UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS PRESENTADA PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES.

TEMA:

"ANÁLISIS E IMPLEMENTACIÓN DE HERRAMIENTAS DE SOFTWARE LIBRE PARA LA SEGURIDAD Y MONITOREO DE LA RED DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, UBICADA EN EL BARRIO EL EJIDO, CANTÓN LATACUNGA EN EL AÑO 2012"

Autores:

Aymara Quinga Marisol Rocio

Chancúsig Chicaiza Julio César

Director:

Ing. Patricio Navas

Asesor Metodológico:

Lic. Susana Pallasco

Latacunga-Ecuador

Junio - 2013

AUTORÍA

Los criterios emitidos en el presente trabajo de investigación: "**ANÁLISIS E IMPLEMENTACIÓN DE HERRAMIENTAS DE SOFTWARE LIBRE PARA LA SEGURIDAD Y MONITOREO DE LA RED DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, UBICADA EN EL BARRIO EL EJIDO, CANTÓN LATACUNGA EN EL AÑO 2012**", son de exclusiva responsabilidad de los autores.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo de investigación a la Universidad Técnica de Cotopaxi, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

……..	……..
Aymara Quinga Marisol Rocío	Chancúsig Chicaiza Julio César
C.I.: 172268636-5	C.I.: 050345499-3

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE INGENIERÍA Y APLICADAS

AVAL DEL DIRECTOR DE TESIS

Cumpliendo con lo estipulado en el Reglamento de Graduación en el Nivel de Pregrado de la Universidad Técnica de Cotopaxi, es grato informar que el grupo conformado por la: Srta. Aymara Quinga Marisol Rocío con C.I.: 172268636-5 y el Sr. Chancúsig Chicaiza Julio César con C.I.: 050345499-3, egresados de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas han desarrollado su investigación de grado de acuerdo a los planteamientos formulados en el Proyecto de Tesis.

En virtud de lo antes expuesto considero que el grupo se encuentra habilitado para presentarse al acto de Defensa de Tesis, cuyo tema es: **"ANÁLISIS E IMPLEMENTACIÓN DE HERRAMIENTAS DE SOFTWARE LIBRE PARA LA SEGURIDAD Y MONITOREO DE LA RED DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, UBICADA EN EL BARRIO EL EJIDO, CANTÓN LATACUNGA EN EL AÑO 2012"**

Latacunga, 12 de Marzo del 2013.

……..

Ing. Patricio Navas

DIRECTOR DE TESIS

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE INGENIERÍA Y APLICADAS

AVAL DEL ASESOR DE TESIS

En calidad de Asesor de trabajo de investigación sobre el tema:

"ANÁLISIS E IMPLEMENTACIÓN DE HERRAMIENTAS DE SOFTWARE LIBRE PARA LA SEGURIDAD Y MONITOREO DE LA RED DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, UBICADA EN EL BARRIO EL EJIDO, CANTÓN LATACUNGA EN EL AÑO 2012"

Del grupo conformado por la: Srta. **AYMARA QUINGA MARISOL ROCÍO** y el Sr. **CHANCÚSIG CHICAIZA JULIO CÉSAR**, egresados de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas.

Una vez revisado el documento entregado a mi persona, considero que dicho informe investigativo cumple con los requerimientos metodológicos y aportes Científicos – Técnicos necesarios para ser sometidos a la Evaluación del Tribunal de Validación de Grado que el Honorable Consejo Académico designe para su correspondiente estudio y calificación.

Latacunga, 12 de Marzo del 2013.

……..

Lic. Susana Pallasco

ASESOR METODOLÓGICO

AGRADECIMIENTO

Agradezco en primer lugar a Dios quien me dio la vida y la ha llenado de bendiciones en todo este tiempo, a él que con su infinito amor me ha dado la sabiduría suficiente para culminar mi carrera universitaria.

A mis padres, por todo el esfuerzo que hicieron para darme una profesión y hacer de mí una persona de bien, gracias por los sacrificios y la paciencia que demostraron todos estos años; gracias a ustedes he llegado a donde estoy.

Agradezco también la confianza y el apoyo brindado por parte de mi madre, que sin duda alguna en el trayecto de mi vida me ha demostrado su amor, corrigiendo mis faltas y celebrando mis triunfos.

A mi padre, que con sus consejos me ha ayudado a afrontar los retos que se me han presentado a lo largo de mi vida. Y sé que está orgulloso de la persona en la cual me he convertido.

A mis hermanos, quienes han sido amigos fieles y sinceros, en los que he podido confiar y apoyarme para seguir adelante.

Gracias a todas aquellas personas que de una u otra forma nos ayudaron a crecer como personas y como profesionales.

Agradezco también de manera especial a nuestro director de tesis quién con sus conocimientos y apoyo supo guiar el desarrollo de la presente tesis desde el inicio hasta su culminación.

"Ahora puedo decir que todo lo que soy es gracias a todos ustedes"

Marisol Rocio Aymara Quinga

AGRADECIMIENTO

A Papito Dios, por estar presente en cada momento de mi vida dándome las fuerzas necesarias para continuar luchando día tras día y seguir rompiendo todas las barreras que se me presentan...

A mi madre por brindarme su apoyo incondicional en todo momento de mi vida, educarnos a mis hermanos y a mí para ser personas de bien.

A mi padre por darnos la oportunidad de estudiar lo que mis hermanos y yo deseábamos y darlos los recursos necesarios para desenvolvernos, además de comprendernos y apoyarme en las situaciones críticas de mi vida.

A mis hermanos porque con el apoyo mutuo, que nos damos, podemos sacar adelante cualquier dificultad que se nos presente en la vida.

A los profesores que me acompañaron en toda mi vida estudiantil ya que con su esmero y dedicación me formaron académica y moralmente.

Julio César Chancúsig Chicaiza

DEDICATORIA

Esta tesis se la dedico a mi Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mi familia quienes por ellos soy lo que soy.

A mis padres, por su apoyo, comprensión y ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar, me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

A mi madre, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional, que ha sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante en los momentos más difíciles.

A mi padre quien con sus consejos ha sabido guiarme para culminar mi carrera profesional.

A mis hermanos por estar siempre presentes, acompañándome para poderme realizar.

"La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar". ***Thomas Chalmers.***

Marisol Rocio Aymara Quinga

DEDICATORIA

Mi proyecto de tesis la dedico con todo mi amor y cariño:

A ti Dios que me diste la oportunidad de vivir y de regalarme una familia maravillosa, y a una mujer muy especial en mi vida a quien le debo mi inspiración para realizar este proyecto de tesis y a mis queridos Padres que me dieron la vida y han estado conmigo en todo momento.

A mis hermanos Polivio, Danilo y Alex gracias por estar conmigo y apoyarme siempre, los quiero mucho. Y a mis abuelitos, tíos y tías por estar siempre conmigo y consentirme tanto, los quiero. A ti Ipolito a pesar de que no estás aquí ahora en estos momentos conmigo, sé que tu alma si lo está y por qué tuviste los mismos sueños que Yo te dedico con todo mi corazón mi tesis. Nunca te olvidaré...

To my dearest austrian family, Ajmal, Lourdes, Asif and Elisa thank you very much for being with me I will never forget you. I love you with all my heart.

Julio César Chancúsig Chicaiza

ÍNDICE GENERAL

CONTENIDO PÁG.

CAPÍTULO I

FUNDAMENTOS TEÓRICOS DE OPEN SOURCE

CAPÍTULO II

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO III

IMPLEMENTACIÓN DE LAS HERRAMIENTAS DE SOFTWARE LIBRE PARA LA SEGURIDAD Y MONITOREO DE LA RED DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

ÍNDICE DE GRÁFICOS

CONTENIDO **PÁG.**

ÍNDICE DE TABLAS

CONTENIDOS PÁG.

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

Latacunga – Ecuador

TEMA: "ANÁLISIS E IMPLEMENTACIÓN DE HERRAMIENTAS DE SOFTWARE LIBRE PARA LA SEGURIDAD Y MONITOREO DE LA RED DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, UBICADA EN EL BARRIO EL EJIDO, CANTÓN LATACUNGA EN EL AÑO 2012"

Autores:

Srta. Aymara Quinga Marisol Rocio

Sr. Chancúsig Chicaiza Julio César

RESUMEN

La Universidad Técnica de Cotopaxi cuenta con la carrera de Ingeniería en Informática y Sistemas Computacionales, fue creada en el año de 1997 como respuesta a las demandas del mercado. Su pensum y programas de estudio se han venido actualizando periódicamente para mantenerlo al ritmo de los cambios de la disciplina y de la tecnología que se usa en la profesión.

El presente proyecto detalla el análisis e implementación de un sistema de seguridad y monitoreo para la red de la Universidad Técnica de Cotopaxi, realizado sobre una plataforma GNU/Linux, para la seguridad, medición y monitoreo del tráfico, que circula sobre la red LAN de la Institución.

Para ello el proyecto implementado, se fundamenta en la utilización de herramientas Open Source como son IPCop y Nagios, estos estarán encargados de la administración de la seguridad y monitoreo de la red, respectivamente, el resultado y la interacción de dichas herramientas entre sí, han contribuido entregando sus resultados, para el planteamiento de la solución adecuada a los problemas presentes.

Estos denominados problemas, recaen en tres aspectos esenciales: sobredimensionamiento de las capacidades de la red LAN de la Institución, falta de criterios de seguridad, en cuanto al tráfico real que circula dentro de la red y erróneos o casi nulos criterios del monitoreo y planificación del crecimiento de la red.

Luego del análisis de los resultados, se llega a plantear una solución a estos inconvenientes, implementando criterios de seguridad y control del tráfico generado por los usuarios, y sentando la base de un sistema de seguridad y monitoreo, automático, eficaz y proactivo.

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

Latacunga – Ecuador

TOPIC: "ANALYSIS AND IMPLEMENTATION OF FREE SOFTWARE TOOLS FOR MONITORING AND SECURITY AT COTOPAXI TECHNICAL UNIVERSITY NETWORK, LOCATED EL EJIDO NEIGHBORHOOD, LATACUNGA CANTON IN 2012"

Authors:

Srta. Aymara Quinga Marisol Rocio

Sr. Chancúsig Chicaiza Julio César

ABSTRACT

The Technical University of Cotopaxi has the Computer Engineering and Computer Systems career. It was founded in 1997 as market demands response. Its curriculum and study programs have been updated regularly to maintain market changes in the discipline and the technology used in the profession.

This project details the analysis and implementation of a security and monitoring system for the Technical University of Cotopaxi network, performed on a GNU/Linux platform for the safety, measurement and monitoring of traffic flowing over the network LAN Institution.

For this, the implemented project is based on the use of Open Source tools like IPCop and Nagios. These are responsible for security management and network monitoring, respectively, the interaction result of these tools together, have contributed delivering their results to the approach of the right solution to the current problems.

These so-called problems, fall into three essential areas: Institution LAN network capacities over sizing, lack of safety criteria, in terms like real traffic flowing within the network, and incorrect or almost zero criteria for monitoring and planning network growth.

The results were analyzed. It determined to establish a solution to these problems such as: implementing safety criteria and control the traffic generated by users, and laying the base of a security and monitoring system, automatic, efficient and proactive.

INTRODUCCIÓN

El internet basa su funcionamiento en el protocolo TCP/IP, protocolo que posee innumerables ventajas, una de las principales, es el control y monitoreo que puede ser realizado de múltiples maneras, utilizando diferentes herramientas que permiten conocer el estado de las redes involucradas en el tráfico de datos: flujo de protocolos, estabilidad del enlace, puntos de saturación, y consumo externo e interno.

En estos puntos fundamentales recae la verdadera importancia de un sistema de seguridad y monitoreo con el fin de controlar y personalizar el servicio brindado.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta institucional para concientizar a cada uno de los miembros de una institución sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la institución y su buen funcionamiento.

En la Universidad Técnica de Cotopaxi, institución formativa integral de profesionales, con una planta docente de excelencia a tiempo completo, que genera proyectos investigativos, comunitarios y de prestación de servicios, que aportan al desarrollo local, regional en un marco de alianzas estratégicas nacionales e internacionales.

Difunde el arte, la cultura y el deporte, dotada de una infraestructura adecuada que permita el cumplimiento de actividades académicas, científicas, tecnológicas, recreativas y culturales, fundamentadas en la práctica axiológica y de compromiso social, con la participación activa del personal administrativo profesional y capacitado, ubicada en el Barrio El Ejido, Sector San Felipe, Cantón Latacunga, Provincia de Cotopaxi, no ha podido quedarse al margen de la tecnología actual; por lo que cuenta con el servicio de internet con la Corporación Nacional de Telecomunicaciones como Proveedor de Servicios de Internet (ISP).

En primera instancia se procederá a realizar un análisis de las herramientas de software libre para la seguridad y monitoreo de la red LAN de la Universidad Técnica de Cotopaxi, tomando en cuenta su ingeniería actual. Para esto se realizará un análisis, sobre las ventajas y desventajas de algunos de los sistemas de seguridad y monitoreo más utilizados, con el fin de determinar su adaptabilidad a la ingeniería actual de la red LAN de la Institución, posterior a esto se instalaran las herramientas en un servidor.

Para lo que se ha subdivido este proyecto en tres Capítulos:

En el Capítulo I se ha establecido el marco teórico y conceptual que respalda a la investigación en cuanto a la recopilación de teorías y explicaciones para el análisis e implementación de herramientas de software libre para la seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi.

En el Capítulo II se encuentra el análisis e interpretación de los resultados obtenidos de las encuestas y su respectiva tabulación, para conocer los criterios emitidos por los involucrados dentro del área de cobertura de la red, permiten conocer las necesidades reales de dicha área y la factibilidad para la realización de la propuesta.

En la investigación se empleó los estándares de calidad de servicio para el mejoramiento del flujo de información en la red, como son: IEEE 802.1X, IEEE 802.1Q, IEEE 802.1D, y IEEE 802.1P, Q – QoS sobre el nivel de MAC, para estandarizar la investigación.

Por último en el Capítulo III una vez comprobada las necesidades que actualmente presenta la Universidad Técnica de Cotopaxi en al área de las Redes y Telecomunicaciones, se describe la propuesta de implementación de un sistema de seguridad y monitoreo de la red para la Institución y su correcto funcionamiento se describe en el Manual Técnico.

CAPÍTULO I

1. FUNDAMENTACIÓN TEÓRICA DE OPEN SOURCE

Open Source. (2011). Recuperado el 12 de junio de 2012, de http://www.código austral.com/open-source/

El uso de Open Source nació por primera vez en 1998 de la mano de algunos usuarios de la comunidad del Software libre, tratando de usarlo como reemplazo al ambiguo nombre original free software. Free en inglés significa dos cosas distintas dependiendo del contexto: gratuidad y libertad. Es decir software que podemos leer, modificar y redistribuir gratuitamente.

El término para algunos no resultó apropiado como remplazo para el ya tradicional free software, pues eliminaba la idea de libertad, confundida usualmente con la simple gratuidad. No obstante, el término código abierto continúa siendo ambivalente, puesto que en la actualidad es usado por programadores que no ofrecen software libre pero, en cambio, sí ofrecen el Código fuente de los programas para su revisión o modificación previamente autorizada por parte de sus pares académicos.

Código libre. (2009). Recuperado el 12 de junio de 2012, de http://servidores-linux-para-empresas.hypersys.com.ar/servidores-linux-para-empresas/gnulinux/debían/

open-source.html

> Son programas que ofrecen total libertad de modificación, uso y distribución bajo la regla implícita de no modificar dichas libertades hacia el futuro. Desde el punto de vista de una traducción estrictamente literal, el significado textual de ***código abierto*** es que se ***puede examinar el Código fuente***, por lo que puede ser interpretado como un término más débil y flexible que el del software libre. Sin embargo, ambos movimientos reconocen el mismo conjunto de licencias y mantienen principios equivalentes. Sin embargo, hay que diferenciar los programas de código abierto, que dan a los usuarios la libertad de mejorarlos, de los programas que simplemente tienen el código fuente disponible, previa restricciones sobre su uso o modificación.

Consideramos que en la actualidad el código abierto se utiliza para definir un movimiento nuevo de software, diferente al movimiento del software libre, incompatible con este último desde el punto de vista filosófico, y completamente equivalente desde el punto de vista práctico, de hecho, ambos movimientos trabajan juntos en el desarrollo práctico de proyectos.

1.1. Definición de Open Source

Código Abierto. (2005). Recuperado el 12 de junio de 2012, de http://www.open system.co/index.php/art-acercaopenerp/em-codigoabierto

> La idea bajo el concepto de código abierto es simple, cuando los programadores (en Internet) pueden leer, modificar y redistribuir el código fuente de un programa,

éste evoluciona, se desarrolla y mejora. Los usuarios lo adaptan a sus necesidades, corrigen sus errores a una velocidad impresionante, mayor a la aplicada en el desarrollo de software convencional o cerrado, dando como resultado la producción de un mejor software.

Según la perspectiva grupal, el código abierto o fuente abierta es el término con el que se conoce al software distribuido y desarrollado libremente, tiene un enfoque encaminado a los beneficios prácticos de poder acceder al código, que a las cuestiones éticas y morales las cuales se destacan en el software libre.

1.1.1. Movimientos Open Source

Opensource. (2011). Recuperado el 19 de julio de 2012, de http://www.monparesa .net/index.php/servicios/2-uncategorised/4-opensource

El movimiento Open Source tiene un decálogo que debe cumplir un código para poder llamarse ***Open Source***, es de hacer notar que estas diez premisas son completamente equivalentes con las cuatro libertades del Software Libre, éstas son:

1. ***Libre redistribución:*** Debe poder ser regalado o vendido libremente.
2. ***Código fuente:*** Debe estar incluido u obtenerse libremente.
3. ***Trabajos derivados:*** Redistribución de modificaciones debe estar permitida.
4. ***Integridad del código fuente del autor:*** Las licencias pueden requerir que las modificaciones sean redistribuidas sólo como parches.
5. ***Sin discriminación de personas o grupos:*** Nadie puede dejarse fuera.

6. ***Sin discriminación de áreas de iniciativa:*** Usuarios comerciales no pueden ser excluidos.
7. ***Distribución de la licencia:*** Deben aplicarse los mismos derechos a todo el que reciba el programa.
8. ***La licencia no debe ser específica de un producto:*** El programa no puede licenciarse solo como parte de una distribución mayor.
9. ***La licencia no debe restringir otro software:*** La licencia no puede obligar a que algún otro software que sea distribuido con el software abierto deba también ser de código abierto.
10. ***La licencia debe ser tecnológicamente neutral:*** No debe requerirse la aceptación de la licencia por medio de un acceso por clic de ratón o de otra forma específica del medio de soporte del software.

GRÁFICO N° 1.1. MOVIMIENTO OPEN SOURCE

Fuente: (VARGUX, 2009)
Disponible en Web: http://es.scribd.com/doc/48538134/29/Fuentes-de-imagen-Licencias-y-contribuyentes.

De acuerdo a lo antes mencionado podemos decir qué, el movimiento Open Source le da al usuario la libertad de mejorar y modificar un programa gracias al código fuente que le fue cedido y así aportar con nuevas ideas a la comunidad tecnológica.

1.1.2. Ventajas Open Source

Cobo (2005) enumera:

Algunas de las ventajas que proporciona el software Open Source:

- Las distribuciones de software Open Source son generalmente gratuitas o a un coste muy bajo, teniendo en cuenta que con sus licencias dan al usuario libertad para hacer con la aplicación las modificaciones o distribuciones que consideren oportunas sin ningún coste añadido.

- El código de los programas es abierto y por tanto no depende de una sola empresa desarrollada ni de su política y permite total flexibilidad para adaptar el programa a las necesidades de los usuarios.

- Mayor calidad y seguridad en los programas, esto es debido tanto a que el código sea libre como a la metodología de trabajo de las comunidades, que permite que un elevado número de programadores pueda revisar y trabajar simultáneamente sobre un mismo código, detectado errores que de otra manera serían difíciles de detectar.

- Rapidez de desarrollo, la evolución y lanzamiento de versiones mejoradas en el software Open Source es muy superior al software cerrado.

- Escucha activa a los usuarios y retroalimentación entre la producción del software, desarrolladores y los usuarios mediante una relación directa y de colaboración (p. 51).

Según el criterio de los investigadores se puede definir qué, las ventajas del Open Source cuenta con una gran comunidad de usuarios y como el código es libre, cualquiera puede añadir sus ideas y mejorar los programas, así se actualizan con más frecuencia e incorporan más funciones, su principal ventaja es que es completamente gratuito.

1.2. GNU/Linux

1.2.1. Software Libre

Según Roca (2007) manifiesta qué:

> La noción del software libre inicia con Richard Stallman, y aunque en la actualidad se habla de software libre y de software gratuito no hay que confundir el concepto de libre con gratis. Un software libre debe entenderse como aquello en que el usuario tiene la libertad de acceder a su código, usarlo, copiarlo, estudiarlo, modificarlo, y redistribuirlo libremente. Si el usuario ha modificado el código o ha creado alguna herramienta, este no puede negar tal código ya que al ser libre, otro usuario puede acceder a este, sin embargo la persona quien modificó el software puede optar por redistribuirlo sin costo alguno, o a su vez pedir dinero por su código.
>
> Dentro del software libre existen ciertas libertades los mismos que se definen a continuación:

- ***Libertad 0:*** Permite que el software pueda ser usado para cualquier propósito.

- ***Libertad 1:*** Puede ser estudiado y posteriormente modificado por un determinado usuario, adaptando tales modificaciones a sus necesidades, para ello esta libertad garantiza el acceso al código fuente.

- ***Libertad 2:*** Permite que el software pueda ser distribuido libremente de la voluntad del autor. Es decir un usuario puede copiar, vender o prestar el software a las personas que este lo desee.

- ***Libertad 3:*** Permite que un usuario pueda mejorar el software y hacerlo público, de modo que toda la comunidad se beneficie. (p. 22).

Como investigadores manifestamos qué, el software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software libremente, es decir que viene a ser de gran ayuda a las personas para el estudio, ya que está asequible en Internet sin ninguna restricción, permitiendo el desarrollo de nuevos productos sin la necesidad de desarrollar todo el proceso partiendo desde cero.

1.2.2. Distribuciones GNU/Linux

Distribuciones GNU/Linux. (2007). Recuperado el 29 de julio de 2012, de http:// www.linux10.com.ar/distribuciones/distribuciones.htm

La base del sistema de cada distribución incluye el núcleo Linux, pero suele incluir también varios paquetes de software del proyecto GNU, la mayoría de los sistemas Linux incluyen también aplicaciones procedentes del mundo BSD y usualmente se utiliza la plataforma XFree86 para sostener interfaces gráficas. Actualmente la

mayoría de usuarios se pueden encontrar con una amplia gama de distribuciones todas ellas basadas en GNU/Linux, algunas de estas distribuciones están orientadas al uso en computadores, celulares, etc. A continuación se mencionan las distribuciones más populares que se pueden encontrar: Debian, Gentoo Linux, Mandrake Linux, Red Hat, SuSe y Ubuntu. Los usuarios pueden hacer modificaciones en el código fuente y ajustarlo a sus propias necesidades. Esto ha permitido que cada vez la gente prefiera sistemas basados en GNU/Linux ya que se pueden encontrar con muchas aplicaciones desarrolladas.

En base al criterio de los investigadores, Linux es un robusto Sistema Operativo que permite manejar grandes tareas. Muchas organizaciones e incluso entidades gubernamentales se están cambiando a GNU/Linux en lugar de otros entornos de trabajo como Windows, esto debido al bajo costo que implica adquirir y mantener sus sistemas, que además presta un alto nivel de seguridad.

1.3 Seguridad en las Redes

1.3.1 Definición de Seguridad

ARCERT Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina (2002) define qué "la seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de los bienes informáticos" (p. 21).

Conforme el criterio grupal la seguridad de la red, es un proceso o acción para prevenir el uso desautorizado del computador y no sufrir una invasión a la privacidad

teniendo en cuenta los peligros que los usuarios pueden tener si no están bien informados.

1.3.2 Objetivos de la Seguridad Informática

Según los fundamentos de Gómez (2011) manifiesta qué:

> Entre los principales objetivos de la Seguridad Informática se destacan los siguientes:
>
> - Minimizar y gestionar los riesgos, detectar los posibles problemas y amenazas a la seguridad.
>
> - Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
>
> - Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
>
> - Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.
>
> Para cumplir con estos objetivos una organización debe contemplar cuatro planes de actuación:
>
> - ***Técnico:*** Tanto a nivel físico como a nivel lógico.

- ***Legal:*** Algunos países obligan por Ley a que en determinados sectores se implanten una serie de medidas de seguridad, por ejemplo el sector de servicios financieros.

- ***Humano:*** Sensibilización, formación de empleados y directivos, definición de funciones y obligaciones del personal.

- ***Organizativo:*** Definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación (p. 40).

Los investigadores consideran qué, cada vez aparecen nuevos y complejos tipos de incidentes, aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean, para lo que se requiere efectivas acciones de concientización, capacitación y difusión de mejores prácticas.

1.3.3 Servicios de Seguridad de la Información

De acuerdo a Gómez (2011) expresa qué:

> La seguridad es un elemento muy importante en la gestión de los procesos de información de una institución. La seguridad de la información persigue proteger la información de posibles accesos y modificaciones no autorizadas, para poder alcanzar los objetivos descritos anteriormente es necesario contemplar una serie de servicios o funciones de seguridad de la información:
>
> - ***Confidencialidad:*** Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema

informático solo podrá ser leído por su legítimo destinatario. Este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de *backup* y/o de los datos transmitidos a través de redes de comunicaciones.

- ***Autenticación:*** Podemos hablar de la autenticidad de un equipo que se conecta a una red o intenta acceder a un determinado servicio. En este caso la autenticidad puede ser unilateral, cuando solo se garantiza la identidad del equipo (usuario o terminal que se intenta conectar a la red) o mutua, en el caso de que la red o el servidor también se autentica de cara al equipo, usuario o terminal que establece la conexión.

- ***Integridad:*** Significa que la información no ha sido alterada o destruida, por una acción accidental o por un intento malicioso.

- ***No repudiación:*** Este servicio consiste en implementar un mecanismo probatorio que permita demostrar la auditoria y envío de un determinado mensaje, de tal modo que el usuario que lo ha creado y enviado a través del sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envío.

- ***Disponibilidad:*** Referencia al hecho de que una persona autorizada pueda acceder a la información en un apropiado periodo de tiempo. Las razones de la pérdida de disponibilidad pueden ser ataques o inestabilidades del sistema.

- ***Autorización:*** Se persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático, una vez superado el proceso de autenticación de cada usuario.

- ***Auditabilidad:*** Permite registrar y monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados u autorizados.

- ***Reclamación de Origen:*** El sistema permite probar quien ha sido el creador de un determinado mensaje o documento.

- ***Responsabilidad:*** Asegurar que las acciones realizadas en el sistema por una entidad se puedan asociar únicamente a esa entidad, que será responsable de sus acciones. Es decir que una entidad no pueda negar su implicación en una acción que realizo en el sistema (p. 42).

1.3.4 Tipos de Seguridad

Podemos clasificar a la seguridad en redes en dos tipos que son:

1.3.4.1 Seguridad Física

Huerta (2005) cita qué:

> La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de computo así como los medios de acceso remoto del mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Es muy importante, que por más que nuestra institución sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.
>
> La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta

acceder físicamente a una sala de operaciones de la misma. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma (p. 21).

1.3.4.2 Seguridad Lógica

Según Bustamante (2005) manifiesta qué:

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo, es importante recalcar que la mayoría de los daños que puede sufrir un sitio de cómputo, no será solo sobre los medios físicos, sino, a la información almacenada y procesada. Así, la seguridad lógica, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee dentro de una institución o empresa es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la seguridad lógica.

Los objetivos que se plantean para la seguridad lógica son:

- Restringir el acceso a los programas y archivos.

- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

- Asegurar que se estén utilizando los archivos y programas correctos por el procedimiento correcto.

- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

- Que se disponga de pasos alternativos de emergencia para la transmisión de información (p. 7).

1.3.5 Tipos de Ataques

1.3.5.1 Ataques de intromisión

Consideramos que este tipo de ataque se desarrolla cuando alguien abre archivos, uno tras otro, en un computador hasta encontrar algo que le sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataques registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

1.3.5.2 Ataques de espionaje en líneas

Podemos señalar que este atentado se origina cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información.

1.3.5.3 Ataques de intercepción

Podemos indicar que este ataque se da cuando una entidad no autorizada consigue acceso a un recurso, este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este

ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas intercepción de datos, o bien la lectura de las cabeceras de paquetes para descubrir la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente en la intercepción de identidad.

1.3.5.4 Ataques de modificación

Podemos definir que una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

1.3.5.5 Ataques de denegación de servicio

Consideramos que este tipo de ataque se dedica a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Se puede inutilizar dispositivos de comunicación tan sencilla como cortar un simple cable, como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

1.3.5.6 Ataques de suplantación

Podemos precisar que este ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Este tipo de ataque ha obtenido gran auge; los ***nuevos ladrones*** ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de crédito sin encontrar

respuesta; posteriormente sus tarjetas de crédito son vaciadas. Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

1.3.6 Tipos de Protección en Sistemas de Redes de Computadoras

Para protegerse de todos los ataques existen cuatro esquemas o métodos de seguridad que son:

1.3.6.1 Protección Básica

Mazzari (2006) cita qué "este esquema consiste simplemente en no poner esfuerzo en cuanto a la seguridad, y operar el sistema con políticas mínimas de seguridad que brindan actualmente los sistemas operativos existentes en una red de computadoras, lo que no es aconsejable aplicarlo" (p. 34).

1.3.6.2 Seguridad a través de ocultamiento

Según los preceptos de Mazzari indica qué:

> Este esquema establece que un sistema es seguro si nadie sabe de él, de su existencia, de su contenido y de las medidas de seguridad que posee. El problema es que cualquier red que se desee conectar a Internet tiene que tener un registro autorizado, nombre del dominio, reconocido por el ente que regula las conexiones con Internet, el cual puede ser obtenido por cualquier persona a través de un ping, finger y otros comandos que muestren información del dominio. Es decir, no hay un completo ocultamiento del sistema a proteger. Los intrusos están atentos a nuevas conexiones con la esperanza de que estos nuevos sitios no tengan medidas

de seguridad y así infiltrarse. Por ejemplo, conociendo el hardware, software y la versión del sistema operativo un intruso sabrá los posibles agujeros de seguridad y por donde iniciar un ataque.

Los intrusos pueden obtener esta información del registro del host o intentar conectarse al host. Es por esto que es recomendable ocultar el tipo de sistema operativo cuando alguien se conecta a un host. La manera en que se oculta información puede ser a través de la prohibición de uso de ciertos servicios tales como finger, ping, u otros que otorguen información a los usuarios. Por lo tanto, a largo plazo este acercamiento no es una elección muy acertada (p. 34).

1.3.6.3 Seguridad de Host

Mazzari manifiesta qué:

Este método consiste en darle seguridad por separado a cada host de la red de computadoras. Es decir aplicar todos los esfuerzos para evitar problemas de seguridad en cada host. Esto involucra desactivar servicios (rlogin, TFTP, X11 etc.), procesos del sistema operativo, accesos libres de cuentas sin contraseñas, etc. Pero existe un problema en este esquema, actualmente el ambiente de computadoras es abierto a diversas plataformas lo que hace que este modelo sea impracticable por lo complejo que se pueden tornar las configuraciones en algunas máquinas. La mayoría de ambientes incluyen máquinas de muchos distribuidores (MACHINTOSH, IBM, HP, etc.), cada una con sus propios sistemas operativos y cada una con sus propios problemas de seguridad. Aun si una red de computadoras tiene maquinas del mismo distribuidor, utilizar diferentes versiones del mismo sistema operativo conllevaría problemas de seguridad.

Este método de seguridad es muy apropiado para lugares pequeños o lugares que requieren de extrema seguridad. Sin embargo, muchas organizaciones incluyen

este tipo de métodos en sus planes de seguridad para proteger por separado a todos los hosts considerados importantes (p. 36).

1.3.6.4 Seguridad de red (Firewalls)

Mazzari cita qué "a medida que los ambientes de computadoras han ido creciendo, el asegurar cada host se ha hecho muy difícil. Debido a esto surgió el esquema de seguridad de red, este esquema consiste en controlar todos puntos de accesos a la red, a los hosts y a los servicios que ellos ofrecen mas no asegurarlos uno por uno. En este esquema intervienen ***firewalls*** como mecanismos que protegen hosts y redes internas utilizando técnicas de autenticación, listas de accesos y servicios autorizados, archivos de log y encriptación para salvaguardar los datos en tránsito dentro de las redes" (p. 37).

Según nuestras consideraciones técnicas podemos mencionar qué; Los mecanismos apropiados para que la información de una Empresa o Institución sea segura, dependen de la protección que el Administrador de red aplique a su infraestructura informática, para la protección de la integridad y totalidad de la información, sus métodos de proceso, aplicando políticas de seguridad a través de un firewalls.

1.3.7 Herramientas en Plataforma Linux para la Seguridad de la Red

Consideramos que las herramientas de seguridad de redes pueden utilizarse para revisar la seguridad de un sistema con buenas o con malas intenciones. Estas herramientas buscan equipos en la red, hacen barridos de puertos y descubrimiento de servicios, analizando los resultados para inferir la información, como versión y tipo de sistema y/o servicios, y exponer deficiencias de seguridad, entre algunas herramientas podemos mencionar las siguientes:

1.3.7.1 Uncomplicated Firewall (UFW)

Uncomplicated Firewall. (2011). Recuperado el 6 de agosto de 2012, de https://help .ubuntu.com/community/UFW

El firewall no complicada UFW es un Front End para IPTables y está especialmente bien adaptado para firewalls basados en host. UFW proporciona un marco para la gestión de Netfilter, así como una interfaz de línea de comandos para manipular el servidor de seguridad. UFW tiene como objetivo proporcionar una interfaz fácil de usar para las personas que no están familiarizados con los conceptos de servidor de seguridad, mientras que, al mismo tiempo simplifica los comandos IPTables complejas para ayudar a un administrador del que sabe lo que él o ella está haciendo.

UFW no se puede utilizar en sistemas sin soporte de IPv6 por huellas UFW espalda al intentar ejecutar ip6tables para determinar las capacidades que el sistema tiene. Sería relevante si UFW podría crear una opción NAT, que eliminaría la necesidad de editar manualmente los archivos de configuración para configurar el reenvío.

1.3.7.2 Packet Filter (PF)

Packet Filter. (2006). Recuperado el 29 de agosto de 2012, de http://althox.blogspot .com/2013/03/Antivirus-PF-Packet-Filter-Paquete-deCortafuegos-basado-en-configuracion-dinamica-stateful-rules.html

Es el filtro de paquetes o cortafuegos basado en una configuración dinámica escrito originalmente por Daniel Hartmeier actualmente desarrollado y mantenido por el equipo de desarrollo de OpenBSD. Es funcionalmente comparable a otras soluciones de filtrado de paquetes, como IPTables, IPfw e IPFilter. PF puede

utilizarse para montar dispositivos cortafuegos de gran flexibilidad, ya que incluye características de alta disponibilidad y un protocolo de redundancia para direcciones comunes, identificador de sesión, un proxy ftp y otros extras relacionados con PF.

PF presenta debilidades como, no proteger las capas superiores a nivel OSI, las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos, no son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior, sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades, no soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

1.3.7.3 Shorewall

Shorewall. (2011). Recuperado el 15 de septiembre de 2012, de http://www.alcancelibre.org/staticpages/index.php/como-shorewall-3-interfaces-red

Es una extensible herramienta de alto nivel para la configuración de muros cortafuego, solo se necesita que se proporcionen algunos datos en algunos ficheros de texto simple y éste creará las reglas de cortafuegos correspondientes a través de IPTables. Shorewall puede permitir utilizar un sistema como muro cortafuego dedicado, sistema de múltiples funciones como puerta de enlace, dispositivo de encaminamiento y servidor.

Las desventajas es que son muy simples por lo tanto es posible detectarlos, no ofrecen casi nada de información sobre ataques, diseñados para detectar ciertos comportamientos y sobre todo depende de la habilidad del administrador.

1.3.7.4 IPCop

IPCOP. (2011). Recuperado el 29 de septiembre de 2012, de www.ipcop.tk/

Es una distribución GNU/Linux para servidores dedicados a funcionar como cortafuegos aunque dispone de más funcionalidades, configurables mediante el acceso por interfaz web. El cortafuegos de IPCop está basado en IPTables, es un programa de línea de comandos usado para configurar un conjunto de reglas de filtrado de paquetes. Este programa permite añadir, modificar y eliminar reglas de la configuración de filtrado establecida. Pueden establecerse un conjunto de reglas para cada tipo de interfaz de los vistos anteriormente, puesto que cada interfaz tiene asociado un determinado nivel de confianza en función del tipo de tráfico al que están expuestas.

El filtro de direcciones permite restringir el acceso a una interfaz Azul (WiFi), autorizando únicamente la conexión de los clientes cuyas direcciones estén activadas en la lista de filtrado, siempre dependiendo de la política de acceso establecida. Si esta funcionalidad no está habilitada, tendrán acceso a la interfaz todos los clientes habilitados según la política de acceso.

GRÁFICO N° 1.2. LOGO DE IPCOP

Fuente: Tom Eichstaedt.
Disponible en Web: http://www.tom-e.de/

Como investigadores podemos señalar qué, IPCop es una opción de firewall que nos ayuda a tener nuestra red de datos protegida de amenazas e intrusos, puesto que si se

encuentra una amenaza lo expulsa automáticamente por medio del Internet, o lo registra a través de un log.

