UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO – CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

EVALUACIÓN DE SISTEMAS DE GESTIÓN DE REDES BAJO SOFTWARE LIBRE DE LA ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO"

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

GUERRERO PANTOJA CRHISTIAN DANIEL

DIRECTOR: Ing. Rafael Jaya.

Quito, julio de 2011

DECLARACIÓN

Yo Crhistian Daniel Guerrero Pantoja declaro bajo juramento que el trabajo aquí presentado es de mi autoría; el cual no ha sido presentado anteriormente en ningún grado o calificación profesional; y, que todas las referencias bibliográficas que se exponen en el trabajo han sido consultadas.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, sede Quito - Campus Sur, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

Quito, 13 de julio de 2011

_____

Crhistian Daniel Guerrero Pantoja

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado por Crhistian Daniel Guerrero Pantoja, bajo mi supervisión.

Ing. Rafael Jaya
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Expreso mi agradecimiento a mi familia, a mis hermanos y en especial a mis padres, ya que han sido uno de los principales pilares que han sabido impulsarme en momentos claros y de oscuridad, por su sacrificio al haber fomentado el profesional que seré pero en particular la persona que hoy soy.

Al personal de la Administración Zonal Norte "Eugenio Espejo" por la ayuda conferida al permitirme realizar y culminar este Proyecto de Titulación. En particular quiero dar mis agradecimientos al Ing. Gustavo Correa Carcelén, Jefe Zonal de Informática del Municipio de Quito por el apoyo, tiempo y consejos otorgados en el transcurso del proyecto.

Cabe recordar las acertadas palabras de *Pedro Bonifacio Palacios (Almafuerte)* en momentos de intensa penuria.

No te des por vencido, ni aun vencido,
no te sientas esclavo, ni aun esclavo;
trémulo de pavor, piénsate bravo,
y arremete feroz, ya mal herido.

Ten el tesón del clavo enmohecido
que ya viejo y ruin, vuelve a ser clavo;
no la cobarde estupidez del pavo
que amaina su plumaje al primer ruido.

Procede como Dios que nunca llora;
o como Lucifer que nunca reza;
o como el robledal, cuya grandeza
necesita del agua y no la implora…

Que muera y vocifere vengadora,
ya rodando en el polvo, tu cabeza!

DEDICATORIA

Este trabajo está dedicado a mi madre Isabel Pantoja Guancha, la que con su sabiduría, entrega y dedicación hacia la familia ha sabido motivar mi accionar hacia la vida. A mi padre José Luis Guerrero, a mis hermanos: Ximena y Franklin. A ellos por extenderme su apoyo, conocimientos y sabiduría.

A todas aquellas buenas y malas personas que han influido de una o de otra forma en la culminación de esta etapa de mi vida.

A todos mis amig@s que han colaborado con su apoyo constante, sincero y motivante.

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

El presente documento muestra un análisis pormenorizado que llevará a la Administración Zonal Norte “Eugenio Espejo” a una gestión de red óptima tomando en cuenta que se ha evaluado diferentes Sistemas de Gestión de Red orientados al software libre. Para brindar mejor comprensión al lector, el documento fue dividido en 4 capítulos, el cual posee una cronología clara y concisa.

El primer capítulo tiene como objetivo, evidenciar de una manera rápida los puntos a los que se pretende llegar; también preparando al lector con el conocimiento necesario para comprender de mejor forma aspectos relativos a la Gestión de Red tanto en sus objetivos, arquitectura, protocolos a tener en cuenta, componentes, funcionamiento y versiones.

El segundo capítulo expone toda la situación actual de la red LAN de la Administración Zonal Norte “Eugenio Espejo”, esto incluye: su sistema de comunicaciones, infraestructura de red, equipos utilizados, software y módulos corporativos, etc. Todas las partes mencionadas y muchas más han sido detalladas para comprender el tipo de operatividad que posee en la actualidad la Institución. Seguidamente se presentan datos previos de monitoreo, a razón de un pre análisis con otras herramientas y sistema de gestión, luego de lo cual posibilita continuar con los sistemas de gestión libre que conciernen al proyecto.

El tercer capítulo se enfoca en analizar los distintos Sistemas de Gestión de Red Libre evaluados sobre la red de la Institución; a su vez se presentan datos relacionados al funcionamiento, características, rendimiento y consideraciones de uso que cada uno de ellos posee. Según los datos arrojados y comparando diversos criterios como rendimiento, modularidad, configuración, plataformas compatibles,

etc.; así como también tomado en cuenta para la elección requerimientos funcionales y no funcionales se ha elegido el sistema más idóneo para la Institución.

El cuarto capítulo procura delinear las diferentes áreas funcionales que atañen a la gestión de red intentando rescatar características y propuestas que ayuden al mejoramiento de la Institución. Así para delinear las áreas funcionales se centra el estudio en el modelo de gestión ISO, más comúnmente conocido por sus siglas en inglés FCAPS, la que desglosa las distintas áreas como Gestión de Fallos, Configuración, Contabilidad, Prestaciones y Gestión de Seguridad.

Al final se presentan las conclusiones y recomendaciones que se han obtenido al cabo de este proyecto.

PRESENTACIÓN

El objetivo del presente proyecto es llevar a la Institución a analizar un proceso de cambio que otorga grandes beneficios en la adopción de un Sistema de Gestión de Red Libre que posibilite monitorear y administrar diferentes servicios y dispositivos que se encuentran inmersos dentro de la red LAN.

Este tipo de adopción está particularmente acoplando las circunstancias intrínsecas que la Institución conlleva, así pues toma en cuenta la evaluación de distintos Sistemas de Gestión de Red Libres de acuerdo a sus diversas características y funcionalidades; todo con el fin de conseguir una gestión eficiente y de costo reducido. El garantizar una adecuada gestión de red procura disminuir al mínimo la pérdida del desempeño operacional y aumentar la calidad de servicio otorgado a los usuarios.

También se intenta concientizar sobre el uso y manejo de la información dando propuestas y sugerencias de acuerdo al área funcional que se esté enfocando. Se ha situado un énfasis importante sobre la Gestión de Seguridad no sin antes destacar que cada una de las áreas en sí son importantes; retomando la Gestión de Seguridad se han mencionado propuestas y políticas de seguridad que siendo bien aplicadas otorgarán un alto grado de seguridad sobre todo en el bien más valioso que es la información.

El proyecto en sí puede situarse como referencia para cualquier tipo de Institución sin importar su ámbito de acción o su alcance operativo debido a la magnitud y a los beneficios mostrados por el software libre.

CAPÍTULO 1. ANTECEDENTES E INTRODUCCIÓN

En este capítulo, se pondrá en evidencia todo el contenido teórico que demanda el involucrarse en sistemas de gestión de red orientados a sistemas libres; también se establecerán los objetivos perseguidos por parte del proyecto y la descripción general del mismo.

Esta información permite conocer parámetros claves que serán de gran utilidad para el entendimiento del presente proyecto, en el transcurso de este.

1.1 DESCRIPCIÓN DEL PROBLEMA

En la mayoría de las medianas y grandes empresas una dificultad existente, es la que implica el mantener una efectiva gestión de la red, ya que al depender más que nunca de su infraestructura informática se ve obligada a tener una adecuada gestión acorde a las necesidades de la empresa.

Al existir empresas en que el problema más fundamental del área de sistemas es una limitante económica por no poder sacarle todo el provecho a los recursos económicos asignados, se ve la posibilidad de enfocarse en sistemas libres que ayuden a gestionar la red de una manera accesible sin afectar en gran medida el presupuesto.

La forma de conseguir una gestión de la red más eficiente y de costo reducido, es hablar de software libre, ya que debido al acceso que este nos brinda es posible hacer uso de este tipo de sistemas sin necesidad de preocuparse por licencias que hacen dificultosa la adquisición de estas, además otorgándonos un menor costo de implantación, capacidad de acceso total y control de la tecnología.

La gran problemática que da no tener una adecuada gestión sobre la red, es la pérdida del desempeño operacional y calidad de servicio que se intenta ofrecer del cual derivan problemas subsecuentes como pérdida de productividad, descontento general y credibilidad cuestionada.

También, se desvela la dificultad que la empresa presenta en cuanto a un inadecuado monitoreo, interpretación y control de los comportamientos de la red que no logra garantizar una disponibilidad y rendimiento que coincidan con los objetivos empresariales.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Evaluar la necesidad de una gestión óptima de la red haciendo uso de sistemas libres, con la finalidad de evitar pérdidas en los servicios prestados y lograr un adecuado control, así como también una elevada productividad.

1.2.2 OBJETIVOS ESPECÍFICOS

- Controlar adecuadamente los recursos estratégicos corporativos.
- Disminuir tiempos de inactividad dados por fallas, bajo rendimiento; de los elementos que conforman la red.
- Lograr afianzar un alto nivel de servicio en los recursos gestionados con el mínimo coste.
- Priorizar las áreas funcionales de gestión de red.
- Analizar las funcionalidades de los sistemas libres de gestión de red.
- Elegir un sistema libre que permita una gestión eficiente de la red.
- Evaluar el grado de relación calidad/costo que determina asumir sistemas de software libre como alternativa.

1.3 JUSTIFICACIÓN

Por la escalabilidad que tienen muchas empresas al extender sus redes y no lograr una eficaz gestión de esta, debido a factores tan críticos como es su presupuesto y la poca añadidura a tecnologías propietarias restrictivas en el uso de sistemas de gestión; llevan a las empresas a enfocar sus esfuerzos en tecnologías libres.

La tendencia que tienen varias empresas en comenzar a involucrarse cada día más en este aspecto, nos lleva a indagar el cambio sustancial que ofrece el software libre en la gestión óptima de la red.

El llevar una panorámica de costos tanto de mantenimiento, como de administración, permitirá darnos cuenta la realidad sobre el software libre y su verdadera tendencia para los siguientes años; obligando a exponer el verdadero beneficio que este tiene.

La investigación pondrá en claro el impacto que refleja acceder a software libre frente a software propietario ya que se constatará disminución de costos, acceso sin restricciones a todas las funciones, incremento de la rentabilidad.

Se verá el beneficio de acceder a tecnologías libres que no se rigen de un licenciamiento que conlleva más obligaciones que derechos para el usuario, que a la larga afectan su uso y limitan su acceso.

1.4 ALCANCES

Se realizará un diagnóstico de la red para conocer de manera clara y precisa el estado en el que se encuentra la red.

Se mejorará la capacidad que tiene la red en puntos críticos como monitorización, mantenimiento preventivo, redundancia.

Se identificará las causas que ocasionan un bajo rendimiento de la red.

Se examinará diferentes sistemas libres de gestión de red, de las cuales se realizará sus respectivas comparativas en cuanto a desempeño y funcionalidad.

Se escogerá el sistema libre que nos brinde el mejor desempeño y funcionalidad, esta se utilizará para realizar un sondeo de toda la infraestructura de red.

Se logrará una monitorización de los servicios de red (TCP, UDP, ICMP, SMTP, POP3, HTTP, SNMP, etc.), monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos, etc.).

Se presentará informes de los datos recogidos y anomalías que pueden existir sobre la recolección de paquetes de red.

Se demostrará la rentabilidad que otorga asumir sistemas libres como alternativa.
Se formulará propuestas que determinen una adecuada gestión de las distintas áreas funcionales (Gestión de configuración, Gestión de fallos, Gestión de prestaciones, Gestión de seguridad, Gestión de contabilidad) de la Institución.

1.5 DESCRIPCIÓN GENERAL DEL PROYECTO

El proyecto resolverá la problemática que tiene la empresa en cuanto a su infraestructura de red, la cual demanda una adecuada gestión de red por medio de sistemas libres, que indaguen el buen funcionamiento del mismo y alerten sobre cualquier anomalía que se pueda presentar indistintamente de la gravedad que conlleve.

Para llegar a obtener una gestión óptima de la red, se realizará en una primera etapa un análisis de la situación actual de toda la infraestructura, la cual demostrará su estado. Seguidamente y mediante el análisis y pruebas de distintos sistemas libres de gestión de red, se rescatará el sistema que presente las mejores condiciones de funcionamiento, rendimiento y gestionamiento frente al análisis de tráfico de red.

Realizando el sondeo de la red por medio del sistema escogido, se determinará cualquier anomalía que esté presente y se esbozará una propuesta para corregir los problemas encontrados. Además con los datos recopilados se estará en facultad de proponer formas apropiadas de gestionar las diferentes áreas funcionales que tiene la Administración Zonal Norte “Eugenio Espejo”.

1.6 INTRODUCCIÓN A LA GESTIÓN DE RED

1.6.1 MONITOREO DE RED

En la actualidad la complejidad que contemplan las redes, la infraestructura que presentan, así como sus computadoras hacen que estos recursos lleguen a un punto crítico para una Institución, por tal medida el correcto monitoreo de los servicios (FTP, Web, POP3, etc.) y los recursos (CPU, memoria, disco, etc.) logran establecer una elevada confiabilidad de la red y un desempeño óptimo garantizando al Administrador de la Red, una red operativa y con buen desempeño; mucho de lo cual lo consigue haciendo uso de protocolos como ping, SNMP, NetBIOS, TCP, UDP, etc; los cuales ponen en evidencia tiempos de respuesta, servicios habilitados, puertos activos; estos conjuntamente con sistemas de gestión de redes logran establecer el objetivo buscado.

1.6.2 MONITORIZACIÓN Y CONTROL DE LOS SISTEMAS [1]

En la gestión de red se distinguen dos aspectos:

1.6.2.1 Monitorización

Las acciones consisten en obtener información de la red con el fin de detectar anomalías, son acciones pasivas y su único objetivo, es conocer el comportamiento de los recursos gestionados. Consta de cuatro aspectos:

- **Definir la información de gestión que se monitoriza:** Según su naturaleza temporal podrá ser:
  - Estática: Caracteriza la configuración de los recursos y cambia con muy poca frecuencia. Como ejemplo tenemos la dirección IP de una interfaz.
  - Dinámica: Asociada a eventos que se dan en la red, por ejemplo paquetes transmitidos. Dentro de este segundo tipo vamos a tener la información estadística, obtenida al procesar la información dinámica; por ejemplo el número medio de paquetes transmitidos por segundo.

- **Acceso a la información de monitorización:** Por parte de los módulos gestores a los módulos agentes que se localizan en los recursos, el acceso se realiza mediante los denominados protocolos de intercambio de información de gestión, punto clave en la gestión de red.
- **Diseño de políticas de monitorización:** Se fundamenta en un sondeo periódico por parte del gestor a los agentes, preguntando por los datos de monitorización. Existe además el mecanismo de informe de eventos, en el cual los agentes informan por propia iniciativa a los gestores ante un cambio de estado significativo.
- **Procesado de información de monitorización:** Dándole un tratamiento que dependerá de la función para la que se ha realizado la monitorización.

En definitiva con la monitorización, se va a decidir qué información se va a recoger del sistema, como se accede y que se hace con ella.

1.6.2.2 Control

Por otro lado, el control es la acción activa que determina el comportamiento de la red, se encarga de modificar parámetros e invocar acciones. Las tareas de control aportan potencia a los sistemas de gestión, permiten en todo momento y de forma remota, determinar las características del comportamiento de la red.

Tareas incluidas dentro del control.

- Control de la Configuración: Esta describe la naturaleza y estados de los recursos de la red, tanto lógicos como físicos. Existen diferentes enfoques que van desde cambios de valores de atributos, modificación de los parámetros de los elementos de la red, inicialización terminación de la operación de la red y distribución de software.
- Control de la seguridad: Actuación sobre los mecanismos de seguridad destinados a la protección de la red. Para garantizar aspectos de privacidad, integridad y disponibilidad; evitando típicos ataques de captura de mensajes, modificación de mensajes y muchos que se desprenden de los antes citados.

Las funciones de control están agrupadas según sus funciones. Esta tarea fue estandarizada por la ISO (International Standarization Organization) y clasifico las tareas de los sistemas de gestión en cinco áreas funcionales las cuales son: gestión de fallos, gestión de contabilidad, gestión de configuración, gestión de prestaciones y gestión de seguridad.

1.6.3 GESTIÓN DE RED

En general, la gestión de la red es un servicio que emplea una variedad de herramientas, aplicaciones y dispositivos para ayudar a Administradores de Red humanos en la vigilancia y mantenimiento de redes; siendo su propósito específico monitorizar y controlar los recursos de una red, para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio; reduciendo tiempos de inactividad y controlando los costos.

1.6.4 OBJETIVOS DE LA GESTIÓN DE RED

Los objetivos de la gestión de la red son los siguientes:

- Detección de fallos y corrección con la máxima rapidez posible.
- Monitorización del rendimiento, detección de cuellos de botella, optimización de los mismos.
- Gestión de contabilidad y uso que hace del sistema.
- Gestión de seguridad.
- Instalación y distribución de software en el sistema de una manera controlada.
- Gestión de los componentes del sistema y configuración del mismo.
- Planificación y crecimiento del sistema de manera controlada.
- Almacenamiento y análisis de estadísticas sobre el funcionamiento de la red.
- Formulación de recomendaciones útiles para el usuario.

El objetivo final de la gestión de red, es garantizar un nivel de servicio en los sistemas de una organización el máximo tiempo posible, minimizando la pérdida que ocasionaría una parada o funcionamiento incorrecto del sistema. [1]

1.6.5 ARQUITECTURA DE GESTIÓN DE RED [5]

La gestión de red se suele centralizar en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados en las distintas redes de la empresa en cuestión. Un centro de gestión de red dispone de tres tipos principales de recursos:

- **Métodos de gestión:** Definen las pautas de comportamiento de los demás componentes del centro de gestión de red ante determinadas circunstancias.
- **Recursos humanos:** Personal encargado del correcto funcionamiento del centro de gestión de red.
- **Herramientas de apoyo:** Herramientas que facilitan las tareas de gestión a los operadores humanos y posibilitan minimizar el número de éstos.

En la práctica la totalidad de los sistemas de gestión que existen actualmente, utilizan una estructura básica, conocida por paradigma gestor-agente, cuyo esquema queda reflejado en la Figura 1.1.

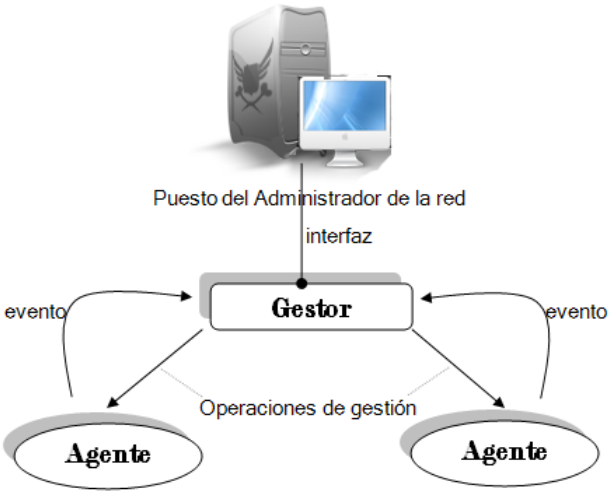


Figura 1.1 Paradigma gestor-agente

Los sistemas de apoyo a la gestión se componen, por lo general:

- Interfaz con el operador o el responsable de la red. Esta interfaz a la información de gestión, a través de la cual el operador puede invocar la realización de operaciones de control y vigilancia de los recursos que están bajo su responsabilidad, es una pieza fundamental en la consecución de un sistema de gestión que tenga éxito. Se puede componer de alarmas y alertas en tiempo real, análisis gráficos y reportes de actividad.
- Elementos hardware y software repartidos entre los diferentes componentes de la red.

Los elementos del sistema de gestión de red, bajo el paradigma gestor-agente, se clasifican en estaciones gestoras y agentes actuando, junto con un protocolo de red.

El esquema de funcionamiento general de una plataforma de gestión se aprecia en la Figura 1.2.

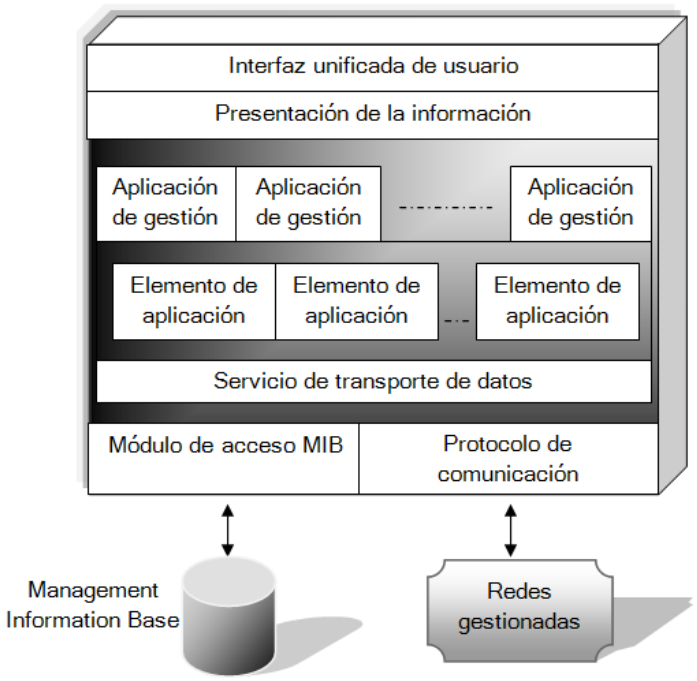


Figura 1.2 Arquitectura de un Sistema de Gestión de Red

1.6.6 GESTIÓN DE RED EN INTERNET

Los componentes indispensables de una red gestionada con SNMP son: NMS (Network Management Station), agente, protocolo de gestión y MIB (Management Information Base); los cuales interactúan entre sí como se muestra en la Figura 1.3.

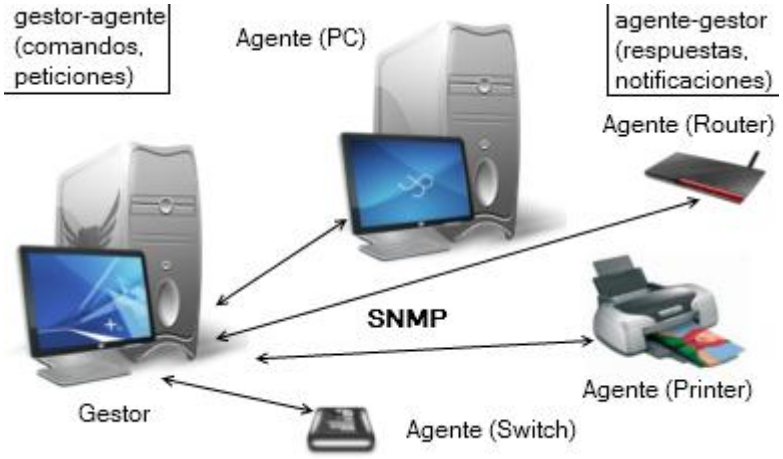


Figura 1.3 Componentes de un Sistema de Gestión de Red

1.6.6.1 SNMP

En la actualidad los protocolos de gestión de red más importantes comprenden el SNMP (Simple Network Management Protocol) y el CMIP (Common Management Information Protocol) sin embargo, el primero por su amplia utilización en redes empresariales y redes de área local es considerado estándar de facto debido a su principal ventaja que para los programadores de gestión de red, es su sencillez frente a la complejidad inherente a CMIP a pesar de que este resuelve la mayor parte de las muchas limitaciones de SNMP, pero por el contrario, consume mayores recursos (alrededor de 10 veces más que SNMP), por lo cual es poco utilizado en las redes de telecomunicaciones empresariales.

SNMP es un protocolo de la capa de aplicación de la arquitectura TCP/IP (Transmission Control Protocol/Internet Protocol), basado en una arquitectura cliente servidor distribuida que facilita el intercambio de información de administración entre dispositivos de red. Utilizado básicamente para el monitoreo de equipos de red,

tales como servidores, estaciones de trabajo, enrutadores, switches y otros dispositivos administrables; basándose en varios datos enviados y recibidos.

El protocolo SNMP está orientado a datagrama que utiliza UDP (User Datagram Protocol) como mecanismo habitual de transporte y así se elimina la necesidad de establecer una conexión antes de la operación del protocolo. Además (por ser orientado a datagrama) no tiene conexión que pueda fallar bajo condiciones adversas. Utiliza dos puertos UDP: el puerto 161 lo abren los agentes para escuchar las peticiones del gestor (mensajes Get, GetNext y Set) y el puerto 162 abre el gestor para recibir los traps de los agentes. [4]

En diversos dispositivos a gestionar es posible encontrar incompatibilidades las cuales son ajustadas por el protocolo SNMP. Los diferentes ordenadores utilizan distintas técnicas de representación de los datos, lo cual puede comprometer la habilidad de SNMP para intercambiar información entre los dispositivos a gestionar. Para evitar este problema, SNMP utiliza un subconjunto de ASN.1 (Abstract Syntax Notation One) en la comunicación entre los diversos sistemas. La sintaxis ASN.1 es necesaria para utilizar una representación de datos común para el intercambio entre sistemas y, dentro de un sistema, intercambio de datos entre aplicaciones que utilizan cada una su representación particular de datos (Más sobre ASN.1 en Anexo A).

1.6.6.1.1 Componentes de SNMP

Los componentes indispensables para su funcionamiento son: consola de administración (NMS), agente, protocolo de gestión y MIB.

a. **Agente:** Es un programa que suele ejecutarse en el dispositivo a gestionar (host, router, hub, switch, etc.) o en una estación con acceso a los recursos gestionados. El mismo que responde a peticiones del gestor(es) y puede enviarle información relativa de algún evento importante.

b. **Consola de administración:** También conocido como gestor, básicamente es la estación de trabajo donde se ejecutan las aplicaciones de gestión de red, y tiene la habilidad de indagar los agentes utilizando SNMP, este dispone de interfaces gráficas para presentar información al usuario y para facilitarle la invocación de operaciones de gestión.

c. **Protocolo de gestión:** Es el conjunto de especificaciones y convenciones que gobiernan la interacción de procesos y elementos dentro de un sistema de gestión; facilitando el intercambio de datos entre agente y gestor.

d. **MIB:** Es una base de objetos administrados es decir, variables que pueden ser monitoreadas o modificadas, las que representan información mantenida en el agente y sobre la que realiza las peticiones el gestor para lograr la administración de la red.

1.6.6.1.2 Ventajas y Desventajas de SNMP

a. **Ventajas de SNMP**

La ventaja fundamental de usar SNMP, es su diseño simple por lo que su implementación es sencilla en grandes redes y la información de gestión que se necesita intercambiar ocupa pocos recursos de la red. Opera fácilmente y no requiere de recursos hardware sofisticado.

Otra ventaja de SNMP, es que en la actualidad, es el sistema más extendido. Ha conseguido su popularidad debido a que fue el único protocolo que existió en un principio y por ello casi todos los fabricantes de dispositivos como puentes y enrutadores diseñan sus productos para soportar SNMP. La posibilidad de expansión es otra ventaja del protocolo SNMP, debido a su sencillez es fácil de actualizar. [3]

b. Desventajas de SNMP

La primera deficiencia de SNMP en su versión original y corregida mayoritariamente en sus versiones posteriores, es que carece de autenticación, lo cual supone una alta vulnerabilidad a varias cuestiones de seguridad, como por ejemplo modificación de información por parte de algún intruso que ha accedido a la red, alteración de la secuencia de mensajes.

La solución a este problema es sencilla y se ha incorporado en la nueva versión SNMPv2 y reforzada en SNMPv3. Básicamente se han añadido mecanismos para resolver:

- Privacidad de los datos, la información que va por la red puede ser cifrada con un algoritmo de clave secreta CBC-DES[1] (Cipher Block Chaining-Data Encryption Standard).
- Autenticación, se utilizan claves por usuario, y los mensajes van acompañados de huellas digitales generadas con una función hash (MD5[2] o SHA[3]) previniendo él envió de información falsa por la red.
- Control de acceso, que restringe el acceso a ciertas variables a determinados usuarios que puedan hacer caer la red.
- Validez temporal y protección de repetición limitada, utiliza relojes sincronizados y una ventana de 150 segundos con chequeo de secuencia, permitiendo proteger un mensaje de un determinado retraso e impidiendo la repetición del mismo.

[1] **CBC-DES:** (Cipher Block Chaining-Data Encryption Standard), conocido también como DES-56. Algoritmo para la encriptación de datos de clave 56-bits, utiliza un cifrado simétrico de bloques.

[2] **MD5:** (Message-Digest algorithm 5), función hash criptográfica de 128-bits comúnmente utilizado para verificar la integridad de los archivos. [6]

[3] **SHA:** (Secure Hash Algorithm) Función hash criptográfica utilizado para aplicaciones de seguridad de uso común y protocolos verificando la integridad de los archivos.

El mayor problema de SNMP, es que se considera tan simple que la información está poco organizada, lo que no lo hace muy acertado para gestionar las grandes redes de la actualidad. Esto se debe en gran parte a que SNMP se creó como un protocolo provisional y no ha sido sustituido por otro de entidad. De nuevo este problema se ha solucionado con la nueva versión SNMPv2 que permite una separación de variables con más detalle, incluyendo estructuras de datos para hacer más fácil su manejo. Además SNMPv2 incluye dos nuevas PDUs (Protocol Data Unit) orientadas a la manipulación de objetos en tablas.

Otro problema que denota SNMP es que la consulta sistemática de los gestores, es más habitual que la emisión espontánea de datos por parte de los agentes cuando surgen problemas, SNMP es un protocolo que consume un considerable ancho de banda, lo cual limita su utilización en entornos de red muy extendidos. [2]

1.6.6.1.3 Ventajas y Desventajas de CMIP

a. Ventajas de CMIP

El principal beneficio que aporta el protocolo CMIP, es que no sólo se puede enviar información de gestión de o hacia un terminal, sino que es posible desarrollar tareas que serían imposibles bajo SNMP. Por ejemplo, si un terminal no puede encontrar un servidor de ficheros en un tiempo predeterminado, CMIP notifica el evento al personal adecuado. En SNMP el usuario tendría que guardar el número de intentos de acceso al servidor mientras que en CMIP de esto se encarga el propio protocolo.
CMIP soluciona varios de los fallos de SNMP. Por ejemplo, tiene incluidos dispositivos de gestión de la seguridad que soportan autorizaciones, control de acceso, contraseñas. Como resultado de la seguridad que de por sí proporciona CMIP no necesita de posteriores actualizaciones.

Otra ventaja de CMIP es que haya sido creado no sólo por gobiernos sino también por grandes empresas, en los que puede tener en el futuro un mercado fiel.

También el protocolo CMIP puesto que trabaja en modo conectado en vez de mediante sondeo secuencia como lo hace SNMP, permite optimizar el tráfico.

b. Desventajas de CMIP

Si todo lo dicho hace a CMIP tan bueno, uno puede preguntarse: ¿por qué no se usa? La respuesta es que CMIP significa también desventajas: CMIP requiere 10 veces más recursos de red que SNMP. En otras palabras, muy pocas redes de la actualidad son capaces de soportar una implementación completa de CMIP sin grandes modificaciones en la red (muchísima más memoria y nuevos protocolos de agente).

Involucrarse en implementar una red con CMIP apunta costos demasiado elevados, tanto a niveles hardware como software.

Otro problema de CMIP, es su dificultad de programación, existe tal cantidad de variables que sólo programadores muy habilidosos son capaces de aprovechar todo su potencial. Por todo lo anterior mucha gente piensa que CMIP está destinado al fracaso.

La única solución es disminuir el tamaño de CMIP cambiando sus especificaciones. Así han aparecido varios protocolos que funcionan con la base de CMIP con menos recursos, pero todavía no ha llegado el momento de prescindir del tan extendido SNMP.

1.6.6.1.4 Funcionamiento de SNMP

Un sistema puede operar exclusivamente como gestor o como agente, o bien puede desempeñar ambas funciones simultáneamente. Por consiguiente el protocolo SNMP funciona según la arquitectura cliente servidor distribuida y habitualmente usa servicios no orientados a la conexión a través del protocolo UDP aunque puede trabajar bajo varios protocolos de transporte.

La parte servidora de SNMP consiste en un software SNMP gestor, responsable del sondeo de los agentes SNMP para la obtención de información específica y del envío de peticiones a dichos agentes solicitando la modificación de un determinado valor relativo a su configuración. Es decir, son los elementos del sistema de gestión ubicados en la plataforma de gestión centralizada de red, que interaccionan con los operadores humanos y desencadenan las acciones necesarias para llevar a cabo las tareas por ellos invocadas o programadas.

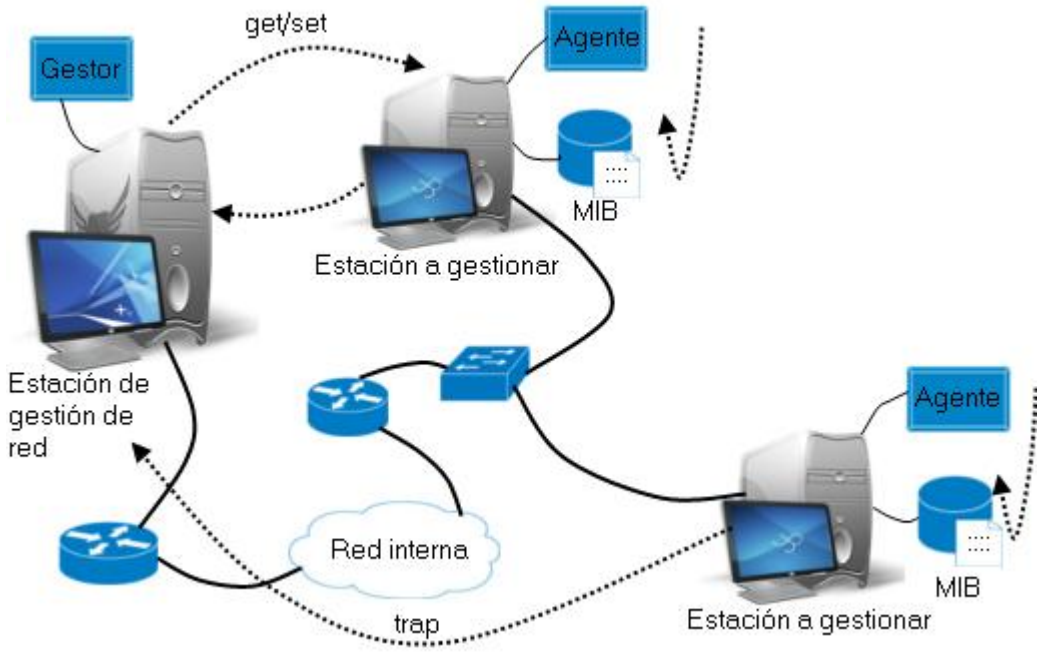


Figura 1.4 Esquema de una red gestionada con SNMP

La parte cliente de SNMP consiste en un software SNMP agente y una base de datos con información de gestión o MIB. Los agentes SNMP reciben peticiones y reportan información a los gestores SNMP para la comunidad a la que pertenecen; siendo una comunidad, un dominio administrativo de agentes y gestores SNMP. Es decir, son los elementos del sistema de gestión ubicados en cada uno de los dispositivos a gestionar, e invocados por el gestor de la red.

El principio de funcionamiento reside, por consiguiente, en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada dispositivo gestionado información acerca de su estado y su configuración. El gestor pide al agente, a través del protocolo SNMP, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento. Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones (traps) que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia. [2]

1.6.6.1.5 Operaciones soportadas por la información de gestión

El SNMP modela las funciones del agente de gestión con lecturas (get) o escrituras (set) de variables. Esta estrategia posee al menos dos consecuencias positivas:

- Limita el número esencial de funciones de gestión realizadas por agente de gestión a dos.
- Evita introducir el soporte de comandos de gestión imperativos en la definición de protocolo.

La estrategia plantea que la monitorización del estado de la red se puede basar a cualquier nivel de detalle en el sondeo (poll) de la información apropiada en la parte de los centros de monitorización.

1.6.6.1.6 Operaciones entre agentes y gestores

Un agente SNMP opera en cada equipo administrado, su función es obtener constantemente información del nodo administrado que el NMS le puede solicitar. Los tipos de PDU que el NMS utiliza para recabar o enviar la información son las siguientes.

- **GetRequest:** Se utiliza para solicitar los valores de una o más variables MIB.
- **GetNextRequest:** Es empleado para leer valores en forma secuencial. Se utiliza generalmente para leer una tabla de valores. Por ejemplo, después de obtener la primera fila con el mensaje GetRequest, los mensajes GetNextRequest se utilizan para obtener los datos de las filas restantes.
- **GetBulkRequest:** Solicita bloques grandes de datos, como por ejemplo varias filas de una tabla.
- **GetResponse:** Este mensaje es la respuesta a GetRequest, GetNextRequest o SetRequest.
- **SetRequest:** Sirve para actualizar, o bien configurar, uno o más valores del MIB.
- **InformRequest:** Comunicación entre gestores SNMP.
- **Trap:** Son mensajes no solicitados que son enviados al NMS por un agente SNMP. Se utilizan para reportar eventos inesperados, como por ejemplo un reinicio por software o hardware, un enlace caído, fallas en un disco duro, fuente de poder, etc.

Las operaciones GetBulkRequest e InformRequest están disponibles desde SNMPv2.

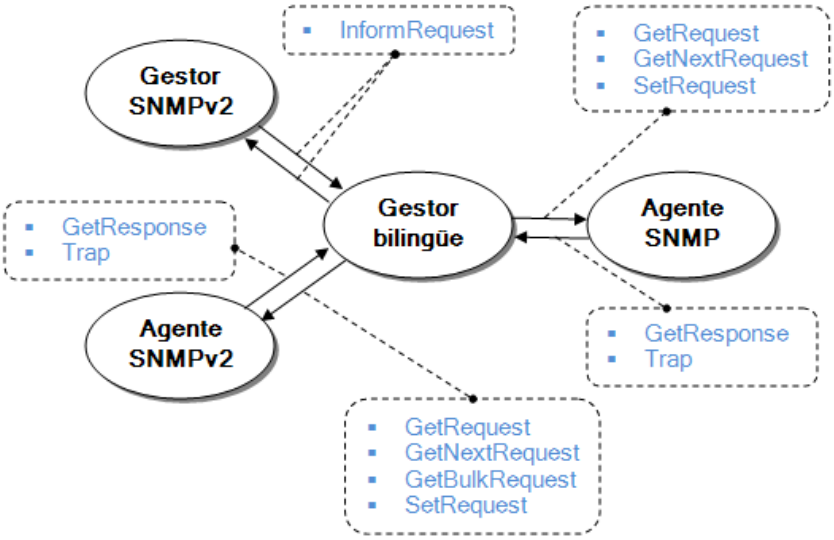


Figura 1.5 Interacción entre agentes y gestores SNMP

En conclusión el accionar de las operaciones es simple.

- Se puede leer u obtener una variable o una lista de variables de un MIB con un mensaje get.
- Es posible acceder a una tabla entera de variables MIB, con el mensaje GetNext.
- Se puede configurar un parámetro con la instrucción set.
- Un nodo puede reportar automáticamente un evento que represente un problema con la instrucción trap.

1.6.6.1.7 Versiones de SNMP

Existen tres versiones de SNMP las cuales veremos a continuación:

a. **SNMPv1:** Representa la primera definición e implementación del protocolo SNMP creado en 1988, definidas en las RFC 1155, 1157 y 1212 del IETF (Internet Engineering Task Force). El cual emplea seguridad basado en nombres de comunidad y perfiles de acceso. Se denomina comunidad al mecanismo de autenticación entre un conjunto de gestores y agentes a los cuales se les asigna nombres para relacionarlos, de tal forma

que este nombre junto con cierta información adicional sirva para validar un mensaje SNMP y al emisor. Los perfiles de acceso se manejan mediante vistas[4] y modos de acceso. Siendo la primera versión, presentaba inconvenientes tanto en seguridad como transferencia de grandes bloques de datos. Dependiendo el tipo de operación pueden tener cinco tipos de PDU: GetRequest, GetNextRequest, GetResponse, SetRequest, Traps.

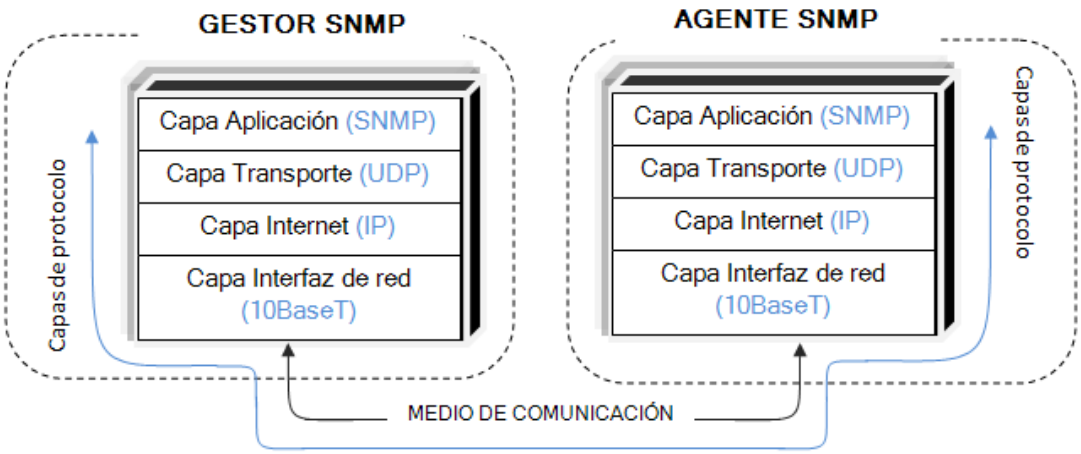


Figura 1.6 Protocolo SNMP intercambio información entre dispositivos de red

Al existir ciertos dispositivos como módems y puentes que no implementaban SNMP, se concibe el concepto de proxy, en el cual el agente SNMP actúa como un proxy para uno o más dispositivos.

Entre un gestor y un agente proxy se usan protocolos estándares, y entre el agente proxy y los dispositivos administrados se usan protocolos propietarios. El proxy asume el rol de un agente con respecto al gestor, y actúa como gestor para los dispositivos administrados.

[4] **Vistas:** Las vistas son una agrupación de determinados objetos de las MIB a los que se les puede añadir uno de los siguientes modos de acceso: solo lectura (read only), solo escritura (write only), lectura-escritura (read-write) o notify. [7]

Una de las principales funciones de un agente proxy es la conversión de protocolos mediante métodos de mapeo[5] o de encapsulamiento[6].

