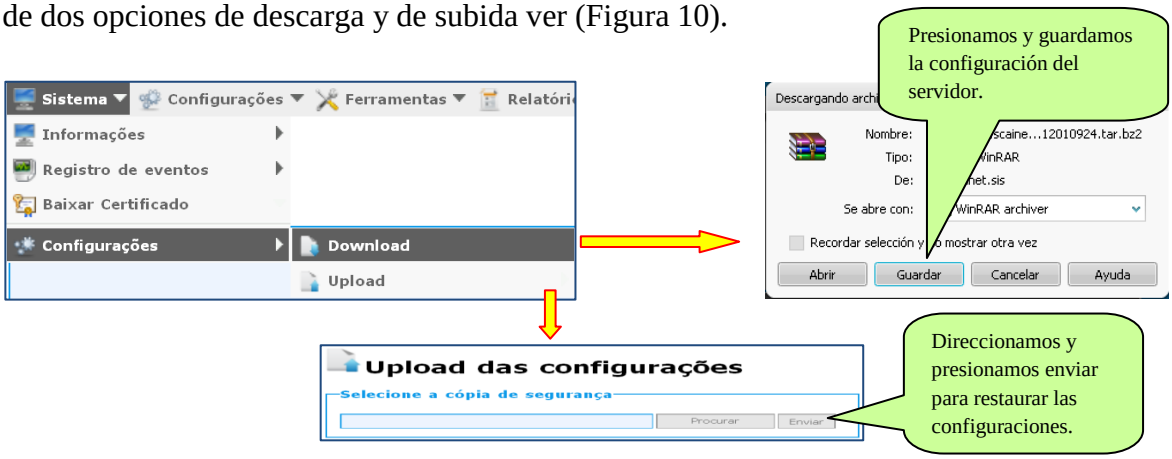


Figura 10.

3. EL MENÚ CONFIGURACIONES

Dentro del menú configuraciones se comprende 4 opciones y 5 sub-menú, este menú es uno del más importante ya que en esta instancia podemos configurar opciones de agregados ver (Figura 11).

Figura 11.

3.1. Sub-Menú Conexiones: En esta opción nos sirve para una configuración, rápida tanto de tarjeta de red física y virtual, muy brevemente se mostrara las opciones ver figura 12.

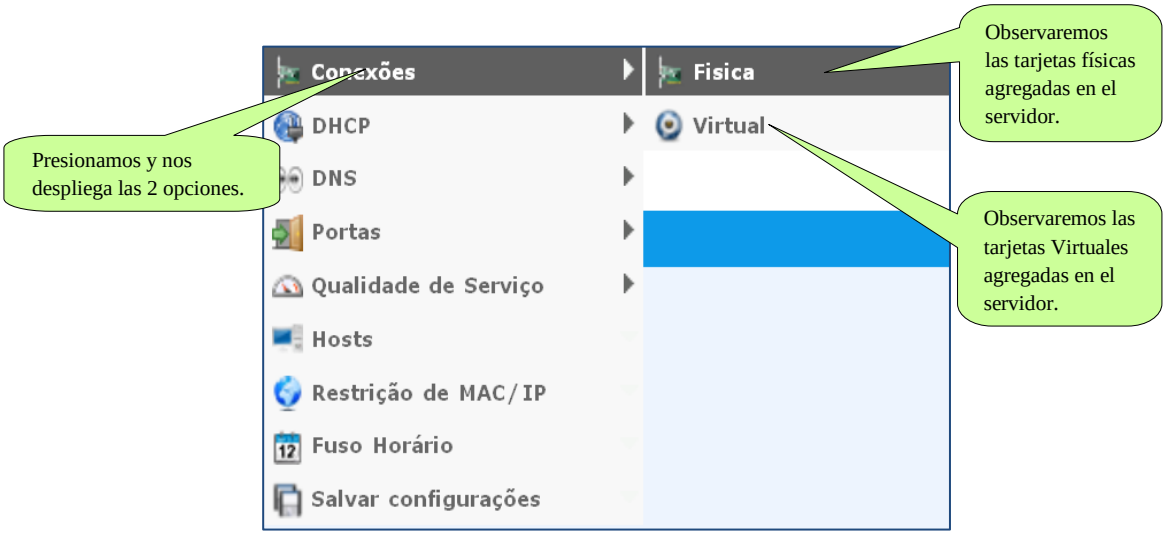


Figura 12.

3.2. Sub-Menú DHCP: En esta tememos las opciones de configurar gráficamente DHCP, pero no es muy necesario ya que en otras instancia como en la de registro de MACxIP, se explicara el agregado manual de equipos, ahora observaremos las opciones que se tienen este sub-menú la cual esta actualizado recientemente ver (Figura 13).

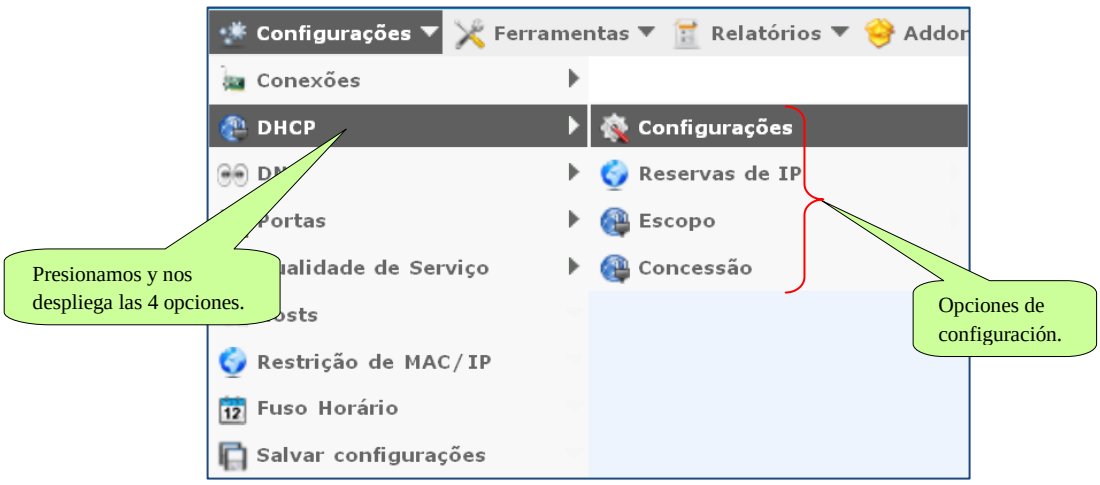
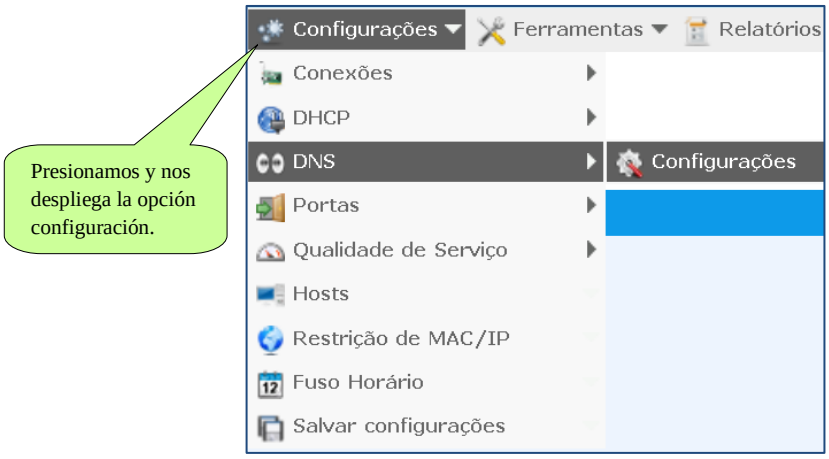