1.4 Monitoreo de Redes

1.4.1 Introducción

Altamirano (2005), expresa qué:

> La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo son actividades de gran relevancia para brindar un buen servicio a los usuarios.
>
> De esto se deriva la importancia de contar con un sistema, capaz de notificar las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico de red (p. 30).

Según el análisis de los investigadores se menciona qué, el monitoreo de redes proporciona un servicio eficiente y de calidad a cada uno de los usuarios, con esto se obtiene la oportunidad de facilitar las actividades y cubrir necesidades que están involucradas dentro de este contexto.

1.4.2 Enfoques de Monitoreo

Existen, al menos, dos puntos de vista para abordar el proceso de monitorear una red: El enfoque activo y pasivo, aunque son diferentes ambos se complementan.

1.4.2.1 Monitoreo Activo

De acuerdo a los fundamentos Altamirano indica qué:

> Este tipo de enfoque se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red, y es utilizado para medir el rendimiento en una red, a través de técnicas que se mencionan a continuación:

1.4.2.1.1 Técnicas de Monitoreo Activo

- **Basado en *ICMP***
  - Diagnosticar problemas en la red.
  - Detectar el retardo y pérdida de paquetes.
  - RTT.
  - Disponibilidad de host y redes.

- **Basado en *TCP***
  - Tasa de transferencia.
  - Diagnosticar problemas a nivel aplicación.

- **Basado en *UDP***
  - Pérdida de paquetes en un sentido (one-way).
  - RTT (traceroute) (p. 31).

En base al criterio grupal, se puede mencionar qué, si se desea que el monitoreo de una red sea lo más exacto posible se lo debe realizar por un periodo de tiempo mayor a lo normal, para poder visualizar el tráfico generado y alejarse de posibles fallas por cambios eventuales en la red y que se dan únicamente en ciertos días u horas.

1.4.2.2 Monitoreo Pasivo

Conforme a los fundamentos Altamirano indica qué:

> Este enfoque se basa en la obtención de datos a partir de la recolección y análisis del tráfico que circula por la red. Ya que se emplean diversos dispositivos como sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para SNMP, RMON Y NETFLOW. Este enfoque no agrega tráfico en la red como lo hace el activo, y es utilizado para caracterizar el tráfico en la red y para contabilizar su uso. A continuación se detalla las técnicas que prevé el monitoreo pasivo:

1.4.2.2.1 Técnicas de Monitoreo Pasivo

- **Solicitudes remotas**

Mediante SNMP

- Se utiliza para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, al mismo tiempo genera paquetes traps que indican que un evento inusual se ha producido.

Otros métodos de acceso

- La realización de scripts que tengan acceso a dispositivos remotos para obtener información importante. En esta técnica se pueden emplear módulos de PERL, SSH con autenticación de llave pública, etc.

Captura de tráfico

Dos formas:

- Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura.

- Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red (p. 33).

- **Análisis de tráfico**

Análisis de tráfico. (2011). Recuperado el 10 de octubre de 2012, de http://www. monografias.com/trabajos95/recursos-red-y-su-monitoreo/recursos-red-y-su-monitoreo.shtml

El análisis de tráfico es usado para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos de prueba que envíen información mediante un estándar que define objetos actuales e históricos de control o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

El análisis de tráfico está muy relacionado con el análisis de paquetes y se suelen usar de forma conjunta. En el análisis de paquetes se estudia la información contenida en los paquetes que circulan por la red y a partir de eso trata de inferir información.

- **Flujo**

Flujo. (2011). Recuperado el 10 de noviembre de 2012, de http://www.monografias .com/trabajos95/recursos-red-y-su-monitoreo/recursos-red-y-su-monitoreo.shtm

Es usado para identificar el tipo de tráfico que existe en la red, un flujo es un conjunto de paquetes con: la misma IP origen/destino, el mismo puerto TCP origen/destino y el mismo tipo de aplicación. Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos capaces de capturar tráfico y transformarlo en flujos, también es usado para tareas de facturación (billing).

1.4.3 Estrategia de monitoreo

Altamirano (2005) indica qué:

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear así como las herramientas que se utilizarán para esta tarea y se detallaran más adelante:

1.4.3.1 Aspectos a monitorear

Uso de ancho de banda, consumo de CPU, de memoria, estado Físico de las conexiones, tipo de tráfico, alarmas, servicios (Web, correo, base de datos), alcance de dispositivos a monitorear:

- Dispositivos de Interconexión: ruteadores, switches, hubs, firewall.
- Servidores: Web, Mail, DB.
- Red de Administración: monitoreo, Logs, Configuración (p. 35).

1.4.3.1.1 Monitorear el rendimiento del sistema.

Según Red Hat, Inc. (2005), menciona qué:

> La revisión de los sistemas a menudo incluye su vigilancia, lo que se denomina medición del desempeño de monitoreo de la red. Los productos para el desempeño de sistemas se han desarrollado para medir todos los componentes de un sistema de información computarizado, lo que abarca el hardware, software, bases de datos, telecomunicaciones y redes. Cuando se usan en forma correcta, estos productos permiten localizar de manera rápida y eficaz problemas reales o potenciales de la red.
>
> El monitorizar el rendimiento del sistema se hace normalmente en respuesta a problemas de rendimiento. Bien sea que el sistema está corriendo muy lentamente, o los programas fallan en ejecutarse. En cualquiera de estos casos, la supervisión del rendimiento del sistema se realiza normalmente como el primer y el último paso de un proceso de tres pasos:
>
> - Monitorizar para identificar la naturaleza y ámbito de la escasez de recursos que están causando los problemas de rendimiento.
>
> - Se analizan los datos producidos a partir de la supervisión y se toma un curso de acción normalmente optimización del rendimiento o la adquisición de hardware adicional.
>
> - Monitorizar para asegurarse de que se ha solucionado el problema de rendimiento (p. 15).

1.4.3.1.2 Monitorear la capacidad del sistema

De acuerdo a Red Hat, Inc. expresa qué:

> La supervisión de la capacidad del sistema se hace como parte de un programa continúo de planificación. La planificación de capacidad utiliza el monitoreo a largo plazo de los recursos del sistema para determinar las tasas de cambio en la utilización de los recursos del sistema. Una vez que se conocen estas tasas de cambio, se hace posible conducir una planificación a largo plazo más exacta con respecto a la adquisición de recursos adicionales.
>
> La planificación de capacidades requiere un punto de vista a corto plazo o el uso incorrecto de recursos es de poco interés. En vez de esto, se recopilan los datos sobre un período de tiempo, haciendo posible categorizar la utilización de recursos en términos de los cambios en la carga de trabajo. En ambientes definidos de forma más limitada donde solamente corre una aplicación, es posible modelar el impacto de la aplicación en los recursos del sistema. Esto se puede hacer con suficiente exactitud para determinar, por ejemplo, el impacto de cinco representantes de servicio al cliente ejecutando la aplicación de servicio al cliente durante la hora pico del día (p. 16).

1.4.3.1.3 Monitorizar el ancho de banda

Red Hat, Inc. cita lo siguiente:

> Es más complicado que la supervisión de otros recursos, la razón de esto se debe al hecho de que las estadísticas de rendimiento tienden a estar basadas en dispositivos, mientras que la mayoría de los lugares en los que es importante el ancho de banda tienden a ser los buses que conectan dispositivos. En los casos donde más de un dispositivo comparte un bus común, puede encontrar estadísticas

razonables para cada dispositivo, pero la carga que esos dispositivos colocan en el bus es mucho mayor.

Otro reto al monitorizar el ancho de banda es que pueden existir circunstancias donde las estadísticas para los dispositivos mismos no estén disponibles. Sin embargo, aun cuando no siempre tendrá disponibles estadísticas relacionadas al ancho de banda 100% exactas, a menudo se encuentra información suficiente para hacer posible cierto nivel de análisis, particularmente cuando se toman en cuenta estadísticas relacionadas.

Algunas de las estadísticas más comunes relacionadas al ancho de banda son:

- ***Bytes recibidos/enviados:*** Las estadísticas de la interfaz de red proporcionan un indicativo de la utilización del ancho de banda de uno de los buses más visibles la red.

- ***Cuentas y tasas de interfaz:*** Estas estadísticas relacionadas a la red dan indicaciones de colisiones excesivas, errores de transmisión/recepción y más. Con el uso de estas estadísticas (particularmente si las estadísticas están disponibles para más de un sistema en su red), es posible realizar un fragmento de resolución de problemas de la red antes de utilizar las herramientas de diagnóstico de la red más comunes.

- ***Transferencias por segundo:*** Normalmente reunida por dispositivos de E/S en bloques, tales como discos y unidades de cinta de alto rendimiento, esta estadística es una buena forma de determinar si se está alcanzando el límite del ancho de banda de un dispositivo particular. Debido a su naturaleza electromecánica, las unidades de disco y de cinta solamente pueden realizar ciertas operaciones de E/S cada segundo; su rendimiento se ve afectado rápidamente a medida que se alcanza a este límite (p. 20).

1.4.3.1.4 Monitorizar la memoria

Red Hat, Inc. menciona qué:

Esta área es donde se puede encontrar gran cantidad de estadísticas de rendimiento, y la utilización de la memoria. Debido a la complejidad inherente de los sistemas operativos con memoria virtual bajo demanda hoy en día, las estadísticas de utilización de memoria son muchas y variadas. Es aquí donde tiene lugar la mayoría del trabajo de un administrador de sistemas con la administración de recursos. Las estadísticas de administración de memoria encontradas más a menudo, son:

- ***Páginas dentro/fuera.-*** Estas estadísticas hacen posible medir el flujo de páginas desde la memoria del sistema a los dispositivos de almacenamiento masivo. Altas tasas de estas estadísticas pueden representar que el sistema está corto de memoria física o está consumiendo más recursos del sistema en mover las páginas dentro y fuera de memoria que en ejecutar aplicaciones.

- ***Páginas activas/inactivas.-*** Estas estadísticas muestran qué tanto se están utilizando las páginas residentes en memoria. Una falta de páginas inactivas puede estar apuntando hacia una escasez de memoria física.

- ***Páginas libres, compartidas, en memoria intermedia o en caché.-*** Estas estadísticas proporcionan detalles adicionales sobre las estadísticas más simples de páginas activas/inactivas. Usando estas estadísticas es posible determinar la mezcla general de utilización de memoria.

- ***Intercambio dentro/fuera.***- Estas estadísticas muestran el comportamiento general de la memoria de intercambio del sistema. Tasas excesivas pueden

estar apuntando a una escasez de memoria física. La supervisión exitosa de la utilización de la memoria requiere una buena comprensión de cómo funciona la memoria virtual bajo demanda de un sistema operativo (p. 25).

1.4.3.1.5 Monitorizar el almacenamiento

Conforme a Red Hat, Inc. cita qué:

> El monitoreo del almacenamiento normalmente tiene lugar en dos niveles diferentes: monitorizar insuficiente espacio en disco y monitorizar problemas de rendimiento relacionados con el almacenamiento. La razón de esto es que es posible tener problemas calamitosos en un área y ningún problema en otra. Por ejemplo, es posible causar que a la unidad de disco se le acabe el espacio sin causar ningún tipo de problemas relacionados al rendimiento.
>
> De la misma manera, es posible tener una unidad de disco que tiene 99% de espacio libre, pero que se ha puesto más allá de sus límites en términos de rendimiento. Las estadísticas siguientes son útiles para supervisar el almacenamiento:
>
> - ***Espacio libre:*** Es probablemente el recurso que todos los administradores de sistemas vigilan más de cerca; sería raro el administrador que no verifica el espacio.
>
> - ***Estadísticas relacionadas al sistema de archivos:*** Estas estadísticas tales como el número de archivos/directorios, tamaño promedio de los archivos, etc., suministran detalles adicionales sobre un porcentaje de espacio libre. Como tal, estas estadísticas hacen posible para los administradores de sistemas configurar el sistema para que entregue el mejor rendimiento, pues la carga de E/S impuesta por un sistema de archivos lleno de muchos

pequeños archivos no es la misma que la carga impuesta por un sistema de archivos lleno con un único archivo enorme.

- ***Transferencias por segundo:*** Esta estadística es una buena forma de determinar si se están alcanzando las limitaciones de ancho de banda de un dispositivo en particular.

- ***Lecturas/escrituras por segundo:*** Con un desglose más detallado de las transferencias por segundo, estas estadísticas permiten al administrador de sistemas entender mejor la naturaleza de las cargas de E/S que está experimentando un dispositivo de almacenamiento. Esto puede ser crítico, ya que algunas tecnologías de almacenamiento tienen características de funcionamiento muy diferentes para operaciones de lecturas contra escrituras.

1.4.3.1.6 Monitoreo de la red

Monitoreo de la red. (2008). Recuperado el 10 de noviembre de 2012, de https:// seguinfo.wordpress.com/category/networking/page/15/

El uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla vía correo electrónico, beeper u otras alarmas. Los aplicativos de monitoreo del estado de red permiten, entre varias cosas:

- ***Revisar los signos vitales de la red en tiempo real.-*** Mientras un sistema de detección de intrusos monitorea una red de amenazas del exterior, un sistema de monitoreo de red monitorea la red de problemas debidos a servidores, conexiones de red u otros dispositivos sobrecargados y/o fuera de servicio.

Para determinar el estado de un servidor Web, un software de monitoreo puede periódicamente mandar una solicitud vía http para mandar a llamar una página; para servidores de correo electrónico, un mensaje de prueba puede ser mandada por SMTP y retomada por IMAP.

1.4.3.1.7 Monitoreo de servidores

Monitoreo de servidores. (2009). Recuperado el 10 de noviembre de 2012, de http://www.cabai.com.ar/2009/03/monitoreo-de-servidores-server-monitoring.html

> El monitoreo de servidores o de los sitios web es un tema muy importante ya que hoy en día existen compañías que brindan dicho servicio para poder conocer el ***uptime*** de nuestras aplicaciones y conocer cuando hay una baja de servicio. Varios pueden crear aplicaciones web pero no están sobre el servidor revisando si está funcionando todo el tiempo y es ahí cuando recurrimos a un servicio de monitoreo online que nos avise cuando está caído.
>
> Porque si nuestra aplicación web está caída significa que estamos perdiendo dinero así que cualquier inversión que hagamos para mantenerla ejecutando o bien avisarnos cuando no lo está, para tomar medidas rápidamente y volver a ejecutar el servicio.

Según el criterio de los investigadores se menciona qué, es de vital importancia monitorear el rendimiento del CPU, el ancho de banda, la utilización de memoria, y el espacio de almacenamiento, estos recursos tienen un impacto directo en el rendimiento del sistema y, por lo tanto, en la productividad y satisfacción de sus usuarios.

1.4.3.2 Métricas

Altamirano (2005), define qué:

> Las métricas permiten establecer patrones de comportamiento para los dispositivos a monitorear. Existen diversos tipos de métricas que dependerán de las necesidades de la red, y estas deben ser congruentes con los objetos a monitorear.
>
> - Métricas de tráfico de entrada y salida.
> - Métricas de utilización de procesador y memoria.
> - Métrica de estado de las interfaces.
> - Métrica de conexiones lógicas.
>
> A cada métrica se le asigna un valor promedio, el cual identifica su patrón de comportamiento (p. 30).

1.4.3.3 Alarmas

Según los fundamentos de Altamirano menciona qué:

> Las alarmas son eventos con comportamiento inusual, las más comunes reportan cuando el estado operacional cambia. Existen otros tipos de alarmas basado en patrones previamente definidos en nuestras métricas, son valores máximos conocidos como umbrales.
>
> Cuando estos patrones son superados se produce una alarma, ya que es considerado como un comportamiento fuera del patrón, algunos tipos de alarmas son: procesamiento, conectividad, ambientales, utilización y disponibilidad (p. 32).

1.4.3.4 Ventajas del monitoreo de la red

- El monitoreo de la red puede indicar la presencia de troyanos o virus, ya que pueden inducir trafico excesivo y ser una brecha de seguridad.

- Se puede ver si la velocidad hacia o desde el internet se está aprovechando, si es la suficiente, si se necesite subir el ancho de banda.

- Se puede poner un ***decoy*** para engañar a los hackers y hacerles creer que están conectados y realmente estás viendo que ***desean*** para bloquearlos o reportarlos a las entidades legales, etc.

- Se puede ver si ciertos usuarios tienen malos hábitos de navegación como paginas eróticas, de seguridad, hackers.

- Se puede hacer bitácoras de trafico de red para ver si cuando insertas una nueva tecnología o servicio el tráfico de la red sube o baja, es decir si es más optimizado o ahora el diseño es más pobre o tiene impacto.

Conforme lo investigado consideramos qué, monitorear una red es una ventaja y una tarea para un administrador, ya que permite saber si el hardware necesita ser suplantado por otro mejor y saber si la utilización de la red no está siendo abusada por parte de los usuarios, evitando accesos no debidos, descargas no autorizadas desde páginas desconfiables, etc.

1.4.4 Herramientas en plataforma Linux para el monitoreo de la red

Luego de un análisis y basándonos de criterios de varios autores podemos mencionar qué, una herramienta de monitoreo de redes es fundamental para asegurar el funcionamiento de los sistemas informáticos y para evitar fallos en la red. La monitorización de redes también nos ayuda a optimizar la red, ya que nos facilita información detallada sobre el uso de los equipos conectados a la red y otros servicios compartidos.

1.4.4.1 Pandora FMS

Pandora FMS. (2009). Recuperado el 30 de noviembre de 2012, de http://www.sd3 .es/area_pandorafms.aspx

Es un software de código abierto que sirve para monitorizar y medir todo tipo de elementos. Monitoriza sistemas, aplicaciones o dispositivos. Permite saber el estado de cada elemento de un sistema a lo largo del tiempo. Puede detectar si una interfaz de red se ha caído, un ataque de ***defacement*** en una web, una pérdida de memoria en algún servidor de aplicaciones, o el movimiento de un valor del NASDAQ.

Pandora FMS también puede monitorizar cualquier tipo de servicio TCP/IP, sin necesidad de instalar agentes, y monitorizar sistemas de red como balanceadores de carga, routers, switches, sistemas operativos, aplicaciones o impresoras si se necesita hacerlo de forma remota. Una de las complicaciones que muestra es que no hay acceso directo desde el PC del operador al servidor que queremos monitorizar y no podemos instalar software de control remoto en el sistema remoto.

1.4.4.2 Zenoss (Zenoss Core)

Zenoss. (2009), Recuperado el 19 de diciembre de 2012, de http://es.scribd.com/doc/89998802/Zenoss-Core

Es una aplicación de informática de código abierto, plataforma para la gestión de red y servidores basada en el servidor de aplicaciones Zope. Liberado bajo la Licencia Pública General de GNU, Zenoss Core provee una interfaz web que permite a los administradores de sistemas monitorear disponibilidad, inventario/configuración, desempeño y eventos.

Zenoss Core combina programación propia y de varios proyectos de código abierto con el fin de integrar el almacenamiento de datos y los procesos para su recolección en una interfaz de usuario orientada a la web, permite manejar eventos provenientes de los equipos monitoreados y generar notificaciones de alertas según lo configure el administrador. Una desventaja, es que el sistema de notificación es algo pobre y algo extraño de configurar. Sirve para recolectar datos estadísticos, no como herramienta de alerta.

1.4.4.3 Hyperic HQ

Hyperic HQ. (2010). Recuperado el 12 de diciembre de 2012, de http://es.scribd.com/doc/42886120/Uso-de-Software-Libre-en-El-Estado

Es una potente herramienta Open Source para monitorear cualquier tipo de aplicación y sistema. Es capaz de administrar aplicaciones locales y aplicaciones web que pueden estar ubicadas en centros de datos o entornos virtuales. Este sistema automáticamente descubre, monitorea y administra software y recursos de red, sin importar el tipo de ubicación. Además proporciona una visión transparente de rendimiento y disponibilidad para compañías que ejecuten sus aplicaciones en

cualquiera de las plataformas comunes, trabaja correctamente en múltiples plataformas como Unix, Linux, Windows, Solaris, AIX, HPUX, VMware, y Amazon Web Services. Pero una gran desventaja de Hyperic HQ es que no es perfecto, ni es para todas las situaciones y configuraciones, ya que recibe la información sin autenticación y en un texto plano sobre la red. Si hay información sensible o confidencial, no es adecuado hacer un monitoreo periódico, cada cinco minutos.

1.4.4.4 Nagios

Nagios. (2006). Recuperado el 21 de diciembre de 2012, de http://es.scribd.com/doc /81329577/Untitled-1

Es un software libre para la monitorización de equipos y servicios de red, está desarrollado en lenguaje C, lo cual asegura portabilidad y una rápida ejecución de la información procesada. Al ser un software gratuito y de libre distribución, permite que el usuario pueda disponer siempre de nuevas actualizaciones y de contar con el soporte de una gran comunidad de desarrolladores, e incluso tener acceso al código fuente para modificarlo y adaptarlo a nuestras necesidades.

Nagios permite al administrador de la red, realizar un monitoreo exhaustivo y tener control total de la misma, determinado los problemas que se presentan en ella antes de que estos sean percibidos por los usuarios de la red, para de esta manera tomar la iniciativa y dar las soluciones más idóneas en base al análisis e interpretación de la información proporcionada por Nagios.

Nagios basa su funcionamiento en distintos archivos de configuración en los cuales se especifica los elementos de red que van a ser monitoreados, con qué frecuencia se lo va a realizar, a quién y de qué manera se van a enviar los resultados de la monitorización, para lo cual cuenta con una gran cantidad de

plugins o script desarrollados en distintos lenguajes de programación y que son los encargados de realizar el monitoreo y recopilar la información de acuerdo a lo especificado en dichos archivos. Esta herramienta dispone de una interfaz web en la cual se puede visualizar de una manera rápida y sencilla el estado de los dispositivos o servicios que se están monitoreando, además proporciona distintas opciones para la generación de reportes en base a la información recolectada.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix. Nagios es muy utilizado en entornos como granjas de servidores o empresas que cuentan con equipos en grandes instalaciones, teniendo un funcionamiento muy optimo mediante la obtención, interpretación y decisión de eventos.

GRÁFICO N° 1.3 LOGO DEL PROYECTO NAGIOS

Fuente: Ethan Galstad, Proyecto Nagios
Disponible en Web: http://www.nagios.org/

1.5 Protocolo Simple de Administración de Red (SNMP)

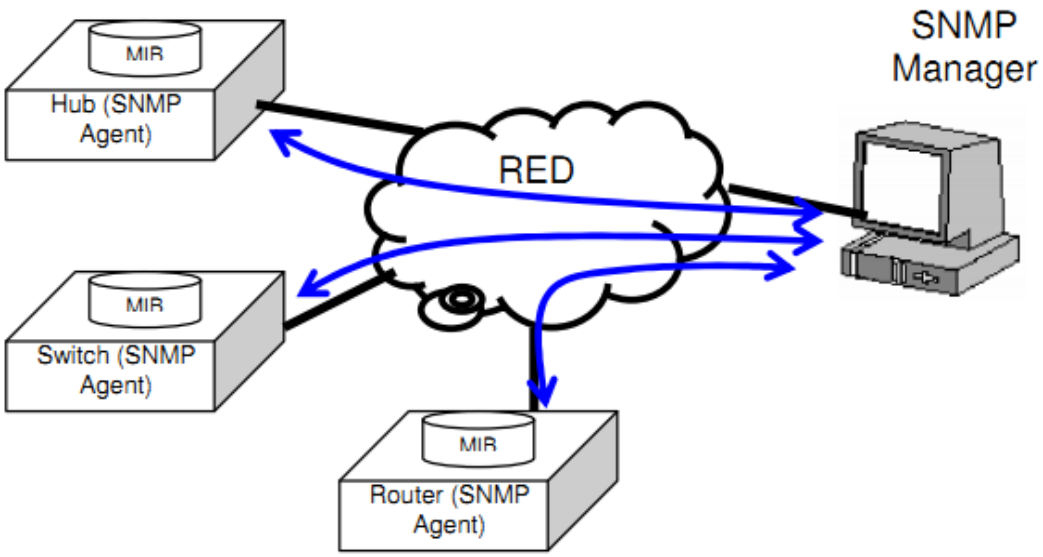
Joskowicz (2008), expresa qué:

SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de la red, permitiendo a los administradores supervisar el funcionamiento de la red, buscando y resolviendo sus problemas y planeando su crecimiento, contiene dos componentes:

- ***SNMP Manager:*** Es una aplicación de software desde la que se realiza la administración, en forma centralizada, de la red.

- ***SNMP Agent:*** Residen en los diversos dispositivos de la red (hubs, switches, routers, etc.) y generan información estadística acerca de sus funciones y recursos.

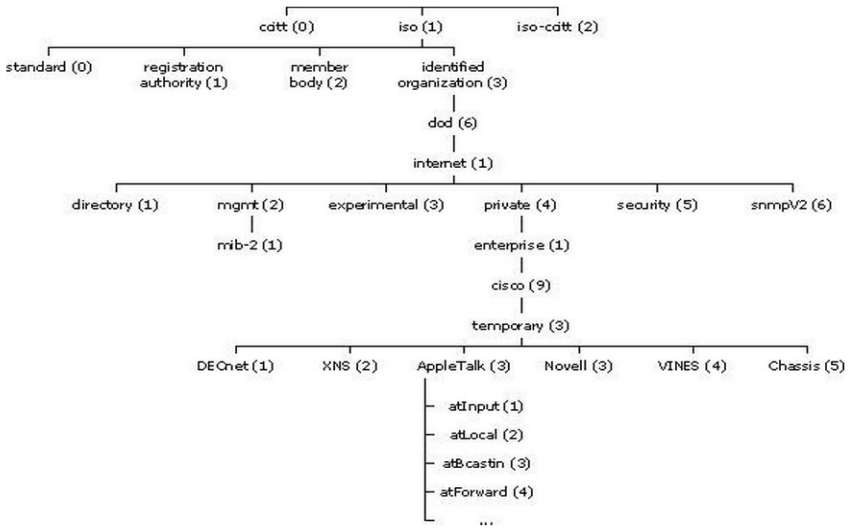
GRÁFICO N° 1.4 SNMP



Fuente: JOSKOWICZ, José. *SNMP*. En: "*Redes de Datos*". 5ta Ed. Universidad de la República Montevideo, Uruguay. Edit. 2008. Pág. 79.
Realizado por: JOSKOWICZ, José.

Y esta información es almacenada en una base de datos local, llamada MIB (Management Information Base). A su vez, los ***Agentes SNMP*** pueden recibir y enviar información desde y hacia el ***Administrador SNMP***, utilizando el protocolo UDP.

GRÁFICO N° 1.5 BASE DE INFORMACIÓN DE ADMINISTRACIÓN

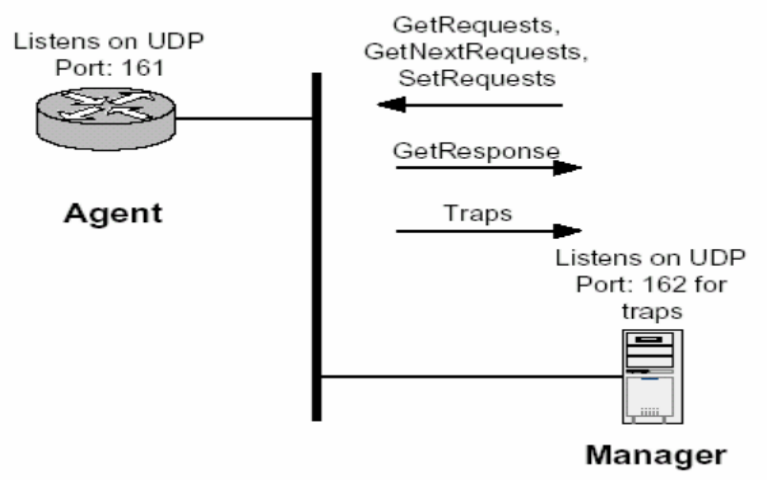


Fuente: JOSKOWICZ, José. *Base de información de administración SNMP (MIB)*. En: "*Redes de Datos"*. 5ta Ed. Universidad de la República Montevideo, Uruguay. Edit. 2008. Pág. 81.
Realizado por: JOSKOWICZ, José.

La información almacenada en MIB está organizada en forma jerárquica, cada elemento de información es una variable que almacena alguna característica o alguna información estadística del dispositivo administrado. Estos objetos MIB pueden ser escalares es decir, contener un único valor, o tabulares es decir, contener varios valores. La estructura jerárquica de la MIB es en forma de ***árbol***, como se muestra en la figura. Cada objeto MIB está unívocamente identificado dentro de la jerarquía de la MIB, ya sea en una notación textual o numérica, indicando los diferentes nombres o números por los que se debe recorrer el árbol hasta llegar al objeto en cuestión. El SNMP manager usa comandos simples, entre los cuales se destacan:

- ***Read:*** Es usado por el Manager para leer las variables del Agente.
- ***Write:*** Es usado para configurar el equipo administrado. El Manager puede escribir ciertas variables de configuración del Agente.
- ***Trap:*** Es utilizada en forma asíncrona por los agentes, para reportar eventos.

GRÁFICO N° 1.6 SNMP MANAGER



Fuente: JOSKOWICZ, José. *SNMP Manager.* En: "*Redes de Datos"*. 5ta Ed. Universidad de la República Montevideo, Uruguay. Edit. 2008. Pág. 81.
Realizado por: JOSKOWICZ, José.

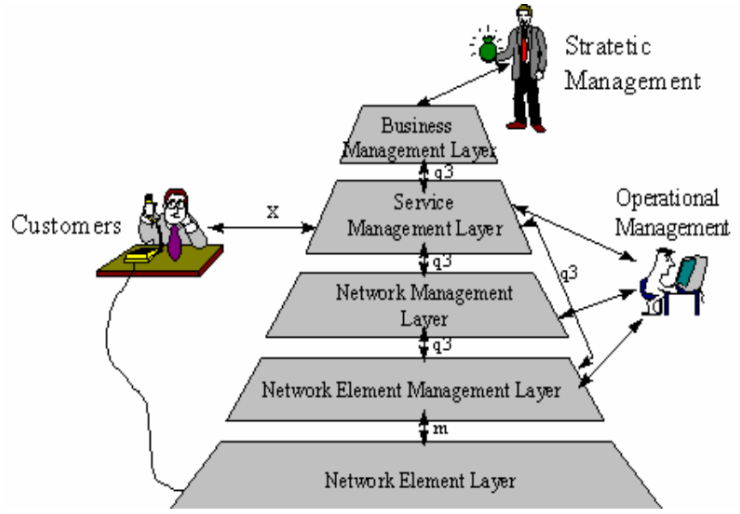
El Protocolo de Simple Administración de Red, es un protocolo de la capa de aplicación que proporciona el intercambio de información de administración entre dispositivos de red, permite a los administradores inspeccionar el desempeño de la red, buscando resolver sus problemas, y planear su crecimiento (p. 81).

1.6 Administración de Redes

1.6.1 Funciones en la Administración de Redes Según ITU-T

Las funciones se organizan en una estructura jerárquica de niveles que cubren todos los aspectos de gestión y clasifica las funciones que se deben realizar en cada nivel según criterios de responsabilidad.

GRÁFICO N° 1.7 ADMINISTRACIÓN DE REDES SEGÚN ITU-T



Fuente: JOSKOWICZ, José. *Funciones a Considerar en la Administración de Redes Según ITU-T.* En: "Redes de Datos". 5ta Ed. Universidad de la República Montevideo, Uruguay. Edit. 2008. Pág. 78.
Realizado por: JOSKOWICZ, José.

1.6.1.1 Gestión de Negocio (Bussines Management)

Según los fundamentos de Joskowicz (2008) menciona qué:

> El nivel superior es el nivel de gestión de negocio que incluye los aspectos relacionados con las estrategias de negocio; en él se definen las acciones para conseguir el retorno de la inversión, aumentar la satisfacción de los accionistas de la compañía y de los empleados, etc. Es decir, la gestión del servicio debe estar alineada con la estrategia de negocio definida en la corporación (p. 78).

1.6.1.2 Gestión de Servicio (Service Management)

Conforme a los conceptos de Joskowicz (2008) cita qué:

> En la capa de gestión del nivel de servicio se decide cómo gestionar los servicios que se van a prestar en la red. En este nivel se incluyen todos los aspectos

relacionados con la atención a los usuarios y operación de los servicios, y se realiza la gestión de las peticiones de servicio, la calidad del servicio, la gestión de problemas, la facturación, etc. (p. 78).

1.6.1.3 Gestión de Red (Network Management)

De acuerdo a los criterios de Joskowicz indica qué:

> Los servicios están soportados sobre las redes de telecomunicaciones, el nivel de gestión de red es responsable del transporte de la información entre dos extremos y de asegurar que ésta se realiza de forma correcta. Cualquier error que se detecte en este nivel y que afecte a los servicios que se prestan a los usuarios debe ser notificado hacia el nivel de gestión de servicio (p. 79).

1.6.1.4 Gestión de Elementos de Red (Network Element Management)

En base a los fundamentos de Joskowicz expone qué "el nivel de gestión de elemento de red se encarga de todos los aspectos relacionados con la infraestructura, considerados como elementos aislados. Cualquier error que se produzca en un equipo que pueda afectar al transporte de la información debe ser notificado hacia el nivel de gestión de red" (p. 79).

Como investigadores podemos manifestar qué, la administración de redes contiene las tareas de diseño, integración y coordinación de los equipos de hardware, los programas de software y los recursos humanos necesarios para monitorear, testear, configurar, analizar, evaluar y controlar la red y sus recursos a los efectos de lograr la calidad de servicio requerida.

CAPITULO II

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

2.1. Entorno de la Universidad Técnica de Cotopaxi

2.1.1. Antecedentes Históricos

En Cotopaxi el anhelado sueño de tener una institución de Educación Superior se alcanza el 24 de enero de 1995. Las fuerzas vivas de la provincia lo hacen posible, después de innumerables gestiones y teniendo como antecedente la Extensión que creó la Universidad Técnica del Norte.

El local de la UNE-C fue la primera morada administrativa; luego las instalaciones del Colegio Luis Fernando Ruiz que acogió a los entusiastas universitarios; posteriormente el Instituto Agropecuario Simón Rodríguez, fue el escenario de las actividades académicas: para finalmente instalarnos en casa propia, merced a la adecuación de un edificio a medio construir que estaba destinado a ser Centro de Rehabilitación Social. En la actualidad son cinco hectáreas las que forman el campus universitario y 82 las del Centro de Experimentación, Investigación y Producción Salache.

Hemos definido con claridad la postura institucional ante los dilemas internacionales y locales; somos una entidad que por principio defiende la autodeterminación de los pueblos, respetuosos de la equidad de género.

Nos declaramos antiimperialistas porque rechazamos frontalmente la agresión globalizadora de corte neoliberal que privilegia la acción fracasada economía de libre mercado, que impulsa una propuesta de un modelo basado en la gestión privada, o trata de matizar reformas a la gestión pública, de modo que adopte un estilo de gestión empresarial.

En estos 18 años de vida institucional la madurez ha logrado ese crisol emancipador y de lucha en bien de la colectividad, en especial de la más apartada y urgida en atender sus necesidades. El nuevo reto institucional cuenta con el compromiso constante de sus autoridades hacia la calidad y excelencia educativa.

2.1.2. Filosofía Institucional

2.1.2.1. Propósito

Poseer profesionales con un perfil que respondan a la realidad social, económica, política, cultural, científica y tecnológica de nuestro país; capaz de proyectar sus experiencias en beneficio nacional; diestro en la utilización de herramientas informáticas; diseña, opera, evalúa proyectos y procesos de desarrollo informático, redes de computadoras; es un eficiente administrador informático, capacitado para resolver grandes avances tecnológicos y ponerlos a disposición de la colectividad.

La aceptación nos indica fundamentalmente que nuestra Universidad está cumpliendo un papel protagónico y el encargado social para lo que fue creada,

esto es entregar profesionales sólidamente preparados dentro del plano científico, técnico y humanístico, encaminados a determinar y solucionar los problemas de diferente índole de la sociedad.

Formar profesionales creativos, críticos y humanistas que utilizan el conocimiento Científico – Técnico, mediante la promoción y ejecución de actividades de investigación y aplicaciones tecnológicas para contribuir en la solución de los problemas de la sociedad.

Promover proyectos de investigación para generar ciencia y tecnología, orientados a solucionar los problemas y satisfacer las necesidades del país.

2.1.2.2. Misión

La Universidad Técnica de Cotopaxi, es pionera en desarrollar una educación para la emancipación; forma profesionales humanistas y de calidad; con elevado nivel académico, científico y tecnológico; sobre la base de principios de solidaridad, justicia, equidad y libertad, genera y difunde el conocimiento, la ciencia, el arte y la cultura a través de la investigación científica; y se vincula con la sociedad para contribuir a la transformación Social – Económica del país.

2.1.2.3. Visión

En el año 2015 seremos una universidad acreditada y líder a nivel nacional en la formación integral de profesionales críticos, solidarios y comprometidos en el cambio social; en la ejecución de proyectos de investigación que aporten a la solución de los problemas de la región y del país, en un marco de alianzas estratégicas nacionales e internacionales; dotada de infraestructura física y tecnología moderna, de una planta docente y administrativa de excelencia; que

mediante un sistema integral de gestión le permite garantizar la calidad de sus proyectos y alcanzar reconocimiento social.

2.1.2.4. Análisis de la Infraestructura de la Red de la Universidad Técnica de Cotopaxi

Actualmente la Universidad Técnica de Cotopaxi cuenta con una infraestructura tecnológica de punta la misma que posee una red de tipo LAN, la cual se encuentra distribuida en VLAN, las mismas que tienen limitaciones tanto para los estudiantes, docentes y administrativos.