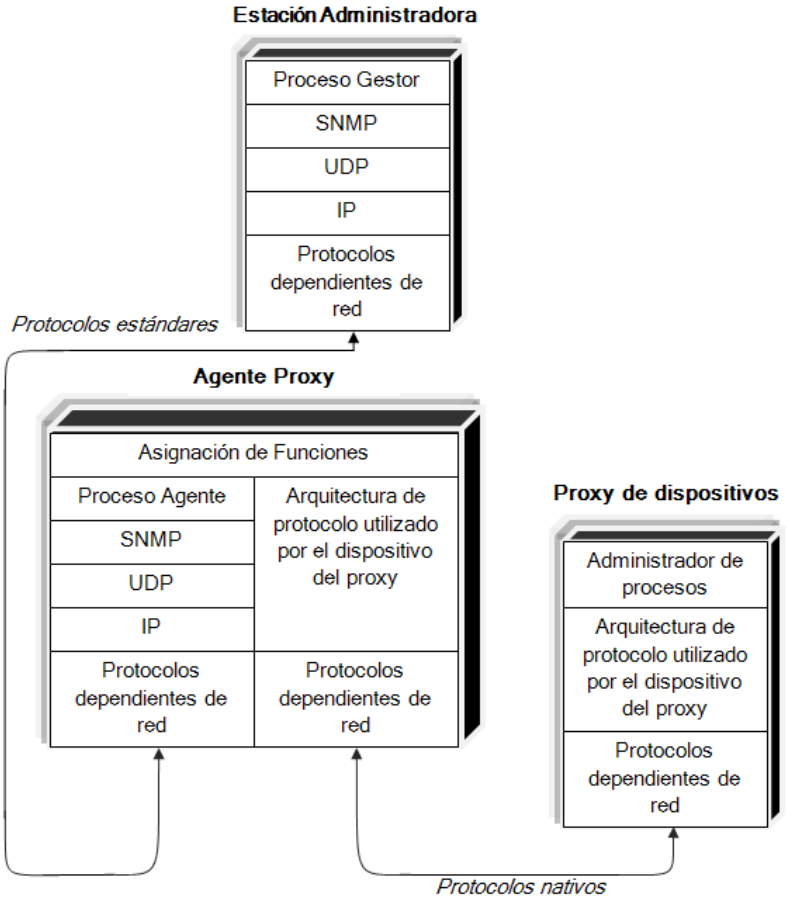


Figura 1.7 Agente SNMP actuando como proxy

b. SNMPv2: Apareció en 1992, definidas en las RFC 1441-1452. Se enfocó principalmente en resolver los problemas de su antecesora en cuestiones de seguridad y transferencia de grandes bloques de datos. Sin embargo solo se resolvió satisfactoriamente el problema de optimización de la transferencia de datos; dejando la seguridad sin cambios, la que se manejaba por medio de comunidades y perfiles de acceso.

[5] **Mapeo:** Acción que permite que una aplicación pueda acceder a un determinado elemento de manera dinámica.

[6] **Encapsulamiento:** Envió de datos de un dispositivo a otro dentro de una red, la que envuelve los datos con la información de protocolo necesaria antes de transitar por la red realizando todo un mecanismo de envío-recepción según el modelo OSI.

Tiene muchas características en común con su antecesora, siendo sus principales mejoras la adición de características de SMI (en colecciones de datos) y la introducción de nuevas operaciones PDU como GetBulkRequest la que ayuda a mejorar la eficiencia en el intercambio de información de gestión, la razón es que GetBulkRequest permite el intercambio de grandes cantidades de información en una sola petición por parte del gestor. Otra PDU añadida es InformRequest la que tiene como función el intercambio de información entre gestores de red. También se introduce la PDU ReportRequest para que el agente envíe de forma espontánea excepciones y errores de protocolo. Cabe destacar que para este momento SNMPv2 tiene soporte de comunicación entre gestores y además es bilingüe[7].

En 1995 apareció una revisión de SNMPv2, denominada SNMPv2c definidas en las RFC 1901-1908, donde la "c" indica que se mantiene el sencillo pero inseguro mecanismo de seguridad basado en comunidades y añade mejoras en configuraciones más sencillas y una mayor modularidad.

c. **SNMPv3:** Representa la última versión de SNMP la que aparece en 1997 y definida en las RFC 1902-1908, 2271-2275, 3410-3415; el cual surge para resolver problemas pendientes de las versiones anteriores.
SNMPv3 reutiliza el trabajo existente en SNMPv1 y SNMPv2 no intenta reemplazarlo, más bien añade una arquitectura de gestión, un nuevo formato de mensaje SNMP y refuerza prestaciones de seguridad, incluyendo autenticación[8] e integridad[9], encriptación[10], y control de acceso; y de administración de protocolo, con una mayor modularidad y

[7] **Bilingüe:** Que tiene soporte dual de administración o sea el gestor bilingüe es compatible con las dos versiones de SNMP y se comunica con el agente usando la versión adecuada de SNMP.

[8] **Autenticación:** Determina que el mensaje proviene de una fuente valida.

[9] **Integridad:** Asegura que un paquete de datos no se ha modificado mientras viajaba por la red.

[10] **Encriptación:** Asegura que una fuente no autorizada no pueda leer el contenido de los paquetes de datos.

la posibilidad de configuración remota; pero no contempla la protección frente a denegación de servicio y análisis del tráfico.

La arquitectura modular que presenta tiene la ventaja de actualizar cada módulo por separado (los que interaccionan entre sí para proporcionar servicios), sin tener la necesidad de modificar el estándar por completo.

En cuanto a las capacidades de seguridad se definen dos modelos.
El modelo de seguridad basado en el usuario o USM (User-based Security Model) proporciona funciones de autenticación y privacidad; operando a nivel de mensaje. El mecanismo de autenticación en USM asegura que un mensaje recibido fue, de hecho, transmitido por la entidad indicada en el campo correspondiente a la fuente en la cabecera del mensaje; y además, que el mensaje no fue alterado durante su tránsito y que no fue retardado artificialmente o repetido.

El modelo de control de acceso basado en vistas o VACM (View-based Access Control Model) determina el acceso de una entidad a ciertos objetos de una MIB; para acceder, consultar y configurar determinada información de gestión. La política de control de acceso consiste básicamente en una tabla que detalla los privilegios de acceso para los distintos gestores autorizados.

Cabe mencionar que, la autenticación es realizada por usuario, el control de acceso es realizado por grupos, donde un grupo podría ser un conjunto de usuarios.

1.6.6.2 Estructura SMI

Para entender cómo trabaja SMI es necesario detallar que el protocolo SNMP es el que establece la comunicación gestor-agente; sin embargo para poder acceder a los recursos que controla el agente se hace uso de la MIB la que contiene información estandarizada del objeto gestionado, a estos objetos es necesario definirlos lo cual se lo hace por medio de ASN.1, la misma que es necesaria para tener una representación de datos común para el intercambio entre sistemas.

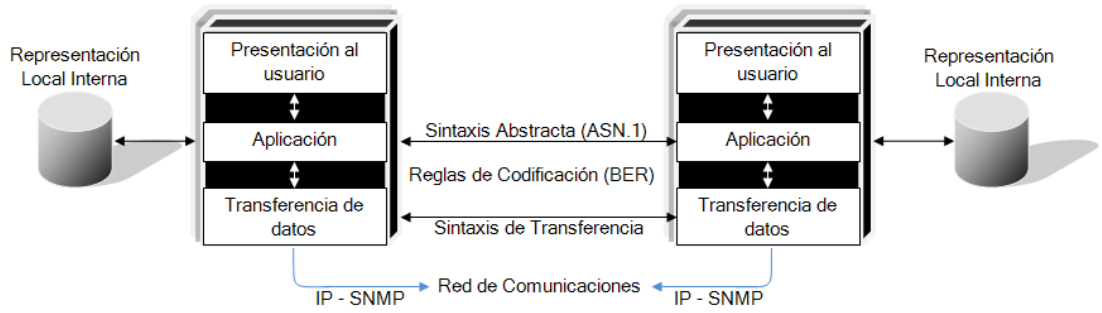


Figura 1.8 Intercambio de información, estructurada mediante SMI

1.6.6.3 MIB

MIB (Management Information Base) es un tipo de base de datos lógica que contiene información de gestión de red local mostrada de manera jerárquica, estructurada en forma de árbol, la que reside en cada uno de los agentes.

Un gestor puede supervisar los dispositivos de una red leyendo los valores de los objetos en la MIB y puede controlar el recurso en ese dispositivo modificando esos valores. Para que la MIB sirva a las necesidades de un sistema de administración de red, este debería conocer ciertos objetivos:

- El objeto u objetos utilizados para representar un recurso particular debería ser el mismo en cada sistema: Este punto se refiere a la definición de objetos y la estructura de estos objetos en la MIB.

- Un esquema común para la representación debería ser utilizado para soporte de interoperabilidad: Se refiere a la definición de una estructura de información administrada SMI (Structure of Management Information).

Los objetos de una MIB se definen usando un subconjunto del ASN.1, la versión 2 de SMI; que simplemente proporciona un sistema de reglas formales para describir la estructura de los objetos que son independientes de técnicas de codificación quitando las ambigüedades existentes.

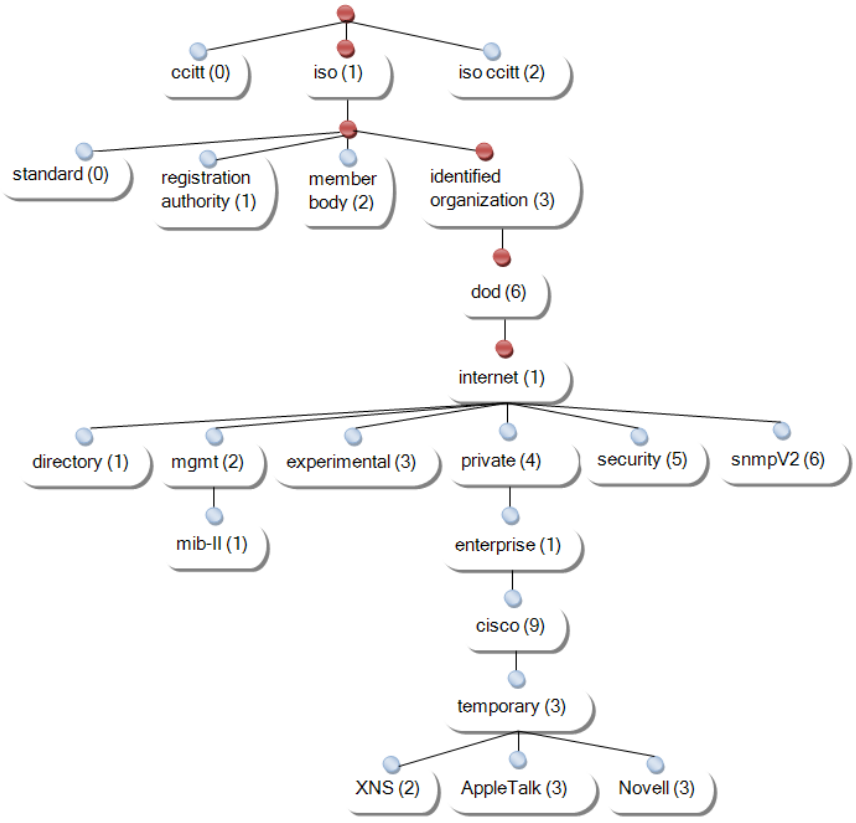


Figura 1.9 El árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones

Los identificadores de los objetos en la parte superior pertenecen a organizaciones estándares, mientras los ubicados en la parte inferior son de organizaciones asociadas. Los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama experimental.

Las MIB’s suelen ser modificadas cada cierto tiempo para añadir nuevas funcionalidades, eliminar ambigüedades y arreglar fallos.

Existen distintos tipos de MIB cada uno con una distinta funcionalidad a continuación se presentan las más representativas.

- Los estándares:
  - **MIB I**: Definida en el RFC 1156.
  - **MIB II**: Definida en el RFC 1213, para gestión de redes de internet basadas en TCP/IP.
- Las experimentales: grupos que se encuentran en la fase de desarrollo.
- Las privadas: información específica de fabricantes de equipos para equipos específicos.

CAPÍTULO 2. ESTADO ACTUAL DE LA RED LAN

En este capítulo, se describirá la situación actual de la red LAN de la Administración Zonal Norte "Eugenio Espejo". Toda la información obtenida fue proporcionada por el personal técnico encargado de la administración de la red de la Institución, así como personal administrativo en áreas adyacentes. La presente etapa específica las características físicas, técnicas que componen la red así como características lógicas.

El objetivo del levantamiento de esta información, es conocer la situación que presenta la Institución; la información que se recoja es de gran utilidad en cuanto en ella se determina requerimientos y se observa las falencias que existan entorno a la gestión de los recursos de la red; esta información se complementará con un sondeo de tráfico de red, el cual servirá de base comparativa en capítulos posteriores.

2.1 UBICACIÓN

La Administración Zonal Norte "Eugenio Espejo" del Distrito Metropolitano de Quito, está ubicada en la Avenida Amazonas 4532 y Pereira. La Figura 2.1, muestra su ubicación.

Figura 2.1 Vista Satelital de la Administración Zonal Norte "Eugenio Espejo" [8]

El objetivo que persigue la Institución es “Garantizar los derechos ciudadanos y el acceso a la cultura y al deporte. Planificar el desarrollo integral y garantizar la participación ciudadana. Garantizar la seguridad ciudadana. Establecer un sistema ágil y seguro de movilidad y transporte. Invertir en espacios públicos y obra pública. Rediseñar el gobierno metropolitano y fortalecer la formación - capacitación del servicio civil.” [9]

El enfoque que pretende es “Promover una ciudadanía y organización social activa que accede con equidad e inclusión al arte, la cultura, el deporte, la recreación a prácticas y saberes ancestrales, a las tecnologías de la comunicación, entre otros.” [9]

2.2 ANTECEDENTES

Actualmente la Administración Zonal Norte “Eugenio Espejo”, se encuentra bajo la administración del Arquitecto Oswaldo Granda Páez, el mismo que se encuentra en funciones desde comienzos del año 2010 con un nombramiento de libre remoción, el tiempo que se halla trabajando conjuntamente con otros Administradores Zonales y con la Alcaldía.

Algunas de las funciones principales que realiza esta Administración Zonal están destinadas a:

- Planificar, organizar, ejecutar, controlar, fiscalizar y evaluar proyectos de desarrollo social, económico y territorial en la jurisdicción zonal integrando la participación ciudadana.
- Administrar los recursos humanos, materiales, financieros y tecnológicos para una adecuada gestión en procura de la satisfacción de las necesidades de la comunidad de la zona.
- Coordinar con las Secretarias y Direcciones y Empresas Metropolitanas las actividades que permitan mejorar el servicio, con entrega oportuna, de calidad y de alto valor agregado. [10] (Más sobre las funciones en Anexo B)

La Administración Zonal está organizada en diferentes dependencias y departamentos los cuales trabajan de manera sistemática en proyectos de gran relevancia, permitiendo enfocar soluciones oportunas para las problemáticas presentes.

Con el fin de promover nuevas y mejores tecnologías libres que facilitan su uso y mejoramiento sin restricciones, la Institución ha enfocado esfuerzos en acoger al software libre como una alternativa viable para satisfacer sus necesidades tecnológicas; por tal motivo al demandar mejoras tangibles en el gestionamiento de la red se está procurando analizar adecuadamente las mejores opciones a seguir y efectivizar su uso.

La misión de la Administración Zonal es de "Ser el brazo operativo del gobierno local eficiente y democrático, que ejerce control y vela por el mantenimiento y desarrollo del espacio urbano, las edificaciones y que preserva el ambiente. Promotor del desarrollo humano y económico sustentable y de la participación ciudadana, respetando su diversidad cultural y social". [10]

La infraestructura de red con la que efectúan sus operaciones es mixta ya que manejan una red cableada por par trenzado, así como enlaces por medio de fibra óptica, las mismas que poseen un esquema topológico físico en doble anillo, incluso el mismo esquema se aplica con las diferentes Unidades Administrativas ubicadas desde la Plaza de Santo Domingo hasta las proximidades de la Avenida Patria.

Debido al surgimiento de problemas como escalabilidad, seguridad y adecuaciones físicas; el personal encargado ha optado por trasladar parte del cuarto de telecomunicaciones a un lugar más apropiado, el cual con el tiempo alojará todos los dispositivos.

2.3 ESTRUCTURA ORGÁNICA

En la Figura 2.2, se ilustra la Estructura Orgánica de la Administración Zonal Norte "Eugenio Espejo". (Detalles Estructura Orgánica, Organigrama Posicional Anexo C)

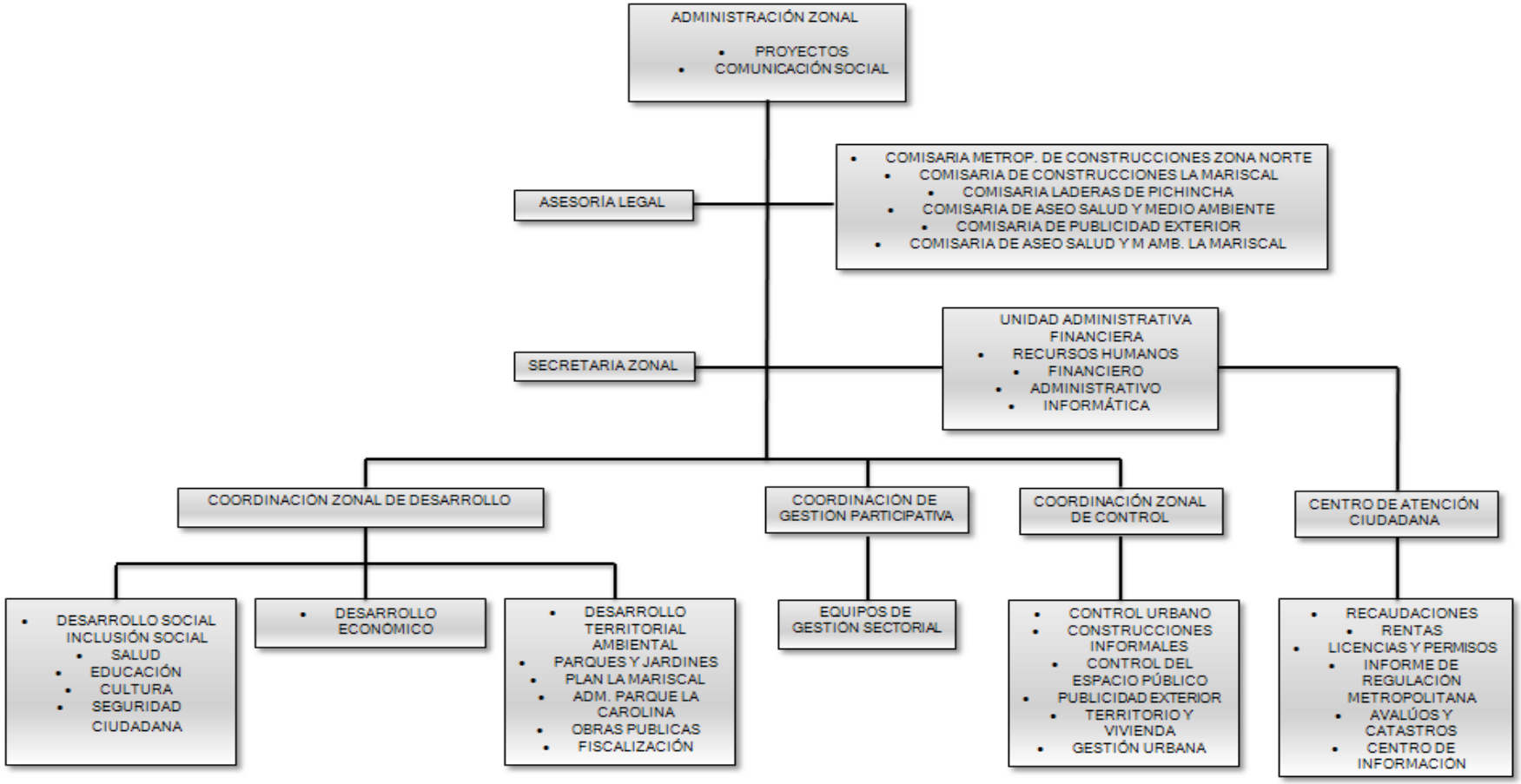


Figura 2.2 Estructura Orgánica de la Administración Zonal Norte "Eugenio Espejo"

El Departamento de Sistemas de la Institución tiene como función principal velar por el óptimo funcionamiento de los diferentes servicios que se albergan y concurren a sus instalaciones; llegando a ser responsables de aplicaciones como "Sistema de Actualizaciones", "Sistema de Instalación Remota de Imágenes", "Sistema de Gestión de Trámites", "Sistema de Control de Bienes", "Sistema de Bodegas", "Sistema de Denuncias", "Sistemas de Informes Técnicos" y "Sistema de Rótulos". Además ofrece soporte y mantenimiento de los diversos dispositivos que se encuentran funcionando en las distintas dependencias.

Existen también funciones que competen directamente con la administración diaria de la red local, la red inalámbrica, generación de perfiles, control de seguridad, registro de usuarios y reservaciones para acceso exclusivo a internet, mediante la gestión del software SQUID[11] el que maneja el acceso por medio de una relación IP-MAC Address.

Además también le compete precautelar el correcto funcionamiento de servicios como DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Web, Correo Electrónico, Internet, Intranet, FTP (File Transfer Protocol), Video Conferencias, OCS[12] (Office Communication Server), etc.

2.4 DESCRIPCIÓN DEL SISTEMA DE COMUNICACIONES

La Administración Zonal posee una infraestructura moderna en la cual converge el servicio de Telefonía IP, el mismo que entro en operación en muchas de las dependencias para reemplazar la obsoleta central PBX que poseían; la necesidad que obligo a este cambio fue estructurar líneas directas y extensiones antes concebidas en la central PBX y ahora migrando a IPPBX la que otorga una mejor administración de los servicios de voz y datos, así como manejo de rutas y remoción excesiva de

[11] **SQUID:** Proxy cache web para apoyo a http, https, ftp. Reduce el ancho de banda y mejora los tiempos de respuesta de almacenamiento en cache, reutiliza con más frecuencia las páginas web. Amplios controles de acceso, optimiza el flujo entre cliente y servidor ahorrando ancho de banda. [11]

[12] **OCS:** Plataforma de comunicaciones y colaboración unificada para uso corporativo, interconectada con Office y Exchange. El cliente de conexión a OCS es Microsoft Office Communicator. [12]

cableado; sin embargo, por inconvenientes logísticos y administrativos los servicios relacionados a esta tecnología se encuentran operando parcialmente.

Actualmente, se ha logrado trabajar de manera conjunta tanto con la antigua central PBX, como la nueva IPPBX, siendo esta última un objetivo a ser alcanzado totalmente para los primeros meses del año 2011 y reemplazando su modelo anterior.

De forma general la red de datos distribuye todos los servicios para que el usuario final acceda sin dificultad al servicio que este requiera, pudiendo ser desde correo electrónico hasta compartición de documentos o recursos de impresión. En la Figura 2.3, se ilustra el diagrama de red de la Administración Zonal enfocada de una manera global.

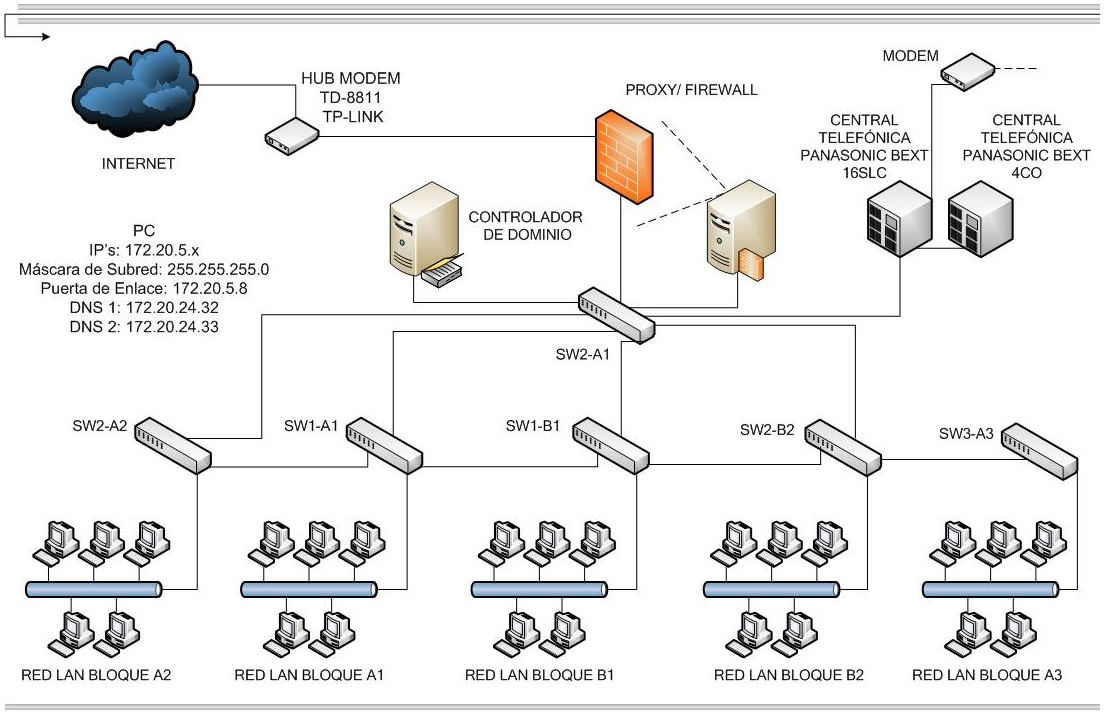


Figura 2.3 Diagrama de red Administración Zonal Norte "Eugenio Espejo"

2.4.1 SERVIDORES DE LA RED

Las comunicaciones que concurren en la Institución son gestionadas por el personal del departamento de informática en el cual se encuentran ubicados 6 servidores, uno dedicado exclusivamente para manejar el Sistema de Archivos el mismo que opera

para todos los Departamentos de la Institución, otro encargado del servidor y consola del antivirus, otro encargado del Directorio Activo.

Además, la red posee un servidor Proxy dedicado a controlar el tráfico web existente en cada uno de los departamentos; así mismo posee un servidor WSUS[13] (Windows Server Update Services) el que gestiona las distintas actualizaciones, parches de seguridad para los sistemas de la Institución; y un servidor de Aplicaciones que permite la instalación de imágenes remotamente.

En la Figura 2.4, muestra el esquema de interconexión que existe entre los servidores y los dispositivos de red para mantener conectada toda la red de la Institución. El tipo de cableado utilizado para la interconexión es de categoría 5e y 6a, al no existir un etiquetado adecuado en el área del rack, se dificulta la administración ya que no poseen un diagrama de red para soporte técnico sin embargo existe mayoritariamente un etiquetado adecuado para cada punto de red en los departamentos que diferencia voz y datos respectivamente.

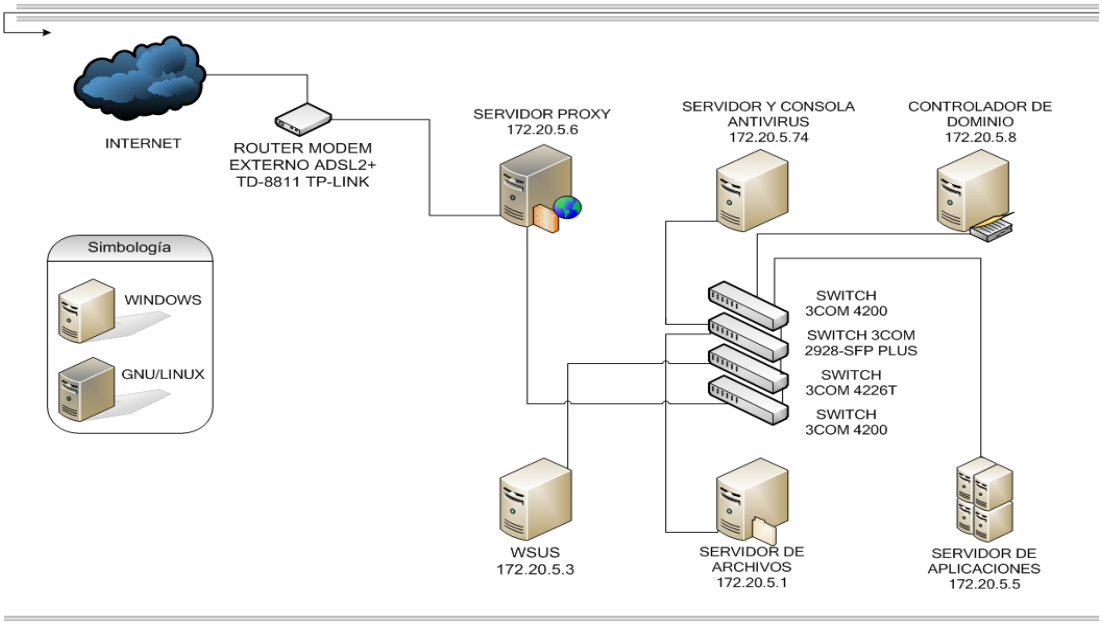


Figura 2.4 Interconexión de los distintos servidores de la Administración Zonal Norte "Eugenio Espejo"

[13] **WSUS:** Provee actualizaciones automáticas de seguridad pudiendo ser críticas, paquetes de servicio, drivers. Permite ahorro de ancho de banda, tiempo y espacio de almacenamiento ya que no se conecta a servidores externos sino locales.

Servidor	Software Base	Ubicación
Directorio Activo	Windows 2000 Server	Dpto. Sistemas Cuarto de Telecomunicaciones
Servidor y Consola de antivirus	Windows 2003 Server R2	Dpto. Sistemas Cuarto de Telecomunicaciones
Proxy	Centos 5	Dpto. Sistemas Cuarto de Telecomunicaciones
WSUS	Windows 2008 Server	Dpto. Sistemas Cuarto de Telecomunicaciones
Archivos	Windows 2003 Server R2	Dpto. Sistemas Cuarto de Telecomunicaciones
Aplicaciones	Windows 2003 Server R2	Dpto. Sistemas Cuarto de Telecomunicaciones

Tabla 2.1 Características de los servidores de la Administración Zonal Norte "Eugenio Espejo"

2.4.2 SERVICIOS DE RED

Los servicios que poseen están basados en la arquitectura TCP/IP implementados tanto bajo plataformas Windows como GNU/Linux [14]integrando dos entornos de trabajo muy demandados en la actualidad.

2.4.3 LA CONEXIÓN A INTERNET

Actualmente la Institución tiene un convenio con dos ISP (Internet Service Provider) uno contratado con la CNT (Corporación Nacional de Telecomunicaciones) la misma que provee dos enlaces; un enlace esta implementado sobre fibra óptica con una capacidad de 8Mbps, mientras que el otro esta implementado sobre cobre con una capacidad de 2Mbps; estos a su vez gestionan la mayor parte del tráfico existente. El otro proveedor que presta servicios es PuntoNet, el mismo que acoge minoritariamente la demanda, con un enlace de fibra óptica de 1Mbps. La Figura 2.5, muestra de manera general la interconexión existente con el proveedor de Internet.

[14] **GNU/Linux:** Término empleado para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux, que es usado con herramientas de sistema GNU. [13]

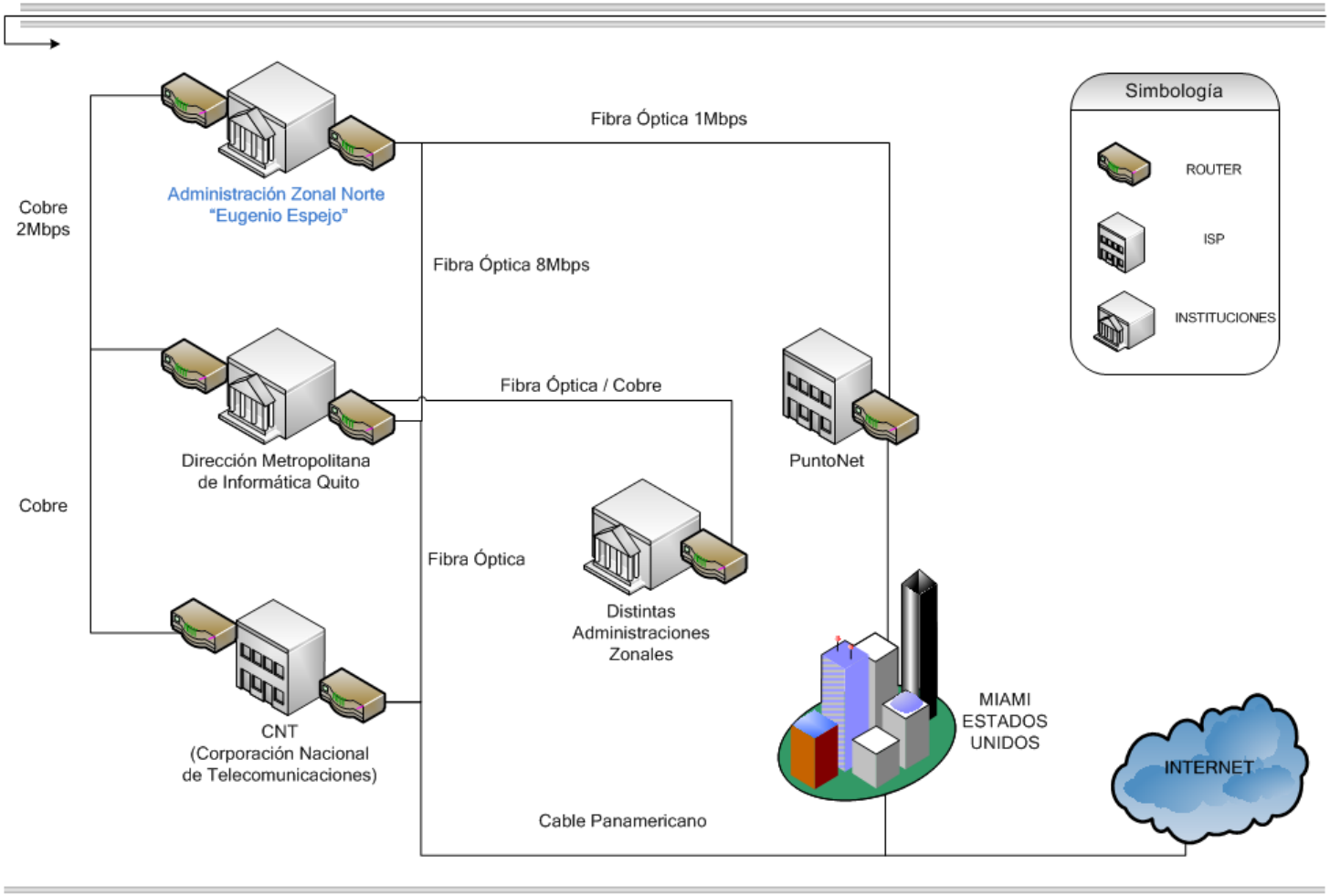


Figura 2.5 Esquema de conexión con el Proveedor de Internet

2.5 INFRAESTRUCTURA DE RED

2.5.1 DESCRIPCIÓN FÍSICA

Las instalaciones constan de una construcción mixta y está dividida en dos plantas. Las instalaciones proporcionan servicios de gran importancia para la municipalidad; en la Tabla 2.2, se mencionan los departamentos y dependencias que pertenecen a cada piso.

Piso	Departamento/Dirección
Primer Piso	Administrador, Coordinación Administrativa y de Servicios, Administración, Financiero, Sistemas, Recursos Humanos, Coordinación Desarrollo Comunitario y Participación Ciudadana, Avalúos y Catastros, Fiscalización, Comisaría de Construcciones, Jefatura de Salud, Obras Públicas, Educación y Cultura, Medio Ambiente, Inclusión Social, Parques y Jardines, Seguridad Ciudadana, Subprocuraduría, Coordinación Desarrollo Zonal.
Planta Baja	Balcón de Servicios, Legalizaciones y Construcciones, Coordinación de Gestión y Control, Gestión Urbana, Control de la Ciudad, Territorio y Vivienda, Trazado Vial, Secretaría General, Archivo, Control Espacio Público, Comisaría Salud Aseo y Ambiente, Comisaría Publicidad Exterior, Licencias.

Tabla 2.2 Departamentos y dependencias

Existen departamentos que es encuentran ubicados en las afueras de la Institución y que por motivos de complejidad y extensible capacidad que denota cada uno de ellos, no se tomaran en cuenta en la elaboración de este proyecto. Así se tiene departamentos que aunque su área administrativa, son casi de similar envergadura que la Administración Zonal Norte “Eugenio Espejo” pertenecen a esta Institución y no son nuevos ejes administrativos; los cuales son:

- Gerencia La Mariscal
- Administración Parque La Carolina
- Administración Canchas La Carolina
- Comisaría Laderas del Pichincha

2.5.2 RED CABLEADA

El sistema de cableado estructurado está constituido por cable de par trenzado sin apantallamiento UTP categoría 5e y 6a, este último permitiendo frecuencias de hasta 550 MHz y proveyendo transferencias de hasta 10GBits/s. El actual sistema de cableado da servicio a aproximadamente 200 puntos de voz y datos. Como anteriormente se indica existe una transición que se encuentra en condiciones intermedias de funcionamiento en el uso del nuevo sistema de voz sobre IP el cual operará totalmente en los primeros meses del 2011.

Luego de una supervisión a las distintas áreas de la Institución, se ha observado que existen algunos inconvenientes tanto en el cableado horizontal, vertical como en las áreas de trabajo; siendo estos los siguientes:

- En ciertas secciones del cableado el cable presenta torceduras las que según los estándares no están permitidas.
- En algunas estaciones de trabajo el cable de enlace (el que va desde el cajetín o toma de comunicaciones a la estación de trabajo) está elaborado manualmente y no presenta alguna certificación como lo sugiere el estándar.
- Algunos cajetines no poseen una nomenclatura clara o no están etiquetados.
- Existen en ciertos departamentos cables de enlaces puestos de manera inadecuada exponiéndolos a ser pisados.
- Mayoritariamente los departamentos que se encuentran en el bloque superior presentan puntos de red enrutados por las estructuras metálicas del edificio, exponiéndolos a encontrarse con otros tipos de cables como el del par telefónico y cables coaxiales. Este tipo de condiciones provoca el deterioro del cableado así como exponerlo a interferencias electromagnéticas.
- Ciertos departamentos no poseen las bandejas por las que extienden los puntos de red.

El cuarto de telecomunicaciones se encuentra ubicado en una parte del bloque superior del edificio, propiamente en el Departamento de Sistemas, dicho cuarto posee dimensiones de 3x4 metros, el que comparte su espacio físico como depósito

para equipos obsoletos, que necesitan reparación, o están siendo dados de baja; las existentes condiciones dificultan la administración tanto de equipos como puntos de red que convergen al cuarto. Dichas condiciones han provocado la construcción de un nuevo cuarto de telecomunicaciones que cumpla con las condiciones adecuadas; a la flecha está funcionando de manera parcial en un bloque distinto del edificio.

Gran parte del cableado estructurado está orientado al cuarto de telecomunicaciones del bloque superior; mientras que la restante parte del cableado, se orienta al nuevo cuarto de telecomunicaciones en el bloque inferior, en las cercanías del Parqueadero Interno que posee la Institución.

A continuación, se pondrá de manifiesto la situación existente tanto de hardware como de software por cada piso. Para lograr un mejor análisis de lo antes mencionado se ha dividido a cada piso en bloques, esto debido a la extensible capacidad que presenta la Institución.

2.5.3 PRIMER PISO (BLOQUE A1)

2.5.3.1 Descripción de la red

En este bloque se encuentran Departamentos como el Financiero, Administrativo, Coordinación Administrativa y de Servicios, Sistemas, Tesorería. En el presente bloque concretamente en el Departamento de Sistemas se encuentra ubicado el cuarto de telecomunicaciones, el mismo que posee un rack de Comunicaciones y además se encuentran alojados los distintos servidores; este departamento constituye eje fundamental de operaciones de la Administración Zonal. En la Figura 2.6, se presenta el diagrama de red.

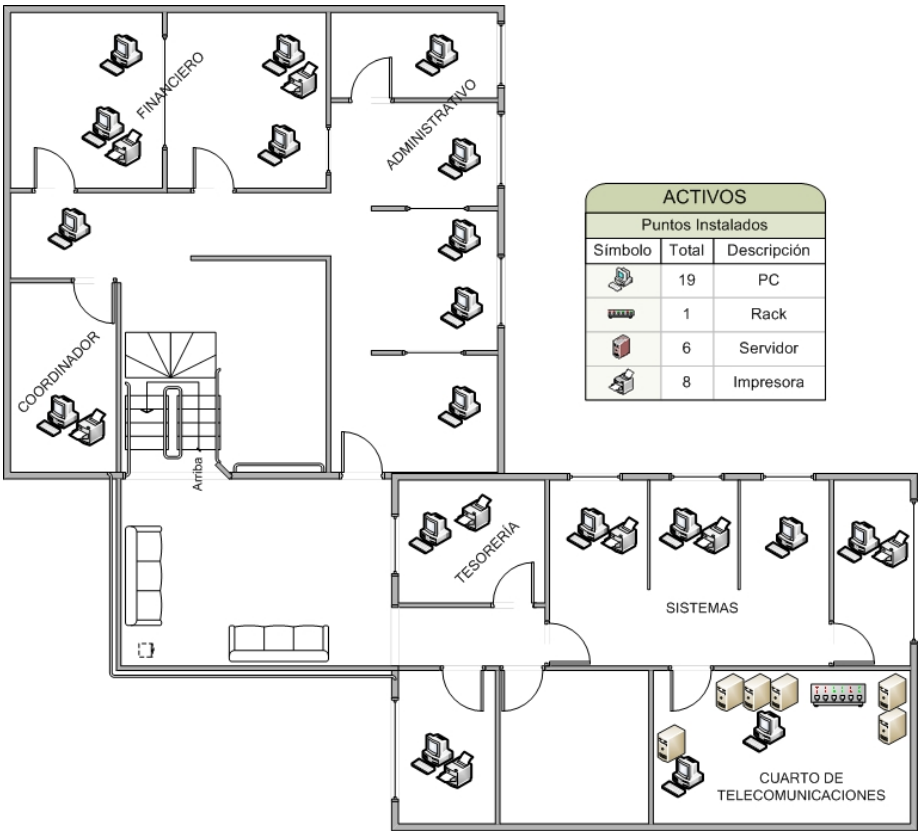


Figura 2.6 Diagrama de red Bloque A1

2.5.3.2 Equipos de red

En la Tabla 2.3, se detalla el número de equipos del Bloque A1.

Departamento	Usuarios de red	Pc	Impresoras	
			red	local
Financiero	5	5	1	1
Administrativo	6	6	-	-
Coordinación Administrativa y de Servicios	1	1	1	-
Sistemas	3	3	-	3
Tesorería	2	2	-	2
Total	17	17	2	6

Tabla 2.3 Equipos existentes en el Bloque A1

2.5.3.3 Equipos de interconexión

Los equipos de interconexión, se encuentran ubicados en el cuarto de telecomunicaciones, el que saldrá de funcionamiento en los primeros meses del 2011, para reubicarlo totalmente en un área adyacente al Parqueadero Interno así tenemos un rack de piso abierto. En la Tabla 2.4, se puede apreciar los equipos de interconexión existentes.