Figura 13.

3.3. Sub-Menú DNS: La configuración del DNS es opcional, ya que es para agregar a dominios y nos puedan ver desde internet ver (Figura 14).



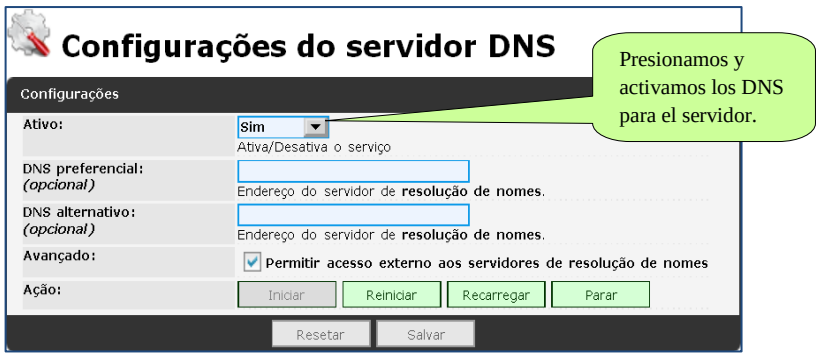


Figura 14.

3.4. Sub-Menú Puertos: Esta nos permite activar como desactivar puertos como también direccionar los puertos ver (Figura 15).

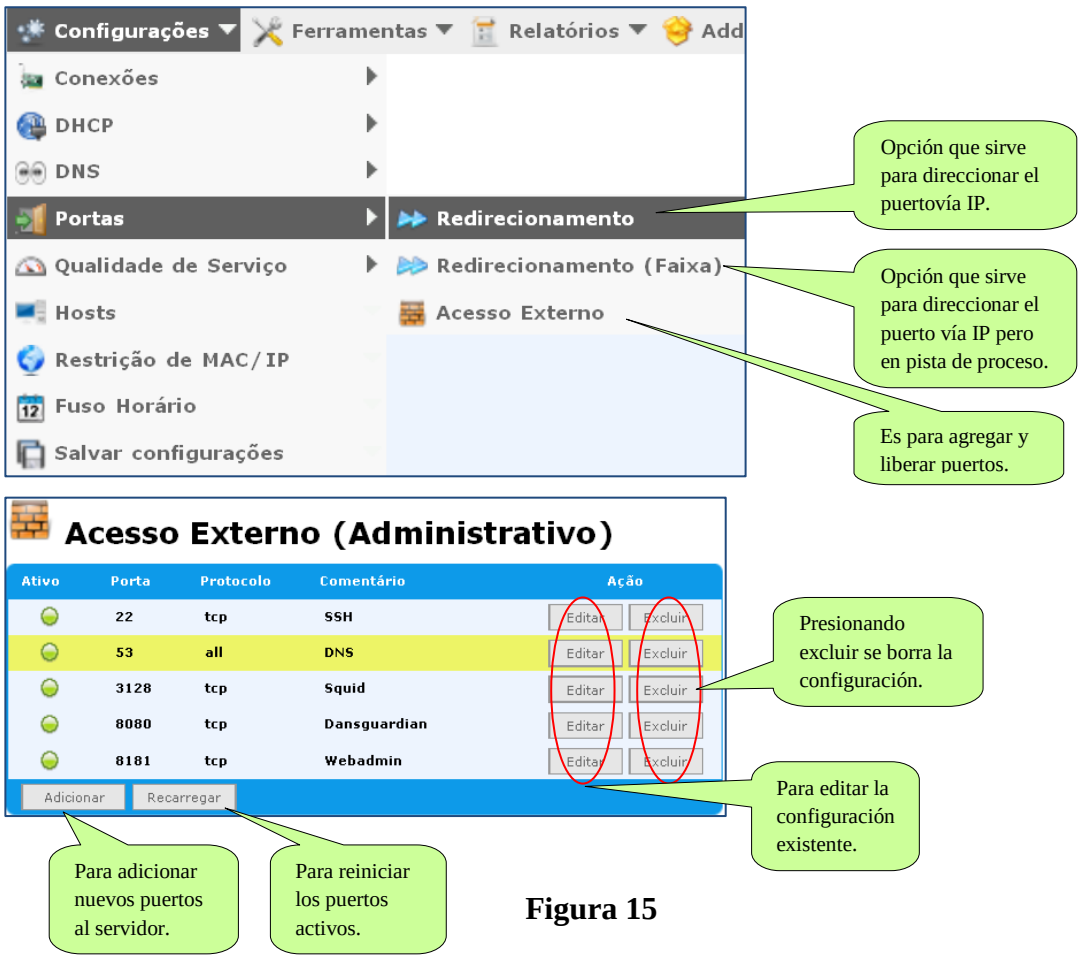


Figura 15

3.5. Sub-Menú Cualidades de Servicio: Esta opciones nos permite trabajar con el QoS, ya que se puede configura el ancho de banda por equipo o por sub-redes ver (Figura 16).