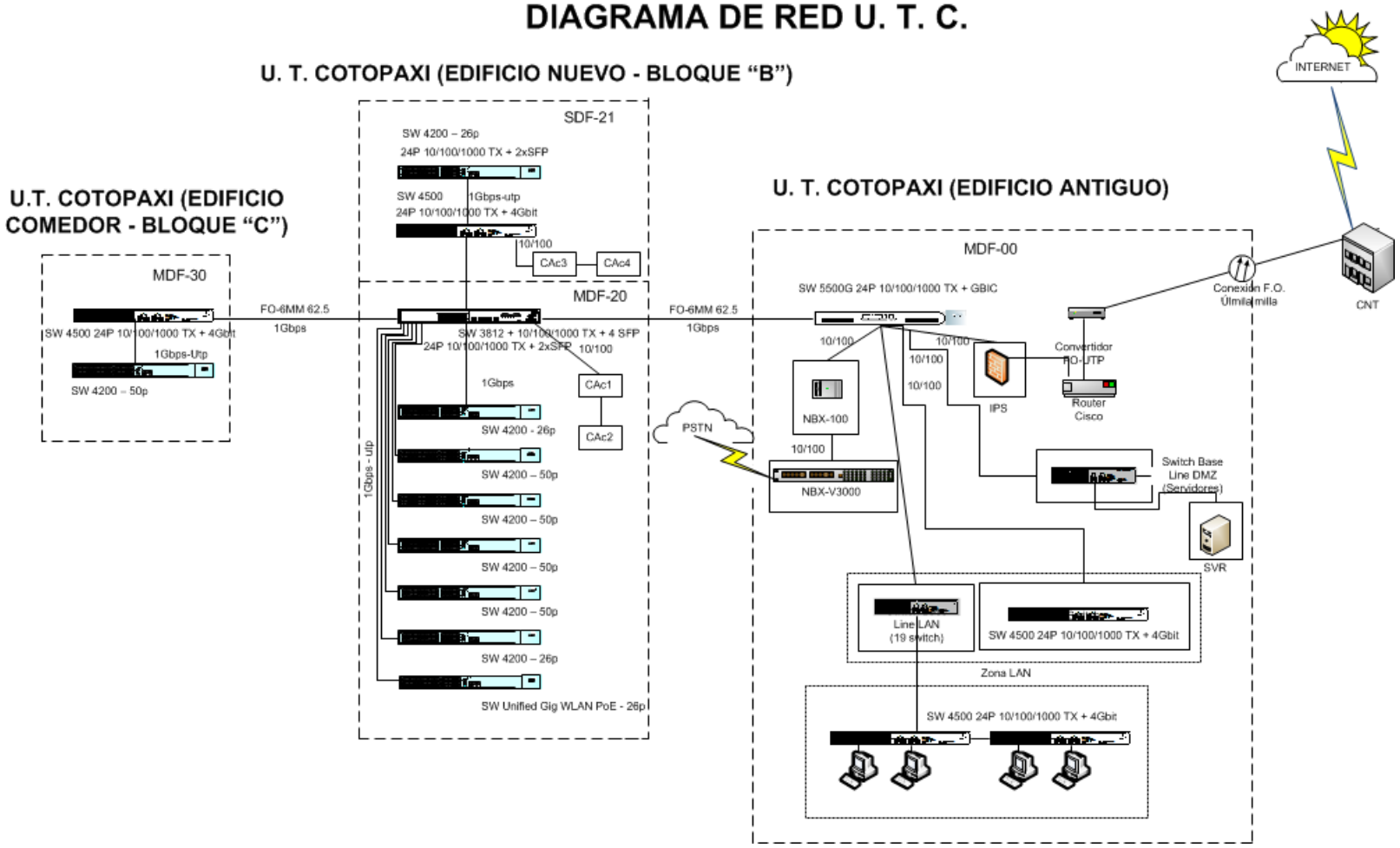
Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios). Las redes LAN se pueden conectar entre ellas a través de líneas telefónicas y ondas de radio. Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación de trabajo puede comunicarse con el resto de equipos informáticos. Suelen emplear tecnología de difusión mediante cable sencillo (coaxial o UTP) al que están conectadas las maquinas, conteniendo una velocidad de transmisión entre 10 y 100 Mbps.

La administración, control y monitoreo de toda la red de la Universidad Técnica de Cotopaxi está a cargo del Departamento de Servicios Informáticos (DSI), su oficina se encuentra en el Bloque "A" del edificio central del sector de San Felipe.

2.1.2.4.1. Diagrama de la red LAN de la Universidad Técnica de Cotopaxi

A continuación se describe en forma general la red LAN existente:

GRÁFICO N° 2.1. DIAGRAMA DE LA RED LAN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI



Fuente: Departamento de Servicios Informáticos
Realizado por: El Departamento de Servicios Informáticos

2.1.2.4.2 Amenazas y Vulnerabilidades que en la Actualidad Presenta la Red Informática de la Universidad Técnica de Cotopaxi

A continuación se detalla las amenazas y vulnerabilidades que en la actualidad presenta la red informática de la Universidad:

TABLA N° 2.1. AMENAZAS Y VULNERABILIDADES

AMENAZAS Y VULNERABILIDADAS	RECOMENDACIONES
En el ciberespacio existen hackers o piratas informáticos que pueden ingresar a los servidores y por ende sustraer cualquier tipo de información, además de causar daños a los equipos informáticos.	Implementar un mecanismo de seguridad para evitar el ingreso de los hackers a los servidores.
Cuando se trabaja con Internet la información puede venir infectada con algún virus informático, que puede ingresar al servidor ocasionando daños en el sistema operativo y por ende dejando fuera de servicio.	Se puede instalar un antivirus actual en el servidor para así evitar el ingreso de virus informático.
La página Web de la Universidad Técnica de Cotopaxi puede ser alterada por los Hackers.	Implementar un nuevo firewall para proteger la red de datos de los ataques externos.
En la Universidad no existe un firewall tipo software que evite el ataque de virus y hackers a los servidores y equipos informáticos.	Implementar un firewall tipo hardware y software para evitar ataques que pueden ser causados por los Virus informáticos y los hackers.
En caso de instalar un software sin su respectiva licencia la compañía de Microsoft, puede realizar auditorías y los equipos que no cumplan con sus respectivas licencias serán retirados excluidas de la red.	Poseer un control de los programas que se encuentran instalados en los computadores de la institución. (Software de Auditoria)

La Universidad no cuenta con un mecanismo de seguridad para proteger a los servidores de los ataques internos y externos.	Crear y establecer un reglamento interno de seguridad para los operadores y ayudantes del Departamento de Servicios Informáticos.
La institución no posee con un sistema de seguridad apropiado, ya que no cuenta con un presupuesto establecido para la adquisición de nuevos equipos para la seguridad de la red.	Diseñar una propuesta de seguridad y monitoreo de la red para la institución.
Las autoridades no reservan un presupuesto para la seguridad informática.	La institución debe asignar un presupuesto para la adquisición de equipos relacionados con la seguridad informática.
La Universidad Técnica de Cotopaxi no cuenta con un cuarto de equipos donde se concentren todos los equipos informáticos para una correcta administración y funcionamiento de la red de datos.	Crear un cuarto de equipos informáticos a los cuales se ingrese, solo el personal responsable de la red de datos.
Existe un dispositivo ***switch*** que protege en parte a los servidores.	Adquirir un firewall que proteja al 100% a los servidores en forma externa e interna.
El servidor de Linux posee un Proxy, el mismo que funciona como firewall pero no cubre en su totalidad la seguridad externa.	Mejorar las reglas de seguridad a través de los IPTables propios de Linux que activa y desactiva direcciones IP de acuerdo a la administración de la red.
La información de los "mails" que viajan por el Internet no es tan confiable desde el origen hacia el destino.	Crear un método de criptografía para proteger los datos dentro de la red, para que de esta manera no puedan ser descifradas por los hackers.
La falta de contraseñas, o el uso de contraseñas fáciles de descifrar, es un problema de seguridad.	Establecer un estándar, para mejorar las contraseñas de los equipos informáticos y los dispositivos de la red.

Fuente: Investigación de Campo, UTC.
Realizado por: Investigadores

2.2 Estándares de Calidad para el Mejoramiento del Flujo de Información en la Red

El presente trabajo investigativo se ha basado en algunos estándares que rigen las redes y las telecomunicaciones, de esta manera aseguraremos un correcto estudio de la situación actual de la Universidad y podemos sugerir con certeza las mejoras que deben implementarse en la red corporativa de la Universidad Técnica de Cotopaxi.

2.2.1 IEEE 802.1X

IEEE 802.1X. (2008). Recuperado el 23 de diciembre de 2012, de http://estandares ieee802redes.blogspot.com

La IEEE 802.1X permite el Control de Admisión de Red basada en puertos, es parte del protocolo IEEE 802. Permite la autenticación de dispositivos interconectados a un puerto LAN, estableciendo una conexión punto a punto o sugiriendo el acceso por ese puerto si la autentificación falla.

Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en protocolo de autentificación extensible (EPA – RFC 2284), el RFC 2284 ha sido declarado obsoleto en favor del RFC 3748.

802.1X está disponible en ciertos conmutadores de red cableados y puede configurarse para autenticar nodos que están equipados con software suplicante, esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

2.2.2 IEEE 802.1Q

IEEE 802.1Q. (2007). Recuperado el 28 de diciembre de 2012, de http://manejo deredesinformaticasexto.blogspot.com/2013/05/vlan-nativo-y-turking-8021q.html

El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales.

2.2.3 IEEE 802.1D

IEEE 802.1D. (2005). Recuperado el 04 de enero de 2013, de http://es.scribd.com/ doc/21146436/Estandares-IEEE-802

La IEEE 802.1D es el estándar de IEEE para bridges MAC (puentes MAC), que incluye bridging que es una técnica de reenvío de paquetes que usan los switches, el protocolo Spanning Tree y el funcionamiento de redes 802.11, entre otros. También impide que los bucles que se forman cuando los puentes o los interruptores están interconectados a través de varias rutas.

El algoritmo BPDU logra mediante el intercambio de mensajes con otros switches para detectar bucles y a continuación, elimina el bucle por el cierre de puente seleccionado interfaces. Este algoritmo garantiza que hay una ruta activa entre dos dispositivos de red.

2.2.4 IEEE 802.1P, Q – QoS SOBRE EL NIVEL DE MAC

IEEE 802.1P, Q – QoS SOBRE EL NIVEL DE MAC. (2009). Recuperado el 08 de enero de 2012, de http://www.geocities.ws/jcredesii/index-2.html

El uso de los estándares IEEE 802.1P y Q, Q es el protocolo de calidad de servicio (QoS) sobre el nivel de MAC, hoy internet provee solamente el servicio de Best Effort. Debido a que la Ethernet es la tecnología de acceso para red de área local más utilizada, la importancia de proporcionar un mecanismo de calidad de servicio no debe ser descuidada.

Para entender mejor, relacionemos los estándares de IEEE 802.1P, 802.1D y 802.1Q, el estándar de 802.1P se encarga de las claves de tráfico y multicast dinámico que son los encargados de filtrar parte del control del medio de acceso (MAC), que en la actualidad se lo conoce como el estándar IEEE 802.1D y el estándar 802.1Q forma parte del estándar IEEE 802.1D.

Los parámetros siguientes son esenciales para suministrar QoS:

1. Disponibilidad de servicio.
2. Perdida de frame.
3. Frame Misordering.
4. Duplicación de frames.
5. Retardo de tránsito.
6. Tiempo de vida del frame.
7. Tasa de error de frame no detectado.

2.2.5 Inteligencia y Calidad en la Red

Inteligencia y Calidad en la Red. (2006). Recuperado el 18 de enero de 2012, de http://www.idg.es/computerworld/Inteligencia-y-calidad-en-la-red/seccion-net/articulo-126258,

Para soportar las aplicaciones que consumen grandes anchos de banda y los nuevos tráficos multimedia, no basta con dotar a la red de mayor capacidad implantando Gigabit Ethernet. Es preciso, además, añadir determinados niveles de inteligencia que permitan controlar los tráficos dando prioridad al más crítico para la actividad de la institución. Aun en el caso de que el tiempo de respuesta de la red sea el suficiente la mayor parte del tiempo, puede haber ocasiones en que se produzcan congestiones. Una red tradicional no es capaz de diferenciar los distintos tráficos y en consecuencia, a todos los trata por igual. Así, una gran transferencia FTP puede causar graves interrupciones de una sesión de videoconferencia de sobremesa. Un primer paso para evitar estas situaciones consiste en aumentar la capacidad de la red adoptando Gigabit Ethernet.

Pero, a la larga, no basta con disponer simplemente de más ancho de banda. Es preciso, además, utilizar técnicas que hagan posible controlar el tráfico de aplicación. La combinación de técnicas de calidad de servicio (QoS) y de conmutadores Gigabit Ethernet en un entorno LAN permite a los administradores de TI tomar el control del tráfico de datos para asegurar el rendimiento de la red y en consecuencia de la institución de un modo eficiente. En condiciones normales, QoS no es necesaria, pero hay eventos que impactan el rendimiento de las redes incluso cuando están bien diseñadas. Aunque la red se sobrecargue, QoS asegura que el tráfico crítico no sea ni perdido ni retardado. En general, añade fiabilidad y disponibilidad, haciendo un mejor uso del ancho de banda existente y dando a los

usuarios tiempos de respuesta más rápidos. Además, permite a los administradores TI controlar el uso de las redes para dotarlas de mayor eficiencia.

Una red con QoS es, una red inteligente capaz de identificar y priorizar los tráficos críticos. Uniendo esta inteligencia a la enorme capacidad que aportan los conmutadores Gigabit Ethernet se consigue niveles de eficacia no disponibles hasta ahora.

2.3 Análisis de las Herramientas de Seguridad y Monitoreo

Esta investigación se basó en la búsqueda de distintos sistemas que sean factibles para la seguridad y monitoreo de la red en plataforma Linux, puesto que estos sistemas son livianos y no es necesario pagar por el uso de licencias.

El estudio arrojó que los sistemas más confiables y más usados en distintas empresas son: ***Packet Filter, Shorewall, Ipcop y UFW*** como sistemas de seguridad y ***Hyperic Hq, Nagios, Pandora*** y ***Fms Zenoss*** como sistemas de monitoreo de la red respectivamente, estos son los más recomendados en el mercado por sus distintas características. Además de su amplio uso en empresas con grandes redes, lo que hace que sean estudiadas de manera sistemática cada una de estas herramientas para determinar cuál es la más factible y la que más se adapte a las necesidades de la Universidad Técnica de Cotopaxi.

Mediante un proceso de diálogo con el Administrador de la red de la Institución, para conocer las necesidades principales que debe poseer el sistema de seguridad y monitoreo de la red a implementar se estableció una lista con los requerimientos para el sistema:

- Ligero
- Confiable
- Mapa estructurado
- Integración con todos los dispositivos
- Notificaciones
- Fácil uso
- Administración a distancia
- Que sea programable
- Funcionamiento en tiempo real

2.3.1 Análisis de las Herramientas de Seguridad

A continuación, se detalla un cuadro comparativo y cuantitativo sobre los aspectos más importantes y relevantes de las herramientas mencionadas anteriormente en el Capítulo I para la seguridad de la red de la Universidad Técnica de Cotopaxi.

TABLA N° 2.2. ANÁLISIS COMPARATIVO

CARACTERÍSTICAS	PACKET FILTER	SHOREWALL	IPCOP	UFW
Interfaz WEB	✓	✓	✓	✓
Documentación suficiente			✓	✓
Reportes	✓	✓	✓	✓
Soporte de Base de Datos	✓		✓	
Manejo de Alertas	✓		✓	✓
Visualización de Gráficos		✓	✓	
Licencia Libre	✓	✓	✓	✓
Autenticación de Usuario	✓		✓	✓
Robustez		✓	✓	
Uso de Redes Locales	✓	✓	✓	✓

Uso de Redes Empresariales		✓	✓	
Manejo de Plugins	✓		✓	
Conexiones Remotas			✓	
Activación, desactivación de servicios de red	✓	✓	✓	✓

Fuente: Investigadores
Realizado por: Investigadores

TABLA N° 2.3. ANÁLISIS CUANTITATIVO

PARÁMETROS	GRADO			
Compatibilidad con otras herramientas de red	**BAJO**	**ALTO**	**ALTO**	**ALTO**
Dificultad para la implementación	**BAJO**	**BAJO**	**ALTO**	**ALTO**
Grado de Personalización	**ALTO**	**ALTO**	**ALTO**	**ALTO**
Estabilidad	**BAJO**	**ALTO**	**ALTO**	**BAJO**
Historial General de la red	**ALTO**	**ALTO**	**ALTO**	**ALTO**

Fuente: Investigadores
Realizado por: Investigadores

Como podemos observar IPCop brinda una amplia gama de funcionalidades que van más allá de las que ofrecen algunos firewalls comerciales, sin pretender explicar cada una de ellas y solo a modo de numeración, tenemos:

- Acceso seguro por SSL a la interface de administración web
- DHCP cliente/servidor
- DNS dinámico
- Lista de hosts estable desde la interface web
- HTTP/FTP proxy (squid)
- IDS (snort) en todas las interfaces
- Log local o remoto
- NTP cliente/servidor
- Servidor SSH (PSK o con password)

- Traffic shaping (en la interface RED)
- Port Forwarding (Redireccionamiento de puertos)
- DMZ Pinholes
- VPN (IPSEC)
- Gráficos de monitoreo de CPU, RAM, swap, HD, tráfico de RED, etc.

2.3.2 Análisis de las Herramientas de Monitoreo

A continuación, se detalla un cuadro comparativo y cuantitativo sobre los aspectos más importantes de las herramientas de monitoreo de la red mencionadas anteriormente en el Capítulo I.

TABLA N° 2.4. ANÁLISIS COMPARATIVO

CARACTERÍSTICAS	HYPERIC HQ	NAGIOS	PANDORA FMS	ZENOSS
Interfaz WEB	✓	✓	✓	✓
Documentación suficiente		✓		
Reportes	✓	✓	✓	✓
Soporte de Base de Datos	✓	✓	✓	✓
Manejo de Alertas	✓	✓	✓	✓
Visualización de Gráficos	✓	✓	✓	✓
Licencia Libre	✓	✓	✓	✓
Autenticación de Usuario		✓		
Robustez	✓	✓	✓	
Uso de Redes Locales	✓	✓	✓	✓
Uso de Redes Empresariales	✓	✓	✓	
Manejo de Plugins	✓	✓	✓	✓

Fuente: Investigadores
Realizado por: Investigadores

TABLA N° 2.5. ANÁLISIS CUANTITATIVO

PARÁMETROS	GRADO			
Compatibilidad con otras herramientas de red.	**BAJO**	**ALTO**	**ALTO**	**ALTO**
Dificultad para la implementación.	**BAJO**	**ALTO**	**BAJO**	**BAJO**
Grado de Personalización.	**ALTO**	**ALTO**	**ALTO**	**ALTO**
Estabilidad.	**BAJO**	**ALTO**	**BAJO**	**BAJO**
Historial General de la red.	**ALTO**	**ALTO**	**ALTO**	**ALTO**

Fuente: Investigadores
Realizado por: Investigadores

Como podemos observar Nagios cuenta con algunas características que se indican a continuación:

- Monitoreo de equipos de red activos, hosts, (Switch, Router, Hubs, CPE, NetWare, etc.).

- Notificación y Alerta personalizadas, del estado de hosts, sistemas y servicios en caso de presentarse inconvenientes en los mismos, a través de diferentes sistemas de comunicación (E-mail, Pagers, SMS a teléfonos móviles, Alertas Sonoras, Gráficas o definidas por el usuario).

- Diseño de Plugins totalmente personalizables para adaptar el sistema acorde a nuestras necesidades.

- Detallado informe gráfico y textual, diario, semanal, mensual, etc., del comportamiento de los sistemas a monitorizarse.

- Publicación de mapas de red, alertas gráficas y configuración a través de su servidor WEB apache2 incluido, con validación de contraseñas y usuarios.

De igual manera existe una verdadera comunidad internacional de miembros, participando en la promoción, soporte y desarrollo de Nagios, aportando con:

- Plugins, aplicaciones adicionales y extensiones, que aumentan las capacidades de Nagios.

- Páginas Web fuentes de información, trucos, consejos y soporte técnico totalmente libre de recargos.

- Conferencias y Talleres para promover Nagios alrededor del mundo.

Nagios ha sido descargado de su sitio web oficial en más de 2 millones de ocasiones, ha llegado a convertirse en la solución industrial estándar, para el monitoreo de redes, sistemas y aplicaciones. Se constituye como una excelente decisión, al momento de implementar un sistema de monitoreo, sus mayores fortalezas radican en: sistema de Código Abierto, robusto, confiable, altamente configurable, desarrollado en Perl, modular y compatible con cualquier sistema operativo basado en Unix.

2.3.3 Elección de las Herramientas de Software Libre para Proporcionar la Seguridad y Monitoreo de la Red de la Universidad Técnica de Cotopaxi

En el análisis realizado anteriormente se comparan ciertas características a las herramientas de seguridad y monitoreo de la red, mediante ese estudio se logró determinar que las herramientas que mejor se adapta a las necesidades de la División de Redes y Comunicaciones IP de la Universidad Técnica de Cotopaxi, son las herramientas ***IPCop*** y ***Nagios***, ya que cumplen con todas las expectativas, en este orden es importante señalar que son unas herramientas que ofrecen respuestas en

tiempo real y que todos los chequeos se pueden programar para que sean realizados por intervalos de tiempo.

Es importante también señalar que IPCop es una opción de firewall que nos ayuda a tener nuestra red de datos protegida de amenazas e intrusos ya que cada vez que encuentre una amenaza lo expulsa automáticamente por medio del Internet o lo registra a través de un log. Siendo una interfaz más sencilla en cuanto a diseño, cuidando más la completitud de los datos y la facilidad de acceso que el aspecto, es decir, la interfaz es más útil que bonita.

IPCop permite también ampliar su funcionalidad mediante la inclusión de add-ons o plugins, además de dar la posibilidad a los usuarios de crear los suyos propios y empaquetarlos. Por último, la representación de los tipos de interfaces mediante colores hace más intuitiva la identificación de una interfaz con su tipo asociado. Además, estos colores van directamente asociados con el riesgo que se asume en cada uno de los tipos, siendo el color rojo para la de mayor riesgo y el verde para la de más confianza.

Y de igual manera Nagios puede ubicar todos y cada uno de los dispositivos que forman la red y de esta manera es posible encontrar de forma exacta y con mayor rapidez cual dispositivo y en qué lugar se está presentando el problema, ofreciendo de este modo una gran ventaja para poder mantener y ofrecer un servicio de mejor calidad para los usuarios finales y evitar las quejas y reclamos, por las caídas del sistema, además muy importante es el hecho de que esta realizado en PHP y es posible que se le puedan agregar diversas aplicaciones realizadas por el usuario y adaptarlas a nuestras necesidades.

Nagios permite también la integración con todos los dispositivos que puedan ser chequeados mediante un ping, sin importar para que arquitectura haya sido desarrollado el dispositivo, la gama de aparatos que pueden ser monitoreados es muy amplia ya que todos los dispositivos existentes que conforman la red pueden ser monitoreados, desde equipos con sistema operativo Windows, Linux, antenas canopy y terabeam, switches cisco, routers, servidores, módems, todos los dispositivos sin excepción pueden ser monitoreados.

Con lo indicado anteriormente es posible concluir, que es sumamente indispensable y necesario la implementación de las herramientas de seguridad y monitoreo de la red en la Universidad Técnica de Cotopaxi, y poder solucionar cualquier eventualidad en tiempo record, demostrando un servicio óptimo y ganado tiempo en la resolución de los problemas, con esto podremos enfrentar cualquier contingencia de cualquier índole que se nos presente.

2.4 Diseño Metodológico

2.4.1 Tipos de Investigación

2.4.1.1 Investigación Bibliográfica

Hernández (2006) manifiesta qué:

> La investigación bibliográfica resulta indispensable para el trabajo de los especialistas en las más variadas disciplinas, así como para las personas que trabajan en la producción y distribución de libros, como bibliotecarios, libreros o bibliófilos, y pueden constituir útiles fuentes de información para todo lector serio, ya que es aquella etapa de la investigación Científica donde se explora que se ha escrito sobre un determinado tema o problema (p. 84).

La investigación bibliográfica será aplicada para recopilar información del pasado y con ello realizar un análisis de nuestro problema, para poder dar una solución eficiente y eficaz.

2.4.1.2 Investigación de Campo

Lerma (2007), menciona qué ” la investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna en donde se desarrolla el problema, en el sitio en que ocurre el fenómeno; el investigador interviene en ellas ya sea como observador o como participante” (p. 69).

La investigación de campo será aplicada para la obtención de información, en relación al número de computadoras y a los usuarios quienes acceden a través de la red de la Universidad Técnica de Cotopaxi.

2.4.1.3 Investigación Experimental

Castilla y Pérez (2005), manifiestan qué:

> La investigación experimental es la búsqueda sistemática, planificada de hechos y sus significados o implicaciones, con referencia a un problema. La investigación experimental se ha ideado con el propósito de determinar, con la mayor confiabilidad posible, relaciones de causa-efecto, para lo cual uno o más grupos, llamados experimentales, se exponen a los estímulos experimentales y los comportamientos resultantes se comparan con los comportamientos de ese u otros grupos, llamados de control, que no reciben el estímulo experimental (p. 53).

La investigación experimental será aplicada para la obtención de resultados, para alcanzar los objetivos del experimento, responder a las preguntas de investigación y someter a verificación la hipótesis.

2.4.2 Métodos de Investigación

2.4.2.1 Método Inductivo

De acuerdo con Ávila (2006), manifiesta qué "el método inductivo es una aproximación a la realidad en la cual el investigador establece una serie de argumentos que van de aspectos particulares a las generalizaciones, se sustenta en la compilación de evidencia empírica" (p. 6).

El método inductivo es muy importante, ya que nos da una aproximación a los hechos reales dentro de nuestra investigación, y nos ayudará a compilar toda la información empírica.

2.4.2.2 Método Hipotético – Deductivo

Bernal (2006), menciona qué "el método Hipotético – Deductivo consiste en un procedimiento que parte de unas afirmaciones en calidad de hipótesis y busca contradecir o falsear tales hipótesis, deduciendo de ellas conclusiones que deben confrontarse con los hechos" (p. 57).

Consideramos que el método Hipotético – Deductivo nos ayudará a resolver nuestra hipótesis, a través de conclusiones conforme a los hechos, ya que este método nos ayudará a tener una visualización más clara del problema que tiene la Universidad,

esto nos permitirá dar una afirmación anticipada de lo que se quiere realizar y de los beneficios que dará nuestro proyecto, la cual debe ser verificada.

2.4.3 Técnicas de Investigación

2.4.3.1 Encuesta

Según Arias (2006) manifiesta qué "la encuesta consiste en obtener información acerca de un grupo de individuos. Constituye un test escrito que el investigador formula a un grupo de personas" (p. 43).

2.4.4 Instrumentos

Se ha visto beneficioso utilizar instrumentos que ayuden a la recolección de la información, y nos facilite el manejo de dicha información para la elaboración de nuestro proyecto de investigación, los instrumentos a aplicarse son:

2.4.4.1 Formulario de Encuesta

Es un instrumento cuantitativo de investigación social, mediante la consulta a un grupo de personas elegidas de forma estadística, realizada con ayuda de un cuestionario que contiene preguntas abiertas y cerradas, que sirve para la obtención de información.

2.5 Población

Para el desarrollo de esta investigación en la Universidad Técnica de Cotopaxi, se ha tomado en cuenta a las personas que trabajan y mantienen una relación directa con el Departamento de Servicios Informáticos y Personal Administrativo, ya que dichas

personas pueden facilitar la información necesaria para la elaboración de nuestro proyecto, puesto que ellos tienen un amplio conocimiento en la red de datos de la institución, obteniendo así los siguientes datos:

TABLA N° 2.6. POBLACIÓN

INVOLUCRADOS	CANTIDAD
- Director del Departamento de Servicios Informáticos. - Personal Administrativo del Departamento de Servicios Informáticos. - Docentes Técnicos de la Carrera de Ingeniería en Informática y Sistemas Computacionales. - Personal Responsable de las Salas de Cómputo de la Universidad Técnica de Cotopaxi (Matriz).	**1** **7** **13** **3**
TOTAL:	**24**

Fuente:

Ing. Adrián Mena **(**Director del Departamento de Servicios Informáticos.)

Ing. Segundo Corrales **(**Coordinador de la Carrera de Informática y Sistemas Computacionales.)

Realizado por: Investigadores

Por ser la población pequeña no amerita calcular la muestra, ya que la población a utilizarse en el desarrollo de este proyecto, considera 24 personas que conocen con exactitud los problemas de la red de datos de la Universidad Técnica de Cotopaxi.

2.6 Operacionalización de Variables

TABLA N° 2.7. OPERACIONALIZACIÓN DE VARIABLES

HIPÓTESIS	VARIABLES	INDICADORES
La implementación de un sistema con plataforma Linux mejorará la seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi.	**Variable Independiente** Implementación de un sistema con plataforma Linux.	- Herramientas Informáticas. - Costos. - Equipos Informáticos. - Financiamiento.
	Variable Dependiente Seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi.	- Disminución de Costos. - Mejoramiento de la red. - Análisis preventivo de la red. - Beneficios a corto plazo. - Generación de reportes sustentados.

Fuente: Análisis grupal.
Realizado por: Investigadores

2.7 Análisis e Interpretación de los Resultados

Encuestas Aplicadas al Personal Administrativo del Departamento de Servicios Informáticos, Docentes Técnicos de la Carrera de Ingeniería en Informática y Sistemas Computacionales y Personal Responsable de las Salas de Cómputo de la Universidad Técnica de Cotopaxi (Matriz)

1.- ¿Cómo califica Ud. el decreto que hizo el Eco. Rafael Correa, al proporcionar el apoyo de su Gobierno al software libre como herramienta para generar innovación en el Ecuador, adoptando el software libre como una política de estado mediante el Decreto 1014?

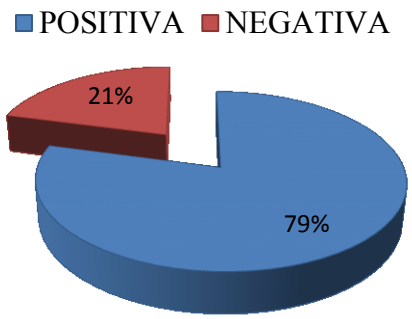
Los resultados obtenidos, son los siguientes:

TABLA N° 2.8. DECRETO ECO. RAFAEL CORREA

N°	OPCIÓN	VALOR	%
1	POSITIVA	19	79
2	NEGATIVA	5	21
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.2. DECRETO ECO. RAFAEL CORREA



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: Al observar este estadígrafo podemos apreciar que, el 79% afirma como positivo que el software libre pase a ser una política de Estado, este es un gran paso para la comunidad ecuatoriana de software libre, ya que se alcanzará, la libertad del conocimiento y tendremos las mismas oportunidades que los ciudadanos de cualquier parte del mundo para hacer cosas grandes, esto permite que el proyecto investigativo sea factible.

2.- ¿Considera Ud. importante la implementación de herramientas de software libre para la seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi?

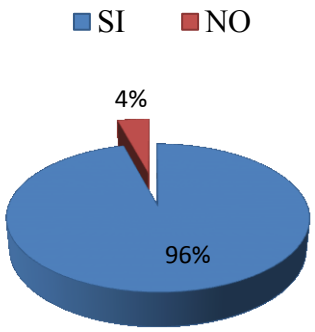
Los resultados obtenidos, son los siguientes:

TABLA N° 2.9. HERRAMIENTAS DE SOFTWARE LIBRE

N°	OPCIÓN	VALOR	%
1	SI	23	96
2	NO	1	4
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.3. HERRAMIENTAS DE SOFTWARE LIBRE



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: De la población encuestada, el 96% afirma la importancia que tiene la implementación de herramientas de Software libre para la seguridad y monitoreo de la red, lo que demuestra los altos beneficios e innumerables ventajas que trae consigo esta investigación, las que se pueden resumir en tres aspectos: costo, seguridad y velocidad.

3.- ¿Señale con una [X] si Ud. conoce una de estas herramientas de software libre que permiten el monitoreo de los equipos informáticos y servicios más importantes de una red?

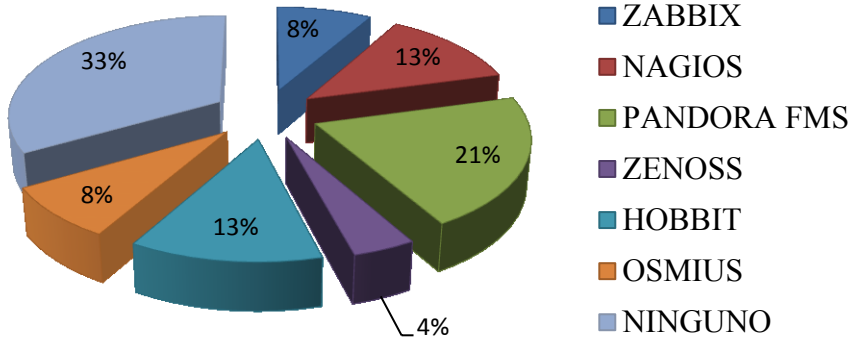
Los resultados obtenidos, son los siguientes:

TABLA N° 2.10. HERRAMIENTAS DE MONITOREO DE RED

N°	OPCIÓN	VALOR	%
1	ZABBIX	2	8
2	NAGIOS	3	13
3	PANDORA FMS	5	21
4	ZENOSS	1	4
5	HOBBIT	3	13
6	OSMIUS	2	8
7	NINGUNO	8	33
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.4. HERRAMIENTAS DE MONITOREO DE RED



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: Según los resultados, la mayoría de los profesionales encuestados (33%) no están al tanto de algunas herramientas para monitorear la red, mientras que otra

parte de encuestados, divide sus conocimientos entre una y otra herramienta. Por cuanto el propósito de este análisis está en extender la protección de las redes y el obtener un excelente resultado que estará en la elección del mejor software de código abierto dirigido a monitorear las redes, tomando en cuenta todas las funcionalidades y beneficios que poseen para acoplarlas a nuestro favor.

4.- ¿Señale con una [X] si Ud. conoce una de estas herramientas de software libre que permiten la seguridad de la información a través de un firewall?

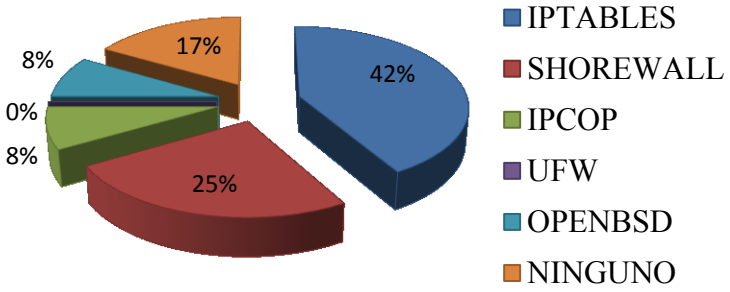
Los resultados obtenidos, son los siguientes:

TABLA N° 2.11. HERRAMIENTAS DE SEGURIDAD DE RED

N°	OPCIÓN	VALOR	%
1	IPTABLES	10	42
2	SHOREWALL	6	25
3	IPCOP	2	8
4	UFW	0	0
5	IPFIRE	2	8
6	NINGUNO	4	17
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.5. HERRAMIENTAS DE SEGURIDAD DE RED



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: Se observa una mayor preferencia por la aplicación IPTables con un 42% y Shorewall en un 25% mientas que los demás encuestados distribuyen sus conocimientos en uno y otro software, con similares o mejores funcionalidades, lo que nos obliga a hacer la mejor elección en base a un análisis sustentable, con el único objetivo e intención de formalizar una metodología práctica y factible para convertir entornos informatizados inseguros en entornos protegidos.

5.- ¿Señale con una [X] los aspectos que se pueden monitorear a través de un sistema de monitoreo dentro de una red?

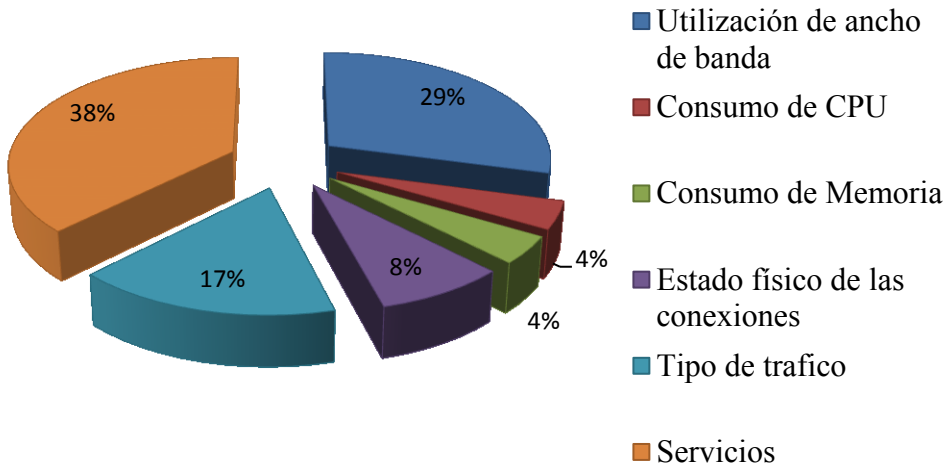
Los resultados obtenidos, son los siguientes:

TABLA N° 2.12. ASPECTOS QUE SE PUEDEN MONITOREAR

N°	OPCIÓN	VALOR	%
1	Utilización de ancho de banda	7	29
2	Consumo de CPU	1	4
3	Consumo de Memoria	1	4
4	Estado físico de las conexiones	2	8
5	Tipo de trafico	4	17
6	Servicios	9	38
	TOTAL	24	100

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.6. ASPECTOS QUE SE PUEDEN MONITOREAR



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: Según los resultados de los profesionales encuestados, los mayores porcentajes afirman que el sistema debería monitorear aspectos importantes como: los servicios 38%, ancho de banda 29%, y tráfico de red 17%, de esto se deriva la importancia de contar con un esquema capaz de notificarnos las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico, por lo que estos aspectos a monitorear serán primordiales al momento de realizar la selección y configuración de la herramienta de monitoreo y así brindar un buen servicio a los usuarios.