Marca	Tipo/Serie	Núm. equipos
3COM	Switch 4200	2
3COM	Switch 2928-SFP Plus	1
3COM	Switch 4226T	1
TP-Link	Router Modem Externo ADSL2+ TD-8811	1

Tabla 2.4 Equipos de interconexión existentes en el Bloque A1

2.5.4 PRIMER PISO (BLOQUE A2)

2.5.4.1 Descripción de la red

Este bloque contiene Departamentos como la Coordinación de Desarrollo Comunitario y Participación Ciudadana, Avalúos y Catastros, Recursos Humanos, Fiscalización, Unidad Especial Regula tu Barrio, Jefatura Zonal de Salud. En este bloque se encuentran departamentos que prestan servicios críticos a la comunidad como es Fiscalización, el mismo que vela por el cumplimiento de los cronogramas de trabajo y especificaciones técnicas de las obras contratadas, así como del uso de los fondos para el avance de las obras. La Figura 2.7, muestra el diagrama correspondiente a este bloque.

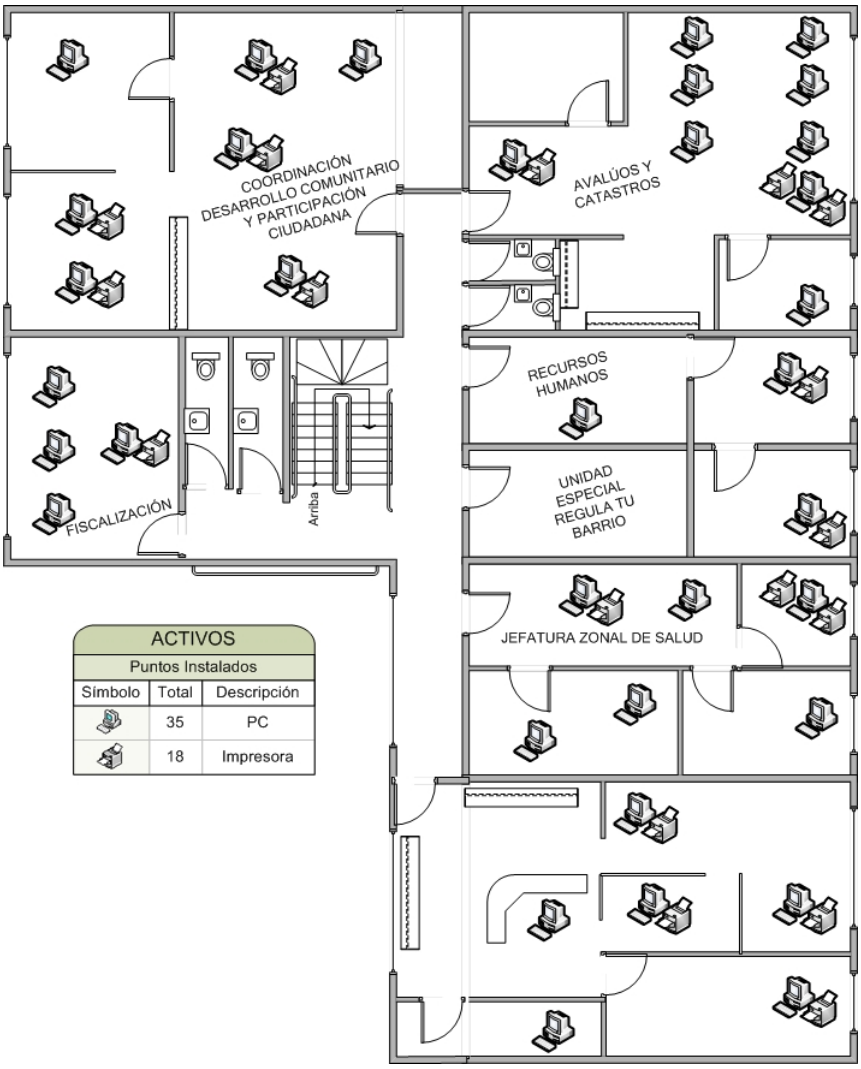


Figura 2.7 Diagrama de red Bloque A2

2.5.4.2 Equipos de red

En la Tabla 2.5, se detalla el número de equipos del Bloque A2.

Departamento	Usuarios de red	Pc	Impresoras	
			red	local
Coordinación de Desarrollo Comunitario y Participación Ciudadana	7	7	-	5
Avalúos y Catastros	9	9	1	2
Recursos	3	3	-	2

Humanos				
Fiscalización	4	4	1	-
Unidad Especial Regula tu Barrio	1	1	-	1
Jefatura Zonal de Salud	6	6	1	2
Inclusión	6	6	-	4
Total	36	36	3	16

Tabla 2.5 Equipos existentes en el Bloque A2

2.5.5 PRIMER PISO (BLOQUE A3)

2.5.5.1 Descripción de la red

Aquí se encuentra el Departamento del Administrador Zonal; así como también la Sala de Reuniones, Parques y Jardines, Seguridad Ciudadana, Subprocuraduría, la Asesoría de la Administración, Comunicación Social, Obras Públicas, Medio Ambiente, Educación y Cultura, Inclusión Social, Sala de Talleres.

El bloque concentra autoridades importantes como el Administrador, su Asesor entre las más importantes; cabe mencionar que el Departamento del Administrador Zonal es el único sitio que goza los servicios de Telefonía IP, que aunque no está operativo en el resto de departamentos, entrará en funcionamiento en pocos meses. La Figura 2.8, muestra el diagrama correspondiente a este bloque.

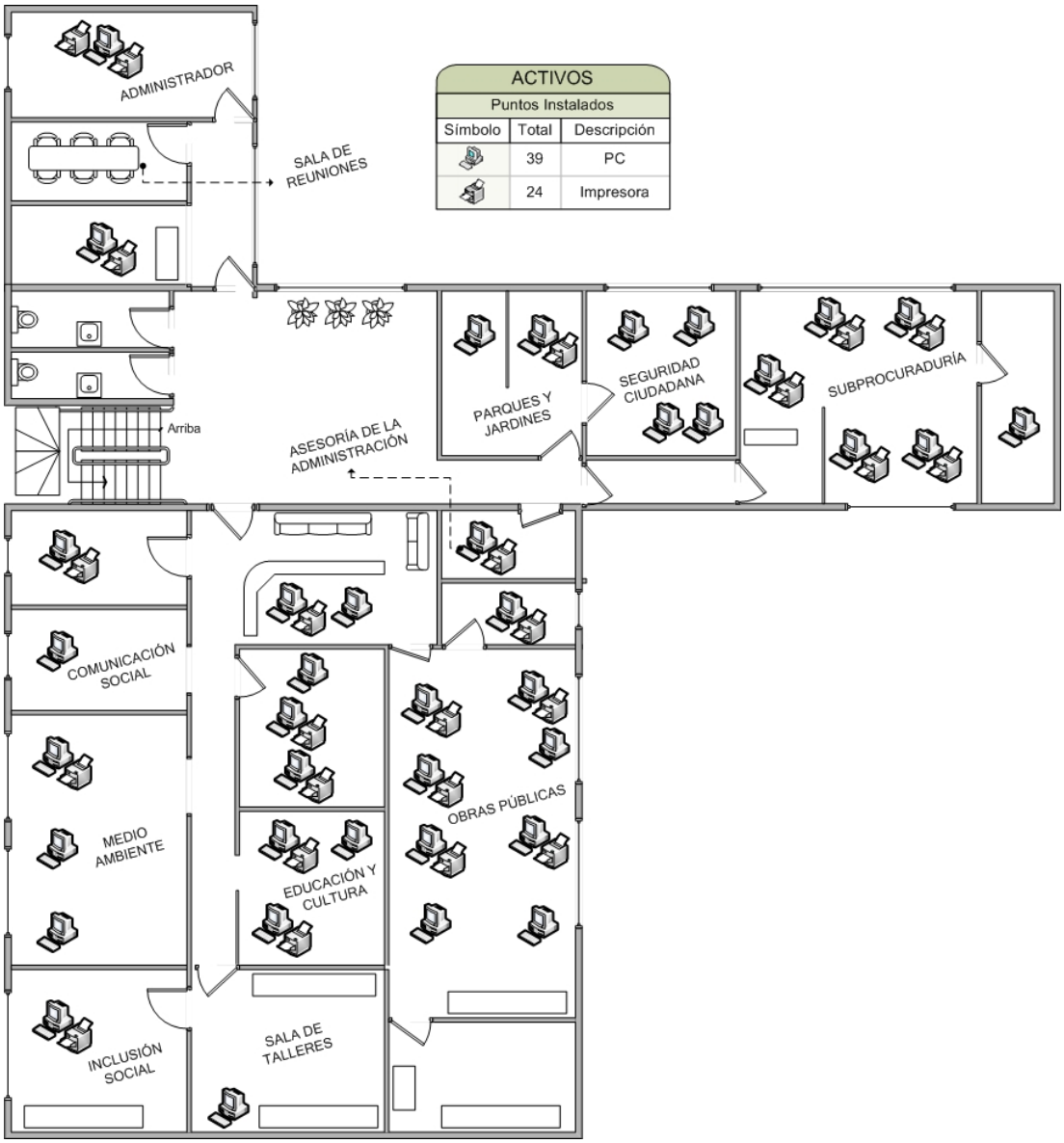


Figura 2.8 Diagrama de red Bloque A3

2.5.5.2 Equipos de red

En la Tabla 2.6, se detalla el número de equipos del Bloque A3.

Departamento	**Usuarios de red**	**Pc**	**Impresoras**	
			red	**local**
Administrador	2	2	1	2
Parques y Jardines	2	2	1	-
Seguridad Ciudadana	4	4	-	-

Subprocuraduría	6	6	1	4
Asesoría de la Administración	1	1	-	1
Comunicación Social	2	2	-	1
Obras Públicas	11	11	3	4
Medio Ambiente	3	3	1	-
Educación y Cultura	6	6	1	3
Inclusión Social	1	1	-	1
Sala de Talleres	1	1	-	-
Total	39	39	8	16

Tabla 2.6 Equipos existentes en el Bloque A3

En la sala de reuniones se efectúan ocasionalmente videoconferencias en las que intervienen los distintos Administradores Zonales, Alcalde, Concejales, Directores, entre otros. Los que dialogan y presentan propuestas sobre proyectos de interés colectivo para la municipalidad.

2.5.6 PLANTA BAJA (BLOQUE B1)

2.5.6.1 Descripción de la red

En este bloque concurren varios servicios, que tienen como representante a un delegado de su respectivo departamento, así esto se lo conoce como Balcón de Servicios, el mismo posee varias funciones como brindar asesoría para la obtención de permisos, certificaciones, realizar trámites catastrales, receptar y gestionar denuncias entre las funciones más principales. El conglomerado que abarca el Balcón de Servicios presenta falencias, en cuanto a los sistemas que maneja, ya que al presentar un sistema centralizado con la Dirección Metropolitana de Informática, se ven en la necesidad de establecer conexiones de varias sesiones por usuario, para proveer los servicios a los clientes que demandan la atención. Esta amplia demanda de sesiones por usuario, influye negativamente en la saturación de recursos de red, ocasionando cuelgues y desconexiones en los sistemas.

En este bloque, se encuentran Departamentos como Comisaría de Publicidad Exterior, Comisaría de Salud Aseo y Ambiente, Legalizaciones y Construcciones, Archivo, Balcón de Servicios, Territorio y Vivienda. La Figura 2.9, presenta el diagrama de red correspondiente.

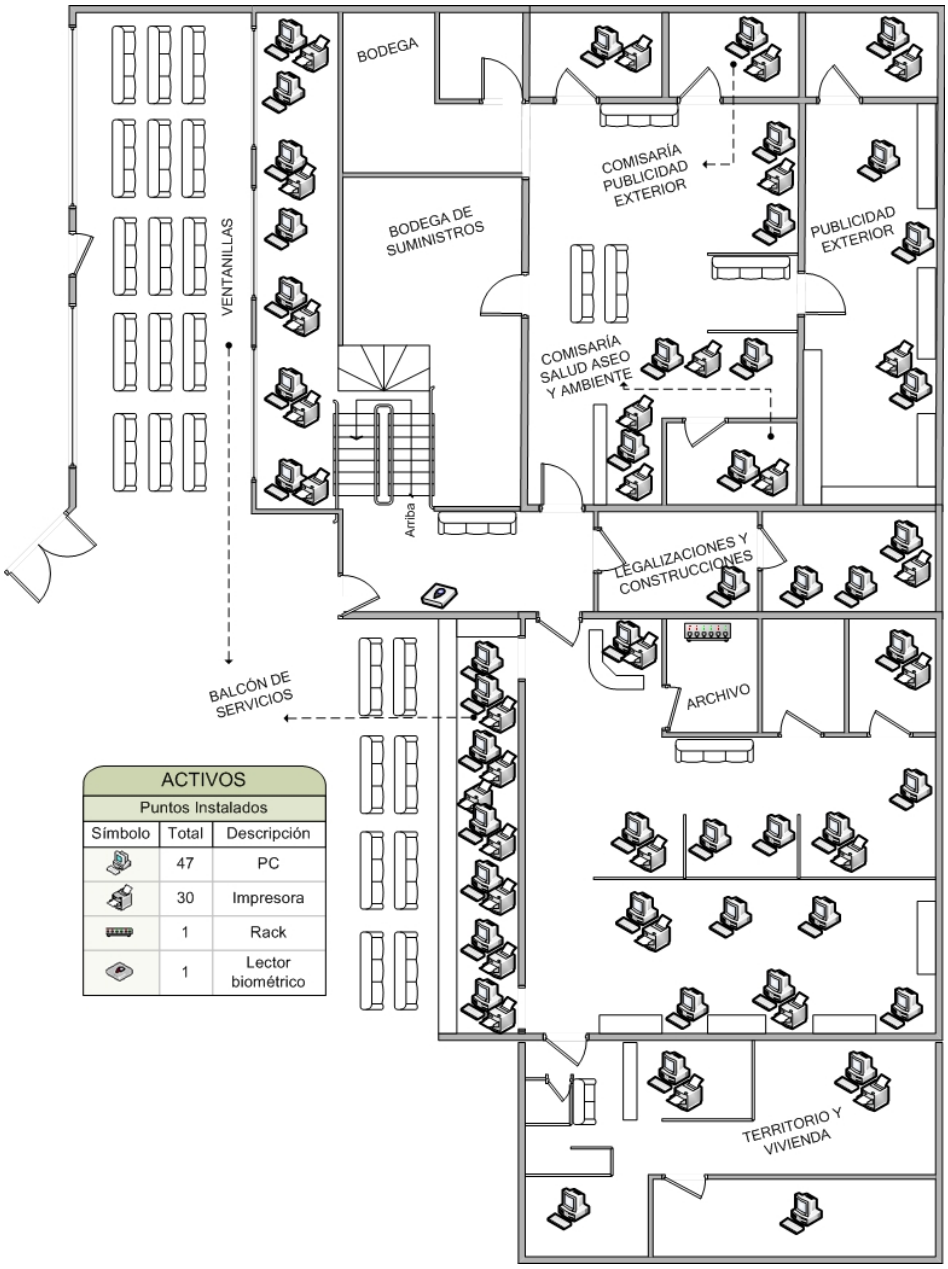


Figura 2.9 Diagrama de red Bloque B1

2.5.6.2 Equipos de red

En la Tabla 2.7, se detalla el número de equipos del Bloque B1.

Departamento	Usuarios de red	Pc	Impresoras	
			red	local
Comisaría Publicidad Exterior	10	10	-	7
Comisaría Salud Aseo y Ambiente	2	2	-	3
Legalizaciones y Construcciones	4	4	1	-
Archivo	13	13	4	2
Balcón de Servicios	14	14	12	-
Territorio y Vivienda	4	4	-	2
Total	47	47	16	14

Tabla 2.7 Equipos existentes en el Bloque B1

2.5.6.3 Equipos de interconexión

En este bloque los equipos de interconexión se encuentran ubicados en el área del Archivo. El rack de pared que facilita la comunicación de los departamentos se encuentra en un lugar accesible para cualquier persona y no presenta ninguna seguridad, como la que se obtiene al hacer uso de un rack de pared cerrado, además no existe un adecuado etiquetamiento, ni ordenamiento de los cables en sus organizadores. El rack contiene los siguientes equipos:

Marca	Tipo/Serie	Núm. equipos
Advantek	Switch ANS-24R	2

Tabla 2.8 Equipos de interconexión existentes en el Bloque B1

2.5.7 PLANTA BAJA (BLOQUE B2)

2.5.7.1 Descripción de la red

Este bloque contiene Departamentos como Secretaría General del Archivo, Balcón de Servicios, Rentas Municipales, Información y además existe una dependencia que aunque externa funciona dentro de las instalaciones que es el Centro de Servicio al Cliente de la EMMAP-QUITO.

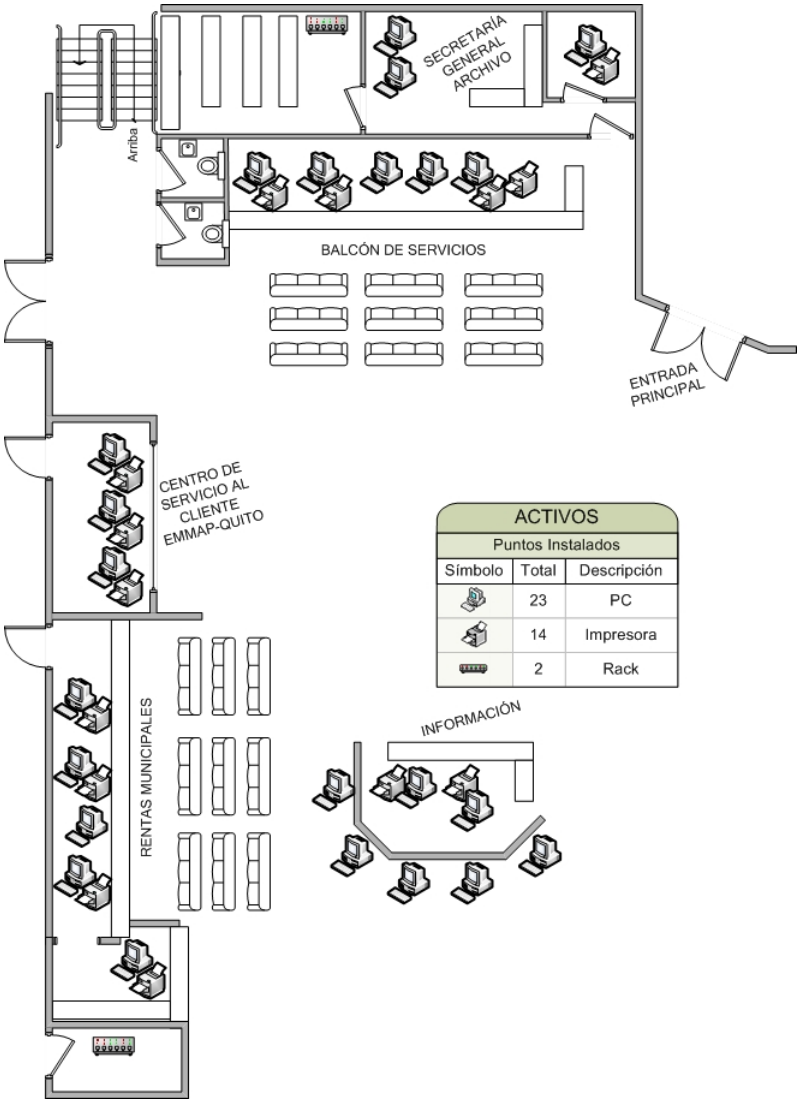


Figura 2.10 Diagrama de red Bloque B2

En la Tabla 2.9, se detalla el número de equipos del Bloque B2.

2.5.7.2 Equipos de red

Departamento	Usuarios de red	Pc	Impresoras	
			red	local
Secretaría General Archivo	4	3	-	1
Balcón de Servicios	10	5	4	-
Rentas Municipales	5	5	3	1
Información	2	2	-	2
Centro de Servicio al Cliente EMMAP-QUITO	3	3	-	3
Total	24	18	7	7

Tabla 2.9 Equipos existentes en el Bloque B2

2.5.7.3 Equipos de interconexión

Este bloque contiene dos racks, uno situado en el área de la Secretaría General del Archivo, el mismo que no presenta un adecuado etiquetado y la falta de un rack de pared cerrado lo hace inseguro; mientras que el otro está ubicado en un sitio adecuado para albergar al nuevo cuarto de telecomunicaciones, en el área posterior adyacente al Parqueadero Interno, el sitio designado para el rack de piso fue analizado con anterioridad por el personal encargado y aunque presenta mejores condiciones para su funcionamiento este aún no ha sido provisto de un sistema de enfriamiento y un entendible etiquetado.

Marca	Tipo/Serie	Núm. equipos
D-Link DES	Switch 1024D	2
D-Link DES	Switch 1024R+	1
D-Link DES	Switch 3226S	1
3COM	Switch 5500G-EI	2
3COM	Switch 4226T	1
Cisco	Router 800	1

Tabla 2.10 Equipos de interconexión existentes en el Bloque B2

2.6 ANÁLISIS DEL EQUIPAMIENTO ACTIVO Y PASIVO DEL DEPARTAMENTO DE SISTEMAS

2.6.1 DEPARTAMENTO DE SISTEMAS

El Departamento de Sistemas constituye la columna vertebral de la Institución, por ende, se debe tener en claro, que una gestión adecuada de los recursos existentes repercute enormemente en los servicios prestados; cabe distinguir que las personas involucradas en velar su óptimo funcionamiento, tienen en sus manos la posibilidad de analizar tecnologías adecuadas que incrementen la productividad de los servicios.

Entre las funciones principales que competen al Departamento de Sistemas están:

- Brindar soporte técnico y capacitación para el uso de software y hardware.
- Coordinar el mantenimiento preventivo y correctivo del hardware informático y de comunicaciones.
- Determinar requerimientos y necesidades de equipamiento y sistemas de información.
- Administrar eficientemente los recursos informáticos de la zona y la conexión con los servidores centrales. [10]

Para lograr un mejor entendimiento de la importancia de este Departamento, se efectuará una descripción de los equipos de comunicaciones que brindan servicios.

La Institución tiene a su disposición el uso de una planta eléctrica; la cual provee de energía cuando el suministro que proporciona la Empresa Eléctrica, sufre alguna anomalía. El fin que tiene la planta eléctrica, es proveer una continuidad en la atención a los clientes y en las operaciones corrientes que existen actualmente.

Cabe destacar que el cuarto de telecomunicaciones adicionalmente posee un UPS (Uninterruptible Power Supply) de 5kVA, el que asiste en funciones operativas a los

equipos críticos (servidores, routers, switch), para procurar una transición adecuada entre el corte de energía y la operatividad de la planta eléctrica.

La continuidad que presta la planta eléctrica, es activada de manera manual, la que al no existir una conectividad automática con un PLC (Programm Logic Control), se debe activar de forma manual, debiendo una persona encargada encender el generador a diesel de unos 75 kVA de marca SDMO, para lograr restablecer las operaciones.

Este respaldo de energía mantiene en funcionamiento a todos los departamentos que abarca la Institución, así como la mayoría de puntos de iluminación. Cada uno de los departamentos constituyen áreas concurrentes de servicios, que no pueden cesar funciones de forma inadvertida.

A continuación, se describirán los principales componentes de hardware y software de la Institución.

2.6.2 ANÁLISIS DE SOFTWARE Y MÓDULOS CORPORATIVOS

Las aplicaciones que la Institución ocupa y ofrece a los usuarios han sido elaboradas por el Área de Desarrollo de Sistemas bajo plataformas Windows. Cabe mencionar que el área de desarrollo se encuentra concentrada en la Dirección Metropolitana de Informática Quito.

A continuación, se describen los sistemas que permiten la gestión de información en diversas áreas, así se tiene:

2.6.2.1 Sistema Catastros

El Sistema de Catastros es uno de los sistemas que hace uso la Institución y está basado bajo VSAM[15], el personal que trabaja con este sistema lo usa habitualmente para generación y administración de todos los predios de la ciudad tanto en su entorno urbano como en sus parroquias.

2.6.2.2 Sistema Financiero

Es uno de los sistemas que más demanda tiene dentro de la Institución pues el mismo maneja todo lo relacionado con la Contabilidad, Tesorería, Garantías, Presupuestos, Roles de Pago; el sistema está basado bajo AS/400[16], entre las funciones principales que tiene son ejecutar los procesos presupuestarios, contables y de Tesorería de la Institución, así mismo este permite presentar informes financieros de todos los procesos que se van ejecutando, así como también trabaja con procesos de garantías, especies y títulos a favor de la Administración Zonal. Cabe mencionar que el sistema administra la información de múltiples Instituciones, pero los derechos del sistema no son propiedad de ninguna Institución.

2.6.2.3 Sistema GDOG

Este sistema es el artífice de la comunicación social de documentación, el mismo comunica a todas las áreas administrativas procesos (asignación de actividades, circulares, etc.) que se están llevando a cabo o procesos que podrían tener un inicio cercano, en los cuales se ven involucrados uno o varios de los funcionarios. Este sistema es uno de los cuales ha sido desarrollado bajo un lenguaje de programación que tiene una gran difusión en la actualidad y por su alta convergencias entre los diferentes sistemas viene siendo explotado, así C# o también llamado C Sharp

[15] **VSAM:** (Virtual Storage Access Method). Es un sistema de archivos usado en mainframes de IBM. VSAM acelera el acceso a los datos en archivos utilizando un índice invertido (llamado árbol B+) de todos los registros añadidos a cada archivo. [14]

[16] **AS/400:** Es un sistema integrado muy complejo que incluye el hardware, el software, la seguridad, una base de datos y otros componentes. El AS/400 se diseña para separar el software y el hardware así que los cambios en uno tienen poco efecto en el otro. [15]

lenguaje de programación que está incluido en la Plataforma .NET, presenta un nuevo enfoque que facilita una integración de actividades sin mayor dificultad.

2.6.2.4 Sistema de Trámites

El sistema de trámites es el encargado de gestionar toda la documentación ingresada, esta a su vez es catalogada según su ámbito de acción y designada adecuadamente al departamento o persona encarga de llevar el proceso. Entre los diversos tipos trámites que se pueden ingresar, se tiene pedidos, trámites catastrales, modificación de predios, etc. El sistema ha sido desarrollado bajo FOX y aunque es un sistema antiguo no ha sabido presentar mayor inconveniente entre las personas que lo utilizan, siendo uno de los sistemas más difundidos en la Institución.

2.6.2.5 Sistema Tramifácil

Este sistema facilita el uso de la información generada por el sistema AS/400, este a su vez permite la generación de licencias de funcionamiento, aprobaciones y regulaciones de construcciones. El sistema tiene la funcionalidad de trabajar en un entorno web, facilitando su uso debido a la gran apertura de recursos que tiene este tipo de aplicaciones, sin embargo en los inicios la administración y soporte del sistema se encontraban gestionadas por una empresa externa, que no lograba cubrir las expectativas de funcionamiento requeridas; en la actualidad la Administración ha tomado bajo su control el sistema, logrando expandir su campo de acción eficazmente.

2.6.3 PLATAFORMAS USADAS

Mayoritariamente las computadoras hacen uso del sistema operativo Windows XP Profesional aunque existen computadoras que han sido actualizadas bajo sistemas Windows 7 Profesional, esto gracias a la compra de licencias corporativas.

2.6.4 ANÁLISIS DE EQUIPOS UTILIZADOS

Los equipos que la Institución utiliza facilitan la interconexión de los distintos departamentos, así también permite la comunicación externa con la Dirección Metropolitana de Informática Quito y otras Administraciones Zonales.
A continuación, se mencionan los equipos que integran la red.

2.6.4.1 Switch 3COM 4200

Es un switch de alto rendimiento con una gran fiabilidad, presenta modelos de 26, 28 ó 50 puertos. En la Administración Zonal este dispositivo se encuentra ubicado en el Departamento de Sistemas con una cabida de 26 puertos, este a su vez tiene una capacidad integrada de apilamiento, puertos Gigabit Ethernet y STP[17] (Spanning Tree Protocol). Entre su principal característica posee veinticuatro puertos 10/100 de cobre con detección automática proporcionando conexiones flexibles para grupos de trabajo y escritorio, mientras que dos puertos de up-link[18] 10/100/1000 de cobre con detección automática permite conexiones Gigabit Ethernet. Los puertos Gigabit integrados pueden emplearse como up-link o para apilamiento con una combinación de otras unidades switch 4200 26-, 28-, 50-puertos.

Figura 2.11 Switch 3COM 4200

En la Tabla 2.11, se detallan las principales características del switch 3COM 4200.

[17] **STP**: Protocolo que evita la generación de lazos de enrutamiento.

[18] **Up-link**: (Enlace o conexión de subida) término utilizado en un enlace de comunicación para la transmisión de señales.

Características	Especificaciones
Número de puertos	26
Velocidad por puerto	24 puertos 10/100 Mbps. 2 puertos 10/100/1000 Mbps.
Escalabilidad	2 puertos pueden ser usados para up-link
Función especial	Conmutación Ethernet, velocidad completa sin bloqueo en todos los puertos Ethernet, negociación automática full/half dúplex y control de flujo, filtrado multicast de nivel 2

Tabla 2.11 Características del switch 3COM 4200 de la Institución

2.6.4.2 Switch 3COM 5500G-EI

Este equipo permite tener una red convergente y segura con capacidad de apilamiento. La Institución utiliza el equipo para obtener una conectividad flexible y escalable para una combinación heterogénea de datos, voz, video y otros servicios, que se adapta con una alta disponibilidad y resistencia ante fallos. Las funciones avanzadas de QoS[19] y el filtrado independiente de las aplicaciones ayudan a optimizar el rendimiento de voz y video. Las funcionalidades de seguridad (SNMPv3, SSH[20], login de red) y administración protegen a los datos, usuarios y dispositivos del acceso no autorizado y de la corrupción.

Figura 2.12 Switch 3COM 5500G-EI

En la Tabla 2.12, se detallan las principales características del switch 3COM 5500G-E1.

[19] **QoS:** Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado. [16]

[20] **SSH**: (Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. [17]

Características	Especificaciones
Número de puertos	24
Velocidad por puerto	20 puertos 10/100/1000 Mbps. 4 puertos Gigabit de uso dual 10/100/1000 Mbps o SFP 1 ranura para módulo de expansión
Escalabilidad	La ranura para módulo de expansión ofrece conectividad adicional Gigabit o 10-Gigabit Ethernet.
Función especial	La autenticación basada en el usuario y la encriptación DES de 56 ó 168 bits ayudan a asegurar los protocolos de Capa 3 y los controles de administración.

Tabla 2.12 Características del switch 3COM 5500G-EI de la Institución

2.6.4.3 Switch 3COM 2928-SPF Plus

Es un switch administrable a través de la web con amplias funcionalidades de nivel 2 y rutas estáticas de nivel 3. Proporciona un rendimiento sin bloqueo que ayuda a eliminar los cuellos de botella de la red. Ademas, dispone de funciones que ayudan a construir una red preparada para voz, administración basada en SNMP, IGMP snooping[21], así como IEEE 802.1x y listas de control de acceso avanzadas para reforzar la seguridad.

Figura 2.13 Switch 3COM 2928-SFP Plus

En la Tabla 2.13, se detallan las principales características del switch 3COM 2928-SFP Plus.

[21] **IGMP snooping:** (Internet Group Management Protocol) tiene la característica de escuchar en la conversación IGMP entre hosts y routers.

Características	Especificaciones
Número de puertos	28
Velocidad por puerto	24 puertos autosensing 10/100/1000 Mbps. 4 puertos SFP 10/100/1000 Mbps.
Estándares que soporta	IEEE 802.1d Spanning Tree IEEE 802.1p Priority Tags IEEE 802.1q Vlans IEEE 802.1x Port Security IEEE 802.3ab Gigabit Ethernet IEEE 802.3ad Link Aggregation IEEE 802.3u Fast Ethernet IEEE 802.3x Flow Control IEEE 802.3z Gigabit Ethernet

Tabla 2.13 Características del switch 3COM 2928-SFP Plus de la Institución

2.6.4.4 Switch 3COM 4226T

Este equipo posee una conmutación de nivel 2, proporciona veinticuatro puertos 10/100 Mbps con detección automática de cobre, mientras que dos puertos de enlace ascendente autosensing 10/100/1000 de cobre permiten Gigabit Ethernet de red troncal y conexiones de servidor. Los puertos Gigabit integrados pueden emplearse como up-link o para apilamiento con la combinación de otros dispositivos de esta rama.

Figura 2.14 Switch 3COM 4226T

En la Tabla 2.14, se detallan las principales características del switch 3COM 4226T.

Características	Especificaciones
Número de puertos	26
Velocidad por puerto	24 puertos 10/100 Mbps. 2 puertos 10/100/1000 Mbps.
Escalabilidad	2 puertos pueden ser usados para up-link o para apilamiento
Función especial	El switch puede configurar sus propios ajustes de IP para la gestión a través de SNMP, web o la CLI

Tabla 2.14 Características del switch 3COM 4226T de la Institución

2.6.4.5 Switch Advantek ANS24R

Este dispositivo de 24 puertos de Advantek Networks mejora notablemente el rendimiento de una red local de pequeña o mediana escala. Este equipo permite la interconexión con los diferentes departamentos de la Institución.

Figura 2.15 Switch Advantek ANS24R

En la Tabla 2.15, se detallan las principales características del switch Advantek ANS24R.

Características	Especificaciones
Número de puertos	24
Velocidad por puerto	10/100 Mbps.
Tipo de procesamiento	Store and Forward, Full/Half Duplex, Non-Blocking Flow Control
Estándares que soporta	IEEE 802.3, IEEE 802u, IEEE 802.3x

Tabla 2.15 Características del switch Advantek ANS24R de la Institución

2.6.4.6 Switch D-Link DES 1024D

Este equipo no cuenta con capacidad administrable, está diseñado para aumentar el rendimiento y proporcionar un alto nivel de flexibilidad. Provee soporte para la detección Auto MDI/MDIX Crossover en todas las puertas, eliminando la necesidad de cables crossover o puertas Up-Link. Además permite multiplicar el ancho de banda, tiempo de respuesta y satisfacer requerimientos de acceso a los servicios de red. Este equipo tiene como función proveer acceso a la red LAN de los distintos departamentos.

Figura 2.16 Switch D-Link DES 1024D

En la Tabla 2.16, se detallan las principales características del switch D-Link DES 1024D.

Características	Especificaciones
Número de puertos	24
Velocidad por puerto	10/100 Mbps.
Estándares que soporta	IEEE 802.3 10Base-T Ethernet, IEEE 802u 100Base-TX Fast Ethernet, ANSI/IEEE 802.3 Nway auto-negotiation
Tasa de transferencia de datos	Ethernet: 10Mbps (half-duplex), 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half-duplex), 200Mbps (full-duplex)

Tabla 2.16 Características del switch D-Link DES 1024D de la Institución

2.6.4.7 Switch D-Link DES 1024R+

Este equipo posee 24 puertos 10/100 Mbps, no administrable. Este tipo de puertos detectan la velocidad de la red y autonegocian entre 10Mbps y 100Mbps, así como entre modo full y half-duplex. El control de flujo incorporado disponible en modo full dúplex previene la perdida de datos durante las transmisiones de red. Este equipo tiene como función proveer acceso a la red LAN de los distintos departamentos.

Figura 2.17 Switch D-Link DES 1024R+

En la Tabla 2.17, se detallan las principales características del switch D-Link DES 1024R+.

Características	Especificaciones
Número de puertos	24
Velocidad por puerto	10/100 Mbps.
Estándares que soporta	IEEE 802.3 Ethernet, Fast Ethernet IEEE 802.3u, Control de flujo IEEE 802.3x, IEEE 802.1p QoS.

Tabla 2.17 Características del switch D-Link DES 1024R+ de la Institución

2.6.4.8 Router Modem ADSL2+ TP-LINK TD-8811

Este equipo es utilizado para la conexión a Internet, de banda ancha de alta velocidad con el proveedor de Internet. Además soporta una amplia gama de velocidades de hasta 24Mbps para descarga y 3.5Mbps para subida de archivos. Por su funcionalidad detecta y autonegocia el tipo de conexión para un mejor rendimiento. En la Figura 2.18, se muestra al equipo mencionado.

Figura 2.18 Router Modem ADSL2+ TP-LINK TD-8811

En la Tabla 2.18, se detallan las principales características del router modem ADSL2+ TP-LINK TD-8811.

Características	Especificaciones
Protocolos	PPP (RFC 1661), PPPoA (RFC 2364), PPPoE (RFC 2516), IP sobre ATM (RFC 1577).
Interfaz	WAN: Un puerto RJ-11 para Línea ADSL2+ LAN: 1 Puerto Ethernet 10/100 Base T (RJ-45) USB: 1 Puerto USB 1.1
Estándares que soporta	Compatible con múltiples estándar ADSL como: ANSL T1.413 ISSUE 2, ITU G.992.1 (G.dmt), ITU G.992.2 (G.lite), ITU G.992.3 (ADSL2), ITU G.994.1 (G.hs), ITU G.992.5 (ADSL2+)

Tabla 2.18 Características del Router Modem ADSL2+ TD-8811 TP-LINK de la Institución

2.6.4.9 Router Cisco 800 Series

Este equipo es utilizado para la conexión WAN con la Dirección Metropolitana de Informática Quito, otorga transferencia de archivos y operaciones confiables, además proporciona una seguridad integrada, ya que posee un firewall integrado y encriptación con IP Security para habilitar VPNs. En la Figura 2.19, se muestra al equipo mencionado.

Figura 2.19 Cisco 800 Series

En la Tabla 2.19, se detallan las principales características del router cisco 800 series.

Características	Especificaciones
Número de puertos	4 puertos 10/100 Mbps Fast Ethernet con opción PoE en dos de los puertos de conmutación
Función Especial	Hasta 20 túneles VPN
Estándares que soporta	IEEE 802.11n, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n

Tabla 2.19 Características del Router Cisco 800 Series de la Institución

2.6.5 ANÁLISIS SERVIDORES

Los servidores están destinados para el procesamiento de solicitudes por parte de todos los clientes que se conectan a él, como también entregar datos dependiendo del servicio que ofrezcan. Los servidores poseen características especiales que los diferencian de otros equipos, así estos presentan hardware con mejores prestaciones como procesadores de alto rendimiento, mayor capacidad de memoria RAM, unidades con un gran volumen de almacenamiento, etc.

Tomando en cuenta las características mostradas en la Tabla 2.1 al comienzo de este capítulo y que por cuestiones de índole restrictiva no se ha podido acceder ni de manera directa como indirecta a las características hardware principales de todos los servidores, se ha visto limitada la apreciación total de los datos.

Existen servidores que no poseen un sistema de almacenamiento avanzado, es decir, no son tolerantes a fallos. Además no existe un sistema de enfriamiento adecuado para mantener un ambiente de operaciones óptimo. Se ha podido observar que existe una desorganizada utilización de utilitarios en más de uno de los servidores. La

ausencia de un rack de equipos suficientemente amplio, ha ocasionado la improvisación de un lugar, para posicionar los servidores; esto puede repercutir negativamente en la administración y soporte que se debe otorgar a cada equipo.

A continuación, se hará referencia brevemente a algunos servidores.

2.6.5.1 Servidor de Dominio

Este servidor tiene alojado el controlador de dominio el mismo que permite organizar la información, controlar el acceso y establecer la seguridad de un árbol de objetos de recursos (computadores, impresoras), servicios (correo electrónico, web, FTP) y usuarios (perfiles, cuentas o usuarios, grupos). La Figura 2.20, permite observar la distribución organizativa de la Institución.

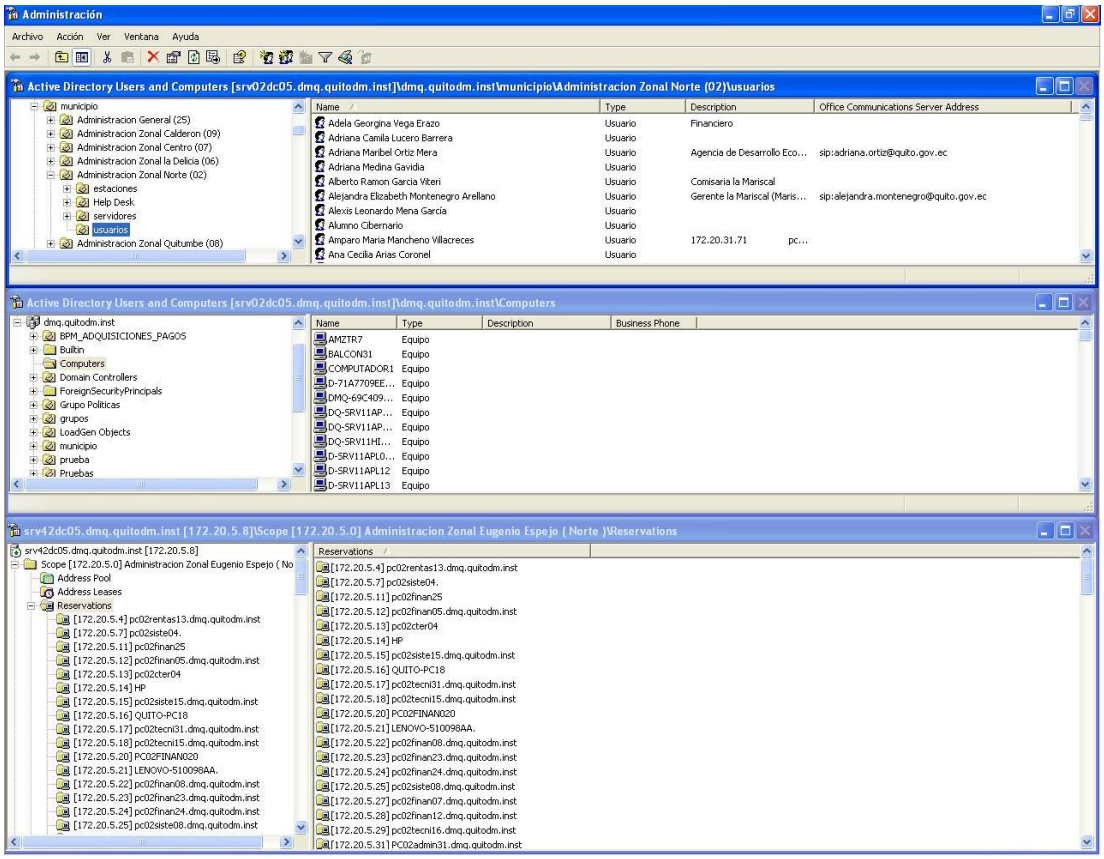


Figura 2.20 Controlador de Dominio de la Administración Zonal Norte "Eugenio Espejo"

Una de las principales causas de tener un controlador de dominio es la ayuda que presta a un administrador, con la gestión de usuarios y recursos, además que facilita el acceso de los usuarios, a recursos de todo el dominio usando un único login a la red.

