



FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE RED Y
MENSAJES DE ALERTA BASADO EN LA PLATAFORMA NAGIOS

Trabajo de Titulación en conformidad con los requisitos establecidos para optar
por el título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía
Iván Ricardo Sánchez Salazar

Autor
Paúl Vinicio Madril Acurio

Año
2014

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el/la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

Iván Ricardo Sánchez Salazar
Ing. Electrónica y Telecomunicaciones
C.I. 1803456142

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

Paúl Vinicio Madril Acurio

0503161259

AGRADECIMIENTOS

Agradezco a todas las personas que me apoyaron en la elaboración de este Trabajo de Titulación ya sea con su tiempo o palabras de aliento, y en especial a mi familia y a Iván Sánchez por todo el tiempo y dedicación que utilizó para guiarme en este camino.

RESUMEN

Debido al gran avance tecnológico que se ha dado a nivel mundial, las empresas medianas y grandes han sufrido cambios importantes dentro de sus redes empresariales, a tal punto que han llegado a converger toda su información, aplicaciones y servicios a una red de datos. Es por esto que los departamentos de tecnologías deberán implementar sistemas de monitoreo adecuados para el control de los distintos componentes de red con la finalidad de alcanzar una alta disponibilidad. Una razón puede ser que los computadores y servicios estén defectuosos o lentos. Otra es el seguimiento que se debe realizar de los componentes de red que suelen tener un mal funcionamiento de hardware o software en un momento inesperado, ocasionando inestabilidad. También es importante evitar fallos en la red instalando alertas en caso de alguna avería. En el presente texto se tratará sobre la plataforma de monitoreo Nagios como un instrumento útil para monitorizar la red.

ABSTRACT

Due to the technological breakthrough that has occurred worldwide, medium and large companies have undergone significant changes within their business networks, to the point that have come to converge all their information, applications and services to a data network. This is why technology departments should implement adequate monitoring systems for the control of different network components in order to achieve high availability. One reason may be that computers and services are defective or slow. Another is tracking to be performed in the network components that usually have a hardware malfunction or software at an unexpected time, causing instability. It is also important to avoid network failure alerts if installing to a fault. Here in will be discussed on the Nagios monitoring platform as a useful tool to monitor the network.

INDICE

Introducción	1
Antecedente	2
Justificación	3
Objetivos	3
Alcance	3
1. GNU/Linux	5
1.1 Historia	5
1.2 Diferencia entre Software libre y Software gratuito	7
1.3 Distribuciones	7
1.4 Núcleo de GNU/Linux	8
1.5 Comandos Básicos de Linux.....	9
1.6 Editores de Texto vs Procesador de Palabras.....	10
1.7 Instalación del Sistema Operativo Linux	12
1.8 Configuración Bios	12
1.9 Opciones de instalación	13
1.10 Instalación y Configuración del Sistema Operativo Linux	
Ubuntu Server 12.04 LTS	13
1.11 Sistema de archivos.....	25
1.12 Monitoreo de Redes.....	26
1.13 Concepto de monitoreo	27
1.14 Concepto Redes LAN	27
1.15 Administración de Redes LAN.....	27
1.16 Concepto Redes de Área Extendida WAN	28
1.17 Herramientas de Monitoreo de Redes.....	29
1.18 Características entre las distintas Herramientas de	
Monitoreo.....	29

2. Instalación del Sistema de Monitoreo Nagios	30
2.1 Historia	30
2.2 Nagios	31
2.3 Estructura	32
2.4 Características de sistema de monitoreo Nagios.....	34
2.5 Ficheros y Directorios	35
2.6 Ajustes de Configuración	36
2.7 Instalación del sistema de monitoreo Nagios.	38
2.8 Concepto de Red.....	46
2.9 Concepto de Intranet	48
2.10 Red GSM	53
2.11 Soluciones de monitoreo mediante el uso de SMS y Correo Electrónico.....	64
2.12 Problemática Banco Procredit S.A	70
3. Pasos, Diseño e Implementación de la Plataforma Nagios.	71
3.1 Pasos para la instalación del sistema Nagios, Correo Electrónico y SMS	71
3.2 Diseño de red y conectividad para sistema Nagios.....	73
3.3 Configuración de <i>Script</i> Sistema Nagios.....	76
3.4 Interfaz web de Nagios.....	86
3.5 Instalación y Configuración de Clientes	95
3.6 Instalación y configuración de <i>Postfix</i> para envío de correo electrónico	97
3.7 Instalación de aplicativo Ozeki NG SMS Gateway para él envío de SMS	101

4. Pruebas del sistema de Monitoreo Nagios	108
4.1 Pruebas de funcionalidad	108
4.2 Análisis de costo solución del sistema de monitoreo Nagios	110
4.3 Costo Beneficio de solución	112
4.4 Costo Mantenimiento Servidor	112
4.5 Costo Mantenimiento Plataforma Nagios.....	113
4.6 Tiempo puesto operativo sistema Nagios.....	113
5. Conclusiones y Recomendaciones	116
5.1 Conclusiones	116
5.2 Recomendaciones.....	118
Referencias	120
Anexos	120

Introducción

Las tecnologías de la información juegan un rol importante en la sociedad a nivel mundial, en un estudio realizado por *Gartner*, empresa líder en estadísticas en el mundo indica que, “hoy en día existe más de mil millones de computadores personales en el mundo, y se espera que como se mantiene el crecimiento, se podrían superar los 2.000 millones de PCs en uso en 2014” (D'appollonio, 2008). Esto nos lleva a pensar que las empresas son las que tienen una mayor cantidad de equipos y por lo tanto tendrían más probabilidad de que existan problemas dentro de sus redes y servicios. La herramienta de monitoreo Nagios cuenta con la posibilidad de monitorear un computador de escritorio sin problemas, incluso tiene un agente que se puede instalar en los equipos para que se unifique con este servicio de monitoreo, por ende, permite tener reportes en tiempo real del estado del disco duro, memoria, procesador, etc. Los técnicos de sistemas al implementar Nagios pueden alcanzar mayor disponibilidad dentro de su red.

Por otro lado una herramienta de monitoreo mal configurada puede arrojar datos erróneos y los técnicos de TI pueden tomar acciones malas gastando tiempo y recursos de las empresas que se encuentran usando tecnologías en base a monitoreo. La herramienta escogida debe ser fiable y adecuada para el correcto uso de sus bondades dentro de la empresa.

En la actualidad hay una necesidad de supervisión de la red de las empresas dentro de sus redes corporativas privadas. Es importante que el software de Monitoreo de red pueda enviar alertas cuando la red se cae o deja de estar disponible a partir de un fallo de hardware. El software puede enviar alertas a los administradores de personal clave en su buscapersonas, correo electrónico o teléfono celular, por consiguiente, los tiempos de respuesta del personal técnico a cargo van a ser mejores y se puede llegar a solventar incluso problemas mayores antes de que sucedan. La importancia del tiempo para una red se ha incrementado con la dependencia de la tecnología y las

computadoras. Incluso una pequeña empresa puede perder miles de dólares de ingresos por hora si su red se queda abajo.

Desde otro aspecto de vista la implementación de alarmas puede saturar la memoria de los equipos y pueden ser el origen de la caída de los sistemas. Por este motivo es importante que se configure todos los parámetros de la red de una forma óptima para el desempeño de las tecnologías de monitoreo.

Finalmente el Monitoreo de red es una herramienta vital para las empresas para evaluar el tiempo de inactividad, estado de los servicios, caídas, problemas de red, etc. Las estadísticas pueden ayudar a los administradores de red, debido a que les permite analizar los problemas y estar preparados para los cortes de sus servicios.

Antecedente

En la actualidad las empresas, tienen la tarea necesaria de implementar herramientas de gestión para las áreas productivas, así como también es de vital importancia implementar en los departamentos de TI, con la finalidad de que tengan la capacidad de tener una visión global de toda su infraestructura para una buena administración y control de todos los equipos que la componen. Es aquí donde los departamentos de TI juegan un papel muy importante con un conglomerado de técnicas que integran los diferentes ámbitos de una red tanto de datos como de voz. Estas tecnologías son susceptibles a estados no deseados, por lo cual las empresas necesitan contar con herramientas de monitoreo para su red. Nagios es un sistema robusto de monitoreo que brinda a las empresas la oportunidad de conocer el estado actual de sus equipos activos de red, los servicios que en la red interna se ejecutan, con la única misión de solventar problemas que puedan ocasionarse dentro su infraestructura. Además Nagios es un sistema de código abierto, que sirve para la monitorización de infraestructura de redes, puede monitorear desde hardware hasta software que se especifiquen en su configuración, enviando mensajes de alertas cuando el comportamiento de los mismos no sea

el correcto. Entre sus funciones principales se tiene la monitorización de los protocolos y servicios de red (SSH, POP3, HTTP, SNMP, etc.), los sistemas hardware como por ejemplo: espacio en discos duros, memoria RAM, Memoria SAWP, Carga del Procesador, Usuarios conectado a un equipo, etc.

Justificación

Debido al gran crecimiento de las redes y a fallos constantes que se presentan en el día a día con los equipos activos de red, se ha pensado en el desarrollo de este trabajo de titulación, si bien hoy en día se tienen herramientas para monitorear de forma gráfica los sucesos y fallos de red, se presenta como parte de la solución una herramienta que tiene la capacidad de enviar mensajes de alertas mediante el uso de mensajes de texto, buscando no impactar en el tema económico, mejor brindando una solución para que a futuro se convierta una herramienta de gran utilidad para él o las personas que están a cargo de la administración una red.

Objetivos

Objetivo General

Diseño e implementación de un sistema de monitoreo de red y mensajes de alerta basado en la plataforma Nagios.

Objetivos Específicos

- Analizar la situación actual de la infraestructura tecnológica de la empresa Banco Procredit S.A.
- Analizar el funcionamiento de la herramienta Nagios para su personalización.
- Personalizar la herramienta Nagios con las nuevas características especificadas en el proyecto.
- Integrar el sistema con el servidor de correo electrónico de la empresa.
- Realizar pruebas de prototipo.

Alcance

El alcance del presente proyecto contemplará diferentes etapas, en primer lugar se realizará un análisis de la infraestructura de equipos activos donde se

detallará las características de los mismos, este análisis permitirá tener un esquema general de la red de la empresa. A continuación se seleccionará las diferentes herramientas que permitirán realizar la personalización de Nagios, entre ellas se analizará las diferentes versiones de la aplicación para seleccionar la más adecuada, el editor de líneas de código adecuado, se investigará las plataformas de correo electrónico y de mensajería instantánea.

Como paso final se realizará la implementación de la plataforma ya personalizada en la empresa para verificar el funcionamiento de todos los módulos y la integración con las demás plataformas.

1. GNU/Linux

1.1 Historia

En la década de los años 60 el Instituto Tecnológico de *Massachusetts*, la *General Electric*, los Laboratorios Bell de AT&T, comenzaron con un proyecto el cual era el desarrollo de un sistema operativo diferente al que llamaron *Multics (Multiplexed Information and Computing Service)* o también conocido como Sistema de Computación y Multiplexación de la información. El proyecto fue abandonado años más tarde por los laboratorios Bell de AT&T.

Ken Thompson y *Dennis Ritchie* investigadores de laboratorios Bell, crearon las primeras versiones de lo que hoy en día se conoce como sistema operativo Unix, sistema que fue desde su inicio escrito en lenguaje ensamblador y que a partir de los años 70 sus líneas de código se lo desarrollaron en lenguaje de programación C.

El sistema operativo Unix se lo caracteriza por ser un sistema multiusuario y multitarea, en un inicio Unix fue utilizado para procesos de investigación y que con el pasar de los años este fue donado a universidades en donde tuvo gran aceptación. Años más tarde los laboratorios Bell deciden comercializar el sistema operativo con una licencia que permitía la modificación del código base y redistribuirlo, debido a las modificaciones realizadas al sistema Unix con el transcurso del tiempo aparecieron variedad de sistemas operativos derivados de Unix.

Por el años de 1983 *Richard Stallman* de origen estadounidense decide crear una opción libre del sistema Unix emprendiendo un proyecto al cual lo llamo GNU. *Stallman* y varios programadores iniciaron a insertar modulo tras modulo al GNU, además empezaron a escribir un núcleo o *Kernel* llamado *Hurd*, el cual es un pequeño código que permite iniciar a las computadoras. En el año 1990 el proyecto ya contaba con un editor de texto llamado *Emacs* más un compilador con nombre GCC y una gama de librerías. Linus Torvalds

estudiante e investigador de la Universidad de Helsinki aparece un año más tarde en el desarrollo del *kernel* del sistema GNU. (<http://histinf.blogs.upv.es/2011/12/23/historia-de-linux/>)

1.1.2. Definición GNU

El nombre GNU significa (*Not Unix*) en inglés, fundado por *Richard Stallman* en el año 1984, es un sistema operativo creado con el fin de tener un sistema operativo similar a Unix pero con la diferencia de que este sistema operativo sea libre y abierto a sufrir modificaciones, permitiéndole a los usuarios tener acceso a las fuentes de código ya sea para visualizarlos, utilizarlos, modificarlos y redistribuirlo de ahí sus siglas. (Universidad San Francisco de Quito, 2013, pp.1-10)

1.1.3. Definición de Linux

El termino Linux es una denominación que se da al sistema operativo tipo Unix y al nombre del núcleo o *kernel* comúnmente conocido. Linux fue desarrollado por Linus Torvalds el cual utiliza la filosofía y la metodología de un sistema operativo *Open Source* o de código abierto, integrando una gran variedad de utilidades y aplicaciones.

Las utilidades permite al usuario realizar la gestión de los recursos del sistema y las aplicaciones se encarga tener una herramienta fácil para la realización de las tareas del sistema

GNU/LINUX se hizo popular por la implementación estándar *POSIX* (Interfaz de Sistema Operativo Portable) y además por tener la característica de ser multiusuario, multitarea y multiplataforma, que se describen a continuación:

- **Multiusuario.-** Permite tener dos o más usuarios en sesiones simultaneas haciendo uso de los recursos del computador.

- **Multitarea.-** Significa que un usuario puede ejecutar varias tareas o programas al mismo tiempo.
- **Multiplataforma.-** Puede ser usado por varias plataformas, ejemplo: AMD, HP, *Sun*, Macintosh, etc. (Universidad San Francisco de Quito, 2013, pp.10-14)

1.2 Diferencia entre Software libre y Software gratuito

En la actualidad se menciona mucho acerca de software libre y software gratuito, hay que tener muy en claro cuál es la diferencia entre libre y gratuito.

- **Software Libre.-** Significa que el usuario puede hacer uso del código fuente, el cual lo puede utilizar, manipular, modificar y hasta redistribuirlo, una vez realizado algún cambio en código no se le debe negar.
- **Software gratuito.-** Significa que si mejoro una versión de Linux o realizo un nuevo sistema operativo este se lo debe publicar, entregar y comercializar sin costo alguno

1.3 Distribuciones

Las distribuciones GNU/Linux son diferentes variantes de software que hacen uso del núcleo de Linux, con la finalidad de adaptar particularidades características o para suplir falencias y necesidades de los usuarios, existen distribuciones sencillas que son orientadas a labores y otras que son orientadas a servicios.

En la actualidad contamos con una gran variedad de distribuciones todas basadas en GNU/Linux, varias de las distribuciones son orientadas a computadores de escritorio, celulares, servidores, etc. A continuación se listara las más populares versiones que se puede encontrar:

Red Hat, CentoS, Debian, Ubuntu, Fedora, Suse, LinuxMatic y Mandriva.

El concepto de software libre hace que los usuarios puedan realizar modificaciones al código fuente adaptado así al sistema operativo a las necesidades propias del usuario, esto ha permitido que muchas personas a nivel mundial prefieran sistemas basados en GNU/Linux. (Universidad San Francisco de Quito, 2013, pp.15-20)

1.4 Núcleo de GNU/Linux

El kernel de Linux es un sistema operativo, como Windows, MacOS y OS / 2 son sistemas operativos. El sistema operativo es un entorno en el que se ejecutan los programas, proporcionando mecanismos para que los programas interactúen con el hardware del equipo. El núcleo de los programas permite saber cuándo fue presionado una tecla del teclado, cuando el *mouse* se mueve, o cuando un paquete destinado para el programa llegó a través de la red. El *kernel* permite el acceso a los programas del disco duro, tal vez para leer un archivo de configuración o almacenar datos.

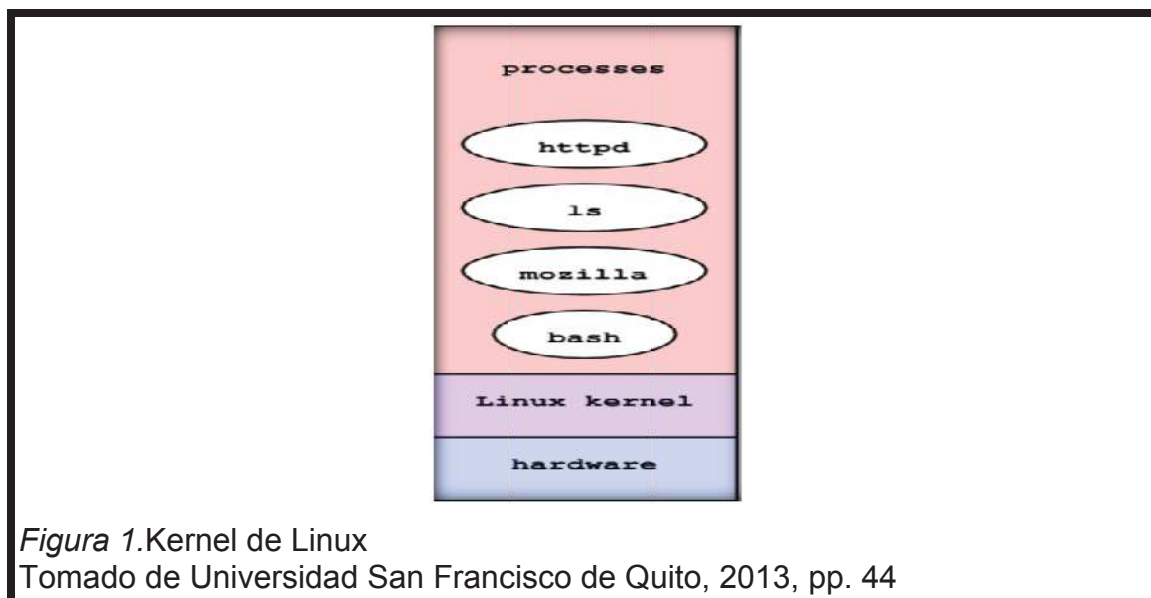


Figura 1. Kernel de Linux

Tomado de Universidad San Francisco de Quito, 2013, pp. 44

Es elemento principal o el corazón de un sistema operativo basado en GNU/Linux es el núcleo o también llamado *kernel*, la principal meta del núcleo

es permitir el funcionamiento tanto de *hardware* y de *software* de un computador, las principales responsabilidades de un *kernel* son:

- **CPU.-** El *Kernel* se encarga de verificar de que todos los procesos que estén en ejecución puedan usar el procesador
- **Memorias.-** EL *Kernel* es el encargado de asignar el espacio de memoria para los programas
- **Periféricos de E/S.-** Controla los periféricos de entrada como los de salida como por ejemplo teclado, mouse, pantalla, etc.

1.5 Comandos Básicos de Linux

El sistema operativo Linux tiene una gran variedad de comandos, los cuales pueden ser ejecutados desde un terminal o consola, con la finalidad de ser utilizados para ejecutar desde tareas sencillas hasta el más complejo, ejemplo: manejo de directorios, archivos, administración de usuarios y grupos, verificación de procesos, administración de servicios, etc.

GNU/Linux tiene un comando especial al cual se le conoce con el nombre (*man*), dicho comando es utilizado para conocer la funcionalidad de otro comando, presentando un pequeño manual detallado con las opciones acerca de los modos de utilización del comando a consultar, así como el comando *man* se tiene otros como por ejemplo el *help*, el cual tiene la misma funcionalidad pero con la particularidad que no presenta un detalle completo del comando a buscar. (Universidad San Francisco de Quito, 2013, pp.1-4)

A continuación se listaran y se detallaran los comandos necesarios que resultan de suma importancia en el desarrollo del presente trabajo.

Lectura de archivos:

- **cat.-** Muestra el contenido de un fichero, la sintaxis a utilizar es:

```
cat nombre_archivo
```

- **head.-** Muestra el inicio de un fichero, por defecto presenta las primeras 10 líneas

```
head -num_líneas nombre_archivo
```

- **tail.-** Se utiliza para visualizar las últimas líneas del fichero, también se usa para el monitoreo de log con la opción -f

```
tail -opciones nombre_archivo
```

- **grep.-** Realiza una búsqueda en el contenido de un archivo un determinado conjunto de caracteres e indica por pantalla las líneas que concuerden con la búsqueda. Es sensible a mayúsculas y minúsculas siempre y cuando no se use el parámetro -i

```
grep -opciones carácter(s)_a_buscar nombre archivo
```

Adaptado de (Universidad San Francisco de Quito, 2013, pp. 44)

1.6 Editores de Texto vs Procesador de Palabras

Una de las maneras que Linux logra su alto grado de flexibilidad es a través de la solidez de su configuración. La información de configuración normalmente se almacena en archivos de texto ASCII. La administración del sistema implica a menudo la actualización o corrección de estos archivos de configuración. La herramienta para hacer este trabajo es un editor de texto.

Un editor de texto no es lo mismo que un procesador de textos. Los procesadores de texto permiten al usuario especificar las fuentes, los ajustes de la ficha, los márgenes, la justificación, y muchas otras características

diseñadas para afectar a la forma en que un documento aparece en el papel. Los documentos generados por procesadores de texto contienen incrustados códigos binarios que especifican la configuración de estas características adicionales. Un archivo de texto plano, como un archivo de configuración no contiene este tipo de códigos y no está diseñado para imprimir en papel. Un editor de texto está diseñado sólo para modificar el contenido de texto de un archivo formato ASCII y no contiene los códigos binarios incrustados.

Un procesador de textos sería una opción apropiada para escribir una carta, una nota, un boletín, un folleto de publicidad o cualquier otro documento que la presentación visual es controlada por el *software* de edición.

Un editor de texto es la opción adecuada para crear o modificar los archivos de configuración, el código fuente del programa, la documentación del sistema, o cualquier otro documento por ejemplo, un documento HTML en la presentación visual es controlado por el *software* de visualización por ejemplo un navegador web y no el software de edición.

Linux viene con un completo conjunto de editores de texto, cada uno con fortalezas y debilidades específicas. Linux también incluye los procesadores de texto para la creación de documentos como parte de productos como *OpenOffice*. (Fedora Project, 2014)

Dado que todos los editores de texto funcionan en simples archivos de texto, los usuarios pueden elegir el que tenga gusto, no hay problemas de compatibilidad entre un producto y otro. Normalmente, al hacer la elección en función de la disponibilidad, la facilidad de uso, familiaridad y características especiales. Algunos editores, por ejemplo facilitan la generación de código de programa con el formato correcto, por lo que la programación se hace más fácil y rápida.

1.6.1 Vi

El editor de texto más popular en los sistemas Linux es vi, también es el más resistente y el más complicado. La complejidad de este editor hace que su uso sea menos utilizado por los usuarios

1.6.2 Nano

Nano es un editor simple, pantalla orientado a texto. Los comandos se muestran en la parte inferior de la pantalla, y hoy en día es uno de los más utilizados.

1.6.3 Gedit

1Gedit es un editor gráfico de texto disponible para el entorno X-Window. Se puede acceder mediante la introducción del comando gedit en un símbolo del sistema en una ventana de terminal, o seleccionando Accesorios -> Editor de texto desde el Menú de *GNOME*. Proporciona una interfaz de ventana de documento común para crear y editar archivos de texto e iconos, barra de herramientas para acceder a funciones como la búsqueda y reemplazo, *cut-copy-paste*, y la impresión. (Universidad Rey Juan Carlos, 2013, pp. 6,17-31)

1.7 Instalación del Sistema Operativo Linux

1.8 Configuración Bios

Antes de iniciar cualquier instalación de un sistema operativo Linux, se debe conocer el equipo y las características que posee, en primer lugar se deberá verificar el hardware como son: los tipos de memoria, dispositivos de entrada y de salida (teclado, *mouse*), discos duros, adaptadores gráficos, adaptadores de red, etc. Así como además verificar la compatibilidad con la versión de Linux a instalar

1.9 Opciones de instalación

Para realizar el proceso de instalación del sistema operativo Linux se tiene diferentes formas de realizarlo, una de ellas se la conoce como *Kitstart* que procede a la configuración mediante el uso de un demonio llamado *anaconda.pk.cfg*.

Un segundo método se basa a partir de un servidor *ftp*, su proceso consta de iniciar el arranque del computador con el CD de instalación de cualquier versión y escoger el modo que se va a realizar el proceso y apuntar hacia la dirección del servidor donde se aloja la imagen con las particiones y configuraciones pre establecidas.

El tercer método es el proceso manual que comúnmente se lo realiza en el día a día, el cual es la instalación desde un CD, DVD o en una *Memory Flashbootable* donde nosotros podemos ir realizando los cambios en particiones y configuraciones que lo requerimos y que consideramos necesarios.

1.10 Instalación y Configuración del Sistema Operativo Linux Ubuntu Server 12.04 LTS

Antes de comenzar con la instalación, se deberá verificar las características mínimas de *hardware* que necesita el sistema operativo para que pueda funcionar en óptimas condiciones.

Los requerimientos mínimos de *hardware* deberán ser:

Tabla 1. Requisitos mínimos de *hardware*

Requerimientos de <i>Hardware</i> para S.O Ubuntu Server 12.04 LTS	
Procesador	Procesador x86 o x64 a 2GHz
Memoria RAM	2GB
Disco Duro	80GB
Unidades Ópticas	CD/DVD-R

Después de verificar si el computador posee los requisitos mencionados en la tabla 1, se procederá a realizar los siguientes pasos de instalación.