6.- ¿Señale con una [X] los requerimientos que pueden ser controlados por un firewall dentro de una red?

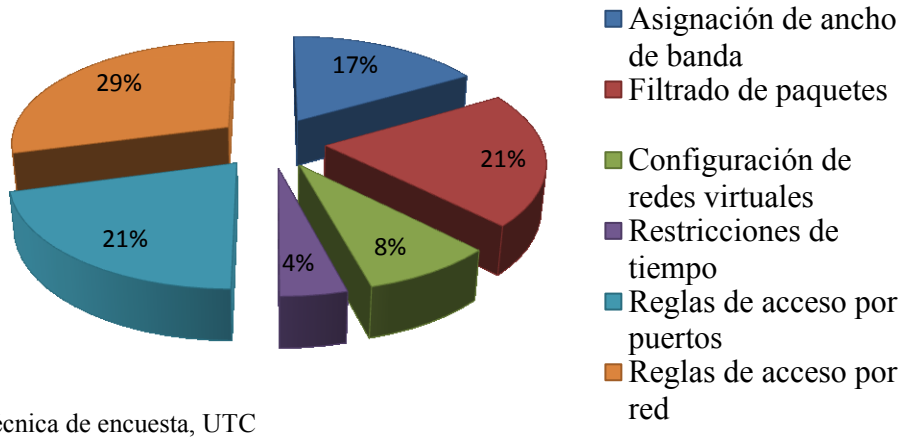
Los resultados obtenidos, son los siguientes:

TABLA N° 2.13. CONTROLES DE UN FIREWALL

N°	OPCIÓN	VALOR	%
1	Asignación de ancho de banda	4	17
2	Filtrado de paquetes	5	21
3	Configuración de redes virtuales	2	8
4	Restricciones de tiempo	1	4
5	Reglas de acceso por puertos	5	21
6	Reglas de acceso por red	7	29
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.7. CONTROLES DE UN FIREWALL



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: Del gráfico mostrado se puede deducir que, hay una mayor preferencia por los siguientes requerimientos: Reglas de acceso a la red del 29%, Reglas de acceso por puertos y Filtrados de paquete del 21%, aunque también hay que resaltar el porcentaje de 17% que prefiere la asignación de Ancho de banda. Estas necesidades se ven justificadas debido a la importancia que tiene el Internet en la actualidad, ya que está considerada dentro de los servicios informáticos más utilizados e influyentes de todos los tiempos.

Otro aspecto importante es la utilización de las funciones de filtrado de paquetes ya que un administrador podría restringir el acceso a determinados sistemas, segmentos de red, rangos de direcciones y servicios, basándose en una serie de criterios. Todos estos aspectos serán fundamentales al momento de establecer el conjunto de reglas de filtrado de paquete para el software de seguridad.

7.- ¿Piensa Ud. que la Universidad Técnica de Cotopaxi debería tener un sistema de control para detectar y prevenir el ingreso de intrusos o hackers a los servidores?

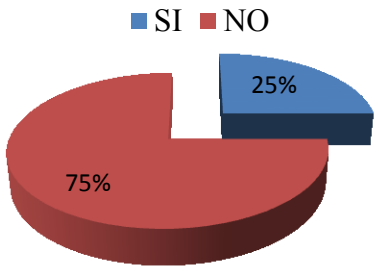
Los resultados obtenidos, son los siguientes:

TABLA N° 2.14. CONTROL PARA EL INGRESO A LOS SERVIDORES

N°	OPCIÓN	VALOR	%
1	SI	18	75
2	NO	6	25
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.8. CONTROL PARA EL INGRESO A LOS SERVIDORES



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: Un gran porcentaje afirma (75%) que la Universidad Técnica de Cotopaxi debe contar con un sistema de control para prevenir el ingreso de intrusos,

por lo tanto es importante dejar en claro que la confidencialidad de la información privada, no puede garantizarse, sin la posibilidad de analizar el funcionamiento de los sistemas que la manipulan. La mayoría de entornos informáticos padecen los efectos de la inseguridad dado que no tenemos una cultura desarrollada, pues las técnicas de seguridad que se practica son débiles, por ello los índices de estafas, de atentados y delitos informáticos aumentan.

8.- ¿Conoce Ud. si la Universidad Técnica de Cotopaxi cuenta con un plan de contingencia en caso de fallar la interconexión entre los servidores?

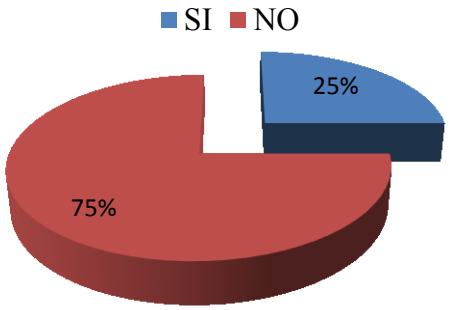
Los resultados obtenidos, son los siguientes:

TABLA N° 2.15. PLAN DE CONTINGENCIA

N°	OPCIÓN	VALOR	%
1	SI	6	25
2	NO	18	75
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

GRÁFICO N° 2.9. PLAN DE CONTINGENCIA



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: El 75% afirma que la Universidad no posee un plan de contingencia en caso de fallar la interconexión entre los servidores, por lo cual se está de manera directa expuesto a posibles ataques de personas inescrupulosas, por ello nos corresponde convertirnos en agentes activos para resguardar y no esperar que nos protejan. Las técnicas de seguridad son un método que podemos usar para poder educar a las personas, ya que ellos son los principales agentes activos, que por desconocimiento permiten ataques.

9.- ¿Considera Ud. que el ancho de banda contratado por la Universidad Técnica de Cotopaxi es suficiente para toda la institución?

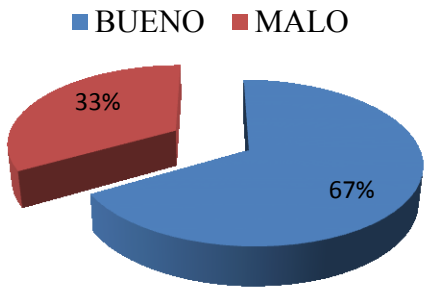
Los resultados obtenidos, son los siguientes:

TABLA N° 2.16. ANCHO DE BANDA DE LA RED DE LA UNIVERSIDAD

N°	OPCIÓN	VALOR	%
1	SI	8	33
2	NO	16	67
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC.
Realizado por: Investigadores

GRÁFICO N° 2.10. ANCHO DE BANDA DE LA RED DE LA UNIVERSIDAD



Fuente: Técnica de encuesta, UTC
Realizado por: Investigadores

ANÁLISIS: De acuerdo al gráfico, podemos observar que del 100% de la población encuestada, el 67% de profesionales técnicos afirman que el ancho de banda contratada no cumple con las necesidades de la institución, mientras que el 33% asegura que el ancho de banda es adecuado, ya que se encuentra en pleno desarrollo de nuevas tecnologías. Por lo que en la elección del sistema de monitoreo a emplear debe partir del enfoque activo que agrega tráfico a la red en dependencia del ancho de banda que se dispone para mejorar el servicio a los usuarios de la Institución.

10.- ¿Piensa Ud. que la Universidad Técnica de Cotopaxi debería contar con una herramienta que monitoree constantemente la red?

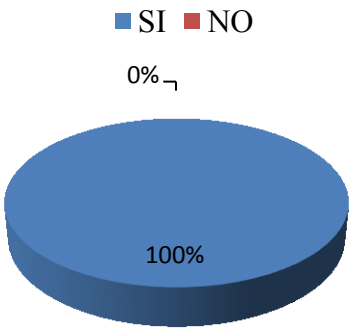
Los resultados obtenidos, son los siguientes:

TABLA N° 2.17. HERRAMIENTA DE MONITOREO

N°	OPCIÓN	VALOR	%
1	SI	24	100
2	NO	0	0
	TOTAL	**24**	**100**

Fuente: Técnica de encuesta, UTC.
Realizado por: Investigadores

GRÁFICO N° 2.11. HERRAMIENTA DE MONITOREO



Fuente: Técnica de encuesta, UTC.
Realizado por: Investigadores

ANÁLISIS: Todos los profesionales encuestados afirman que la Institución debe tener una herramienta que monitoree la red, porque cada vez es mayor el número de atacantes y constantemente están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización las cuales son de las más comunes. Por lo tanto resulta de vital importancia el monitoreo y seguridad en las redes para no perder datos de gran valor, ni bajar el desempeño de la red.

2.7.1 Análisis de las Encuestas

Como investigadores luego de haber aplicado las encuestas al Personal Administrativo del Departamento de Servicios Informáticos, Docentes Técnicos de la Carrera de Ingeniería en Informática y Sistemas Computacionales y Personal Responsable de las Salas de Cómputo de la Universidad Técnica de Cotopaxi (Matriz), determinamos que la implementación de las herramientas de software libre para la seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi recae en ***IPCop*** y ***Nagios*** respectivamente, ya que generará grandes beneficios en la Administración de la red. Analizando en el transcurso de la investigación y las diferentes tendencias de los estadígrafos llegamos a la conclusión que las herramientas elegidas son las más notorias y con más beneficios en el mercado.

2.8 Verificación de la Hipótesis

La hipótesis planteada al inicio de esta Tesis de Grado fue la siguiente: "La implementación de un sistema con plataforma Linux mejorará la seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi".

El objetivo principal fue el mejorar la seguridad y monitoreo de la red y con ello a su vez optimizar el ancho de banda para la transferencia de paquetes de datos, permitiendo alcanzar una mayor eficiencia, manejando adecuadamente la infraestructura de red con la que cuenta la Institución.

El motivo de esta investigación es para definir su factibilidad pues consta de varias herramientas, las cuales fueron analizadas y de estas elegimos dos, para la seguridad y monitoreo de la red de la Institución respectivamente como son ***IPCop*** y ***Nagios***, para mejorar el desempeño de las redes de datos, su implementación dependió en varias ocasiones de las necesidades que el administrador detectó en la red o de las necesidades de los usuarios. Actualmente e independientemente de las necesidades que el administrador detectó son aplicadas en muchas redes como acciones preventivas a posibles problemas de conectividad. Al seleccionar las herramientas a utilizar se tomó en cuenta si la red será capaz de crecer, tanto lógica como físicamente y seleccionar aquellas que le den mayor flexibilidad y escalabilidad.

Con el respaldo de las fuentes consultadas se realizaron las pruebas que consistieron desde verificar la conectividad entre equipos de diferentes LAN hasta el monitoreo del tráfico, culminando el proyecto, con la observación del comportamiento de la red mostrando periódicamente el tráfico generado. Sin embargo, en el desarrollo del proyecto también se hicieron pruebas que corroboraron la conectividad entre hosts, aplicando diversas técnicas con el objetivo de poder implementar reglas para permisos y restricciones de conectividad. Todo esto fue verificado ya que es un proceso serial en donde cada actividad realizada depende de la anteriormente ejecutada. Además en esta investigación se llegó a compartir similares puntos de vista entre varios autores en cuanto a las técnicas utilizadas en este proyecto.

El monitoreo de tráfico también fue muy importante, observando así el comportamiento de la red al elevar el tráfico generado por aplicaciones ejecutadas en los equipos de cómputo. Además, de identificar las IPs que generaban mayor tráfico y

como consecuencia la LAN también se pudieron observar los puertos, protocolos e IPs utilizados en el envío de paquetes entre los hosts origen y los hosts destino. Toda esta información y mucha más se observó con el monitoreo de los equipos, dejando en claro que es indispensable la implementación de este tipo de herramientas en una red.

Al finalizar el presente trabajo de tesis y tras el desarrollo del análisis de estadígrafos se ha podido establecer los siguientes resultados que permiten verificar la hipótesis planteada:

- ***Se conoce específicamente la arquitectura de IPCop y Nagios:*** Este proyecto de tesis muestra un estudio completo de cuáles son los componentes que forman parte de la arquitectura de ***IPCop*** y ***Nagios***, como estos interactúan entre sí, su funcionamiento y requerimientos para su utilización.

- ***Manual de usuario o guía para la administración de las herramientas de seguridad y monitoreo de la red como son IPCop y Nagios respectivamente:*** Describe las configuraciones realizadas y los complementos que se pueden implementar para el mejor funcionamiento de las herramientas, tales como:

    - Módulos que Integran el Sistema.
    - Módulo para el Monitoreo de la Red.
    - Módulo para la Seguridad de la Red.
    - Configuración de las herramientas.
    - Complementos de Nagios e IPCop.
    - Módulo de Alertas y Reportes.

CAPITULO III

3. IMPLEMENTACIÓN DE LAS HERRAMIENTAS DE SOFTWARE LIBRE PARA LA SEGURIDAD Y MONITOREO DE LA RED DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

3.1. Presentación

En este capítulo se explica el desarrollo de los módulos que conforman el sistema de seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi. Desde los albores de la administración de redes y recursos compartidos, los administradores de redes de comunicaciones, tanto a nivel local de pequeñas y medianas empresas, como a nivel extendido como metropolitano, regional e internacional, se han visto en la necesidad de realizar un seguimiento del escenario administrativo de manera automática y eficaz.

Con la finalidad de atenuar o erradicar en su totalidad, problemas presentes en el estado del arte de los mismos, como son los cuellos de botella, protocolos, puertos no permitidos o restringidos, por otro lado monitorizar con el fin de planear el crecimiento o migración de la red, a nuevas y más amplias tecnologías.

Este reto del administrador de red se detalla en ciertos puntos, presentados a continuación:

- Incremento de la velocidad, protocolos y tecnologías dentro de la red.

- La interconexión de diferentes tipos de equipos, sistemas y servicios, entrando en un tema de reserva de canal para determinado trafico específico.

- Los usuarios se encuentran en capacidad de administrar su propio computador, con cierto grado de independencia, lo cual aumenta el riesgo y la inseguridad de la red en general.

- La ardua labor que involucra dar seguimiento desde una perspectiva globalizada, a una red donde se ruedan subredes, VPN, VLAN, etc. Con restricciones específicas para cada segmento de red.

Existen un sinnúmero de herramientas útiles en el campo de las telecomunicaciones, y específicamente en el ámbito de las redes basadas en conmutación de paquetes, para el monitoreo de redes tanto de tipo local o LAN como redes de área extendida y metropolitana WAN y MAN respectivamente.

La alternativa que en este caso presenta este trabajo de tesis, incluye un requisito indispensable, planteado como un objetivo general; sea cual fuere la herramienta o herramientas escogidas para cumplir el objetivo general de este trabajo de tesis, dicha herramienta, debe ser desarrollada utilizando software de código abierto basado en GNU (*General Public License*).

3.2. Objetivos

3.2.1. Objetivo General

Analizar e implementar herramientas de software libre a través de un sistema de seguridad y monitoreo para garantizar la seguridad de la información y el monitoreo de la infraestructura y servicios de la red de la Universidad Técnica de Cotopaxi, ubicada en el Barrio El Ejido, Sector San Felipe, Cantón Latacunga, Provincia de Cotopaxi.

3.2.2. Objetivos Específicos

- Controlar la utilización del ancho de banda en cada estación de trabajo, a través de un control de restricciones por IP, para mejorar la calidad de servicio que actualmente presta la Universidad Técnica de Cotopaxi.

- Monitorear continuamente el estado de la red, a través del sistema para tener un adecuado control de la red y poder tomar las acciones necesarias para solucionar los problemas presentados antes que estos sean percibidos por los usuarios.

- Generar reportes periódicamente sobre el estado, rendimiento, disponibilidad y funcionamiento de los equipos conectados a la red, mediante la utilización de paquetes tales como webalizer y graph, mismos que permitirán visualizar gráficamente la información generada para la toma de decisiones.

- Informar al administrador en caso de que se presenten cambios dentro de la red, mediante la utilización de notificaciones automáticas vía e-mail y SMS, los mismos que ayudarán al administrador a estar informado del correcto funcionamiento de la infraestructura de red.

3.3. Análisis de Factibilidad

Una vez planteada la propuesta de implementar un sistema de seguridad y monitoreo de la red en la Universidad Técnica de Cotopaxi, se procedió a la recolección de información y al diálogo con el personal administrativo del Departamento de Servicios Informáticos. Luego de un análisis se define como realizable esta implementación, pues los requisitos expuestos y las herramientas de software libre disponibles permiten que este proyecto se pueda implementar en un tiempo prudencial y con el apoyo de quienes serán los beneficiarios del sistema y el grupo investigador, en la finalización del proyecto se hará la entrega de un Manual de Usuario al Departamento de Servicios Informáticos.

Según DIÉGUEZ, (2005) menciona qué:

> El manual de usuario expone los procesos que el usuario puede realizar con el sistema implementado. Para lograr esto, es necesario que se detallen todas y cada una de las características que tienen los programas y la forma de acceder e introducir información. Permite a los usuarios conocer el detalle de qué actividades ellos deberán desarrollar para la consecución de los objetivos del sistema. Reúne la información, normas y documentación necesaria para que el usuario conozca y utilice adecuadamente la aplicación desarrollada.

De acuerdo a lo antes mencionado, se llega al acuerdo de anexar un Manual de Usuario, ya que sería una guía técnica destinada a dar asistencia a las personas que utilizan el sistema. Ya que tiene como objetivo instruir al usuario en el uso del sistema y la solución de los problemas que se presentan en la operación.

3.3.1. Factibilidad Técnica

Es elevado el porcentaje de redes que son instaladas sin tener en consideración la seguridad, convirtiendo las mismas en redes abiertas o vulnerabilidades, sin proteger la información que por ellas circulan. Todos los sistemas de comunicación, desde el punto de vista de seguridad, presentan en general un problema común: la información que transita por lugares alejados de las personas responsables. Esto reconoce un compromiso en la seguridad ya que no existen procedimientos para garantizar la inviolabilidad de la información. Por causas fraudulentas, es posible interceptar la información por la cual es importante un método de seguridad para encontrar los puntos de acceso vulnerables a nuestra red.

La Universidad Técnica de Cotopaxi, con el pasar del tiempo ha venido realizando progresos significativos en el área tecnológica siendo estos cada vez más notorios, no se puede dejar de mencionar la implementación de las Redes de Área Local las mismas que han permitido crecer en buena medida los números de usuarios por maquina o punto de red, así como también podemos mencionar que es de gran ayuda la implementación de dispositivos Wireless para que puedan utilizar algunos recursos como el Internet o el intercambio de información entre usuarios de red.

El objetivo del sistema de seguridad y monitoreo de la red es de ser un proceso pro-activo, ya que al tener un sistema que ayude a detectar los problemas de la red, permite al administrador de la red a corregir el problema a tiempo y prevenir futuros inconvenientes que puedan surgir con el pasar del tiempo y traer grandes costos a la Institución.

3.3.2. Factibilidad Económica

Para realizar la implementación del sistema de seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi, para ayudar a la calidad de servicio y la medición del flujo de tráfico de la red se utilizó herramientas acorde a la tecnología actual como son IPCop y Nagios, entre otras herramientas de software libre.

Las aplicaciones Open Source últimamente han tenido una gran escala en el mundo de las redes, por su confiablidad y estabilidad. Existen un sin número de aplicaciones para casi cualquier propósito que no tienen ningún costo y se pueden modificar según las necesidades de la institución que lo adquiera.

Una herramienta de seguridad y monitoreo de redes, facilita el control de la información en la institución. Para una mejor productividad institucional, los responsables de los sistemas, que usan los distintos departamentos deben conocer los riesgos derivados de una inadecuada administración de la información lo que puede causar pérdidas económicas en la Institución. El monitoreo a la red puede ayudar a ver como se están empleando los recursos de la red.

3.3.3. Factibilidad Operacional

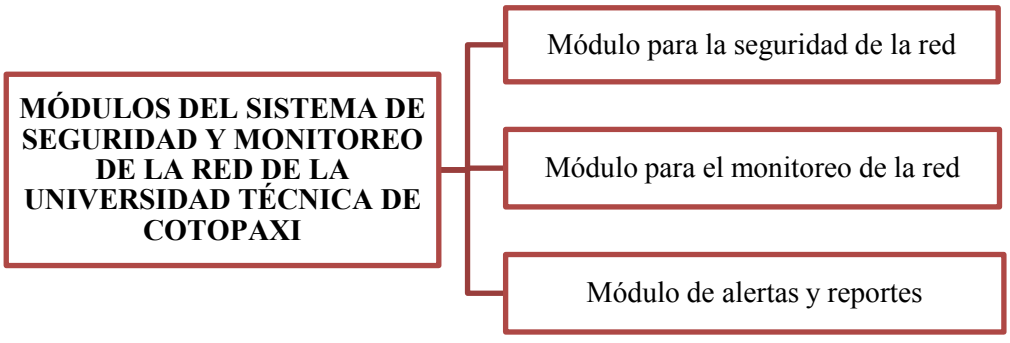
El presente proyecto investigativo es factible operativamente debido a que cuenta con todos los elementos necesarios para su manejo, el sistema de seguridad y monitoreo de red está realizado sobre software libre procurando la atención de los enlaces y los equipos que inspeccionan la Universidad.

Se basa en el control y monitoreo de los servicios de la red, a través de un sistema de seguridad y monitoreo de red, que permite almacenar la información de cada uno de los host ingresados al sistema, es posible conocer los estados y datos de estos diferentes equipos como: reportes, logs, gráficas, etc., haciendo uso del protocolo SNMP que nos permite gestionar y/o supervisar datos de diferentes elementos y componentes de la red, y al ser un protocolo estándar es posible monitorizar una amplia variedad de casos en escenarios con sistemas o equipos diferentes.

3.4. Diseño Esquemático del Sistema a Ser Implementado

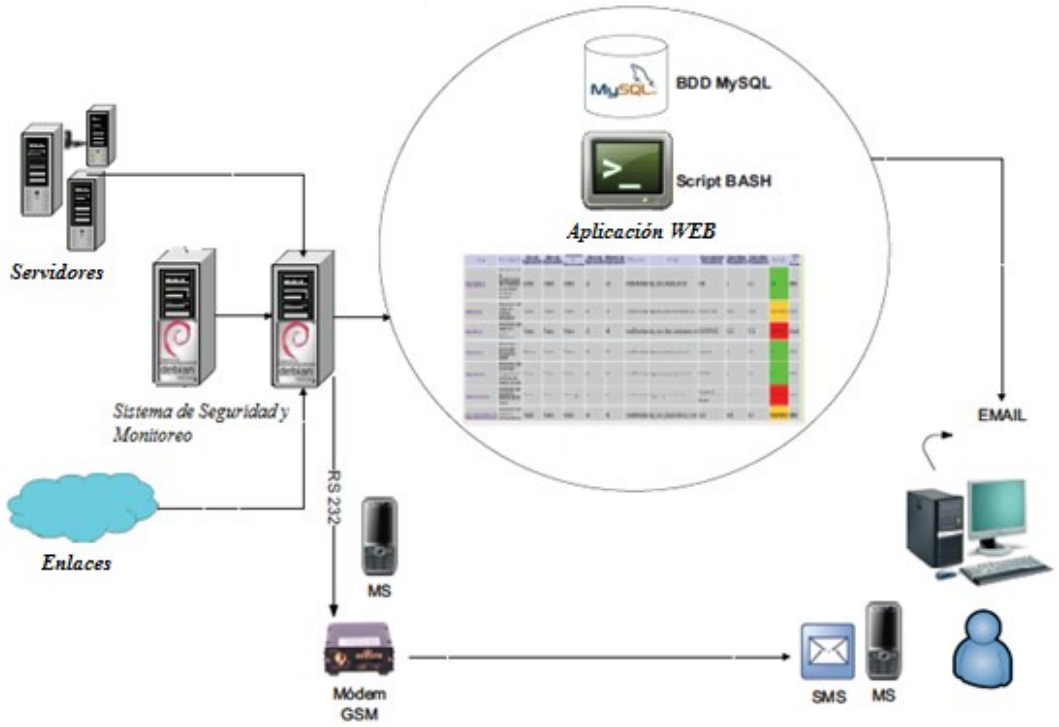
En base al análisis de la infraestructura de la red de datos de la Universidad se ha considerado elaborar el diseño del sistema de seguridad y monitoreo para la Universidad Técnica de Cotopaxi, el mismo que se lo ha estructurado en tres módulos a fin de contar con un sistema modular que facilite el desarrollo y explicación del proyecto. Cada uno de los módulos cumplirá una función específica e interactúan entre sí a fin de cumplir con los requerimientos propuestos por el administrador. Los módulos que conforman el sistema así como el esquema total del proyecto se ilustran a continuación:

GRÁFICO N° 3.1. MÓDULOS DEL SISTEMA



Fuente: Investigadores
Realizado por: Investigadores

GRÁFICO N° 3.2. ESQUEMA DEL SISTEMA



Fuente: Investigadores
Realizado por: Investigadores

3.5. Módulo para la Seguridad de la Red

Este módulo tiene como objetivo dar seguridad informática permanentemente a la red de datos de la Universidad Técnica de Cotopaxi. Este módulo adicionalmente puede funcionar como servidor DHCP, puede alterar el flujo de tráfico de la conexión a Internet asignando mayor prioridad a puertos y protocolos específicos, y también posee un sistema de detección de intrusiones, configurable a través del servicio snort.

La solución elegida para nuestra autenticación es la utilización de 802.1x, estándar de la IEEE para redes inalámbricas y cableadas. Es un estándar que nos permite el transporte de tramas EAP sobre redes cableadas e inalámbricas.

El protocolo 802.1x involucra tres participantes, como son:

- Cliente, que desea conectarse con la red.

- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios está autorizado para acceder a la red.

- El identificador, que es el equipo de red (switches, Acces Point, Firewall) que recibe la conexión del cliente. El identificador actúa como intermediario entre el cliente y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

Las ventajas que tendremos al utilizar el estándar 802.1x, son:

- ***Control de acceso y autenticación mutua:*** Protegernos de ataques.

- ***Flexibilidad:*** Adaptación al entorno y características de la red.

- ***Seguridad omnipresente:*** Ofrecer seguridad incluso si hay movilidad.

- ***Potente confidencialidad:*** Actualización de las claves WEP dinámicas.

- ***Escalabilidad:*** Ofrecer seguridad incluso con un aumento de usuarios.

De igual manera se ha creído favorable la utilización del estándar 802.1Q de la IEEE, para la seguridad de la red ya que es una prioridad máxima en cualquier institución. Ya que las redes virtuales VLAN permiten que la red pueda ser segmentada en

grupos o por departamentos, jerárquicamente y por grupos de seguridad, de este modo se mejora la seguridad de la red.

Las redes de área local pueden interconectarse utilizando los puentes transparentes, definidos en la IEEE 802.1D, por que permiten utilizar diferentes tecnologías de red, los puentes ofrecen ciertas ventajas como:

- Interconectan LAN dispersas geográficamente utilizando distintos medios en los segmentos de backbone (fibra) y de acceso (UTP).

- Dividen segmentos LAN con mucha carga, en segmentos LAN con menor carga, lo que incrementa su rendimiento.

- Mejora la robustez de la red, pues facilitan la localización de errores y posibilitan caminos alternativos.

- Mejora la seguridad en la red, pues confinan el tráfico a segmentos LAN de menor tamaño, especialmente útil en las tramas de difusión.

Para hacer posible lo indicado anteriormente, se ha seleccionado como herramienta de seguridad informática a IPCop, debido a que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

3.5.1. Requerimientos del Sistema

En cuanto al hardware IPCop se caracteriza por ser un aplicativo bastante liviano, los recursos que consume tanto en almacenamiento como en memoria de proceso son bastante bajos, podría decirse que prácticamente cualquier computador de escritorio con requerimientos mínimos y cuatro tarjetas de red adicionales está en condiciones de albergar a IPCop.

TABLA N° 3.1. IMPLEMENTACIÓN DE IPCOP

REQUERIMIENTOS
Servidor Torre o Rack.
Intel Core2Quad 2.0 GHz
1 GB RAM
500 GB Disco Duro
4 Tarjetas de Red NIC 100/1000 BASE-T

Fuente: Requisitos de Hardware
Realizado por: Investigadores

La distribución IPCop está preparada para funcionar en equipos con un mínimo de 512 MB de memoria RAM, 5 GB libres de espacio en disco y una variante de Linux Kernel 2.6.x, por lo que el consumo de memoria no es excesivo.

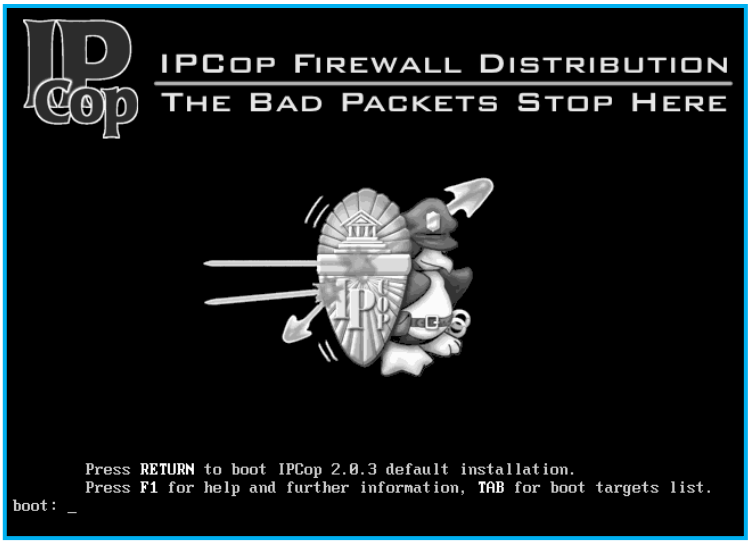
La velocidad de ejecución y de uso es, en general, fluido, en la mayoría de los casos, la fluidez dependerá de las características y el estado de la red, al acceder mediante interfaz web desde un equipo externo.

3.5.2. Instalación de IPCop

Para el correcto funcionamiento del sistema de seguridad IPCop, es necesario instalar de acuerdo a los siguientes ítems básicos:

a) Descargamos la imagen ISO de la distribución IPCop, disponible en: ***http://ipcop.org/download.php*** y grabamos en un CD, luego iniciamos el ordenador desde el CD y presionamos ***ENTER*** para empezar la instalación:

GRÁFICO Nº 3.3. PANTALLA PRINCIPAL DE IPCOP



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

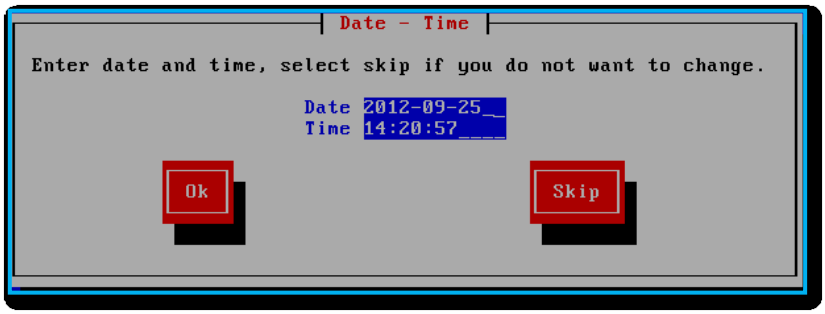
b) Seleccionamos el idioma que se desea utilizar para instalar IPCop. Utilizamos las teclas de flecha para mover hacia arriba o hacia abajo en la lista, y la tecla ***Tab*** para moverse entre los elementos, utilizamos la barra espaciadora o la tecla ***INTRO*** para seleccionar:

GRÁFICO Nº 3.4. SELECCIÓN DEL DISEÑO DEL TECLADO

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

c) Seleccionamos la zona horaria que se encuentra en la lista, e introducimos la fecha y la hora. Seleccionamos ***Skip*** si deseamos mantener la configuración actual.

GRÁFICO Nº 3.5. SELECCIÓN DE LA HORA Y FECHA



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

d) Seleccionamos la partición lógica en el que se desea instalar IPCop, y a continuación, seleccionamos el modo de instalación.

GRÁFICO Nº 3.6. SELECCIÓN DEL MODO DE INSTALACIÓN

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

GRÁFICO Nº 3.7. BIENVENIDA A IPCOP

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

e) A continuación introducimos el nombre del host y el nombre del dominio que deseamos dar.

f) En la pantalla inicial se mostrara una lista de las tarjetas de interfaz de red que se han detectado automáticamente durante la exploración del hardware. A continuamos asignaremos las direcciones IP, para las distintas interfaces ***GREEN***, ***RED***, ***BLUE*** y ***ORANGE***.

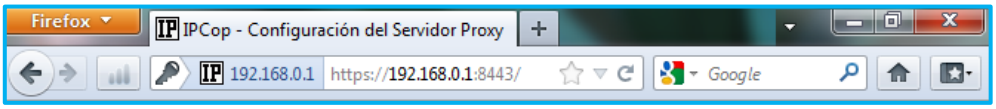
g) A continuación, escribimos una contraseña para el usuario "***admin***". Ya que cuando iniciamos sesión en la interfaz web de IPCop se le pedirá un nombre de usuario y contraseña.

h) Por último, nos pedirá una contraseña para el "***backup***", esto se utiliza para restaurar los archivos del sistema de la copia de seguridad de memorias USB u otros sistemas de archivos. Finalmente pulsamos ***Ok*** para reiniciar el sistema, después del reinicio se ha completado, sin duda la instalación de IPCop. (**VER ANEXO Nº 3, PÁG. 187**)

3.5.3. Configuración de IPCop

Para acceder a la interfaz gráfica del usuario IPCop es tan sencillo como iniciar el navegador e introducir la dirección IP de la interfaz Green, o el nombre de host del IPCop, junto con un director de puerto: ***https://ipcop.localdomain:8443 o https://192.168.0.1:8443***.

GRÁFICO Nº 3.8. ACCESO A LA INTERFAZ GRÁFICA



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Nos solicitara un nombre de usuario y contraseña, utilizaremos "***admin***" como nombre de usuario y la contraseña que elegimos durante la instalación de IPCop.

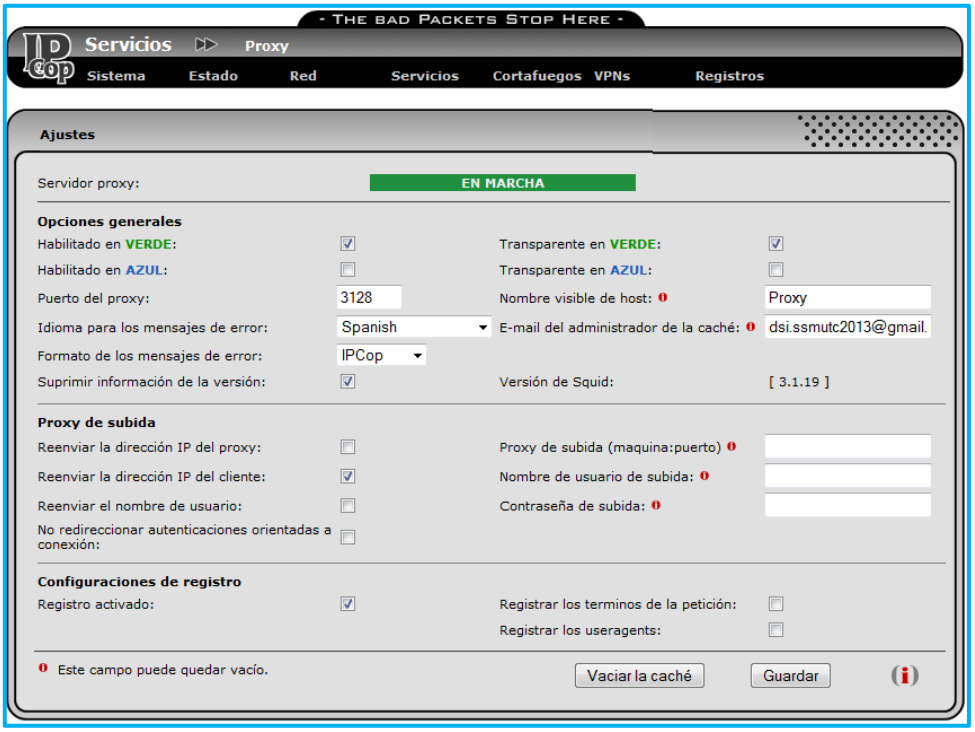
GRÁFICO Nº 3.9. HOME PAGE DE IPCOP

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

3.5.3.1.Configuración de IPCop: Web proxy

En ***Opciones generales*** marcamos ***Habilitado en Green***, esto permite al servidor proxy escuchar las peticiones de los clientes en esta interfaz. En nuestro caso solo tenemos la interfaz ***Green***, luego habilitaremos el modo ***Transparente en Green***, activamos esto para que todas las solicitudes para el puerto de destino 80 (HTTP) sean enviados al servidor proxy sin necesidad de ningún cambio de configuración especial para los clientes.