2.6.5.2 Servidor y Consola Antivirus

Este servidor es de vital importancia ya que provee la protección necesaria en caso de que algún archivo malicioso intente irrumpir en la red de la Institución, ocasionando saturación de recursos o pérdidas de información.

La Institución tiene contratado los servicios de un antivirus corporativo como lo es el ESET Smart Security 4.0.474 el que proporciona la seguridad necesaria en la red. La Figura 2.21, muestra la consola de operación del antivirus.

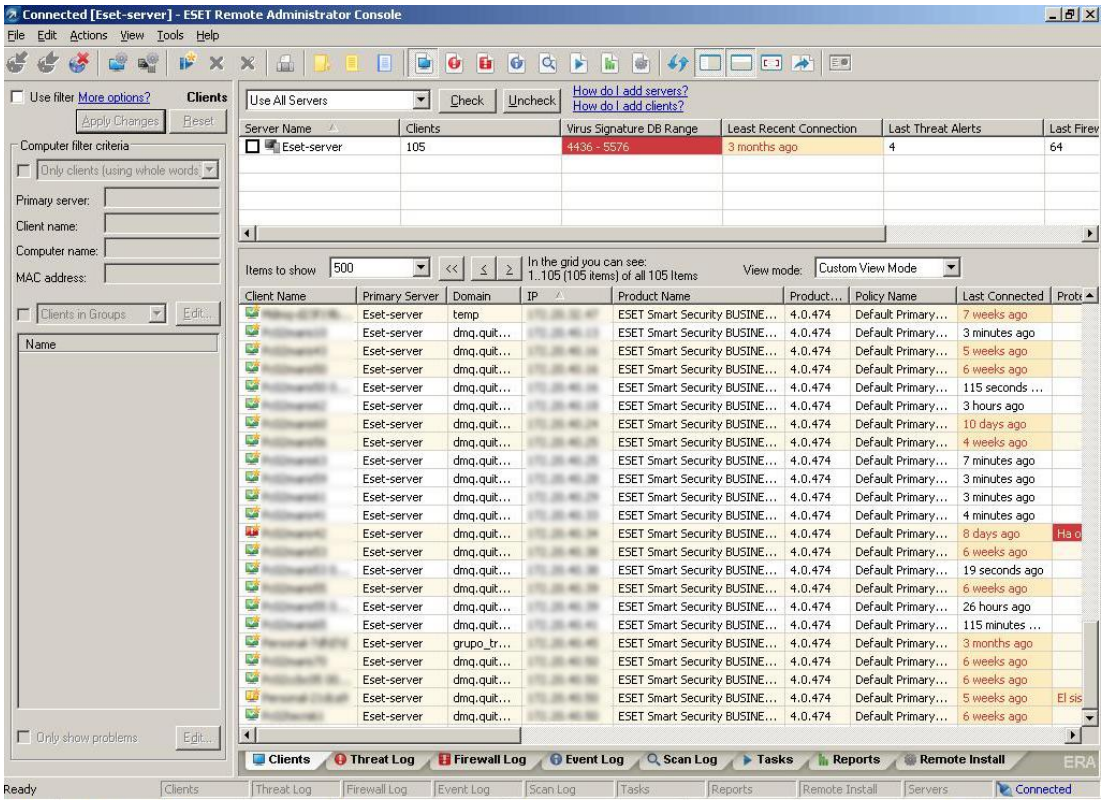


Figura 2.21 Consola de Administración del Antivirus

2.6.6 MONITOREO DEL TRÁFICO DE LA RED DE DATOS

Una de las principales causas que afectan a una red de datos es la saturación parcial o total de su canal de comunicaciones debido a factores como uso inadecuado de los recursos de internet, periféricos de red, actualizaciones de sistemas; entre los más importantes y que ocasionan una disminución considerable del ancho de banda.

Esta disminución parcial o total de los recursos ocasiona problemas de descarte de paquetes, encolamiento de los procesos de red, retransmisiones, retardos y jitters[22].

Para determinar si las operaciones en la red de datos manifiestan anomalía alguna, se ha realizado un análisis del tráfico de red, el que presenta un enfoque esquemático de lo que sucede en la red. A continuación, se describen los resultados obtenidos del análisis de tráfico, haciendo uso de software de monitoreo PandoraFMS y Wireshark.

2.6.6.1 Descripción del software libre Wireshark.

Wireshark anteriormente conocido como Ethereal es un analizador libre de protocolo para entornos UNIX, GNU/Linux y Windows; permite identificar y analizar el tráfico existente en una red en un momento determinado. Utilizado principalmente por administradores de red para analizar los paquetes que circulan por la red o comúnmente denominado packet sniffer. La aplicación tiene la particularidad de analizar tanto paquetes de una red activa como también de un archivo generado con anterioridad.

Es importante destacar que Wireshark no es un IDS (Instrusion Detection System) ya que no genera alertas cuando existen eventos anómalos en una red. Wireshark tiene funcionalidades que facilitan un análisis pormenorizado de una cantidad extensa de protocolos; generalmente para una captura más efectiva de paquetes, su interfaz de red trabaja en modo promiscuo logrando excelentes resultados.

[22] **Jitters**: Son oscilaciones de la separación temporal entre paquetes. En aplicaciones que requieren sincronización (videoconferencia, sincronizar audio con vídeo), es muy importante que esas oscilaciones sean pequeñas. [18]

El aplicativo permite a los usuarios aprender en corto tiempo un manejo adecuado de la información capturada ya que dispone de filtros que al relacionarse con un criterio determinado exponen la información buscada de forma rápida, además se puede visualizar los datos de forma estadística con la ayuda de colores y filtros por protocolo. Haciendo uso de muchas de las características que proporciona el aplicativo se ha procedido a analizar los datos capturados en el transcurso de una semana.

2.6.6.1.1 Análisis de paquetes con Wireshark

Para el análisis, se han tomado diferentes capturas de paquetes en intervalos de tiempo para determinar los principales protocolos usados, rutas de destino y efectuar los cuadros estadísticos según los datos arrojados. La Figura 2.22, muestra cómo se visualiza una captura de datos por medio de Wireshark.

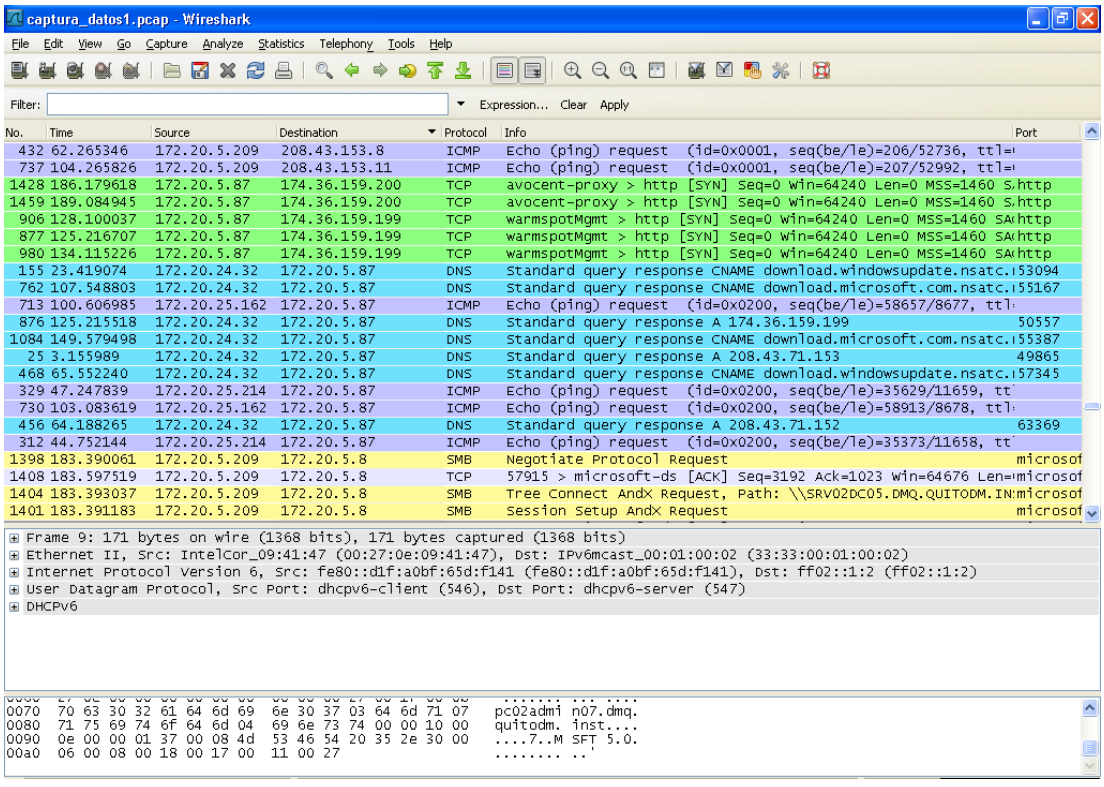
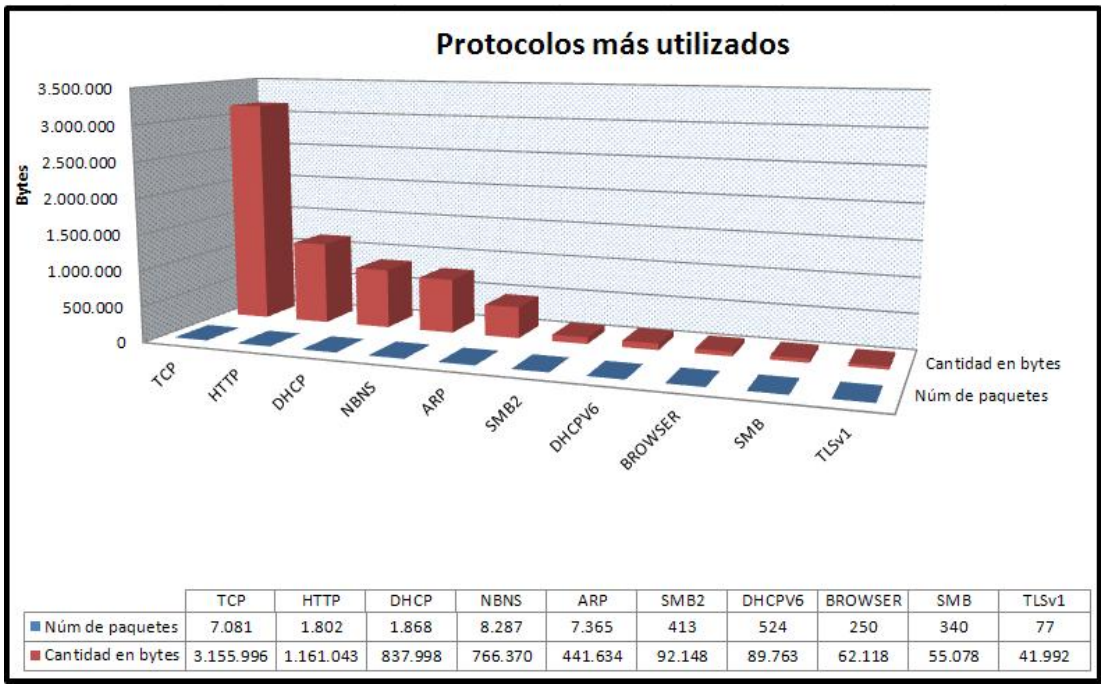


Figura 2.22 Captura de paquetes con Wireshark

La muestra representativa de la Figura 2.23, corresponde a una instancia específica de 16 minutos y no denota mayores cambios en el transcurso del día; cabe mencionar que los datos no representan valores totalmente exactos debido a que no es un sondeo continuo sino por intervalos de tiempo; las datos tomados por intervalos de tiempo, son con el afán de no provocar saturación en los servicios utilizados ni de exagerar el tamaño de los archivos generados por el aplicativo.

Para la realización de las gráficas estadísticas se han llevado los datos sondeados con Wireshark a Excel para exponer de mejor manera todos sus detalles.

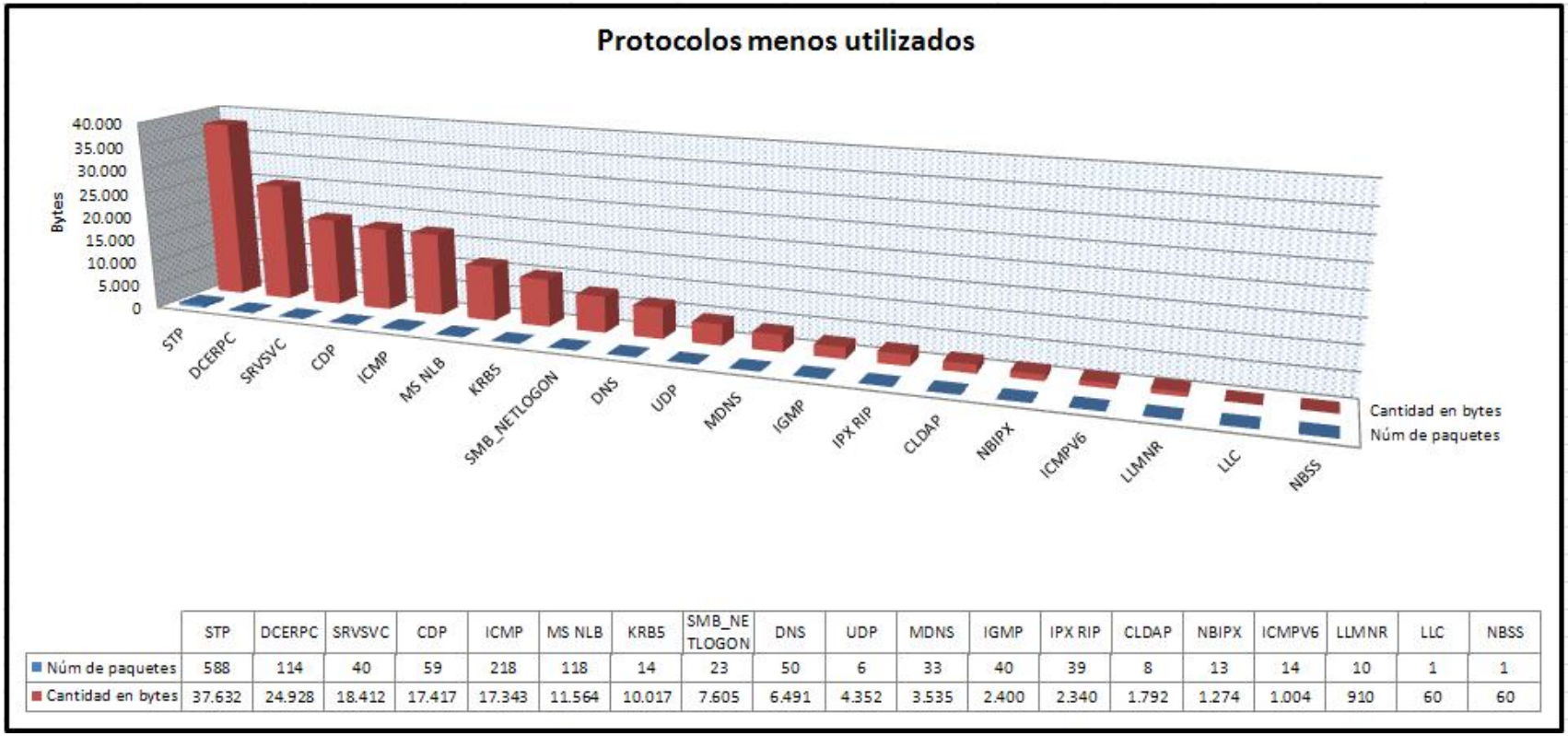


	TCP	HTTP	DHCP	NBNS	ARP	SMB2	DHCPV6	BROWSER	SMB	TLSv1
Núm de paquetes	7.081	1.802	1.868	8.287	7.365	413	524	250	340	77
Cantidad en bytes	3.155.996	1.161.043	837.998	766.370	441.634	92.148	89.763	62.118	55.078	41.992

Figura 2.23 Protocolos más utilizados en base a datos de Wireshark

La Figura 2.23, desvela que el protocolo más utilizado es TCP ya que el mismo es utilizado para la compartición de archivos, aplicaciones de base de datos y todo tipo de procesos orientados a la conexión que llegan a ser de vital importancia en una red Institucional. El protocolo HTTP representa el segundo más utilizado debido a que este permite la conexión de los usuarios a distintos portales web con índoles investigativas, informativas y de ocio.

Se puede notar que no necesariamente un mayor número de paquetes representa una mayor cantidad de bytes, como se puede constatar entre DHCP y HTTP.



	STP	DCERPC	SRVSVC	CDP	ICMP	MS NLB	KRB5	SMB_NETLOGON	DNS	UDP	MDNS	IGMP	IPX RIP	CLDAP	NBIPX	ICMPV6	LLMNR	LLC	NBSS
Núm de paquetes	588	114	40	59	218	118	14	23	50	6	33	40	39	8	13	14	10	1	1
Cantidad en bytes	37.632	24.928	18.412	17.417	17.343	11.564	10.017	7.605	6.491	4.352	3.535	2.400	2.340	1.792	1.274	1.004	910	60	60

Figura 2.24 Protocolos menos utilizados en base a datos de Wireshark

La Figura 2.24, anteriormente mostrada indica los protocolos menos utilizados esto debido a que no son protocolos de gran importancia, aunque si solventan necesidades específicas como el DNS, UDP, ICMP y el IGMP de entre los más conocidos.

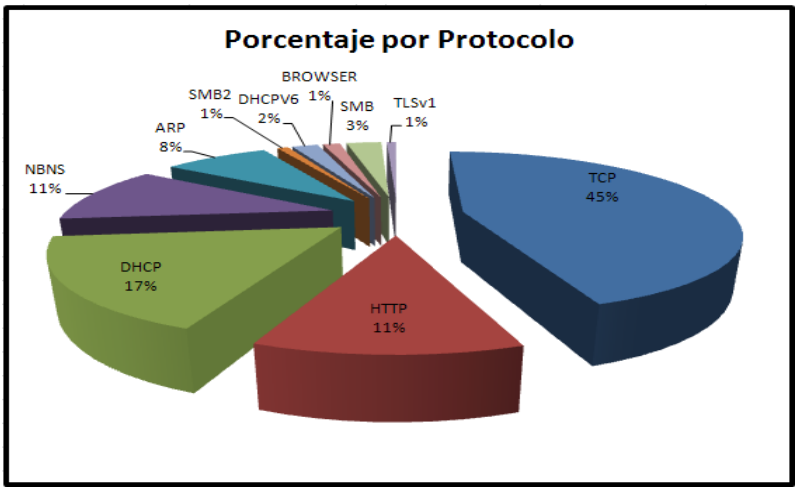
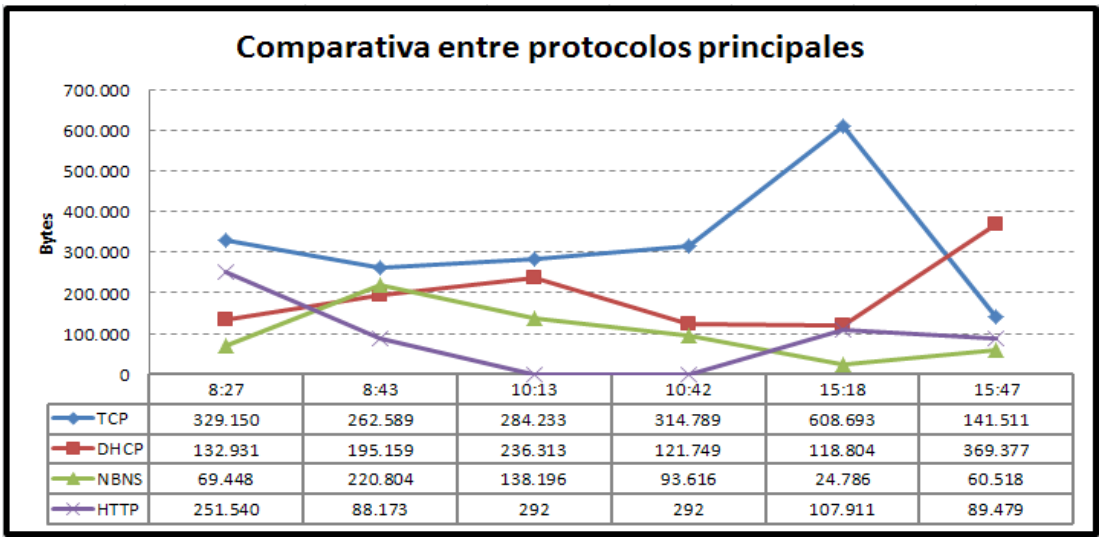


Figura 2.25 Uso de protocolos en base a datos de Wireshark

El uso más extendido de protocolos se evidencia en la Figura 2.25, la que al ser analizada con una cantidad mayor de datos muestra que ha existido una variación entre el segundo y tercer protocolo más utilizado respecto a los datos de la Figura 2.23; así la Institución presenta un uso de un 45% con TCP, seguidamente DHCP con un 17% y en tercer lugar HTTP con un 11%.



	8:27	8:43	10:13	10:42	15:18	15:47
TCP	329.150	262.589	284.233	314.789	608.693	141.511
DHCP	132.931	195.159	236.313	121.749	118.804	369.377
NBNS	69.448	220.804	138.196	93.616	24.786	60.518
HTTP	251.540	88.173	292	292	107.911	89.479

Figura 2.26 Comparativa entre protocolos principales en base a datos de Wireshark

La Figura 2.26 anteriormente mostrada, evidencia las variaciones que presenta cada uno de los protocolos principales en una jornada laboral; cabe mencionar que solo se han tomado en cuenta a los cuatro protocolos principales de una toma de 29 protocolos existentes.

2.6.6.2 Monitoreo de servicios con Pandora FMS.

Para conocer mejor cual es la situación actual de los equipos frente a su rendimiento y como están operando sus diferentes servicios en uso cotidiano, se ha utilizado el software Pandora FMS, el mismo que ha sondeado la red por una semana y a provisto los datos que se presentan más adelante.

2.6.6.2.1 Descripción del software Pandora FMS

Pandora FMS (FMS viene de Flexible Monitoring System) es una aplicación de monitorización para vigilar todo tipo de sistemas y aplicaciones. Pandora FMS permite conocer el estado de cualquier elemento de sus sistemas de negocio. Pandora FMS vigila el hardware, el software, las aplicaciones y por supuesto, el Sistema Operativo. Pandora FMS es capaz de detectar una interfaz de red que se ha caído, así como el movimiento de cualquier valor del NASDAQ[23]. Si es necesario, Pandora FMS puede enviar un mensaje SMS[24] cuando falle cualquier sistema o aplicación, o cuando el valor de Google caiga por debajo de los 330US$. [20]

El diseño modular, abierto y multiplataforma que presta Pandora FMS permite adaptar necesidades según los entornos a monitorizar sean estos del tipo software o hardware. El aplicativo no puede ser catalogado como un sistema de detección o prevención de intrusiones, aunque informa sobre host caídos o puertos abiertos y cerrados; al ser un sistema generalista no efectúa un monitoreo en tiempo real aunque se pueden programar periodos cortos de tres a cinco segundos y utilizar redundancia para entornos críticos.

---

[23] **NASDAQ:** (National Association of Securities Dealers Automated Quotation) es la bolsa de valores electrónica automatizada más grande de Estados Unidos. [19]

[24] **SMS:** Servicio de Mensajes Cortos (Short Message Service, en inglés) sistema de mensajes de texto para teléfonos móviles.

Pandora FMS utiliza agentes para recolectar la información pero también posee una monitorización remota que permite conocer otros parámetros de utilidad como un puerto remoto TCP abierto o no, información mediante SNMP, consultar registros de Windows, etc. El sistema posee una parte comercial que otorga funcionalidades adicionales como, soporte profesional, actualizaciones y mantenimiento automático a través del sistema Open Update Manager, pero aun así esto solo representa el 10% de toda la aplicación concebida bajo una licencia de Código Abierto Especial, mientras que el restante es netamente Open Source.

Para el análisis se ha procedido a la instalación de agentes en distintos puntos de la Institución para recabar la información necesaria y pertinente.

En la Figura 2.27, se muestra la consola web de Pandora FMS, la que permite la administración y operación de diferentes administradores con sus respectivos privilegios; los agentes instalados pueden rescatar información de cada host, el sistema operativo que cada uno posee, el grupo al que pertenece, los módulos activos, las alertas y el último contacto que se tuvo con ese agente.

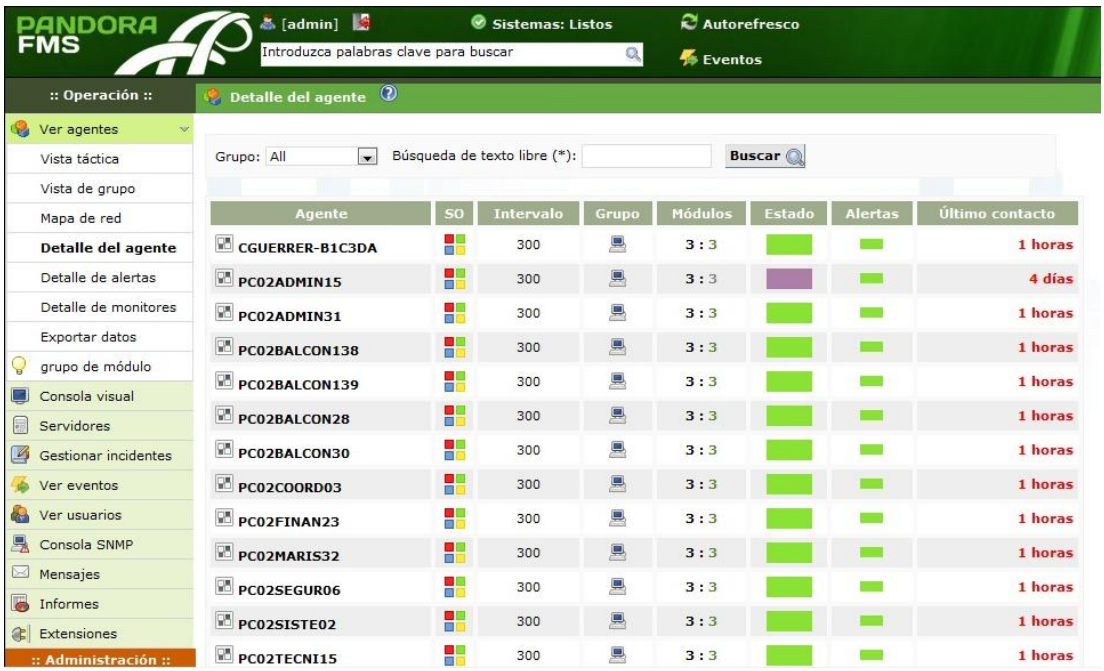


Figura 2.27 Detalles de agentes instalados

A continuación en la Figura 2.28, se muestran los parámetros que cada agente están en posibilidad de informar, también se presenta una gráfica sobre la accesibilidad del agente en las últimas 24 horas y una lista de los monitores que están en ejecución.

Figura 2.28 Parámetros del agente Pandora FMS

El sistema que provee Pandora FMS permite ver un enfoque global de los agentes instalados, así en la Figura 2.29, se puede apreciar los host gestionados.

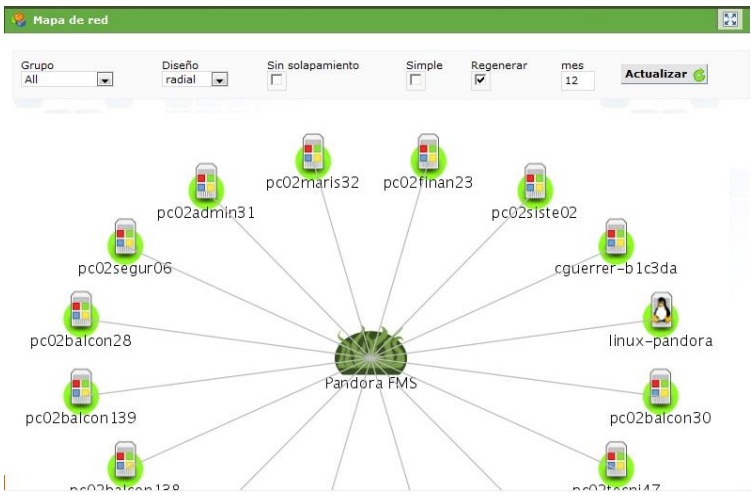


Figura 2.29 Host gestionados con Pandora FMS

2.6.6.2.2 Análisis del rendimiento de los servicios con Pandora FMS

Pandora FMS recaba información que permite determinar un estado de criticidad para cualquier host que contenga el agente instalado; existen diferentes estados los que pueden ser desde leves a graves de atención inmediata, no iniciado, o desconocido; cada estado dependerá de si existe una mayor o menor cantidad de módulos caídos por host gestionado.

Cabe destacar que los agentes están basados en lenguajes nativos de cada plataforma por ende se puede decir que el desarrollo podría efectuarse en casi cualquier lenguaje, siempre y cuando cumpla la API de intercambio de datos con el servidor de datos Pandora FMS (definido por un XML de intercambio de datos).

En el análisis se ha tomado en cuenta parámetros como uso de CPU, espacio libre en disco y memoria libre. Los datos expuestos son de host, que por su nivel de desempeño, son de gran importancia para la Institución; además la información proporcionada a provisto de parámetros muy similares con equipos de gran demanda funcional.

Figura 2.30 Espacio libre en disco sondeado con Pandora FMS

La Figura 2.30, mostrada anteriormente representa una comparativa de datos tanto diaria como semanal de las condiciones del espacio libre en disco, para uno de los host de la Institución. De acuerdo a los datos obtenidos a existido apenas unos ligeros cambios en el espacio libre del equipo lo que implica que no se ha añadido mayores documentos en su disco.

Por otro lado, también se presenta una comparativa de datos tanto diaria como semanal de las condiciones de la memoria libre, en la que se evidencia que han existido fluctuaciones considerables en su uso, las que son provocadas mayoritariamente por la utilización de aplicaciones que demandan del host más memoria. La Figura 2.31, muestra las variaciones que ha tenido la memoria del host.

Figura 2.31 Memoria libre del host sondeado con Pandora FMS

Uno de los parámetros más importantes que permite sondear Pandora FMS es el relacionado con el uso de CPU, el mismo enfoca las variaciones surgidas por el host estableciendo picos altos y bajos según la carga de trabajo que ha existido; en la Figura 2.32 mostrada a continuación se puede notar esas fluctuaciones en el uso de CPU tanto en una gráfica diaria como semanal.

Figura 2.32 Uso de CPU sondeado con Pandora FMS

CAPÍTULO 3. ANÁLISIS Y PRUEBAS DE LOS SISTEMAS DE GESTIÓN DE REDES

En este capítulo, se llevará a cabo un análisis pormenorizado de los diferentes sistemas libres de gestión de red con el afán de determinar cuál es la que muestra las mejores prestaciones acorde a las necesidades de la Institución, tratando de rescatar cualidades como rendimiento, funcionalidades, condiciones de uso, etc.

El precisar el sistema libre de gestión de red con las mejores prestaciones, encaminara a la Institución en la adopción de nuevas y mejores tecnologías que brinden una alta capacidad de monitorización de los servicios de red, monitorización de los recursos de sistemas hardware, mantenimiento preventivo y redundancia. La información que proporcione el aplicativo mejor valorado, servirá de base para la formulación de propuestas, que determinen una adecuada gestión de las distintas áreas funcionales, a elaborarse en el capítulo posterior.

3.1 SISTEMAS LIBRES DE GESTIÓN DE REDES

3.1.1 NTOP (Network TOP)

3.1.1.1 Descripción general

NTOP es un proyecto libre que esta licenciado bajo GNU[25] Licencia Pública General, inicialmente concebida por Luca Deri y Stefano Suin para enfrentar problemas de rendimiento en la red del campus de la Universidad de Pisa, Italia.

Esta aplicación posibilita el monitoreo en tiempo real, además de identificar el consumo de recursos de red por parte de usuarios y aplicaciones en un instante determinado. A su vez es capaz de detectar malas configuraciones de un equipo ya que la anomalía la visualiza por medio de un banderín amarillo o rojo al lado del

[25] **GNU**: Licencia Pública General (General Public License, en inglés) es una licencia creada por la Free Software Foundation y orientada principalmente a los términos de distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es Software Libre.

equipo, dependiendo la gravedad del caso. Actualmente la aplicación se enfoca en parámetros importantes como:

- Medición de tráfico.
- Observación de tráfico.
- Optimización y planificación de la red.
- Detección de infracciones de seguridad de la red.

3.1.1.2 Funcionamiento

Posee un microservidor web que permite que cualquier usuario, que sepa la clave, pueda ver la salida NTOP de forma remota con cualquier navegador. La información que puede registrar por cada host conectado, relaciona aspectos como los que se indican a continuación en la Tabla 3.1.

Parámetro	Descripción
Datos enviados/recibidos	Tráfico total generado o recibido por el host. Clasificado acorde al protocolo de red.
Ancho de banda usado	Uso de ancho de banda promedio y máximo.
IP Multicast	Cantidad total de tráfico multicast generado o recibido por el host.
Historial de Sesiones TCP	Sesiones activas TCP establecido/aceptado por el host y asociado a las estadísticas de tráfico.
Tráfico UDP	Cantidad total de tráfico UDP ordenado por puerto.
Servicios usados TCP/UDP	Lista de servicios basados en IP (puertos abiertos y activos) proveído por el host con la lista de los últimos cinco host que los usaron.
Distribución de tráfico	Tráfico local, local a tráfico remoto, remoto a tráfico local (los host locales son añadidos a la red broadcast)
Distribución de tráfico IP	Tráfico UDP vs. TCP, relativa distribución de los protocolos de IP de acuerdo con el nombre del host.

Tabla 3.1 Información que registra NTOP por cada host

También NTOP registra estadísticas de tráfico global las que se indican a continuación en la Tabla 3.2.

Parámetro	Descripción
Distribución de tráfico	Tráfico local (subred), local vs. remota (fuera especificado/subred local), remoto vs. local
Distribución de paquetes	Número total de paquetes ordenado por tamaño de paquetes, unicast vs. broadcast vs. multicast y IP vs. tráfico no IP.
Ancho de banda usado	Uso de ancho de banda promedio y máximo.
Distribución y utilización de protocolo	Distribución del tráfico observado de acuerdo con el protocolo y el origen/ destino (local vs. remoto).
Matriz de tráfico de subred local	Tráfico monitoreado entre cada par de host en la subred.
Flujos de red	Estadísticas de tráfico por flujos de usuarios definidos (tráfico de interés particular al usuario)

Tabla 3.2 Estadísticas globales que registra NTOP

Para extender las funcionalidades de NTOP están dispuestas extensiones plug-ins que permite según el caso monitorizar otros protocolos como ICMP, ARP/RARP y WAP. NTOP permite la visualización de la información sondeada de la red por medio de un acceso vía browser que apunta a la dirección IP del host donde se encuentra corriendo NTOP en el puerto 3000; esto lo hace gracias a que internamente posee un servidor web que especifica el puerto y lo levanta. La manera que estructura la dirección web de acceso a la aplicación se representa como, http://hostname:portnumber/ la misma que muestra toda la información registrada por NTOP.

3.1.1.3 Rendimiento y pruebas

A continuación, se presentan algunas capturas de NTOP en las que se rescata sus funcionalidades más relevantes y determina el estado de la red en un lapso de tiempo determinado.

La Figura 3.1, muestra el porcentaje de uso por protocolo, la cual también es reflejada en MBytes o KBytes; cabe destacar que el tráfico TCP se eleva debido en parte al funcionamiento de NTOP y su accionar en toda la red.

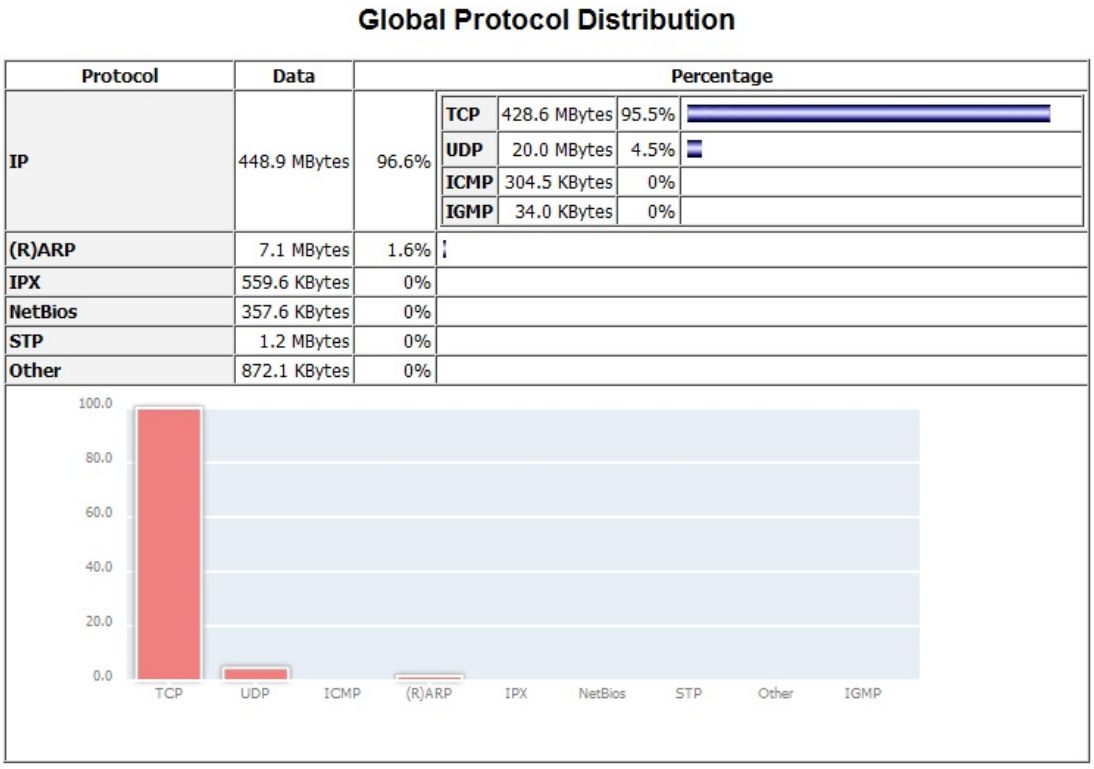


Figura 3.1 Distribución global de protocolos, registrado por NTOP

A continuación la Figura 3.2, muestra el tamaño de los paquetes de acuerdo a cierto rango especificado; de aquello se determina que existe una cantidad considerable de paquetes que se encuentran con un tamaño inferior a los 64 bytes circulando para ese momento, mientras que los paquetes que se encuentran dentro de un rango de 1024 a 1518 bytes solo representan el 9.8%.

Traffic Report for 'le0' [switch]

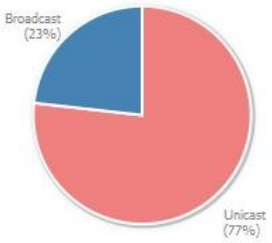
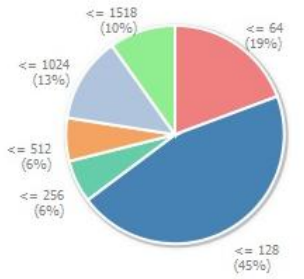
Packets	Dropped (libpcap)	2.9%	46,730
	Dropped (ntop)	0.0%	0
	Total Received (ntop)		1,595,135
	Total Packets Processed		1,595,135
	Unicast	76.7%	1,223,646
	Broadcast	23.3%	370,870
	Multicast	0.0%	619
			
	Shortest		42 bytes
	Average Size		302 bytes
	Longest		1,514 bytes
	Size <= 64 bytes	19.3%	309,522
	64 < Size <= 128 bytes	45.4%	726,895
	128 < Size <= 256 bytes	6.3%	100,181
	256 < Size <= 512 bytes	6.4%	102,871
	512 < Size <= 1024 bytes	12.7%	203,256
	1024 < Size <= 1518 bytes	9.8%	157,209
	Size > 1518 bytes	0.0%	0
			
	Packets too long [> 1514]	0.0%	0
	Bad Packets (Checksum)	1.3%	21,467

Figura 3.2 Tamaños de paquetes, registrados por NTOP para la tarjeta le0

Es de mencionar que no existió ningún error al procesar los datos registrados por NTOP ya que los datos recibidos y procesados son 1.595.135 que equivale a 466.1 MBytes de los cuales 450.3 MBytes, era tráfico IP; mientras que el restante consistía, de diversos tipos de protocolos que en conjunto apenas representa 15.8 MBytes. Los datos mencionados se representan a continuación en la Figura 3.3.

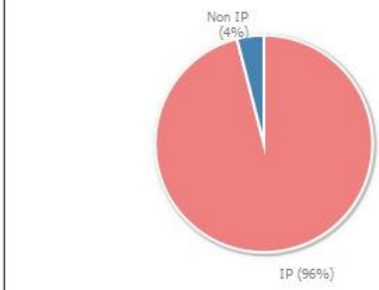
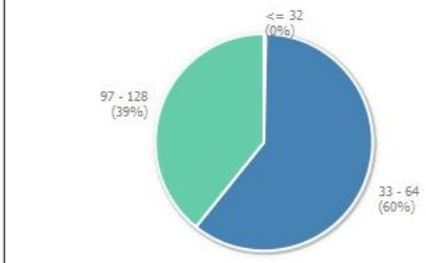
	Total	466.1 MBytes [1,599,934 Pkts]	
	IP Traffic	450.3 MBytes [1,400,213 Pkts]	
	Fragmented IP Traffic	0 [0.0%]	
	Non IP Traffic	15.8 MBytes	
			
Traffic	**Average TTL**		71
	TTL <= 32	0.3%	4,357
	32 < TTL <= 64	52.1%	835,928
	64 < TTL <= 96	0.0%	0
	96 < TTL <= 128	33.8%	542,138
	128 < TTL <= 160	0.0%	0
	160 < TTL <= 192	0.0%	0
	192 < TTL <= 224	0.0%	0
	224 < TTL <= 256	0.0%	156
			

Figura 3.3 Reporte de tráfico, registrados por NTOP para la tarjeta le0

Existe también un descubrimiento de la información de host, la que se puede percibir en diferentes unidades de tráfico sean estas bytes o paquetes; también se destaca información importante acerca del tipo de dominio que posee cada host, el sistema operativo, el ancho de banda siendo este en datos enviados/recibidos, servicios relacionados a este host, nivel de riesgo de operación según el banderín mostrado, equipos de interconexión, número de contactos con otros host; entre los parámetros más importantes y que se los puede observar a continuación en la Figura 3.4.