Paso 1.- Se realizará el *boot* desde el CD y se tomará la primera opción (*Install Ubuntu Server*)



Figura 2. Primera pantalla de instalación del sistema Linux Ubuntu
Tomado de Caballero, 2013, pp.1-12

Paso 2.- Se elegirá el idioma para iniciar la instalación



Figura 3. Elección del lenguaje para el sistema

Tomado de Caballero, M, 2013, pp.1-12

Paso 3.- Se escogerá la zona horaria, si no se encuentra el país como opción se escogerá (*Other*)

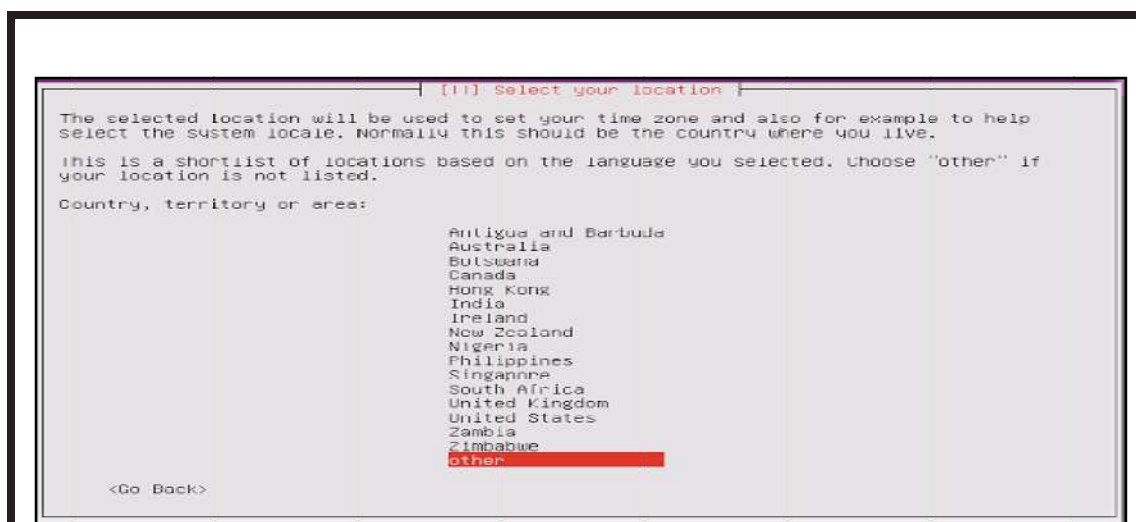


Figura 4. Selección de ubicación

Tomado de Caballero, M, 2013, pp.1-12

Paso 4.- Se escogerá el continente.

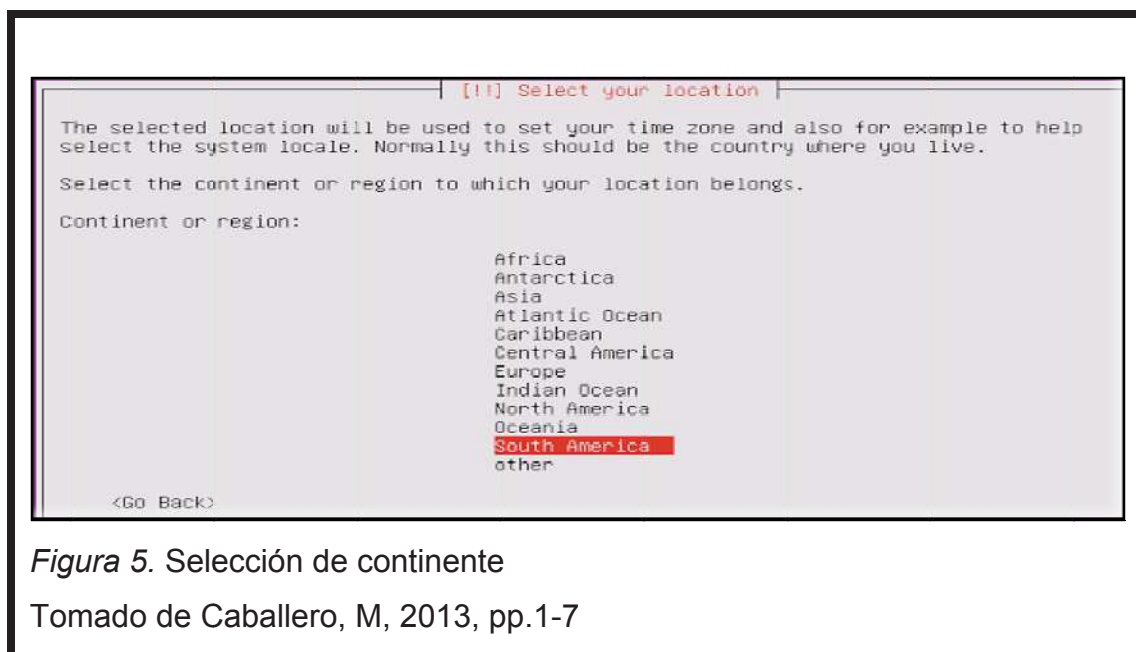


Figura 5. Selección de continente

Tomado de Caballero, M, 2013, pp.1-7

Paso 5.- El país

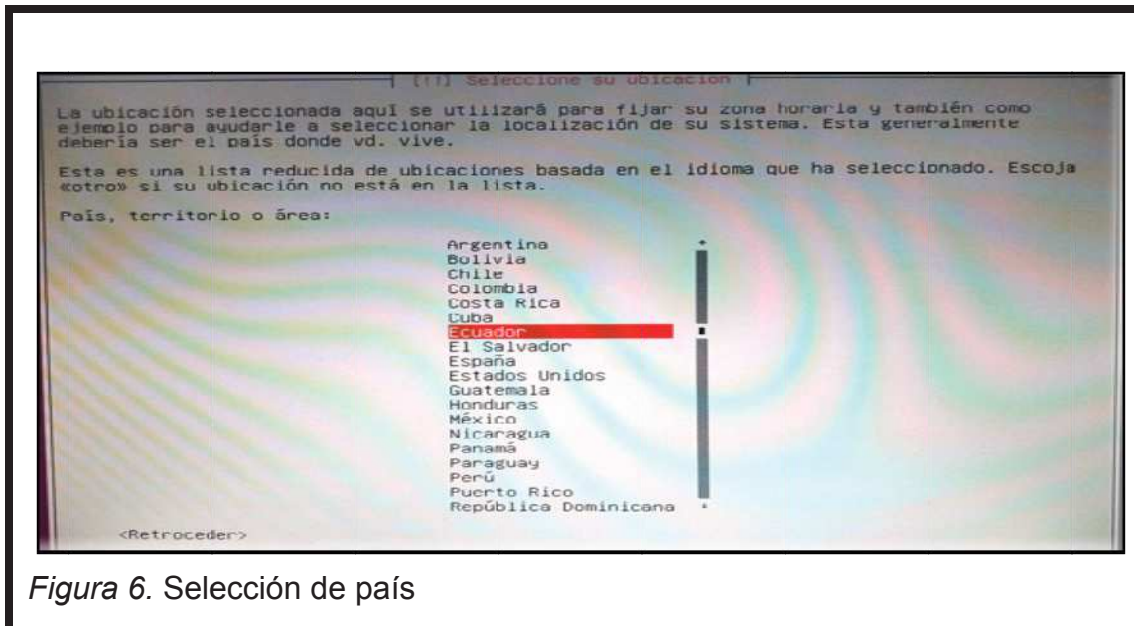


Figura 6. Selección de país

Paso 6.- El tipo de teclado

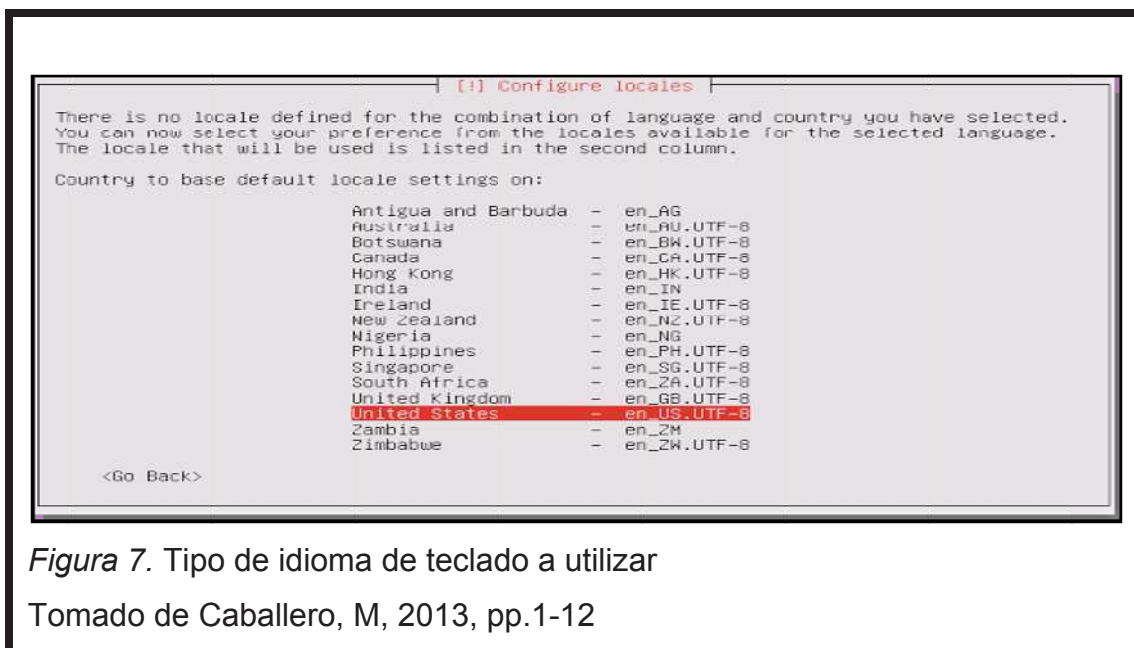


Figura 7. Tipo de idioma de teclado a utilizar

Tomado de Caballero, M, 2013, pp.1-12

Paso 7.- Se indica que no se buscará el tipo de teclado que se utilizará.

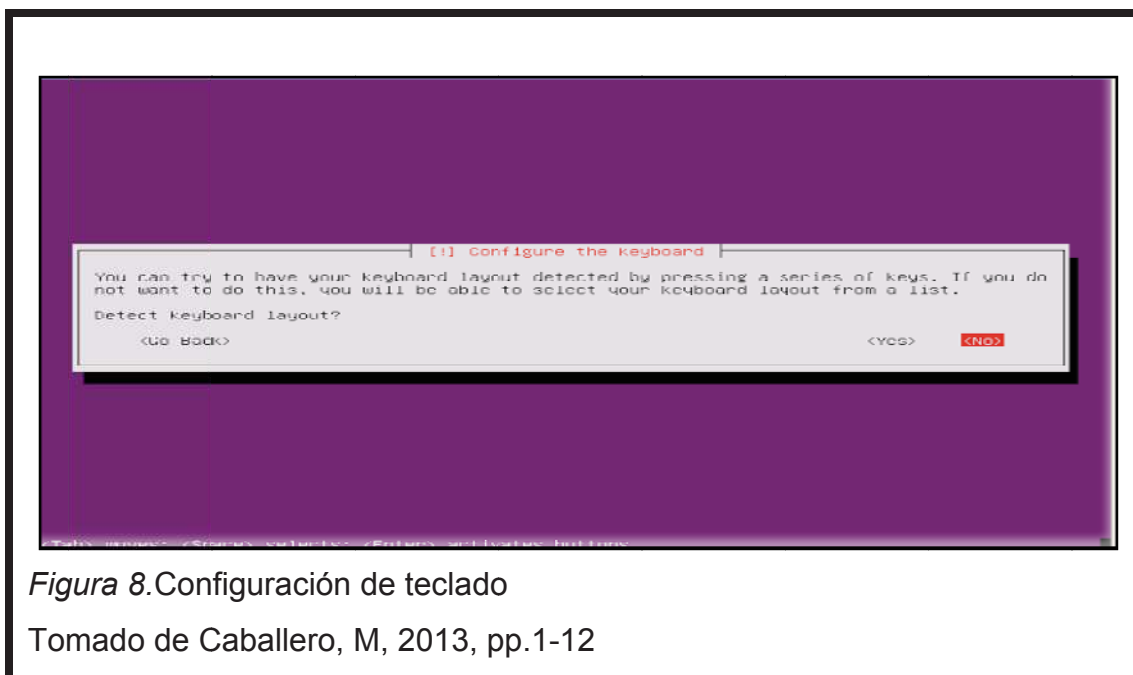


Figura 8. Configuración de teclado

Tomado de Caballero, M, 2013, pp.1-12

Paso 8.- Se escogerá el tipo de teclado latino.

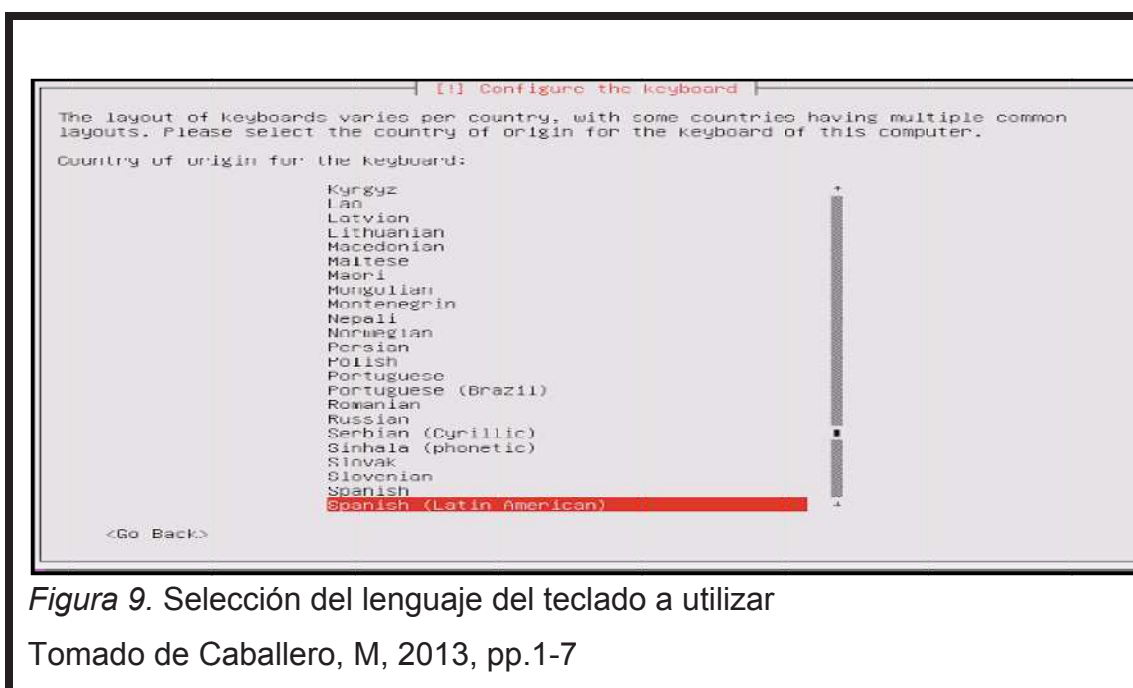


Figura 9. Selección del lenguaje del teclado a utilizar

Tomado de Caballero, M, 2013, pp.1-7

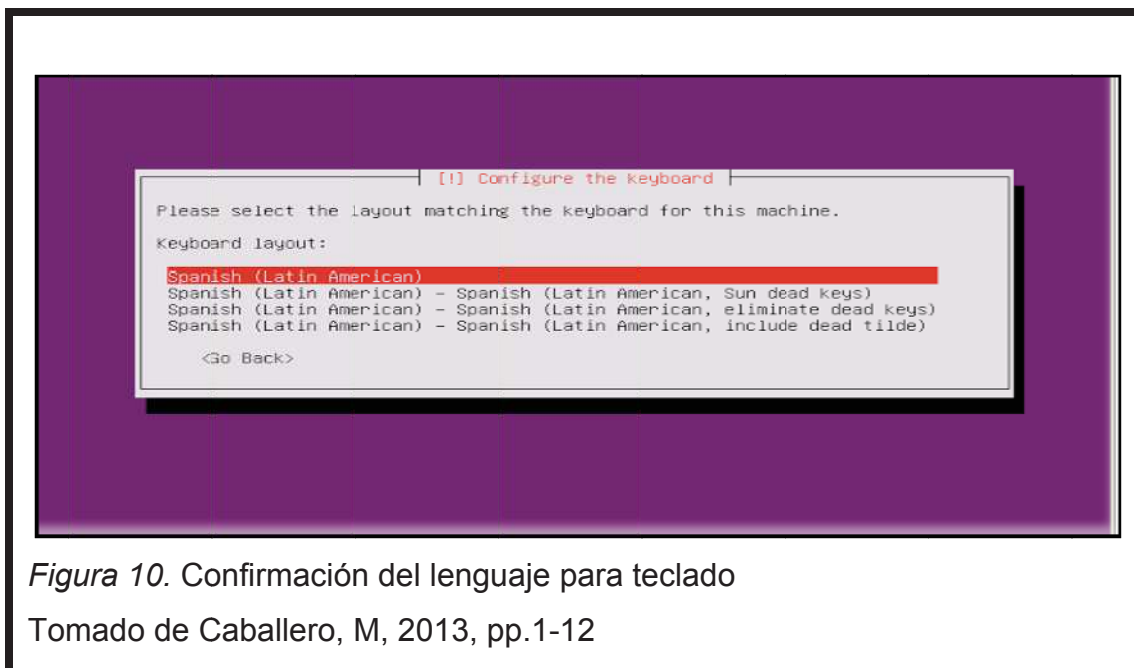


Figura 10. Confirmación del lenguaje para teclado

Tomado de Caballero, M, 2013, pp.1-12

Paso 9.- Se iniciara la carga de los componentes indicados.

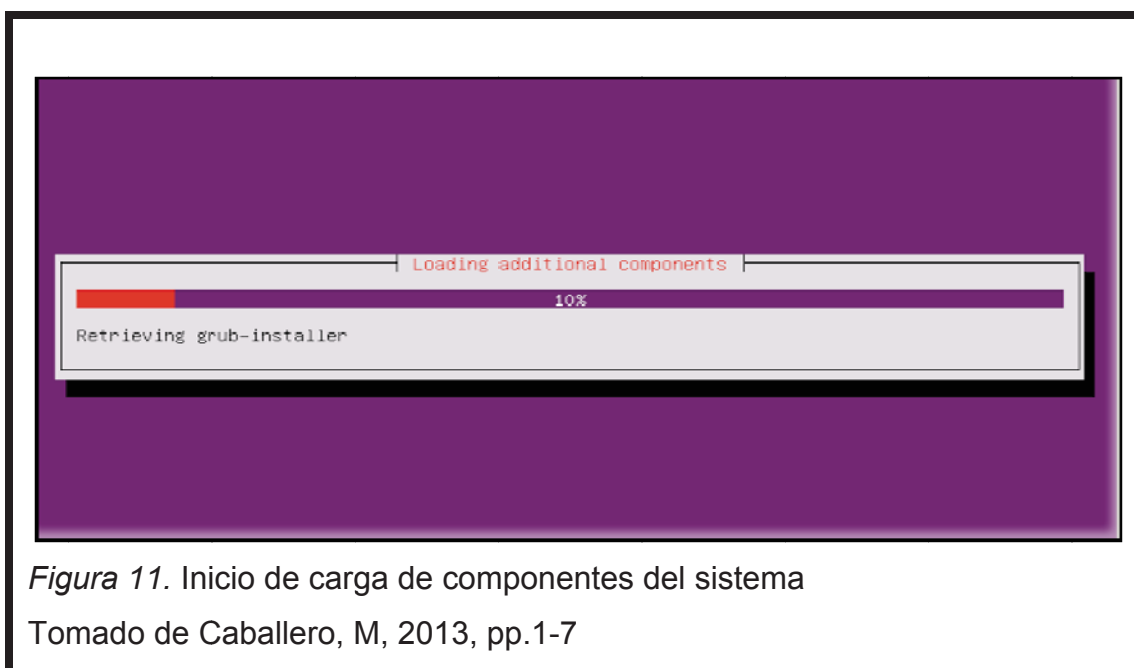
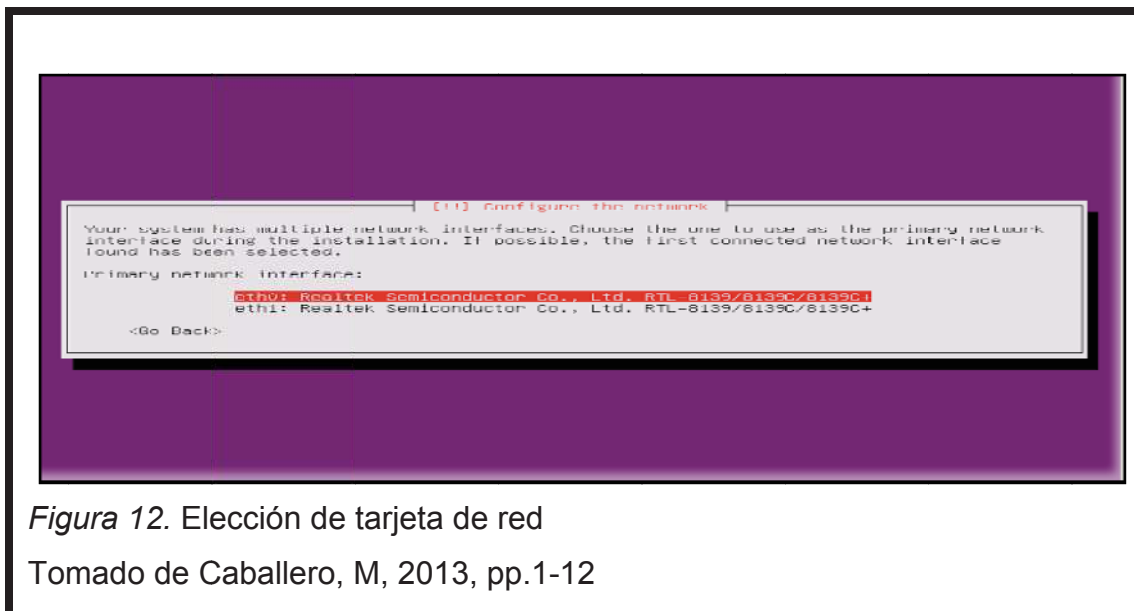


Figura 11. Inicio de carga de componentes del sistema

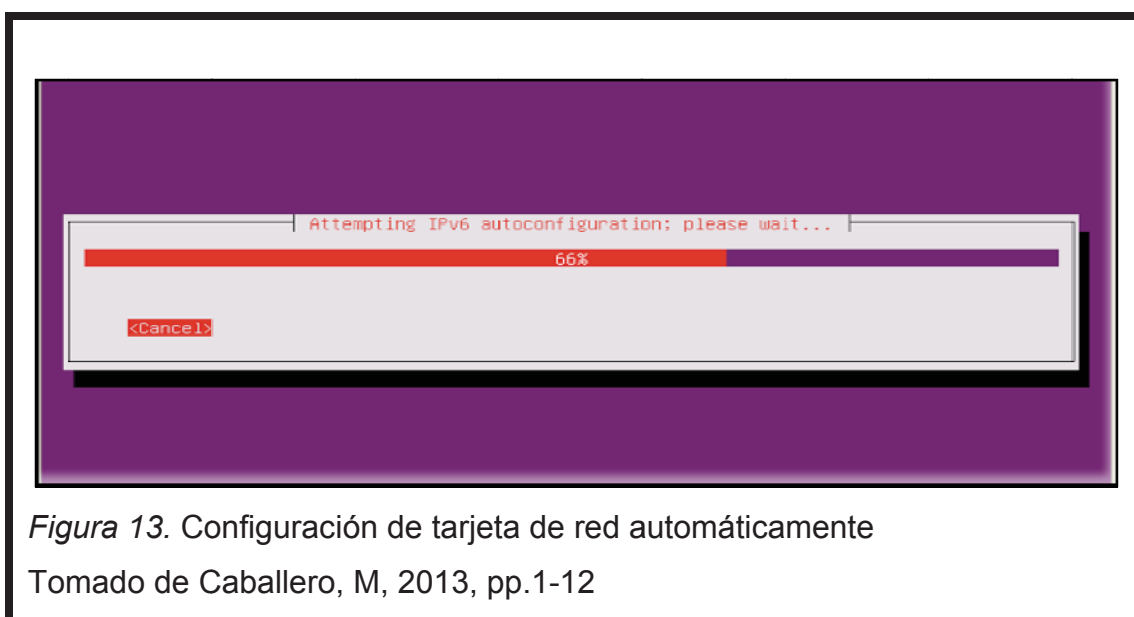
Tomado de Caballero, M, 2013, pp.1-7

1.10.1 Configuración de Red

Finalizada la carga de los componentes mencionados, el sistema comenzará a la detección y configuración de la o las tarjetas de red que el servidor posee.



Si la red tiene un servidor DHCP, intentará obtener una dirección ip automáticamente.



Finalizada la configuración de la tarjeta de red, solicitará un nombre o hostname con el cual se identificará el servidor al igual que se creará un usuario administrador con una contraseña.