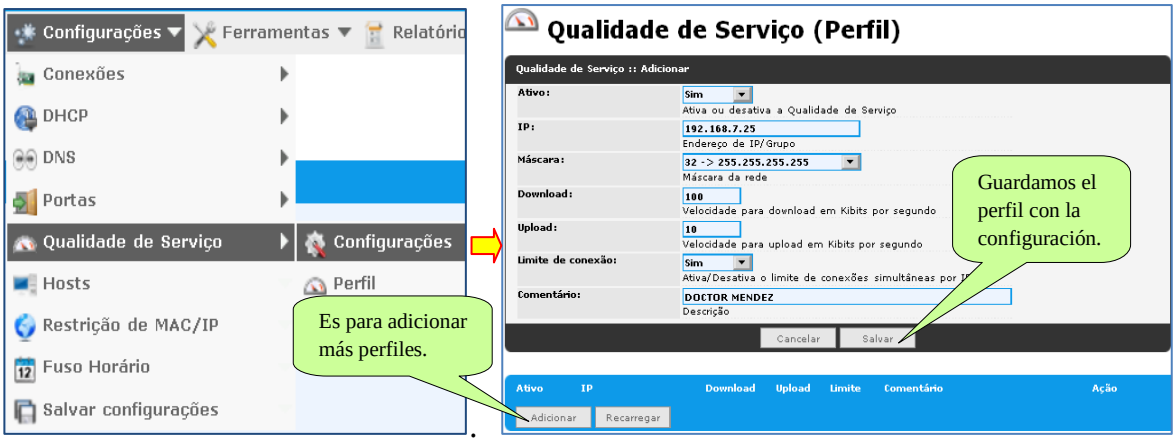


Figura 16

3.6. Opción Hosts: Es usado por el sistema operativo para guardar la correspondencia entre dominios de Internet y direcciones IP ver (Figura 17).

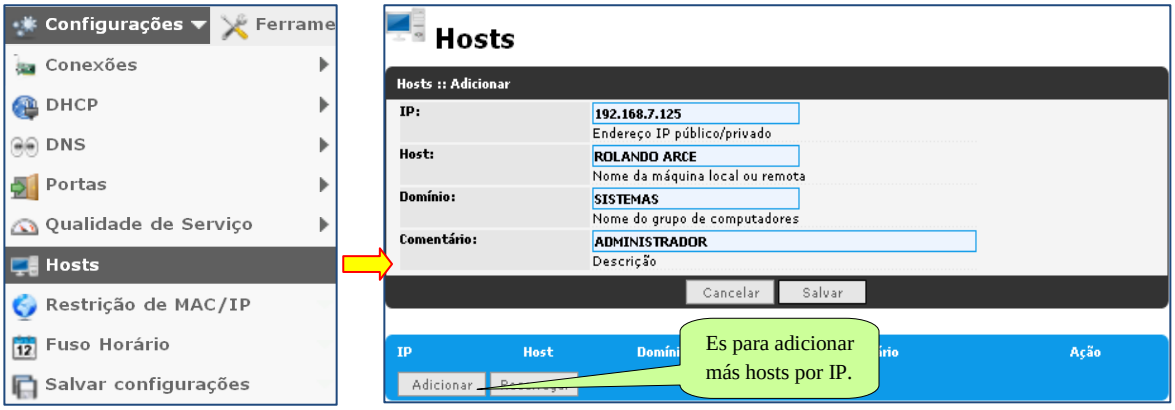


Figura 17.

3.7. Opción Restricción de MAC/IP: Esta es una de las opciones más importantes que cuenta del servidor, por eso es necesario habilitar el control MACxIP, en este caso mostraremos las adiciones de equipos, como también esto hace parte del reserva del DHCP, en la sólo navegarán quienes estén registrados en la lista, si el Control MAC x IP está habilitado en el *brazilfw.cfg*, y el MAC no está en la lista, el cliente no conseguirá hacer nada, ni siquiera podrá conseguir hacer ping al BFW. A través del MAC no registrado sólo se podrá tener acceso al puerto del webadmin y al puerto ssh para realizar un eventual mantenimiento ver (Figura 18).

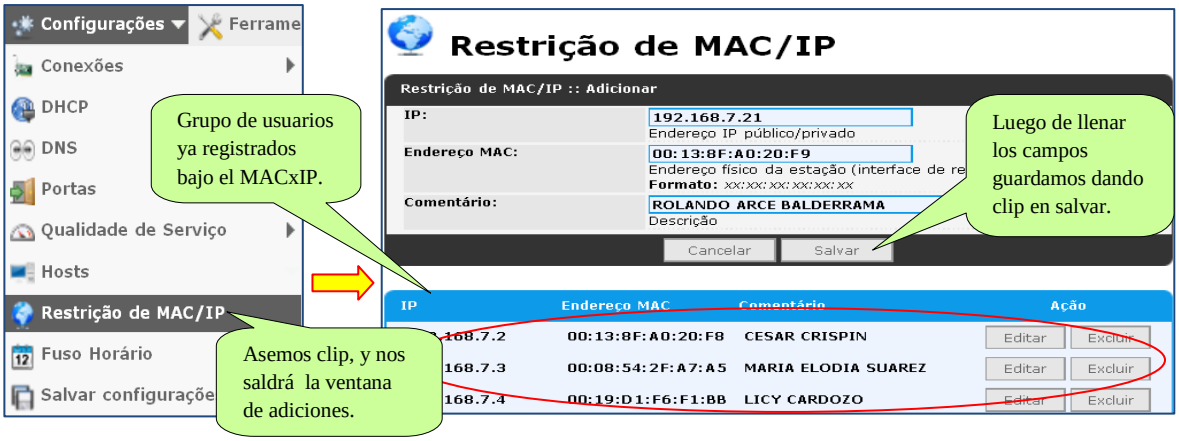


Figura 18.

3.8. Opción Zona Horaria: En esta podemos cambiat nuestra zona horaria, de manera muy facil, ya que es importante para los reportes de usu ver (Figura 19).