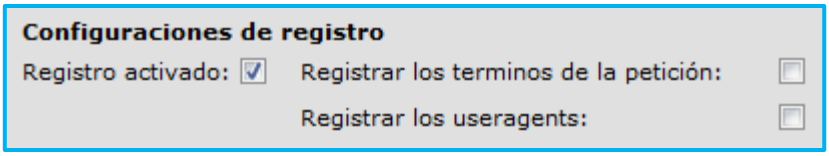
GRÁFICO Nº 3.10. WEB PROXY – CONFIGURACIÓN COMÚN



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Las demás opciones permiten configurar datos de las pantallas de error que aparecerán en nuestros clientes: Nombre del Host, Idioma de los mensajes, información de la versión, y el formato.

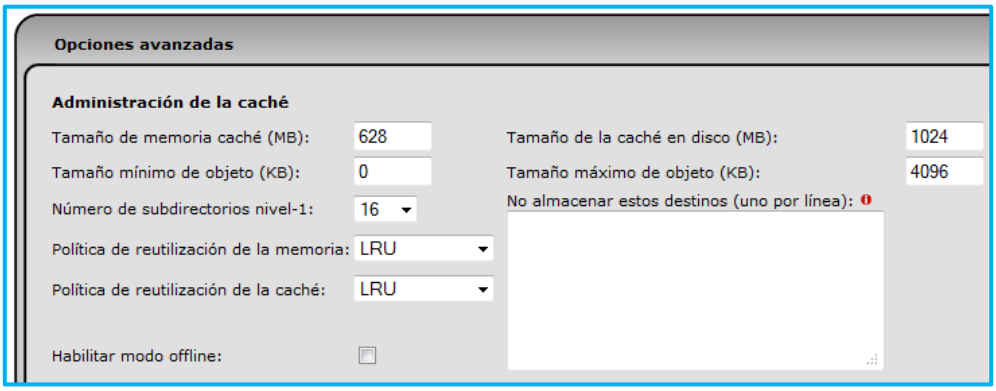
GRÁFICO Nº 3.11. CONFIGURACIÓN DEL LOG



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

La ***administración de la caché*** es un espacio que se utiliza como memoria para agilizar ciertos procesos, aquí es donde se almacenarán páginas y/o documentos web para reducir el ancho de banda consumido y la carga de trabajo del proxy, esto lo hace respondiendo algunas peticiones con información en la caché, para nuestro ejemplo dejaremos los valores por defecto pero en algún caso podríamos incrementar los valores, tomando en cuenta siempre el hardware donde instalamos IPCop.

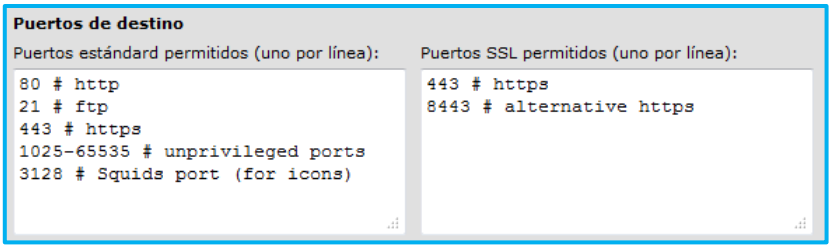
GRÁFICO Nº 3.12. GESTIÓN DE CACHÉ



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

En ***Puertos de destino*** se enumeran los puertos permitidos para HTTP y SSL, aquí podemos añadir o quitar puertos para nuestras aplicaciones, por ahora los que tiene agregados es suficiente para nuestra infraestructura.

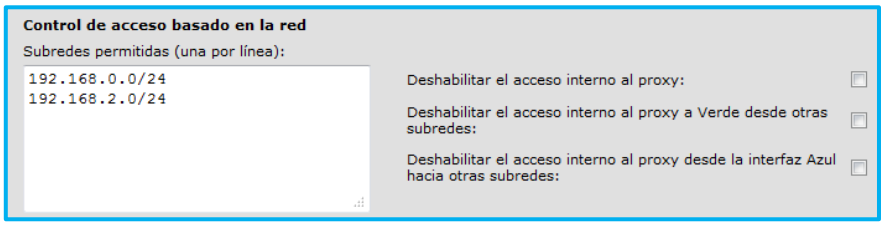
GRÁFICO Nº 3.13. PUERTOS DE DESTINO



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Lo siguiente es el ***Control de acceso basado en la red***, aquí definiremos quienes utilizarán el servidor proxy basado en la dirección de red del cliente, todas las subredes que figuran se les permite acceder al servidor proxy. Por defecto, las subredes de ***Green*** y ***Blue*** si está disponible figuran en esta lista.

GRÁFICO Nº 3.14. RED DE CONTROL DE ACCESO



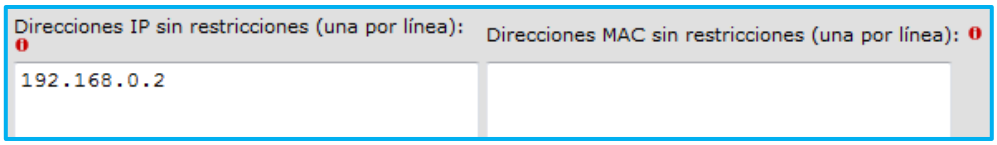
Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Usted puede agregar otras subredes a esta lista en entornos más grandes. Todas las subredes que no figuran en esta lista serán bloqueadas al acceso web, las ***direcciones IP sin restricciones*** anulan las siguientes restricciones:

- Restricciones de tiempo.
- Límites de tamaño máximo de descargas.
- Límite del ancho de banda de descargas.
- Filtros MIME.

Agregare la *IP 192.168.0.2* que es la de ***PC Administrador***, para que no tenga ninguna restricción, cabe destacar que también se pueden agregar direcciones MAC. Las ***direcciones IP Banneadas*** son los clientes que serán bloqueados, y no tendrán ningún acceso al proxy.

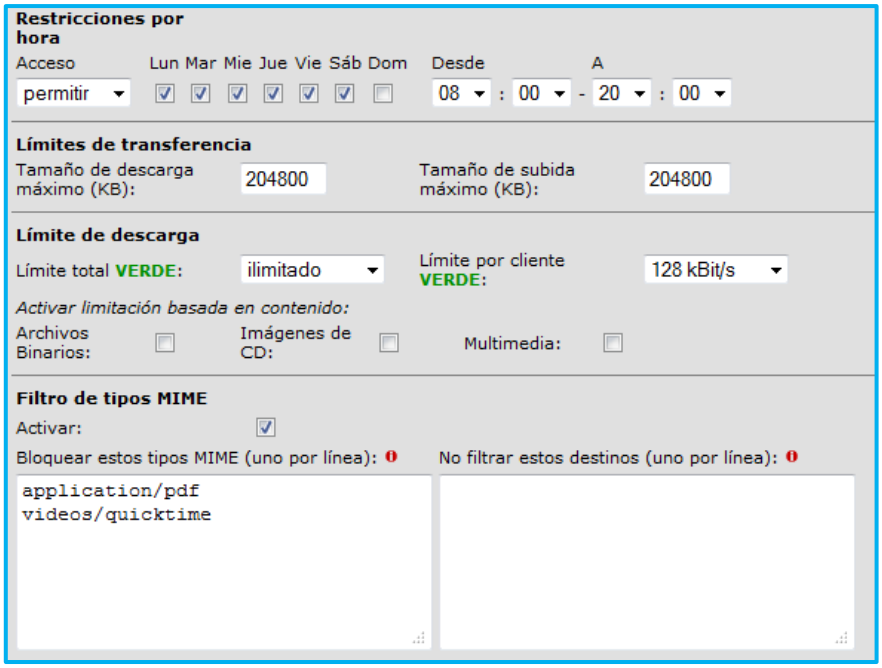
GRÁFICO Nº 3.15. DIRECCIONES IP SIN RESTRICCIONES



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Las ***Restricciones de tiempo*** permiten bloquear el acceso web en días y horas determinadas, en este caso bloquearemos el acceso web el día Domingo y lo permitiremos de lunes a sábado de 8:00 am hasta 20:00.

GRÁFICO Nº 3.16. CONFIGURACIÓN DE RESTRICCIONES



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

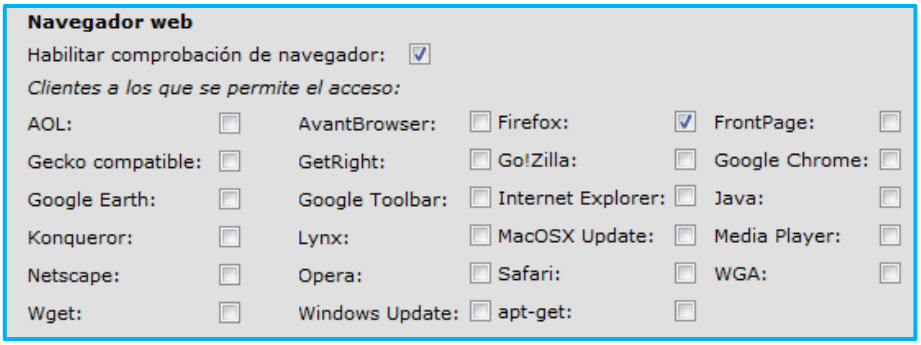
El ***Límite para transferencias*** se refiere al tamaño máximo de un archivo que nos permitirá descargar o cargar, limitaremos el tamaño máximo de una descarga a *204800KB (200MB)* y carga a *204800KB (200MB)* con lo que evitamos que los clientes suban o descarguen archivos que superen los *200 MB*.

La ***Limitación de descargas*** es algo muy útil cuando queremos administrar el ancho de banda, podemos limitar cuanto ancho de banda queremos que utilice cada cliente, en este caso permitiré que al servidor ingrese todo el ancho de banda disponible pero que a los clientes solo se les permita ***128Kbps*** como máximo, también se puede habilitar limites basados en el contenido.

Un ***MIME*** de un archivo es una descripción de lo que es el archivo y que nos sirven para decirle al servidor de que archivo se trata, IPCop nos permite utilizar esta descripción para filtrar contenidos, por ejemplo bloquear la descarga de ***videos quicktime*** y los ***documentos PDF*** utilizando sus respectivos MIME, no debemos olvidar marcar la casilla ***Habilitado***.

Las opciones ***Navegador Web*** permiten controlar con qué software el cliente puede tener acceso a los sitios web. Primero ***Habilitare chequeo de navegador*** y marcaré los programas que podrá usar el usuario para acceder a sitios web, como se ve no podrá ingresar por ejemplo a través de la aplicación de Google Earth y otros, estas limitaciones no se aplican a las IP sin restricción.

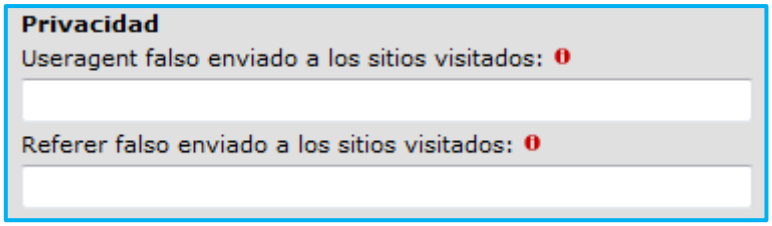
GRÁFICO Nº 3.17. NAVEGADOR WEB



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Las opciones ***Privacidad*** permiten la modificación de algunos campos de la cabecera HTTP para proteger su privacidad, por ahora dejaremos los campos en blancos, por ahora no utilizaremos ningún ***Tipo de Autenticación***.

GRÁFICO Nº 3.18. PRIVACIDAD



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Para que toda la configuración tenga efecto presionamos el botón ***Guardar*** y tenemos el proxy configurado. Ahora configuremos las propiedades del ***protocolo internet TCP/IP*** en la ***PC Administrador*** para poder navegar, naturalmente para los demás clientes la configuración de red será similar cambiando únicamente la dirección *IP (192.168.0.x)*, no olvidemos que la *IP 192.168.0.2* está dentro de las IPs sin restricciones así que configuremos una ***PC Cliente*** con la dirección IP *192.168.0.3* para ver el funcionamiento del proxy. (**VER ANEXO Nº 4, PÁG. 190**)

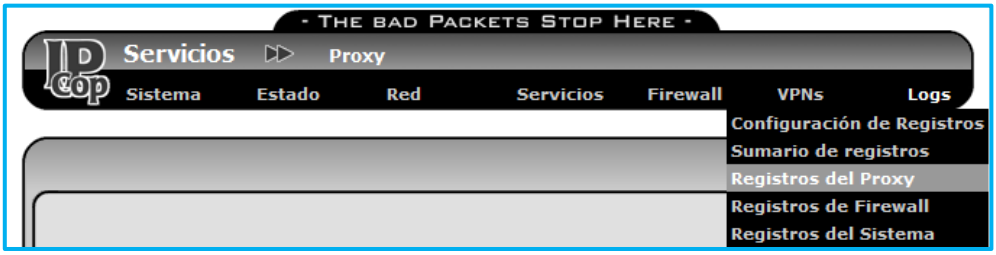
Probemos el ancho de banda, desde la ***PC cliente*** (***192.168.0.3***) utilizaremos el medidor de ***http://speedtest.net/*** que nos servirá como parámetro, recordemos que habilitamos ***128Kbps*** para cada cliente, lo que nos refleja el testeo es bastante cercano a lo deseado (***0.12*1024 = 122.88 Kbps***).

GRÁFICO Nº 3.19. MEDICIÓN DEL ANCHO DE BANDA PC CLIENTE

Fuente: PC Cliente
Realizado por: Investigadores

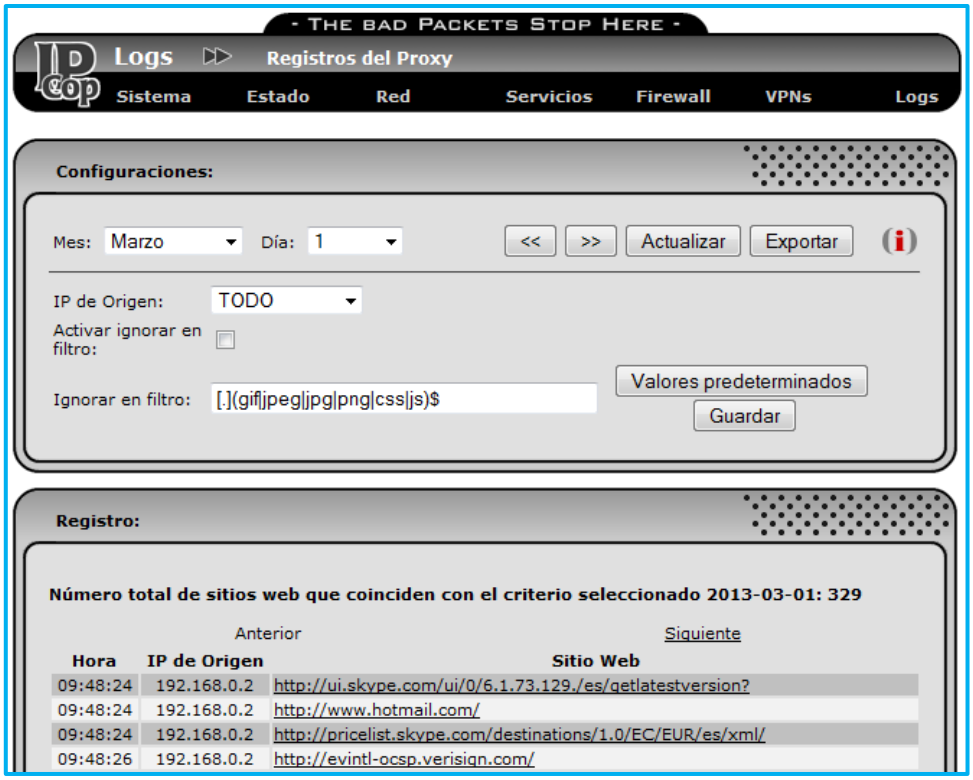
La pantalla de error que nos muestra en el explorador Firefox cuando queremos descargar un ***archivo PDF***, bloqueado con ***filtro MIME***. La pantalla de error que despliega ***Internet Explorer***, es porque no se encuentra en los programas permitidos para acceder a sitios web, y de esta manera aparecerán, en los clientes, las políticas que nosotros implementemos. Para terminar la configuración veremos los registros del Proxy, para lo que elegimos la pestaña ***Logs - Registros del Proxy***.

GRÁFICO Nº 3.20. REGISTRO DEL PROXY



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

GRÁFICO Nº 3.21. REGISTRO DEL PROXY II



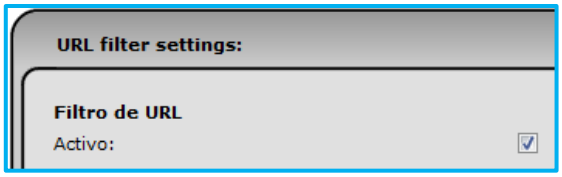
Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Aquí podemos ver las páginas que fueron accedidas por las diferentes direcciones IP de nuestra red, por ejemplo veremos las páginas que accedió la PC con la IP *192.168.0.2*, elegimos en ***IP de Origen*** la IP deseada, la fecha, marcaremos la opción ***Activar ignorar filtro*** para que en los resultados no estén las URL de las imágenes con las extensiones de ***Ignorar filtro*** y clic en ***Actualizar***.

3.5.3.2. Configuración IPCop: URL Filter

Ahora en el administrador web de IPCop actualizamos la página y vamos al siguiente enlace: ***https://192.168.0.1:8443/cgi-bin/urlfilter.cgi***, y activamos la casilla de activación de URL Filter, para poder visualizar en la página web proxy guardamos los cambios efectuados.

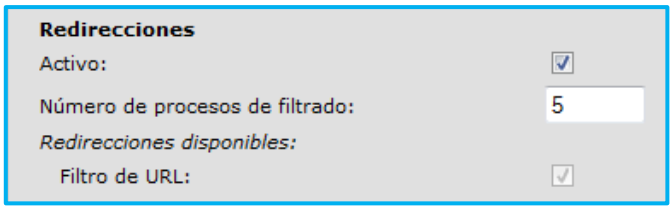
GRÁFICO Nº 3.22. URL FILTER



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Ahora notaremos que dentro de las opciones de ***Web Proxy*** tenemos una nueva opción llamada Filtro de URL, habilitaremos esta opción para que nuestro proxy pueda utilizarlo, y damos clic en ***Guardar***.

GRÁFICO Nº 3.23. REDIRECCIONES



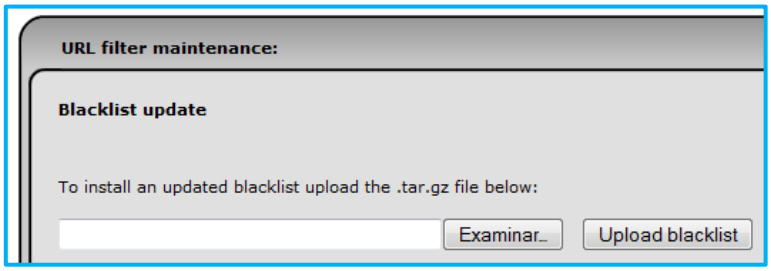
Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Antes de continuar revisemos algunos conceptos que necesitaremos para nuestras configuraciones; Una lista negra o ***blacklist*** es una lista de dominios y URL's que serán bloqueados por algún filtro, esto constituye lo más importante para un filtrado URL, existen varias distribuciones de ***blacklist***, algunas comerciales, otras gratis o una combinación de ambas.

El Filtro URL posee una lista negra que si bien es útil queda de cierta forma corta para un filtrado optimo, por lo que instalaremos una nueva lista negra descargada de ***http://urlblacklist.com***, claro que podrían descargar una más actualizada para instalar. Para instalar esta lista buscamos las opciones en ***Mantenimiento del filtro URL*** y

damos clic en ***Examinar*** de Actualización de la lista negra, direccionamos el archivo ***bigblacklist.tar.gz***.

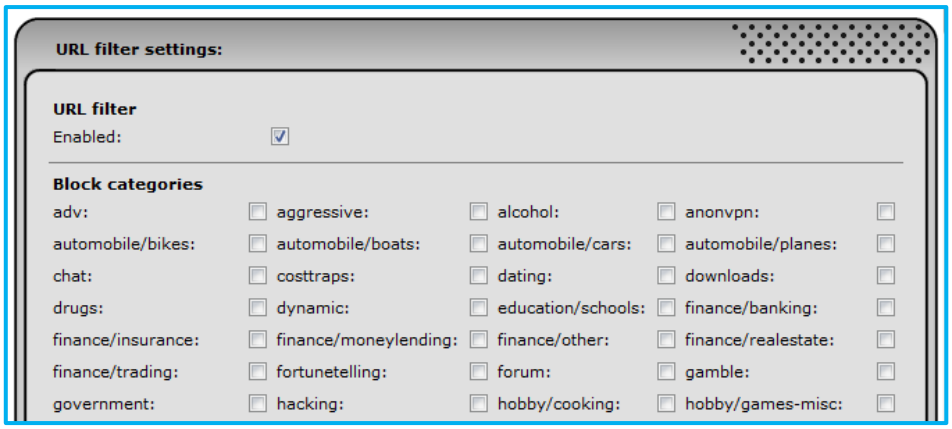
GRÁFICO Nº 3.24. MANTENIMIENTO DEL FILTRO URL



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Una vez encontrado damos clic en abrir, y luego clic en ***Upload blacklist***. Actualizamos el Administrador web y ahora tenemos más categorías para filtrar, ahora bloquearemos algunas categorías, prestemos atención a la categoría ***social_networks***, con esto restringimos el acceso a páginas como facebook o twitter damos clic en ***Guardar***:

GRÁFICO Nº 3.25. CONFIGURACIÓN DEL FILTRO URL



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

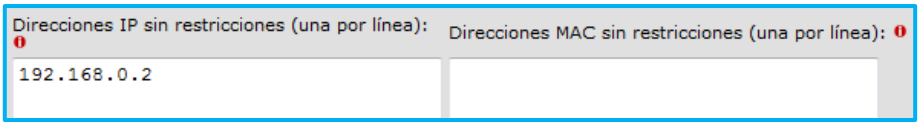
Ahora revisemos algunas opciones que podemos utilizar; por ejemplo las opciones en lista negra personalizada, aquí podemos ingresar dominios o URL's que tal vez no estén dentro de las categorías o que simplemente consideremos bloquear, para ejemplo bloquearemos el dominio ***yahoo.com***, no olvidemos que al "***bloquear el dominio***" cualquier página que contenga todo o parte del mismo estará bloqueada, noten que debemos marcar la opción ***Habilitar*** lista negra personalizada. Ahora al abrir la página ***www.facebook.com*** o ***www.youtube.com***, nos desplegará la pantalla de acceso denegado. (**VER ANEXO Nº 5, PÁG. 191**)

GRÁFICO Nº 3.26. BLOQUEAR EL DOMINIO

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Otra opción que probablemente necesitemos es para levantar las restricciones para determinadas direcciones IP, en este caso la *IP 192.168.0.2* no tendrá las restricciones, también podemos habilitar la restricción por tiempo y la cuota de usuarios.

GRÁFICO Nº 3.27. DIRECCIONES IP SIN RESTRICCIONES II

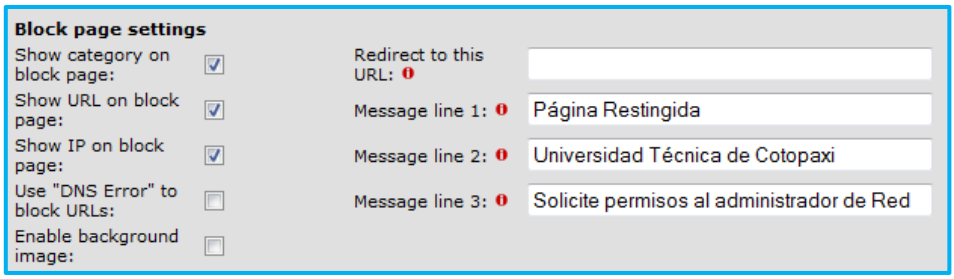


Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Las opciones de ***Configuración de la página de bloqueo*** son para personalizar la pantallas que aparecen en el cliente cada vez que el filtro URL realiza un bloqueo,

aquí marcaremos ***Mostrar URL en la página de bloqueo*** para que muestre al cliente que URL fue bloqueada, también cambiaremos los mensajes para que se muestren en español, también podemos colocar un fondo de pantalla que por ahora no utilizaremos.

GRÁFICO Nº 3.28. CONFIGURACIÓN DE LA PÁGINA DE BLOQUEO



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

En configuración avanzada, habilitaremos el log para tener un registro de los suceso, además marcaremos la opción Bloquear sitios accedidos por su dirección IP, esto es muy importante porque si no está marcado se podrán acceder al algunos dominios a través de sus direcciones IP. Finalmente aplicamos los cambios dando clic en ***Guardar***.

3.6 Módulo para el Monitoreo de la Red

Este módulo tiene como objetivo monitorear permanentemente los host de la Universidad Técnica de Cotopaxi. Este módulo permite adicionalmente monitorear la disponibilidad de los principales servicios manejados por el área de sistemas. Se ha seleccionado como herramienta de monitorización a ***Nagios***, debido a que es estable y ampliamente utilizado en el monitoreo de redes.

Para mejorar la calidad de servicio utilizaremos el siguiente estándar 802.1P, Q – QoS sobre el nivel de MAC de la IEEE, puesto que un administrador puede designar la prioridad del tráfico basado en una variedad de medios, incluyendo la dirección IP o MAC, TCP o UDP número de puerto, etc., para garantizar que la transmisión de paquetes no fallen.

Para hacer posible la implementación de QoS en su totalidad, debemos contar con equipamiento activo que cumpla con las normas y soporte los protocolos desarrollados para tales fines, ya que la calidad de servicio es una de las claves del éxito para el despliegue de las redes convergentes.

Entre las características más relevantes se puede especificar en términos cuantitativos o estadísticos algunos parámetros, tales como: ancho de banda, latencia, utilización de memoria y CPU, pérdida de paquetes en la red, etc.; asegurándonos un grado de fiabilidad preestablecido que cumpla los requisitos de tráfico, en función del perfil y ancho de banda de la institución para un determinado flujo de datos dentro de la red, ya que la calidad de servicio se basa en estándares de funcionalidad QoS.

El desarrollo de un modelo de datos flexible que permita la integración de la gestión de la calidad de servicio en sistemas heterogéneos, y que tenga en cuenta distintos aspectos que influyen en la calidad de un servicio.

3.6.1 Requerimientos del Sistema

En cuanto al Hardware cualquier equipo capaz de ejecutar una variante de Unix, sin necesidad de instalar un entorno gráfico:

TABLA N° 3.2. IMPLEMENTACIÓN DE NAGIOS

REQUERIMIENTOS
Servidor Torre o Rack
Intel Core2Quad 2.0 GHz
1 GB RAM
500 GB Disco Duro
NIC 100/1000 BASE-T

Fuente: Requerimientos de Hardware
Realizado por: Investigadores

En cuanto al software el sistema operativo debe estar basado en una variante de Linux Kernel 2.6.x, se recomienda cualquiera de estas distribuciones Linux.

3.6.2 Instalación de Nagios

Primeramente debemos especificar que no es necesario realizar la instalación de cada uno de los paquetes por separado, para facilitarlo usaremos una distribución de Linux que ya tiene todo preconfigurado, su nombre es Fully Automated Nagios y está basada en CentOS actualmente en la versión 5.7

La forma de instalar FAN Nagios, se indica a continuación:

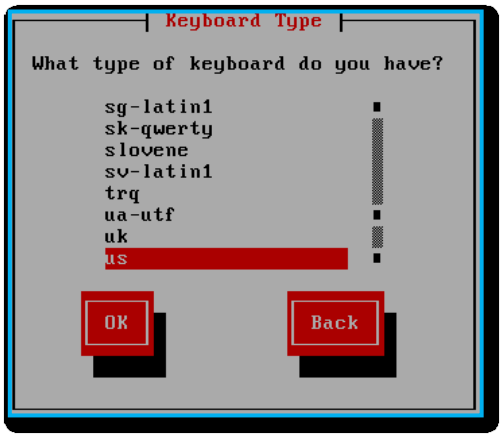
a) Descargamos la imagen ISO de la distribución FAN Nagios, disponible en: ***http://fanNagioscd.sourceforge.net/drupal/?q=node/11*** y grabamos en un CD, e iniciamos el ordenador desde el CD en la máquina destinada a monitorear y presionamos ***ENTER*** para empezar la instalación:

GRÁFICO Nº 3.29. PANTALLA PRINCIPAL DE FAN NAGIOS

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

b) Seleccionamos el idioma que se desea utilizar para instalar FAN Nagios y presionamos ***ENTER*** para continuar con la instalación, de igual manera seleccionamos el diseño del teclado que se desea utilizar y presionamos ***ENTER*** para continuar.

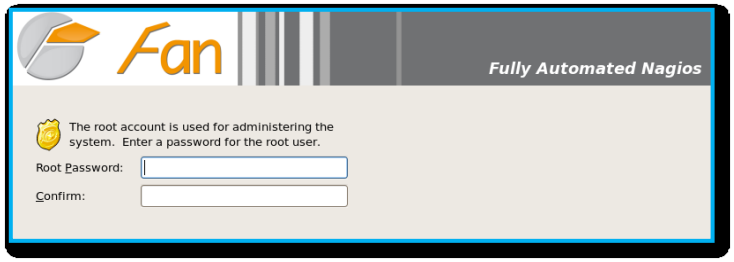
GRÁFICO Nº 3.30. SELECCIÓN DEL DISEÑO DEL TECLADO



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

c) Seleccionamos por defecto el particionado recomendado para la instalación de FAN Nagios y presionamos ***NEXT***, de igual manera seleccionamos la zona horaria que se encuentra en la lista y presionamos ***NEXT***, luego introducimos la contraseña del administrador (***root***), y presionamos ***NEXT*** para continuar.

GRÁFICO Nº 3.31. ASIGNACIÓN DEL PASSWORD



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

d) Una vez finalizada la instalación e iniciado el sistema, será necesario gestionar algunas configuraciones, para lo cual invocaremos el comando "***setup***" y elegiremos la opción ***Network Configuration***, y seleccionamos la opción ***Edit Devices*** y configuramos lo siguiente:

IP address:	172.16.10.100
Netmask:	255.255.255.0
Default Gateway:	172.16.10.1

e) A continuación introducimos el nombre del host, para lo cual utilizaremos el comando "***setup***", elegiremos la opción ***Network Configuration*** y seguidamente la opción ***Edit DNS Configuration***, guardamos los cambios y reiniciamos nuestro servidor de monitoreo.

Hostname:	smutc
Primary DNS:	172.16.10.1
Secondary DNS:	8.8.8.8

3.6.3 Configuración de Nagios a través de Centreon

Para empezar el monitoreo de la red de la Universidad Técnica de Cotopaxi es de vital importancia saber que equipos o hosts son los que van a ser monitoreados, así como los servicios que serán monitoreados de dichos equipos. Routers, switches, servidores, hosts particulares, todos estos pueden ser monitoreados, y su información presentada de manera ordenara gracias a los complementos de ***Centreon***.

Para empezar a usar el complemento ***Centreon*** debemos acceder a la interfaz gráfica del usuario desde un navegador web e introducir la dirección IP, o el nombre de host de ***FAN Nagios***: ***http://localhost/centreon o http://172.16.32.103/centreon***, para poder ingresar al sistema de monitoreo tenemos que introducir el nombre de usuario y contraseña, escogidos durante la instalación, que en este caso es ***login:*** *nagiosadmin*, y ***password:*** *xxxxxx*.

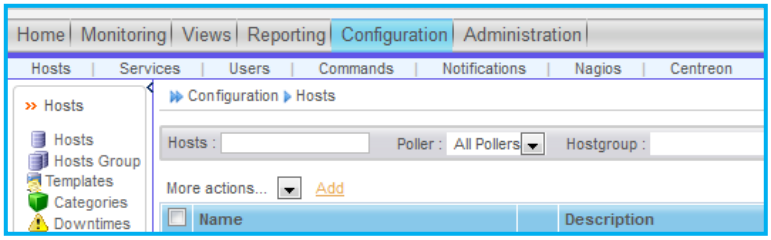
GRÁFICO Nº 3.32. PÁGINA DE INICIO DE CENTREON

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

3.6.3.1 Configuración de Hosts

a) Para agregar los hosts al sistema de monitoreo entramos al menú "***Configuration***", y damos clic en el apartado de "***Hosts***", seguidamente damos clic en la opción de "***Add***" para agregar un nuevo host:

GRÁFICO Nº 3.33. INGRESO DE HOSTS



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

b) Esto nos llevará a la pantalla de configuración del equipo, aquí es donde se le asignará la información necesaria para su correcto funcionamiento, se recomienda que todos los hosts partan del template "***generic-host***":

1) Host Name: Especificamos el nombre con el que se le conocerá al equipo tanto en Centreon, como en Nagios. El nombre en este campo debe de ser único, por lo que ningún otro equipo puede tener el mismo nombre.

2) Alias: Este campo es opcional y solo sirve para definir un nombre más largo, o para anexar una descripción pequeña del equipo.

3) IP Address/DNS: Agregamos la IP del equipo que deseemos monitorear.

4) SNMP Community & versión: Para que el equipo pueda responder a las peticiones es necesario que tenga SNMP habilitado, en este campo

podemos especificar la comunidad y la versión de SNMP del equipo para que haya respuesta por parte del Host.

5) ***Check Period:*** Define el horario en el cual se harán chequeos del HOST. ***24x7*** significa que se harán chequeos a todas horas. ***Workhours*** es solo para horas de trabajo, lo opuesto para ***Non workhours***. ***None*** significa que nunca hará chequeos.

6) ***Check command:*** Es el comando que utilizará para hacer los chequeos.

7) ***Actice/Passive Checks Enabled:*** Nos permite definir si queremos chequeos activos o pasivos. Un chequeo se considera activo si fue iniciado por Nagios. Un chequeo será pasivo cuando sea iniciado por un proceso externo, sin embargo los resultados son presentados a Nagios para que sean procesados.

8) ***Notification:*** Aquí especificaremos si deseamos que el Host mande notificaciones. (**VER ANEXO Nº 6, PÁG. 192**)

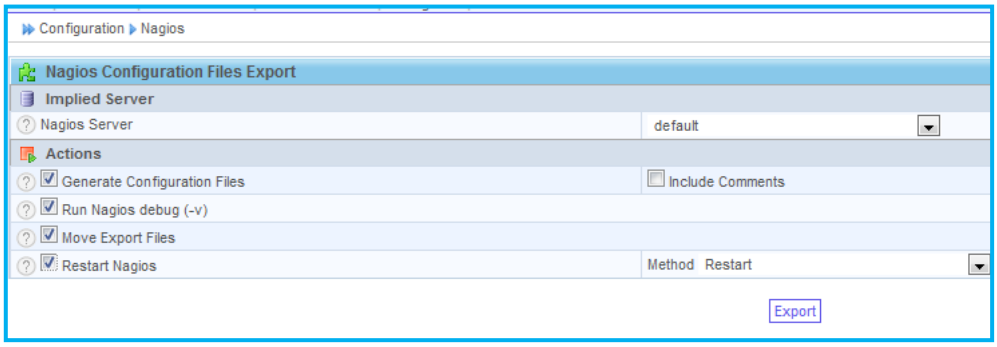
3.6.3.2 Guardando los cambios en Nagios

Cuando dimos clic en "***Save***", guardamos los cambios y el host quedo agregado a Centreon, sin embargo este equipo no podrá ser monitoreado por Nagios a menos que recompilemos los archivos de configuración. Por suerte Centreon cuenta con una función para reconstruir los archivos y reiniciar Nagios, de manera que los cambios estén disponibles en el sistema.

a) Para reconstruir los archivos de Nagios nos vamos al menú "***Configuration***", seguidamente a ***Nagios***, para crear la nueva configuración habilitamos la

casilla de "***Move Export Files***" y "***Restart Nagios***". Posteriormente damos clic en "***Export***":

GRÁFICO Nº 3.34. RESTAURAR LOS ARCHIVOS A NAGIOS



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

b) Nagios creará los nuevos archivos de configuración y desplegará un Log, si el Log contiene errores, será necesario corregirlos antes de que Nagios sea capaz de reconstruir los archivos de configuración. (**VER ANEXO Nº 7, PÁG. 193**)

3.6.3.3 Opciones de hosts

En el menú de "***More actions***" existen más opciones disponibles aparte de "***Massive Change***", todas estas funciones se aplican a los host seleccionados.

1) ***Duplicate:*** Esta opción crea un duplicado de los hosts seleccionados. Estos duplicados conservan los mismos atributos con excepción del nombre, al cual se le anexa un "_1" para diferenciar al duplicado del original.

2) ***Delete:*** Elimina los hosts seleccionados, debemos tener mucho cuidado al utilizar esta opción, ya que una vez eliminados los hosts no podemos recuperarlos.

3) ***Enable:*** Esta opción habilita al host.

4) ***Disable**:* Deshabilita los hosts seleccionados.

3.6.3.4 Configuración de Servicios

Una vez que los hosts estén dados de alta, el siguiente paso es monitorear el mayor número de información posible de ellos. Nagios no cuenta con un modo de discovery, por lo que tendremos que especificarle la información que queramos que tome de cada equipo.