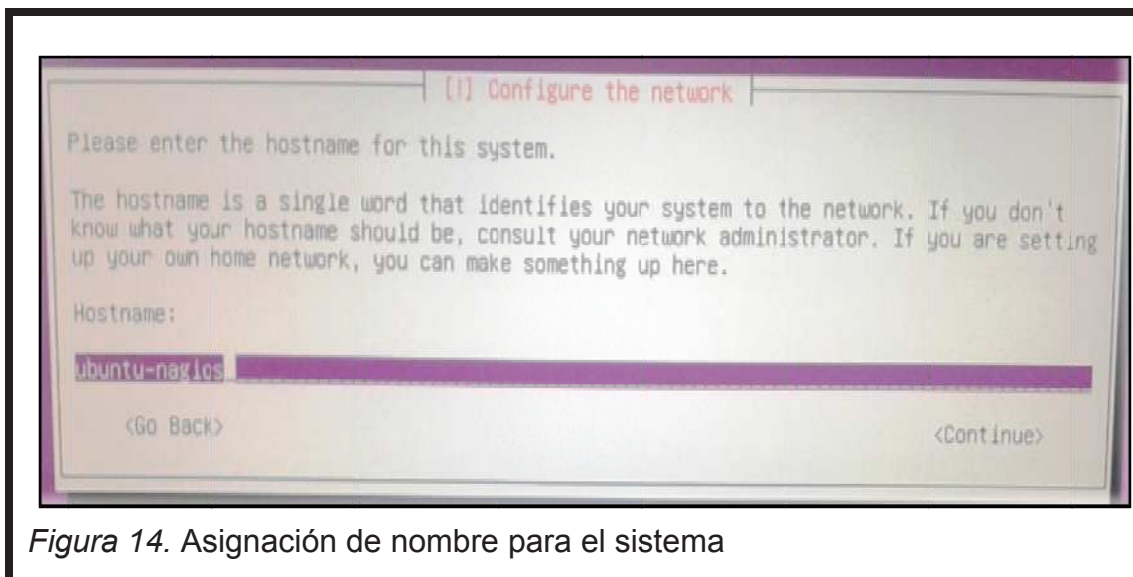


Figura 14. Asignación de nombre para el sistema

En el proceso de instalación, nos dará una opción de encriptar el directorio home, se indicará que no

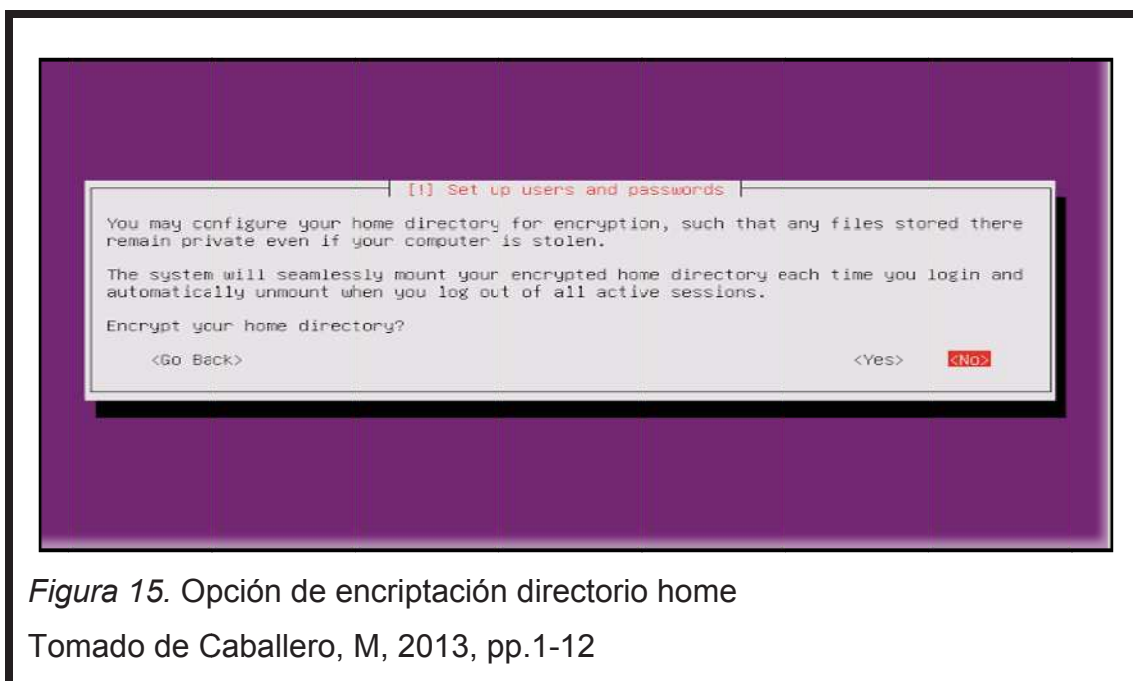


Figura 15. Opción de encriptación directorio home

Tomado de Caballero, M, 2013, pp.1-12

1.10.2 Particiones (Boot, Root, Home, Swap)

Para que el sistema operativo Linux funcione correctamente de cualquier distribución será necesario realizar las siguientes particiones al disco duro.

- **Boot (/boot).**-Almacena la imagen del kernel al iniciar el sistema operativo
- **Root (/).**-Esta partición hace referencia al **home directory** de la raíz del sistema
- **Home (/home).**-Es el directorio del usuario creado, regularmente del o de los usuarios regulares
- **Memoria o Área de Intercambio (Swap).**- Está memoria hace referencia a una memoria **RAM** virtual, que para el sistema Linux deberá ser el doble de la memoria física instalada.

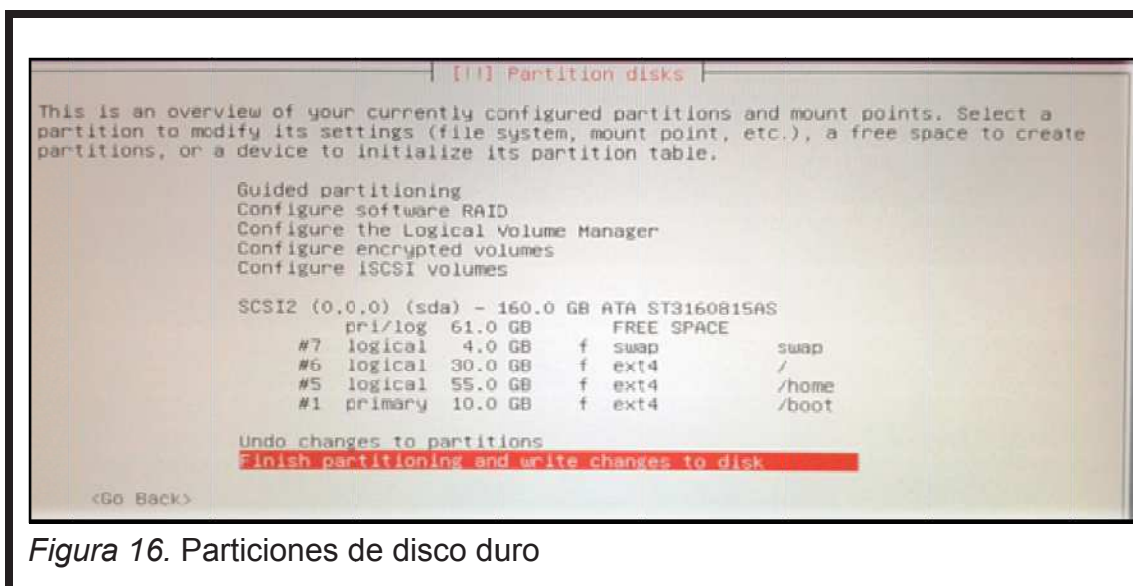


Figura 16. Particiones de disco duro

Una vez finalizada las particiones se acepta los cambios y se formatea el disco duro

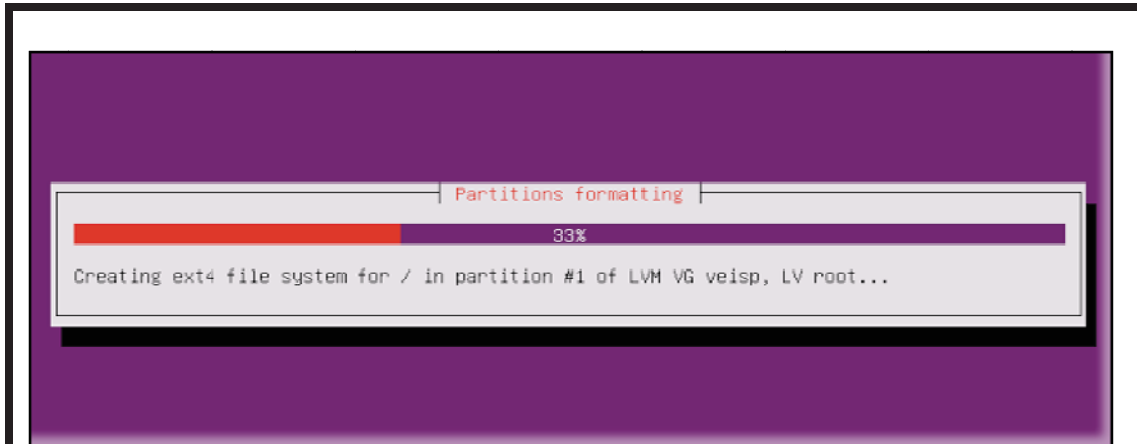


Figura 17. Formateo de disco duro

Tomado de Caballero, M, 2013, pp.1-12

Luego de formatear el disco, comenzara el proceso de instalación del sistema operativo.

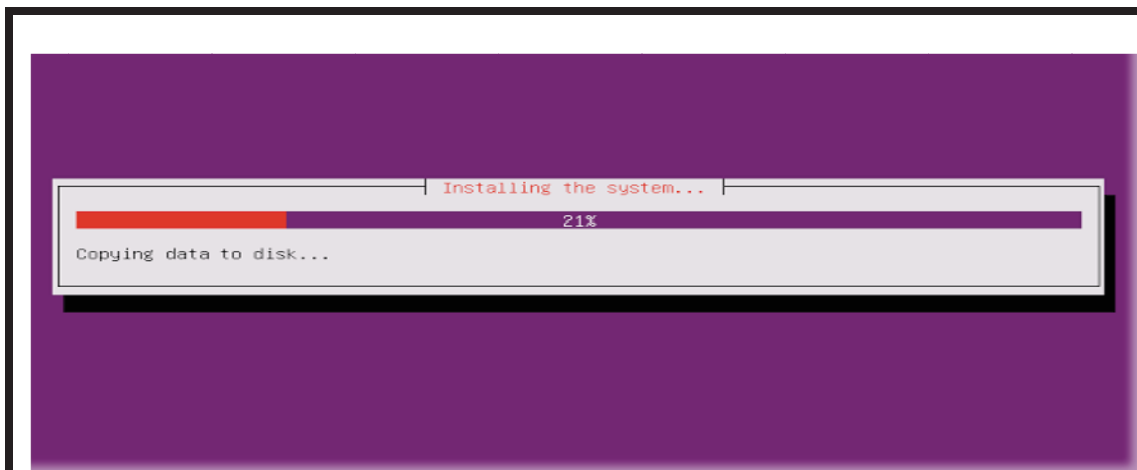


Figura 18. Instalación del sistema operativo

Tomado de Caballero, M, 2013, pp.1-12

En el transcurso de la instalación el programa solicitará información acerca de la puerta de salida a internet, si cuenta con *proxy* se ingresara la información o si no se continuara con la instalación dejando el campo en blanco.

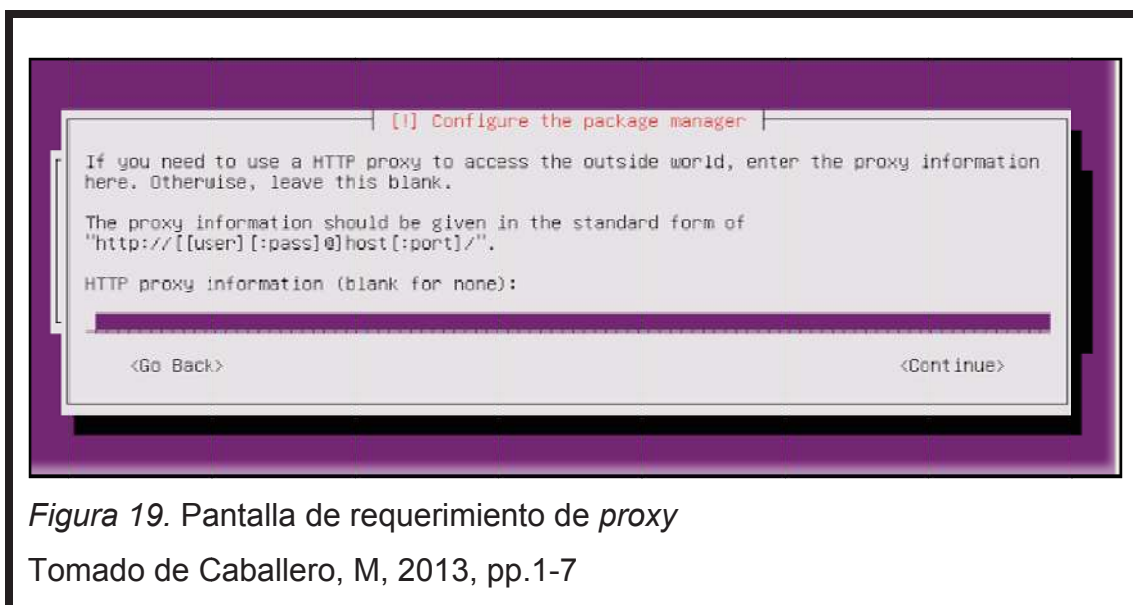


Figura 19. Pantalla de requerimiento de proxy

Tomado de Caballero, M, 2013, pp.1-7

Posteriormente otra pantalla permite realizar las actualizaciones automáticas, en este caso la opción “*Noautomaticupdate*” debido a que el proceso se lo realiza cuando el sistema operativo este instalado y se usara comando de actualización desde consola.

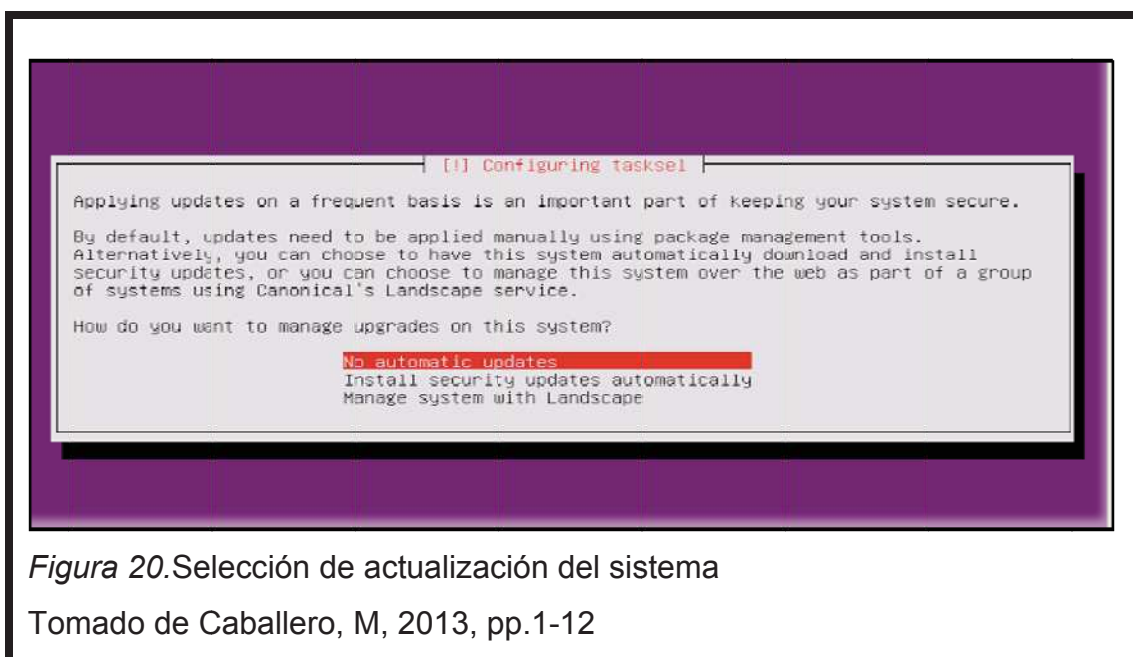


Figura 20. Selección de actualización del sistema

Tomado de Caballero, M, 2013, pp.1-12

Al final se tendrá opciones de configuración de programa considerando que lo instalado es un servidor básico, en este punto para poder acceder desde otro computador hacia el servidor se escogerá la opción (*OpenSSH server*)



Figura 21. Instalación de instalación de SSH

Tomado de Caballero, M, 2013, pp.1-7

1.10.3 Instalación del gestor de arranque *GRUB*

Como último paso se realizará la instalación del gestor de arranque (*GRUB*), este gestor tiene como función principal interactuar con los distintos sistemas operativos instalados y dar al usuario al momento de iniciar el servidor o computador la opción a elegir qué sistema arrancará.

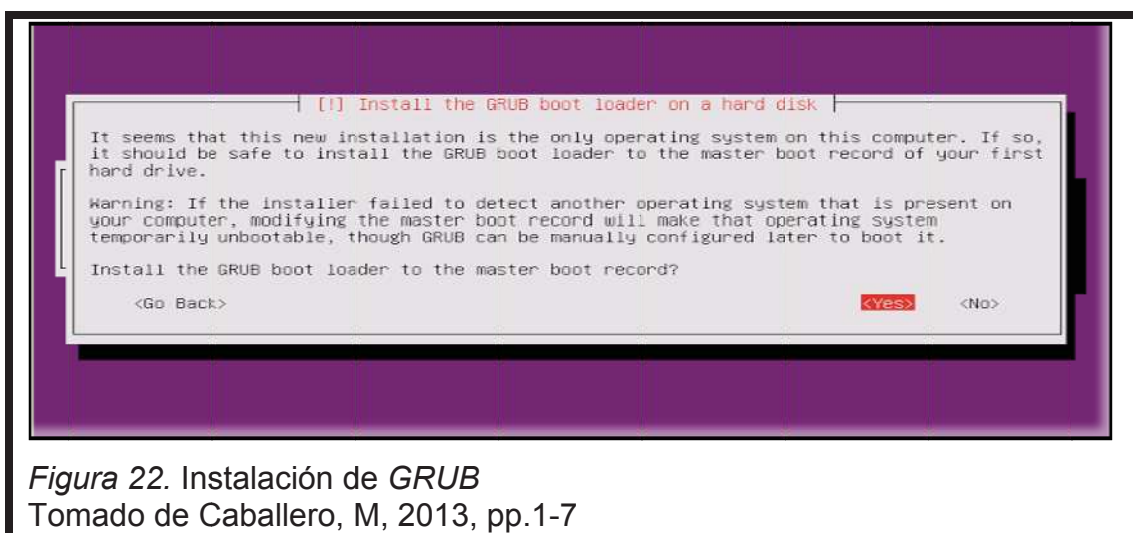
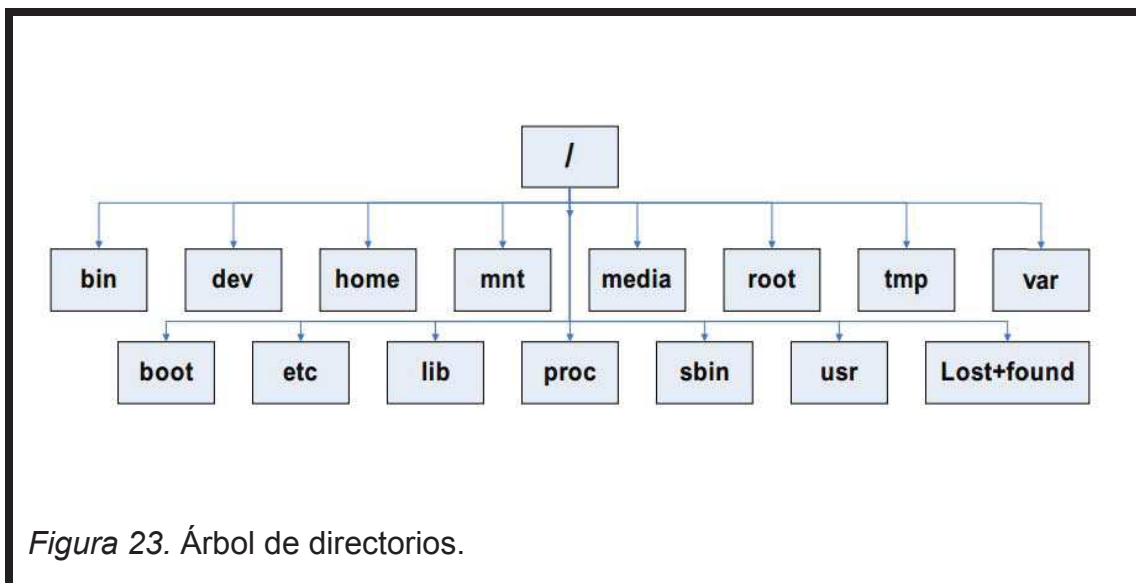


Figura 22. Instalación de *GRUB*

Tomado de Caballero, M, 2013, pp.1-7

1.11 Sistema de archivos

Los sistemas operativos basados en Linux no poseen el concepto de discos duros así como lo tiene Windows. Todos los directorios son archivos que se encuentran contenidos en un *(filesystem)* unificado virtual los mismos que se encuentran en un árbol jerárquico similar a la estructura de archivos de la plataforma Unix.



Descripción Directorios

Sistema de archivos: Integrado por los siguientes directorios:

Directorios

- **(/bin).**- Contiene archivos ejecutables para cada uno de los usuarios
- **(/dev).**- Contiene los dispositivos de entrada y salida, ejemplo: teclado, mouse, tarjeta de sonido etc.
- **(/home).**- Es el *home directory* de todos los usuarios que se crea, usuarios regulares.
- **(/mnt).**- Es el punto de montaje para otros sistemas de archivos, es recomendado pero no obligatorio, se utiliza para montar dispositivos, ejemplo: *CDROM, FLOPPY*, etc.

- **(/root).**- Es únicamente el *home directory* de la raíz.
- **(/tmp).**- Directorio de almacenamiento temporal.
- **(/var).**-Residen los *log* de los servicios de correo y sus eventos.
- **(/boot).**- Se tiene la imagen del *kernel* en el inicio del sistema.
- **(/etc).**- Residen todos y cada de unos de los archivos de configuración de los servicios ejemplo: *mail, dhcp, iptables,etc.*
- **(/lib).**- Contiene las librerías para los usuarios como para el *root*.
- **(/proc).**- Directorio virtual del sistema de archivos, se obtiene únicamente resultados o estadísticas del sistema.
- **(/sbin).**- Contiene la administración de los archivos ejecutables para el *root*.
- **(/usr).**-Contiene archivos, librerías, programas, ejecutables para los usuarios.
- **(/lost+found).**- Se almacena los archivos o bloques perdidos cuando el sistema falla, similar como el comando (*chkdsk /r*) utilizado en Windows.

1.12 Monitoreo de Redes

Introducción al monitoreo de redes.

Debido al gran avance tecnológico que se ha dado a nivel mundial, las empresas medianas y grandes han sufrido cambios importantes dentro de sus redes empresariales, a tal punto que han llegado a converger toda su información, aplicaciones y servicios a una red de datos. Es por esto que los departamentos de tecnologías deberán implementar sistemas de monitoreo adecuados para el control de los distintos componentes de red con la finalidad de alcanzar una alta disponibilidad. Una razón puede ser que los computadores y servicios estén defectuosos o lentos. Otra es el seguimiento que se debe realizar de los componentes de red que suelen tener un mal funcionamiento de hardware o software en un momento inesperado, ocasionando inestabilidad. También es importante evitar fallos en la red instalando alertas en caso de alguna avería.

1.13 Concepto de monitoreo

Se define como monitoreo de red al uso de un sistema que constantemente verifique el estado de los componentes activos que integran una red, sean estas: computadoras, servidores, *switch*, etc. En busca de alguna anomalía presentada a nivel de *hardware* o *software* para luego informar al personal de TI mediante herramientas como correo electrónico u otros métodos establecidos.

1.14 Concepto Redes LAN

Las siglas LAN vienen de (*Local Área Network*), Red de área local. Una LAN es una red que conecta a varios computadores dentro de un espacio relativamente pequeño en donde los usuarios pueden compartir y acceder a los recursos compartidos como impresoras, archivos, datos, etc. (Toranzo y Rivas, 2009, p.6)

1.15 Administración de Redes LAN

La administración de redes es un conglomerado de técnicas y herramientas, con la finalidad de mantener un desempeño óptimo, eficiente y seguro ante amenazas o anomalías que se pueden presentar en su operación diaria y actuar de forma inmediata antes que estas afecten a la parte operacional.

Las exigencias de hoy en día cada vez son mayores, por tal motivo se tiene cinco áreas de funcionalidad que un administrador de red deberá conocer para garantizar una red operativa, que son:

1.- Configuración

Obtención de información de todos los elementos activos de red y sus configuraciones para realizar cambios preventivos o correctivos

2.- Fallas

Se encarga de documentar y reportar los eventos no deseados, para corregir problemas y así aumentar la productividad de todos los usuarios que hacen uso de la red.

3.- Desempeño

Principal responsabilidad de un administrador de red es garantizar el desempeño óptimo de la red, así como también sacar estadísticas de tráfico de red mediante la monitorización.

4.- Seguridad

Es uno de los puntos más discutidos hasta el momento, ya que aun que se tenga grandes herramientas de protección de información son susceptibles de ser vulneradas por los conocidos *hacker's*, más que garantizar la completa seguridad de la información se trata de mitigar y prevenir los ataques de usuarios externos como internos mediante el uso políticas y técnicas de seguridad.

5.- Contabilidad

Este paso se encarga de llevar el costo y el beneficio que con lleva a los usuarios como a los departamentos el uso de la red, conociendo cuantas veces estos hacen uso de los recursos.

1.16 Concepto Redes de Área Extendida WAN

Las siglas WAN viene de (*Wide Área Network*) que significa Red de Área Amplia, Una red WAN es aquella que cubre distancias muy extensas, la cual permite brindar una conectividad a toda una ciudad e incluyendo aún país, este tipo de red usan la gran mayoría de empresas que tienen oficinas entre distintas ciudades o también un proveedor de internet, los cuales usan para dar conectividad a sus clientes. (Toranzo y Rivas, 2009, p.6)

1.17 Herramientas de Monitoreo de Redes

Para realizar una monitorización de una red de datos se tiene en el mercado y en el Internet una variedad de programas pagados o libres que cumplen las expectativas, pero que cada uno de ellos carece de ciertas aplicaciones o necesidades que un administrador de red lo requiere.