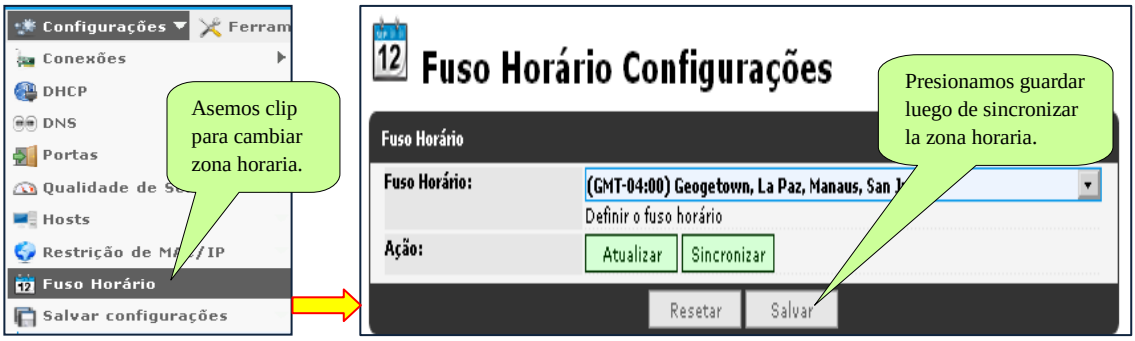


Figura 19

3.9. Opción Guardar Configuraciones: Esta opción como el nombre lo dice es para realizar el guardado de la configuraciones realizadas en el entorno grafico ver (Figura 20).

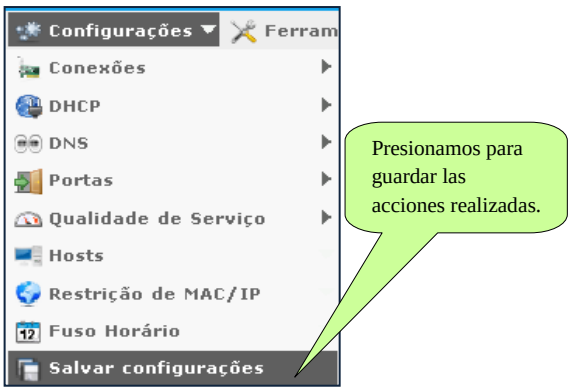


Figura 20.

4. MENÚ HERRAMIENTAS:

Dentro del menú herramienta comprende de 1 sub-menú y 2 opciones, este menú contiene opciones importantes, porque tenemos las opciones de manipular los archivos y redes ver (Figura 21).

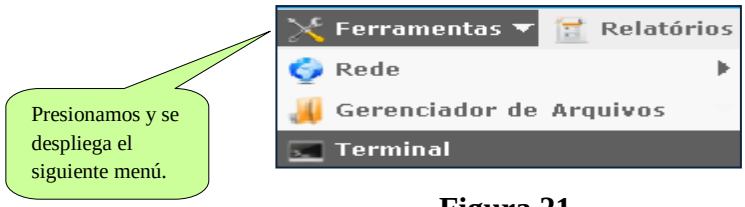


Figura 21.

4.1. Sub-Menú Redes: En esta opción se encuentra la mayoría de las herramientas, de redes para así por realizar los escaneos, escaneos, test de velocidad ver (Figura 22).

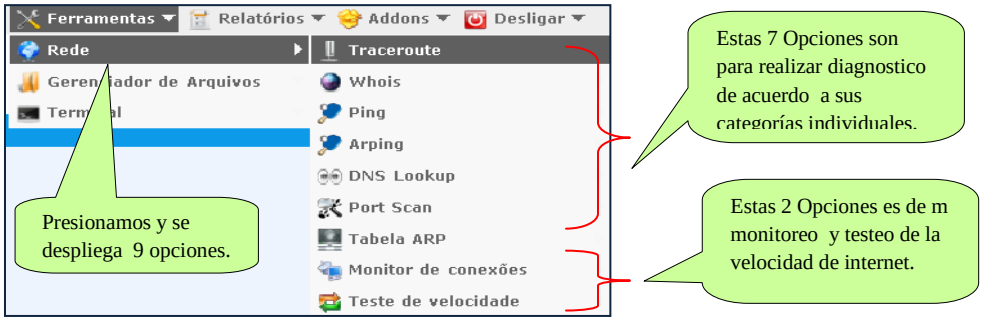


Figura 22.

4.1.1. Opción de Tracerouter: Herramienta de diagnóstico de redes que permite seguir la pista de los paquetes que van desde un host (punto de red) a otro ver Figura 23.

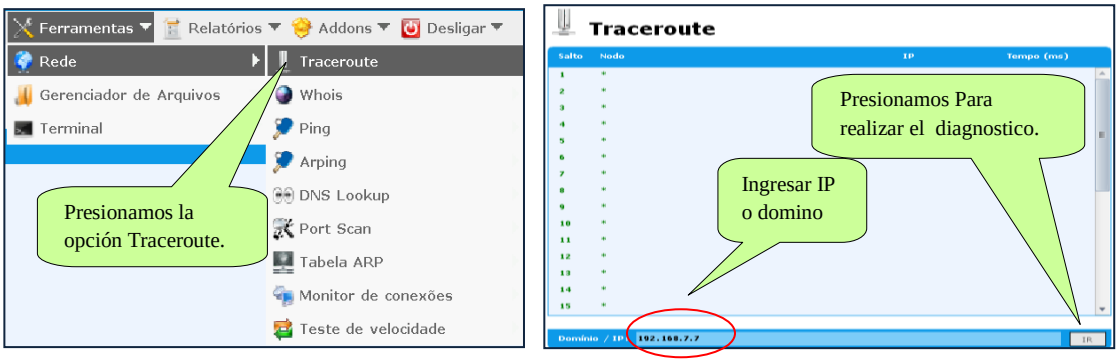


Figura 23.

4.1.2. Opcion Whois: Essta herramieenta esta en protocolo TCP, basado en preguntas y repuestas que es utilizado para consultas en base de datos para determinar el propietario de un nombre de dominio o una dirección IP ver (Figura 24).

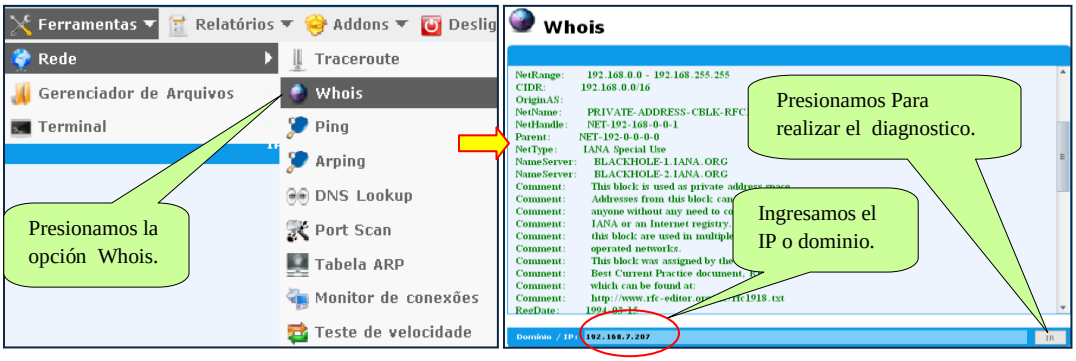


Figura 24.