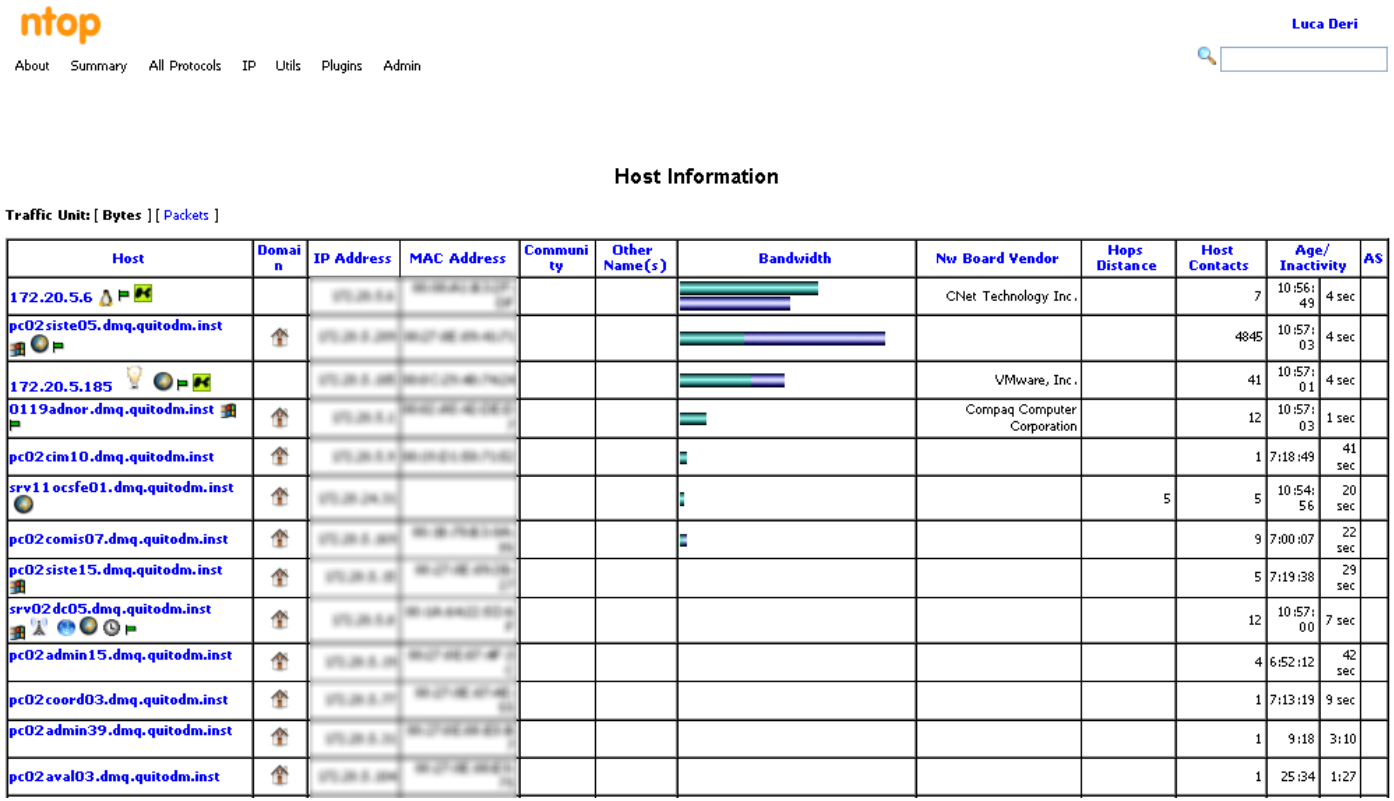


Figura 3.4 Extracto de información de host, registrado por NTOP

Network Traffic [TCP/IP]: All Hosts - Data Sent

Hosts: [**All**] [Local Only] [Remote Only]

Data: [All] [**Sent Only**] [Received Only

Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS	VoIP	X11	SSH
172.20.5.6		195.6 MBytes	43.7 %	0	148.7 MBytes	0	0	0	0	0	0	0	0	0	0	0
172.20.5.185		100.6 MBytes	22.5 %	0	810	42.3 KBytes	0	162	0	7.3 KBytes	0	0	0	0	0	0
pc02siste05.dmq.quitodm.inst		91.4 MBytes	20.4 %	0	79.3 MBytes	59.7 KBytes	0	301.2 KBytes	0	0	0	0	0	1.9 KBytes	0	0
0119adnor.dmq.quitodm.inst		37.0 MBytes	8.3 %	0	186	0	0	1.6 MBytes	0	0	0	0	0	0	0	0
pc02cim10.dmq.quitodm.inst		9.6 MBytes	2.1 %	0	0	0	0	9.5 MBytes	0	5.3 KBytes	0	0	0	0	0	0
srv11ocsfe01.dmq.quitodm.inst		3.7 MBytes	0.8 %	0	9.8 KBytes	0	0	0	0	0	0	0	0	0	0	0
pc02comis07.dmq.quitodm.inst		2.5 MBytes	0.6 %	0	558	0	0	16.9 KBytes	0	0	0	0	0	0	0	0
srv02dc05.dmq.quitodm.inst		1.5 MBytes	0.3 %	0	18.8 KBytes	64.4 KBytes	0	83.6 KBytes	0	155.6 KBytes	0	0	0	0	0	0
pc02siste15.dmq.quitodm.inst		1.2 MBytes	0.3 %	0	0	0	0	9.0 KBytes	0	0	0	0	0	0	0	0
pc02tecni39.dmq.quitodm.inst		521.9 KBytes	0.1 %	0	186	0	0	260.8 KBytes	0	0	0	0	0	0	0	0
hp.dmq.quitodm.inst		385.6 KBytes	0.1 %	0	0	0	0	385.6 KBytes	0	0	0	0	0	0	0	0
172.20.5.3		240.9 KBytes	0.1 %	0	0	0	0	240.9 KBytes	0	0	0	0	0	0	0	0
srv02sccmp01.dmq.quitodm.inst		232.8 KBytes	0.1 %	0	176.3 KBytes	0	0	56.5 KBytes	0	0	0	0	0	0	0	0
pc02admin33.dmq.quitodm.inst		196.0 KBytes	0.0 %	0	0	0	0	194.9 KBytes	0	0	0	0	0	0	0	0
pc02obras10.dmq.quitodm.inst		146.5 KBytes	0.0 %	0	0	0	0	144.2 KBytes	0	2.0 KBytes	0	0	0	0	0	0
172.20.24.44		139.8 KBytes	0.0 %	0	9.0 KBytes	0	0	0	0	0	0	0	0	0	0	0
pc02comis07.dmq.quitodm.inst		81.6 KBytes	0.0 %	0	0	0	0	78.4 KBytes	0	1.3 KBytes	0	0	0	0	0	0
pc02cim01.dmq.quitodm.inst		68.2 KBytes	0.0 %	0	0	0	0	63.2 KBytes	0	4.9 KBytes	0	0	0	0	0	0
pc02tecni24.dmq.quitodm.inst		66.7 KBytes	0.0 %	0	0	0	0	61.0 KBytes	0	5.7 KBytes	0	0	0	0	0	0
pc19comis148.dmq.quitodm.inst		66.6 KBytes	0.0 %	0	0	0	0	66.6 KBytes	0	0	0	0	0	0	0	0
pc02comis14.dmq.quitodm.inst		65.0 KBytes	0.0 %	0	0	0	0	64.8 KBytes	0	0	0	0	0	0	0	0
pc02tecni47.dmq.quitodm.inst		64.1 KBytes	0.0 %	0	0	0	0	63.7 KBytes	0	0	0	0	0	0	0	0
pc19segur127.dmq.quitodm.inst		63.3 KBytes	0.0 %	0	0	0	0	63.3 KBytes	0	0	0	0	0	0	0	0

Figura 3.5 Extracto de tráfico de red que se envía por host, registrado por NTOP

También se puede observar la cantidad de datos recibidos o enviados por host, la que al final puede determinar el tráfico total, así como el ancho de banda usado. La Figura 3.6, detalla de mejor manera lo anteriormente expuesto e indica los porcentajes efectuados por cada host.

Local IP Traffic

Host	IP Address	Data Sent		Data Rcvd	
0119adnor.dmq.quitodm.inst		37.0 MBytes	8.4 %	1.5 MBytes	0.4 %
bartpe-4852		14.2 KBytes	0.0 %	0	0.0 %
equipo5.dmq.quitodm.inst		9.1 KBytes	0.0 %	0	0.0 %
eset-server.dmq.quitodm.inst		54.5 KBytes	0.0 %	0	0.0 %
evegal.sonda.com.ec		57.2 KBytes	0.0 %	0	0.0 %
hp.dmq.quitodm.inst		400.6 KBytes	0.1 %	0	0.0 %
hp23037206161		1.2 KBytes	0.0 %	0	0.0 %
jhonatan-4e5480		20.7 KBytes	0.0 %	0	0.0 %
mdmq-2fad7c2104.dmq.quitodm.inst		4.7 KBytes	0.0 %	0	0.0 %
mdmq-73023eace7		5.1 KBytes	0.0 %	0	0.0 %
municipi-67c475		8.8 KBytes	0.0 %	60	0.0 %
norte21.dmq.quitodm.inst		3.1 KBytes	0.0 %	0	0.0 %
pc02admin02.dmq.quitodm.inst		1.0 KBytes	0.0 %	0	0.0 %
.					
.					
.					
pc02tecni39.dmq.quitodm.inst		523.1 KBytes	0.1 %	276.9 KBytes	0.1 %
pc02tecni46.dmq.quitodm.inst		5.4 KBytes	0.0 %	0	0.0 %
pc02tecni47.dmq.quitodm.inst		64.2 KBytes	0.0 %	0	0.0 %
pc02tecni70.dmq.quitodm.inst		9.2 KBytes	0.0 %	0	0.0 %
pc02tecni83.dmq.quitodm.inst		5.9 KBytes	0.0 %	0	0.0 %
pc08tecni08.dmq.quitodm.inst		5.1 KBytes	0.0 %	0	0.0 %
pc19admin154.dmq.quitodm.inst		1.2 KBytes	0.0 %	0	0.0 %
pc19comis148.dmq.quitodm.inst		13.8 KBytes	0.0 %	0	0.0 %
pc19comis148.dmq.quitodm.inst		66.9 KBytes	0.0 %	0	0.0 %
pc19segur127.dmq.quitodm.inst		63.8 KBytes	0.0 %	0	0.0 %
procelec-norte.dmq.quitodm.inst		9.3 KBytes	0.0 %	0	0.0 %
quito-pc10.dmq.quitodm.inst		54.3 KBytes	0.0 %	1.4 KBytes	0.0 %
quito-pc12.dmq.quitodm.inst		6.4 KBytes	0.0 %	0	0.0 %
quito-pc14.dmq.quitodm.inst		45.8 KBytes	0.0 %	0	0.0 %

[1 / 2]

Total Traffic	Data Sent	Data Rcvd	Used Bandwidth
434.1 MBytes	441.6 MBytes	426.5 MBytes	90.6 Kbit/s

Figura 3.6 Información de tráfico IP, registrado por NTOP

Existen también gráficas específicas que denotan valores altos o bajos del rendimiento de la red, las cuales determinan los momentos que han existido fluctuaciones considerables de carga en la red, mostradas en la Figura 3.7; mientras que la Figura 3.8 muestra estadísticas que permiten registrar valores por dominios dependiendo protocolo, datos enviados y datos recibidos.

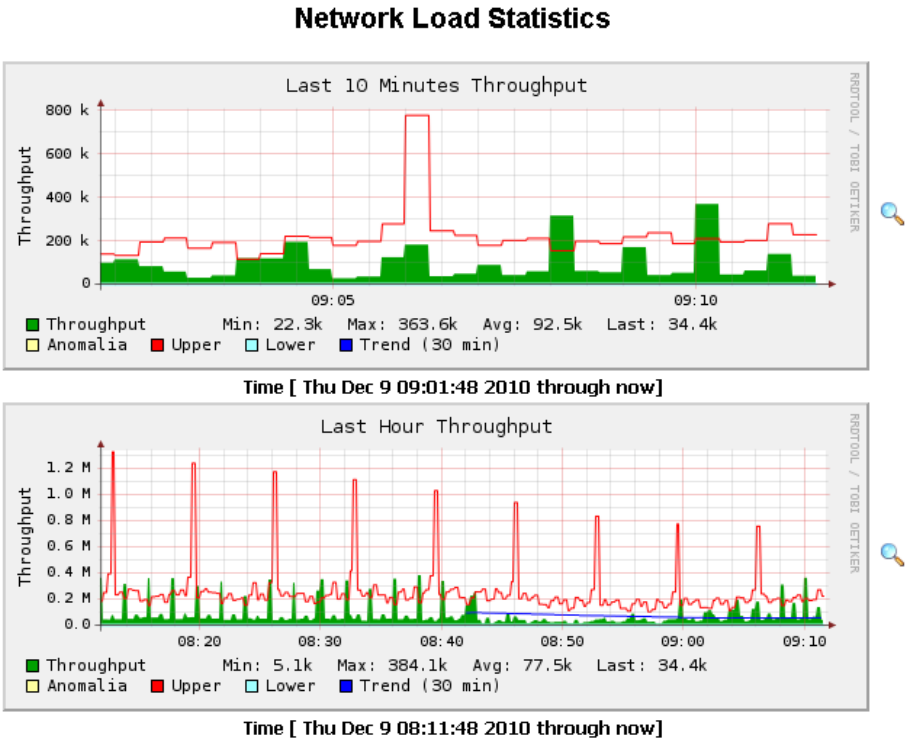


Figura 3.7 Estadísticas de carga de red, registrado por NTOP

Statistics for all Domains

Name	Domains	TCP/IP								ICMP				Graphs
		Total				TCP		UDP		IPv4		IPv6		
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	
avast.com		0	0.0%	1.9 KBytes	0.0%	0	1.9 KBytes	0	0	0	0	0	0	
sonda.com.ec		177.6 KBytes	0.1%	0	0.0%	0	0	57.2 KBytes	0	0	0	0	0	
dmq.quitodm.inst		155.4 MBytes	99.8%	208.5 MBytes	100.0%	136.0 MBytes	208.1 MBytes	14.7 MBytes	223.4 KBytes	52.2 KBytes	78.9 KBytes	0	0	
mcast.net		0	0.0%	960	0.0%	0	0	0	0	0	0	0	0	
localdomain		106.9 KBytes	0.1%	2.7 KBytes	0.0%	0	1.7 KBytes	82.4 KBytes	0	0	814	0	0	

NOTE: The domain is determined by simply stripping off the first name, so for host x.yz.com, the domain is yz.com and for host x.y.z.com, the domain is y.z.com.

Figura 3.8 Estadísticas para todos los dominios, registrado por NTOP

3.1.1.4 Consideraciones de uso

Es importante notar que NTOP, tanto como otras aplicaciones de esta índole, podría plantear una amenaza de seguridad si no se instala y configura apropiadamente. El acceso libre para NTOP por la interfaz Web permite que cualquier usuario con el acceso a la web lea toda la información proveída por NTOP, adquiriendo conocimientos sobre la red.

Una adecuada configuración de la red puede detectar anomalías como:

- Uso de direcciones IP duplicadas.
- Identificación de host locales en modo promiscuo.
- Aplicaciones software que están analizando los datos de tráfico de red.
- Identificación de host que no hacen uso del proxy especificado.
- Identificación de host que están usando protocolos innecesarios.
- Excesiva utilización de ancho de banda de red.

La Tabla 3.3, pretende rescatar parámetros que identifican prestaciones mostradas por NTOP en el ejercicio del análisis.

Parámetro	**Descripción**
Rendimiento	Bueno
Manejo de información	Entendible
Funcionalidades	Expandible por medio de plug-ins
Cantidad de recursos hardware/software para operatividad	Bajo
Plataformas compatibles	UNIX, Win32
Aplicaciones binarias o Paquetes binarios para diferentes UNIX	GNU/Linux, IRIX 6.2, Solaris 2.7 i386/SPARC, HP-UX 11.X, FreeBSD 3.X, AIX 4.1
Software necesario para operatividad respecto al aplicativo base	GDChart, lsof, nmap, bibliotecas OpenSSL, Servidor MySQL
Costo de operación	Bajo
Monitorización de protocolos	TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

Tabla 3.3 Prestaciones principales de NTOP

3.1.2 Nagios

3.1.2.1 Descripción general

Nagios es una acrónimo recursivo (Nagios Ain't Gonna Insist On Sainthood) el cual originalmente fue escrita por Ethan Galstad; presenta un sistema de monitorización de código abierto, escrito en C y utilizado ampliamente por administradores de redes con un licenciamiento GNU General Public License Version 2 publicada por la Free Software Fundation, el mismo proporciona notificaciones del comportamiento de los equipos y servicios en caso de existir problemas. Entre las características principales que figuran se tiene:

- Monitorización de servicios de red (SMTP, POP3, HTTP, NNTP[26], ICMP, SNMP, FTP, SSH o SSL).
- Monitorización de los recursos de sistemas hardware (carga del procesador, uso de discos, memoria, estado de puertos, registros del sistema) por medio de plug-ins como NRPE_NT o NSClient++, estos para sistemas Microsoft Windows; aunque existen plug-ins para varios sistema operativo.
- Monitoreo remoto mediante túneles SSL cifrados o SSH.
- Monitoreo de factores ambientales a través de sondas físicas (temperatura, humedad relativa, luminosidad, líneas de tensión.
- Posibilidad de programar plug-ins específicos según la necesidad en distintas lenguajes como (Bash, C++, Perl, Ruby, Python, PHP, C#).
- Notificación de anomalías por medio de correo electrónico, buscapersonas, mensajes a celular, junto con su respectivo complemento.
- Visualización del estado de la red en tiempo real por medio de su interfaz web, generación de informes, gráficas del comportamiento de los sistemas, notificaciones, historiales, archivos de registro, etc.
- Capacidad de definir una topología o jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Capacidad de acceso para múltiples administradores de red, a la interfaz web sin la tendencia de sobrecarga de información y entornos únicos para cada uno de forma limitada.

[26] **NNTP:** Protocolo de red de transferencia de noticias (Network News Transport Protocol, en inglés) utilizado para la transferencia de artículos entre los servidores, así como leer y publicar artículos.

- Capacidad de acoplarse con complementos de aplicaciones de terceros como cacti[27], MRTG[28], RRD-tool[29].

3.1.2.2 Funcionamiento

Nagios permite la monitorización de host y servicios; además de proporcionar alertas para cuando se producen anomalías. La manera como se accede a Nagios es por medio de su interfaz web la que al ser configurable proporciona información detallada del estado de la red desde cualquier navegador.

La arquitectura extensible que proporciona Nagios permite utilizar más de 200 plug-ins los cuales son desarrollados por la comunidad Nagios; el manejo de plug-ins permite recabar la información que luego será presentada y analizada según la necesidad que demande. El aplicativo hace uso de un servidor web que permite la visualización de los datos sondeados en una página web con un refresco de x minutos, la sintaxis que se aplica en el navegador para acceder remotamente al servidor que contiene Nagios es http://hostname/nagios/ la cual despliega una ventana de autenticación permitiendo el acceso solo al personal encargado, luego de lo cual es posible verificar los datos recabados hasta ese momento en la red.

Nagios siendo un aplicativo que presenta gran versatilidad consulta parámetros detallados del sistema, además tiene la facultad de informar anomalías mediante la generación de alertas que pueden ser recibidas por las personas encargadas del seguimiento del estado de la red, los cuales pueden enviarse por medios como correo electrónico, jabber[30] y mensajes SMS según la configuración que se le haya otorgado

---

[27] **Cacti:** Solución de monitoreo de red, que presenta mediante gráficas el tráfico existente en diferentes puntos de conexión.

[28]**MRTG:** (Multi Router Traffic Grapher) software libre que permite realizar gráficas del comportamiento de red por parte de dispositivos SNMP, de manera que se pueda analizar la performance.

[29] **RRD-tool:** (Round Robin Database Tools) software libre para generación de gráficas de red y estadísticas que además contiene el módulo de integración con el lenguaje Perl.

[30] **Jabber: S**istema de mensajería instantánea basado en el XMPP (Extensible Messaging Presence Protocol) un protocolo extensible, abierto y estándar basado XML (Extensible Markup Language) para el intercambio en tiempo real de mensajes.

inicialmente, además permite el escalamiento de notificaciones que en el caso de no recibir respuesta de la persona informada de la anomalía, prosigue con una notificación al siguiente en la línea de sucesión para que proceda a tomar las medidas correspondientes.

3.1.2.3 Rendimiento y pruebas

A continuación, se exponen algunas capturas de Nagios en las que se pueden apreciar sus funcionalidades más relevantes entorno al gestionamiento de distintos dispositivos de red.

La Figura 3.9, muestra como el sistema proporciona de manera conveniente una pequeña ventana de autenticación en la que es posible filtrar accesos no autorizados al sistema, cabe mencionar que dicha configuración de acceso se la efectúa en el momento de levantar el servidor Nagios con sus prestaciones y servicios.

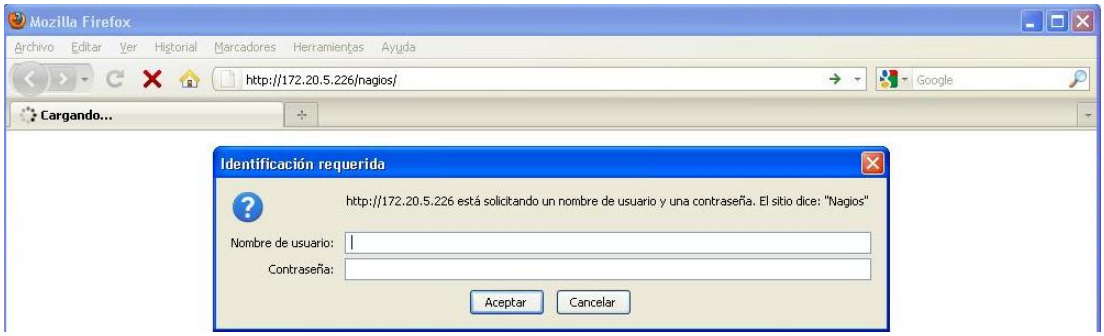


Figura 3.9 Interfaz de autenticación proporcionada por Nagios

Una vez realizada la autenticación necesaria para el ingreso a Nagios, el mismo provee información útil de cómo añadir la configuración adecuada para sondear distintos dispositivos sean estos impresoras de red, switch, routers, host, distintos servicios, etc. De manera centralizada el vínculo de vista táctica permite mostrar desde una sola pantalla las distintas condiciones en las que se pueden encontrar los dispositivos añadidos. La Figura 3.10 a continuación, permite visualizar como gestiona la información de los dispositivos y sus distintos estados.

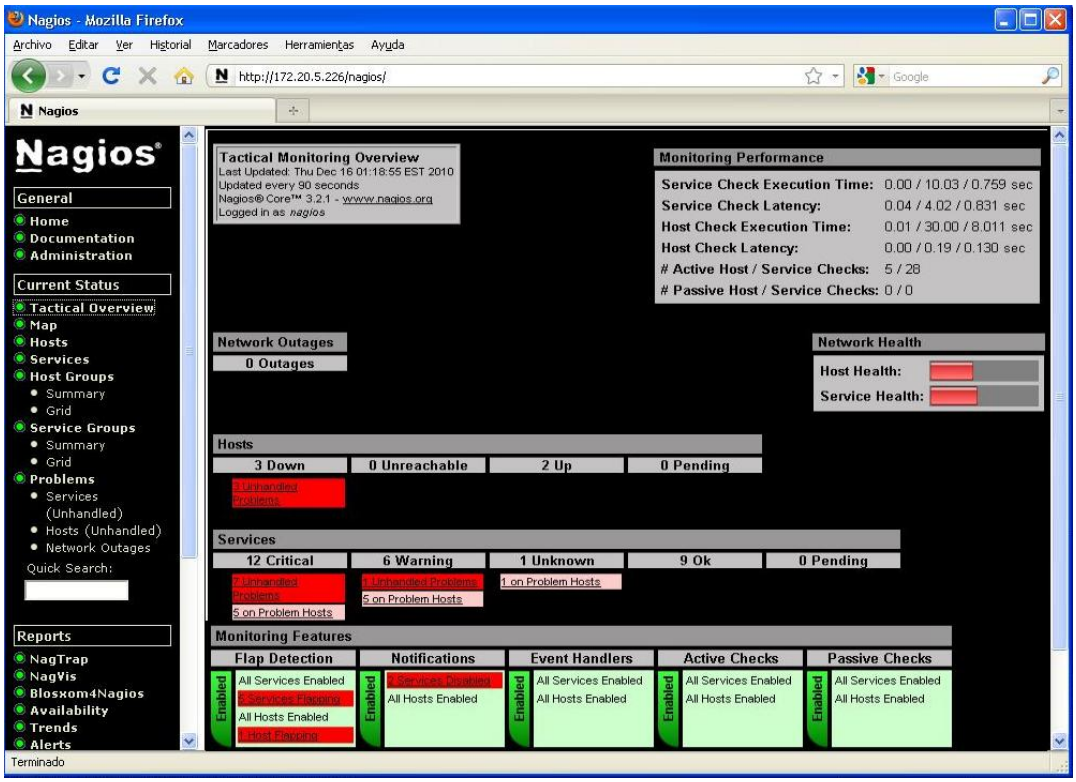


Figura 3.10 Vista Táctica proporcionada por Nagios

El sistema revela información detallada de cada host siguiendo estados de pérdidas de paquetes, chequeos de latencia, notificaciones, últimos chequeos, rendimientos de datos; así a continuación la Figura 3.11, muestra datos relacionados al comportamiento de uno de los hosts.

La existencia de vínculos que permiten activar o desactivar opciones especiales como chequeos para el host, programar próximos chequeos, deshabilitar notificaciones, deshabilitar notificaciones para todos los servicios, detección de fluctuaciones de la operación del host y muchas más opciones, logran una gran operatividad por parte del sistema.

En el caso particular de los datos mostrados para el host de la Figura 3.11, se determina que las notificaciones muestran detalles de cómo existen fluctuaciones de operación entre diferentes estados que van de un 48% al 20%; el porcentaje implica que después de efectuada la fluctuación el host se estabiliza y se detienen los cambios, así las notificaciones quedan reactivadas para posteriores cambios.

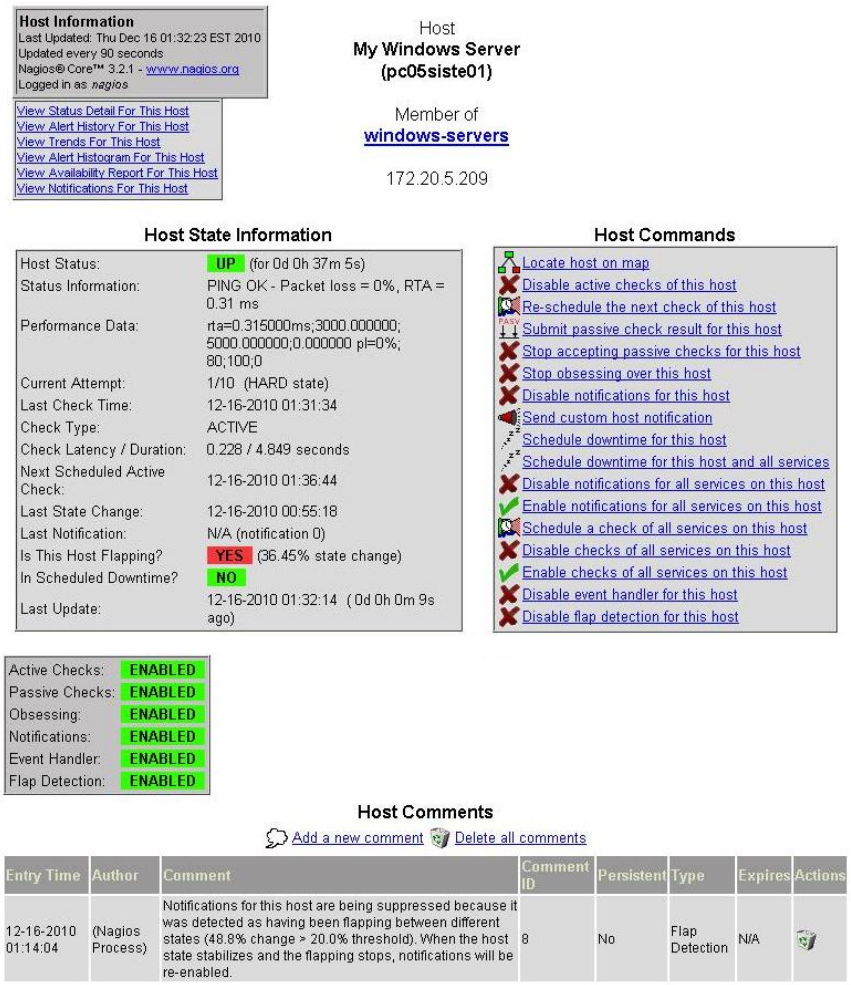


Figura 3.11 Información del estado del host proporcionada por Nagios

Como se puede apreciar en la Figura 3.12, los servicios que determinan el estado de los discos proveen información de su espacio libre, espacio usado; haciendo referencia a uno de los host gestionados se puede concluir que su carga no excede el 7%, además de utilizar NSClient++ 0.3.8.75 el mismo que al ser instalado hace las veces de agente y envía la información obtenida al gestor; también se puede obtener datos precisos del uso de las memorias, notificaciones de los estados, últimos chequeos y alertas.

La facultad de Nagios de acceder a plantillas para presentar la información sondeada otorga al administrador del sistema un mayor entendimiento, dominio del sistema y ofreciendo opciones agradables para mejorar la experiencia con el aplicativo.

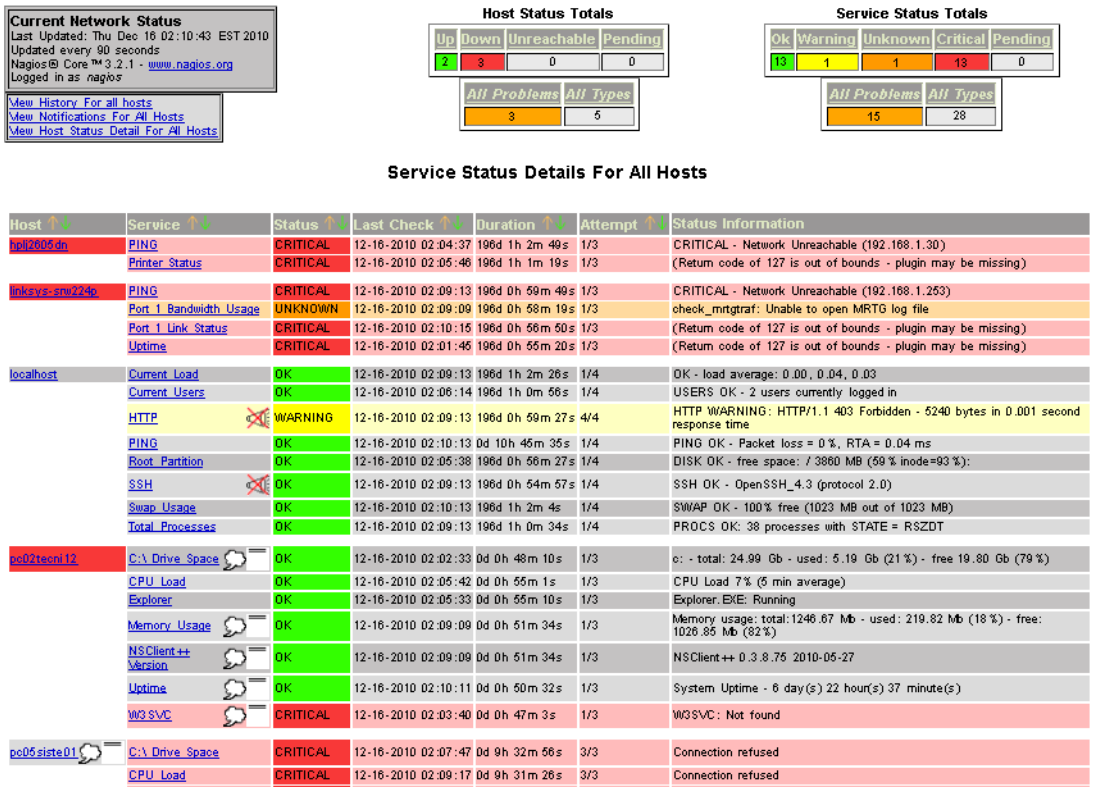


Figura 3.12 Servicios gestionados por Nagios

Existe la posibilidad de acceder de una manera fácil a distintos tipos de consultas que otorgan información del estado de todos los host, estados de los servicios, mapa de red de los host existentes, vista de servicios agrupados por dispositivos (servidores GNU/Linux, servidores Windows, impresoras de red, switch y host de usuarios); cabe mencionar que estas consultas posibilitan de forma clara la detección de problemas de servicios, problemas de host, problemas de red.

Los reportes es una funcionalidad extensible de Nagios ya que permite añadir complementos de gran valor productivo conforme a los datos mostrados; así se tiene complementos como NagVis que provee una visualización dinámica de diagramas estructurales de red, exponiendo los datos de forma clara, en una gráfica del estado actual de la red. También es posible observar reportes en los cuales se escoge tipos de reportes, estado del software, periodos iniciales y finales de tiempo entre muchas opciones. La Figura 3.13 a continuación, muestra las opciones para la creación de un reporte.

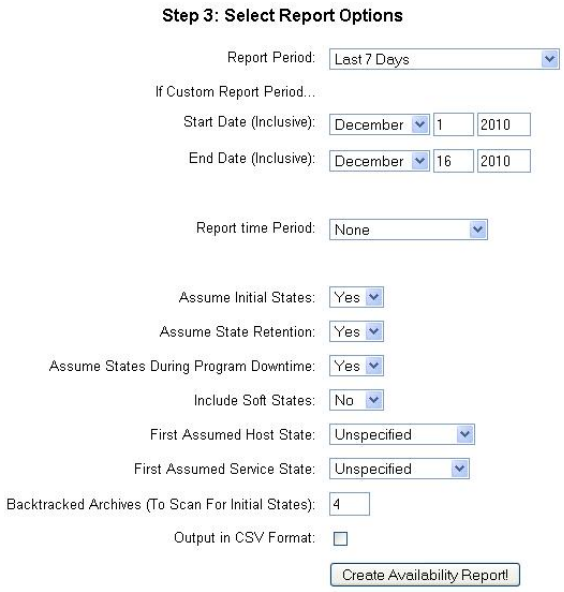


Figura 3.13 Opciones de reporte que proporciona Nagios

El reporte también puede mostrar un histórico de alertas en las que por fechas, tipos de alertas, indican las variaciones que han existido con los dispositivos. A continuación en la Figura 3.14, se puede observar las alertas surgidas en la red, así como los distintos filtros para este tipo de reporte.

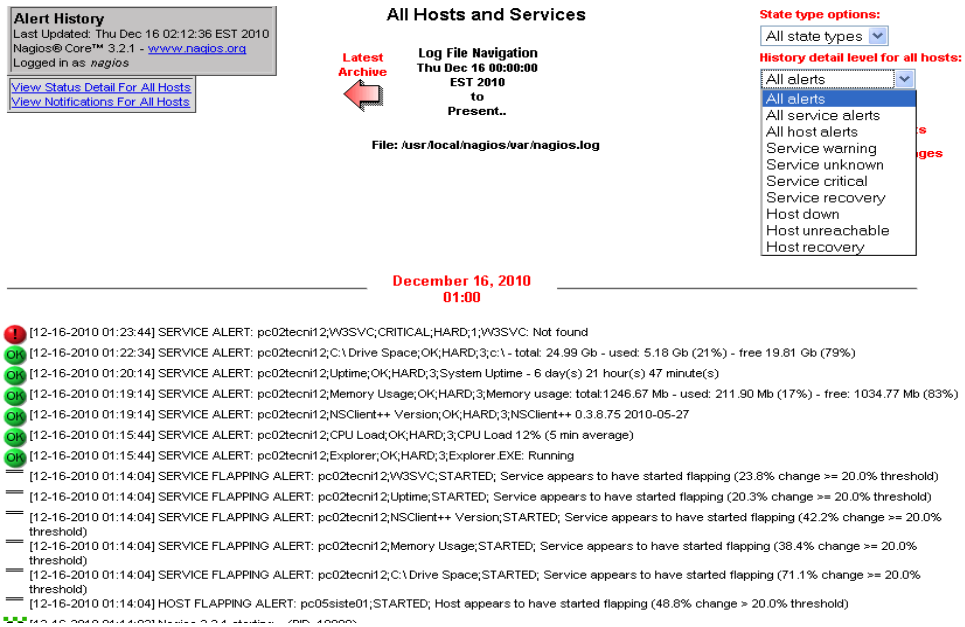


Figura 3.14 Reporte de historial de alertas que proporciona Nagios

Nagios extiende aún más sus posibilidades de uso, gracias a que puede acoplarse con complementos de aplicaciones de terceros. Una forma de observar distintos cambios que se producen en la red sean estos en períodos de minutos, semanas, meses o años es gracias al uso de complementos como MRTG que muestran toda la información sin ningún inconveniente. La gráfica que se presenta en la Figura 3.15, contiene los valores bajos y altos del estado de algunos servicios.

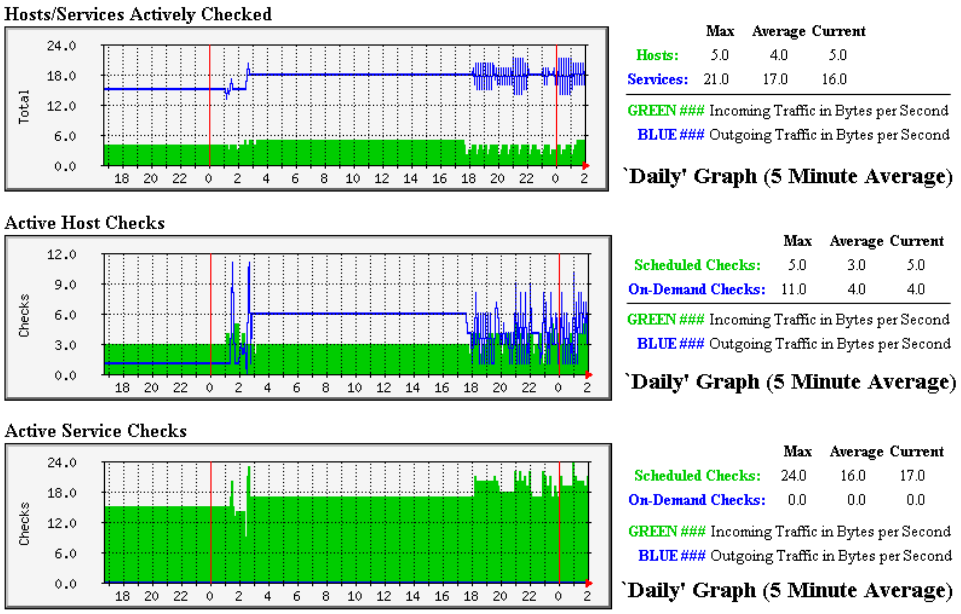


Figura 3.15 Complemento MRTG utilizado por Nagios

3.1.2.4 Consideraciones de uso

Es importante notar que una instalación y configuración completa demanda de la persona que lo realiza un tiempo de aprendizaje significativo por lo que existe una documentación extensa y detallada de la aplicación. Además existen ficheros de configuración de ejemplo que ayudan a la persona inmersa en esta tarea a relacionarse con la sintaxis que se utiliza, logrando disminuir en parte la curva de aprendizaje que demanda. Es de destacar que Nagios permite manejar la información de forma cifrada por SSL/TLS[31] la cual otorga una encriptación simétrica y mantiene una comunicación aceptablemente segura en el Internet.

[31] **SSL/TLS:** (Secure Sockets Layer/Transport Layer Security) protocolos criptográficos que proporcionan comunicaciones de forma segura en el Internet. TLS es la versión más reciente de SSL.

La Tabla 3.4, pretende rescatar parámetros que identifican prestaciones mostradas por Nagios en el ejercicio del análisis.

Parámetro	Descripción
Rendimiento	Bueno
Manejo de información	Entendible
Funcionalidades	Expandible por medio de plug-ins
Cantidad de recursos para operatividad	Bajo
Plataformas compatibles	FreeBSD, Solaris, HP-UX Ubuntu 10.4LTS, Centos5.5, Fedora 14, diferentes variantes de GNU/Linux
Software necesario para operatividad respecto al aplicativo base	Apache 2, Postfix, PHP5, GCC (librerías de desarrollo y compilación), GD (librerías de desarrollo), RRD-tool, Perl, Net::SNMP, Crypt::DES, Zlib, LibjPEG, LibPNG, Freetype2, Graphviz, XFree86-libs, MySQL, GD, Nagvis, PNP4Nagios, NDO, SNMP Plug-ins, NagiosQL. Nota: La instalación puede variar según la distribución GNU/Linux si lo tenemos empaquetado, o si lo tenemos que compilar e instalar manualmente
Costo de operación	Bajo
Monitorización de protocolos	SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH o SSL

Tabla 3.4 Prestaciones principales de Nagios

3.1.3 OpenNMS

3.1.3.1 Descripción general

OpenNMS (Network Management System) es un sistema que permite una supervisión y gestión de red el cual esta licenciado bajo Licencia Pública General GNU. Es la primera plataforma de grado empresarial en el mundo y galardonada como mejor Sistema de Gestión de Herramientas con varios premios por parte de la comunidad TIC (Tecnologías de la Información y de la Comunicación) debido a que es una alternativa a soluciones de pago como HP OpenView [32]o IBM Tivoli[33]. Consta de una comunidad que soporta el proyecto como de una organización que se encarga de la parte comercial, es decir servicios, entrenamiento a los usuarios y soporte.

OpenNMS principalmente escrito en Java, se caracteriza por monitorizar servicios, host que corren en la red, proveer de informes y cuadros estadísticos que detallan anomalías producidas; pero su característica principal es correr en forma distribuida y escalonada en un número ilimitado de dispositivos. Posee funcionalidades de autodescubrimiento de distintos dispositivos conectados a la red.

Entre las características principales que posee el sistema son:

- Servicio de votación: para determinar la disponibilidad del servicio y la latencia, incluyendo la medición distribuida de disponibilidad y latencia, e informar sobre los resultados.

[32] **HP OpenView:** Proporciona un conjunto de aplicaciones comerciales que conforman un sistema a gran escala de gestión de red que gerencia y optimiza los servicios de TI e infraestructura de voz y de datos.