1.18 Características entre las distintas Herramientas de Monitoreo

Entre las distintas herramientas de monitoreo que existe bajo la licencia de *Software* libre, se ha realizado un cuadro comparativo con las características de cada una de las aplicaciones mencionadas.

Tabla 2. Características entre distintos sistema de monitoreo

Características	Nagios	Zabbix	Pandora FMS	Zenoss	Osmius	Hobbit
Interfaz WEB	✓	✓	✓	✓	✓	✓
Suficiente Información	✓					
Reportes	✓	✓	✓	✓	✓	
Bases de Datos	✓	✓	✓	✓	✓	✓
Vista Gráfica	✓	✓	✓	✓	✓	
Licencia Libre	✓	✓	✓	✓	✓	✓
Autenticación de Usuarios	✓					
Envío de Alertas	✓	✓	✓	✓	✓	✓
Robustez	✓	✓	✓			
Uso en redes locales	✓	✓	✓	✓	✓	✓
Uso en redes empresariales	✓	✓	✓			✓
Manejo de plugins	✓	✓	✓	✓	✓	✓

Nota: Como parte importante de un sistema de monitoreo se procede a comparar las fortalezas y las debilidades de acuerdo a los parámetros requeridos y solicitados por parte de la empresa para la monitorización, obteniendo como resultado que el programa nagios cumple con todas las exigencias, por tal motivo se toma la decisión de optar por él para la implementación del sistema de monitoreo.

2. Instalación del Sistema de Monitoreo Nagios

2.1 Historia

En el año 1996 el *Ethan Galstad* crea una sencilla aplicación para servidores Novell en MS-DOS, llamado *Netware "ping"*, la misma que tuvo aplicaciones externas de terceros. Este concepto básico de arquitectura da paso al nacimiento de Nagios

En 1998, considerando entrar al negocio de monitoreo, *Ethan* utiliza las ideas y la arquitectura de su trabajo anterior para comenzar a construir una aplicación nueva, mejorada y diseñada para funcionar bajo ambientes Linux

Un año más tarde 1999, *Ethan* decide publicar su obra como un proyecto de código abierto bajo el nombre de **"NetSaint"** el mismo que utiliza *plugins* en dicha distribución.

Los *plugins* que fueron distribuidos originalmente como parte de la distribución de *NetSaint*, pronto se separarían como un proyecto de Nagios *Plugins*.

En el año 2002, debido a cuestiones de marcas con el nombre *NetSaint*, *Ethan* decide cambiar el nombre del proyecto a "Nagios".

A partir del año 2007. Nagios es honrado como uno de *Infoworld* de *Best of Open Source Software*, así permitiéndole ganar varios premios como por ejemplo: Premios de la Asociación *SourceForge.net* entre otros. (Nagios Enterprise, 2014)

2.2 Nagios

En la actualidad el proyecto que inicio como *NetSaint* ahora llamado Nagios es un *software* de código libre siendo su principal función la monitorización de equipos y servicios de red. Fue desarrollado en lenguaje C, el cual asegura una rápida ejecución cuando la información sea procesada, de igual manera accede a actualizaciones de manera libre, de tal manera que él o a los usuarios del sistema siempre cuenten con nuevas actualizaciones y con soporte de una gran cantidad de colaboradores, como también tener acceso a su código fuente para que un usuario que tenga un conocimiento mediano alto pueda modificar las características a sus necesidades.

Con Nagios el o los administradores de red pueden realizar un monitoreo completo de los equipos activos de una manera exhaustiva, de tal manera que tendrán el control para determinar y encontrar problemas que puedan ocasionar un mal funcionamiento de una red antes de que los usuario lo perciban, permitiéndoles tomar acciones inmediatas e idóneas en base a los resultados obtenidos por parte de la herramienta.

(Dorado y Moran, 2009, pp.6-9)

La funcionalidad de Nagios se basa en los distintos archivos de configuración en donde se puede especificar los componentes red a ser monitoreados, con qué periodo y con qué frecuencia se lo realizara, a quien y como se enviará los resultados de la monitorización, para que funcione todas estas especificaciones Nagios cuenta con una gran cantidad de *plugins* los cuales son desarrollados en varios lenguajes de programación, estos se encargan en el monitoreo y recopilación de información de acuerdo a las especificaciones dadas en los archivos de configuración especificados. La herramienta tiene una interfaz web con la cual permite visualizar de una manera amigable, rápida y sencilla los estados de los distintos servicios y dispositivos de red que se encuentran monitoreando, además tiene la capacidad de presentar reportes en base a la

información recolectada de los sucesos o anomalías generadas en la red. (Nagios Enterprise, 2014)

2.3 Estructura

Nagios como parte esencial para su funcionamiento y ejecución tienen la siguiente estructura que se detallará brevemente a continuación.

Núcleo.- Su objetivo principal es el de procesar toda la información enviada por los *plugins*, además es el contenedor de todo el programa para la realización del monitoreo de los equipos y servicios de red.

Plugins.- También conocidos como *script*, son programas pequeños escritos en varios lenguajes de programación, ejemplo: en lenguaje c, c++, perl, php, java, python o bash, que como labor principal es la recolección de información de la monitorización predefinidos en los archivos de configuración, además Nagios es independiente del lenguaje con los cuales fueron desarrollados los *scripts*, por que únicamente procesa la información proporcionada por el mismo.

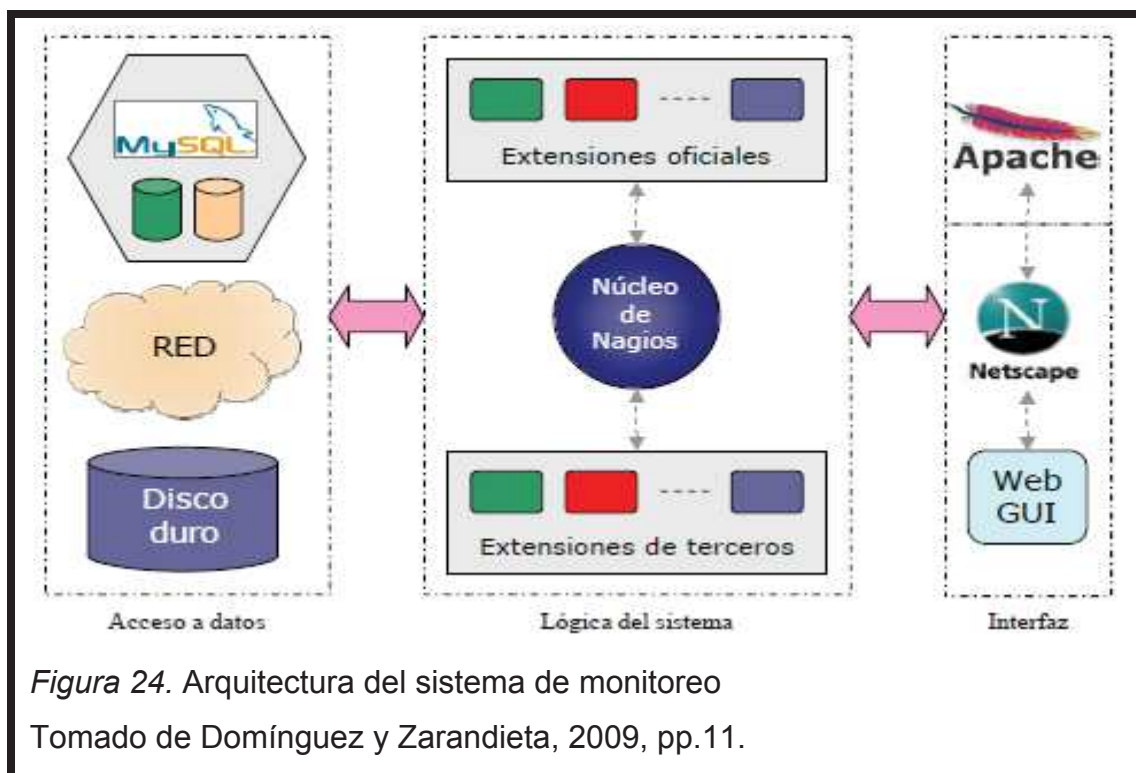
Interfaz web.- Mediante esta herramienta, al administrador le permitirá visualizar de forma gráfica los distintos equipos activos de red y además obtener los resultados de la monitorización, permitiéndole encontrar las distintas anomalías que se pueden presentar dentro de ella, como también proporciona opciones para la elaboración y generación de reportes.

Adicionalmente dentro de la interfaz web se tiene varias opciones los cuales se explica brevemente.

- **Mapa.-** Muestra de forma gráfica el diseño global de todos los equipos y enlaces de comunicación que se encuentran monitoreados.
- **Equipos.-** Presenta información del estatus de todos los equipos, indicándonos si se encuentran activos o no.

- **Servicios.-** Muestra servicios que se están ejecutando con sus diferentes estados.
- **Grupo de equipos.-** Muestra de forma grupal de cada componente de red con su estado y servicios que se ejecutan en cada uno de los equipos.
- **Información de un equipo.-** Presenta información como nombre, dirección ip, grupo, etc., de un solo equipo.
- **Información resumida.-** Muestra información de forma grupal de los componentes de red, de los equipos y el estado de los servicios resumida.
- **Servicio de alertas.-** Muestra información de todos los equipos y servicios que presentan fallos o comportamientos anormales dentro de la red.
- **Disponibilidad.-** Indica que porcentaje de disponibilidad ha tenido un servidor o un equipo.
- **Histogramas.-** Mediante esta opción nos permite seleccionar el tipo de reporte sea este equipo o servicio de un determinado componente de red y generar información detallada de forma gráfica de una fecha específica.
- **Historial.-** Mediante esta opción da a conocer información detallada de todos los equipos y servicios que han sufrido anomalías en su comportamiento, así el administrador puede ejecutar acciones preventivas o correctivas frente a los resultados obtenidos en este módulo. (Nagios Enterprise, 2014)

En la siguiente figura se indicará la estructura general y el funcionamiento del sistema nagios.



Su funcionamiento parte desde el núcleo de Nagios con los plugins de extensiones de terceros instalados recolectan información de una red LAN o WAN, base de datos, discos duros, etc., y a su vez presentan la información por medio del servidor web Apache en un navegador de internet.

2.4 Características de sistema de monitoreo Nagios

Las principales características del sistema de monitoreo Nagios son las siguientes:

- Visualización global de la red en tiempo real mediante el uso de la interfaz web, permitiendo generar información de forma gráfica.
- Monitorización de los servicios definidos en el archivo de configuración como son: HTTP, SSH, SNMP, POP3, etc.
- Servicios de monitoreo de equipos activos de red como son: servidores, impresoras, *Switch* y *Router's*.

- Servicio de monitoreo de los recursos y servicios de los equipos, ejemplo: uso de memoria swap, memoria RAM utilizada, carga del procesador, espacio utilizado en disco duro. Ping, etc.
- Servicios de monitorización de equipos clientes como Microsoft Windows mediante el uso de agentes como por ejemplo: *NRPE_NT oNSClient++*.
- Servicios de monitorización remota a través de *Secure Sockets Layer(SSL)* o *SSH*
- Múltiples formas de envío de mensajes de notificación de monitoreo como correo electrónico, mensajería instantánea (sms), audio, etc.
- Permite diferenciar entre equipos caídos y equipos inalcanzables.
- Jerarquización de red
- Notificación de forma grupal a los contactos, de manera que cuando ocurren problemas en los equipos o servicios se envíe una notificación a todos los administradores y no a uno solo.

2.5 Ficheros y Directorios

Cuando se realiza una instalación de Nagios, este por defecto se instala en *(/usr/local/nagios/)*, en donde se encuentran todos los archivos de funcionamiento, configuración y ejecución. Así como también está formado por otros subdirectorios los cuales se detalla a continuación.

- **bin.-** En este directorio se encuentran los archivos principales de ejecución, se encuentra el ejecutable nagios, el cual se mantiene ejecutándose en un segundo plano.
- **etc.-** Dentro de este directorio se encuentran los archivos de configuración nagios, es aquí donde se define y se especifica los equipos y servicios a ser monitoreados así como también los tiempos de actualización, periodos, contactos y los comandos.
- **libexec.-** Almacena todos los archivos ejecutables de los *plugins*, mismos que pueden ser archivos binarios o *scripts* escritos en cualquier lenguaje de programación.

- ***sbin.***- Almacena los archivos ejecutables llamado *Common Gateway Interface (cgi)* que traducido al español significa Interface de Entrada Común, estos permitirán al administrador solicitar información de un equipo o servicio mediante la interfaz gráfica.
- ***share.***- Contiene toda información que se visualiza en la interfaz web, ejemplo: logos, imágenes, etc.
- ***var.***- En este directorio almacena todos los *logs*, estadísticas e información de la monitorización, dentro del directorio se encuentra el archivo *nagios.log* donde el cual registra información más importante del monitoreo. (Nagios Enterprise, 2014)

2.6 Ajustes de Configuración

2.6.1 Versiones del sistema Nagios

A partir del año 2007 aparece el primer sistema nagios con la versión 3.0a1, esta versión sufrió cambios importantísimos, con el pasar del tiempo surgió varias versiones hasta que llegaron a la versión 3.0.1, ya en esta versión fueron solucionados varios problemas que arrastraron las anteriores versiones como la pérdida de los diferentes tipos de vistas del mapa global, el acceso de usuarios no autorizados a los archivos de host y servicios y entre otros.

Transcurrido el tiempo los desarrolladores a nivel mundial han ido incrementando nuevas funcionalidades y además corrigiendo error encontrados del sistema.

En la actualidad se tiene la versión 3.5.1, esta versión se encuentra estable y recomendada por varios usuarios a nivel mundial, es por esto que se ha tomará la decisión de instalar dicha versión en un ambiente pruebas dentro del Banco Procredit S.A. (Nagios Enterprise, 2014)

2.6.2 Reconfiguración de Red

Cuando se instala un servidor con cualquier sistema operativo que sea este por defecto adquiere una dirección de red asignada dinámicamente o en otras ocasiones no toma ningún tipo de dirección ip, como buena práctica es la reconfiguración de la red, de tal manera que se deberá poner una dirección ip estática. Dentro del ambiente Linux existen diferentes maneras de asignar una dirección ip, uno es por entorno gráfico y otro por consola, en este caso se asignará por consola mediante el uso del siguiente comando: (*nano /etc/network/interfaces*).

Dentro de este archivo de configuración se especificará la dirección ip, la máscara de red, puerta de enlace, y la red a la que pertenece.

2.6.3 Instalación SSH

El protocolo SSH significa *Secure Shell,ssh* es un protocolo que permite realizar conexiones remotas de forma segura hacia otros equipos en la red, la característica más principal es que la información viaja encriptado a través de la red.

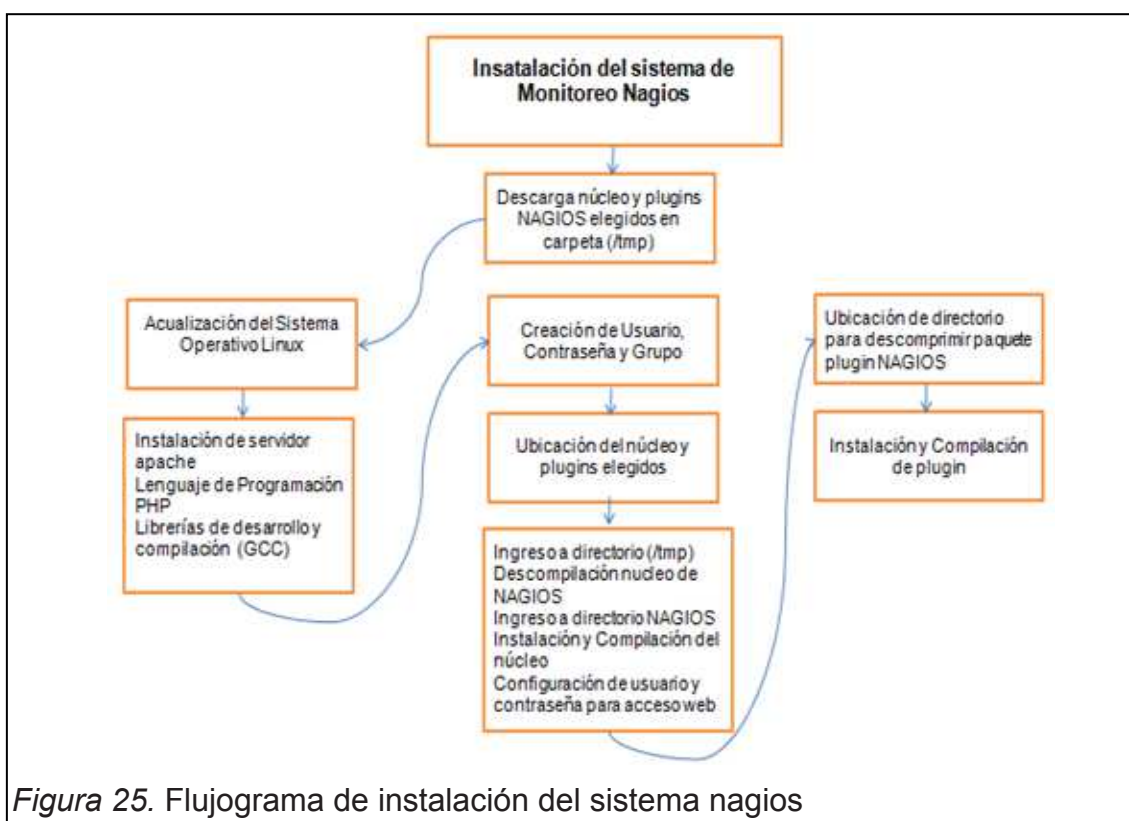
Para un administrador se convierte en una herramienta fundamental ya que podrá acceder a cualquier servidor o equipo de red desde cualquier lugar sin preocuparse de que en el medio haya personas mal intencionadas tratando de obtener información para beneficio propio o para causar daños y perjuicios, esta es una manera en la cual se puede mitigar un problema de seguridad. En entornos Linux este protocolo se lo puede activar al momento de realizar la instalación del sistema operativo, o también se lo puede realizar mediante consola con el siguiente comando dependiendo la distribución, ejemplo Ubuntu: (*apt-getinstall ssh*).

2.7 Instalación del sistema de monitoreo Nagios.

2.7.1 Requisitos de instalación

Como se mencionó en el primer capítulo, la instalación del sistema de monitoreo nagios se hará en un computador de escritorio el cual tendrá el sistema operativo Ubuntu server 12.04 LTS.

Se realizará la actualización completa del sistema mediante el uso del comando *aptitude update*, cabe mencionar que todo el proceso de instalación y configuración se lo ejecutará con el usuario raíz del sistema (*root*).



Las siguientes figuras 26, 27 y 28 se indicarán los pasos para realizar una conexión remota hacia el servidor, autenticación del sistema y la ejecución del comando para la actualización.

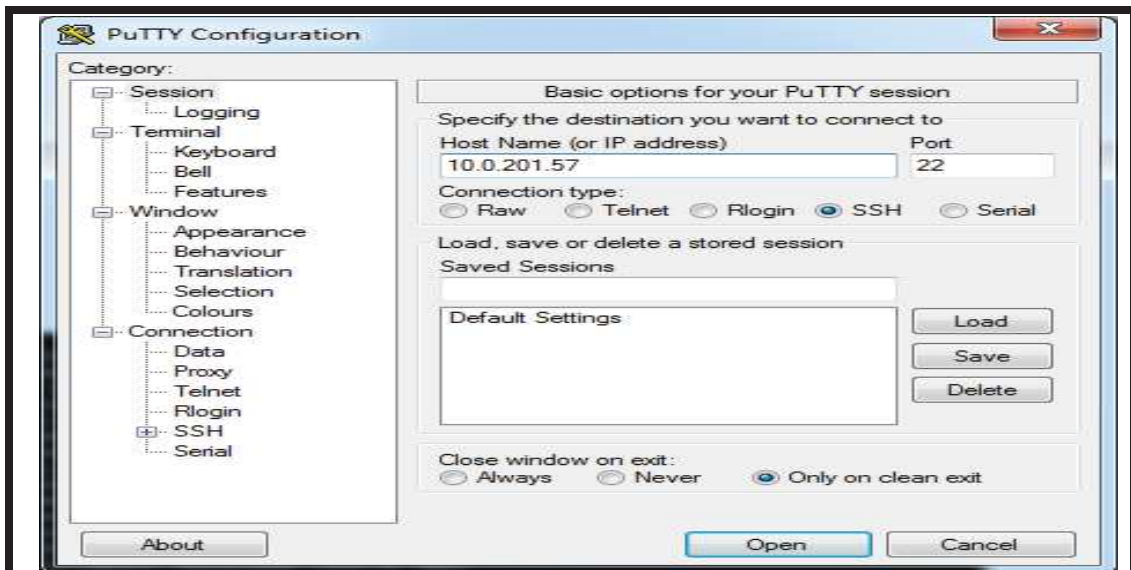


Figura 26. Conexión remota con programa *putty*

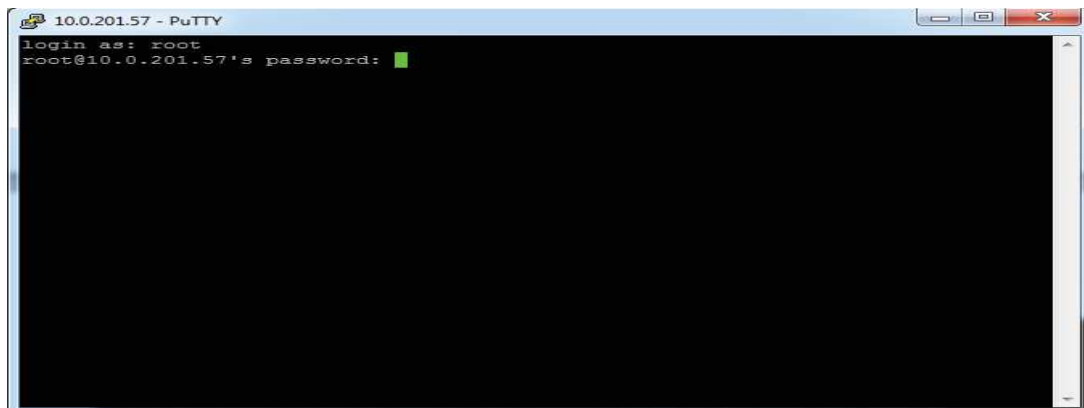


Figura 27. Autenticación de usuario *root*

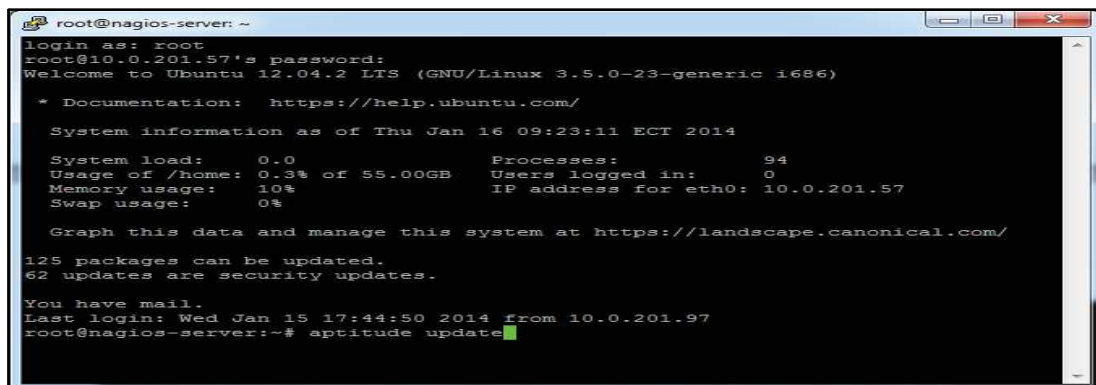


Figura 28. Ejecución de comando para actualización.

Finalizada la actualización se procederá a descargar los paquetes y el *plugin* que se utilizará en la instalación desde la página oficial de nagios, los cuales se guardaran en el directorio temporal (*/tmp*).

La figura 29 muestra los paquetes a utilizarse en la instalación.

Version	Date	Notes	Type	Link
3.5.1	2013-08-30	Latest stable release	Source code	nagios-3.5.1.tar.gz
Version	Date	Notes	Type	Link
1.5	2013-11-27	Latest stable release	Source code	nagios-plugins-1.5.tar.gz

Figura 29. Paquete núcleo de nagios y plugin
 Recuperado el 17 de enero del 2014 de <http://www.nagios.org/downloads>

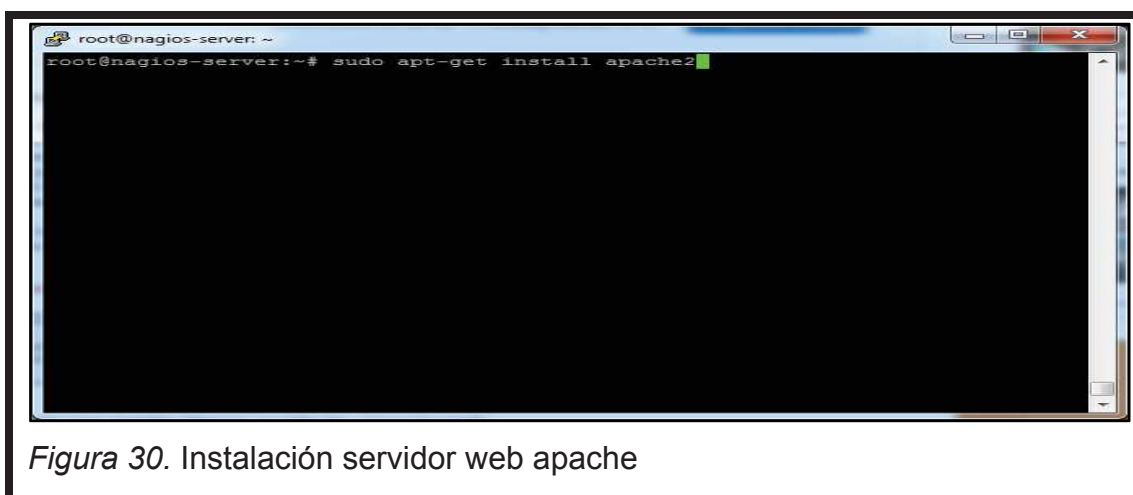
A continuación se instalarán las librerías que utilizará el sistema nagios. Todas las instalaciones se realizarán por conexión remota.