4.1.3. Opción Ping: Esta herramienta: Comprueba el estado de la conexión con uno o varios equipos remotos, por medio de los paquetes de solicitud de eco y de respuesta de eco (ambos definidos en el protocolo de red ICMP) ver (Figura 25).

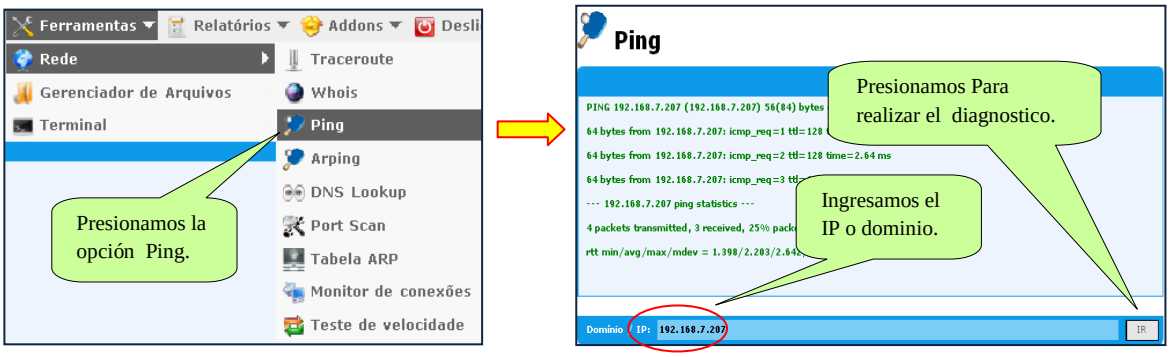


Figura 25

4.1.4. Opción Arping: Esta herramientas es idéntica al ping, la única diferencia es que comprueba el estado de la conexión y también nos muestra el address del equipo escaneado, como el tiempo estimado de paquetes ver (Figura 26).

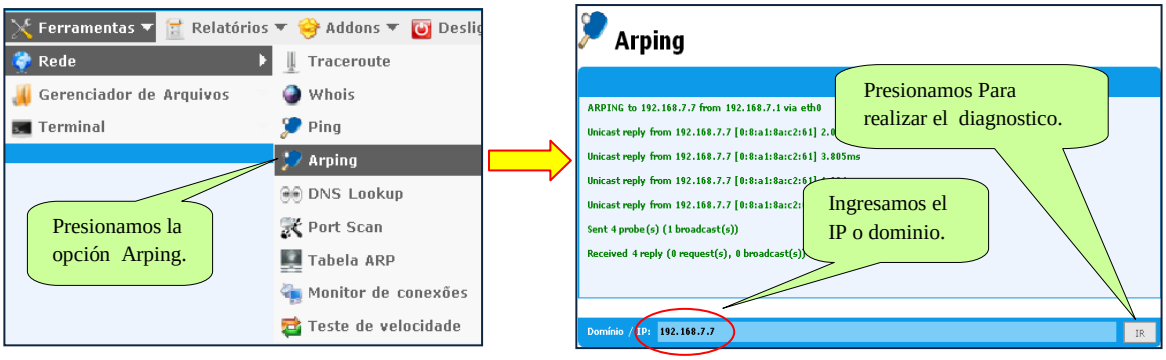


Figura 26.

4.1.5. DNS Lookup: Esta herramienta es para verificar, el nombre o dirección IP del DNS que pertenece, búsqueda a través de la IP o dominio ver (Figura 27).

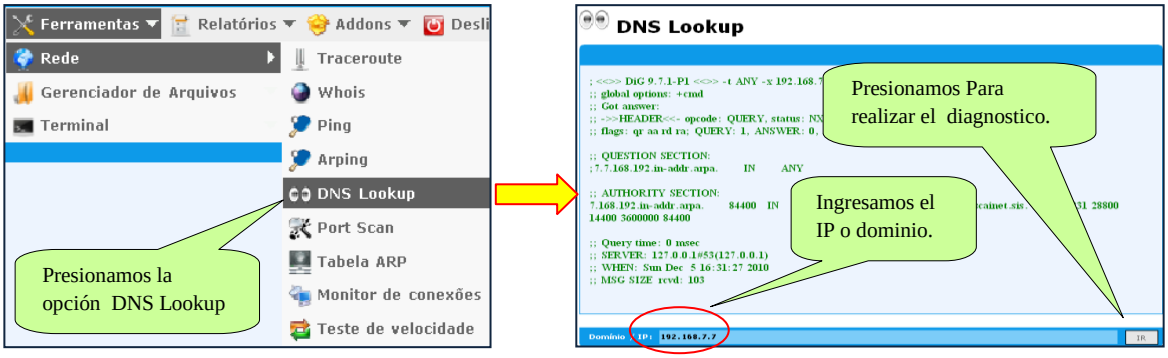


Figura 27.

4.1.6 Port Scan: Esta herramienta es para el escaneno de puertos que estan abiertos o cerrados su busqueda se realizar por IP o dominio ver (Figura 28).

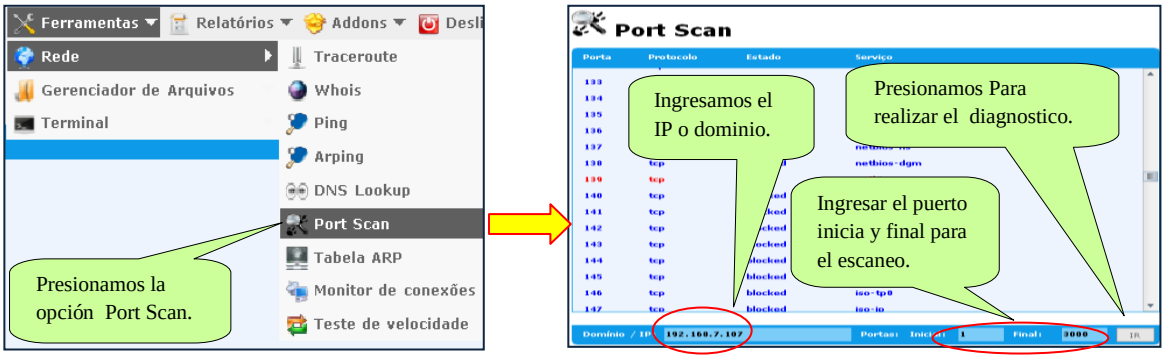


Figura 28.