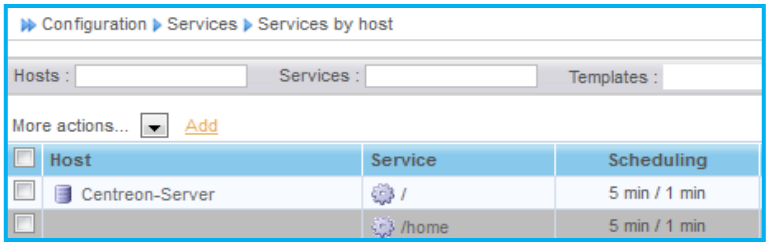
Un ***servicio*** es un comando que ejecuta Nagios diariamente para obtener información de un host por medio del SNMP. La frecuencia con la que hace estos chequeos está definida en los hosts en la casilla de "***Normal check interval***". Estos servicios después de recibir información, la presentan por medio de Nagios.

Algunos servicios comunes son el ***Ping***, que pingea al host para obtener una respuesta, ***CPU***, que obtiene la utilización de CPU de los servidores, ***Traffic***, que obtiene el tráfico que está entrando y saliendo por una interfaz que le especifiquemos y ***C:/*** que nos dice la ocupación del disco duro de un servidor compatible.

3.6.3.5 Agregando servicios por host

a) Para agregar un nuevo servicio a un host nos vamos a ***Configuration***, seguidamente a ***Services***, seleccionamos ***Services by host***, y damos clic en ***Add***, esto nos llevará a la página de configuración principal para los servicios, su configuración es parecida a la de los hosts, sin embargo tienen detalles que son únicos para la configuración de los servicios.

GRÁFICO Nº 3.35. AGREGANDO SERVICIOS A LOS HOSTS



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

1) ***Description:*** Es la manera con que identificaremos el servicio, se le puede dar un nombre o alguna descripción de lo que hará el servicio.

2) ***Service Template:*** Nos permite basarnos en una configuración antes creada, que dará valores a los campos de la configuración.

3) ***Is Volatile:*** Nos permite definir si el servicio será o no volátil, un servicio volátil es aquel que después de cada reporte, reinicia su valor a OK.

4) ***Check Period:*** Especifica los horarios en lo que se harán chequeos al servicio.

5) ***Check command:*** Los chequeos de los servicios funcionan por medio de comandos.

6) ***Args:*** Nos permite establecer los parámetros que necesita el comando para funcionar.

7) ***Active checks enabled/Passive checks enabled****:* Especifica si se van a utilizar o no chequeos pasivos y activos.

8) ***Notification Enabled:*** Definimos si queremos que el servicio mande notificaciones a sus contactos en caso de que encuentre un estado anormal. La funcionalidad es semejante a las notificaciones de host, pero difiere en los estados que anuncia, donde un host anuncia estados como "***Down***" si el host está apagado o "***Recovery***" si está en recuperación, los servicios mandan notificaciones si sus servicios están en un estado de "***Warning***", "***Critical***" o "***Unknown***".

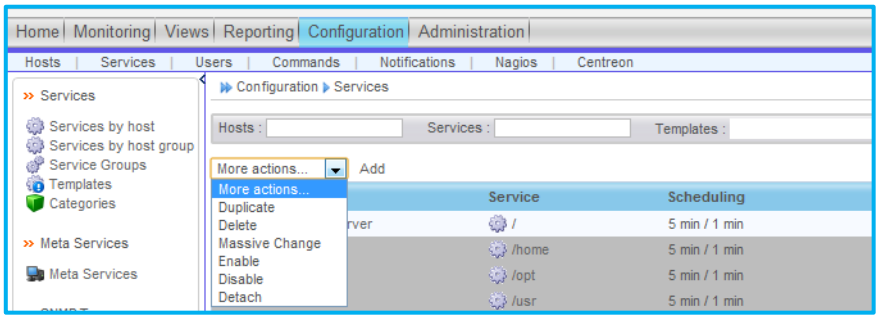
9) ***Notification Interval:*** Es el tiempo en minutos entre cada notificación del servicio. (**VER ANEXO Nº 8, PÁG. 194**)

b) Para reconstruir los archivos de Nagios, procedemos como se hizo anteriormente en la exportación de archivos de configuración para los hosts.

3.6.3.6 Opciones de servicios

Las opciones de ***Duplicate***, ***Delete***, ***Enable*** y ***Disable*** funcionan igual para los servicios.

GRÁFICO Nº 3.36. MASSIVE CHANGE



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

3.6.3.7 Creando el comando para checar el tráfico de red

Para crear un comando nos vamos a ***Configuration***>***Commands***, y damos clic en la opción de "***Add***" para agregar un nuevo comando, e ingresamos la siguiente información: El nombre no es nada especial, es simplemente una forma de reconocer el servicio, el comando que utilizamos es:

$USER1$/check_centreon_snmp_traffic –H $HOSTADDRESS$-C $_HOSTSNMPCOMMUNITY$ -i $ARG1$ -n

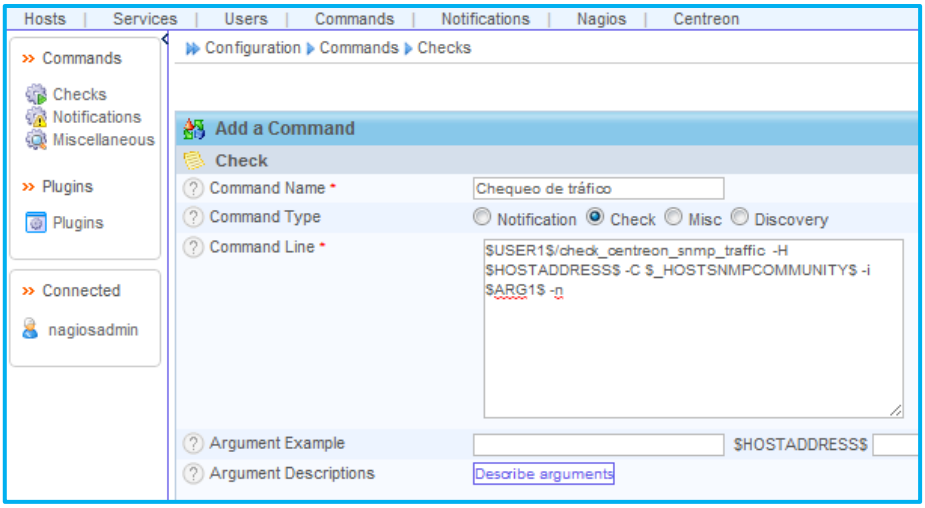
- ***$USER1$:*** Es el directorio en el que se encuentran los plugins de nuestro servidor de seguridad y monitoreo.
- ***check_centreon_snmp_traffic:*** Este es el plugins específico que usaremos para recolectar la información del tráfico.

- ***-H $HOSTADDRESS$:*** Esta opción nos indica el host al que se aplicará el comando.

- ***-C $_HOSTSNMPCOMMUNITY$:*** Indica la comunidad de SNMP.

- ***-i $ARG1$ -n:*** La opción "***–i***" es para indicar la interfaz de la que se quiere obtener la información del tráfico. "***$ARG1$***" representa un argumento que tenemos que definir cada vez que creamos un servicio, en cuanto a la opción *"**-n**"*, hay 2 maneras por las que se le conoce a una interfaz: por su OID (Object ID) y por el nombre de su interfaz.

GRÁFICO Nº 3.37. INGRESAR LOS ARGUMENTOS DEL COMANDO



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Para finalizar damos clic en el botón de *"**Save**"* que se encuentra en la parte inferior de la página web. Para ver los cambios que acabamos de hacer tenemos que reiniciar Nagios. Una vez que se haya reiniciado, es necesario darle tiempo para que el nuevo servicio entre a la fila del Nagios, una vez que sea su turno empezaremos a recibir una respuesta: La primera vez que se ejecuta un chequeo de tráfico, se crea un buffer, es hasta el siguiente chequeo que empezamos a recibir información de la interfaz.

Ahora si podremos observar el tráfico que está entrando y saliendo por dicha interfaz. Esta información se muestra en función de la unidad más cercana, sean Mb, Kb o hasta Bytes por segundo.

3.6.3.8 Creando el comando para revisar la utilización del CPU

Si se cuenta con Hosts en la red que se está monitoreando, es posible obtener el porcentaje del CPU que se está utilizando, también es posible saber cuánta memoria se está utilizando. Primero vamos a empezar configurando un servicio que nos mida

la utilización del CPU, para configurar el comando le agregamos la siguiente información:

$USER1$/check_snmp_load.pl -H $HOSTADDRESS$ -C $_HOSTSNMPCOMMUNITY$ -T $ARG1$ -w $ARG2$ -c $ARG3$ -f

- ***$USER1$:*** Para empezar agregamos ***$USER1$*** para que acceda al directorio de plugins.

- ***Check_snmp_load.pl:*** Este plugins nos permite checar la utilización del CPU de un equipo determinado.

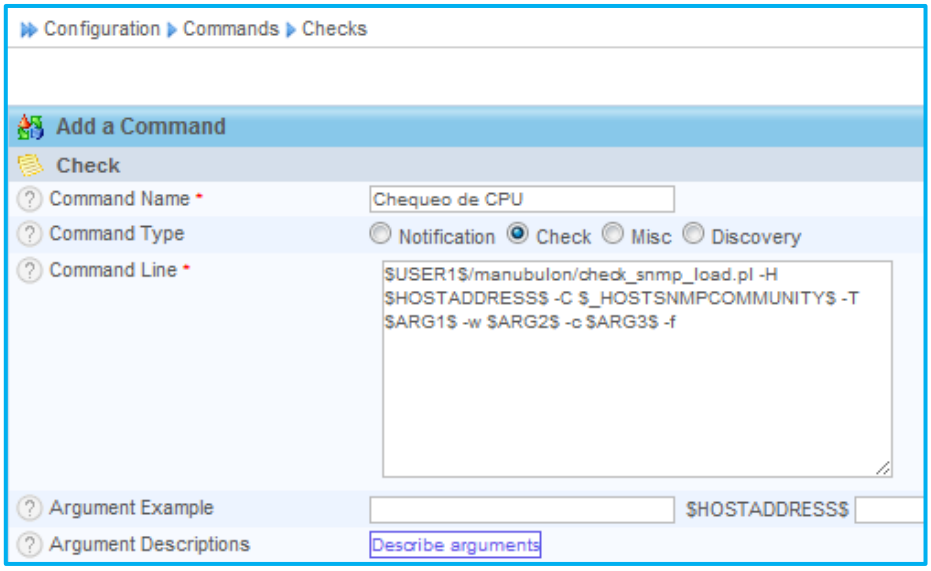
- ***-H $HOSTADDRESS$ -C $_HOSTSNMPCOMMUNITY$:*** Nos permiten obtener la dirección IP del host, así como la comunidad de SNMP que le hayamos incluido en la configuración.

- **-T $ARG1$:** Con esta opción le indicamos la marca del equipo al cual aplicaremos el chequeo.

- **-w $ARG2$ -c $ARG3$:** "**-w**" y "**–c**" especifican los niveles en los que el servicio mandará una advertencia o un estado crítico respectivamente.

- **-f:** Hay servicios que mandan información llamada "Performance Data". Este tipo de información tiene la característica de que puede ser almacenada por Centreon y posteriormente utilizada para crear graficas de desempeño.

GRÁFICO Nº 3.38. AGREGAR UN NUEVO COMANDO



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Finalmente damos clic en *"**Save**"*, y una vez que reiniciemos Nagios le damos tiempo para que se reconstruya este nuevo servicio, con el pasar del tiempo podremos visualizar la información obtenida de la utilización del CPU dentro de la interfaz web de Centreon.

3.6.3.9 Creando el comando para revisar la utilización de memoria

Lo primero que haremos será crear el comando para chequear la memoria, antes de continuar vamos a mencionar que la función que estamos a punto de configurar ya está definida en la instalación de FAN Linux, el comando que necesitamos se llama ***"check_centreon_memory"***, al cual vamos agregarle la siguiente información:

$USER1$ check_centreon_memory -H $HOSTADDRESS$ -C $_HOSTSNMPCOMMUNITY$ -w $ARG1$ -c $ARG2$ -I -f

- ***$USER1$:*** Esta línea la ocupamos para definir el directorio en donde se encuentra el plugins, así como el plugins que usaremos que en este caso es "***check_centreon_memory***".

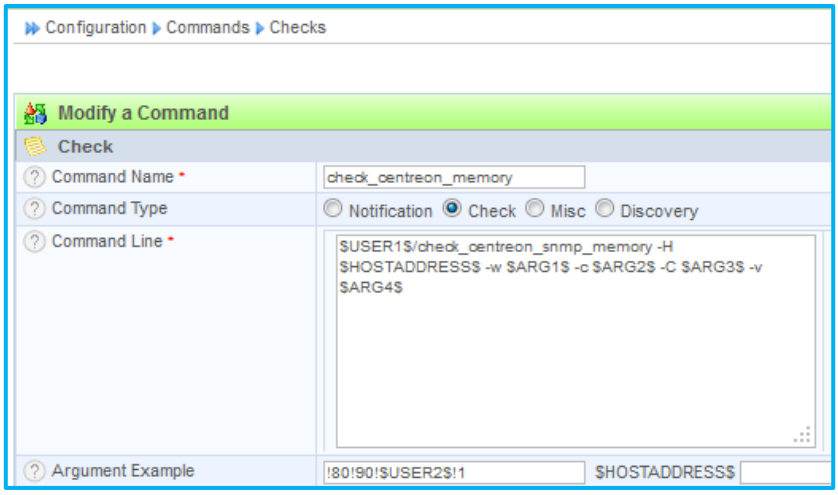
- ***-H $HOSTADDRESS$ -C $_HOSTSNMPCOMMUNITY$:*** Con estas 2 opciones hacemos que nuestro comando tome la dirección IP y la comunidad SNMP.

- ***-w $ARG1$ -c $ARG2$:*** Este par de opciones nos permite especificar, en porcentaje, el punto en el cual el servicio mandará una advertencia y el punto en el cual será considerado crítico.

- ***-I:*** Para este comando también se le tiene que indicar la marca del equipo, sin embargo este opera diferente.

- **-f:** Esta opción permite que el comando genere Performance Data para poder ser graficado más adelante.

GRÁFICO Nº 3.39. AGREGAR UN NUEVO COMANDO II



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

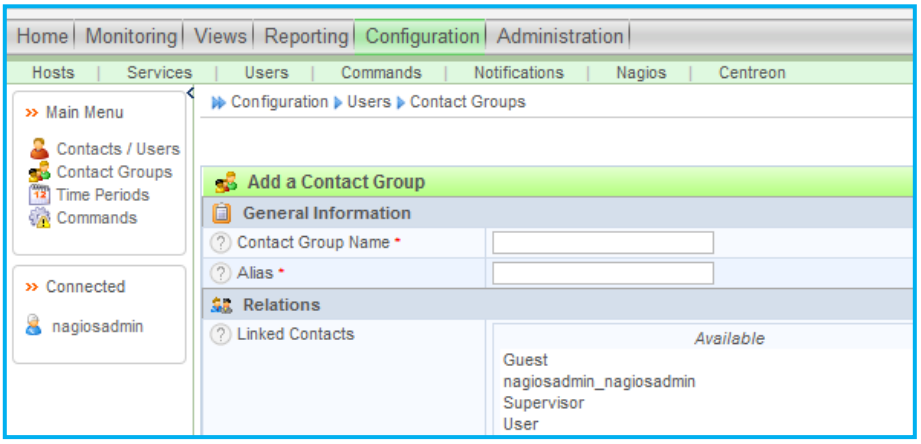
Para continuar hacemos los mismos pasos que realizamos para el chequeo de la utilización del CPU, y para finalizar le damos clic en ***"Save"***, guardamos la configuración y reiniciamos Nagios, después de un tiempo podremos visualizar la utilización de la memoria.

3.6.3.10 Creando grupos de contacto en Centreon

Antes de empezar a definir a los usuarios, es necesario crear los grupos de contacto a los que van a pertenecer, ya que tener grupos de contactos nos facilita la configuración de las notificaciones de los servicios, ya que se pueden mandar avisos al grupo que corresponda, una alerta de exceso de tráfico, por dar un ejemplo.

a) Primero vamos a crear un grupo de administradores, este tipo de usuario tendrá acceso a todos los aspectos del sistema, así como a su configuración. Para crear un grupo de Contacto nos vamos a "***Configuration***", seguidamente a "***Users***", y luego a "***Contact groups***", y le damos clic en "***Add***":

GRÁFICO Nº 3.40. AGREGAR UN NUEVO GRUPO DE USUARIOS



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Seguidamente agregamos la siguiente información:

1) ***Contact Group Name:*** Nombre del grupo de Contacto.

2) ***Alias:*** Una descripción, puede ser del tipo de usuarios que habrá en el grupo, de sus funciones, etc.

3) ***Linked Contacts:*** En este apartado señalamos que usuarios son los que pertenecerán al grupo de contacto. Para formar parte del grupo también es posible que se especifique este grupo en el momento que se esté creando el contacto.

4) ***Status:*** El estado del grupo, por medio de esta opción podemos habilitar o deshabilitar el grupo de contacto.

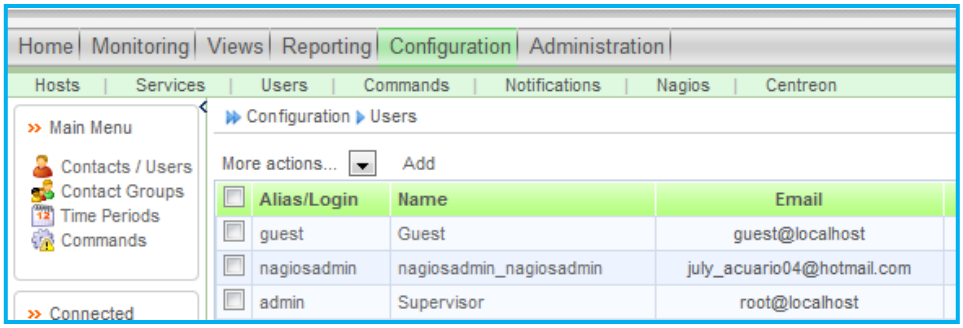
5) ***Comments:*** Comentarios adicionales acerca del grupo, la información que va en esta casilla es opcional.

b) Para finalizar le damos clic en "**Save**".

3.6.3.11 Creación de nuevos usuarios en Centreon

a) Ahora que nuestro grupo de contacto está definido, es tiempo de que creemos a los usuarios. Para crear un nuevo usuario nos vamos a "***Configuration***", seguidamente a "***Users***", después a "***Contacts***", y finalmente a "***Users***", e ingresamos los datos del contacto:

GRÁFICO Nº 3.41. AGREGAR UN NUEVO USUARIO



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

1) ***Full name:*** En esta casilla se escribe el nombre completo del usuario.

2) ***Alias/Login:*** Este es el nombre de usuario con el que va a ingresar al Centreon.

3) ***E-mail:*** El correo electrónico del usuario. Esta dirección de correo es utilizada por el sistema para mandar notificaciones a los contactos relacionados con un servicio, cuyo estado se encuentre crítico según los parámetros definidos.

4) ***Pager*****:** Especifica un número o dirección de contacto para el usuario.

5) ***Contact template used:*** Especifica el template en el que se basará la información de usuario.

6) ***Linked to Contact Groups:*** Si un usuario no fue agregado a un grupo de contacto a la hora de haber configurado dicho grupo, puede usarse esta opción para agregar el grupo o grupos a los que pertenezca el usuario.

7) ***Enable Notifications:*** Centreon puede enviar notificaciones a los usuarios si es que algún servicio llegara a presentar un estado anormal.

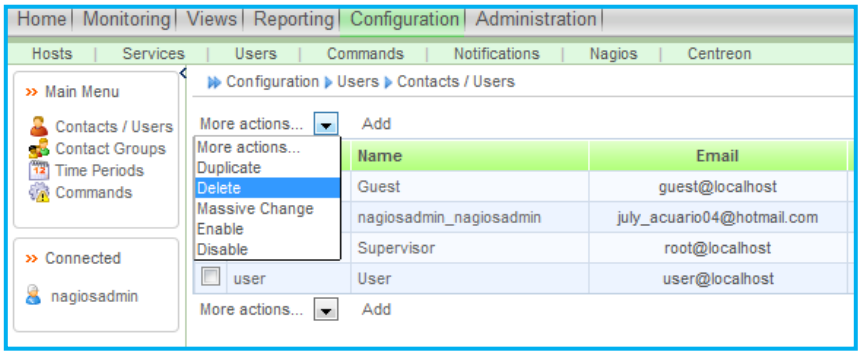
8) ***Host Notification Options:*** Aquí definiremos que estados anormales queremos que nos informe el Centreon en caso de que se presentaran en alguno de nuestros hosts.

9) ***Service Notification Options:*** De la misma manera que definimos cuales estados de los hosts queremos que manden notificaciones a este usuario, podemos configurar qué estados de los servicios queremos que manden notificaciones. (**VER ANEXO Nº 9, PÁG. 195**)

3.6.3.12 Eliminando a un usuario existente en Centreon

a) Para eliminar un usuario primero nos vamos a nuestra lista de usuarios en "***Configuration***", seguidamente a "***Users***", y finalmente a "***Contacts/Users***", y seleccionamos el usuario que deseamos eliminar, damos clic en "***More actions***" y seleccionamos "***Delete***":

GRÁFICO Nº 3.42. ELIMINAR UN USUARIO SELECCIONADO



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

3.7 *Módulo de Alertas y Reportes*

Este módulo ofrece un elemento de seguridad pasiva, esto significa que no evitan una situación anormal dentro de la red, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas. Una vez que las notificaciones se activan dependiendo del sistema instalado, este puede tomar acciones en forma automática.

3.7.1 Notificaciones por E-mail

Una de las funciones más interesantes de Nagios es la notificación de los eventos de la red. Una avería en una línea no es difícil de detectar, suelen ser los usuarios los primeros en quejarse. Pero una caída de un servicio que en ese momento no se está usando es más complicada de ver.

Para no tener que estar todo el día mirando el monitor del Nagios, existe la opción de crear contactos y que se les notifiquen los eventos de la manera que se elija. Obviamente la herramienta más común para estas notificaciones será el correo, ya que no todas las empresas o instituciones disponen de una pasarela de envío de SMS o similar. (**VER ANEXO Nº 10, PÁG. 196**)

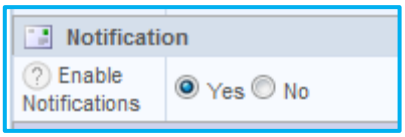
3.7.1.1 Configuración de notificaciones por E-mail

Una vez que el sistema contenga hosts y servicios, es tiempo de hacer que mande notificaciones para alertar si algo está fallando. Este proceso requiere de dos etapas diferentes: En la primera tenemos que definir las notificaciones que el usuario recibirá, cuando se habla de hosts entonces debemos de especificar qué estados nos interesa que manden notificaciones, sea UP, DOWN, UNREACHABLE, etc.

Aparte se establece el horario en el que recibe notificaciones, así como el comando que utilizará el CLI para enviar el correo. La segunda etapa es ir a la configuración de los hosts y servicios y autorizar que ellos también sean capaces de mandar notificaciones, así como especificar cuáles van a mandar.

a) Empecemos por la primera etapa, para ajustar la configuración de notificaciones nos vamos a: ***Configuration***>***Users***, y damos clic en el nombre de usuario que queramos modificar, en esta ocasión modificaremos al usuario ***nagiosadmin***, y ponemos atención a la sección "***Notification***", lo primero es que nos aseguremos de que el usuario pueda recibir notificaciones:

GRÁFICO Nº 3.43. ACTIVAR NOTIFICACIONES

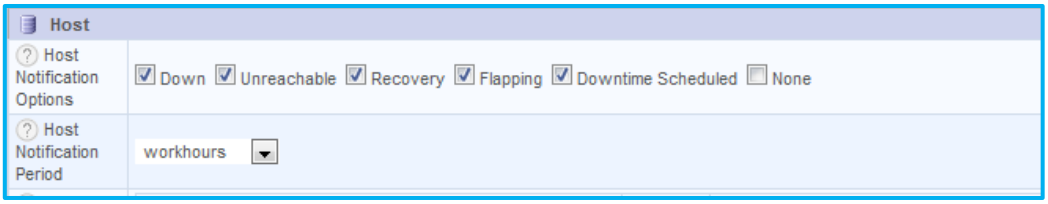


Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

Ahora solo resta que le especifiquemos que estados nos interesan tanto de los hosts como de los servicios a través del comando ***host-notify-by-email***, los estados de los Hosts pueden ser: Down, Unreachable, Recovery, Flapping, y Downtime Schedules.

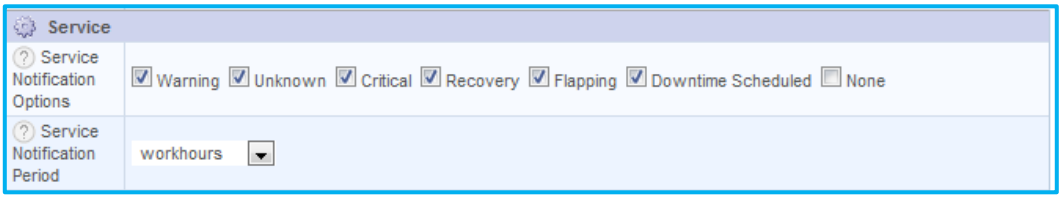
A continuación le especificamos en que horario va a recibir notificaciones. Aun cuando un host esté programado para mandar notificaciones las 24 horas, si el usuario no tiene registrada esa hora, entonces no llegará nada de correo a su bandeja de entrada. En cuanto a los servicios, los parámetros son similares, con la única diferencia siendo que los estados que pueden mandar notificaciones son diferentes.

GRÁFICO Nº 3.44. ACTIVAR ESTADOS DE HOSTS



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

GRÁFICO Nº 3.45. ACTIVAR SERVICIOS DE HOSTS



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

b) Para finalizar le damos clic en "***Save***" y reiniciamos nuestro servidor de monitoreo de la manera antes descrita.

3.7.2 Notificaciones por SMS

Es muy sencillo integrar el envío de SMS en las notificaciones de Nagios, para lo cual se empleara una herramienta denominada "SMS Server" que puede actuar como un servidor de SMS, se ha desarrollado para enviar y recibir mensajes cortos usando módems GSM o teléfonos móviles.

Puede ser usado para mensajes de texto con 7, 8 y 16 caracteres Juego de bits, así como para mensajes binarios, para enviar mensajes cortos, es necesario crear un simple archivo de texto en un directorio de cola. El programa supervisa ese directorio

y envía automáticamente los archivos nuevos, los mensajes recibidos se almacenan en archivos de texto en otro directorio de cola.

El programa se ejecuta en cualquier versión de Linux y Unix, solo se necesita de un compilador C para crear el programa (por ejemplo gcc), constituye un importante avance a la hora de enviar notificaciones de carácter relevante garantizando la autenticidad y confidencialidad en las transacciones, así como la integridad de los contenidos y las fechas de envío y acuse de recibo. (**VER ANEXO Nº 11, PÁG. 197**)

3.7.2.1 Instalación de SMS Server

Antes de comenzar con la instalación del SMS Server, herramienta de utilidad para enviar alertas a través de SMS a teléfonos móviles. Debemos conectar un módem GSM con una tarjeta SIM válida en el servidor a través del puerto USB. La manera de instalar SMS Server, se indica a continuación:

a) Descargamos el paquete ***smstools-2.2.20.tar.gz***, disponible en: ***http:// stefanfrings.de/smstools/index-en.html*** y guardamos en nuestro computador.

b) Una vez que hayamos descargado el paquete, utilizaremos una herramienta muy útil denominado ***WinSCP*** que es una aplicación de software libre para facilitar la transferencia segura de archivos entre nuestro sistema operativo Windows y nuestra distribución basada en Linux.

c) Iniciamos ***WinSCP***, en ***Host name*** colocamos la dirección IP del servidor de monitoreo (*192.168.1.3*) el ***Port number:*** *22*, que es el puerto que utiliza FAN Nagios, como ***User name:*** *root* y el ***password:*** *xxxxxx*, que asignamos al momento de la instalación.

d) Después que hayamos ingresado a nuestro servidor de monitoreo, a través de ***WinSCP***, seleccionamos el paquete ***smstools-2.2.20.tar.gz*** y lo transferimos hacia la siguiente ruta ***/root***. (**VER ANEXO Nº 12, PÁG. 198**)

e) Nuevamente hacemos uso de otra herramienta de software libre, denominado ***PuTTY*** que es un cliente de red que soporta protocolo SSH que utilizaremos para iniciar sesión de forma remota a nuestro servidor de monitoreo.

f) Iniciamos ***PuTTY***, en ***Host name*** colocamos la dirección IP del servidor de monitoreo (*192.168.1.3*) el ***Port number:*** *22*, que es el puerto que utiliza FAN, como ***User name:*** *root* y el ***password:*** *xxxxxx* que asignamos al momento de la instalación. (**VER ANEXO Nº 13, PÁG. 199**)

g) Una vez que estamos conectados remotamente al servidor de monitoreo a través de ***PuTTY***, descomprimimos el paquete ***smstools-2.2.20.tar.gz*** ejecutando el siguiente comando:

 # tar-xvzf smstools-2.2.20.tar.gz

h) Luego de a ver ejecutado el comando anterior, ingresamos al directorio que se creó al momento de descomprimir el paquete anterior, a través del siguiente comando:

 # cd sms

i) Para instalar el paquete ***smstools-2.2.20.tar.gz***, debemos ejecutar el siguiente comando:

#. / install.sh

j) Para iniciar el servicio de SMS Server, hay que ejecutar el siguiente comando:

 # /etc/init.d/sms start

k) Si la instalación fue un éxito, ya podemos enviar un SMS a través de consola, siguiendo los siguientes comandos:

#sendsms 0999013010 "Prueba en Linux"

l) Por ultimo debemos, interconectar al usuario Nagios con SMS Server, para lo cual ejecutamos el siguiente comando:

#chown –R nagios.nagios /var/spool/sms

m) Para verificar la información de propiedad de Nagios ejecutamos el siguiente comando:

#ls –la /var/spool/sms

n) Si todo lo anterior se realizó correctamente, el resultado debe ser el siguiente:

drwxr-xr-x 5 nagios nagios 4096 Aug 8 11:59 .
drwxr-xr-x 17 root root 4096 Aug 8 11:59 ..
drwxr-xr-x 2 nagios nagios 4096 Oct 13 23:36 checked
drwxr-xr-x 2 nagios nagios 4096 Oct 11 11:44 incoming
drwxr-xr-x 2 nagios nagios 4096 Oct 13 23:36 outgoing

3.7.2.2 Configuración de SMS Server

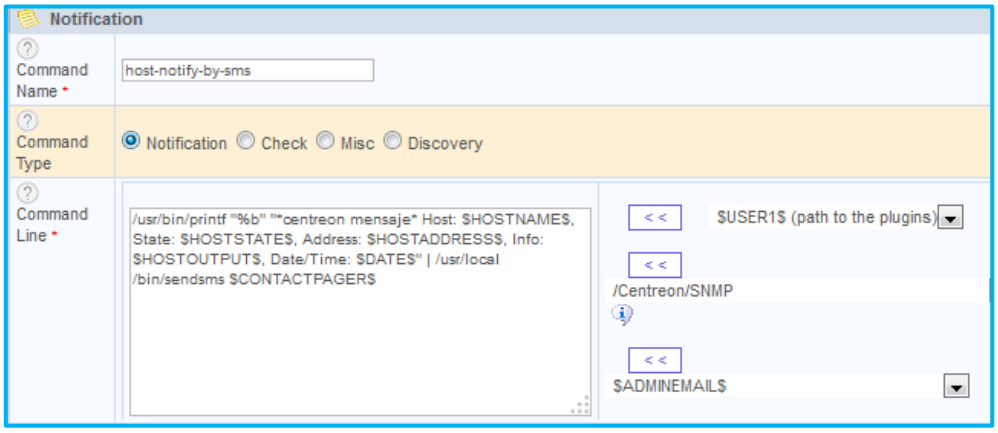
Las notificaciones por e-mail vienen por defecto, para las notificaciones vía SMS es necesario crear algunos comandos:

a) Empecemos por crear un nuevo comando, para lo cual nos vamos a: ***Configuration>Commands>Notifications***, e ingresamos el nombre del comando, tipo de comando, y la sentencia para la ejecución de la línea de comando, la estructura es la siguiente:

/usr/bin/printf "%b" ""centreon mensaje" Host: $HOSTNAME$, State: $HOSTSTATE$, Address: $HOSTADDRESS$, Info: $HOSTOUTPUT$, Date/Time: $DATE$" | /usr/local/bin/sendsms $CONTACTPAGER$

b) Para finalizar la creación del nuevo comando para el envío de mensajes cortos, es necesario dar clic en "***Save***" y reiniciar nuestro servidor de monitoreo de la manera antes mencionada.

GRÁFICO Nº 3.46. COMANDO SMS



Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

c) Ahora que ya tenemos nuestro nuevo comando ***host-notify-by-sms***, solo resta que le especifiquemos que estados nos interesan tanto de los hosts como de los servicios, la configuración es similar a las notificaciones vía e-mail, solo se cambia el comando.

3.7.3 Reportes de IPCop

IPCop, junto a los complementos que hemos probado, han hecho y hacen un trabajo estupendo, ya que recibimos reportes en tiempo real, de la actividad del equipo; los logs del sistema son simples de interpretar incluso para no entendidos en la materia; las actualizaciones son muy sencillas de instalar; las opciones que IPCop ofrece al usuario para adaptarse a sus necesidades son enormes; además, IPCop ha sido instalado en un equipo con recursos medianos y es totalmente estable. (**VER ANEXO Nº 14, PÁG. 200**)

3.7.3.1 Instalación de webalizer

Webalizer es un pequeño programa hecho en C el cual nos permite generar reportes de alguna página web. Gracias a esos reportes, podemos observar el número de personas que han entrado en la web, este complemento no sólo nos da los reportes cuantitativos, sino que también nos da repostes gráficos, lo que hace más elegante y sencillo.

La manera de instalar ***webalizer-3.0.0.tar***, es similar a la instalación del paquete ***smstools-2.2.20.tar.gz*** a continuación, se indica los pasos para una correcta instalación:

a) Descargamos el paquete ***webalizer-3.0.0.tar***, disponible en: ***http://***

sourceforge.net/apps/trac/ipcop/wiki/Addons y guardamos en nuestro computador.

b) Iniciamos ***WinSCP*** para transferir el paquete ***webalizer-3.0.0.tar*** en nuestro servidor de seguridad, para lo cual en ***Host name*** colocamos la dirección IP del servidor de seguridad (*192.168.0.1*) el ***Port number:*** *8022*, que es el puerto que utiliza IPCop, como ***User name:*** *root* y el ***password****: xxxxxx*, que asignamos al momento de la instalación.

c) Una vez que estamos conectados remotamente a través de ***PuTTY*** al servidor de seguridad y hayamos transferido el paquete, descomprimimos el paquete ***webalizer-3.0.0.tar*** ejecutando el siguiente comando:

 # tar-xvzf webalizer-3.0.0.tar

d) Luego de a ver ejecutado el comando anterior, ingresamos al directorio que se creó al momento de descomprimir el paquete anterior, a través del siguiente comando:

 # cd webalizer

e) Para instalar el paquete ***webalizer-3.0.0.tar***, debemos ejecutar el siguiente comando:

#. / setup

3.7.3.2 Configuración de Webalizer

Una vez que hayamos instalado el paquete ***webalizer-3.0.0.tar***, en nuestro servidor de seguridad ingresamos a nuestro sistema de seguridad y monitoreo de la red, seleccionamos la sección de seguridad IPCop. Una vez que estamos conectados dentro del sistema de seguridad, nos dirigimos a la sección de ***Estado*** de la página de administración web de IPCop, luego a la sección de ***Webalizer*** y marcamos ***Activar***, esta activación permite generar estadísticas de proxy en intervalos de tiempo.

GRÁFICO Nº 3.47. WEBALIZER

Fuente: Sistema de Seguridad y Monitoreo de la Red
Realizado por: Investigadores

3.7.4 Reportes de Nagios

Una vez que el sistema ya está funcionando y hemos declarados los hosts necesarios, ya podemos empezar a monitorear su desempeño. En Nagios nos es posible ver todos los servicios disponibles en una lista, también podemos ver el estado de cada host que tengamos configurado. Para ver el estado de los hosts nos vamos a "***Host Detail***" en el menú principal de Nagios, y nos mostrara los detalles más relevantes de todos los hosts, para ver información más específica de un host, damos clic en su nombre y nos desplegara toda la información relevante del estado y los servicios del host. (**VER ANEXO Nº 16, MANUAL DE USUARIO PÁG. 52**)

3.7.5 Reportes de Centreon

Centreon cuenta con más opciones para monitorear los servicios, es posible que desde Centreon se vean todos los detalles que se pueden ver en Nagios, sin embargo la función más importante es la de guardar la información que ocurre en un periodo de 180 días, con lo que puede crear gráficas con la información de desempeño de un equipo, recordando agregar la opción de –f en cada servicio para que habilite el "***Performance Data***". (**VER ANEXO Nº 16 MANUAL DE USUARIO, PÁG. 71**)

3.8 Funcionamiento y Pruebas del Sistema

3.8.1 Administrador de Red

El administrador de red debe poder controlar la actividad en la red y llamar a los técnicos rápidamente en caso de congestión o problemas de acceso. Debe poseer conocimiento preciso de todos los equipos de la red, de los diferentes protocolos de comunicación, del modelo OSI y de diferentes arquitecturas de redes. Además, debido a los cambios vertiginosos de la tecnología y de los medios de transmisión, el administrador de red debe estar permanentemente atento y mantener actualizados sus conocimientos sobre los últimos avances para poder modernizar la infraestructura de red de la institución.