2.7.2 Instalación de paquetes y librerías.

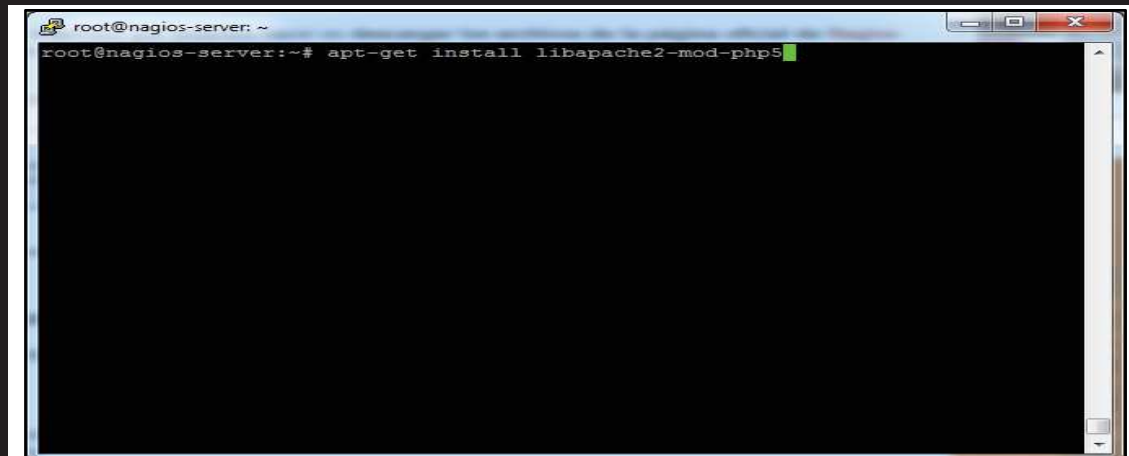
Como prerequisites el sistema requerirá de la instalación de las siguientes librerías.

- Servidor web (Apache 2)
- Lenguaje de programación (PHP)
- Librerías de desarrollo y compilación (GCC)

En la gráfica 30, mediante el uso del comando `apt-get install` se procederá a la instalación del servidor web apache2, terminada la instalación se podrá acceder mediante un navegador de internet.



En la siguiente gráfica 31, se realiza la instalación del lenguaje de programación PHP. Este lenguaje es uno de los más usados para el desarrollo de páginas web.

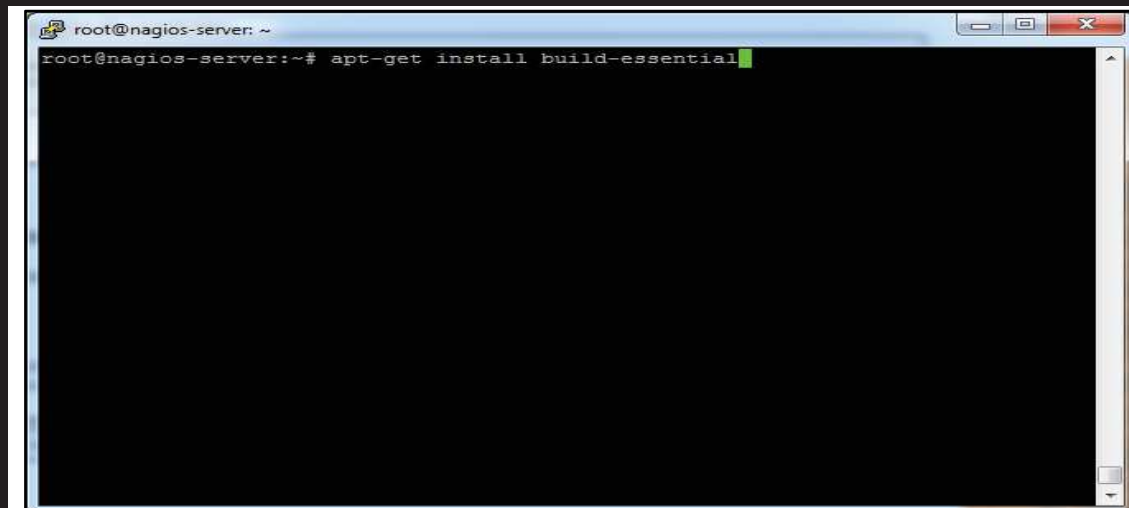
A terminal window titled 'root@nagios-server: ~' with a dark background. The command 'apt-get install libapache2-mod-php5' is entered at the prompt, with a green cursor at the end of the line. The rest of the terminal is empty.

```
root@nagios-server: ~  
root@nagios-server:~# apt-get install libapache2-mod-php5
```

Figura 31. Instalación del lenguaje de programación PHP

Nota. Nagios utiliza el lenguaje PHP en su interfaz gráfica.

En la siguiente gráfica 32, se presenta la instalación de las librerías de desarrollo y compilación que el sistema utilizara para su funcionamiento

A terminal window titled 'root@nagios-server: ~' with a dark background. The command 'apt-get install build-essential' is entered at the prompt, with a green cursor at the end of the line. The rest of the terminal is empty.

```
root@nagios-server: ~  
root@nagios-server:~# apt-get install build-essential
```

Figura 32. Instalación de librerías

En la siguiente figura 33, instalación de las librerías de desarrollo.

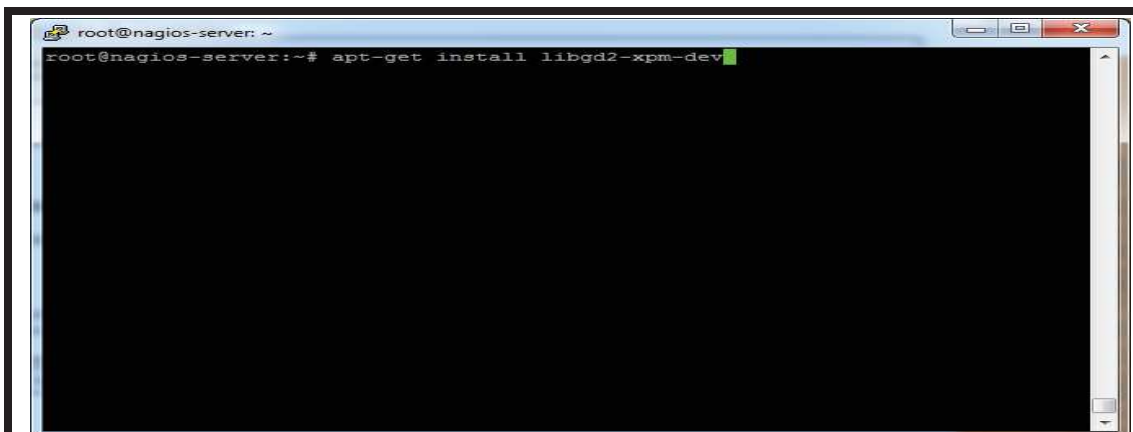


Figura 33. Instalación librerías de desarrollo.

2.7.3 Creación de usuario, contraseña y grupo.

Una vez instalado los paquetes y librerías requeridas por el sistema, se procederá a la configuración del usuario, contraseña y grupo que utilizará el sistema para su funcionamiento. El nombre del usuario a utilizar es: nagios, mismo que será utilizado para la instalación de los demás componentes así como también el grupo llevará el mismo nombre. Con la siguiente orden de comandos se crea lo antes mencionado.

- *root@nagios-server:~# usradd nagios*
- *passwd: Procredit1*
- *usermod -G nagios nagios*

2.7.4 Instalación del núcleo del sistema nagios.

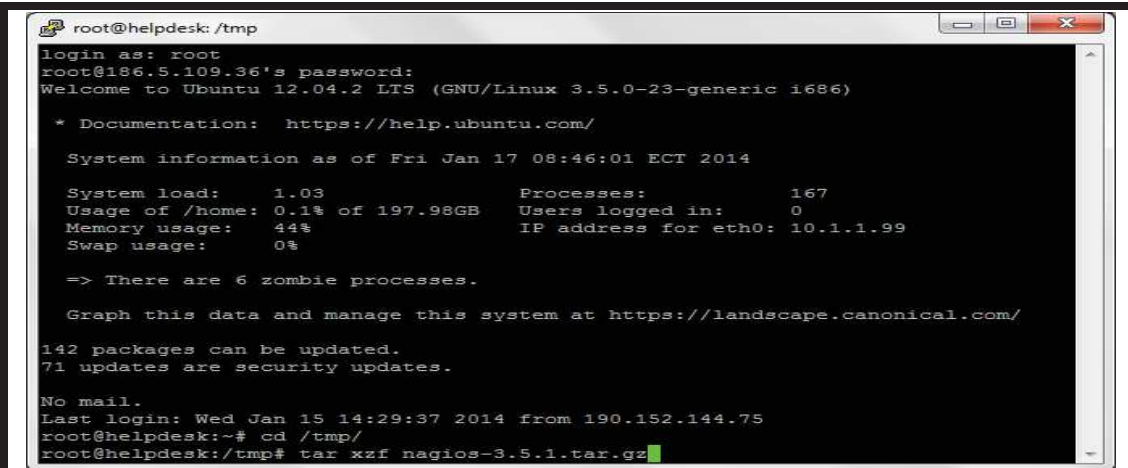
La versión del núcleo de nagios que se instalará es 3.5.1, este núcleo al momento de la instalación fue el actual y el más estable de las anteriores versiones.

Como se observara en la figura 29, se descarga el paquete con su respectivo *plugin*, estos se almacenarán en el directorio (*/tmp*), los pasos de instalación del núcleo serán los siguientes.

Cambiar el directorio en donde se ubica los paquetes del sistema, una vez dentro del directorio se procederá a descomprimir el paquete el cual viene comprimido con la extensión *tar. gz*.

- `root@nagios-server:~# cd /tmp`
- `root@nagios-server:/tmp#`
- `root@nagios-server:/tmp# tarxzf nagios-3-5-1-tar.gz`

En la figura 34 se indicará en la consola la ejecución del comando.



```

root@helpdesk: /tmp
login as: root
root@186.5.109.36's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-23-generic i686)

* Documentation:  https://help.ubuntu.com/

System information as of Fri Jan 17 08:46:01 ECT 2014

System load:   1.03                Processes:    167
Usage of /home: 0.1% of 197.98GB   Users logged in: 0
Memory usage:  44%                IP address for eth0: 10.1.1.99
Swap usage:    0%

=> There are 6 zombie processes.

Graph this data and manage this system at https://landscape.canonical.com/

142 packages can be updated.
71 updates are security updates.

No mail.
Last login: Wed Jan 15 14:29:37 2014 from 190.152.144.75
root@helpdesk:~# cd /tmp/
root@helpdesk:/tmp# tar xzf nagios-3.5.1.tar.gz

```

Figura 34. Descomprimiendo paquete en Linux

Al descomprimir el paquete se accederá a la carpeta del sistema, esto se realiza con la ejecución del comando (*/cd*)

- `root@nagios-server:/tmp# cd /nagios-3-5-1-tar.gz`
- `root@nagios-server:/nagios#`

Una vez dentro del paquete se procederá a realizar la ejecución del paquete de configuración del sistema núcleo de nagios pasándole el nombre del grupo

creado anteriormente, terminada la ejecución del script se procederá a la compilación del núcleo y por último se instalarán los archivos binarios del sistema.

- *root@nagios-server:/nagios# ./configure --with-command-group=nagios*
- *root@nagios-server:/nagios# make all*
- *root@nagios-server:/nagios# make install*

En el proceso de instalación de los archivos binarios del sistema indicarán que además de esos se necesita otros *script* que ayudan al proceso de configuración, estos *script* son de inicio, configuración y directorio de comandos externos.

- *root@nagios-server:/nagios# make install --init*
- *root@nagios-server:/nagios# make install-config*
- *root@nagios-server:/nagios# make install commandmode*

2.7.5 Configuración de interfaz web.

En este punto se continúa con la configuración del sistema nagios para poder ingresar a él mediante la interfaz web. Además se instalará el archivo de configuración del sistema nagios para el servidor apache, este archivo permitirá ver la presentación de nagios mediante web, también se creará el usuario y contraseña para el acceso al sistema, el nombre del usuario es: nagiosadmin y la contraseña: Procredit1, al final se reinicia el servidor apache para que se ejecute los cambios indicados.

Los siguientes comandos son necesarios para configurar lo mencionado:

- *root@nagios-server:/nagios# make install --webconf*
- *root@nagios-server:/nagios# htpasswd -c /usr/local/nagios/etc/htpasswd.usersnagiosadmin*

- *Password: Procredit1*
- *root@nagios-server:/nagios# /etc/init.d/ apache2 reload*

2.7.6 Instalación de Plugin

Terminada la instalación y configuración de los archivos de nagios, se procederá a descomprimir el *plugin*, este paquete contiene todos los objetos que se utilizan para la configuración y monitorización del sistema.

Los pasos y el comando para descomprimir son similares a los que se utilizaron en el paquete núcleo.

- *root@nagios-server:/nagios# cd /tmp*
- *root@nagios-server:/tmp# tarxzf nagios-plugins-1.4.15.tar.gz*
- *root@nagios-server:/tmp# cd nagios-plugins-1.4.15.tar.gz*
- *root@nagios-server:/nagios-plugins#*

Por último se compila e instala el paquete.

2.7.7 Acceso al sistema por interfaz web.

Al final de todas las instalaciones realizadas se podrá acceder mediante el uso de un navegador de internet al sistema de monitoreo, la dirección que debe apuntar el navegador es la ip del servidor o con el nombre *localhost* seguido de “/” con la palabra nagios. Ejemplo: 10.0.201.57/nagios. (Nagios Enterprise [APA], 2011, pp.1-3)

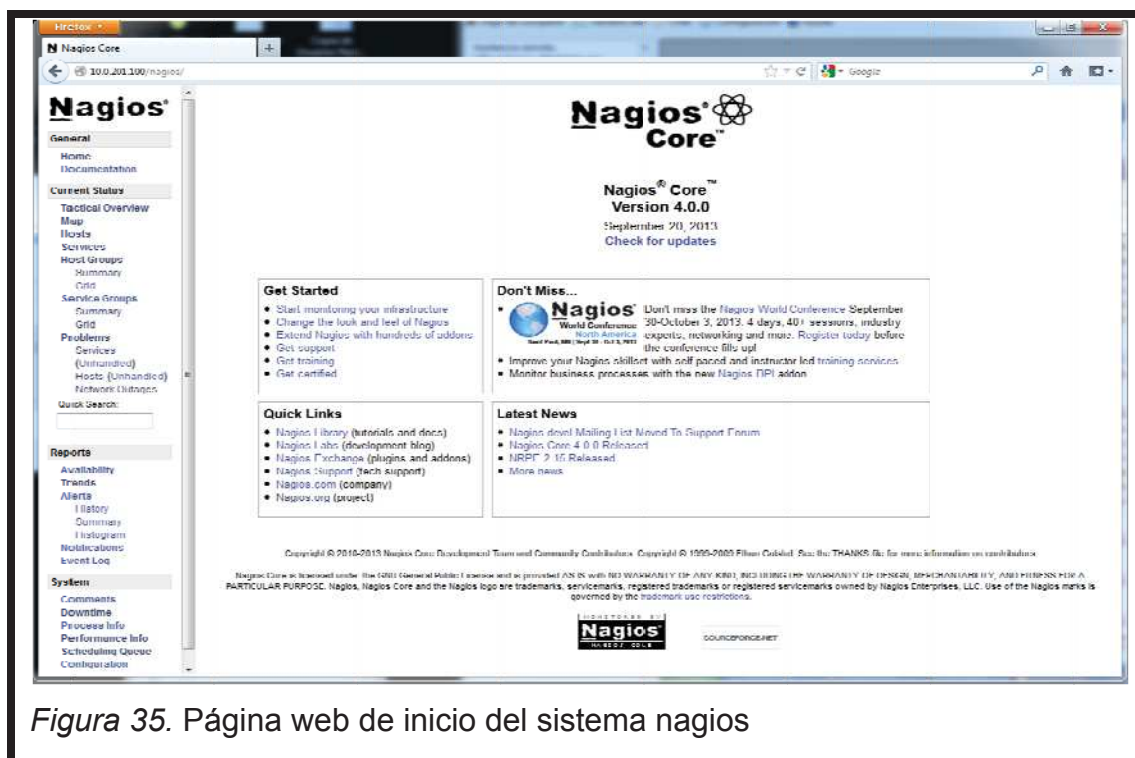


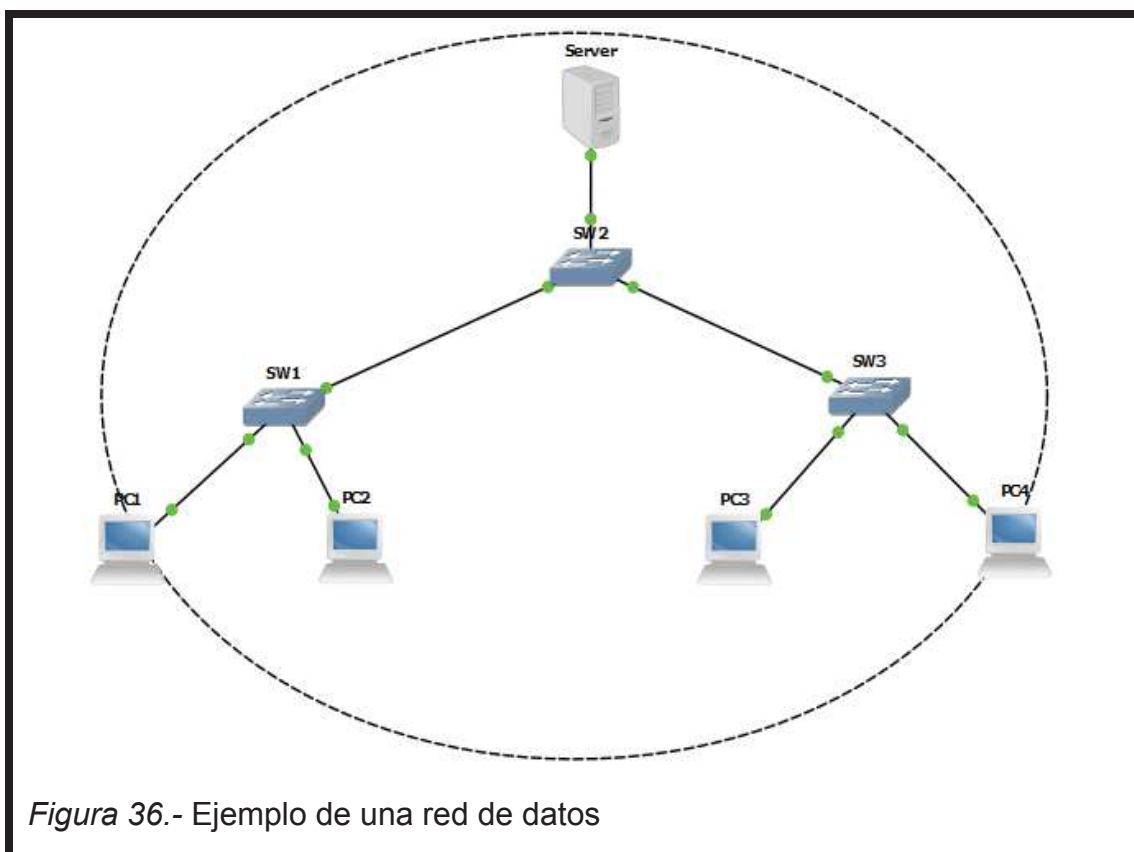
Figura 35. Página web de inicio del sistema nagios

2.8 Concepto de Red

La palabra red proviene del latín (*rete*), que significa la unión o la interconexión de computadoras y dispositivos que comparten recursos entre sí.

Así como también la palabra datos que en latín es (*datum*), este término hace referencia al paso de información o documentos.

Uniendo estos conceptos se tiene que una red es aquella que posibilita la transmisión de la información a través de un canal de comunicación, las cuales son diseñadas para satisfacer las necesidades y requerimientos de cada una de las personas. (Word Press, 2014)



Dependiendo el tipo de información a ser transmitida en la red, se clasifican en las siguientes:

- Red de Datos.- Se define así debido que envía exclusivamente datos, ejemplo: Servicio de mensajería corta, Voz IP y proveedores de internet.
- Red de Voz.- Conocida como red **PSTN**, que únicamente se dedica a paso de llamadas telefónicas.
- Red de Video.- Son aquellas que mediante el canal de comunicación se envía video, ejemplo: *Skype*, TVCABE, Direc TV.
- Red de Audio.- Se basa en aplicaciones diseñadas para transmitir música o audio, ejemplo: *Youtube*.
- Red Multimedia.- Es tipo de redes son las más críticas en la administración, porque combinan voz y video simultáneamente.

Dependiendo del tipo de información que se transmitiera en las distintos tipos de redes mencionadas, se deberá tomar en cuenta la seguridad de la información que viaja a través de los enlace de comunicación.

Banco Procredit tiene una amplia red de computadores distribuidas en las distintas ciudades y agencias del país, además con enlaces de comunicación concentrada en casa matriz.

2.9 Concepto de Intranet

Intranet es una palabra inglesa que en español significa “red interna”. Una red interna es aquella que está compuesta por un conjunto de componentes activos de red como por ejemplo: computadores, *software*, bases de datos, etc., generalmente tienen la misma funcionalidad como un internet, esto quiere decir que utilizan servidores con interface web y protocolos de comunicación similares al internet, con la diferencia de que los servicios ofertados en la red interna únicamente son visibles a los colaboradores o empleados de una misma empresa.











Además como definición técnica, indica que una intranet es un conglomerado de sitios web instalados dentro de una red interna de empresas pequeñas, medianas y grandes, permitiendo tener acceso a los archivos o documentos puestos en la red interna. (Bernard, 1996.)

2.9.1 Intranet Banco Procredit S.A.

La intranet del Banco Procredit S.A. está compuesta por los siguientes servidores con las siguientes características:

2.9.2 Características de servidores a monitorear

Tabla 3. Características de servidores a monitorear dentro del Banco Procredit.

	Nombre servidor	Descripción del servicio	Dirección IP	Sistema Operativo	Aplicaciones
	srvapl01	Servicio de aplicaciones	172.22.4.17	Windows Server 2003	Docuclass
	urano	Correo	172.22.2.10	Windows Server 2008	Exchange
	Jupiter	Servicio HTTP	172.22.2.5	Linux Centos 5.5	Web server Banco
	Ahorros	Servicio HTTP	172.22.2.8	Linux Centos 5.5	Web Server Banco
	srvvmsep	Antivirus Computadores	172.22.4.54	Windows server 2008 R2	Symantec Endpoint
	srvvmsepatm	Antivirus Cajeros	172.22.4.38	Windows server 2008 R2	Symantec Endpoint
	gup-gye	Servicio DNS, DHCP, Antivirus	10.0.9.10	Windows server 2003	Replica
	Inst	Instaladores	10.0.201.118	Windows XP SP3	Software
	Pruebas	nsclient++	10.0.201.97	Windows 7	
	srvvapl01	Servicio de aplicaciones	172.22.4.31	Windows server 2003	Sistema de Firmas

Nota: Los servidores mencionados en la tabla, son aquellos que el departamento de Riesgo y el coordinador infraestructura autorizaron para realizar el presente proyecto, estos servidores son parte importante de la operación bancaria.

2.9.3 Descripción de servidores

A continuación se detalla brevemente cada uno de los equipos mencionados en la tabla 3 con sus respectivas funciones y su rol que cumplen dentro de la empresa.

- Srvapl01.- Este servidor tiene instalado el sistema operativo Windows Server 2003 Enterprise, dentro de él ejecuta una aplicación llamada DocuClass.
El aplicativo tiene una interfaz de usuario donde mediante un escáner especializado para cheques recolecta la información de cada uno de ellos de distintos bancos, verifica los datos, genera un archivo y este se sube al sitio web del Banco Central.
- Urano.- Es el nombre que tiene el servidor *Exchange*, su sistema operativo es un Windows Server 2008 R2 el cual se usa para correo electrónico.
- Jupiter.- Es un servidor que tiene instalado el sistema operativo Linux Centos 5.5, dentro del tiene instalado y configurado la página web del banco, este servidor es utilizado por el personal de Desarrollo.
- Ahorros.- De igual manera este servidor tiene como sistema operativo Linux Centos 5.5, dentro de este servidor se encuentra la página web pero al contrario del servidor jupiter este es administrado por el personal de Marketing, aquí realizan pruebas de productos antes que salga a producción.
- Srvvmsep.- En este servidor se encuentra instalado la consola del antivirus *Symantec Endpoint* misma que está sincronizada con el directorio activo del banco. Dentro de esta aplicación se encuentra configurada las políticas y grupos de usuarios tanto de la matriz como de las sucursales para uso de Flash usb, cd, puetosusb, etc.
Este servidor es uno de las más importantes debido a las políticas de control de dispositivos y aplicaciones para el usuario final.