4.1.7. Tabela ARP: Esta herramienta nos muestra una tabla de todos los equipos que se encuentran en la red y captura su IP, MAC y Host ver (Figura 29).

Figura 29.

4.1.8. Monitor de Conexiones: Esta herramienta es pera ver todas las conexiones que pasan a través del servidor de redes ver (Figura 30).

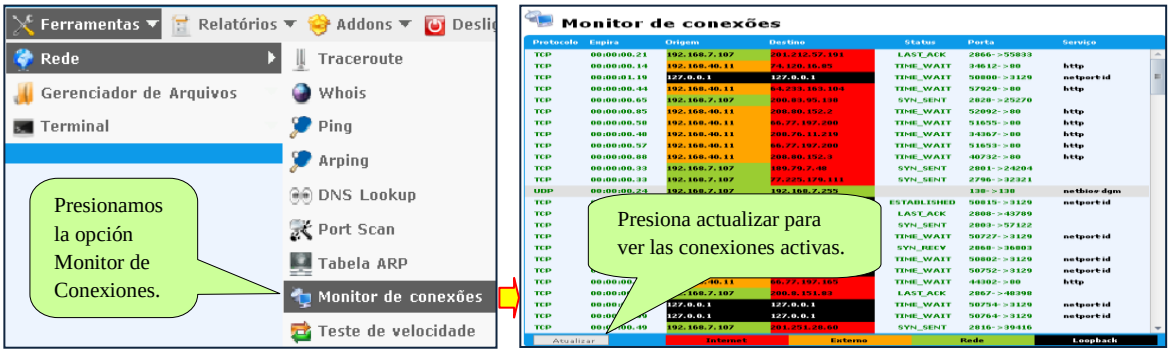


Figura 30.

4.1.9 Teste de velocidad: Esta herramienta es muy útil para poder testear la velocidad de conexión de internet de bajada como de subida ver (Figura 31).

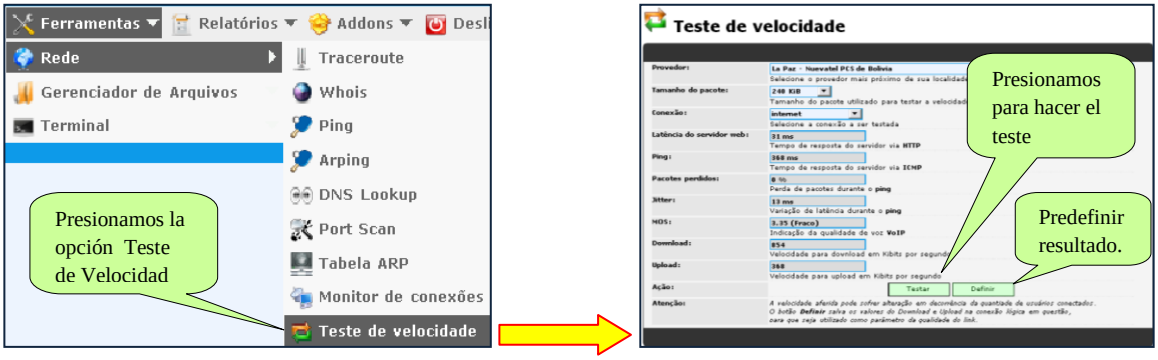


Figura 31.

4.2. Opción Generador de Archivos: Nos Muestra todos los directorios del servidor, mediante una ventana de exploración ver (Figura 32).

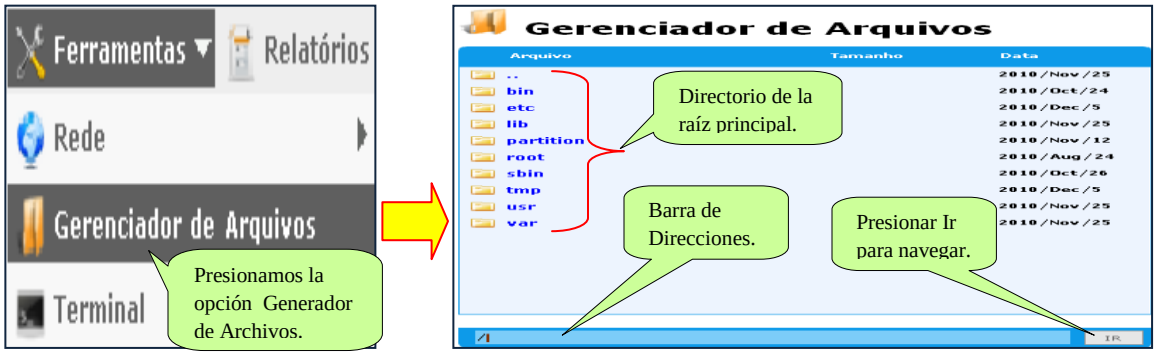


Figura 32.

4.3 Opción Terminal: herramienta remota de la terminal de Linux ver (Figura 33).

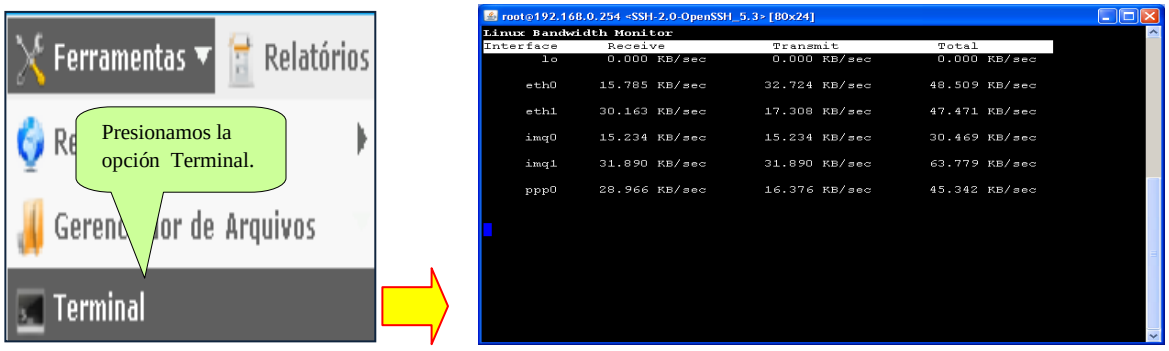


Figura 33.