En relación con el jefe de seguridad, el administrador de red está a cargo de implementar medidas de protección adecuadas, supervisar los registros de actividades y controlar las alertas de seguridad. Para anticiparse a peligros posibles, debe implementar un plan de recuperación definiendo lo que se debe hacer para restablecer el acceso lo antes posible, de acuerdo con la política de seguridad de la institución.

3.8.2 Resultados Obtenidos en la Seguridad

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados (Ethical Hacking) en sistemas de pruebas o en laboratorios permite evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia.

Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados.

Para asegurar los fondos necesarios para las pruebas, es importante que los directivos sean conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los Administradores y del personal de seguridad, y para

determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

La realización de pruebas y de ajustes en las directivas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo de aprendizaje. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

3.8.3 Resultados Obtenidos en el Monitoreo

La evaluación es fundamental para el logro de resultados y para la demostración de los mismos. El fortalecimiento de nuestra capacidad organizativa para realizar esta función trascendental forma parte del cambio estratégico hacia una gestión basada en los resultados, una mayor atención al aprendizaje institucional y una rendición de cuentas más estricta.

El servicio de Monitoreo de Redes permite visualizar gráficamente el estado de sus dispositivos, previniendo errores en la plataforma TI y permitiendo tomar decisiones correctas a tiempo. En el acelerado ritmo de la economía mundial, el valor y la seguridad de las redes de datos, son factores que unidos a la expectativa de los usuarios por recibir un excelente servicio de comunicaciones tiene hoy día una importancia crucial.

3.8.4 Resultados Obtenidos del Envío de SMS / E-Mail

Las ventajas de utilizar los mensajes de texto o SMS frente a otros métodos de mensajería son muy numerosas, convirtiéndolo en un sistema ideal para determinados servicios, para empresas y particulares. Los SMS son transferidos al dispositivo

móvil del usuario esté donde esté, sin necesidad de conexión a Internet ni ordenador. Además, el móvil avisa de la llegada, minimizando el tiempo que transcurre desde el envío hasta captar la atención del destinatario.

El correo electrónico es la herramienta más antigua y a la vez más útil de Internet, permite enviar y recibir mensajes a cualquiera de los/as usuarios/as de Internet en el mundo. Dichos mensajes consisten en la transferencia de información, es decir ficheros electrónicos de diversos tipos, entre dos ordenadores. (**VER ANEXO Nº 15, PÁG. 203**)

CONCLUSIONES

- La implementación del sistema de seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi se encuentra desarrollado sobre una plataforma GNU/Linux por ser un sistema estable y estar orientado a un ambiente de servidor.

- El sistema implementado se centra en cumplir los requerimientos proporcionados por el administrador de la red, el cual cubre el monitoreo de los servicios de red, disponibilidad de equipos y la seguridad de los datos.

- IPCop es un Firewall basado en Linux, que nos permite gestionar el acceso a Internet, controlar de acceso a páginas mediante un filtrado URL, con lo que podemos evitar que nuestros usuarios ingresen a determinados sitios web (sexo, violencia, etc.).

- IPCop requiere pocos requerimientos de hardware, y puede ser administrado a través de una interfaz web, con funcionalidades básicas y avanzadas, yendo

desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada estación de trabajo o la configuración de redes virtuales VPN.

- Nagios es una poderosa herramienta de monitoreo que proporciona una gran cantidad de información, tanto en su archivo de log como en su interfaz web, que permiten al administrador identificar los problemas presentados en la red de forma rápida y sencilla, contando con la información necesaria para tomar las decisiones más adecuadas al momento de solucionar un problema presentado en la red.

- Nagios en comparación a otras herramientas para el monitoreo de una red se utilizó por ser flexible, tener alto desempeño, ser confiable y fácilmente adaptable a cambios, ya que incluye un conjunto de plantillas y plugins los cuales facilita la definición de los host y servicios a monitorear.

- La utilización de plugins propios de las herramientas y comandos proporcionados por GNU/Linux, contribuyeron a solucionar de forma sencilla muchos de los problemas presentados en el desarrollo del sistema a fin de cumplir con los requerimientos establecidos por el administrador.

- Para el envío de mensajes de texto se empleó un paquete denominado SMS Server debido a las grandes ventajas que esta herramienta cuenta, principalmente la disposición de librerías para el manejo del puerto serial y USB del computador, para transmitir la información de los estados de los host.

- El sistema implementado dispone de un módulo para la generación de reportes sobre el estado de cada log, disponibilidad de servidores y enlaces de comunicación monitoreados, permitiendo visualizar gráficamente el comportamiento de los mismos en un determinado periodo de tiempo,

proporcionando al administrador de la red información suficiente que le permita interpretar los resultados y realizar las correcciones necesarias a fin de evitar que estos problemas vuelvan a presentarse.

- Una de las ventajas del sistema implementado es contar con dos mecanismos para el envío da notificaciones como: SMS y correo electrónico, ya que en el caso de que un SMS no sea enviado debido a causas externas a la aplicación el correo electrónico será enviado, garantizando con ello que al menos una de las notificaciones sean recibidas por el administrador.

RECOMENDACIONES

- Para la implementación del ***Sistema de seguridad y monitoreo de la red de la Universidad Técnica de Cotopaxi*** se recomienda crear un grupo de usuarios y establecer los permisos adecuados, de tal manera que cada usuario sea el único autorizado a realizar la lectura, escritura y ejecución de los scripts que forman parte del sistema.

- Cuando se trabaja bajo un ambiente GNU/Linux y se presenten errores en la utilización de comandos, se recomienda emplear el comando ***man*** para obtener información de ayuda.

- Es recomendable revisar la información proporcionada por los logs de una aplicación, pues ello ayuda en gran medida a determinar el problema que se está generado y encontrar la solución al mismo, e incluso disponer de la información necesaria para solicitar ayuda en foros.

- Se recomienda recurrir al manual de usuario, según sea el requerimiento para despejar inquietudes o aclarar errores generales.

- La copia de los archivos de logs implican una conexión remota hacia los servidores en donde se encuentran estos archivos razón por la cual se implementó un sistema de copia segura mediante SSH, empleando para ellos llaves de autentificación públicas y privadas, evitando de esta manera que cada vez que se acceda remotamente al servidor no se requiera autenticación manual.

- Se recomienda albergar a IPCop en un equipo destinado a ser servidor, ya que ayudaría a mantener la red informática protegida de forma eficiente y eficaz, a través de configuraciones básicas y avanzadas.

- Si se realizan cambios en la configuración del servidor Nagios, es necesario documentar los cambios que se realizan, y notificar al administrador de la red en el caso de que exista un problema en la generación y restauración del código fuente.

- Es recomendable utilizar plugins propios de las herramientas y comandos proporcionados por GNU/Linux, ya que son de gran ayuda en el momento de solucionar las necesidades que se presentan al momento de implementar el sistema a fin de cumplir con los requerimientos establecidos por el administrador de la red.

- Se recomienda que para el envío de mensajes de texto, se emplee un modem GSM o a la vez contratar un paquete de SMS debido a las grandes ventajas que este servicio presenta, principalmente la disposición de enviar mensajes cortos a los administradores de red, para notificar los estados y servicios de los equipos configurados dentro del sistema.

- Es recomendable revisar las notificaciones enviadas por el sistema de seguridad y monitoreo de la red, ya que permiten al administrador de la red,

realizar las debidas acciones y correcciones de manera que los inconvenientes presentados puedan ser resueltos en el menor tiempo posible.

- El sistema implementado dispone de un módulo para la generación de reportes sobre el estado de cada hosts y servicio, es recomendable llevar una auditoria de cada reporte generado ya sea semanal o mensual, ya que ayudaría a comparar el rendimiento de los distintos equipos dentro de la red informática.

DEFINICIÓN DE SIGLAS

A

ADSL: Asymmetric Digital Subscriber Line o Línea de abonado digital asimétrica.

B

BPDU: Bridge Protocol Data Units o Puente unidades de datos de protocolo.

D

DHCP: Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Host.

DMZ: Demilitarized zone o Zona desmilitarizada.

DNS: Domain Name System o Sistema de Nombres de Dominio.

H

HTTP: HyperText Transfer Protocol o Protocolo de transferencia de hipertexto.

F

FTP: File Transfer Protocol o Protocolo de Transferencia de Ficheros.

FOSS: Free and Open Source Software o Software Libre y de Código Abierto.

I

IBM: International Business Machines.

IDS: Intrusion Detection System o Sistema de Detección de Intrusiones.

IETF: Internet Engineering Task Force o Fuerza de Tareas de Ingeniería de Internet.

IMAP: Internet Message Access Protocol o Protocolo de aplicación de acceso a mensajes electrónicos almacenados en un servidor.

IPSEC: Internet Protocol Security o Seguridad del protocolo Internet.

***IPX/SPX*:** Internetwork Packet Exchange/Sequenced Packet Exchange.

L

LAN: Local Área Network o Red de Área Local.

M

MAC: Media Access Control o Control de acceso al medio.

N

NTP: Network Time Protocol o Protocolo de tiempo de red.

P

PDA: Personal Digital Assistant o Asistente digital personal.

POP3: Post Office Protocol o Protocolo de Oficina de Correo.

R

RMON: Remote Network MONitoring o Red de Monitoreo Remoto.

S

SMTP: Simple Mail Transfer Protocol o Protocolo para la transferencia simple de correo electrónico.

SNMP: Simple Network Management Protocol o Protocolo Simple de Administración de Red.

SSH: Secure Shell o Intérprete de órdenes segura.

SSID: Service Set Identifier o Servicio identificador de conjunto.

SSL: Secure Sockets Layer.

T

TCP: Transmission Control Protocol o Protocolo de Control de Transmisión.

U

UDP: User Datagram Protocol.

V

VLAN: Virtual Local Area Network o Red de Área Local Virtual.

VPN: Virtual Private Network o Red Privada Virtual.

GLOSARIO

A

Access Point: Es un punto de acceso, se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada.

Add-ons: Conocidos como extensiones, plugins, snap-ins, etc., son programas que sólo funcionan anexados a otro y que sirven para incrementar o complementar sus funcionalidades.

Agujeros: Agujero informático, agujero de seguridad, hole, bug.

B

Backup: Una copia de seguridad o backup (su nombre en inglés) en tecnología de la información o informática es una copia de seguridad.

Back-End: Se refiere al estado final de un proceso.

Beeper: Dispositivo muy pequeño para recibir mensajes, los cuales pueden ser enviados por Internet, desde otro beeper, etc.

Bridging (Networking): Puentes de red describe la acción tomada por el equipo de la red para crear una red global.

Bytes: Un byte es la unidad fundamental de datos en los ordenadores personales, un byte son ocho bits contiguos.

C

Caché: En informática, el caché de CPU, es una área especial de memoria que poseen los ordenadores.

Ciberespacio: También llamado ciberinfinito, es una realidad espacio virtual, ya que no tiene una locación física espacial.

Contramedidas: Las medidas que contraatacan físicamente una amenaza entrante y por consiguiente destruyendo o alterando su sistema.

Crosstalk: Es el acoplamiento no deseado de las señales eléctricas presentes en un medio de transmisión con las de otro próximo.

D

Decoy: Son programas diseñados con la misma interface que otro original.

Defacement: Significa desfiguración y es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante.

DHCP: El protocolo de configuración dinámica de host, es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red.

Distribución: En informática, una distribución de software (o Distro) es un conjunto de aplicaciones reunidas, por ejemplo: Distribución GNU/Linux y Distribución BSD.

DMZ: Conocida también como una zona desmilitarizada.

DNS dinámico: Es un sistema que permite la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres.

Dominio: Es un conjunto de ordenadores conectados en una red que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios.

Denial-of-Service: Se refiere a una forma de atacar los sistemas informáticos en red.

dot1Q: Permite usar una interfaz de router como un puerto troncal a un interruptor.

E

Encriptación: Es el proceso para volver ilegible información considera importante.

Ensamblar: Es seguir una secuencia lógica de pasos que nos llevará de tener unos componentes que por sí solos no ofrecen grandes prestaciones, a tener una máquina poderosa para desarrollar actividades relacionadas con nuestros trabajos.

Error de bugs: Un error de software, comúnmente conocido como bug (bicho), es un error o falla en un programa de computador o sistema.

EtherType: En redes de ordenadores es un campo de un paquete Ethernet, que define qué protocolo de capa superior transporta el paquete.

F

Fichero: Es un conjunto de bits almacenado en un dispositivo.

Filtrado de paquetes: Mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos.

Finger: Programa que muestra información acerca de un usuario(s) especifico(s) conectado(s) a un sistema local o remoto.

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

Frame: Área rectangular en una página web que la separa de otra.

Front End: Hace referencia al estado inicial de un proceso.

G

Gentoo Linux: Es un sistema operativo libre que puede estar basado tanto en Linux como en FreeBSD y tiene la capacidad de ser optimizado y personalizado automáticamente para cualquier aplicación o necesidad.

Gigabit Ethernet: También conocida como GigaE, es una ampliación del estándar Ethernet concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo.

H

Host: Es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.

Hubs: Es un equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás.

I

IPFilter: Se usa para bloquear el tráfico de determinadas direcciones que podrían ser perjudiciales para la red.

IPfw: Es un programa de cortafuegos propio de los sistemas UNIX, principalmente FreeBSD y Mac OS X.

IPTables: Es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red.

L

Log: Es un registro oficial de eventos durante un rango de tiempo en particular.

M

Malware: Es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

Mandrake Linux: Es un sistema operativo basado en Linux creado por Mandriva.

Métricas: Es cualquier medida o conjunto de medidas destinadas a conocer o estimar el tamaño u otra característica de un software o un sistema de información, generalmente para realizar comparativas o para la planificación de proyectos de desarrollo.

Multicast: Es un método para transmitir datagramas IP a un grupo de receptores interesados.

N

NTP cliente/servidor: Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

Núcleo Linux: Es un núcleo libre de sistema operativo basado en Unix.

O

Open Source Initiative: Asociación que analiza y certifica los programas de código fuente abierto.

OpenBSD: Es un sistema operativo libre tipo Unix multiplataforma.

P

Pagers: Dispositivo pequeño en donde se reciben mensajes por teléfono o email, originalmente sólo se podían leer pero no enviar, ahora ofrecen en ambos sentidos.

Perl: Es un lenguaje de programación diseñado por Larry Wall en 1987.

Plugins: Es una aplicación informática que añade funcionalidades específicas a un programa principal.

Port Forwarding: La redirección de puertos es la acción de redirigir un puerto de red de un nodo de red a otro.

R

Traceroute: Es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host.

S

Scanning: Método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo.

Sensor: Es un transductor que detecta objetos o señales que se encuentran cerca del elemento sensor.

Shoulder Surfing: Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente.

Software de Auditoria: Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio informático.

Squid: Es un popular programa de software libre que implementa un servidor proxy y un dominio para caché de páginas web, publicado bajo licencia GPL.

SuSe: Es una de las más conocidas distribuciones Linux existentes a nivel mundial, se basó en sus orígenes en Slackware.

Swap: Permite que una computadora simule más memoria principal de la que posee. La técnica es usada por la mayoría de los sistemas operativos actuales.

REFERENCIAS BIBLIOGRAFÍA

Básica:

1. Hernández, S. (2006). Roberto. "*Metodología de la Investigación"*. México: Ultra.
2. Lerma, G. (2007). Héctor Daniel. "*Metodología de la Investigación"*. Colombia: Ecoe.
3. Castilla, E. y Pérez, R. (2005). "*Teoría de la Educación"*. Barcelona: Grao.
4. Ávila, B. (2006). "*Introducción a la Metodología de la Investigación"*. México: San Andrés.
5. Bernal, T. y Augusto C. (2006). "*Metodología de la Investigación para administración, economía, humanidades y ciencias sociales"*. México: Pearson.
6. Arias, F. (2006). "*El Proyecto De Investigación Guía para su Elaboración"*. Caracas: Episteme.

Citada:

1. Cobo, A. *(*2005). "*Tecnología para el desarrollo de aplicaciones web"*. España: Díaz de Santos.
2. Roca, M. (2007). "*Empresa y Administración en España y Cataluña"*: España: UOC.
3. ARCERT Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina, Subsecretaría de Tecnologías Informáticas, Secretaría de la Función Pública. (2002). *"Manual de seguridad en redes."* Argentina: NEUQUEN.

4. Gómez, V. (2011). *"Enciclopedia de la Seguridad Informática*". México: Alfaomega.
5. Huerta, A. (2005). "*Seguridad en Unix y redes"*. México: Prentice Hall.
6. Red Hat, Inc. (2005). *Red Hat Enterprise Linux 4: Introducción a la administración de sistemas.* Estados Unidos: Mandriva.

Virtual:

1. Alierta. (2006) *Inteligencia y Calidad en la Red.* Extraído el 18/01/13 desde http://www.idg.es/computerworld/Inteligencia-y-calidad-en-la-red/seccion-net/articulo-126258.
2. Altamirano, C. (2005). "*Monitoreo de Recursos de Red".* (Tesis inédita de maestría). Universidad Nacional Autónoma de México. Recuperado de http://www.dissoc.org/recursos/tesis/Tesis%20Nora%20Kaplan.pdf
3. Bustamante, R. (2005). "*Seguridad en Redes*". Universidad Autónoma del Estado de Hidalgo: CONACYT Recuperado de http://www.ibiologia .unam.mx/informe/informe%202010/informe_2010%20final.pdf
4. Cabai, D. (2009) Monitoreo de servidores. Extraído el 11/11/12 desde http://www.cabai.com.ar/2009/03/monitoreo-de-servidores-server-monitoring.html.
5. Castro, S. (2008) Monitoreo de la red. Extraído el 10/11/12 desde http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/s1-resource-what-to-monitor.html.
6. Colemanres, J. (2008) *IEEE 802.1X.* Extraído el 23/12/12 desde http://es.wikipedia.org/wiki/IEEE_802.1X.
7. Dueñas, J. (2011) Acerca de Shorewall. Extraído el 15/09/12 desde http://www.alcancelibre.org/staticpages/index.php/como-shorewall-3-interfaces-red.
8. Edisino, F. (2006) Nagios. Extraído el 21/12/12 desde http://es.scribd

.com/doc/81329577/Untitled-1.

9. Espartosa, L. (2009) Pandora FMS. Extraído el 30/11/12 desde http://www.sd3.es/area_pandorafms.aspx.

10. Gutierrez, F. (2007) *IEEE 802.1D.* Extraído el 04/01/13 desde http://es.scribd.com/doc/21146436/Estandares-IEEE-802.

11. Hnizdur S.(2010) Hyperic HQ. Extraído el 21/12/12 desde http://es.scribd.com/doc/42886120/Uso-de-Software-Libre-en-El-Estado. http://iie.fing.edu.uy/ense/asign/redcorp/material/2008/Redes%20de%20Datos%202008.pdf

12. IPCOP. (2011). Extraído el 29/09/12 desde www.ipcop.tk/
Joskowicz, José. (2008). "*Redes de Datos"*. (Tesis inédita de maestría).Universidad de la República Montevideo. Uruguay. Recuperado de 03%20VI%20CONGRESO%20EDUCACION%20AMBIENTAL-RESUMENES%20Y%20TRABAJOS.pdf

13. Junco, G. (2007) Flujo. Extraído el 10/11/12 desde http://www. monografias.com/trabajos95/recursos-red-y-su monitoreo/

14. Junco, G. (2011) Análisis de tráfico. Extraído el 10/10/12 desde http://www.monografias.com/trabajos95/recursos-red-y-sumonitoreo/

15. Lamonica, M. (2005) Definición Open Source. Extraído el 12/06/12 desde http://www.opensystem.co/index.php/art-acercaopenerp/emcodigoabierto.

16. León, A. (2009) Zenoss. Extraído el 19/12/12 desde http://es.scribd .com/doc/89998802/Zenoss-Core.

17. Marchesi, J. (2011) Movimientos Open Source. Extraído el 19/07/12 desde http://www.monparesa.net/index.php/servicios/2-uncategorised/4-opensource.

18. Mazzari G. (2002). "*Seguridad en Redes de Computadoras frente a Internet"*. (Tesis inédita de maestría). Escuela Superior Politécnica del Litoral. Recuperado de http://www.cubambiente.com/memorias/2007/

19. Montalvo, J. (2005) *IEEE 802.1 P,Q - QoS en el nivel de MAC.* Extraído el 08/01/13 desde http://www.geocities.ws/jcredesii/index-2.html

20. Oliva, A. (2007) Núcleo Linux. Extraído el 29/07/12 desde http://www. linux10.com.ar/distribuciones/distribuciones.htm.

21. Ortega, Gl. (2007) *IEEE 802.1Q.* Extraído el 28/12/12 desde http://manejo deredesinformaticasexto.blogspot.com/2013/05/vlan-nativo-y-turking-8021q.html.

22. Perens, B. (2009) Historia del software libre y de código abierto. Extraído el 12/06/12 desde http://servidores-linux-para-empresas.hypersys.com.ar/ servidores-linux-para-empresas/gnu-linux/debian/open-source.html.

23. Primucci, E. (2011) Historia del software libre y de código abierto. Extraído el 12/06/12 desde http://www.codigoaustral.com/open-source/. recursos-red-y-su-monitoreo.shtml.

24. Smith, G. (2011) Uncomplicated Firewall. Extraído el 06/08/12 desde https://help.ubuntu.com/community/UFW.

25. Soto, L. (2006) PF (Packet Filter. Extraído el 29/08/12 desde http://althox.blogspot.com/2013/03/Antivirus-PF-Packet-Filter-Paquete-de-Cortafuegos-basado-en-configuracion-dinamica-stateful-rules.html.