- Srvvmsepatm.- Este servidor así con el srvvmsep tiene instalado y configurado la consola *Symantec Endpoint*, la diferencia de este es que se utiliza para la instalación y configuración del antivirus dentro de los cajeros automáticos o también llamados ATM., por orden de la Superintendencia de Compañías y Bancos.
- Servidor gup-gye y gup-Latacunga.- Estos servidores tienen instalado el sistema operativo Windows server Enterprise 2003, realizan réplicas del controlador de dominio, servicio de DHCP y servicios de actualización de antivirus de las computadores de agencias.
- srvvamp101.- Este servidor tiene instalado el sistema operativo Windows Server Enterprise 2003, dentro él se almacena en una base de datos todas las firmas de cada uno de los usuarios del banco, tiene un aplicativo llamado Firmas BPE el cual consiste en la verificación de firmas de los clientes cuando realizan un retiro de dinero de una cuenta.
- Los equipos Inst y pruebas, son computadores de escritorio. El computador Inst tiene almacenado todo el software que utiliza el personal del banco, y el computador de pruebas es donde se ejecuta el aplicativo nsclient++ como ambientes de pruebas de los módulos de nagios antes de ser implementados en los servidores de producción.
(Banco Procredit S.A., 2014)

2.9.4 Enlace de Comunicaciones

Banco Procredit S.A., actualmente tienen sus enlaces de comunicación con las principales ciudades del país, estos se convierte en un punto fundamental de la operación bancaria como a su vez son sus servidores, razón por la cual se convierte parte importante del análisis.

En la siguiente gráfica se describen los enlaces de comunicación que tiene el banco y también se describe características importantes como son: nombre y dirección ip de cada uno de ellos.

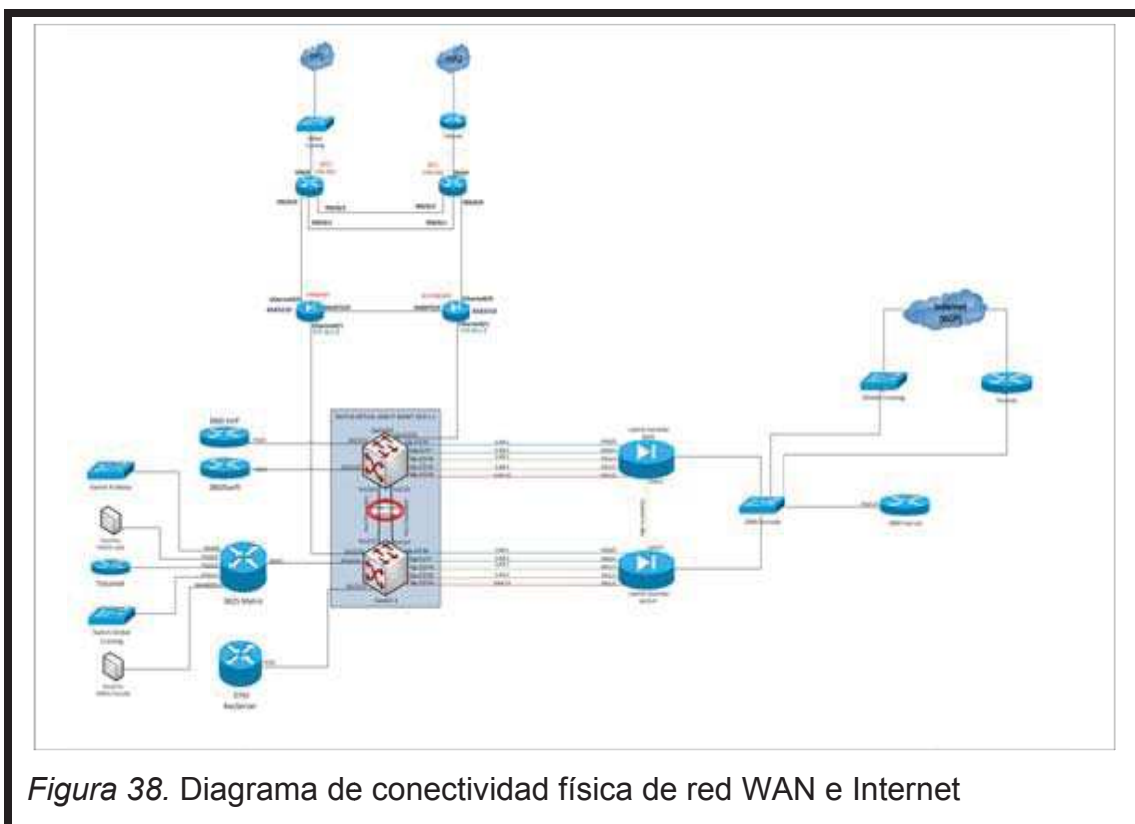
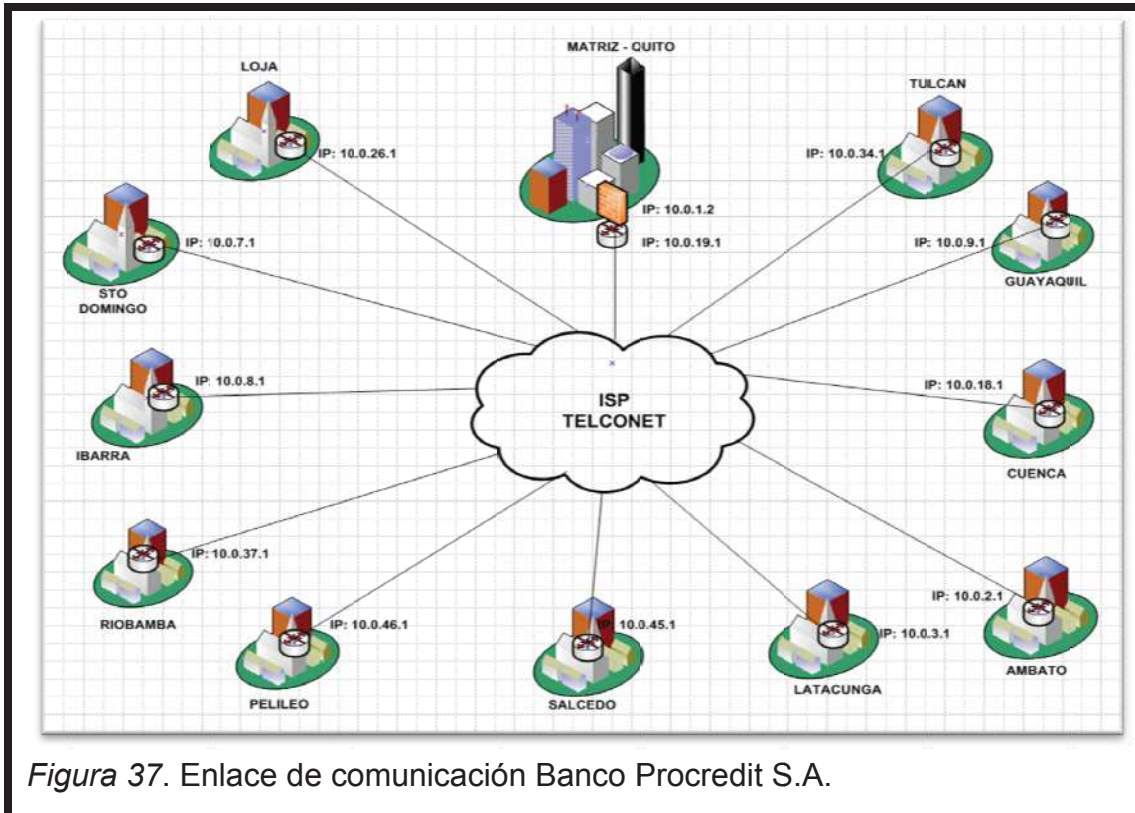


Tabla 4. Dirección ip de los enlaces de comunicación

Nombre Enlace	Dirección IP
Ambato	10.0.2.1
Latacunga	10.0.3.1
Sto Domingo	10.0.7.1
Ibarra	10.0.8.1
Guayaquil	10.0.9.1
Cuenca	10.0.18.1
Matriz	10.0.19.1
Loja	10.0.26.1
Tulcán	10.0.34.1
Riobamba	10.0.37.1
Salcedo	10.0.45.1
Pelileo	10.0.46.1

Adaptado de (Banco Procredit S.A., 2014)

2.10 Red GSM

Las siglas GSM vienen de (*Global System for Mobil communications* o Sistema Global para las comunicaciones Móviles) es un sistema estándar de segunda generación utilizada en la telefonía celular. Su estandarización se llevó a cabo entre los años 1982 y 1992 por la ETSI (*European Telecommunications Estándar* o Instituto Europeo de Estándares en Telecomunicaciones). Las principales características que presenta este estándar son: transmisión digital de voz y datos, control y configuración de SMS, portabilidad de información debido a que se hace uso de un dispositivo móvil llamado SIM, cobertura y eficiencia, todos estos beneficios a permitido que el estándar sea utilizado a nivel mundial

2.10.1 Arquitectura de la red GSM

La arquitectura de red GSM está compuesta por tres subsistemas principales los cuales se detallará y se explicará a continuación.

- **Estación Móvil (MS).** Se conoce como estación móvil o también como terminal y es utilizada por los usuarios para comunicarse con otras terminales. Su funcionamiento consiste en hacer uso de una tarjeta SIM dentro de la cual se encuentra información para identificar al usuario dentro de la red. La SIM es independiente del terminal móvil permitiendo la portabilidad y la flexibilidad al usuario.
- **Subsistema Estación Base (BSS)** La estación base es la encargada de controlar la conexión de radio entre la estación móvil y la red GSM. Dentro del sistema GSM la estación base es considerada una celda o mejor dicho es la zona de cobertura que es cubierta por la estación base.

Una BSS está constituida por dos componentes: la *BTS (Base Transceiver Station* o Estación Base Transceptora), misma que tiene contacto con las estaciones móviles mediante conexiones de radio y la *BSC(Base Station Controller* o Controladora Estación Base), la cual está en contacto con los conmutadores del NSS.

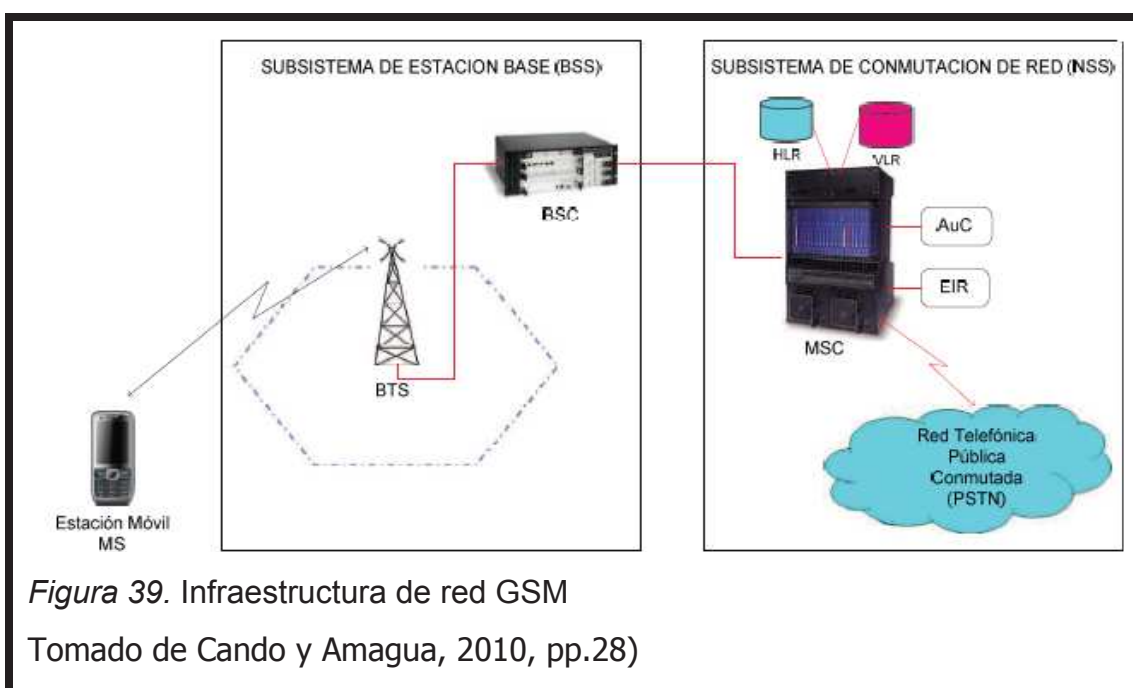
- **Subsistema de Comunicación de Red (NSS).**- Este subsistema tiene como principal función la gestión de las comunicaciones entre los usuarios de la red GSM, así como a los usuarios de otras redes. Los elementos que conforman un NSS son: MSC (*Mobile Switching Center* o Centro de Conmutación de Servicios Móviles), es el encargado de la conexión entre el usuario móvil hacia las redes fijas y móviles, también realiza el control de llamadas.

VLR (*Visitor Location Register* o Registro de Ubicación de Visitantes) es una base de datos dinámica la cual contiene información de la última ubicación del usuario.

HLR (*Home Location Register* o Registro de Ubicación Base) es una base de datos permanente donde se halla información como datos del abonado, servicios y restricciones.

AuC (*Authentication User Center* o Centro de Autenticación del Usuario) y EIR (*Equipment Identification Register* o Registro de Identificación del Equipo) son elementos encargados de proporcionar seguridad al sistema. (Cando y Amagua, 2010, pp.28-40)

INFRAESTRUCTURA GSM



2.10.2 Modem GSM

La necesidad de conectar dos computadores haciendo uso de la red telefónica hizo que por las décadas de los 60 y 70 surgieran dispositivos que permitieran la transmisión de datos digitales a través de este medio. A estos dispositivos se los conoce con el nombre de Módems.

La palabra Modem viene de modulador-demodulador el cual es un dispositivo que sirve para modular y de modular en amplitud, frecuencia o fase una señal llamada portadora mediante una señal de entrada llamada moduladora.

El principal objetivo del módem es transformar una señal analógica a una señal digital y viceversa. En el mercado hoy en día se tiene variedades de marcas y tipos de módems de diferentes fabricantes. Brevemente se mencionara los diferentes tipos de módems que se encuentran en el mercado actual.

Módems Externos.- Son dispositivos externos que suelen ser usados individualmente con el computador. El tipo de modem es similar a una caja en el cual se puede conectar una línea telefónica por un lado y por otro al computador. Existen diferentes formas de conectar un modem al computador una puede ser a través de un puerto serial y otro por puerto usb. Estos tipos de módems suelen ser los más usados por las siguientes características:

- Se conecta al computador por medio de un puerto serial
- Dispone de luces de colores los mismos que indican el buen funcionamiento del modem o falla de conexión del mismo.
- Flexibilidad y portabilidad del dispositivo para ser apagado o reiniciado sin hacer uso del computador y además instalarlo en lugares adecuados para su óptimo funcionamiento.

Una de las desventajas que presentan estos tipos de módems es que requieren de una fuente de energía para su funcionamiento así como también es mandatorio tener un puerto serial disponible para la conexión del modem.

Módems Internos.-Estos tipos de módems se construyen o vienen incorporados en la placa madre del computador, su conexión se lo realiza mediante el uso de ranuras de expansión o mejor conocidas como PCI.

Las ventajas que se puede obtener de estos tipos de módems son las siguientes:

- No requiere de una fuente de poder, por motivo que la energía es proporcionada por el computador

- Es independiente que de si el computador tenga o no tenga un puerto serial para su conexión.
- No ocupa espacio físico.

Las desventajas de estos tipos de módems son:

- Disponibilidad de ranuras en la placa madre del computador
- Al encontrarse en la parte trasera del computador esto impide la visualización correcta de los colores del *led* para verificar su conexión
- En la actualidad no son muy utilizados.

Winmodem.-Es una tercera categoría que actualmente se tiene, a diferencia de los dos anteriores módems resulta ventajoso y económico a la vez. Un *winmodems* un *software* que emula a un modem físico, el encargado de hacer funcionar el modem es el procesador del computador, la desventaja de este tipo modem es que el computador debe poseer características altas debido a que el procesador deberá realizar el procesamiento para emular un modem.

Modem externo con puerto USB.-Estos tipos de módems son los más recientes que han aparecido en el mercado, la ventaja de utilizar este modem es sin duda alguna la conexión a través de un puerto USB resultando más fácil, rápida y eficaz al momento de la transmisión de datos como también no es necesario en fijar la velocidad con el cual se conectara al computador así también no hace uso de una fuente de energía externa.

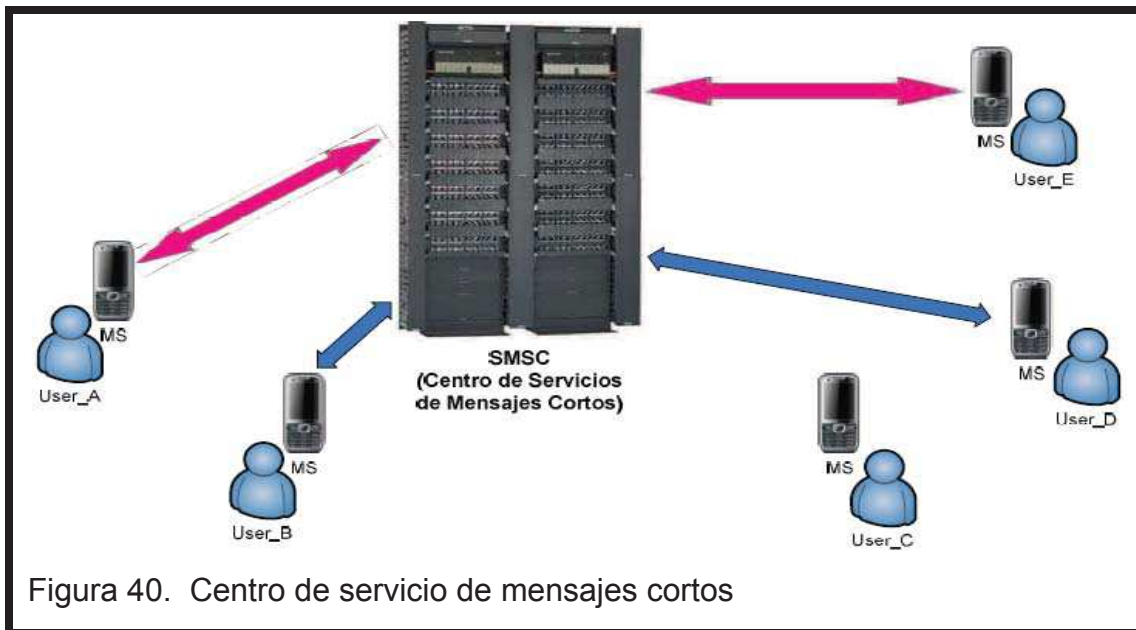
Módem Inalámbrico.-Estos módems son muy particulares a diferencia de los anteriores, se utiliza cuando se realiza transferencia de datos usando tecnología celular inalámbrica es decir dispositivos que son diseñados para trabajar en ambientes móviles, estos módems pueden ser conectados a través de un puerto serial o un puerto USB. En el mercado existen diferentes tipos de estos módems inalámbricos diseñados específicamente para acceder a una determinada red inalámbrica como por ejemplo: Módems GSM, GPRS o EDGE, la desventaja de estos módems es su costo.

Luego de haber visto los distintos módems con cada de sus distintas características, se ha tomado la decisión de hacer uso de un modem externo debido a que estos tipos de modem poseen las características necesarias para el desarrollo de este trabajo como por ejemplo: conexión con puerto serial, manejo de comandos AT, frecuencia de operación con las distintas operadoras telefónicas y como punto específico la unificación y el buen desempeño con el software de administración del sistema de mensajería corta. (Cando y Amagua, 2010, pp.28-40)

2.10.3 Servicio de Mensajería Corta (SMS)

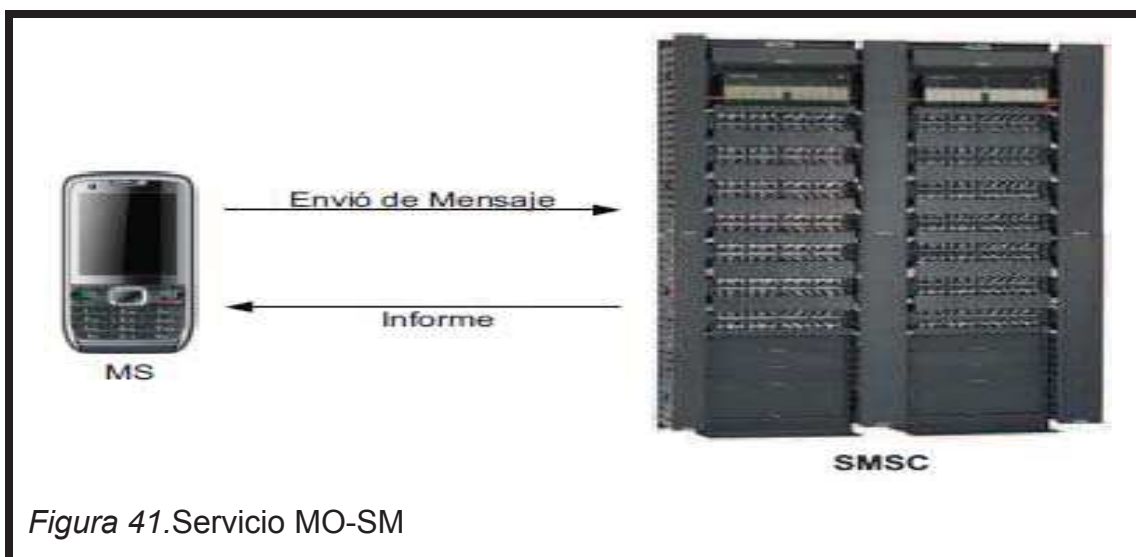
Las siglas SMS vienen de las palabras en inglés (*Short Message Service*) que traducido al español es Servicio de Mensajes Cortos. Es uno de los más populares servicios ofrecidos por el estándar GSM, este servicio permite a un abonado de una operadora telefónica realizar el intercambio de mensajes cortos. El tamaño a ser enviado en cada uno de los mensajes cortos es de 160 caracteres, los mensajes pueden ser recibidos en el transcurso de una llamada telefónica o en una sesión de datos.

Dentro de la infraestructura de la red GSM, la *SMSC (Short Message Service Center)* o Centro de Servicios de Mensajes Cortos, es el encargado de administrar los mensajes permitiendo su almacenamiento y envío de SMS al destinatario. El destino puede ser una entidad inalámbrica o un equipo dentro de la red fija. El estándar GSM únicamente contiene el caso de envío de SMS entre dos estaciones móviles.

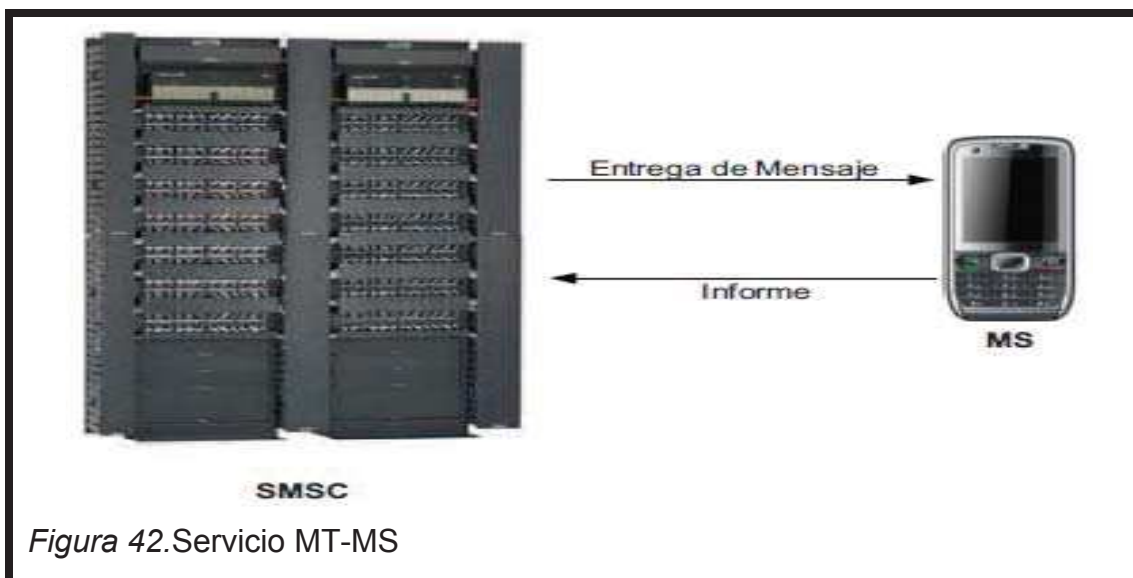


Los servicios SMS están compuestos por dos servicios principales al momento realizar un envío de un mensajes de texto desde una estación móvil a otra, estos servicios se detallaran a continuación en el siguiente gráfico.

Servicio MO-SM



Servicio MT-SM



MT-SM (Mobile Terminated – Short Message).-También conocido como Mensaje corto finalizada en el móvil, es un servicio de entrega de un mensaje desde la SMSC hacia un dispositivo móvil generando un informe sobre lo sucedido.

MO-SM (Mobile Originated – Short Message).-Conocido también como mensaje corto originado en el móvil, este realiza él envío de un mensaje desde la estación móvil hacia la SMSC, obteniendo un informe de lo ocurrido.

En la actualidad los SMS han sido muy utilizados por muchas personas independientemente de la clase social o status económico, las personas lo emplean como una manera sencilla de comunicarse, así como también empresas medianas y grandes han visto la necesidad de optar por este servicio para envío de publicidad, información, deportes, transacción de cuentas bancarias, etc. (Cando y Amagua, 2010, pp.28-40)

2.10.4 Comandos AT utilizados para envío/recepción de SMS

Existen diferentes formas y un gran conjunto de instrucciones que se pueden utilizar para que un usuario pueda comunicarse con un modem, la gran

mayoría de estos comandos son reconocidos por casi todos los módems existentes en el mercado, a continuación se listarán los más importantes y en especial se resumirá brevemente los comandos empleados para la transmisión y recepción de SMS. (Punto Flotante, 2010, pp.1-15)

- **Comandos Generales.-** Por medio de estos comandos generales nos permitirá obtener información específica del modem como por ejemplo: nombre del fabricante, número de serie del modem, estado del equipo, etc. A continuación se presenta la sintaxis de alguno de ellos.
 - **AT+CGMI.-** Con este comando se obtendrá información del fabricante
 - **AT+CGMM.-** Comando para obtener información acerca del modelo del modem
 - **AT+CGSN.-** Comando para obtener el número de IMEI (Entidad Internacional de equipo móvil)

Comandos para servicio de red.- Proporciona información acerca de la calidad de señal, selección de operadora telefónica, etc.