5. MENÚ RELATORÍOS

Este menú comprende de solo 2 opciones una es la de sitios asesados y la otra para las rutas de conexión configuradas ver (Figura 34).

Figura 34.

5.1. Opción Sitios Acezados: Esta opción nos sirve para ver todos los sitios acezados por los usuarios que existen en la red, el SQUID maneja la herramienta de SARG y es con esta que podemos sacar los reportes ver (Figura 35).

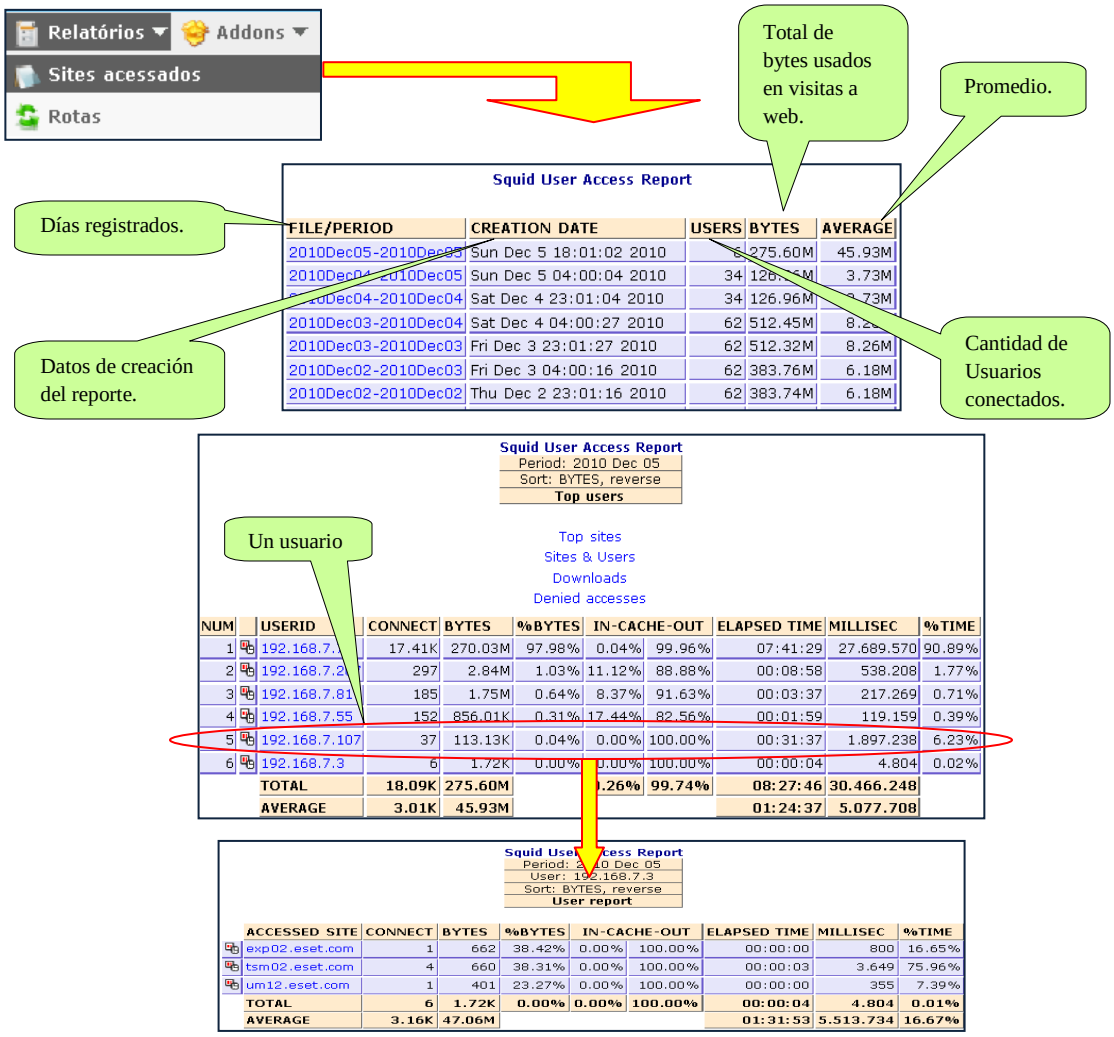


Figura 35.

5.2. Opción Rutas: Esta opción nos proporciona las conexiones físicas que tiene el servidor tanto del proveedor de internet como de red de datos ver (Figura 36).

Figura 36.

6. MENÚ ADDONS

Este menu esta compuesto actualmente de 4 sub-menus, en la que son herramientas opcionales que sólo funcionan anexados a otro y que sirven para incrementar o complementar sus funcionalidades ver (Figura 37).

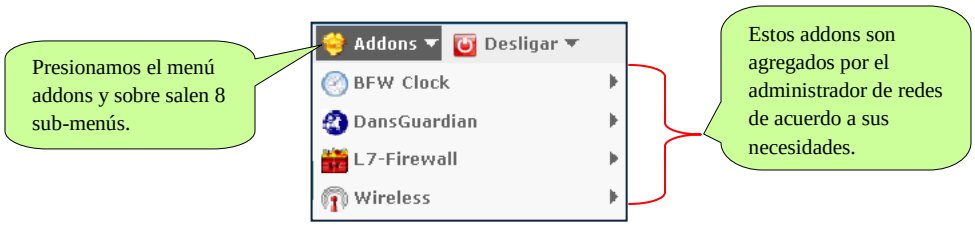


Figura 37.

6.1. Sub-Menú BFW Clock: Esta addons es solamente un reloj de pantalla ver (Figura 38).

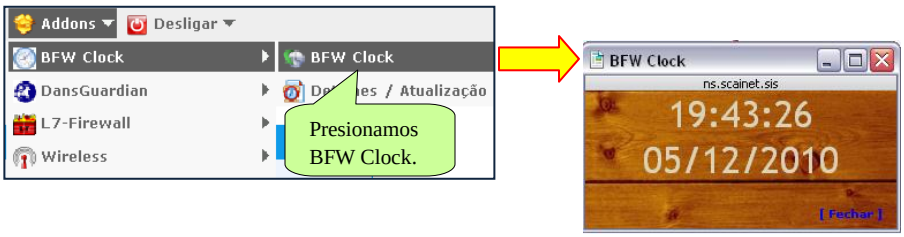


Figura 38.