[33] **IBM Tivoli**: Software utilizado para la administración y orquestación empresarial automatizando y administrando la infraestructura de IT (Tecnología de Información) a nivel mundial.

- Recolección de datos: la recogida, almacenamiento y presentación de informes sobre los datos recogidos de los nodos a través de protocolos como SNMP, JMX[34], HTTP, WMI[35], JDBC[36], y NSClient.
- La gestión de eventos: recepción de eventos, tanto internos como externos, incluso a través de SNMP.
- Alarmas y automatizaciones: reducción de los eventos de acuerdo a una clave de reducción de secuencias de comandos y acciones automatizadas en torno a las alarmas.
- Notificaciones: el envío de avisos sobre eventos más importantes a través del correo electrónico, XMPP, o por otros medios.

3.1.3.2 Funcionamiento

Luego de instalar todos los paquetes necesarios para el correcto funcionamiento del sistema para acceder de manera remota al servidor instalado con OpenNMS se debe digitar la ruta de acceso conforme se haya configurado así por ejemplo será http://hostname:8980/opennms que muestra la interfaz de autenticación para acceder a la consola web con la cual luego de loguearse accedemos a las opciones determinadas por la aplicación.

El sistema permite administrar la red de múltiples maneras, así por ejemplo accediendo desde el vínculo de Administración que por obvias razones solo aparecerá si el usuario tiene los permisos respectivos, se obtiene diversas opciones que facilitan su utilización, entre las opciones principales que se presentan tenemos:

- Configuración de usuarios, grupos y roles.
- Configuraciones de descubrimiento de red.

---

[34] **JMX**: (Java Management Extensions) proporciona la tecnología Java de herramientas para la gestión y seguimiento para las aplicaciones, los objetos del sistema, los dispositivos y servicios orientados a redes.

[35] **WMI:** (Windows Management Instrumentation) conjunto de extensiones para el modelo de controladores de Windows.

[36] **JDBC:** (Java Database Connectivity) es un API (Interfaz de Programación de Aplicaciones) para el lenguaje de programación Java que define como un cliente puede tener acceso a una base de datos.

- Configuraciones de nombres de comunidad SNMP por IP.
- Configuración de colección de datos SNMP por interface.
- Administración y no administración de interfaces y servicios.
- Umbrales de administración.
- Configuración de notificaciones.

Una de las maneras más prácticas de sondear la red es utilizando la configuración de descubrimiento de red, la que permite en pocos pasos incluir o excluir rangos de direcciones IP. Incluyendo rangos de direcciones IP permite modificar tiempos de sondeo y reintentos en caso de existir alguna anomalía. Además la opción de descubrimiento permite incluir un sondeo para direcciones web, que es de utilidad si se desea saber que páginas web tienen más actividad.

3.1.3.3 Rendimiento y pruebas

A continuación, se presentan algunas capturas de OpenNMS en las que se exponen sus funcionalidades más relevantes.

La Figura 3.16, muestra la consola web de inicio de sesión la misma que con su respectiva autenticación determina el usuario y los privilegios que este posee. Siendo el caso de usuario administrador, el sistema nos permite acceso total a los parámetros y configuraciones del sistema.

Figura 3.16 Interfaz de autenticación proporcionada por OpenNMS

Luego de proporcionar los datos de autenticación correctos se presenta la interfaz que permitirá un enfoque general de las opciones a gestionar, así por ejemplo si hemos distribuido y configurado adecuadamente las categorías existentes en nuestra red podremos acceder a los datos que cada una de ellas posee. Esta interfaz esta subdividida en bloques que además de observar las categorías permite una visión inmediata de los nodos o host caídos, búsquedas en base a diferentes parámetros, reportes gráficos creados entorno a las necesidades del administrador, reportes de actividad de un host en particular y notificaciones.

La Figura 3.17 mostrada a continuación, presenta los parámetros antes citados. Cabe mencionar que por motivos de pruebas se ha tomado un rango de direcciones IP pequeño que van desde la 172.20.5.63 hasta la 172.20.5.77 sin incluir para el sondeo direcciones de servidores salvo el servidor y consola antivirus, todo esto con el afán de no disminuir el desempeño de la red de la Institución, que para el momento se encontraba poniendo en producción un nuevo sistema enfocado a la recaudación de valores.

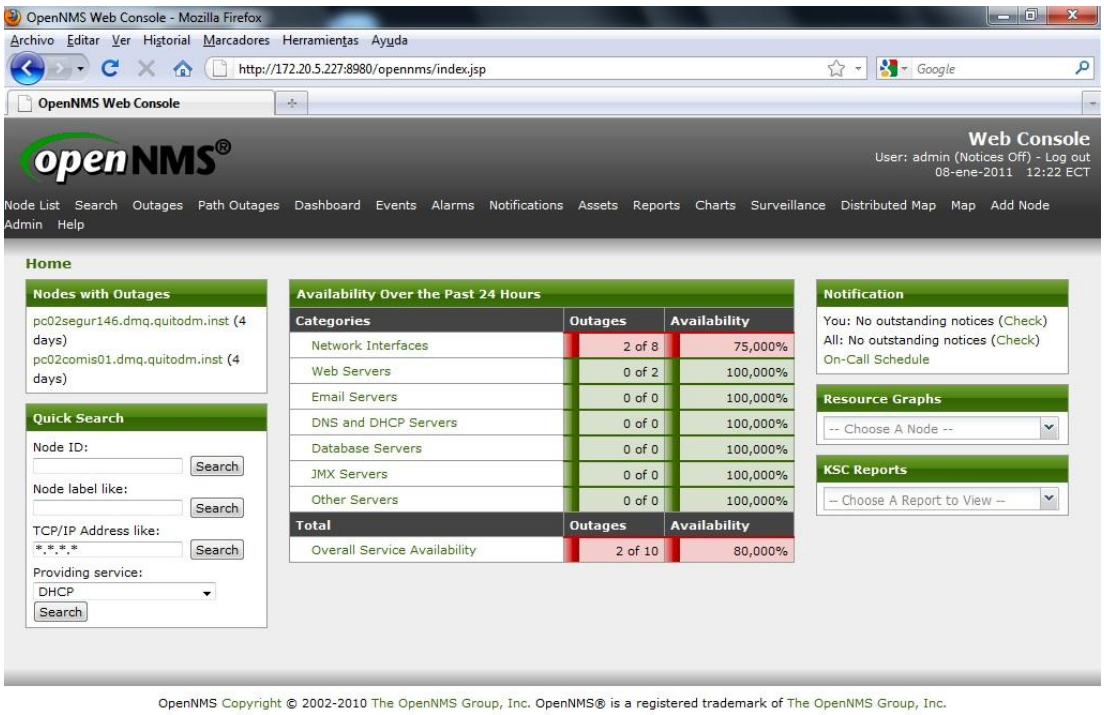


Figura 3.17 Interfaz de inicio proporcionada por OpenNMS

Desde la interfaz principal es posible acceder a búsquedas rápidas por diferentes parámetros como su ID de nodo, etiquetas que identifican un nodo en particular, direcciones IP o una búsqueda por servicios; las búsquedas por servicios se puede indagar por aspectos como DHCP, DNS, FTP, HTTP, HTTP-8080, HTTPS, ICMP, IMAP, NSClient entre muchas otras opciones.

Los datos que denota la interfaz para el momento del sondeo prescribe que existen anomalías en ciertos host, por ende muestra la disponibilidad de solo un 80%; la interfaz permite detectar de manera inmediata en otro bloque cuales son los host que no se encuentran disponibles así para ese sondeo representan los host pc02segur146 y pc02comis01.

La posibilidad de realizar reportes de manera particular o dinámica dependiendo las necesidades otorga a OpenNMS una gran versatilidad. Así la Figura 3.18 a continuación, representa la manera en que se expone un reporte en particular de un host, este a su vez puede ser mostrado con diferentes tipos de periodicidad ya sea esto en día, semana, mes, año o con la oportunidad de personalizar la periodicidad. Personalizar la periodicidad es un proceso práctico que no va más allá de seleccionar sobre el mismo gráfico el intervalo de tiempo y ampliarlo o disminuirlo según la necesidad, pero lo más loable es la capacidad de personalizar los combos de ayuda que permiten una exactitud de meses, días, años y hasta horas.

La información que arroja la Figura 3.18, manifiesta que han existido variaciones considerables en ese periodo de tiempo siendo la más representativa la ubicada a medio día, lo que indica un incremento de tráfico para ese momento que por lo general es un indicativo común para esas horas debido al aumento de actividades por parte de los usuarios y las distintas transacciones que ejecutan.

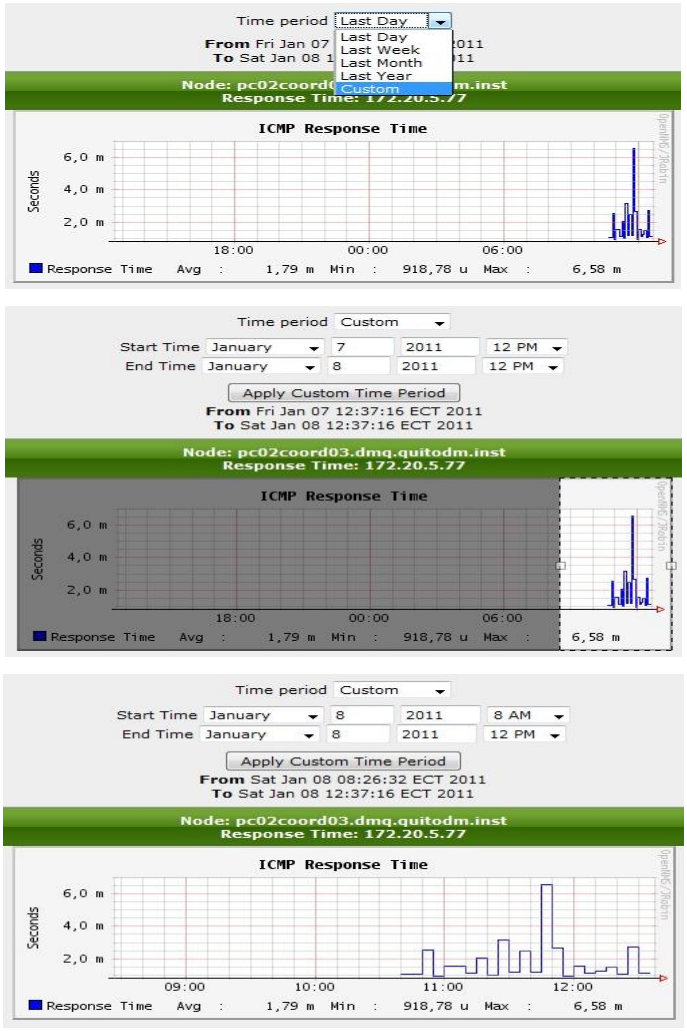


Figura 3.18 Reporte de host y evolución de personalización de periodicidad

Otra forma de mostrar la información es mediante reportes dinámicos los mismos que permiten crear, visualizar y editar reportes personalizados que contienen cualquier número de reportes prefabricados, de cualquier recurso de gráfico disponible, lo que no es posible en un reporte simple; este tipo de reporte puede enfocarse en datos más concisos como tiempos, servicios (en host que habilitan distintos servicios como ICMP, HTTP, HTTP-8080, etc), manipulación global del espacio de tiempo y manipulación global del tipo de gráfico prefabricado. A continuación la Figura 3.19, esboza lo anteriormente expuesto.

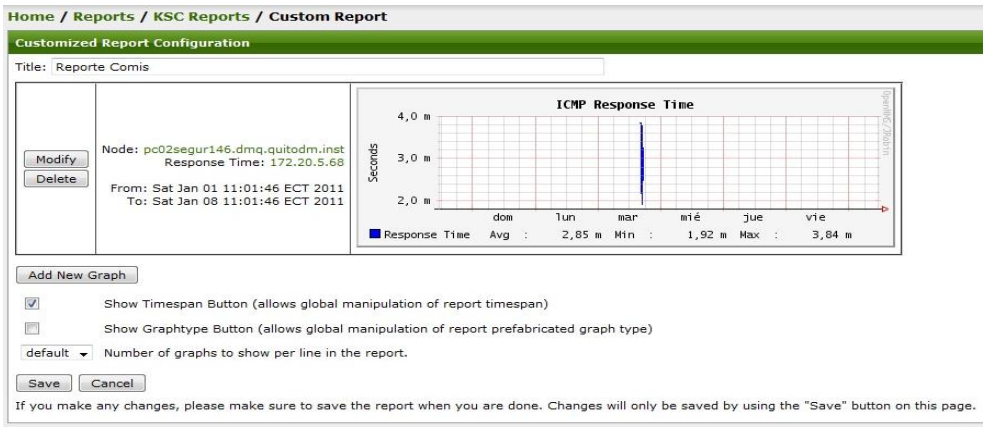


Figura 3.19 Reporte dinámico con ICMP

OpenNMS provee de información detallada para cada uno de sus nodos o host así este puede denotar eventos recientes, disponibilidad, interfaces físicas, interfaces IP, notificaciones y categorías. Como se muestra a continuación en la Figura 3.20, se permite apreciar detalles específicos de la disponibilidad del host en las últimas 24 horas, para esta disponibilidad acoge ciertos parámetros como sondeo por ICMP, StrafePing [37]y Telnet que en conjunto otorgan el nivel de disponibilidad; así también cualquier evento que ocasione una descompensación de los servicios, se muestra como una alerta para realizar las correcciones pertinentes.

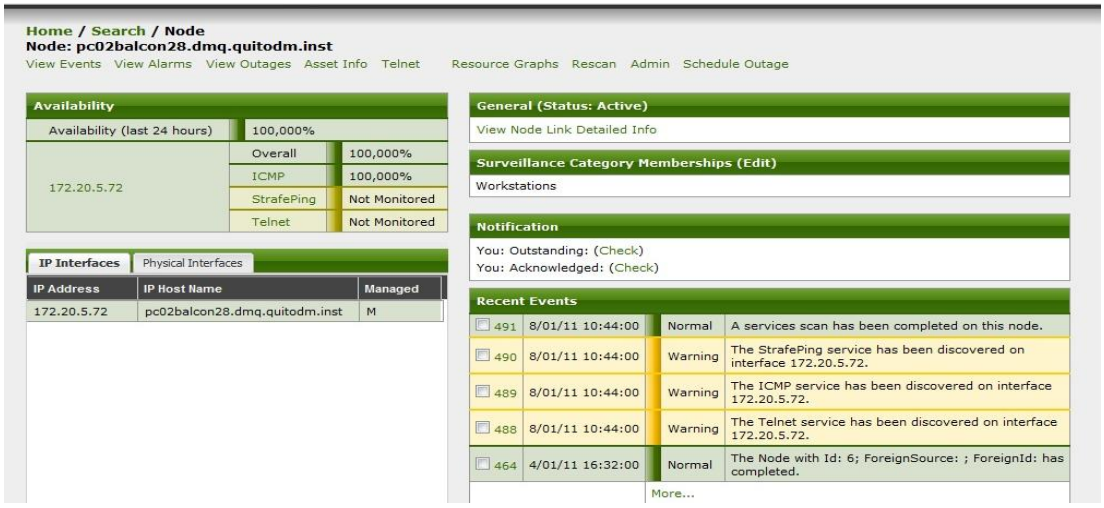


Figura 3.20 Parámetros de situación de host

[37] **StrafePing**: Similar a SmokePing el cual realiza un seguimiento de la latencia de la red. Este tipo de monitor realiza múltiples solicitudes ICMP echo (ping) y almacena el tiempo de respuesta de cada uno, así como la pérdida de paquetes, en un archivo de RRD.

Existen tipos de host que para conocer su disponibilidad abarcan servicios como ICMP, HTTP, HTTP-8080 y StrafePing; así el caso del servidor y consola antivirus. Igualmente la representación de los reportes para este tipo de host equipara una gráfica conjunta de estos servicios. La Figura 3.21 y 3.22 respectivamente evidencia lo anteriormente mencionado.

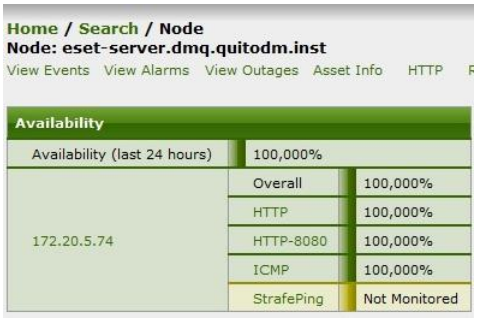


Figura 3.21 Disponibilidad de host con distintos servicios

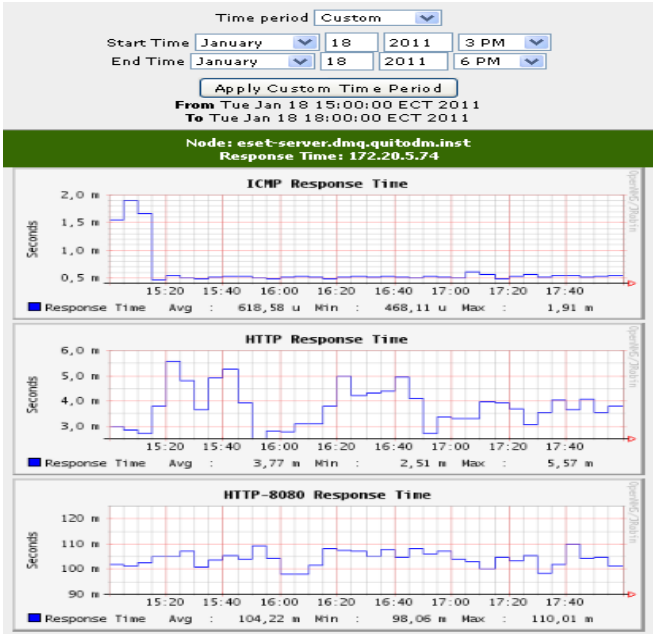


Figura 3.22 Reporte conjunto con distintos servicios

La perspectiva que da OpenNMS para el manejo de anomalías por medio de eventos evidencia una forma distinta de manejar problemas presentes dentro de una red, este manejo muestra detalles que permite un mejor entendimiento de la anomalía suscitada; así una representación de los detalles que contiene un evento se los aprecia a continuación en la Figura 3.23.

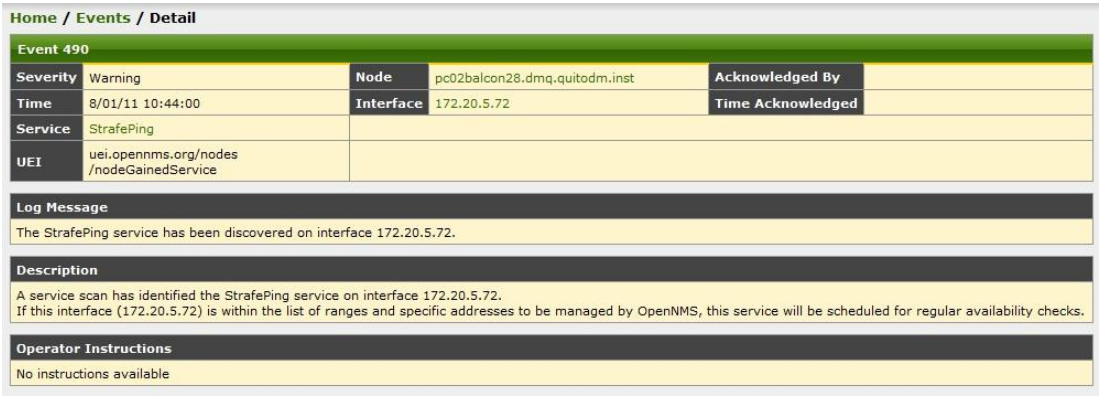


Figura 3.23 Detalle de evento para un host

También es posible analizar este tipo de evento de forma conjunta, por la severidad que representa o realizar una búsqueda avanzada que determine un aspecto en particular (tipo de servicio, criticidad). La Figura 3.24, muestra un listado de eventos acontecidos para uno de los host.

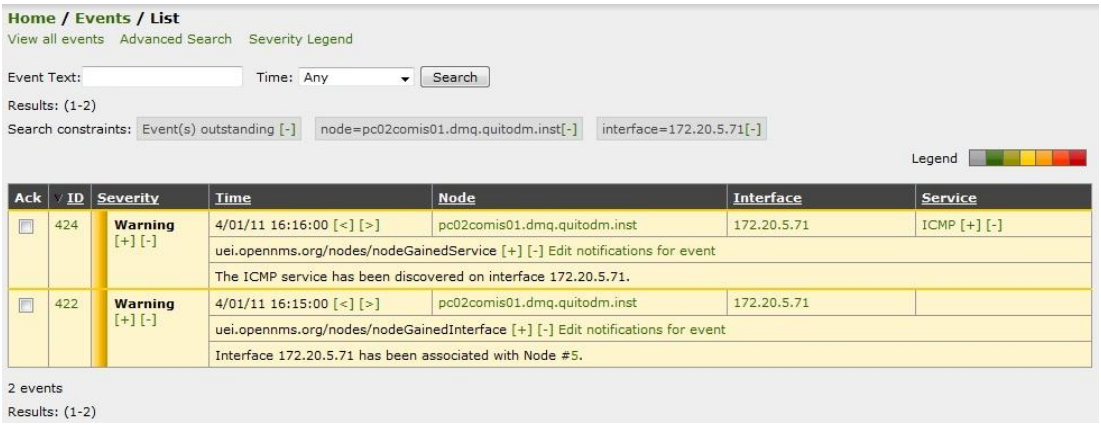


Figura 3.24 Listado de eventos para un host

3.1.3.4 Consideraciones de uso

Debido a que OpenNMS ofrece una escalabilidad y flexibilidad que otros sistemas sean estos comerciales o libres no han podido igualar, ha sido galardonado en distintas ocasiones frente a aplicaciones de renombre internacional; así una de las causas que hace más atractiva su adopción por parte de empresas grandes es la detección automática que posee, la misma que facilita enormemente si se toma en

cuenta que una empresa de esas dimensiones alberga miles de dispositivos ahorrando horas de horas de configuración.

El modelo de datos básico que maneja el sistema menciona que un dispositivo físico debe corresponder a un nodo en OpenNMS. Esto no siempre es así, como las máquinas virtuales pueden aparecer como si fueran máquinas reales. El nodo soporta al menos una interfaz IP, y en esa interfaz serán algunos servicios.

La Tabla 3.5, pretende rescatar parámetros que identifican prestaciones mostradas por OpenNMS en el ejercicio del análisis.

Parámetro	**Descripción**
Rendimiento	Bueno
Manejo de información	Entendible
Funcionalidades	Expandible por medio de plug-ins en el caso de NSClient, NSClient++
Cantidad de recursos para operatividad	Bajo
Plataformas compatibles	Mandrina, Debian, Ubuntu, Red Hat, SuSe, Mac OS X, Windows, Solaris, FreeBSD, OpenBSD, Gentoo, CentOS
Software necesario para operatividad respecto al aplicativo base	Java 1.6 SE JDK, PostgreSQL, tomcat, RRDtool, curl
Costo de operación	Bajo
Monitorización de protocolos / Disponibilidad de servicio	Sesiones BGP, Citrix Metaframe, Procedimientos Almacenados (Oracle, PostgreSQL, MySQL, SQL Server, entre otros), SNMP, JMX, HTTP, WMI, JDBC, DHCP, DNS, FTP, HTTP, HTTPS, ICMP Ping, StrafePing, LDAP, LDAPS, SMTP, POP3, IMAP, IIOP Lotus Domino, NTP, Autenticación RADIUS, Telnet SSH, NRPE, NSClient y NSClient++

Tabla 3.5 Prestaciones principales de OpenNMS

3.1.4 Webmin

3.1.4.1 Descripción general

Webmin es un sistema enfocado en la realización de tareas comunes de administración de múltiples servidores GNU/Linux y Unix.
El sistema es desarrollado por Jamie Cameron conjuntamente con toda la comunidad detrás del proyecto; escrito en Perl versión 5 y ejecutando su propio servidor web, Webmin elimina la necesidad de editar manualmente los archivos de configuración sean estos de Unix o GNU/Linux permitiendo administrar un sistema desde la consola o de forma remota.

El diseño modular que posee el sistema otorga la facilidad de añadir nuevas funcionalidades escribiendo extensiones que ayuden a una tarea en particular. Es así que el modo de actuar de los módulos es encargarse de la administración de una parte concreta del sistema operativo y de los diferentes servicios que se tengan instalados.

Webmin posee versiones de desarrollos paralelos como Usermin y Virtualmin las mismas que son ofrecidas como módulos. Usermin es una versión reducida de Webmin, adecuada para administradores que solo necesitan las funciones esenciales, como administración de servidores web y correo; mientras que Virtualmin es una alternativa a Plesk y Cpanel, para administrar servidores virtuales, dominios, servidores de correo y bases de datos. [21]

Además existe un tercer desarrollo ligado a su aplicativo principal, conocido como Cloudmin el cual trata de una interfaz de usuario desarrollada sobre Webmin para la gestión de sistemas virtuales como Xen[38], KVM[39] e instancias de OpenVZ[40]. Cloudmin es adecuado para crear, destruir, cambiar el tamaño, arranque/parada y restringir el uso de varias instancias de distintas tecnologías de virtualización desde una única interfaz.

[38] **Xen:** Monitor de máquina virtual (hypervisor) de código abierto en la industria de la virtualización que permite implementar distintas instancias de máquinas virtuales.

[39] **KVM: (Kernel-based Virtual Machine)** Software de código abierto que permite implementar virtualización completa con Linux sobre hardware x86.

[40] **OpenVZ:** Es una tecnología de virtualización en el nivel de sistema operativo para Linux. [22]

Webmin es un sistema multiplataforma licenciado bajo BSD, el cual posee características importantes como:

- Configuración de múltiples sistemas desde un servidor maestro.
- Configuración de los propios módulos de Webmin.
- Configurar el sistema operativo, sus usuarios, espacio, servicios, configuraciones, apagado del equipo.
- Configurar y controlar aplicaciones libres como Apache, Sendmail, Squid, Samba, PHP, MySQL, PostgreSQL, servicios de FTP, DNS, DHCP y otros más.
- Permite escribir módulos propios para el aplicativo e incluso temas.
- Permite controlar varias máquinas a través de una interfaz simple, o iniciar sesión en otros servidores Webmin de la misma subred o red de área local.

3.1.4.2 Funcionamiento

Webmin por defecto se comunica a través del puerto TCP 10000, y puede ser configurado para usar SSL si OpenSSL[41] está instalado con módulos de Perl adicionales requeridos. [24]
El aplicativo es accesible vía web lo que permite una administración desde cualquier punto de nuestra red local o remotamente cifrando las conexiones con SSL.

Para acceder a las distintas funcionalidades que ofrece Webmin se debe conectar a la ruta que se haya definido, la sintaxis que se aplica en el navegador para acceder remotamente al servidor que contiene Webmin es http://hostname:10000/ la cual despliega una ventana de autenticación permitiendo el acceso solo al usuario debidamente acreditado, luego de lo cual es posible verificar las diferentes funcionalidades que ofrece el aplicativo.

[41] **OpenSSL:** Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS). [23]

Webmin posee aproximadamente 113 módulos estándar, mientras que muchos otros módulos son diseñados por terceros. A continuación la Tabla 3.6, detalla una lista de algunos de los módulos estándar más utilizados:

Nombre	Descripción	Soporte
BIND 4 de servidor DNS	Creación y edición de dominios y registros de DNS.	La mayoría de los sistemas operativos.
BIND DNS Servidor	Creación y edición de dominios, registros de DNS, opciones de BIND y puntos de vista.	La mayoría de los sistemas operativos.
Sistema de copias de seguridad Bacula	Configuración de Bacula para realizar copias de seguridad y restaurar de forma manual o en la fecha prevista, para los sistemas de uno o muchos.	Todos los sistemas operativos.
Administrador de Archivos	Ver, editar y cambiar los permisos de archivos y directorios en su sistema con un gestor de archivos al estilo Windows.	Todos los sistemas operativos.
Gestor de arranque GRUB	Configurar el gestor de arranque GRUB Linux para permitir la selección de varios sistemas operativos en el arranque.	Linux y Sun Solaris.
Servidor de mensajería instantánea Jabber	Configuración multi-protocolo de servidor de mensajería Jabber.	Todas, excepto los de Windows.
Servidor SSH	Configurar el servidor SSH para inicios de sesión remoto en forma segura.	Todos los sistemas operativos.
Túneles SSL	Configuración de túneles SSL para encriptar servicios como POP3 e IMAP.	Todas, excepto los de Windows.

Tabla 3.6 Módulos estándar más utilizados en Webmin

3.1.4.3 Rendimiento y pruebas

A continuación, se exponen algunas capturas de Webmin en las que se pueden apreciar sus funcionalidades más relevantes entorno a la administración de sistemas y los módulos cargados.

La Figura 3.25, permite apreciar como el sistema proporciona con fines de seguridad una ventana de autenticación para el logueo del personal autorizado que se va a encargar de administrar los distintos sistemas (sean estos servidores y en menor medida host) que se encuentren ubicados dentro de la red.

Figura 3.25 Interfaz de autenticación proporcionada por Webmin

Una vez que se haya accedido al sistema este proporciona información concerniente al hardware y al software que estamos utilizando, así como la cantidad de procesos que están ejecutándose en ese momento, el promedio de carga del CPU, el estado de la memoria física, el estado de la memoria virtual y el espacio utilizado por el disco local. La Figura 3.26, muestra la información antes mencionada así como también las diferentes opciones que permiten acceder a la administración.

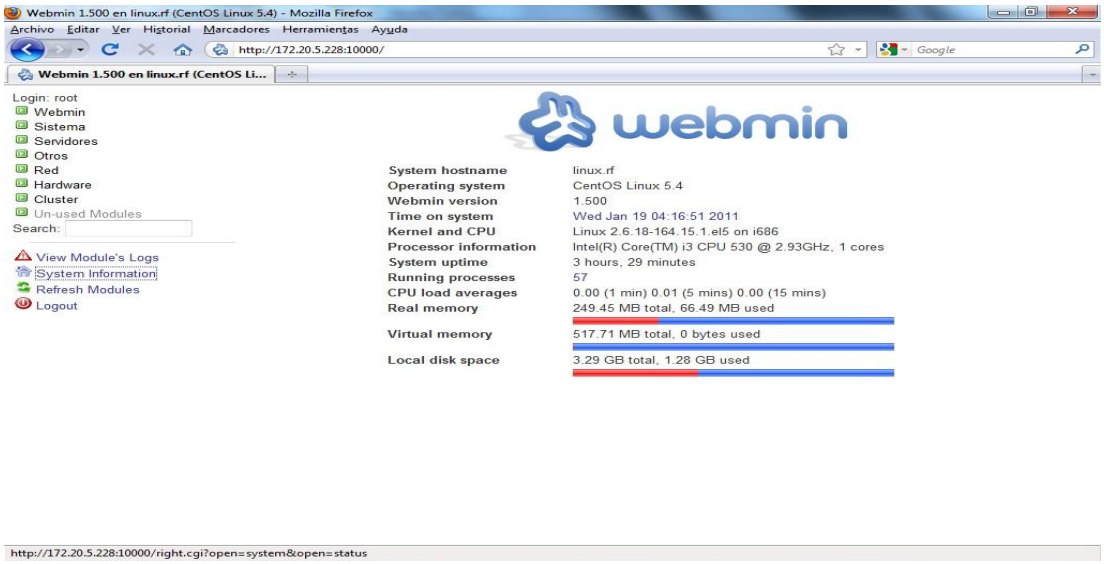


Figura 3.26 Interfaz de inicio proporcionada por Webmin

El vínculo Webmin permite la configuración interna de los parámetros generales de Webmin. También permite administrar usuarios, módulos, configuraciones de idioma y tema, copia de seguridad de archivos de configuración, histórico de acciones y búsqueda de otros servidores Webmin dentro de la red. En la Figura 3.27, se observa las distintas opciones de configuración interna de Webmin.

Figura 3.27 Interfaz de configuración interna de Webmin

El vínculo Sistema provee opciones para administrar el servidor, esto puede ser cambios de contraseñas, usuarios y grupos, copias de seguridad, paquetes de software, opciones de arranque/parada entre otras. A continuación la Figura 3.28, muestra los usuarios locales que posee Webmin, así también se encuentran presentes opciones que facilitan crear, modificar y borrar usuarios según las necesidades que se tengan.

Figura 3.28 Usuarios y grupos que conforman Webmin

El vínculo Servidores muestra los servidores (Apache, MySQL, SSH, ProFTPD) que se encuentran instalados y que se pueden configurar y administrar. Dependiendo el tipo de servidor que se quiera administrar el aplicativo presenta opciones específicas para cada uno de ellos. En la Figura 3.29, se puede observar el servidor de bases de datos (MySQL) el cual tiene albergado ciertas bases de datos a las cuales se pueden asignar parámetros como permisos de tabla, de usuario, de máquina, etc y establecer conexiones o algún tipo de cambio de índole intrínseco a la base de datos.

Figura 3.29 Servidor MySQL y opciones de configuración

El vínculo Otros contiene ciertos módulos que no encajan en otras secciones así se tiene opciones variadas como conexiones por Telnet y SSH, explorador de archivos, creación de comandos personalizados, ejecución de comandos, estado del sistema y del servidor entre las opciones más destacadas. Las opciones concernientes al estado del sistema y del servidor se las presenta en la Figura 3.30 a continuación; de la que se puede rescatar que es posible añadir distintos tipos de monitores para conocer su estado.

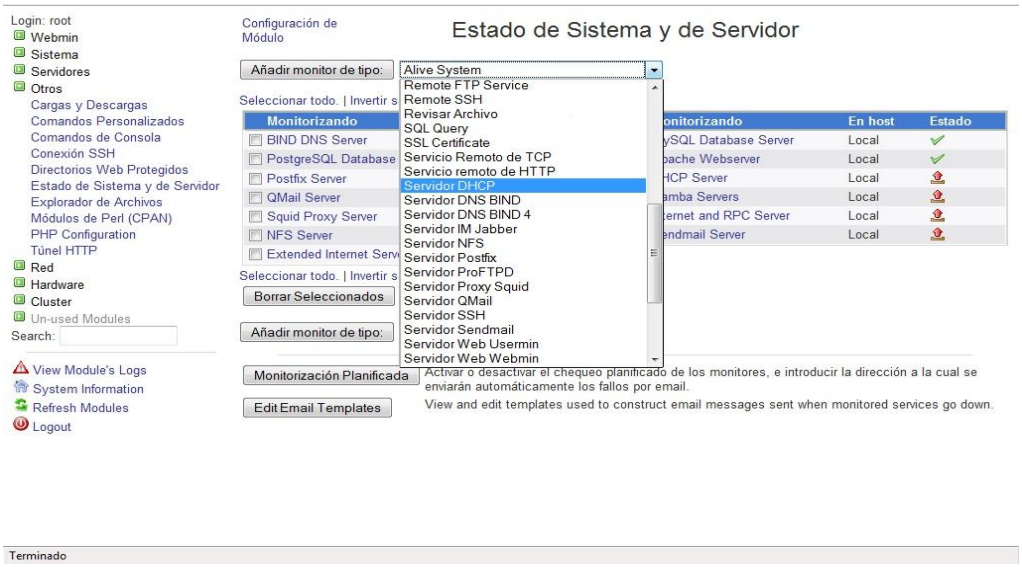


Figura 3.30 Estado de Sistema y de Servidor

El vínculo Red por otro lado presenta herramientas de monitorización de ancho de banda, configuraciones de red, cortafuegos con accionar sobre paquetes (entrantes, redirigidos, salientes) que permiten establecer ciertas configuraciones, esto de entre las opciones más destacadas. A continuación la Figura 3.31, permite de una manera muy simplista tener una idea del tráfico existente que aunque tiene opciones de filtrado genera un informe escasamente detallado.

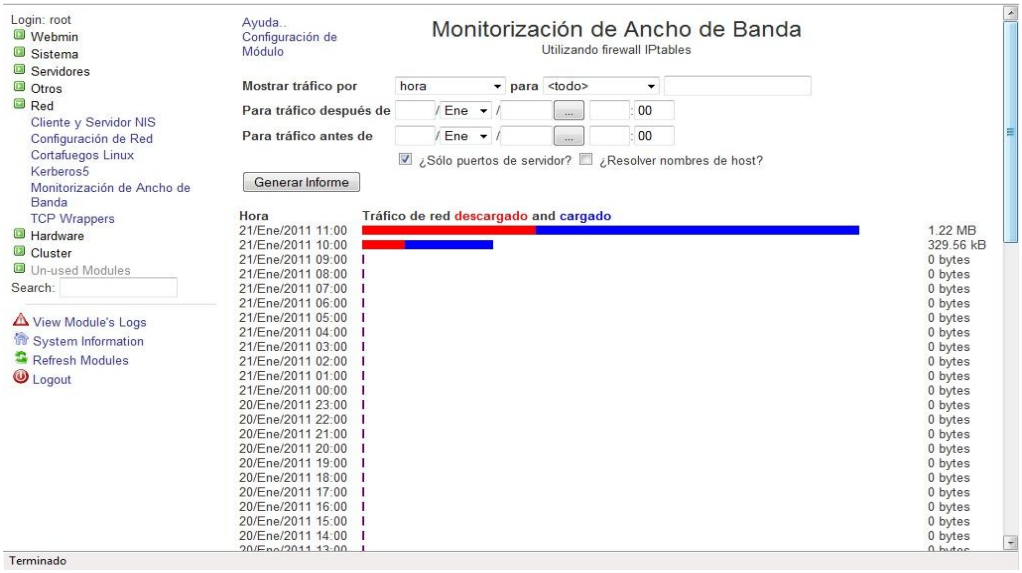


Figura 3.31 Monitorización de Ancho de Banda

El vínculo Hardware posibilita administrar impresoras, nuevas opciones de arranque en GRUB, discos duros y sus particiones, la hora del sistema e incluso grabadoras de CD. La Figura 3.32, muestra cómo están conformadas las particiones del disco y permite agregar particiones primarias o extendidas según la necesidad, también permite editar los parámetros que se tienen para ese momento.

Figura 3.32 Particiones en Discos Locales

El vínculo Clúster permite una administración a ese nivel, con opciones sobre el dispositivo que admiten, crear tareas, cambiar usuarios, ejecutar comandos y copiar ficheros. A estos equipos se los puede definir desde el vínculo Webmin, introduciendo su dirección IP, usuario y clave en Índice de Servidores Webmin.

El sistema permite observar que tipos de módulos se pueden añadir para mejorar nuestra interacción y administración de los sistemas; los módulos sin usar (no se encuentran instalados) se despliegan desde el último vinculo presente y da la facultad de gestionar más ampliamente nuestro sistema. Se puede determinar que cada módulo se enfoca en gestionar diferentes aspectos como gestionar el o los servidores, gestionar paquetes, gestionar la red, gestionar usuarios y poseer una gestión de seguridad.

3.1.4.4 Consideraciones de uso

Debido a que la traducción de Webmin a diferentes idiomas es realizado por voluntarios, no todas las traducciones se han finalizado completamente. De entre 40 idiomas accesibles el inglés es el único que proporciona una traducción total, mientras que las traducciones al español solo bordean el 63% por debajo de traducciones al catalán, holandés o el checo.

Webmin otorga una modularidad que pocos sistemas tienen y la relativa facilidad de uso tanto como su flexibilidad proponen un sistema muy adecuado para entornos GNU/Linux aunque posibilita entornos Windows.

La Tabla 3.7 a continuación, pretende rescatar parámetros que identifican prestaciones mostradas por Webmin en el ejercicio del análisis.

Parámetro	Descripción
Rendimiento	Bueno
Manejo de información	Relativamente entendible respecto al nivel alto de gestionamiento de diferentes servidores y servicios que acoge.
Funcionalidades	Expandible por medio de módulos que permiten la administración, configuración, edición, etc. de diversos servidores y servicios.
Cantidad de recursos para operatividad	Medio acorde a módulos.
Plataformas compatibles	Los mejores sistemas de apoyo son Solaris, Red Hat y FreeBSD mientras que los que son compatibles entre los principales tenemos Mandrina, Debian, Ubuntu, SuSe, Windows, OpenBSD, Gentoo, CentOS, IBM AIX.
Software necesario para operatividad respecto al aplicativo base	Perl, OpenSSL, MySQL, Apache, PHP, Sendmail.
Costo de operación	Bajo
Monitorización de protocolos / Disponibilidad de servicio	DHCP, BIND DNS, NIS, NFS, Samba, ProFTPD, FTP, Telnet, LDAP, MySQL, PostgreSQL, SSH.

Tabla 3.7 Prestaciones principales de Webmin

3.1.5 JFFNMS

3.1.5.1 Descripción general

JFFNMS (Just For Fun Network Management System) es un sistema basado en web que permite la gestión y monitorización de red el cual esta licenciado bajo Licencia Pública General GNU. El sistema hace uso del lenguaje PHP para recoger y mostrar la información de diversos dispositivos disponibles en una red.

JFFNMS proyecto desarrollado por Javier Szyszlican se encuentra en constante evolución puede ser utilizado para monitorizar cualquier dispositivo SNMP, servidor, router, puerto TCP o cualquier elemento que se desee siempre que se programe una extensión adecuada a dicho elemento para JFFNMS.

Entre las características principales que posee el sistema son:

- Permite monitorizar una red IP mediante SNMP, Syslog[42] y Tacacs+.[43]
- Dispone de características orientadas al manejo de dispositivos Cisco.
- Posee una consola de eventos que muestra todos los tipos de eventos de manera ordenada en el mismo Display.
- Generación de gráficas para todos los dispositivos de la red, tráfico de red, utilización de CPU, etc.
- Soporte de base de datos MySQL o PostgreSQL, integra logs de Syslog y autenticación e informes de Tacacs+.
- Modular y extensible lo que permite programar extensiones en caso de no disponer soporte para un elemento especifico de la red.
- Dispone de un mapa de estado que permite visualizar la red de manera sencilla.

[42] **Syslog:** Estándar de facto para el envío de mensajes de registro en una red informática IP.

[43] **Tacacs+: S**istema de Control de Acceso del Controlador de Acceso a Terminales (Terminal Access Controller Access Control System, en inglés) es un protocolo de autenticación remota que se usa para gestionar el acceso (proporciona servicios separados de autenticación, autorización y registro) a servidores y dispositivos de comunicaciones. [25]

3.1.5.2 Funcionamiento

Luego de concluir con la instalación y configuración de todos los paquetes necesarios para el funcionamiento, el sistema permite monitorizar dispositivos a través de la utilización del protocolo SNMP. Para realizar el sondeo es necesario configurar el planificador del sistema lo que conlleva a que se ejecute periódicamente y así actualice toda la información. JFFNMS luego de identificar la red y los dispositivos conectados a ella permite identificar las interfaces de cada dispositivo permitiendo monitorizar elementos dentro de un dispositivo como memoria, almacenamiento, etc. Para llegar a este tipo de monitoreo es necesario definir y configurar los dispositivos de tal manera que los valores de las variables que representan las interfaces sean recogidos dentro de una MIB.