- **AT+CPAS.-** Muestra información acerca de la actividad del teléfono móvil
- **AT+CSQ.-** Indica la calidad de señal
- **AT+COPS.-** Permite seleccionar la operadora telefónica
- **AT+WOPN.-** Muestra nombre de la operadora.

Comandos de seguridad.- Permite realizar la configuración de los parámetros de seguridad del modem como por ejemplo: cambio de contraseña, ingreso de PIN, etc.

- **AT+CPIN.-** Ingreso de código PIN (Número de Identificación Personal) para autenticación y acceso al dispositivo móvil.

- **AT+CPINC.-** Muestra el número de intentos que quedan al ingresar erróneamente el PIN

Comandos SMS.-Estos comandos se emplean en el manejo de mensajes de texto, dentro de este conjunto de comandos podemos:

Definir el formato de los SMS.- Los SMS pueden ser transmitidos en modo texto en modo PDU, su diferencia entre estos dos modos es que al cambiarlo en modo PDU el mensaje es fácilmente transmitido por el dispositivo ya que no tiene que ser codificado/decodificado a diferencia del modo texto.

Cuando la transmisión de los comandos no es por la red sino más bien es a través de la utilización del puerto serial lo más sencillo es utilizar el modo texto. El comando que permite realizar la especificación del modo que transmitirá es el siguiente:

- **AT+CMGF=<mode>.-** Este comando es el que indica el modo que serán transmitido los mensajes, para la transmisión en modo PDU el valor que se le da al comando es 0, mientras que para el modo texto el valor del comando será 1.

- **AT+CMGF = 0** envío de mensajes en modo PDU
- **AT+ CMGF = 1** envío de mensajes en modo Texto

El comando que permite conocer el modo en que se realiza el envío de un SMS es:

- **AT+CMGF?** Retorna el valor tomado por <mode>

Envío de SMS.- El comando para realizar el envío de un SMS al centro de servicios de mensajes cortos que es donde primeramente será almacenado nuestro SMS para posteriormente ser enviado al destinatario es AT+CSCA, a continuación se muestra la sintaxis del uso del comando.

- **AT+CSCA?.-** Mediante esta opción lo que se obtiene es el número de centro de servicio de mensajería (SMSC), el resultado es el siguiente:
+CSCA:<número>,<tipo>

Dónde:

<número> representa el número de servicio

<tipo> presidido del signo (+) representa el código para acceso internacional

Si se quiere ingresar de forma manual el número del centro de servicio y el código de acceso se emplea la siguiente instrucción.

AT+CSCA = <número>, <tipo>

Enviar un mensaje.-Para el envío de mensaje el comando que permite al usuario realizar el envío es: **AT+CMGS**, a continuación se indicaran los pasos que se deberá realizar para el envío.

-AT+CMGS="<número del destinatario>"

>Este es un mensaje <CTRL+Z>

Para realizar el envío de un SMS en primer lugar se requerirá el número del destinatario, este número a su vez será ingresado entre comillas.

Ingresado el número se deberá presionar la tecla *ENTER* y esperar hasta que aparezca el carácter (>), Luego se escribirá el texto deseado y finalmente para el envío del mensaje de presionaran las teclas CTRL+Z

Si el mensaje fue enviado de forma correcta el comando devolverá como respuesta +CMGS:<mr>, donde: <mr> es un índice de referencia al mensaje enviado.

Leer un mensaje.-Para la lectura de mensajes se utiliza el comando **AT+CMGL**, así como se demuestra a continuación.

- **AT+CMGL="<mode>"** donde el parámetro <mode> puede ser uno de los que se menciona a continuación.

- **REC READ.**- Muestra mensajes recibidos que se han leído
- **REC UNREAD.**- Muestra mensajes recibidos que aún no se han leído
- **STO UNSENT.**- Muestra mensajes guardados que aún no se han enviado
- **STO SET.**- Muestra mensajes guardados que ya han sido enviados.
- **ALL.**- Muestra todos los mensajes almacenados.

Borrar mensaje.-Con el uso del comando *AT+CMGD* se puede borrar un mensaje almacenado en la memoria, la sintaxis de eliminar un mensaje se muestra de la siguiente forma:

- **AT+CMGD=<índice>** donde el índice es la posición del mensaje almacenado en la memoria

En algunos de los comandos mencionados anteriormente se ha hecho uso de caracteres especiales como: ?, = y =?. A continuación se explicara brevemente el significado que tiene cada uno de ellos.

- **Interrogación (?).**- Indica solicitud de información
- **Igual (=).**- Significa paso de uno o más parámetros que son definidos por el usuario.
- **Igual interrogación (=?).**- Permite al usuario visualizar un rango de valores devueltos por un comando AT. (Punto Flotante, 2010, pp.1-15)

2.11 Soluciones de monitoreo mediante el uso de SMS y Correo Electrónico

Existen distintos métodos para realizar envío de mensajes de texto corto comúnmente conocidos como SMS hacia teléfonos celulares o dispositivos móviles, a continuación se explicara brevemente los diferentes métodos que se

puede utilizar con sus respectivas características principales que de tal forma poder determinar el método más adecuado que se ajuste al proyecto.

2.11.1 Envío de SMS mediante Internet

Como primer método se tiene el envío de mensajes SMS mediante el uso de internet. El proceso de este servicio se lo realiza mediante una previa suscripción en cualquier página web que oferta este tipo de solución a un costo determinado. La desventaja es que la gran mayoría de estas páginas no permiten el envío a diferentes países que no se encuentran registrados en su nómina, además es el tiempo que podría tardar de llegar un mensaje al destinatario dependiendo de la saturación de la red.

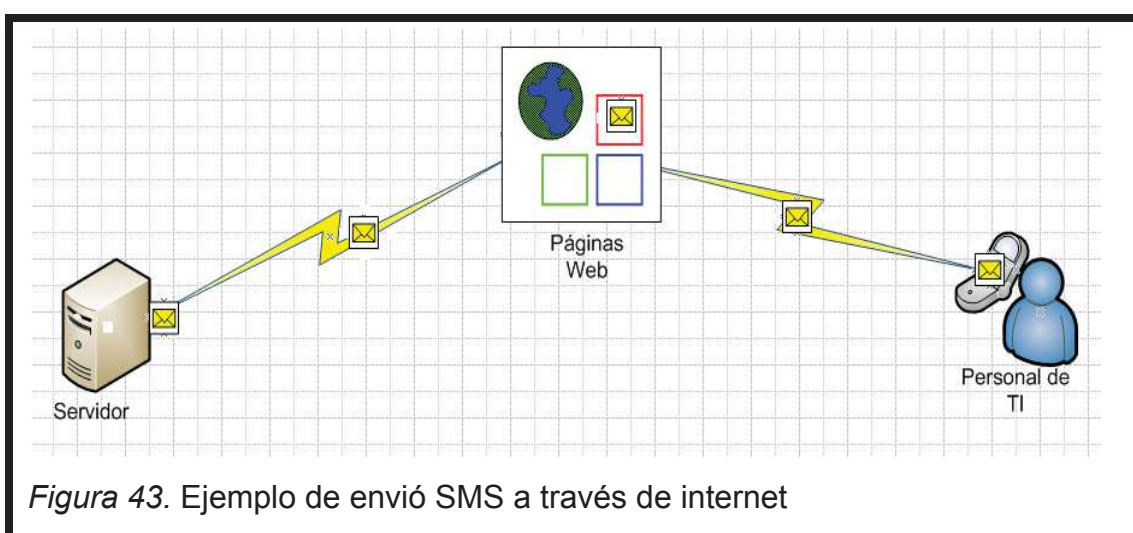


Figura 43. Ejemplo de envío SMS a través de internet

Esta solución no es muy garantizada debido que si en algún momento se tiene problemas con el proveedor de internet o si existen fallas en los equipos de comunicación los mensajes de alertas no llegarían al personal de TI, la única ventaja es que el costo de envío de mensajes que son más baratos al compararlos con envío entre celulares.

2.11.2 Envío de SMS mediante uso de celular conectado al servidor

Una segunda opción de envío de mensajes es mediante la conexión de un celular al servidor usando como medio de transmisión un cable de datos, señales infrarrojas o mediante *Bluetooth*.

El celular se usaría como un modem o pasarela con la finalidad de procesar la información que sea enviada por el servidor y está a sus veces realice un reenvío hacia los celulares del personal de TI.

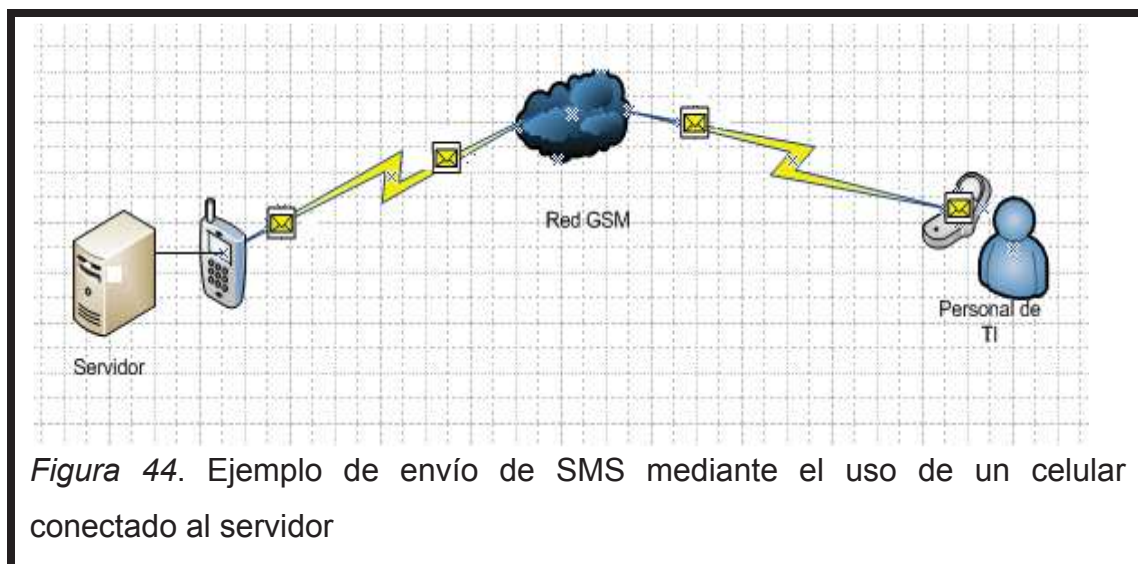


Figura 44. Ejemplo de envío de SMS mediante el uso de un celular conectado al servidor

La comunicación entre el servidor y el dispositivo móvil se realiza utilizando comandos AT, estos comandos se envía desde el servidor utilizando una aplicación la cual permite tener control sobre el dispositivo.

La desventaja de este método es el tipo de aplicación que se utilice para el control del equipo móvil, debido a que algunas marcas y modelos de teléfonos celulares no soportan los comandos AT, así mismo se debe tener los complementos necesarios para la conexión con el servidor.

2.11.3 Envío de SMS mediante uso de un modem GSM

Esta tercera solución a diferencia de las otras dos utiliza un modem GSM externo, una de sus principales funciones y características es la posibilidad que tienen para usar la red GSM y mediante el uso de la red poder transmitir voz, datos y en especial el envío de mensajes SMS.

Como parte de la solución planteada para el presente proyecto se hará uso de un modem por los siguientes motivos.

- Cuenta un set amplio de comandos AT
- Poseen un puerto RS232 para la comunicación en el servidor
- Poseen un completo manual para su utilización
- Mejor funcionalidad y un buen desempeño
- Hace uso de una tarjeta SIM

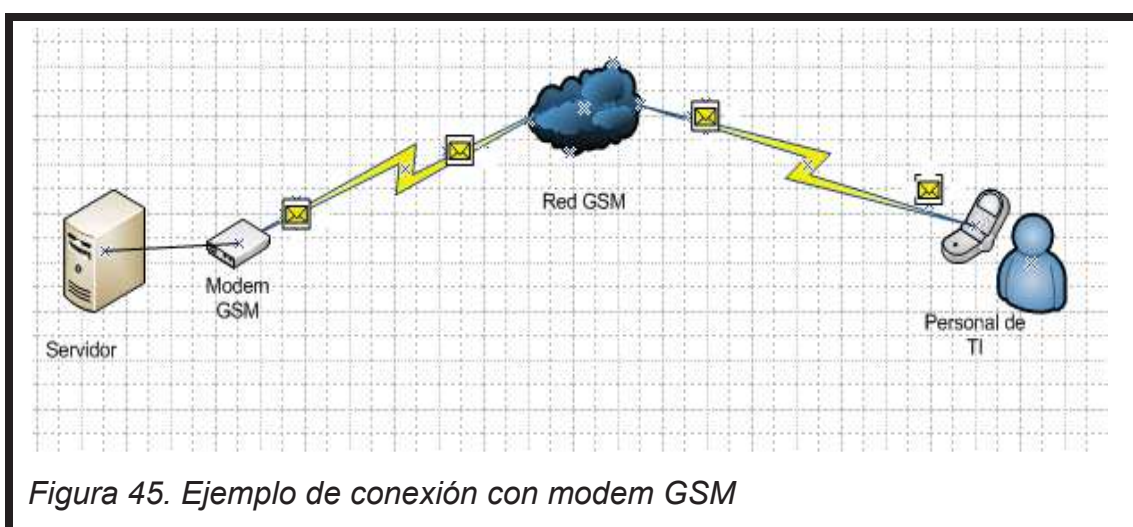


Figura 45. Ejemplo de conexión con modem GSM

2.11.4 Solución para el envío mediante correo electrónico

Además de las soluciones planteadas anteriormente, es de vital importancia contar con el servicio de correo electrónico para informar a los administradores de red acerca del monitoreo de los equipos y servicios dentro de la empresa. El

sistema de monitoreo aparte que cuenta con el envío de SMS tiene la posibilidad de enviar información a una o varias cuentas de correo corporativo. Se cuenta con dos opciones para que se pueda habilitar este tipo de servicio, a continuación se nombra y se detalla brevemente los más utilizados:

- Instalación y configuración de un servidor de correo
- Usando a un servidor de correo intermediario

En la primera opción se puede realizar un servidor de correo, convirtiéndose en agente de transporte de correo (*Mail Transfer Agent MTA*). Los MTA pueden ser usados tanto el sistema Windows como en Linux.

Dentro del sistema Linux se tiene a los siguientes MTA los cuales posibilitaran la habilitación del servicio de correo electrónico.

Sendmail.- Este tipo de servicio es considerado como un MTA, es el más antiguo y utilizado a la vez en los sistemas Unix, las características más relevantes de *sendmail* es:

- Tiene una amplia gama de información para su instalación y configuración
- Su licencia es de código libre
- Utiliza el puerto 25 para la comunicación con clientes
- Permite asignar nombres a cada dirección de correo
- Tiene la funcionalidad de almacenamiento y encolamiento de correos que no pudieron recibir el o los destinatarios finales.

Postfix.- Es un MTA al igual que *sendmail*, viene incorporado en algunas distribuciones de Linux, la diferencia entre *postfix* y *sendmail* es la fácil instalación y configuración que se realiza, entre sus principales características se tiene:

- Muy fácil de administrar
- Gran cantidad información
- Utiliza cifrado para autenticación

- Manejo de listas negras
- Su licencia es de código libre

El segundo método es mediante un servidor intermediario sea este *Gmail*, *Hotmail*, u otros, para realizar esta solución antes que nada se deberá tener una cuenta de correo registrada en uno de estos servidores y después se realiza el proceso de instalación de cualquier MTA mencionado en la parte superior con su respectiva configuración de archivos, como requisito fundamental es necesario que el servidor cuente con acceso a internet.

La solución optada para el envío de correo electrónico es la utilización de un servidor intermediario como en este caso *Gmail* porque posee gran cantidad de información acerca de los parámetros de configuración, además se ocupa servidores externos conocidos con disponibilidad alta asegurando así el envío de las alertas a cualquier parte del mundo al personal de TI, como también se trata de causar el menor impacto en el uso de los recursos de la empresa por temas de seguridad.

Se creará una cuenta genérica y este a su vez se unirá con el MTA *postfix*, el servidor de *gmail* tendrá la funcionalidad de un *relay* y este se encarga del reenvío de correo hacia las cuentas corporativas de los usuarios de TI.

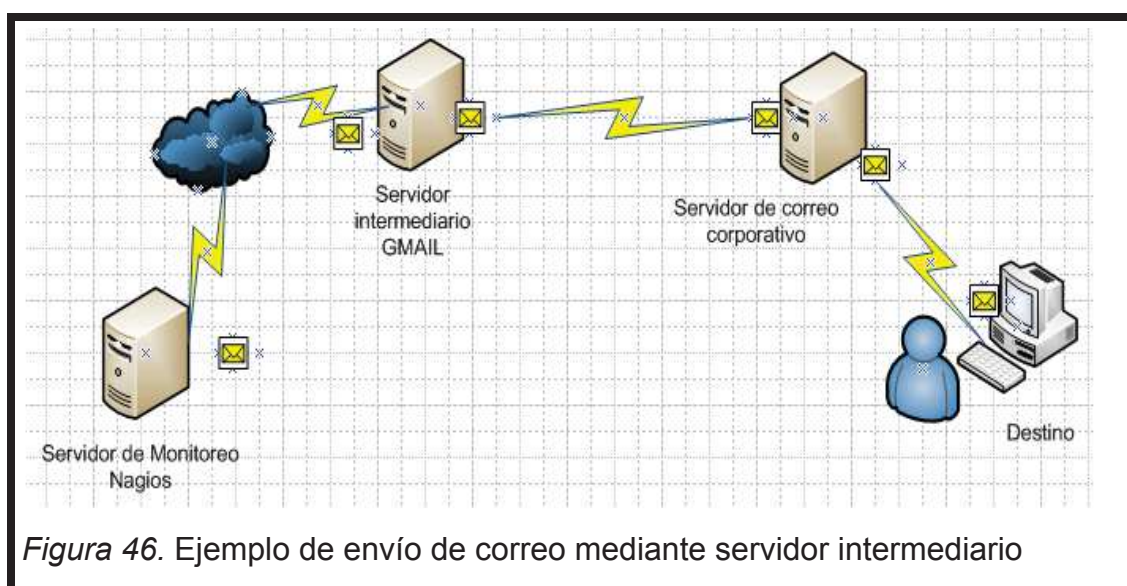


Figura 46. Ejemplo de envío de correo mediante servidor intermediario

Con esta solución se busca causar el menor impacto posible con el tema de seguridad dentro de la institución financiera.

2.12 Problemática Banco Procredit S.A

La situación actual del Banco Procredit S.A. continuamente presenta fallos en los enlaces de comunicación por procesos de criptografía o por fallos eléctricos y por cuestiones de los proveedores de los enlaces de comunicaciones.

Para el monitoreo de los enlaces de comunicación el personal de TI tiene una herramienta de monitorización pero no es lo suficientemente efectivo debido a que el personal debe estar revisando periódicamente de forma gráfica los diferentes estados que pueden presentar los enlaces, ocasionando la poca oportunidad de reacción ante problemas suscitados antes que los usuarios finales se den cuenta de la falla.

Una segunda problemática son los servidores de gama media que se encuentran en producción, estos no poseen una herramienta de monitorización de fallos en los diferentes componentes de *Hardware* como son: espacios en disco duro, memoria RAM, carga del procesador, etc.

Debido a toda esta problemática el sistema nagios tiene la posibilidad de realizar una monitorización de todos los componentes de red que se especifiquen en cada uno de los módulos, basados en las distintas configuraciones que este ejecuta dentro de él cubriendo las necesidades que requiere el personal de TI, de esta manera nagios se convierte en una potente herramienta de monitorización añadiendo al sistema la opción de envío de mensajes de alertas mediante el uso de correo electrónico y SMS.

3. Pasos, Diseño e Implementación de la Plataforma Nagios.

3.1 Pasos para la instalación del sistema Nagios, Correo Electrónico y SMS

En el primer paso se explica y grafica el diseño de las conexiones de los enlaces de comunicación de las distintas agencias que conforman Banco Procredit a nivel nacional, después de tener el diseño se continuará con la personalización y configuración de los diferentes módulos y *scripts* del sistema nagios. En este caso la cantidad de equipos a monitorear serán todos los componentes principales (Servidores, Switch y Router) de cada agencia que el banco tiene, dando como un total de 56 equipos monitoreados en tiempo real, cabe mencionar que el sistema como tal tiene la capacidad de monitorear hasta 1000 equipos. (Nagios Enterprise, 2014), por consiguiente el porcentaje que actualmente se encuentra utilizando es el 5,6% de capacidad total, esto significa que si la red empresarial crece el sistema soportara el incremento de equipos sin problema alguno.

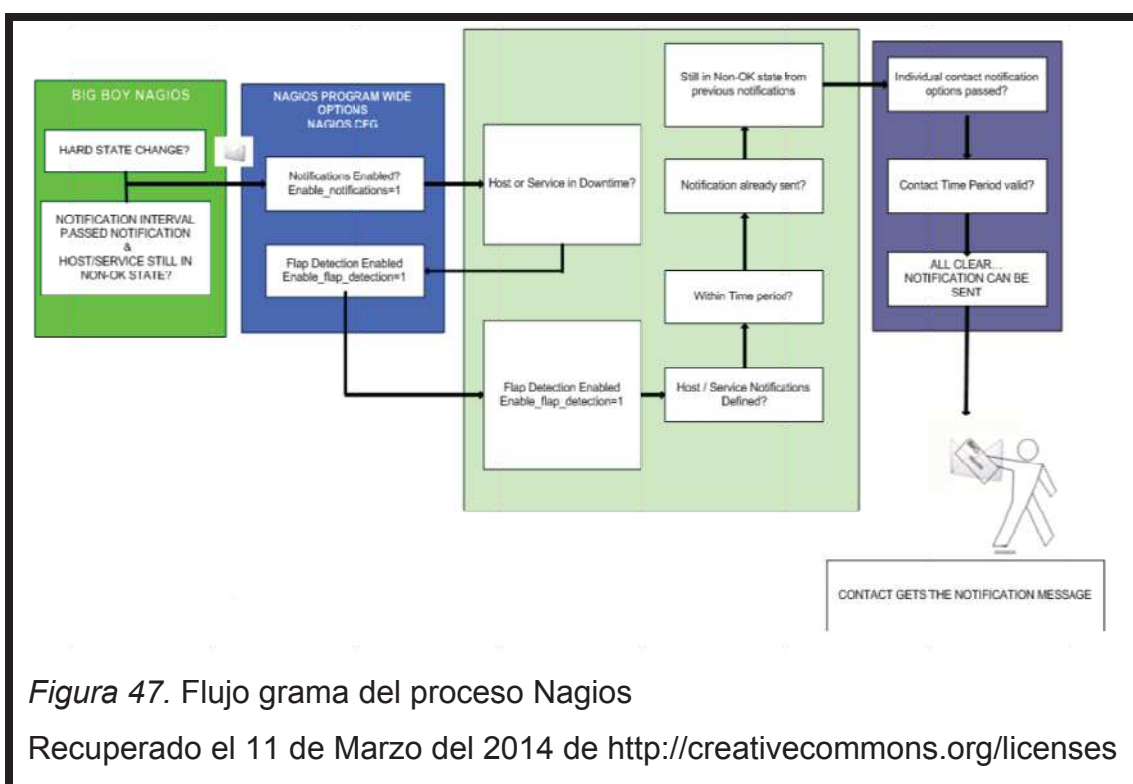


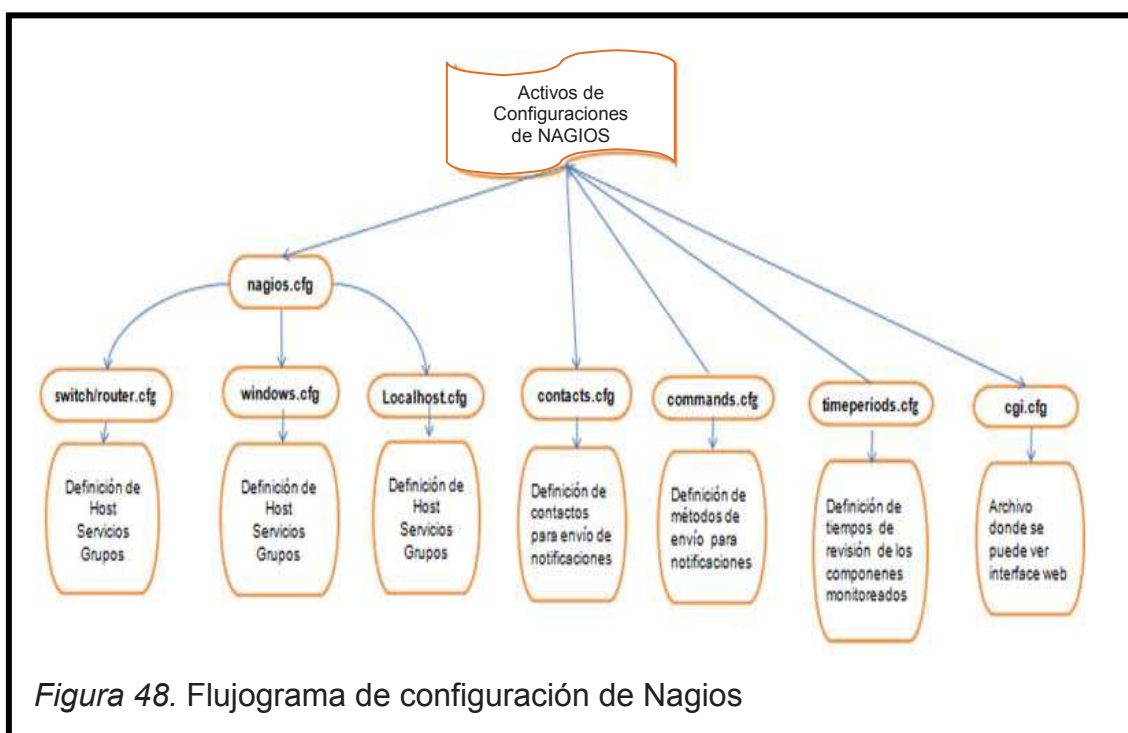
Figura 47. Flujo grama del proceso Nagios

Recuperado el 11 de Marzo del 2014 de <http://creativecommons.org/licenses>

En un segundo paso se instalará y se configurará los archivos correspondientes al agente de transporte de correo *Postfix*, posteriormente se procederá a integrar la cuenta de correo del sistema nagios con las cuentas de correo corporativo.