6.2. Sub-Menú DansGuardian: Este addons es uno de los mas importantes ya que facilita las restriciones por filtrado y se puede aser de forma mas facil ver (Figura 39).

Figura 39.

6.3. Sub-Menu L7-Firewall: Este addons es importante ya que, trabaja directamente con los layer 7, que son una serie de protocolos para firewall ver (Figura 40).

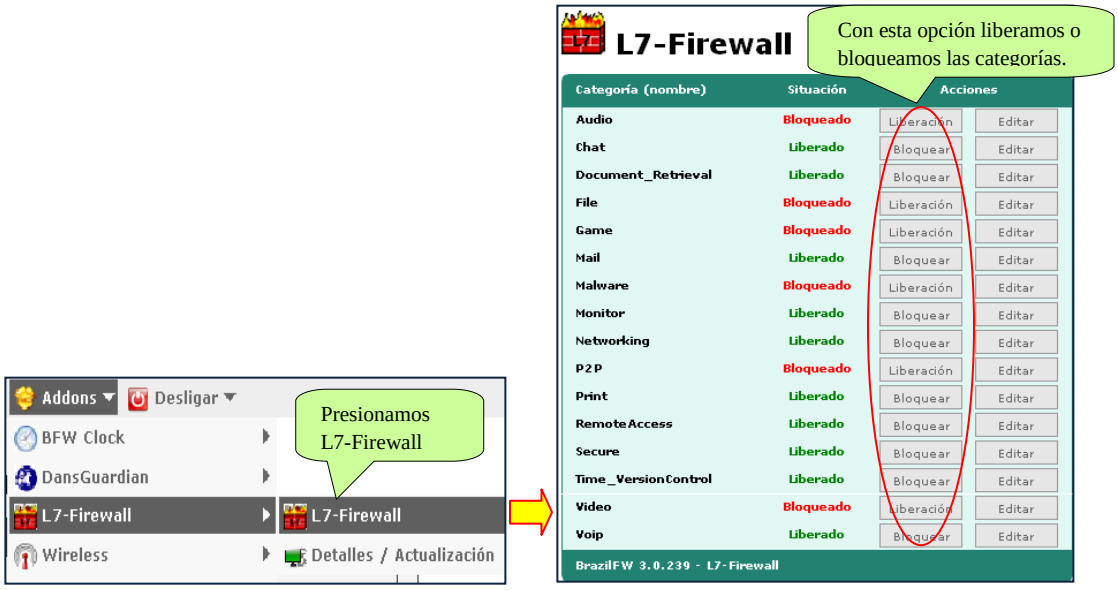


Figura 40.

6.4. Sub-menú Wireless: Este addons solo funciona si tenemos instalado una antena de Wireless en el servidor en este caso solo mostraremos su opción ver (Figura 42).

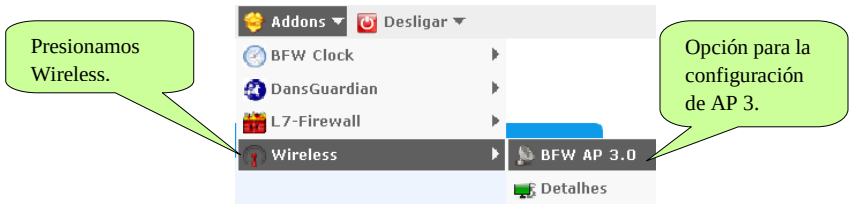


Figura 42.

7. MENÚ DESLIGAR

Este menú simplemente es de dicado para apagar y reiniciar el servidor ver (Figura 43).

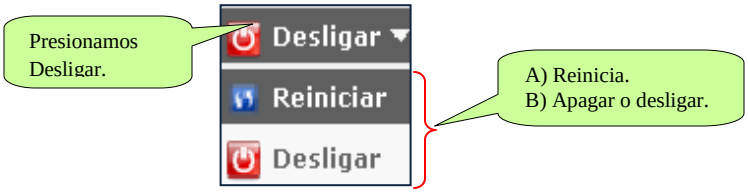


Figura 43.

Cobija, 1 de Diciembre del 2010

Señor:

Lic. Milton Ramírez Linares.
DOCENTE DE LA ASIGNATURA DE
TALLER DE LICENCIATURA II

Presente.-

REF: **CONFORMIDAD Y AVAL DEL PROYECTO DE GRADO A NIVEL LICENCIATURA DEL POSTULANTE UNIV. ROLANDO ARCE BALDERRAMA.**

De mi mayor consideración:

En calidad de asesor del proyecto de grado, se ha realizado el seguimiento continuo del desarrollo del proyecto de grado del postulante,**Univ. Rolando Arce Balderrama,**para la unidad de **Sistemas,** dependiente del **predio central de la prefectura de Pando,** es que mediante el presente expreso mi conformidad, que el contenido de forma y fondo del proyecto de grado presentado, amerita su aprobación y su posterior defensa final.

Es cuando informo para los fines consiguientes.

Atentamente:

Ing. Jhonny Mamani Yanaca.
Assesor

Cc. Archivo.

Cobija, 13 Diciembre del 2010

Señor:
Ing. José E. Balderrama Méndez.
COORDINADOR DE PROGRAMA DE ING. INFORMÁTICA

Presente.-

REF.: CONFORMIDAD Y AVAL PARA LA PRESENTACIÓN DEL INFORME FINAL DEL PROYECTO DE GRADO NIVEL LICENCIATURA DEL POSTULANTE UNIV. ROLANDO ARCE BALDERRAMA.

De mi mayor consideración:

En calidad de tutor colectivo de la asignatura Taller de Licenciatura II, se ha realizado el seguimiento continuo del desarrollo del Proyecto de Grado Titulado, **IMPLEMENTACIÓN DE UN SERVIDOR DE ADMINISTRACIÓN DE RED DE DATOS PARA EL PREDIO CENTRAL DE LA PREFECTURA DE PANDO,** del postulante Univ. Rolando Arce Balderrama, y habiéndose cumplido con todos los requisitos exigidos en el reglamento. En tal seguimiento expreso ante su autoridad, que el contenido de forma y fondo del informe Final del Proyecto de Grado presentado, a merita el aval para que el postulante efectué la presentación y defensa de su proyecto de grado a objeto de optar el título de ing. Informática.

Es cuanto informo para los fines consiguientes.

Atentamente.

Lic. Milton Ramírez Linares.
TUTOR COLECTIVO DEL PROYECTO DE GRADO