ANEXOS

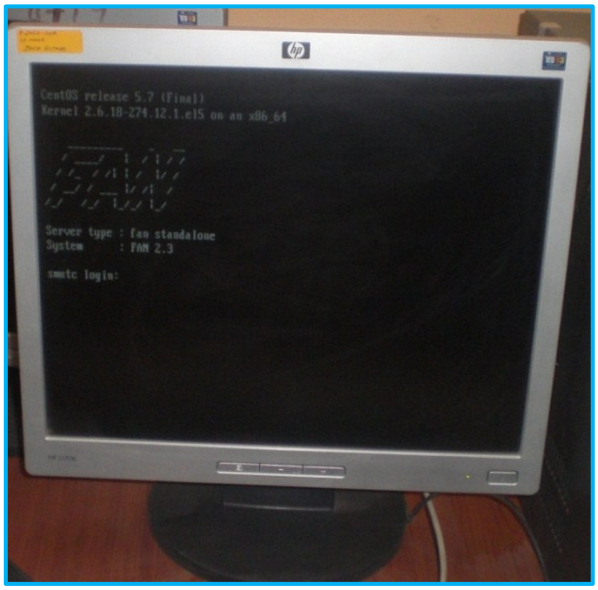
ANEXO Nº 1

INFRAESTRUCTURA TECNOLÓGICA
UNIVERSIDAD TÉCNICA DE COTOPAXI

SALA DE COMPUTO – BLOQUE B

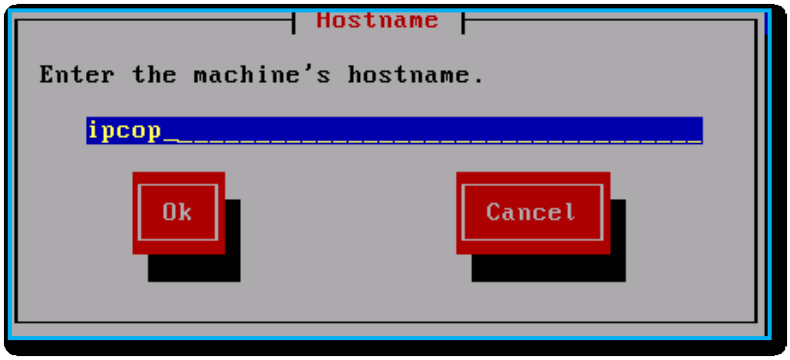
ANEXO Nº 2

EQUIPOS INSTALADOS Y CONFIGURADOS

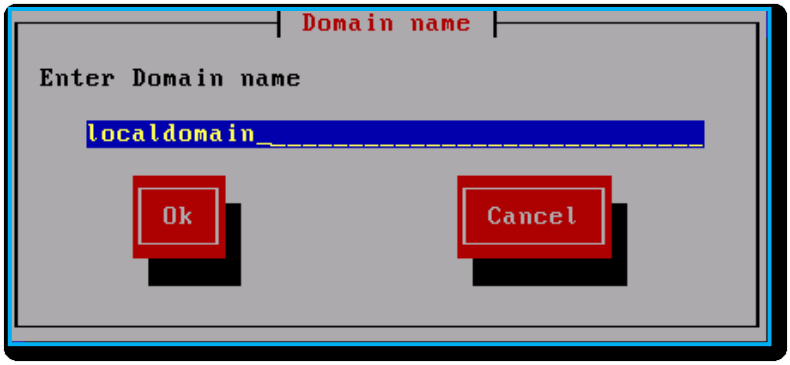


ANEXO Nº 3

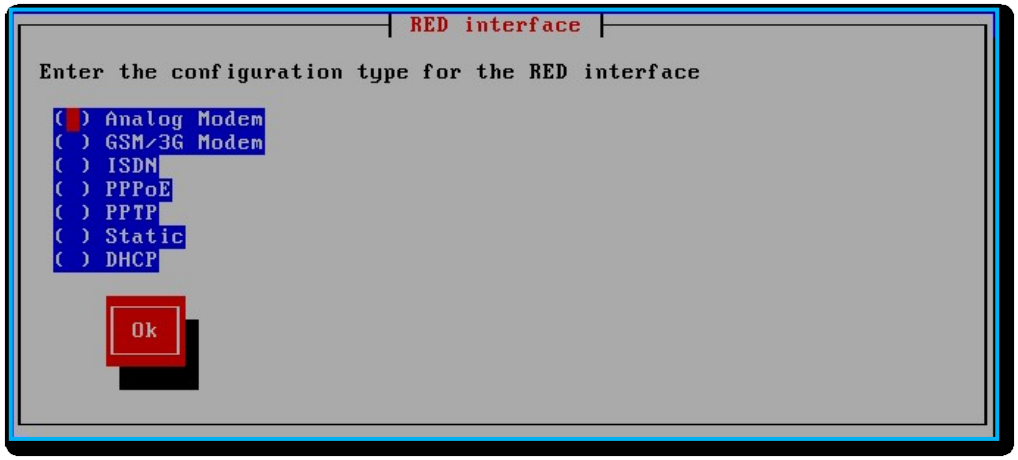
ASIGNACIÓN DEL NOMBRE



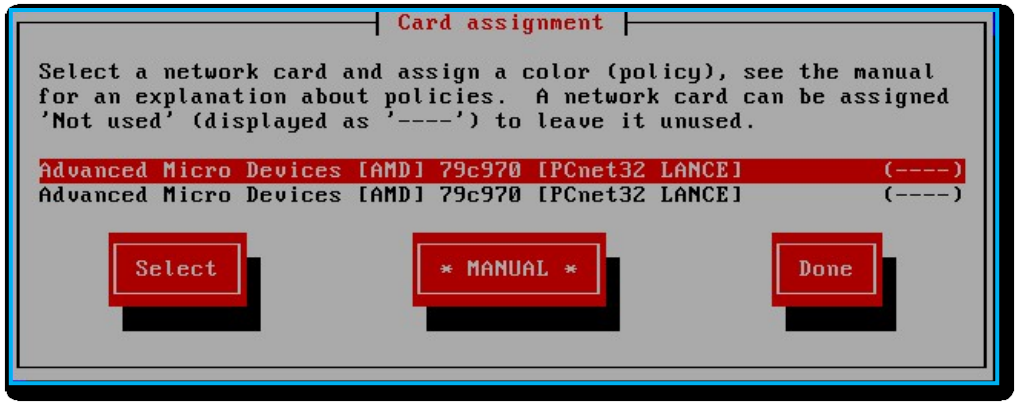
ASIGNACIÓN DEL DOMINIO



ASIGNACIÓN DEL MODO DE INTERCONEXIÓN

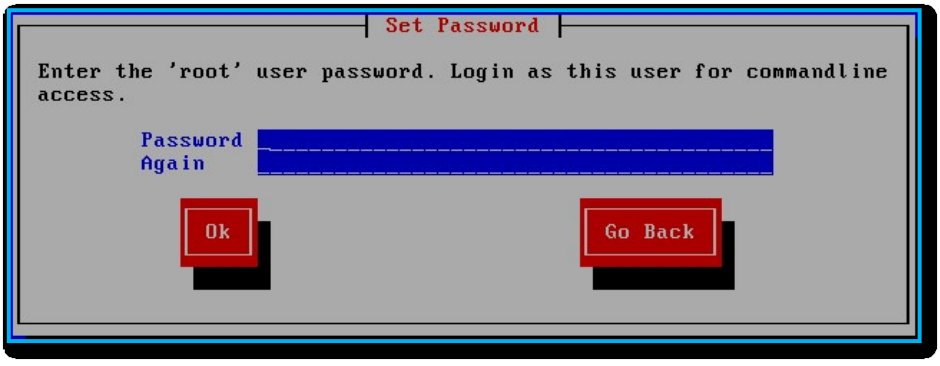


ASIGNACIÓN DE LA TARJETA DE RED



ASIGNACIÓN DE LAS INTERFACES DE RED

ASIGNACIÓN DEL PASSWORD PARA EL USUARIO ROOT

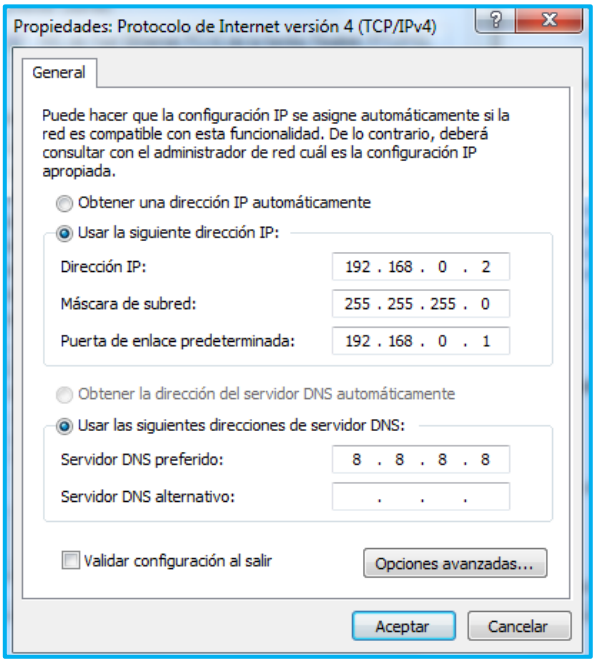


ASIGNACIÓN DEL PASSWORD PARA EL USUARIO ADMIN

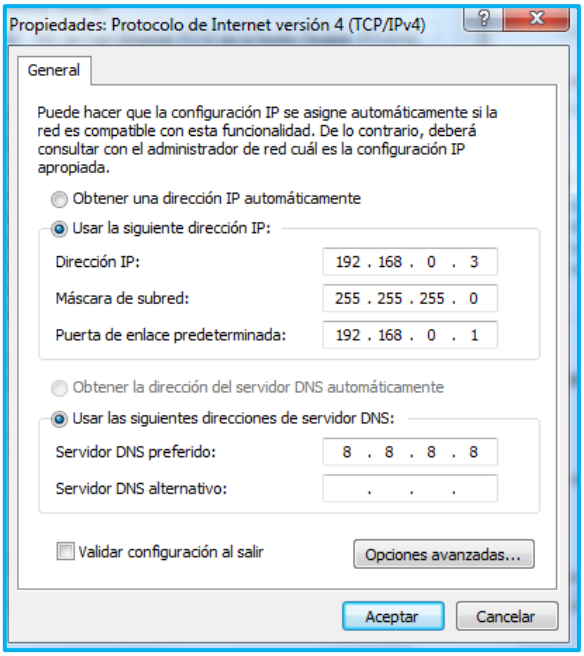
ASIGNACIÓN DEL PASSWORD PARA EL BACKUP

ANEXO Nº 4

CONFIGURACIÓN PC ADMINISTRADOR



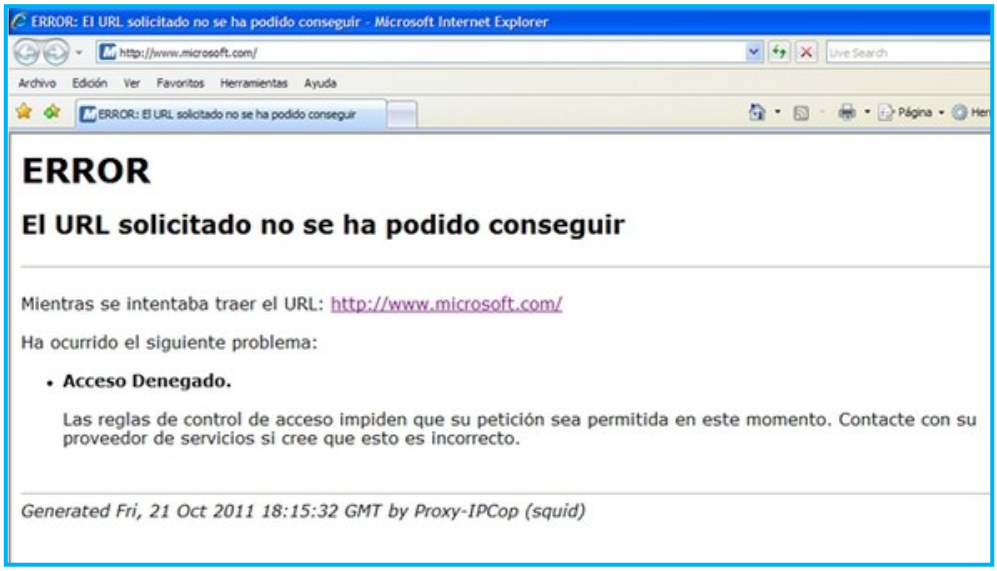
CONFIGURACIÓN PC CLIENTE



ANEXO Nº 5

PANTALLA DE ERROR DESCARGA DE PDF

PANTALLA DE ERROR INTERNET EXPLORER



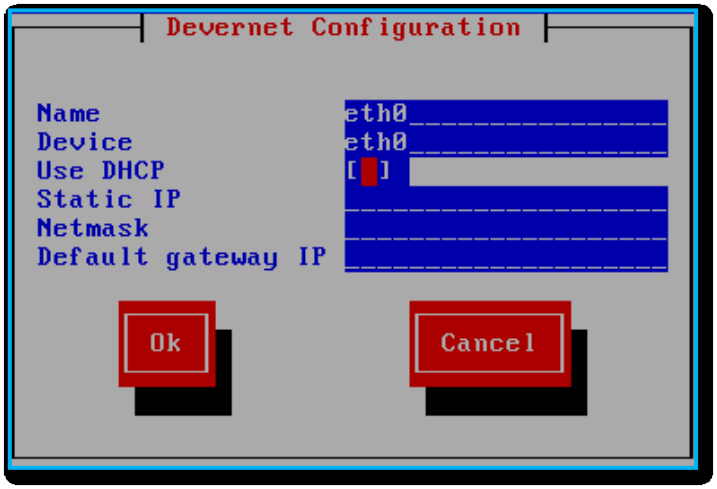
ANEXO Nº 6

PÁGINA DE ERROR AL INGRESAR A FACEBOOK

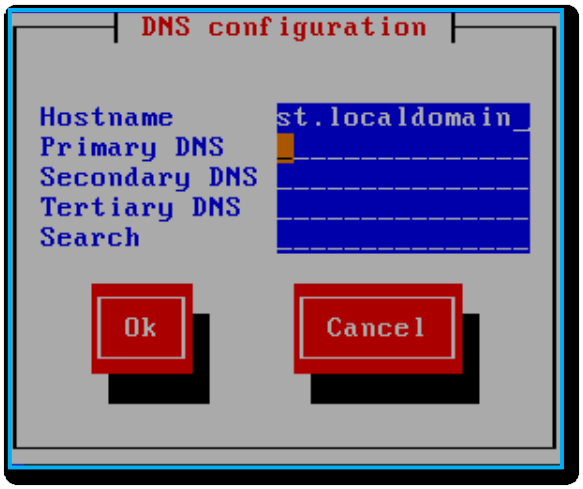
PÁGINA DE ERROR AL INGRESAR A YAHOO

ANEXO Nº 7

CONFIGURACIÓN DE LA TARJETA DE RED

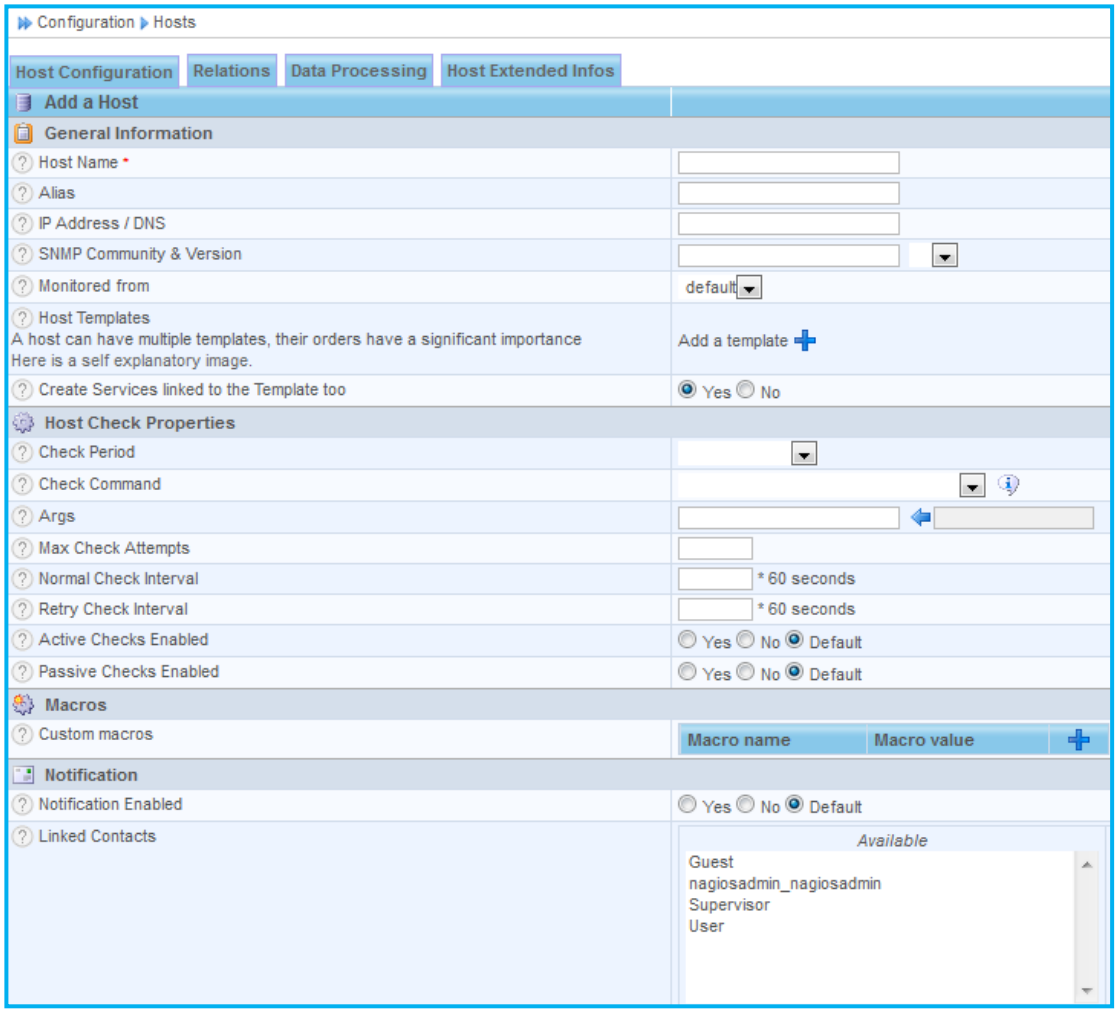


CONFIGURACIÓN DE LOS DNS



ANEXO Nº 8

INGRESO DE LOS DATOS DEL HOSTS



ANEXO Nº 9

LOGS DE NAGIOS

default

Status

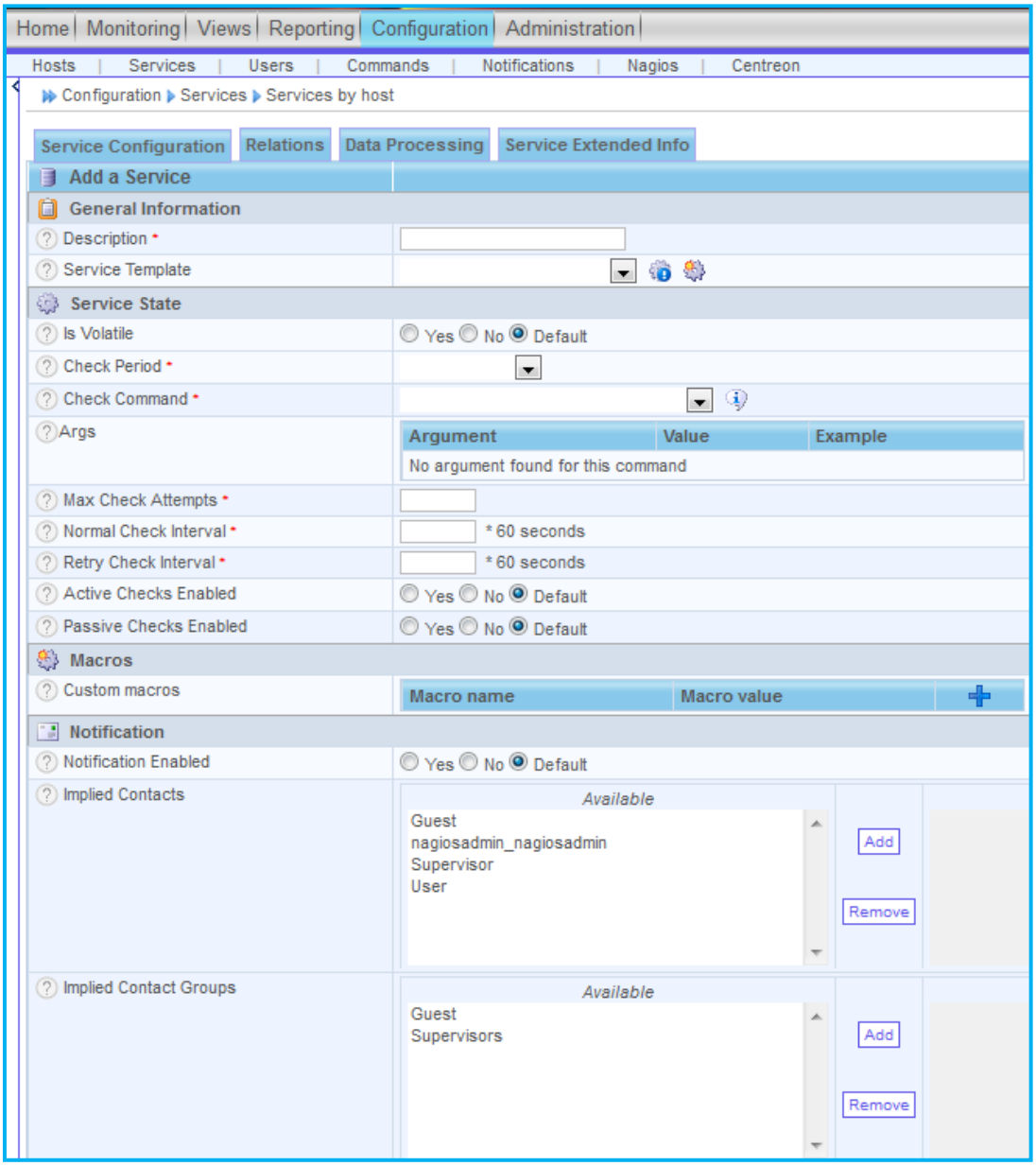
```
Nagios Core 3.3.1
Copyright (c) 2009-2011 Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 07-25-2011 - License: GPL

Reading configuration data...
Read main config file okay...
Read object config files okay...

Running pre-flight check on configuration data...

Checking services...
Checked 4 services.
Checking hosts...
Checked 1 hosts.
Checking host groups...
Checked 1 host groups.
Checking service groups...
Checked 0 service groups.
Checking contacts...
Checked 4 contacts.
Checking contact groups...
Checked 2 contact groups.
Checking service escalations...
Checked 0 service escalations.
Checking service dependencies...
Checked 0 service dependencies.
Checking host escalations...
Checked 0 host escalations.
Checking host dependencies...
Checked 0 host dependencies.
Checking commands...
Checked 89 commands.
Checking time periods...
Checked 5 time periods.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
```

Centreon : All configuration files copied with success.

```
Running configuration check...done.
Stopping nagios: done.
Starting nagios: done.
```

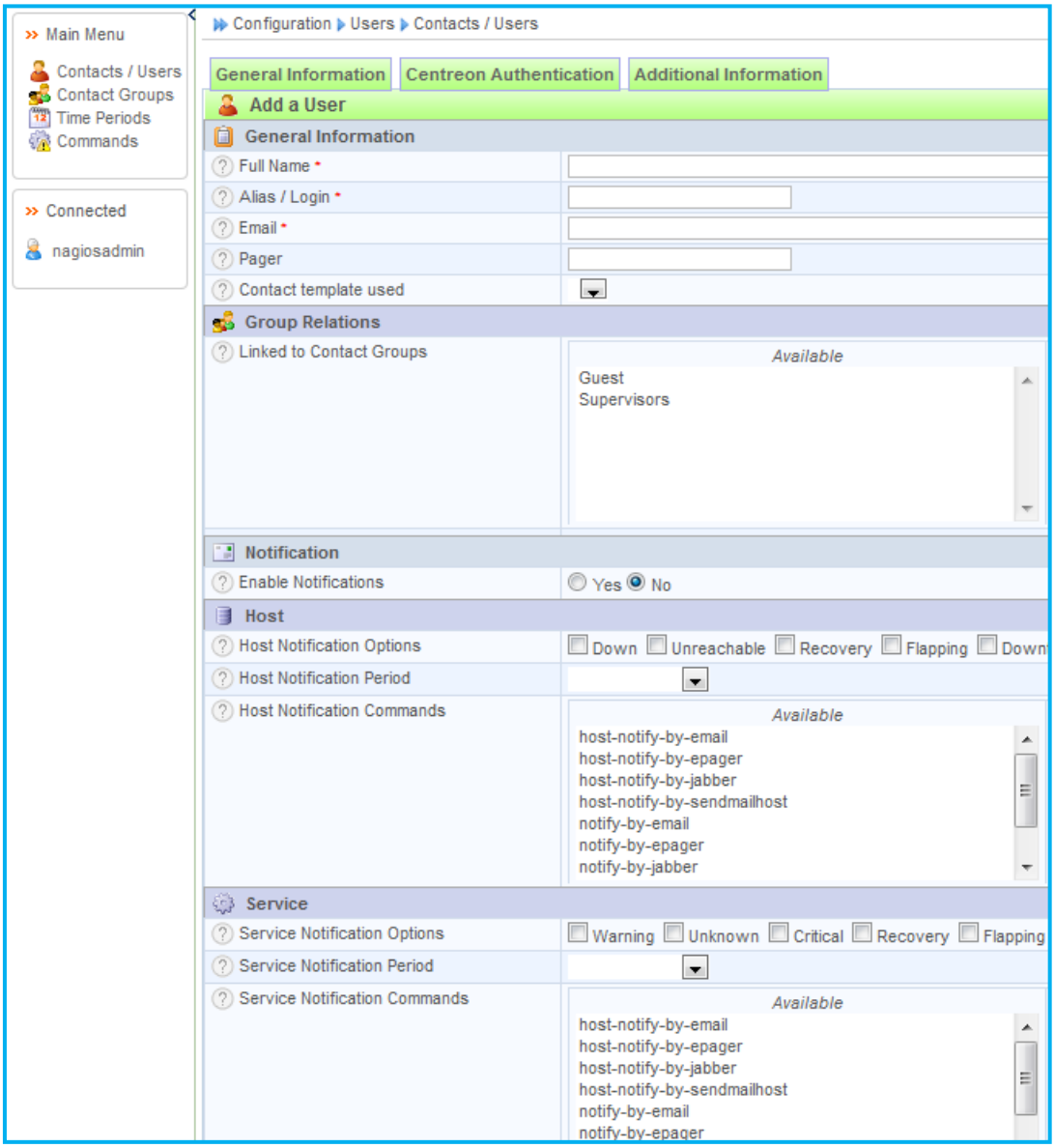
ANEXO Nº 10

AGREGANDO LOS DATOS DEL SERVICIO



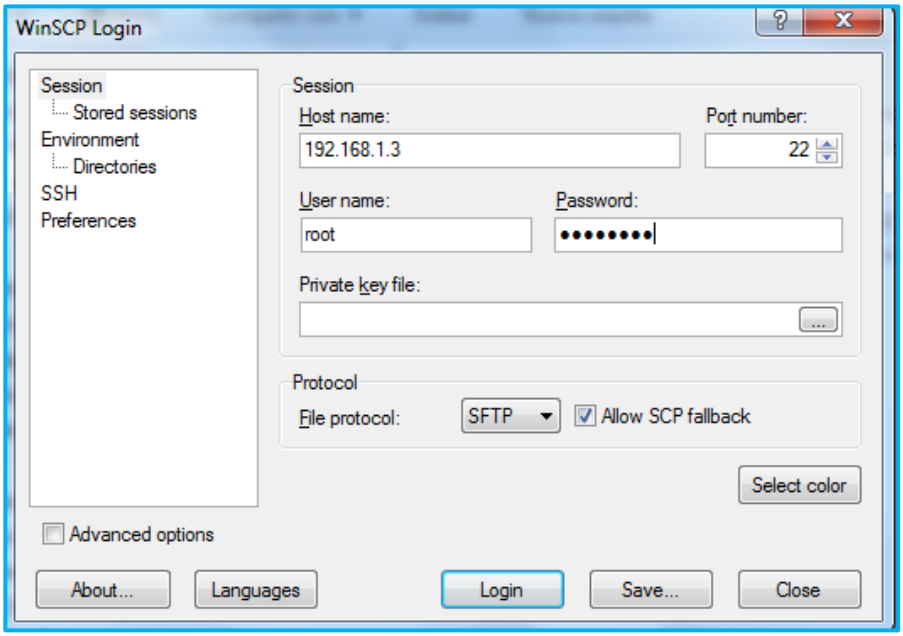
ANEXO Nº 11

AGREGAR LA INFORMACIÓN DEL USUARIO

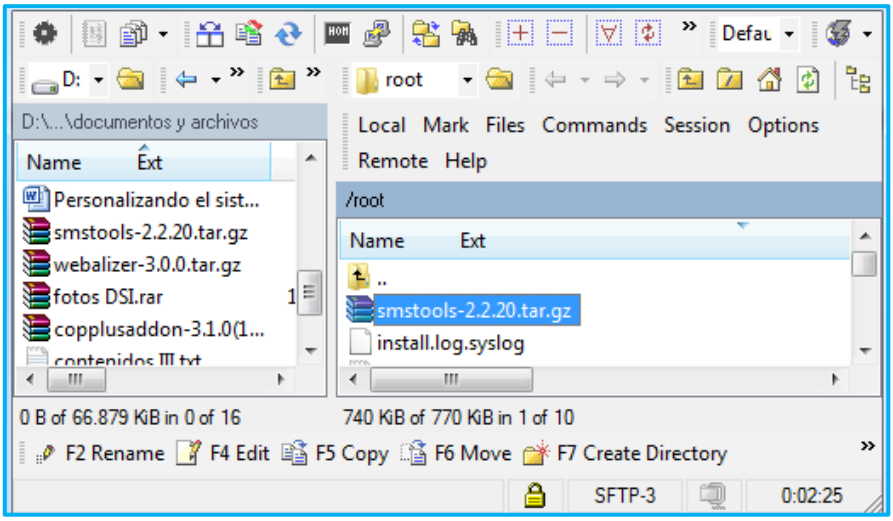


ANEXO Nº 12

PANTALLA PRINCIPAL DE WINSCP

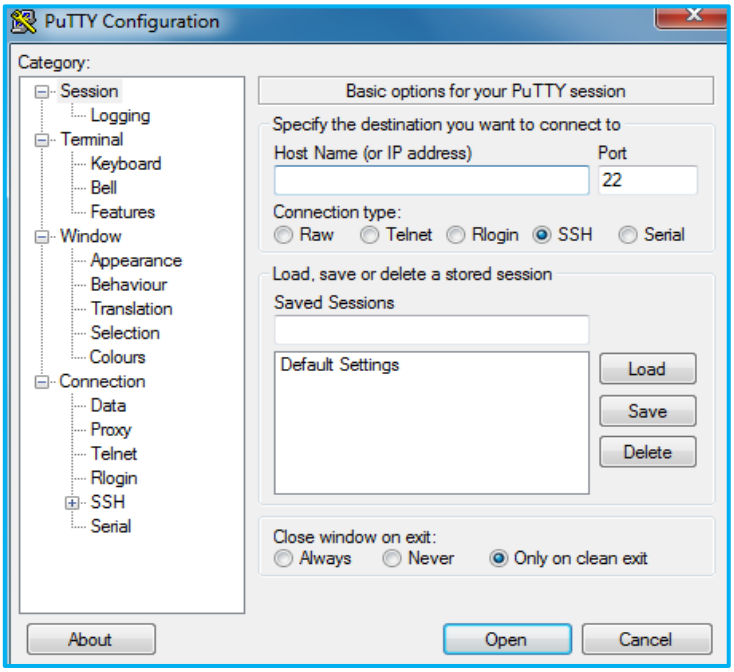


TRANSFERENCIA DE ARCHIVOS

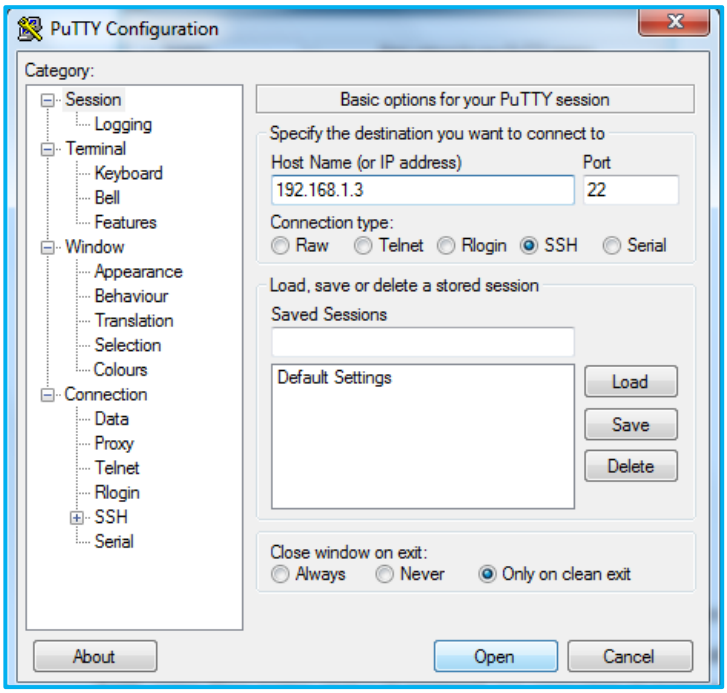


ANEXO Nº 13

PANTALLA PRINCIPAL DE PUTTY



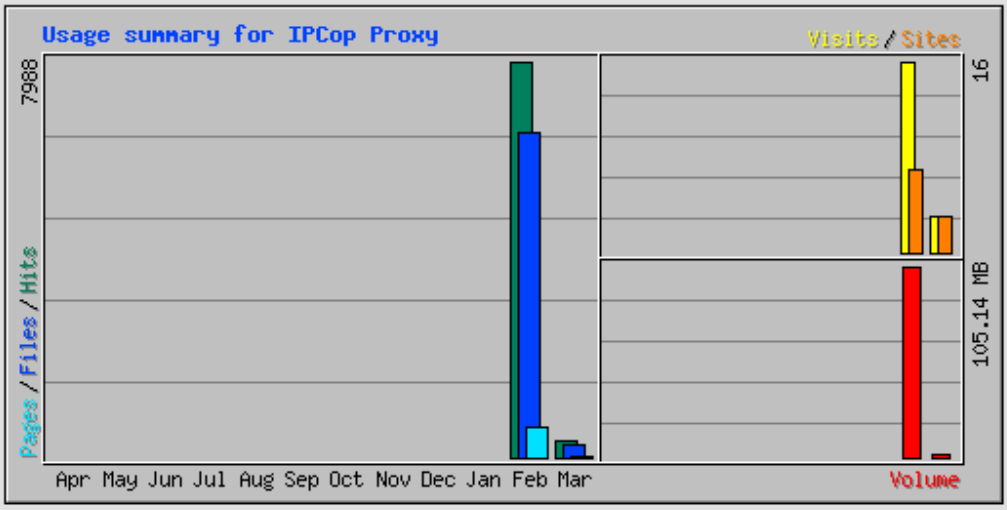
INGRESO A PUTTY



ANEXO Nº 14

REPORTES DE IPCOP

Summary by Month
Generated 01-Mar-2013 10:15 ECT
Webalizer Xtended (RB29)



REPORTES DE IPCOP II

Summary by Month

Month	Daily Avg				Monthly Totals							
	Hits	Files	Pages	Visits	Sites	Volume	Vol. In	Vol. Out	Visits	Pages	Files	Hits
Mar 2013	329	256	26	3	3	2.03 MB	0 bytes	0 bytes	3	26	256	329
Feb 2013	1997	1642	157	4	7	105.14 MB	0 bytes	0 bytes	16	628	6571	7988
Totals						**107.17 MB**	**0 bytes**	**0 bytes**	**19**	**654**	**6827**	**8317**

REPORTES DE IPCOP III

Estad♦sticas diarias de Febrero 2013

D♦a	Accesos		Archivos		P♦ginas		Visitas		Clientes		Volume		Vol. In		Vol. Out	
19	154	1.45%	107	1.23%	13	2.53%	1	16.67%	1	20.00%	489.84 KB	0.75%	0 bytes	0.00%	0 bytes	0.00%
20	691	6.51%	500	5.77%	118	23.00%	3	50.00%	2	40.00%	9.08 MB	14.24%	0 bytes	0.00%	0 bytes	0.00%
21	9766	92.04%	8060	93.00%	382	74.46%	2	33.33%	3	60.00%	54.17 MB	85.01%	0 bytes	0.00%	0 bytes	0.00%

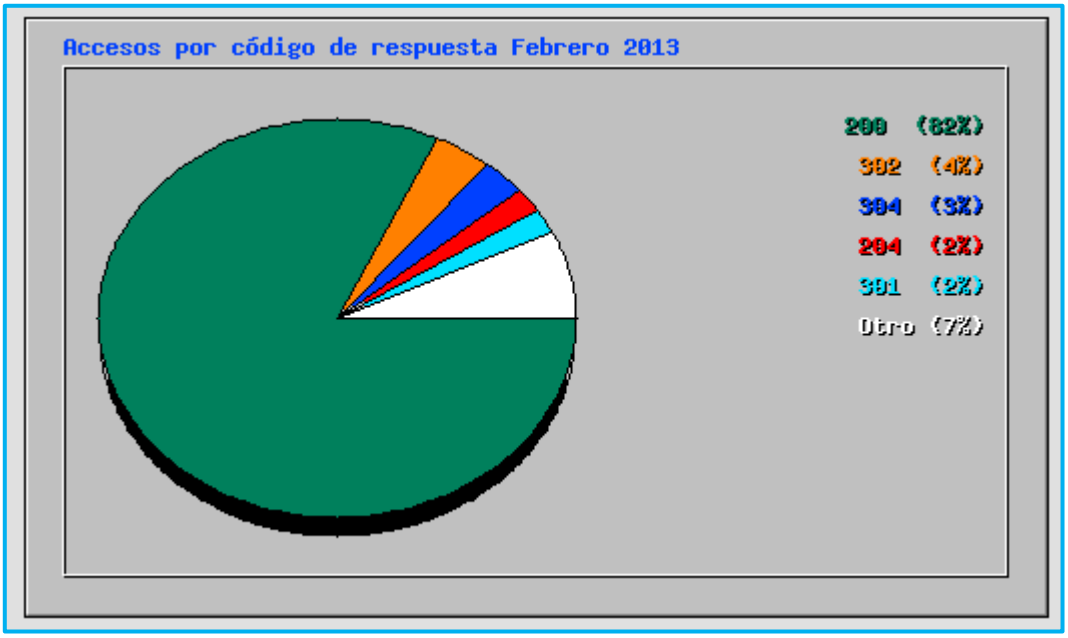
REPORTES DE IPCOP IV

Per&#65533;odo resumido: Febrero 2013
Generado el 21-Feb-2013 13:10 ECT
Webalizer Xtended (RB29)

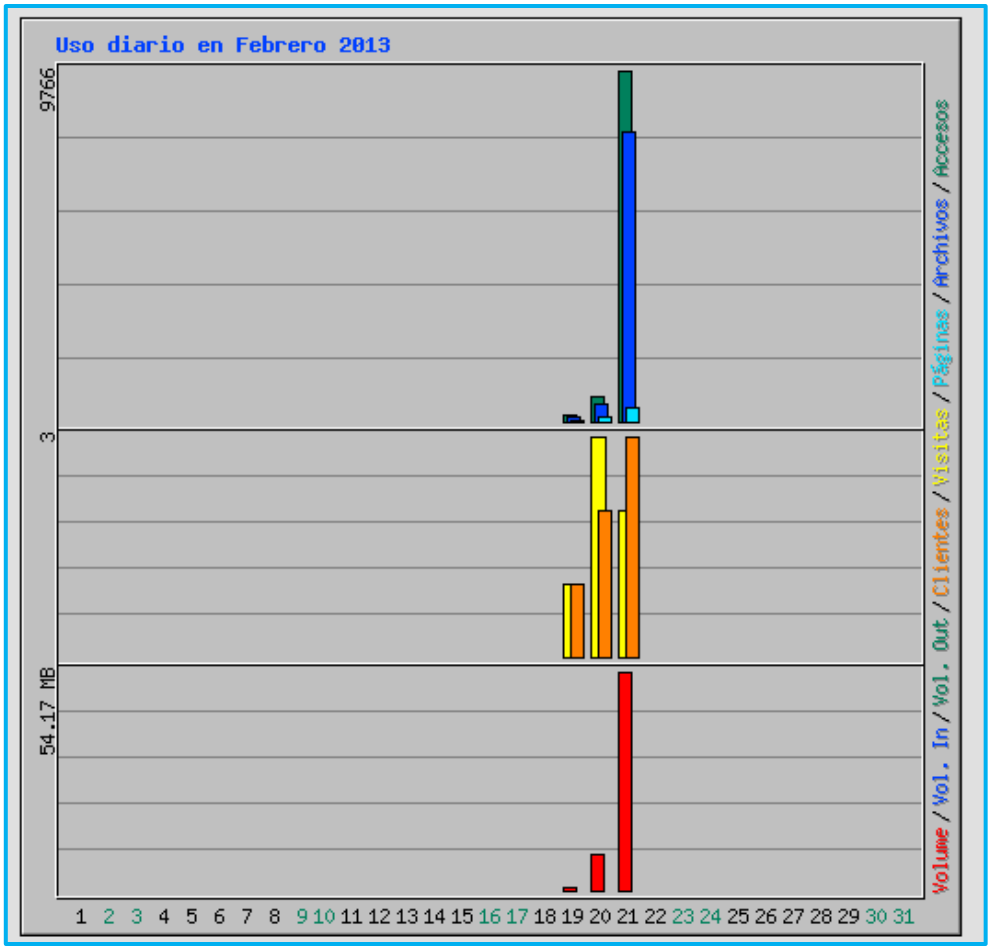
[Main] [Code 404] [Estad&#65533;sticas diarias] [Estad&#65533;sticas por horas] [URLs] [Entrada] [Salida] [Clientes] [B&#65533;squeda] [Pa&#65533;ses]

Estad&#65533;sticas mensuales de Febrero 2013		
Total Accesos		10611
Total Archivos		8667
Total P&#65533;ginas		513
Total Visitas		6
Total Volume		63.73 MB
Total Vol. In		0 bytes
Total Vol. Out		0 bytes
Total Clientes		5
Total URLs		3460
	Media	Max
Accesos por Hora	147	3345
Accesos por D&#65533;a	3537	9766
Archivos por D&#65533;a	2889	8060
P&#65533;ginas por D&#65533;a	171	382
Clientes por D&#65533;a	1	3
Visitas por D&#65533;a	2	3
Volume per Day	21.24 MB	54.17 MB
Vol. In per Day	0 bytes	0 bytes

REPORTES DE IPCOP V



REPORTES DE IPCOP VI



REPORTES DE IPCOP VII

Los 5 primeros de un total de 5 clientes

#	Accesos		Archivos		Volume		Vol. In		Vol. Out		Visitas		Máquina
1	7382	69.57%	6223	71.80%	45.29 MB	71.06%	0 bytes	0.00%	0 bytes	0.00%	1	16.67%	192.168.0.4
2	2252	21.22%	1856	21.41%	8.41 MB	13.20%	0 bytes	0.00%	0 bytes	0.00%	1	16.67%	192.168.0.198
3	619	5.83%	444	5.12%	7.65 MB	12.00%	0 bytes	0.00%	0 bytes	0.00%	2	33.33%	192.168.0.2
4	226	2.13%	163	1.88%	1.91 MB	2.99%	0 bytes	0.00%	0 bytes	0.00%	2	33.33%	192.168.0.206
5	132	1.24%	0	0.00%	485.91 KB	0.74%	0 bytes	0.00%	0 bytes	0.00%	0	0.00%	192.168.0.3

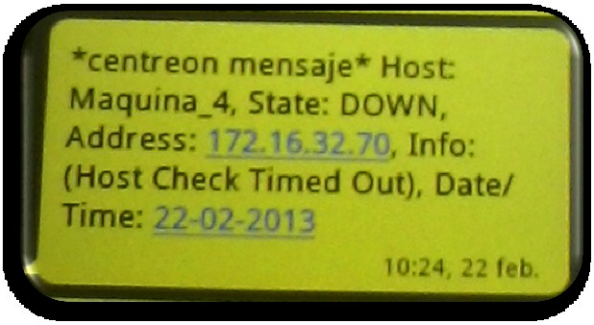
Los 5 primeros de un total de 5 clientes Por Volume

#	Accesos		Archivos		Volume		Vol. In		Vol. Out		Visitas		Máquina
1	7382	69.57%	6223	71.80%	45.29 MB	71.06%	0 bytes	0.00%	0 bytes	0.00%	1	16.67%	192.168.0.4
2	2252	21.22%	1856	21.41%	8.41 MB	13.20%	0 bytes	0.00%	0 bytes	0.00%	1	16.67%	192.168.0.198
3	619	5.83%	444	5.12%	7.65 MB	12.00%	0 bytes	0.00%	0 bytes	0.00%	2	33.33%	192.168.0.2
4	226	2.13%	163	1.88%	1.91 MB	2.99%	0 bytes	0.00%	0 bytes	0.00%	2	33.33%	192.168.0.206
5	132	1.24%	0	0.00%	485.91 KB	0.74%	0 bytes	0.00%	0 bytes	0.00%	0	0.00%	192.168.0.3

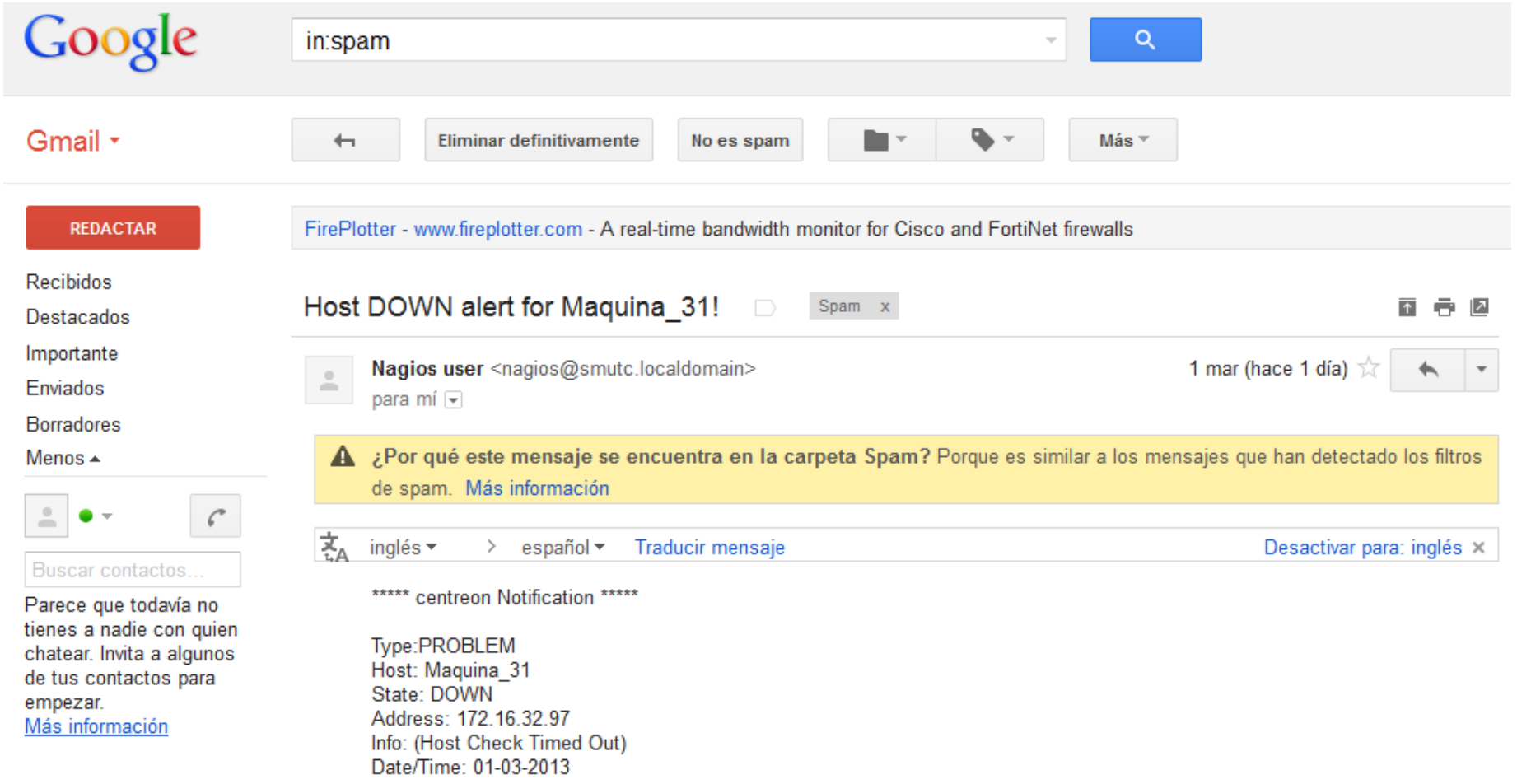
ANEXO Nº 15

NOTIFICACIONES POR SMS

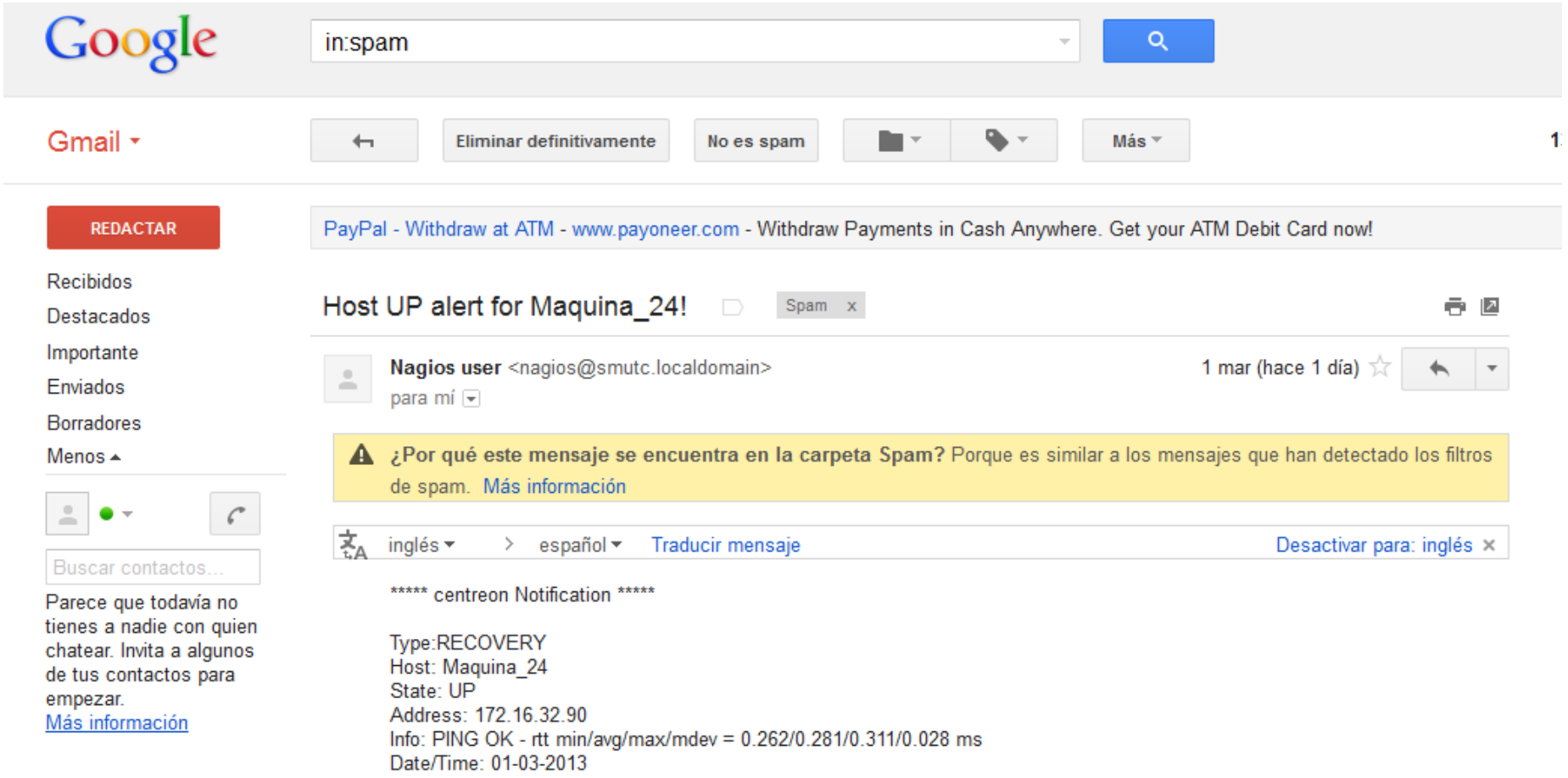
NOTIFICACIONES POR SMS II



NOTIFICACIONES POR E-MAIL



NOTIFICACIONES POR E-MAIL II



ANEXO Nº 16

MANUAL DE USUARIO