La información recogida por JFFNMS permite determinar el estado de los dispositivos si se encuentran activos o inactivos, realizar gráficas de rendimientos, mostrar alarmas cuando se alcanzan ciertos límites.

Para acceder al sistema se digita en el navegador web el nombre asignado inicialmente en el servidor web así por ejemplo será http://server1.dmq.com lo cual permitirá ingresar a la interfaz inicial que mostrará los parámetros de las configuraciones realizadas y permitirá cerciorarse que las rutas de los distintos directorios estén correctos; luego de lo cual accediendo al vínculo main se presentará una pequeña ventana de autenticación que facilitará el ingreso al usuario debidamente autorizado. Cabe mencionar que el usuario administrador es el que determina el nivel de acceso para cada usuario creado, permitiendo el acceso a parámetros generales y denegando accesos de configuración.

3.1.5.3 Rendimiento y pruebas

A continuación, se exponen algunas capturas de JFFNMS en las que se pueden apreciar sus funcionalidades más relevantes.

La Figura 3.33 a continuación, presenta en primera instancia la interfaz en la que se constatan las rutas de los directorios y las configuraciones realizadas. Se puede detectar ciertos errores que involucran directamente directorios que enfocan una raíz GNU/Linux que no están siendo tomadas en cuenta al tratarse de otro entorno.

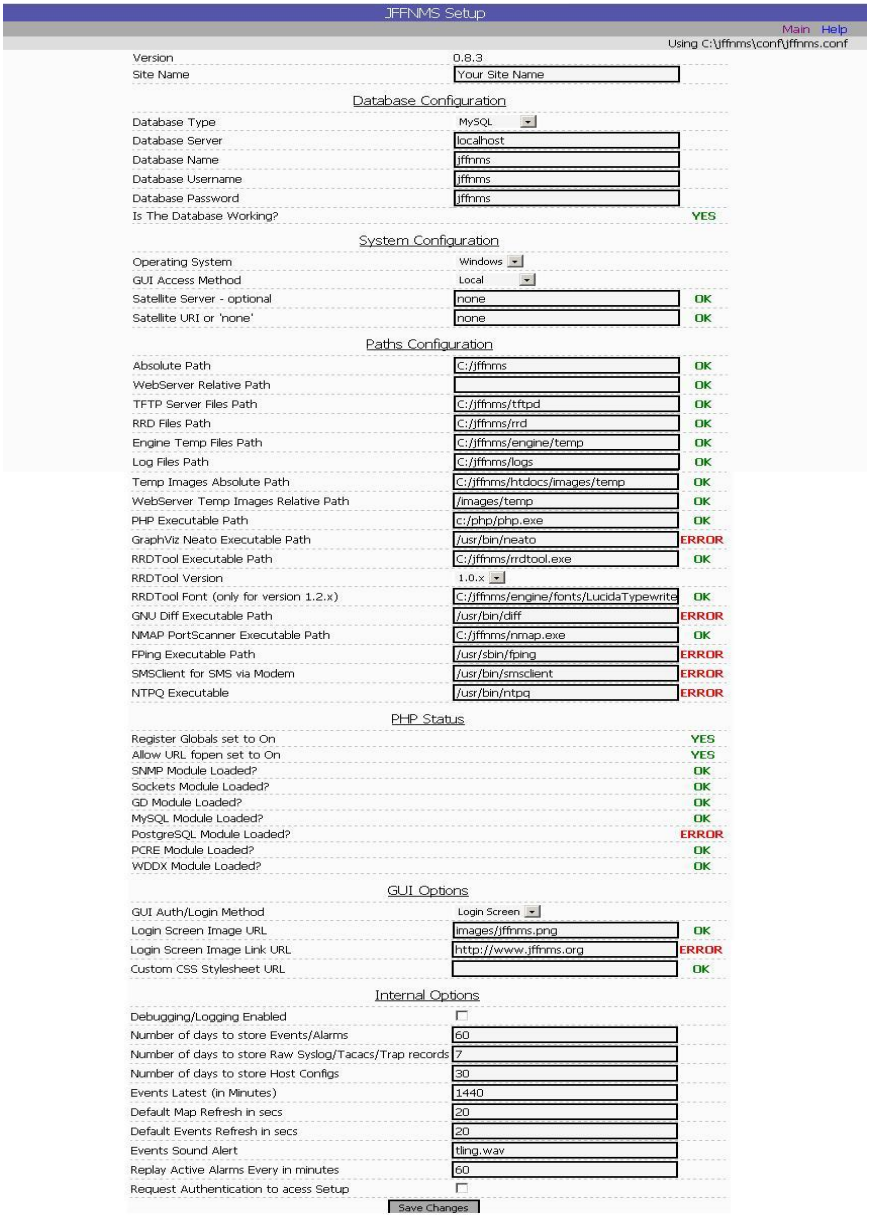


Figura 3.33 Interfaz inicial de JFFNMS

Luego de detectar si existe algún parámetro que no concuerde con la configuración otorgada, es posible acceder al vínculo main para ingresar a la ventana de autenticación; se puede observar a continuación en la Figura 3.34.

Figura 3.34 Interfaz de autenticación proporcionada por JFFNMS

Inmediatamente luego que el administrador del sistema se haya identificado el mismo tiene que determinar que se desea monitorizar; es por tal motivo que se añaden zonas o comúnmente llamadas grupos de host, mismas que permitirán situar los host y las interfaces a monitorizar. Las versiones recientes del sistema permiten utilizar zonas de autodescubrimiento de redes, además las interfaces que detecta JFFNMS no solo son los dispositivos físicos host conectados a la red, sino que incluyen servicios o parámetros SNMP. La Figura 3.35, permite observar los detalles de las interfaces y eventos asociados a una zona establecida.

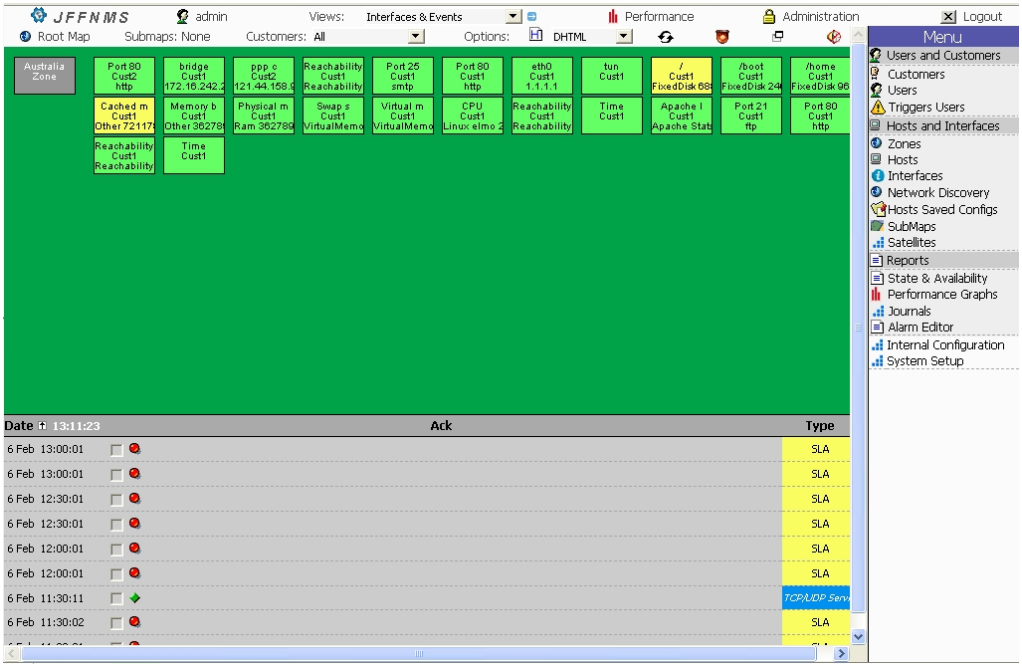


Figura 3.35 Interfaz de eventos proporcionada por JFFNMS

El aplicativo permite acceder a diferentes instancias desde su interfaz principal simplemente desde un combo desplegable que identifica sus opciones. La Figura 3.36, permite apreciar las opciones del elemento mencionado el cual otorga vínculos a distintas interfaces.

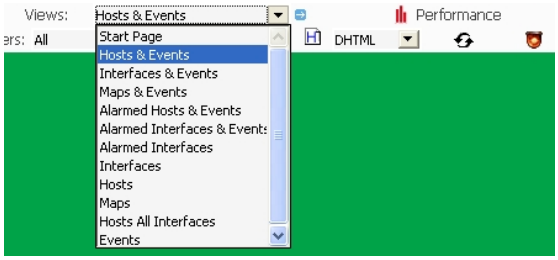


Figura 3.36 Elementos que permite apreciar JFFNMS

Así mismo, los datos mostrados por el aplicativo pueden ser visualizados en diferentes formatos, dada la facultad de presentarlos como texto simple, DHTML[44], texto normal, etc.

De cada uno de los host o interfaces que se monitoreen existe la posibilidad de conocer el estado de sus elementos internos los mismos que pueden detectar el estado de los puertos TCP y UDP, CPU, memoria RAM, disco duro, tarjeta de red.

La Figura 3.37, muestra los elementos vinculados a uno de los host en el cual se aprecia el estado del puerto TCP, el estado de los discos, la conexión de red y la CPU.

Figura 3.37 Elementos de un host detectados por JFFNMS

[44] **DHTML:** HTML Dinámico (Dynamic HTML, en inglés) designa el conjunto de técnicas que permiten crear sitios web interactivos utilizando una combinación de lenguaje HTML estático, un lenguaje interpretado en el lado del cliente (como JavaScript), el lenguaje de hojas de estilo en cascada (CSS) y la jerarquía de objetos de un DOM. [26]

Cada elemento es permisible para analizar una gráfica de rendimiento, en la que se puede detectar con facilidad el comportamiento que ha tenido en un tiempo determinado. La Figura 3.38 comprende la gráfica tanto de uso de CPU como de interfaz de red en la que se puede distinguir picos altos y bajos según la carga de trabajo y las actividades que para ese momento se efectuaban.

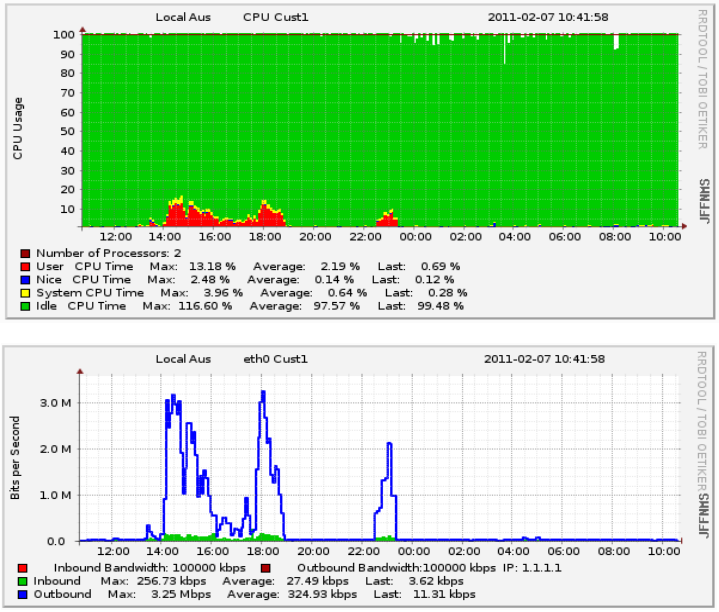


Figura 3.38 Gráfica de rendimiento de los elementos de un host

JFFNMS provee de herramientas que permiten configurar eventos los mismos que permiten enviar un correo electrónico o SMS al administrador del sistema informando la exposición de una anomalía que ha desencadenado una alarma, opción conocida como SLA. Las alarmas se generan cuando se sobrepasa de un determinado nivel donde se debe cumplir una o varias condiciones en las que el valor medido se compara con el valor prefijado.

3.1.5.4 Consideraciones de uso

Pese a que el sistema permite que el administrador añada nuevos módulos de acuerdo a la necesidad existente y permitiendo ampliar la funcionalidad, la escasez de documentación viene a ser por parte del sistema punto fundamental por solventar ya que gran parte de la información existente viene dada por sus colaboradores y muy

poca de la fuente oficial. Por otra parte la evolución del sistema contiene periodos largos para liberar la siguiente versión poniendo en duda la continuidad del proyecto. La Tabla 3.8, pretende rescatar parámetros que identifican prestaciones mostradas por JFFNMS en el ejercicio del análisis.

Parámetro	**Descripción**
Rendimiento	Medio
Manejo de información	Entendible
Funcionalidades	Expandible por medio de módulos
Cantidad de recursos para operatividad	Bajo
Plataformas compatibles	GNU/Linux, FreeBSD y Windows
Software necesario para operatividad respecto al aplicativo base	Apache, MySQL/PostgreSQL, PHP, RRDtools, Nmap, WinPcap.
Costo de operación	Bajo
Monitorización de protocolos / Disponibilidad de servicio	TCP, UDP, SNMP, BGP 4, Cisco PIX, Cisco NAT, Cisco CSS, Cisco ambientes, Cisco MAC, Cisco IP.

Tabla 3.8 Prestaciones principales de JFFNMS

3.2 ESTUDIO COMPARATIVO DE SISTEMAS LIBRES

Luego de haber evaluado los diferentes sistemas de gestión de redes con enfoque en software libre, probar las diversas funcionalidades que estos poseen y apreciar distintos aspectos (rendimiento, modularidad, configuración, plataformas compatibles, etc.), se ha procedido a elegir el sistema más idóneo para la Institución el cual destaca sobre los demás aplicativos en distintos parámetros los que se exponen más adelante.

Para llegar a la elección del sistema más idóneo también se han tomado en cuenta requerimientos funcionales y no funcionales que debe cumplir cada uno de los sistemas evaluados.

- Monitoreo de al menos 10 elementos.
- Implementación sobre cualquier sistema operativo.
- Debe gestionar distintas plataformas.
- El sistema de gestión de redes debe vigilar sistemas y aplicaciones.
- Monitoreo de hardware y software tales como (aplicaciones, sistemas operativos, bases de datos, servidores web, procesos, servicios, etc.).
- Debe detectar interfaces de red caídas.
- Debe enviar mensajes SMS informando cuando falle algún sistema o aplicación que se considere esencial.
- Debe generar alertas cuando se sobrepasen umbrales definidos.
- Debe generar informes, estadísticas.
- Debe monitorear cortafuegos, proxies, routers, switches.
- Debe permitir la generación de complementos (plug-ins) y brindar información de cómo desarrollarlos.
- Poseer documentación suficiente y clara.
- El sistema tiene una comunidad que lo respalde.
- Correcciones de problemas del sistema y publicaciones de nuevas versiones en el último año.

Una consideración no funcional entorno al sistema elegido es conocer en qué medida trabaja o no con agentes y que ventajas o desventajas puede provocar. A continuación en la Tabla 3.9, se manifiesta ventajas y desventajas de sistemas con o sin agentes.

Tipo	Ventajas	Desventajas
Sistema con Agentes	• Información más específica y más detallada. • Mayor flexibilidad para realizar monitoreo personalizable. • Posibilidad de crear soluciones de monitoreo que controlen estados de servicios o métricas no estándares sobre aplicaciones o hardware. • El control de las aplicaciones y servicios se realiza directamente en el nodo monitoreado. • Mayor seguridad en la red ya que se manejan protocolos propietarios de encriptación. • Menor riesgo de detección de inactividades.	• Puede provocar mayor carga de actividad en el cliente • Se debe instalar el agente en todos los equipos que se van a monitorear.
Sistema sin agentes	• No hay que instalar el agente en el cliente. • No se genera carga de trabajo en el cliente. • Es una opción para casos en los que no es posible instalar aplicaciones en los clientes.	• Tiene métricas menos especificas por consiguiente se pueden realizar análisis menos detallados. • Pueden ser afectadas por hechos que sucedan en la red. • El desarrollo de complementos puede ser más complicado, o directamente imposibles de realizar. • No son seguros.

Tabla 3.9 Ventajas y desventajas de sistemas con o sin agentes

Expuestas las ventajas y desventajas que ejerce la adopción de un sistema con o sin agentes se ha tomado como requerimiento que el sistema trabaje con agentes ya que aporta más beneficios. A continuación la Tabla 3.10, presenta el cumplimiento de requerimientos por parte de los diferentes sistemas.

Además de cumplir los requerimientos se ha expuesto una cuantificación que permite evaluar de mejor manera los distintos sistemas; así para la cuantificación se han elegido 7 categorías comprendidas de mayor a menor según su importancia y representadas en porcentajes (en conjunto deben sumar 100%). La valoración identifica el grado de aceptación por parte del aplicativo (Valoración: 1 = inaceptable, 2 = pobre, 3 = aceptable, 4 = muy bueno, 5 = excelente). La Tabla 3.11, muestra las categorías de cuantificación, los factores que comprende cada una y la valoración de cada sistema.

Requerimiento	Ntop	Nagios	OpenNMS	Webmin	JFFNMS
• Monitoreo de al menos 10 elementos.	X	X	X	X	X
• Implementación sobre cualquier sistema operativo.	-	X	X	-	X
• Gestionar distintas plataformas.	-	-	X	-	X
• Vigilancia de sistemas y aplicaciones.	-	X	X	X	X
• Monitoreo de hardware y software tales como (aplicaciones, sistemas operativos, bases de datos, servidores web, procesos, servicios, etc.).	-	X	X	X	X
• Detección de interfaces de red caídas.	-	X	X	X	X
• Envió de mensajes SMS informando cuando falle algún sistema o aplicación que se considere esencial.	-	X	X	-	X
• Generación de alertas cuando se sobrepasan umbrales definidos.	-	X	X	X	X
• Generación de informes, estadísticas.	X	X	X	X	X
• Monitoreo de cortafuegos, proxies, routers, switches.	-	X	X	-	X
• Generación de complementos (plug-ins) y brindar información de cómo desarrollarlos.	X	X	X	X	X
• Documentación suficiente y clara.	-	X	X	X	-
• El sistema tiene una comunidad que lo respalde.	X	X	X	X	X
• Correcciones de problemas del sistema y publicaciones de nuevas versiones en el último año.	X	X	X	X	X
• Manejo de agentes.	-	X	X	-	X

Tabla 3.10 Requerimientos cumplidos por parte de los sistemas de gestión

Ranking	Categoría	Factores	Ntop	Nagios	OpenNMS	Webmin	JFFNMS
			Valoración: 1 = inaceptable, 2 = pobre, 3 = aceptable, 4 = muy bueno, 5 = excelente				
1	Funcionalidad	▪ Monitoreo de distintos sistemas operativos. ▪ El servidor se instala en ambiente GNU/Linux. ▪ Tener agentes de monitoreo que trabajen en los clientes ▪ Generar alarmas ante caídas. ▪ Enviar alarmas si se llega a determinados umbrales (CPU, disco duro, memoria). ▪ Permite el envío de notificaciones vía email.	2	4	5	4	4
2	Calidad	▪ Cantidad de revisiones no menores en los últimos 12 meses. ▪ Numero de errores corregidos. ▪ Cantidad de bugs críticos solucionados.	3	4	4	3	3
3	Usabilidad	▪ Experiencia con la interfaz de Usuario. ▪ Tiempo para instalar prerrequisitos previo a instalar el sistema. ▪ Tiempo para la instalación terminada y configurada.	3	3	4	3	3
4	Rendimiento	▪ Documentación o herramienta para ayudar a afinar el componente en cuanto a rendimiento y configuración. ▪ Pruebas de rendimiento e informes de referencia disponibles.	3	4	4	3	3
5	Apoyo	▪ Calidad de apoyo profesional. ▪ Respuesta ante consultas de usuarios.	3	4	5	3	3
6	Comunidad	▪ Número de contribuyentes código único en los últimos 6 meses.	3	4	5	4	3
7	Arquitectura	▪ Existen plug-ins implementados por terceras partes. ▪ Api Pública y servicios externos, mide si permite realizar extensiones y personalizar el sistema. ▪ Se puede configurar desde la aplicación.	2	4	5	4	4

Tabla 3.11 Categorías de cuantificación por importancia

Categoría	Ntop	Nagios	OpenNMS	Webmin	JFFNMS
Funcionalidad (25%)	10	20	25	20	20
Calidad (20%)	12	16	16	12	12
Usabilidad (20%)	12	12	16	12	12
Rendimiento (15%)	9	12	12	9	9
Apoyo (10%)	6	8	10	6	6
Comunidad (5%)	3	4	5	4	3
Arquitectura (5%)	2	4	5	4	4
TOTAL (100%)	**55**	**76**	**89**	**67**	**66**

Tabla 3.12 Resultados Evaluación de Sistemas de Gestión de Redes bajo software libre

Dado tanto la evaluación previa a cada uno de los sistemas, el análisis de requerimientos, la cuantificación y los resultados arrojados (mostrados en la Tabla 3.12), se ha llegado a la conclusión que el sistema que otorga las mejores condiciones es OpenNMS por cuanto el mismo tiene gran posibilidad de implantación en la Institución.

CAPÍTULO 4. ÁREAS FUNCIONALES EN LA GESTIÓN DE RED

En este capítulo, se procurará delinear las diferentes áreas funcionales que conlleva la gestión de red intentando rescatar características y propuestas que ayuden al mejoramiento de la Institución.

4.1 MODELO DE GESTIÓN ISO

En la actualidad, se manejan distintos modelos que ayudan a una gestión integrada; de la cual el modelo de gestión ISO clasifica las tareas de administración en cinco áreas funcionales, más comúnmente conocido por sus siglas en inglés FCAPS (Fault, Configuration, Accounting, Performance, Security). No requiere de la implementación de algún protocolo en específico, sin embargo SNMP y CMIP son los más comúnmente utilizados. La Figura 4.1, muestra las distintas áreas funcionales que comprende el modelo de gestión ISO.

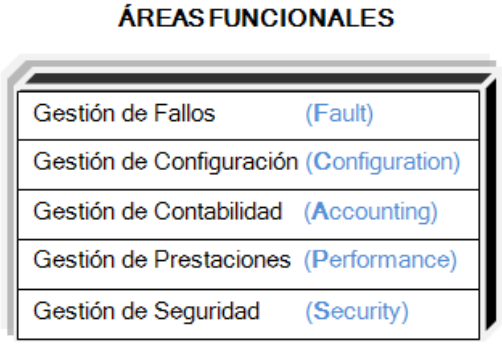


Figura 4.1 Áreas Funcionales FCAPS

4.1.1 ÁREAS FUNCIONALES

A continuación, se presentan las distintas áreas funcionales de gestión de red que corresponden al modelo de gestión ISO.

4.1.1.1 Gestión de Fallos

Este tipo de gestión procura mantener un óptimo funcionamiento del conjunto de componentes que conforman una red y de cada uno de los elementos que se encuentren inmersos, tratando de protegerla de los fallos o anomalías que afecten un servicio o en sí un sistema. El objetivo fundamental, es diagnosticar y determinar el fallo llegando a un aislamiento del mismo y solventando el problema.

Por otro lado, el establecimiento de alarmas que evocan umbrales previamente establecidos por el administrador, predice fallos que garantizan la disponibilidad de la red todo gracias a la posibilidad de notificaciones automáticas al personal encargado.

También conviene diferenciar un fallo de un error ya que un fallo requiere de algún tipo de acción correctora ocasionada habitualmente por una gran cantidad de errores; mientras que los errores y su concurrencia no tienen por qué ser fallos (Por ejemplo, todo enlace tiene una tasa de error de un bit).

Existen también metódicamente pasos para el manejo de fallas las que pueden delinearse de la siguiente manera.

- Identificación de la falla, mediante el sondeo regular de la red.
- Aislamiento de la falla, para que disminuya el impacto en la red.
- Reacción ante la falla, estableciendo recursos y prioridades para la resolución.
- Resolución de la falla, probando en todos los subsistemas importantes la validez de la solución.
- Almacenamiento de reportes de estado que permiten detallar el seguimiento efectuado y la resolución del problema.

4.1.1.1.1 Manual de Procedimientos de Gestión de Fallos

Dada la ardua operatividad que poseen los equipos de la Institución en diversas áreas críticas, el desempeño al que se ven expuestos no debe decaer; es por eso que resulta viable estructurar un Manual de Procedimientos de Gestión de Fallos que mitigue y controle cualquier eventualidad.

La efectividad de una Gestión de Fallos se ve muy ligada a un parámetro adicional conocido como Gestión de Incidencias el que enfoca su accionar en puntos claves como:

- Resolución de incidencias rápidamente para mantener la calidad del servicio IT. El cual establece con indicadores valores máximos, mínimos y medios para la resolución de incidencias, que denotan la efectividad de nuestro accionar según a donde tienda el indicador. Se debe tender a la disminución del porcentaje en tiempo medio de una llamada por asistencia, la cual es recogida por un operador de primera línea (Un operador de primera línea es la personas encargada de HelpDesk el que por lo regular acoge un 80 a 85% de las causas, mientras que los operadores técnicos acogen de un 5 a 10%, los especialistas en comunicaciones acogen de un 2 a 5%, los especialistas en aplicaciones acogen de un 1 a 3% y por último los fabricantes de un 1 a 2%), además la efectividad de los operadores de primera línea a la primera respuesta debe incrementarse. Así también la adecuada asignación de las incidencias a operadores de primera, segunda, tercera línea etc.
- Una base de datos común que otorgue un adecuado manejo de incidencias, otorga un acceso rápido a incidencias resueltas por ende optimizando tiempos.
- Tener un sistema de incidencias automatizado es de vital importancia para un funcionamiento óptimo del HelpDesk. Tener dicho sistema faculta obtener variables de incidencias por nivel de las cuales se pueden desglosar en solucionadas, no solucionadas y pendientes; llegando a tomar medidas según los datos arrojados. Este tipo de sistemas TTS (Trouble Ticket Systems) posee parámetros de quien es el equipo afectado, su localización, la

descripción del problema, el operador que atiende, el grado de severidad y obviamente tener un historial de incidencias.

a. Proceso de Solución de Fallos

Dado que se ha expuesto un proceso metódico que va desde identificación hasta la documentación el éxito está en respetar este ciclo, el cual se muestra en la Figura 4.2.

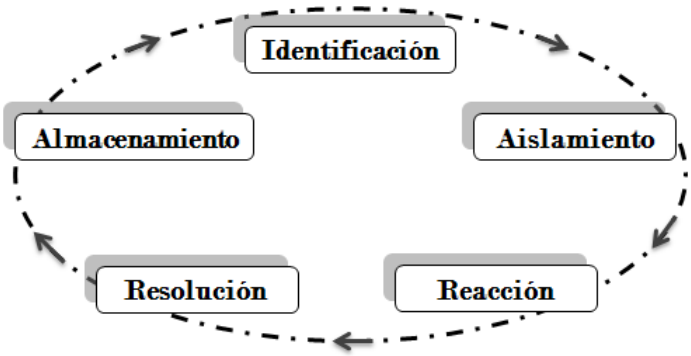


Figura 4.2 Proceso de solución de fallos

a1. Identificación

La consola web que proporciona OpenNMS (refiérase a Figura 3.17) mostraría de manera clara los problemas que afecten a cualquier dispositivo de red, alertando al administrador para que efectúe los correctivos necesarios.
Así también los problemas que no sean detectados por el aplicativo deben ser sujetos de atención inmediata por parte del área de soporte o por parte de los operadores de primera línea; el administrador deberá hacer visible la falla por la consola de monitoreo de acuerdo al nivel de criticidad que esta posea.
Los pasos que se deben seguir son:

- Monitorio de la consola web, detectando que los dispositivos activos se encuentran sin fallos (color verde).

- Si existiera una alerta de dispositivo (color amarillo o rojo) se debe identificar el número del evento, la fecha y la descripción.

El monitoreo que permite la consola web puede ser adaptado para un sondeo continuo de acuerdo al nivel de exigencia que se determine. Es aconsejable el ingreso de valores medios de monitoreo (de 5 a 10 minutos), los que procuran mantener una adecuada vigilancia de los dispositivos.
Además la identificación de la falla por medio de la alarma presta la pauta para realizar lo siguiente:

- Verificación de conectividad con el dispositivo.
- Análisis de los resultados (peticiones CMIP o SNMP) arrojados por el dispositivo.
- Comprobar tiempos de respuesta.

a2. Aislamiento de la falla

Aislar el dispositivo que ha desencadenado una falla; es de relevancia la información que otorgue el usuario de las actividades presentadas antes y durante la falla. Es útil culturizar al usuario para que no intente remediar el suceso por su cuenta y que acuda al personal encargado.

a3. Reacción ante la falla

La adecuada reacción que pueda existir por parte del personal encargado es de gran importancia ya que de él dependen ciertos pasos:

- Asignación de recursos (técnicos, operativos, etc.) para resolver la falla.
- Determinación de prioridades (áreas críticas, niveles de criticidad).
- Escala técnica y de gestión (escalar la incidencia de acuerdo al operador; quiere decir primera, segunda, tercera línea, etc.).

a4. Resolución de la falla

En reciprocidad con una adecuada aislación del fallo y una reacción diligente; la resolución de la falla procederá con las soluciones más sencillas escalando con las más complejas. Los procesos que impliquen resolución de fallos deben estar adecuadamente documentados y notificados. Además la documentación en un fallo de software debe contener datos específicos de configuración.

La resolución de fallos amerita una adhesión de propuestas que controlen o mitiguen los problemas imprevistos; el cual se presenta en el punto 4.1.1.1.2.

Para conocer más de cerca los puntos críticos existentes en la Institución y los niveles de criticidad que cada punto refleja, se ha visto la necesidad de efectuar una encuesta con las personas encargadas de velar por el óptimo funcionamiento de los diferentes dispositivos. A continuación la Tabla 4.1, muestra los niveles de criticidad que se pueden suscitar, mientras la Tabla 4.2 evidencia cada punto crítico y el nivel que acoge.

Cabe la posibilidad de generación de dos fallos con un mismo nivel de criticidad, en cuyo caso el administrador pondrá a su consideración las medidas a efectuarse.

Nivel de Criticidad	Descripción
(1) Poco crítico	Indica la existencia de una falla menor de la cual se deben tomar medidas para que no escale su accionar.
(2) Algo crítico	Indica la existencia de una falla de servicio que requiere atención inmediata. (Se brinda el servicio pero con calidad baja)
(3) Crítico	Fallo de afectación global que necesita atención inmediata. (Enlace de red importante caído)
(4) Muy crítico	Fallo muy severo de atención extremadamente urgente.

Tabla 4.1 Niveles de criticidad

Factores de Fallo	Niveles de criticidad				Área Responsable
	Nivel: 1 = poco crítico, 2 = algo crítico, 3 = crítico, 4 = muy crítico				
	1	**2**	**3**	**4**	
▪ Caída de enlace con la Dirección Metropolitana de Informática.				X	Dpto. Redes
▪ Caída de enlace de Internet (CNT).					Dpto. Redes
▪ Caída de enlace de Internet (PuntoNet).		X			Dpto. Redes
▪ Caída de servidor Controlador de Dominio.	X				Dpto. Producción
▪ Caída de servidor de Aplicaciones.			X		Dpto. Producción
▪ Caída de otros servidores como: Antivirus, WSUS, Archivos.	X				Dpto. Producción
▪ Corte inesperado del suministro eléctrico.			X		Dpto. Técnico
▪ Problemas de operatividad del Sistema Financiero.		X			Dpto. Desarrollo
▪ Problemas de operatividad del Sistema de Catastros.		X			Dpto. Desarrollo
▪ Problemas de operatividad del Sistema de Trámites.			X		Dpto. Desarrollo
▪ Problemas de conectividad con un Switch.		X			Dpto. Redes y Soporte
▪ Problemas de conectividad con un Router.			X		Dpto. Redes
▪ Problemas con impresoras locales.	X				Dpto. Soporte Técnico
▪ Problemas con impresoras de red.	X				Dpto. Soporte Técnico
▪ Problemas con utilitarios, Sistema Operativo o Hardware de host de usuarios.		X			Dpto. Soporte Técnico
▪ Problemas internos de Cableado Estructurado y puntos de red.		X			Dpto. Redes y Soporte
▪ Problemas de dispositivos por variaciones eléctricas bruscas.			X		Dpto. Técnico

Tabla 4.2 Puntos críticos y niveles de criticidad

Además de establecer los factores críticos y niveles de criticidad; la Tabla 4.3 menciona tiempos relativos en los cuales el personal encargado debe solucionar los fallos; mismos que están ligados directamente a la criticidad.

Tipo de Tiempo	**Descripción**	**Niveles de criticidad**		
		Nivel: 1 = poco crítico, 2 = algo crítico, 3 = crítico, 4 = muy crítico		
		1 y 2	**3**	**4**
Atención	Tiempo para llegar a atender un fallo.	1 hora	30 minutos	15 minutos
Aislamiento	Tiempo para aislar el fallo y determinar una solución.	2 hora	6 horas	3 horas
Resolución	Tiempo máximo para resolver el fallo.	1 día	Aprox. 2 días	1 día

Tabla 4.3 Tiempos estimados de acuerdo a criticidad

Cabe mencionar que para los tiempos mencionados existe la posibilidad de traslados del personal hacia sitios fuera de la Institución, en cuyo caso el tiempo de atención aumenta. Otro parámetro a considerar es la aplicación de garantías de dispositivos, los que al ser indispensables (de mediana a gran necesidad) tienen que ser mitigados con soluciones temporales hasta la reposición en un tiempo prudencial de dicho dispositivo.

La resolución del fallo también conlleva pruebas de verificación que ratifican el éxito indudable en la restauración del fallo; en cuyo caso no podrá extenderse por un máximo de 30 minutos. Toda resolución de fallo debe comprender una adecuada documentación de todo el proceso seguido hasta el cierre del mismo.

a5. Documentación o almacenamiento de la falla

Esta etapa intenta recabar todo el proceso efectuado en la resolución de un problema. Además la misma proporciona agilidad a eventualidades

producidas con anterioridad ya que en ellas se encuentran soluciones comprobadas y documentadas.

Es una buena práctica optar por una buena y detallada administración de los activos que posee la Institución, ya que los mismos contienen información necesaria en caso de alguna eventualidad o cambio de dispositivo. La Tabla 4.4, muestra un modelo de datos referencial que contiene información para un dispositivo (switch, router, servidor).

	Parámetro	**Descripción**
General	Tipo de dispositivo	Puede ser switch, router, servidor.
	Marca-Modelo	Dispuestos por el fabricante.
	Número de Inventario	Código asignado por activos fijos.
Parámetros Técnicos	Características Hardware	Procesador (tipo y velocidad), motherboard (fabricante, versión), memorias (tipo y velocidad), disco duro (marca, tipo y capacidad), tarjetas de red, fuente de alimentación.
	Características Software	Sistema Operativo, firmware, parches instalados, componentes instalados, versiones de todos los productos, controladores.
Ubicación	Área	Área específica de localización
	Rack número	Etiqueta de rack
Configuración	Dirección IP	IP, máscara, Gateway, DNS
	Claves de acceso	Clave de acceso a dispositivo
	Tablas de enrutamiento	Rutas estáticas, dinámicas, protocolo de enrutamiento.
	Dispositivos ligados o dependientes	Dispositivos que trabajan en conjunto.
Registro	Fallo anterior	Eventualidad acontecida (causa, efecto ocasionado).
	Nivel de criticidad	Dimensionamiento del problema.
	Aislamiento fallo	Medida tomada para aislar el fallo
	Resolución	Soluciones aplicadas.
	Tiempo de resolución	Tiempo medido desde su reporte hasta la resolución.
	Pruebas de verificación	Pruebas efectuadas para ratificar la resolución.

Tabla 4.4 Modelo de datos referencial para documentación

La manera de llevar un esquema de reporte de fallos que permita documentar y dar seguimiento al fallo, pretende establecer un ciclo de creación, seguimiento, manejo y finalización del reporte con la finalidad de acudir a ella y optimizar tiempos si la falla se dio con anterioridad. La Figura 4.3, permite apreciar una propuesta de modelo referencial de reporte de fallos.

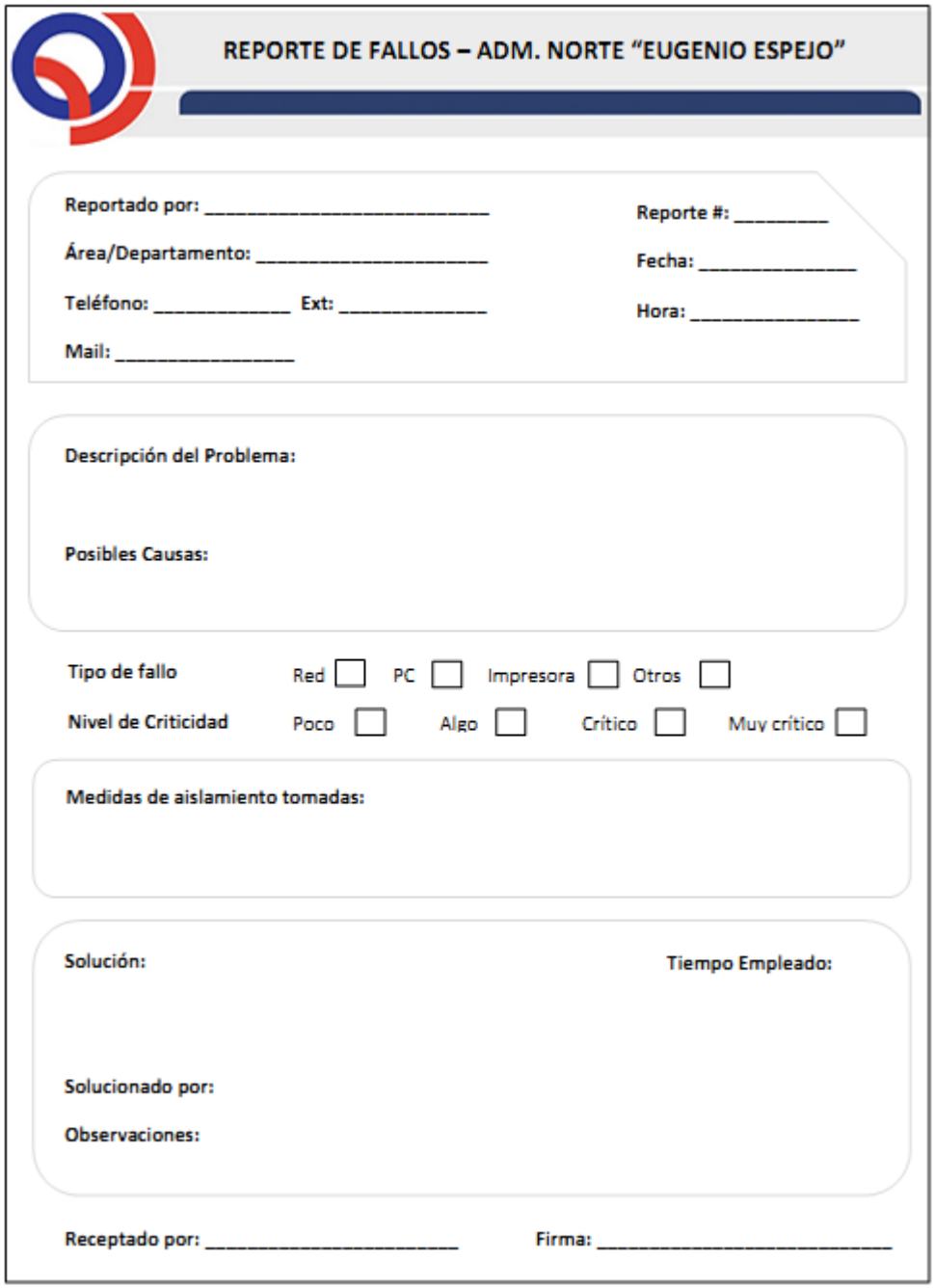


Figura 4.3 Modelo referencial de reporte de fallos

En conclusión el proceso que se sigue para resolver un fallo, desde su notificación hasta su resolución, se presenta en la Figura 4.4.

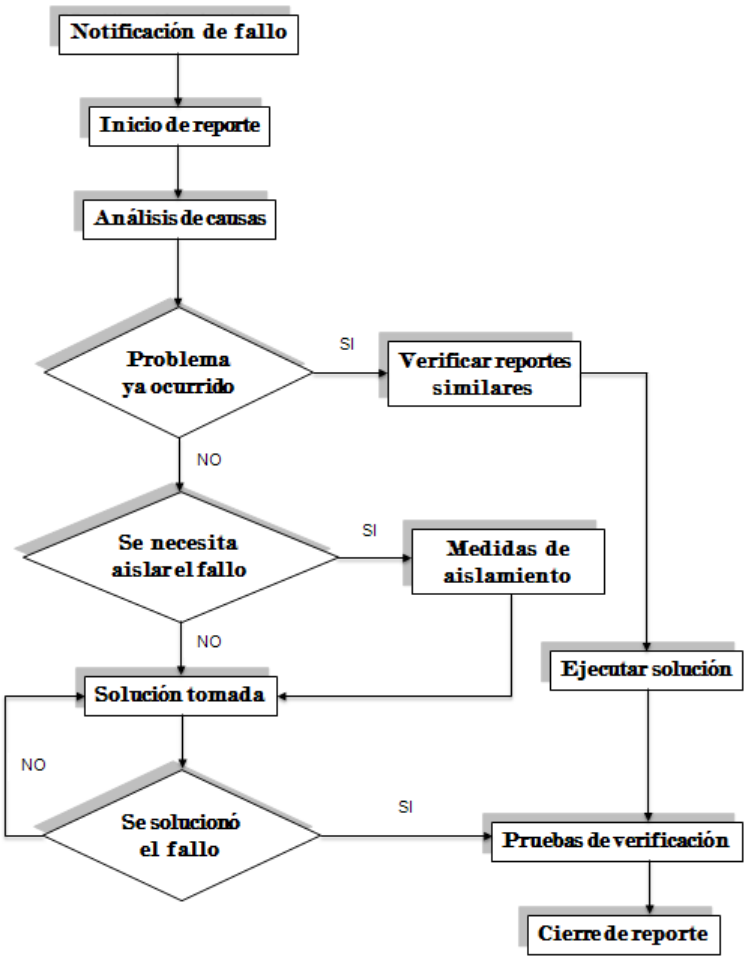


Figura 4.4 Proceso general de resolución de fallos

4.1.1.1.2 Propuestas y consideraciones que aplacan problemas imprevistos

A continuación, se sugieren medidas que fomentan buenas prácticas a la hora de atender una eventualidad. Las eventualidades tomadas en cuenta están dadas por su campo de acción y criticidad. Al establecer la Institución sus operaciones sobre distintos switch se deben aplicar ciertas medidas.

- Es recomendable poseer la documentación adecuada mapas de red, distribución tanto física como lógica de los dispositivos, nomenclatura clara y

especifica; misma que ayudará en su debido momento facilitando operaciones y contrarrestando a tiempo los problemas.

- Es prudente tener dos switch en estado pasivo (un Switch 3COM 4200 el cual tiene directa operatividad con el servidor de aplicaciones y un Switch 3COM 5500G-E1 que opera con el Router de enlace con la Dirección Metropolitana de Informática Quito) los mismos que reemplazarán a los switch que están en producción en caso de daño o falla.
- La utilización de cables certificados que garanticen la correcta interacción entre los dispositivos procurara analizar causas más probables de fallos sin tener que volver a testear los cables; cabe la posibilidad de poseer un cable tester para realizar pruebas y descartar problemas en el cable utilizado.
- Un adecuado mapa de red que establezca las condiciones de interacción con el resto de dispositivos en cada rack, pretenderá dar un seguimiento más ágil a cualquier fallo que pudiera presentarse.
- Los fallos provocados por NIC defectuosas, cables de red que no cumplen la normativa entorno a distancias máximas, problemas de dúplex (modo de puerto), ocasionan colisiones que están ligadas a la configuración full dúplex y half dúplex del dispositivo.
- Saber evidenciar si en un dispositivo existe un daño físico pretende aislar el daño en caso de que sea fallo de un puerto ya que los mismo tienden a dañarse muchas veces por electricidad estática, la notoriedad de una luz naranja que este posee es indicativo que no está trasmitiendo; procurar probar con otro puerto del dispositivo la correcta funcionalidad.
- La posibilidad de fallos internos relacionados directamente al software del switch retoma medidas de sustitución del dispositivo mientras se analiza su sustitución definitiva o recarga del software propio del switch (en caso de recarga del IOS[45]).
- En dispositivos como routers es mucho más prudente adquirir módulos de repuesto (tarjetas seriales, tarjetas Gigabit Ethernet, FXS, FXO) dependiendo la utilización del equipo y la constate discontinuidad que se dan con la adquisición de muchos de los repuestos.

[45] **IOS:** Sistema Operativo de Interconexión de redes (Internetwork Operating System, en inglés) sistema operativo creado por Cisco System para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores). [27]

- Las condiciones de temperatura que deben estar presentes en el cuarto de telecomunicaciones establecen que los equipos tienen una adecuada refrigeración, razón por la cual es conveniente tener a disposición equipos de repuesto y ventiladores convencionales en caso de fallo del sistema de enfriamiento.

4.1.1.2 Gestión de Configuración

La gestión de configuración es ampliamente utilizada para registrar todos los cambios efectuados en los elementos de la red y aunque no necesariamente un elemento en particular es configurado para realizar una única función sino que puede según el caso configurarse para diferentes tareas dependiendo el trabajo que desempeñe (Por ejemplo, un nodo puede actuar como router o como host variando los temporizadores de retransmisión en el nivel de transporte); es por eso que es tan necesaria este tipo de gestión que además permite:

- Controlar y proteger el despliegue de recursos.
- Llevar un registro de la topología, dispositivos instalados (ubicación, como está conectado, personal responsable, estado operacional).
- Registrar la configuración actual de los elementos de la red, así como los cambios que se pueden realizar; almacenando los datos de configuración para su revisión en momentos necesarios.
- Inventariar los elementos que conforman la red (como software y hardware de los distintos componentes).

La importancia de esta gestión viene dada por la productividad que arroja ya que en la actualidad factores como la complejidad escalable que presentan las redes, la poca añadidura a políticas de gestión de configuración provoca situaciones que con su debida atención no ocasionarían pérdidas de tiempo o baja productividad desencadenando problemas mayores.

4.1.1.2.1 Aspectos ligados a la Gestión de Configuración

a. Gestión de Inventario

La Gestión de Configuración viene muy ligada a un aspecto muy importante que dependiendo de la complejidad de la red se lo maneja separadamente, es así como aparece la Gestión de Inventario que trata:

- El historial de cambios y problemas que se presentan en una red.
- Las bases de datos de los elementos de la red.

Se puede rescatar que una adecuada coordinación de los mecanismos que facilitan esta información otorga un incremento en el desempeño de las operaciones.

b. Estado Operacional

Otro aspecto que se toma en cuenta es el Estado Operacional el cual contempla ciertos criterios:

- Inicio de los componentes individuales.
- Cambios en la configuración de dispositivos.
- Actualizaciones de software y hardware.
- Métodos de acceso SNMP.

4.1.1.2.2 Aspectos fundamentales que se consideran

Los puntos fundamentales que acoge este tipo de gestión proporcionan datos que son de gran utilidad y que deben ser considerados inexorablemente.
Uno de los puntos que se deben considerar es manejar adecuadamente los recursos de hardware y software dentro de la red.

a. Instalaciones de Hardware

La instalación o reemplazo (se puede considerar la instalación completa de un nuevo dispositivo o simplemente la instalación de ciertos módulos) de un dispositivo sea este un switch o un router debe comprender ciertos criterios que se mencionan a continuación:

- Análisis adecuado del componente que será instalado o reemplazado.
- Coordinaciones de tiempos para realizar la instalación o reemplazo.
- Estimar horarios no operativos para no afectar operaciones normales.
- Procurar establecer un plan de transición operativa.
- Coordinar una adecuada configuración del dispositivo instalado.
- Cada cambio que ha sido establecido debe ser bien documentado y anexado en caso de futuros cambios.

b. Adecuaciones de Software

Las adecuaciones (instalación/desinstalación, actualización) de software se refieren al cambio que se dé a una aplicación, sistema operativo o dispositivo. Cambios que deben respetar ciertos criterios para mantener el control:

- Tomar en cuenta para aplicativos o sistema operativo el tipo de arquitectura en la que se despliega su funcionalidad (32bits o 64bits).
- Comprobar los requerimientos existentes por parte del host para su instalación (disco, memoria, procesamiento CPU).
- En caso de actualización debe indicarse la versión a actualizarse, porqué parte el cambio (seguridad, desempeño, etc.), seguir un criterio de versionado y cuál es la versión a generarse por parte de la actualización. La información que se mantiene en este registro permite ver como se ha dado la evolución del sistema y de los aplicativos que lo conforman.
- En caso de actualización del aplicativo comprobar su correcto funcionamiento (conflictos con otras aplicaciones).

- Muchas de las actualizaciones del host referente al BIOS solo deben ser contempladas cuando se requiere hacer cambios necesarios de componentes hardware y en tal medida se debe realizar adecuadamente para no provocar daños.
- Todos los cambios deben contemplar una documentación adecuada.

4.1.1.2.3 Configuraciones de Seguridad

Un parámetro importante es gestionar configuraciones con índoles restrictivas al que solo pueden tener acceso personal autorizado. Se debe tener como premisa que la información es el bien más importante dentro de una Institución ya que el mismo no puede estar sometido a las mismas instancias de otro bien. A continuación, se establecen ciertos lineamientos a seguir para evitar accesos no autorizados.

- Sectorizar o dividir áreas importantes mediante configuraciones de VLANs.
- Creación de direccionamiento de red exclusivo para dispositivos de interconexión con conocimiento solo de personal autorizado.
- Utilizar conexiones seguras para el ingreso y configuración remota de dispositivos.
- Coordinar planes periódicos que fortalezcan las configuraciones de los dispositivos.
- Establecer políticas claras entorno a configuraciones tomadas en servidores.

4.1.1.2.4 Procedimientos y políticas de Gestión de Configuración

A continuación, se establecen ciertos procedimientos y políticas a tomarse en cuenta:

a. Procedimiento para la instalación de aplicaciones

El procedimiento sugerido para la instalación de aplicaciones es:

- Constatar los requerimientos de hardware mínimos para la instalación de la aplicación.

- Realizar pruebas previas que determinen la apropiada operatividad de la aplicación con el resto de aplicativos.
- Organizar un cronograma que especifique los tiempos que llevaran las distintas instalaciones.
- Notificar a los usuarios previamente el cronograma a ejecutarse.
- Documentar adecuadamente las configuraciones establecidas en las instalaciones, misma que podrá ser referida en posteriores ocasiones.

b. Procedimiento de instalación de nuevo Sistema Operativo

El procedimiento sugerido para la instalación de nuevo Sistema Operativo es:

- Analizar la capacidad del hardware a ser actualizado.
- Respaldar minuciosamente toda la documentación existente en el equipo antes que se efectúe la actualización.
- Organizar un cronograma que especifique los tiempos que llevaran las distintas instalaciones.
- Notificar previamente a los usuarios las tareas a efectuarse.
- Realizar pruebas que ratifiquen la operatividad del nuevo sistema en conjunto con sus aplicaciones.
- Documentar configuraciones, detallando criterios escogidos el momento de la instalación y el porqué de los mismos.

c. Políticas a tomarse en cuenta para respaldo de configuraciones

A continuación, se presentan políticas de respaldo de configuración que deben ser tomadas muy en cuenta:

- Definir el lineamiento que exponga una periodicidad de respaldo de configuración (tomar en cuenta los cambios que se efectúen y con periodicidades a considerarse diarias, semanales, quincenales, mensuales o cada x días).

- Definir el tipo de respaldo a ser sometido; esto se presenta a consideración dependiendo si se necesita el respaldo completo de la configuración o tomando un aspecto diferencial que en este caso sería solo una pequeña parte de toda la configuración.
- Determinar el lugar de almacenamiento; se pueden considerar discos duros, servidor de archivos y medios digitales (CD, DVD).
- Fijar el método de respaldo a utilizarse; se puede considerar métodos manuales o automáticos.
- Especificar la persona que será responsable de constatar el adecuado respaldo realizado.

4.1.1.3 Gestión de Contabilidad

La Gestión de Contabilidad o también conocida como Gestión de Tarifación tiene por objeto establecer tasas e identificar costos relacionados con el uso de los elementos que conforman la red y los servicios que este provee. Además, este permite imponer límites de costos, informarlos y distribuirlos a los distintos departamentos de la empresa.

Entre las tareas que engloba esta área, están:

- Recolección de datos sobre la utilización de los recursos.
- Establecimiento de políticas de tarifación.
- Definición de procedimientos para tarifación.
- Gestión de facturas.
- Cobro a los usuarios con las tarifas derivadas de la utilización de los recursos.
- Integración con la contabilidad de la empresa.

Cabe mencionar que lo relacionado a tarifación está ligado directamente a las redes públicas (muy común en los proveedores de servicio de Internet o ISP) mientras que las redes corporativas se centran más en los objetivos que se mencionan a continuación.

Los objetivos que persigue esta área vienen dados por:

- Identificar el uso ineficiente de la red o uso excesivo por parte de un usuario.
- Distribuir el gasto entre departamentos.
- Planificar el crecimiento de la red.
- Redistribución adecuada de los recursos de la red en función de las necesidades de cada usuario.

Como parte de la contabilización del uso de los recursos y servicios de red el aplicativo OpenNMS logra captar información que es de gran relevancia para este tipo de gestión; así se tiene parámetros como el estado de las interfaces de red, usuarios conectados, capacidades de disco, uso de memoria, uso de procesador, entre otros. La contabilización de información referente a recursos y servicios de red están sujetas a parámetros que permiten revelar de una manera clara y precisa el funcionamiento de la red, es así como se tiene que definir ciertos aspectos a considerar.

4.1.1.3.1 Propuestas y consideraciones

- Definir los niveles de tráfico entrante y saliente en puntos claves, es de gran importancia así como los niveles de conectividad entre dispositivos.
- Evidenciar la capacidad que aún posee libre un disco duro, sea este de un servidor o equipos en particular, facilitara la adopción de medidas que solventen este tipo situaciones.
- Los niveles mostrados sobre el uso del procesador permite identificar la carga procesal a la que está siendo expuesto ese equipo; niveles que permiten evaluar cambios o revisiones del flujo de trabajo y servicios ejecutados.
- La contabilización de alarmas mediante los registros que los mismos generan permite evaluar cuáles son los eventos más recurrentes y fortalecer las medidas para solventarlos.
- Identificar el ingreso recurrente a un sitio web que no coincida con las funciones desempeñadas en horario de trabajo, puede suponer el uso

inadecuado de los recursos, el mismo que puede ser alertado y someter al usuario a llamamiento de atención.

- Evaluar los recursos utilizados por parte de los usuarios en función de las estadísticas de interfaces y protocolos permite contabilizar su uso y redistribuir adecuadamente los recursos por bloques.
- Contabilizar las estadísticas entorno a los enlaces que posee la Institución evidencia los niveles de trabajo y periodos de mayor actividad.

Todos los puntos anteriormente mencionados son fácilmente evidenciados por medio de reportes y gráficas que permiten al administrador contabilizar adecuadamente las medidas a tomarse según las necesidades institucionales.

4.1.1.4 Gestión de Rendimiento

La Gestión de Rendimiento o también referida como Gestión de Prestaciones es la encargada de evaluar la efectividad en el rendimiento de la red así como los cambios que lo afectan.

Este tipo de gestión define ciertas posturas que se mencionan a continuación:

- Establecimiento de umbral límite de rendimiento, los que al ser controlados no difunden efectos perceptibles a lo largo de la red y sobre los usuarios.
- Recolección de datos con el propósito de analizarlos y determinar las causas de la disminución del rendimiento; dichos datos alimentan también otras áreas funcionales que contribuyen entre si integrando soluciones.
- Entre las variables de rendimiento (recolección de datos) se tienen dos distintos tipos que se presentan a continuación:

    - Las orientadas al servicio (disponibilidad, tiempo de respuesta o latencia[46], fiabilidad).

[46] **Latencia:** Retardo temporal en la transmisión de la señal o paquetes de datos dentro de la red.

- Las orientadas a la eficiencia (throughput[47], porcentaje de utilización de un recurso en el tiempo).

En cuanto a las orientadas al servicios, la disponibilidad viene a considerar el porcentaje de tiempo que un sistema o servicio se encuentran disponibles para el usuario; la misma que da su importancia según el ámbito de aplicación sea este un banco, un puesto de peaje, etc. Mientras que la fiabilidad considera la probabilidad de que un componente funcione correctamente bajo ciertas condiciones específicas.

Acorde a los datos provistos por este tipo de gestión y las distintas variables que se tienen es posible determinar si una red cumple con los niveles de rendimiento establecidos. También permite pronosticar congestión (cuellos de botella) gracias a los indicios de las distintas variables y poder planificar con antelación las medidas a ejecutarse.

OpenNMS al presentar de manera eficiente gráficas estadísticas del desempeño de los diferentes dispositivos y permitir manipularlos dependiendo el periodo a ser analizado, puede afianzar más su capacidad analítica trabajando con aplicaciones de apoyo.

4.1.1.4.1 Propuestas y consideraciones

A continuación, se presentan propuestas que pretenden incrementar aún más la gestión de rendimiento.

- Se pone a consideración apoyar la aplicación OpenNMS con otra aplicación que desvela parámetros más detallados en este tipo de gestión; aplicación que también ha entrado en análisis para este proyecto, es así como NTOP al poseer una generación de informes y estadística más completa permite

[47] **Throughput:** Volumen de trabajo o de información que fluye a través de un sistema. Así también se le llama al volumen de información que fluye en las redes de datos. Particularmente significativo en almacenamiento de información y sistemas de recuperación de información, en los cuales el rendimiento es medido en unidades como accesos por hora. [28]

afianzar más las prestaciones de la red. La instalación de dicha aplicación debe considerar un lugar estratégico de funcionamiento, esto para no afectar el desempeño de un servidor con otros servicios por lo cual, se toman en cuenta capacidades otorgadas por el servidor y tipo de servicios que alberga.

- Es posible también considerar el uso de otra aplicación libre como MRTG que es destinada exclusivamente a analizar el rendimiento de la red y determinar la utilización de cada uno de los enlaces que contenga la red sean estos Ethernet, FastEthernet, GigabitEthernet, etc. La herramienta permite mostrar gráficas estadísticas de los recursos de la red.
- Se sugiere que al realizarse un monitoreo continuo de los recursos de la red se levanten adecuadamente las estadísticas e informes arrojados del desempeño de la red, debido a que la misma puede ofrecer información valiosa de dispositivos sobrecargados, deterioro de servicios y tráfico inusual. Lo antes descrito permitirá plantear un plan preventivo que solvente las necesidades existentes.
- En vista que la Institución está en vías de implementar voz y video sobre IP es adecuado considerar la posibilidad de adquirir dispositivos switch que otorguen calidad de servicios (QoS) esto porque provee un mejor trato en los recursos y no todos los dispositivos que contemplan la red lo consideran.
- En caso de optar por un enfoque que valore el rendimiento de la red y todos los factores que se ven inmersos sin querer repercutir directamente sobre la red se puede preferir el uso de simuladores de eventos discretos el mismo que presenta un enfoque analítico y una evolución temporal de lo que sucede en la red. La ventaja de hacer uso de este tipo de simuladores se ve porque es adecuado para sistemas complejos con muchos elementos, pero se debe recordar que esto es ideal; de igual forma se puede observar la dinámica de la red y si el modelo es lo más exacto a la realidad los datos obtenidos deberían ser lo más parecidos a la situación actual.
- Se debería considerar una valoración de los niveles de servicio que otorgan los proveedores de Internet todo en base a parámetros objetivos que evidencien valores máximos, mínimos o medios de lo ofrecido por parte del ISP; con el fin de conocer el grado de cumplimiento o incumplimiento de los

acuerdos de nivel de servicio (SLA) y tomar medidas en caso de la inobservancia o quebrantamiento de lo establecido.

4.1.1.5 Gestión de Seguridad

La Gestión de Seguridad tiene como aspecto fundamental mantener la integridad y confidencialidad de los datos esto debido a las múltiples intrusiones que soportan hoy en día muchas redes activas, indistintamente de su razón social. Para mantener una seguridad sostenible vale la creación de políticas de seguridad que siendo bien definidas logran controlar el acceso a los recursos de la red.

Las políticas de seguridad que se difundan deben considerar dos posturas que son:

- Una política defensiva orientada a disminuir o contrarrestar vulnerabilidades.
- Una política curativa orientada a disminuir el impacto que provoca una intrusión.

Entre las funciones que contempla esta gestión, se pueden mencionar las siguientes:

- Identificación de todo recurso sensible a intrusión sea este un dispositivo o información.
- Monitorización de los puntos de acceso a la información o recursos sensibles.
- Catalogar el acceso que tienen los diferentes grupos de usuarios frente a los recursos sensibles.
- Gestionar la generación, distribución y mantenimiento de claves para encriptación o contraseñas.
- Mantener reportes de intentos de intrusiones para su posterior análisis.
- Proporcionar mecanismos de seguridad contra cualquier tipo de ataque (captura no autorizada de información, suplantación de identidad, modificación de información, etc.) sobre la red.

4.1.1.5.1 Propuestas y consideraciones

Algunas de las propuestas que se deben tomar en cuenta se exponen a continuación:

- Una de las primeras fallas que se debe considerar es incrementar el nivel de seguridad de contraseñas por medio de la utilización de caracteres numéricos, alfanuméricos, mayúsculas, minúsculas y caracteres especiales que otorgan un mayor grado de dificultad para ser descubiertos por terceros.
- Se debe definir adecuadamente un análisis de riesgo que otorgue directrices acerca de las diferentes vulnerabilidades que la red o los sistemas pueden estar expuestos así mismo los planteamiento formulados acerca de las políticas de seguridad son de gran importancia en la Institución.
- El detectar si la red está bajo algún tipo de ataque puede ser crítico para una Institución pero el mismo puede ser salvaguardado por un sistema de detección de intrusos que alerte de algún cambio inusual en el tráfico circundante por la red.

4.1.1.5.2 Políticas de Seguridad

Las propuestas planteadas en esta etapa de seguridad deben considerarse como una guía a ser difundidas entre los principales ejes operativos del área de sistemas para lograr una cohesión entre las distintas partes, por otro lado este mismo plan debe sujetarse a un mejoramiento continuo que logre garantizar en gran medida que las últimas formas o métodos de ataque van a ser contenidos; todo en cuanto a las nuevas circunstancias y necesidades que se presenten.

Un factor importante antes de comenzar a elaborar las políticas de seguridad, es la asignación clara de responsabilidades. Responsabilidades que al ser dejadas de lado producirán malentendidos, problemas y retrasos.

Otro factor previo de gran relevancia involucra el sentir de las principales autoridades sean estas Administrativa Financiera, Recursos Humanos, así como la junta de miembros que coordinan directamente con el Administrador Zonal. La

conciencia, que cada uno de ellos demuestre, sobre la importancia vital de la información impulsara o disuadirá la idea de fomentar políticas de seguridad.

Es aconsejable y no es considerada como regla inmutable el evaluar las condiciones vulnerables, amenazas y riesgos que contenga la red antes del desarrollo de las políticas de seguridad. Esta evaluación constatara la seguridad otorgada.

Cabe mencionar que los factores antes mencionados no serán abordados en la elaboración de este proyecto debido en parte a la amplitud que el mismo presenta y la desvinculación del objetivo central que se maneja.

A continuación, se presentan muchas de las políticas que se sugieren someterse a consideración debido al impacto que cada una de ellas representa.

- El acceso a dispositivos de interconexión debe solo ser posible bajo una contraseña de seguridad adecuadamente asignada, que posibilite los permisos necesarios para el acceso y administración remota del dispositivo.
- Es prudente definir acuerdos de confidencialidad con términos legales que salvaguarden información crítica generada dentro de la Institución.
- El establecimiento de responsabilidades y procedimientos aseguran un accionar más rápido y contundente al momento de detectar un cambio o violación de seguridad dentro de las instalaciones.
- Como política general; nadie podrá tener juegos, videos o fotos que no sean de uso estrictamente laboral. En cuanto a música se puede ser permisivo ya que existen ciertos factores a ser tomados en cuenta que afectan directamente a la productividad. En el caso de empleados que están sometidos a tareas altamente repetitivas de corto tiempo, es aconsejable la influencia de cierto tipo de música; mientras que para empleados que demandan un alto nivel de concentración es preferible períodos cortos de este tipo de influencia para solventar mejor las cargas de trabajo. Cada una de estas situaciones bien enfocada (ligada directamente a las preferencias y al tipo de trabajo) estimula

profundamente los estados de ánimo de los individuos y alivian en gran medida a contrarrestar el estrés laboral.

a. Políticas de Servidores con Windows 2003 Server

- Que la política “Reproducción Automática” este deshabilitada.
- Revisión de servicios que vienen por omisión que no son utilizados como por ejemplo IIS, RAS, terminal services.
- Auditar periódicamente y verificar que los servicios que están abiertos son aquellos que están siendo utilizados. Algunos servicios a revisar:
    - Computer Browser
    - Microsoft DNS Server
    - Netlogon
    - NTLM SSP
    - RPC Locator
    - RPC Service
    - TCP/IP NetBIOS Helper
    - Spooler
    - Server
    - WINS
    - Workstation
    - Event Log
- Verificación de puertos abiertos en el servidor y configuración de los mismos vía consola de seguridad TCP/IP. Habilitar específicamente tráfico TCP e ICMP.
- Habilitar la auditoria en el servidor que brindara alertas en aspectos de seguridad como cambios en las políticas de seguridad, intentos en los rompimientos de claves, accesos no autorizados, modificaciones a privilegios de usuarios.
  Habilitar las siguientes opciones:
    - Eventos de login de usuario.

- Gestión de cuentas de usuario.
- Acceso a objetos.
- Cambios en políticas.
- Uso de privilegios.
- Eventos del sistema.

- Es importante registrar tanto los eventos exitosos como los fallidos ya que con las mismas se determinara que persona no autorizada intenta cambios en el servidor.
- Deshabilitar la opción de último usuario a desplegarse en la pantalla de inicio o bloqueo de sistema.
- Verificación de parches de seguridad liberados bajo boletines Microsoft de seguridad.
- Deshabilitar la opción de creación de archivo dump, misma opción que ofrece información valiosa sobre los por menores de los errores surgidos en el servidor (pantallazo azul).

b. Política de Seguridad Física

La seguridad física es uno de los factores dejados de lado en incontables ocasiones más suelen estar inmersos en otros parámetros. A continuación se exponen ciertos parámetros importantes a tomarse en cuenta.

b1. Riesgos de Incendios

Existen varios factores que pueden repercutir en la iniciación de fuego así tenemos:

- Uso inadecuado de combustibles.
- Fallas en instalaciones eléctricas.
- Traslado de sustancias peligrosas.

Además los factores a contemplar para reducir los riesgos de incendios en el interior de las instalaciones de centros de cómputo de la Institución son:

- El sitio donde se alojan las computadoras debe estar en un local que no sea combustible o inflamable.
- El local no debe situarse en las cercanías donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, corrosivos etc.
- Las paredes deben estar diseñadas de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área.
- Se debe hacer uso de muebles incombustibles, y cestos metálicos para papeles. Evitando en gran medida el uso de materiales plásticos e inflamables.
- Se debe tener cuidado que tanto el piso como el techo del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

b2. Seguridad de Equipamiento

Para proteger los equipos informáticos se debe tener especial cuidado de poseer áreas con mecanismos de ventilación y detección de incendios adecuados; además se debe tener presente ciertos factores.

- La temperatura no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos según su equipamiento deben poseer medios de extinción de acuerdo al grado de riesgo y clase de fuego que se pudiere generar.
- Como medida adicional deben existir extintores manuales debidamente ubicados y con instrucciones claras de cómo ser utilizados y bajo qué condiciones.

b3. Inundaciones

Se debe considerar como inundación la invasión de agua o desborde de la misma, ya sea de manera artificial como natural. Cabe la posibilidad de inundación provocada por la necesidad de apagar un incendio en un piso superior. Para procurar solventar estos inconvenientes se debe construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

c. Políticas de Seguridad de Acceso de Personal

- Debe emplearse el uso de tarjetas inteligentes las cuales pueden estar clasificadas de la siguiente manera:

    - Normal o definitiva (personal permanente de la planta).
    - Temporaria (personal recién ingresado).
    - Contratista (personas ajenas a la empresa que por razones de servicio deben ingresar a la misma).
    - Visitas.

  El uso de cada tarjeta otorga al portador privilegios según su status dentro de la Institución.

- El uso de tarjetas inteligentes con acceso especial al cuarto de servidores debe ser otorgado única y exclusivamente al Administrador de Sistemas o a la persona encargada del correcto funcionamiento de los dispositivos que se encuentran en esa área.

d. Políticas de Seguridad para computadores

- Las configuraciones de hardware y software otorgadas por el Departamento de Informática deben respetarse y en ningún caso modificadas sin consentimiento de la autoridad responsable del área de Informática.

- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Institución se requiere una autorización escrita. Se debe llevar un adecuado control al momento de mover o reubicar un equipo mediante la sistematización de un software que registre datos relacionados a las características propias de cada equipo pudiendo estar el mismo vinculado directamente como un módulo al sistema de inventarios y activos fijos. Haciendo uso de estos mecanismos se podrá establecer un mejor control tanto de equipos como dispositivos, evitando confusiones o pérdidas al momento de realizar las búsquedas pertinentes.
- La prevención de accesos no autorizados debe contemplar que el usuario posea contraseñas robustas además actuar directamente con el protector de pantalla mismo que se activara en un periodo prudente de inactividad y que requiere una contraseña al reasumir la actividad. Además en caso de ausentarse el usuario de su oficina deberá activar manualmente el protector de pantalla.

  Parámetros a tomar en cuenta para la elección de claves:

  - No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, lugares u otros relacionados).
  - No usar contraseñas completamente numéricas con algún significado (teléfono, fecha de nacimiento, etc.).
  - Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas, minúsculas) y numéricos.
  - Deben poseer 8 caracteres o más.
  - Tener contraseñas diferentes en máquinas diferentes. Es recomendable hacer uso de una contraseña base y ciertas variaciones lógicas para distintas máquinas.
  - Aunque tengan un grado de dificultad deben ser fáciles de recordar para no verse obligados a escribirlas.

Normas para proteger una clave:

- No permitir ninguna cuenta sin contraseña.
- No mantener las contraseñas por defecto del sistema.
- No escribir la contraseña en ningún sitio.
- No teclear la contraseña si alguien está mirando.
- No mantener una contraseña indefinidamente. Procurar cambiarla periódicamente.

- Todo software que se usa en la Institución debe comprenderse que está protegido por derechos de autor, a no ser que explícitamente se diga lo contrario. Tomando la premisa antes citada está terminantemente prohibido hacer copias o hacer uso del software de la Institución para fines personales de ámbito lucrativo.
- Para intervenir en pérdidas o daños de software original es prudente realizar copias de los discos originales y asegurarse de guardarlos en un lugar seguro.
- Se debe procurar realizar respaldos de la información de forma periódica tanto de pc's como servidores. Tales respaldos deben poseer las mayores normas de seguridad para salvaguardar condiciones como hurto, incendio e inundación. Así también todo dato o programa que tienda a ser de vital importancia debe guardarse en otra sede, lejos del edificio. Aspectos a tomar en cuenta:

  - Se debe de contar con un procedimiento que respalde tanto el sistema operativo como la información que contienen. Para poder reinstalar en caso de sufrir un daño.
  - Deben fijarse las herramientas adecuadas para realizar los respaldos teniendo en cuenta parámetros como, espacio libre, tiempos de lectura/escritura, tipo de backup a realizar.
  - Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. Para descartar daños, datos incompletos o mal almacenados.

- Se debe contar con una política para garantizar la privacidad de la información que se respalda. La información debe ser encriptada antes de respaldarse.
- Se debe contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento antes de desecharlos.

e. Políticas de Seguridad para las comunicaciones y confidencialidad

- El uso de los recursos de la Institución por parte del usuario, en lo referente a Internet debe solo usarse en horarios no laborables y de manera ocasional (con las respectivas delimitaciones de uso) que no interfiera con el desempeño de sus funciones ni ocasione una disminución en las actividades de la Institución.
- Es de comprender que la seguridad que otorgan los sistemas internos no necesariamente son ciento por ciento efectivos al ser expuestos externamente, en tales condiciones el envío o recepción de mensajes de correo con carácter confidencial deben procurar poseer claves de cifrado.
- Es política de la Institución analizar con cierta regularidad el uso y el contenido que en los medios propios de comunicación existen, este tipo de actividad viene a ser necesaria por cuestiones como mantenimiento, seguridad o auditoria.
- Todo el personal nuevo debe conocer con antelación las responsabilidades y obligaciones que genera la violación de normas de seguridad. Al personal nuevo se le debe facilitar el respectivo curso de inducción que muestre de manera clara que está facultado para realizar o no dentro de la Institución.
- El personal no está autorizado a revelar información de contraseña a terceros o permitir el uso de la cuenta. Esto incluye tanto a familiares como personas con algún tipo de nexo.
- El análisis de puertos con propósitos de seguridad solo debe ser realizado con autorización expresa del administrador del sistema.

- No está permitido facilitar información de listas de empleados a personas ajenas a la Institución bajo ninguna circunstancia.
- Se puede someter de una manera sumamente rígida con las medidas dispuestas por la Institución o ejes pertinentes, a la persona o personas que con malas intenciones ocasionen una interrupción de los servicios ligados tanto con la red, como con los distintos servidores que apoyan las actividades de la Institución intentando u ocasionando ataques de negación de servicio.
- Transgredir con el envío no autorizado de mensajes de correo electrónico no solicitado y con enfoque publicitario, supone problemas de seguridad a nivel de spam, en cuyo caso se debe analizar la manera en que los spammers lograron el acceso a las listas de correo de la Institución.
- Es política de la Institución el mantener un adecuado control y mantenimiento sobre herramientas que proveen seguridad ante problemas de virus, spyware o cualquier código malicioso que pueda ocasionar algún tipo de daño en los dispositivos o elementos que integran la red.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se ha logrado prever dificultades que ocasionarían disminución del rendimiento en terminales de usuario o consecuentemente provocar la inactividad de los elementos que conforman la red.
- Analizando los sistemas de gestión libres y poniendo como contraparte los sistemas propietarios se ha llegado a la conclusión que los sistemas libres se acoplan de mejor manera a muchos de los ámbitos empresariales hoy por hoy existentes, demandando pocos recursos tanto económicos, de infraestructura o implementación.
- Se ha llegado a la decisión que el sistema que presenta las condiciones más propicias para llegar a una implantación total por parte de la Institución es OpenNMS por cuanto las distintas valoraciones a las que ha sido sometida han mostrado un desenvolvimiento superior en relación con los otros sistemas de gestión libres analizados.
- El lograr enfocarse en prever situaciones pequeñas que desencadenarían grandes problemas, ha facilitado afianzar un alto nivel de servicio en los recursos gestionados con un coste bajo.
- Uno de los principales problemas que acarrea gestionar una red se enfoca con la expansión de esta, debido a la falta de planificación estratégica que debe ser contemplada para su crecimiento. De hecho un porcentaje muy importante del coste de una red corporativa se atribuye a su gestión y operación.
- El estándar básico de SNMP proporciona solamente autentificación trivial. Así el SNMP básico es más conveniente para monitoreo que para control.
- SNMPv3 define una serie de capacidades de seguridad y un marco que hace posible su uso junto con las PDUs de SNMPv2 por lo cual SNMPv3 acoge una modularidad que la describe como SNMPv2 más seguridad y administración. Lo que busca esta versión es cubrir las falencias de sus

predecesoras, mejorando sus componentes y ofreciendo una fortaleza en su seguridad así como facilidad de administración.

- En reiteradas ocasiones la no existencia o falta de políticas de gestión claras provoca la adquisición de tecnología de punta intentando satisfacer las carencias existentes tanto de computadoras más potentes como de la propia red; esto deriva en un desconocimiento más profundo de las verdaderas causas del bajo rendimiento o la falla frecuente.

RECOMENDACIONES

- Se debe realizar una elección adecuada para determinar el tipo de protocolo a usarse sea este SNMP o CMIP basando la decisión en diferentes criterios como recursos del sistema, un buen sistema de seguridad de red, una interfaz amigable, implementación relativamente barata y una reducción del tiempo empleado en gestión.
- En la gestión de configuración un aspecto importante es la gestión de inventario en la cual centra su accionar en saber que recursos se poseen, tanto en dispositivos como módulos es por eso la importancia de ligar una gestión de inventario que facilite toda esa información de forma clara y transparente.
- Vale la pena dar conciencia a los usuarios de la importancia de la seguridad de la información y la responsabilidad que en cada uno de ellos recae; esto con el afán de precautelar información sensible generada en la Institución.
- Se sugiere analizar los mecanismos y recomendaciones que exponen estándares globalmente reconocidos y ligados a conservar la integridad, seguridad de la información así como otros aspectos importantes; los estándares mencionados son la ISO 27000, COBIT e ITIL. Cabe mencionar que el mejor alineamiento que se pueda realizar entre estos tipos de estándares repercute enormemente en la gestión de negocios que una empresa mantiene pero su enfoque debe ser dirigido a la alta dirección sean estos gerentes, auditores, directores de TI, entre los principales.

REFERENCIAS BIBLIOGRÁFICAS

PROYECTOS DE TITULACIÓN

- BALSECA ALCOCER, Sandra Patricia, CACHIMUEL QUEREMBÁS, Miguel Eduardo, *Evaluación y auditoría informática del sistema de información de la Escuela Politécnica del Ejercito: dominio entrega de servicios y soporte,* ESPE Carrera de Ingeniería de Sistemas e Informática, Sangolquí, 29 de abril de 2008.
- CUEVA PONCE, Andrés Patricio, GARCÍA GUZMÁN, Jessica Alicia, *Rediseño de la red inalámbrica que comunica los centros educativos del proyecto Quito Educ@net con su datacenter*, EPN Facultad de Ingeniería Eléctrica y Electrónica, Quito, julio de 2009.
- ROSERO VLASOVA, Olga Alexandra, PROAÑO SARASTI, Diego Alejandro, *Estudio y Desarrollo de una metodología para la implementación de un modelo de gestión y administración de red para la Universidad Técnica Estatal de Quevedo (UTEQ)*, EPN Facultad de Ingeniería Eléctrica y Electrónica, Quito, julio de 2009.
- PERUGACHI ALVEAR, Félix Tomás, *Reingeniería de la red LAN del ilustre Municipio del Cantón Rumiñahui*, EPN Facultad de Ingeniería Eléctrica y Electrónica, Quito, junio de 2010.
- GHULYAN Karen, *Sistema de Monitorización adaptativo para Sistemas Distribuidos*, Universidad Carlos III de Madrid Carrera de Ingeniería en Informática, Madrid, junio de 2009.

LIBROS

[7] STALLINGS, William, *Fundamentos de seguridad en redes.* Segunda edición. Editorial Pearson Educación. Año 2004.

MANUALES

[10] Manual Orgánico Funcional, Administración Zonal Norte “Eugenio Espejo”, Año 2007.

- SNMP, Dr. Victor J. Sosa Sosa, Año 2008.

PAGINAS WEB

[1] Antonio Martin Montes, Carlos León de Mora, Gestión de Redes, 2002,
URL: http://personal.us.es/toni/_private/ManagementNetwork.pdf

[2] Ramón Millán, SNMPv3, 2003,
URL: http://www.ramonmillan.com/documentos/snmpv3.pdf

[3] Universidad de Salamanca, SNMP, 2006,
URL: http://web.usal.es/%7Eser/rdo/2005-2006/SNMP/Intro%20SNMP.html

[4] Vincenzo Mendillo, Gestión de Redes con SNMP, 2009,
URL: http://gdiaz.serveftp.com/PUBLICACIONES/GESTION_REDES/PLATAFORMAS_GESTION_REDES/Gesti%C3%B3n%20de%20redes%20con%20SNMP.pdf

[5] Ramón Millán, Gestión de Red, 2006,
URL: http://www.ramonmillan.com/tutoriales/gestionred.php#Arquitectura

[6] Wikipedia, MD5, 2011,
URL: http://en.wikipedia.org/wiki/MD5

[8] Google Maps, Foto satelital Administración Norte Municipio, 2011,
URL: http://maps.google.com/maps?ll=-0.220229,-78.512352

[9] Municipio de Quito, Administración Eugenio Espejo, 2011,
URL: http://www.quito.gov.ec/el-municipio/administraciones/administracion-eugenio-espejo.html

[11] Squid-cache.org, Optimising Web Delivery, 2011,
URL: http://www.squid-cache.org/

[12] Microsoft TechNet, Office Communication Server, 2007,
URL: http://www.microsoft.com/latam/technet/articulos/tn/2007/jun-01.mspx

[13] Wikipedia, GNU/Linux, 2011,
URL: http://es.wikipedia.org/wiki/GNU/Linux

[14] ALEGSA, Definición de VSAM, 2011,
URL: http://www.alegsa.com.ar/Dic/vsam.php

[15] Todoexpertos, Arquitectura AS400, 2010,
URL:http://www.todoexpertos.com/categorias/tecnologia-e-internet/software-y-aplicaciones/respuestas/223829/as400

[16] Wikipedia, Calidad de servicio, 2011,
URL: http://es.wikipedia.org/wiki/Calidad_de_servicio

[17] Red Hat, Inc, Protocolo SSH, 2005,

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

[18] Wikipedia, Congestión de red, 2010,
URL: http://es.wikipedia.org/wiki/Congesti%C3%B3n_de_red

[19] Wikipedia, Nasdaq, 2011,
URL: https://secure.wikimedia.org/wikipedia/es/wiki/Nasdaq

[20] PandoraFMS, Sistema de monitorización flexible, 2011,
URL: http://pandorafms.org/

[21] Jorge López, Configuración del Sistema con Webmin, 2010,
URL: http://www.iberprensa.com/todolinux/articulos/TL95_webmin.pdf

[22] Wikipedia, OpenVZ, 2011,
URL: https://secure.wikimedia.org/wikipedia/es/wiki/OpenVZ

[23] Wikipedia, OpenSSL, 2011,
URL: https://secure.wikimedia.org/wikipedia/es/wiki/OpenSSL

[24] Wikipedia, Webmin, 2011,
URL: http://es.wikipedia.org/wiki/Webmin

[25] Wikipedia, TACACS+, 2011,
URL: https://secure.wikimedia.org/wikipedia/es/wiki/TACACS%2B

[26] Wikipedia, HTML dinámico, 2011,
URL: http://es.wikipedia.org/wiki/HTML_dinámico

[27] Wikipedia, Internetwork Operating System, 2011,
URL: http://es.wikipedia.org/wiki/Internetwork_Operating_System

[28] Wikipedia, Throughput, 2010,
URL: http://es.wikipedia.org/wiki/Throughput

- SNMPLink.org, Simple Network Management Protocol, 2011,
  URL: http://www.snmplink.org/
- ENCYDIA, Simple Network Management Protocol, 2011,
  URL: http://es.wikilingue.com/pt/Simple_Network_Management_Protocol
- ARCESIO, Structure of Management Information (SMI) para SNMPv1,
  URL: http://www.arcesio.net/osinm/asn1.html
- SimpleWeb, Network Management, 2011,
  URL: http://www.simpleweb.org/
- Wikipedia, Management Information Base, 2011,
  URL: http://es.wikipedia.org/wiki/Management_Information_Base

- Sun Microsystems, Inc., Best-Practice Recommendations Configuration Management, 2007,
  URL: www.sun.com/emrkt/sunspectrum/configurationwhitepaper.pdf
- Wikipedia, FCAPS, 2010,
  URL: http://es.wikipedia.org/wiki/FCAPS
- William Borbor, Rebeca Estrada, Instalación y configuración de Software Open Source para monitorear el servicio y la carga de un sistema Asterisk,
  URL:
  http://www.dspace.espol.edu.ec/bitstream/123456789/8338/1/Instalaci%25C3%25B3n%2520y%2520Configuraci%25C3%25B3n%2520de%2520Software%2520Open%2520Source.pdf
- Federico Navarro, Administración de Redes,
  URL: www.ecomchaco.com.ar/utn/AdmRedes/Traduccion/Cap8.doc
- Nagios, Welcome To Nagios, 2011,
  URL: http://www.nagios.org
- OpenNMS, Get the Network to Work® with OpenNMS! , 2011,
  URL: http://www.opennms.org
- Ntop, Ntop, 2011,
  URL: http://www.ntop.org
- Wireshark, Wireshark, 2011,
  URL: http://www.wireshark.org
- Wireshark, Wireshark Wiki, 2010,
  URL: http://wiki.wireshark.org
- JFFNMS, Welcome JFFNMS, 2011,
  URL: http://www.jffnms.org
- Webmin, Webmin, 2009,
  URL: http://www.webmin.com
- José Antonio Escartín, Servicio de administración por web (Webmin), 2005,
  URL: http://upcommons.upc.edu/pfc/bitstream/2099.1/3451/10/52096-10.pdf