Y finalmente como tercer paso se realizará la instalación de las librerías del programa que integrará el sistema nagios con él envío de mensajes cortos Ozeki SMS Gateway, posterior a la instalación se conectará el modem GSM y se configurará los archivos específicos para dar paso final a realizar pruebas de funcionalidad del sistema.

3.1.1 Descripción de comandos nagios



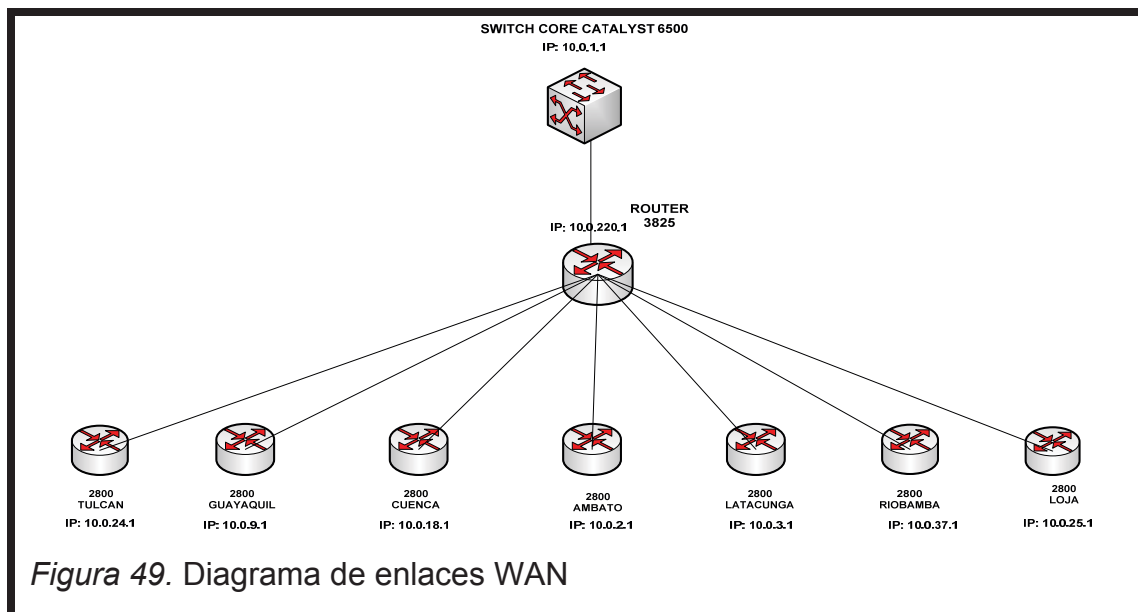
Para la personalización y configuración del sistema de monitoreo nagios es necesario ejecutar y modificar los siguientes archivos que a continuación se explicará brevemente:

- ***nagios.cfg***.- En este archivo de configuración se procederá a habilitar los distintos módulos que contiene a los componentes de red.
- ***cgi.cfg***.- En este archivo se obtendrá información de la interfaz web del sistema, aquí se podrá definir el tiempo que tomara la actualización de la interfaz.
- ***timeperiods.cfg***.- En este archivo se podrá definir el modo y el tiempo que el sistema vigilara a los componentes de red.
- ***commands.cfg***.- En este archivo se definirá el método de envío de las notificación del sistema, por correo o también por SMS
- ***contacts.cfg***.- En este archivo se procederá a definir al o las personas que recibirán las notificaciones por medio de correo electrónico y SMS.
- ***localhost.cfg***.- El script *localhost* es únicamente reservado para el servidor que contiene el sistema, también se utiliza como archivo para agregar equipos con similar sistema operativo.
- ***windows.cfg***.- En este archivo se agregaran equipos que tengan únicamente sistema operativo Windows, sean estos servidores o computadores de escritorio.
- ***switch/router.cfg***.- En este archivo se ingresa información acerca de los equipos de comunicación de cada una de las agencias.

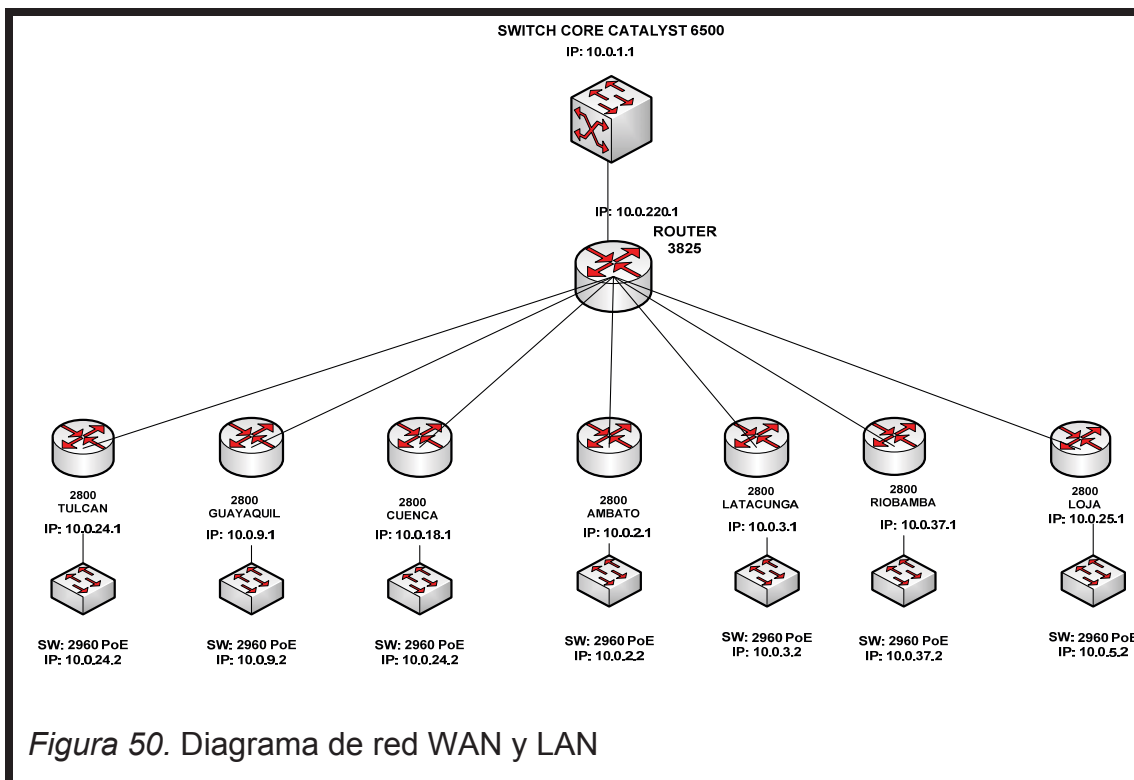
3.2 Diseño de red y conectividad para sistema Nagios

El Banco tiene un *switch* de *core* administrable de capa 3 marca cisco catalyst modelo 6500, dentro del cual se tiene configurado el protocolo de enrutamiento dinámico EIGRP, VLANS troncalizadas, seguridades de acceso, control de intrusos, etc. A este equipo se conecta otro *router* cisco catalyst modelo 3825 capa 3 administrable al igual que el anterior equipo dentro de su configuración se halla el protocolo dinámico, *vlangs*, seguridades, etc. El modelo de *router* utilizado en todas las agencias es el 2800 este a su vez se interconectan con

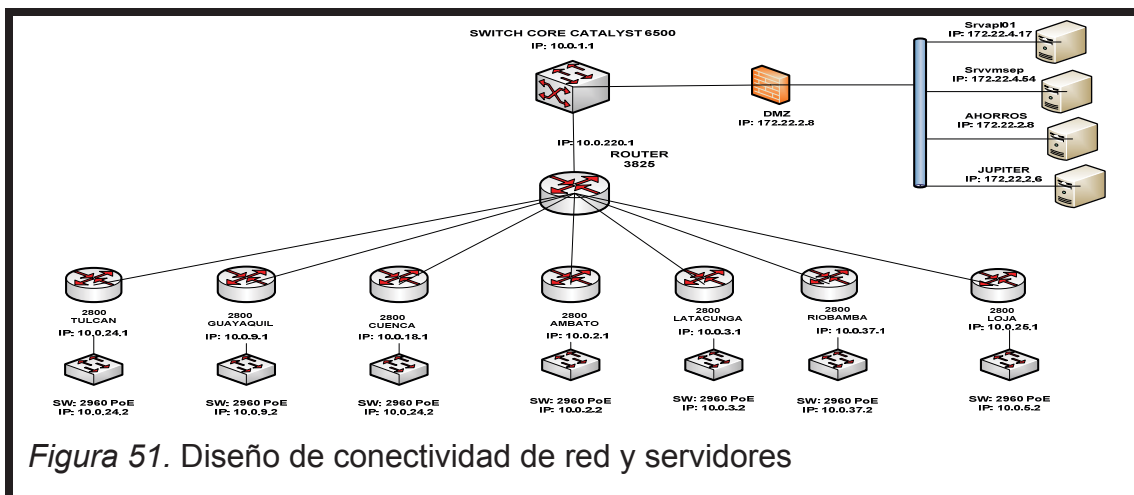
router de borde 3825, como se puede ver el siguiente grafico la red se encuentra dispuesta de la siguiente manera.



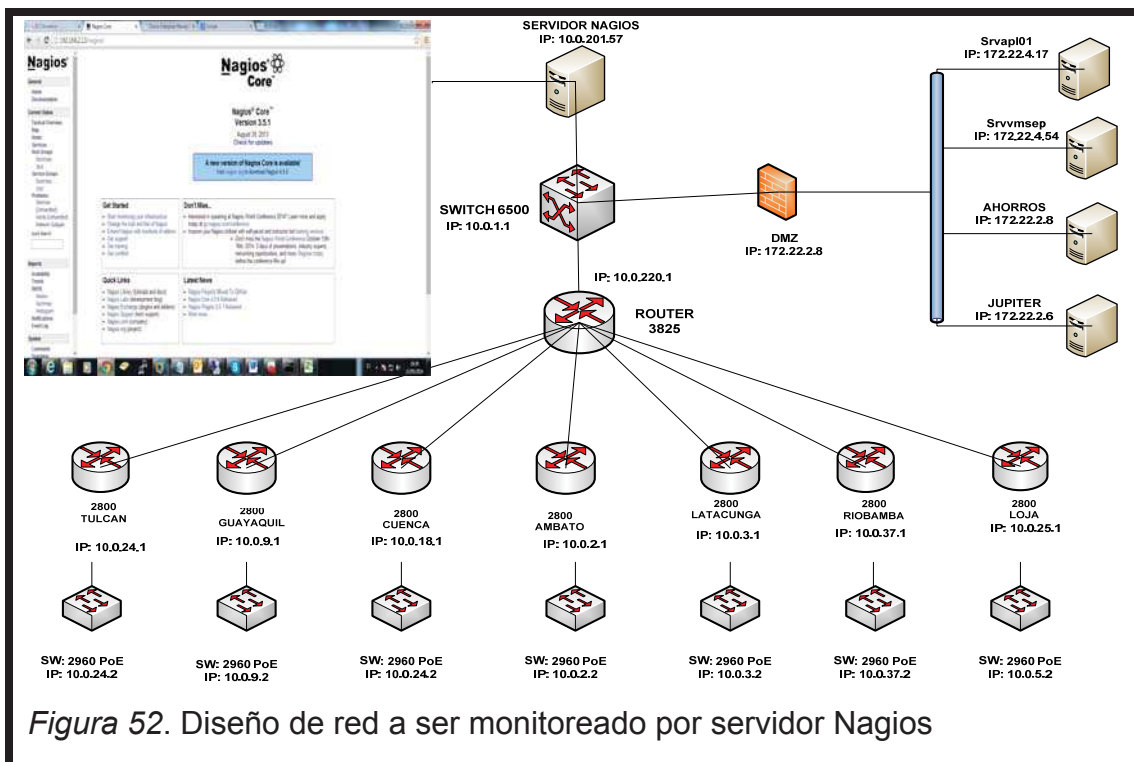
En la parte de red LAN, se utiliza equipos de marca cisco y el modelo de *switch* implementado es el 2960 *PoE* de 48 puertos, se encuentra configurado en el equipo tres *VLAN* que corresponde a: Datos, Voz, y la red de los cajeros automáticos además por seguridad se tiene en cada interfaz del *switch* habilitado el puerto seguro.



Por último se presenta el esquema servidores de aplicaciones, estos se conectarán a un *DMZ* y este a su vez establece comunicación con el *switch core 6500*.



Como parte final se incluye el servidor de monitoreo, mismo que realizara el chequeo de todos los componentes detallados en cada uno de los gráficos mencionados anteriormente. Este será el esquema que se maneja para la aplicación web de nagios y en su configuración.



El servidor de monitoreo se ubica en la parte superior del switch capa 3 debido a la jerarquización implementada por el banco, porque es el elemento principal y el más crítico debido a que ahí residen las configuraciones de los enlaces de comunicación como los permisos y accesos al uso de la red de todas las agencias así como también no se cubriría por completo el monitoreo de toda la red sino más bien se haría una monitorización de una agencia.

3.3 Configuración de *Script* Sistema Nagios

Para la parte de configuración de nagios hay que tener un conocimiento medio alto del Linux, todo el procedimiento de configuración de los script del sistema se realizan mediante consola con el editor de texto nano, en cada uno de estos archivos se pasan parámetros de configuración de los componentes de red que serán monitoreados.

Cada archivo de configuración se aloja en el directorio `"/usr/local/nagios/etc"`.

3.3.1 Script nagios.cfg.

nagios.cfg.- En este archivo reside la parte medular o principal del sistema, donde se habilita y se especifica los archivos de configuración, se puede modificar los siguientes parámetros.

De igual manera para ingresar al archivo se debe utilizar un editor de texto más la ruta del archivo a abrir.

```
nano /usr/local/nagios/etc/nagios.cfg
```

- Especifica los archivos de log de los equipos y servicios

```
log_file=/usr/local/nagios/var/nagios.log
```

La parte principal de nagios.cfg es el archivo de configuración de objetos, es aquí donde se especifica y se habilita los componentes de red que se desean monitorear. Para la habilitación de estos archivos se debe descomentar (#).

- Definición para la monitorización local del equipo

```
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg
```

- Definición para la monitorización de computadores con sistema operativo Windows

```
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

- Definición para la monitorización de routers y switches

```
cfg_file=/usr/local/nagios/etc/objects/switch.cfg
```

En este primer archivo se realiza la habilitación de los diferentes módulos que utilizara el sistema nagios para la monitorización de los distintos componentes de red que se definirán en la configuración.

```

root@nagios-server: ~
login as: root
root@10.0.201.57's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-23-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Mon Jan 27 15:47:52 ECT 2014

System load:  0.0          Processes:    96
Usage of /home: 0.3% of 55.00GB   Users logged in:  1
Memory usage:  13%         IP address for eth0: 10.0.201.57
Swap usage:    0%

Graph this data and manage this system at https://landscape.canonical.com/

125 packages can be updated.
62 updates are security updates.

You have new mail.
Last login: Mon Jan 27 14:56:44 2014 from 10.0.201.97
root@nagios-server:~# nano /usr/local/nagios/etc/nagios.cfg

```

Figura 53. Ejemplo de acceso al archivo nagios.cfg

```

GNU nano 2.2.6 Archivo: /usr/local/nagios/etc/nagios.cfg

# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch

```

Figura 54. Módulos de activación de componentes de red.



Figura 55 Habilitación de módulo de componentes de red

3.3.2 Archivos *cgi.cfg*

cgi.cfg.- Este script define la ruta principal del archivo de configuración, dentro de él se encuentra contenido de la ubicación web, especificación de usuarios que pueden visualizar información de la aplicación, etc.

Para ver el contenido del archivo se utiliza un editor de texto más la ruta del archivo: (*nano /usr/local/nagios/etc/cgi.cfg*), dentro del cual se destaca la siguiente información.



```

root@nagios-server: ~
GNU nano 2.2.6 Archivo: /usr/local/nagios/etc/cgi.cfg
#####
#
# CGI.CFG - Sample CGI Configuration File for Nagios 3.5.1
#
# Last Modified: 06-17-2009
#
#####

# MAIN CONFIGURATION FILE
# This tells the CGIs where to find your main configuration file.
# The CGIs will read the main and host config files for any other
# data they might need.

main_config_file=/usr/local/nagios/etc/nagios.cfg

# PHYSICAL HTML PATH
# This is the path where the HTML files for Nagios reside. This
# value is used to locate the logo images needed by the statusmap
#
[ 364 líneas leídas ]
^G Ver ayuda ^C Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^O Pos actual
^X Salir ^U Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía

```

Figura 56. Ejemplo de archivo *cgi.cfg*

- Especifica la ubicación principal del archivo de configuración
main_config_file=/usr/local/nagios/etc/nagios.cfg
- En el siguiente *path* especifica los archivos HTML residentes en el sistema los cuales nos permitirá ver la interface web
physical_html_path=/usr/local/nagios/share
- En este otro *path* muestra los tipos de graficas que se pueden modificar entorno al mapa global
default_statusmap_layout=5

- Permite especificar el tiempo en segundo la actualización de la página web

```
refresh_rate=10
```

- Permite añadir un archivo de audio cuando exista un problema con la red, se utiliza como un medio de notificación mediante el sonido.

```
<varname>=<sound_file>
```

3.3.3 Script commands.cfg

Este archivo de configuración provee ejemplos de definición de comandos para él envió de las notificaciones de información generadas por la monitorización de los equipos y servicios dentro de la red.

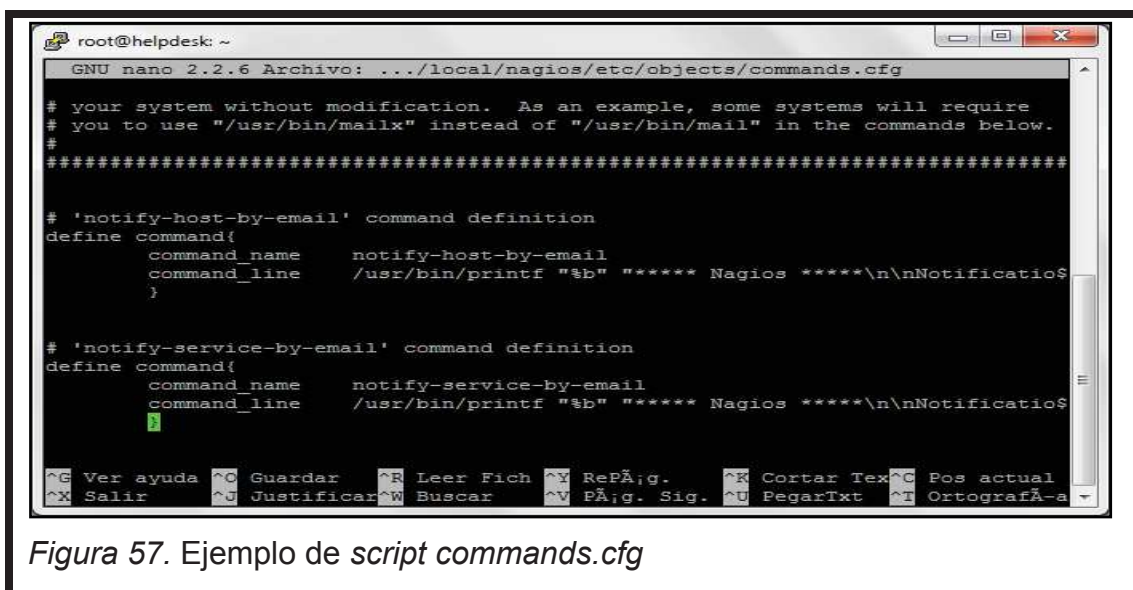


Figura 57. Ejemplo de *script commands.cfg*

3.3.4 Definición de servicios.

En cada uno de los archivos de configuración sean estos, *localhost*, equipos *windows*, *switch*, etc., se tendrá que definir los tipos de servicios que se monitorizara en cada uno de estos compones, además se podrá crear otros tipos de servicios dependiendo de las necesidad requeridas.

```

# Create a service for monitoring memory usage
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name          srvvmsep, srvvmsep@tm, srvvmp101, srvvap101, Pruebas, Ints
    service_description Memory Usage
    check_command      check_nt!MEMUSE!-w 80 -c 90
}

# Create a service for monitoring C:\ disk usage
# Change the host name to match the name of the host you defined above

define service{
    use                generic-service
    host_name          srvvmsep, srvvmsep@tm, srvvmap101, srvvap101, Pruebas, Ints
    service_description C:\ Drive Space
    check_command      check_nt!USEDISKSPACE!-1 c -w 80 -c 90
}

```

Figura 58. Ejemplo de *script* de servicios

3.3.5 Script contacts.cfg

En este archivo de configuración se incluirán al o a los usuarios que recibirán la información de las notificaciones del sistema mediante correo electrónico, en este archivo se tendrá usuarios genéricos.

A continuación se detallara brevemente los campos importantes que contiene el archivo.

Tabla 5. Campos a ser ingresados en el script contacts.cfg

<i>contact_name</i>	pmadril	—————▶	Nombre de usuario
<i>usegeneric-contact</i>		—————▶	Plantilla genérica de contacto
<i>alias</i>	Admin Procredit	—————▶	Un alias de descripción
<i>email</i>	pmadril@bancoprocredit.com.ec	—————▶	Dirección de correo



```

root@helpdesk: ~
GNU nano 2.2.6 Archivo: .../local/nagios/etc/objects/contacts.cfg Modificado
contact_name      nagiosadmin      ; Short name of$
use               generic-contact ; Inherit defau$
alias             Nagios Admin    ; Full name of $
email            nagiosprocredit@gmail.com ; <<***$
}

define contact{
contact_name      pmadril          ; Short name of user
use               generic-contact ; Inherit defau$
alias             Admin Procredit ; Full name of $
email            pmadril@bancoprocredit.com.ec ; <<***$
}

define contact{
contact_name      rsalceso        ; Short name of$
use               generic-contact ; Inherit defau$
alias             Admin Procredit ; Full name of $
email            rsalcedo@bancoprocredit.com.ec ; <<***$
}

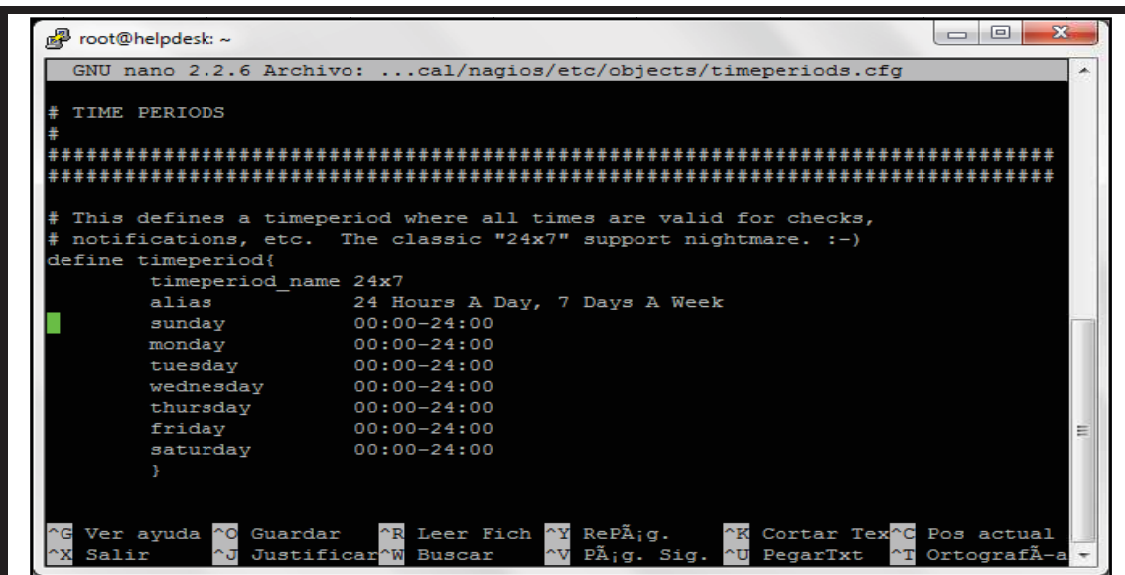
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePÃ;g. ^K Cortar Tex ^C Pos actual
^X Salir    ^J Justificar ^W Buscar ^V PÃ;g. Sig. ^U PegarTxt ^T OrtografÃ-a

```

Figura 59. Ejemplo de *script contacts.cfg*

3.3.6 Script timeperiods.cfg

El *script timeperiods* es el cual donde se definirá el tiempo que va a monitorear el sistema nagios a los componentes de red, en donde se indicará que el periodo de tiempo será las 24 horas del día por los 7 días de la semana.



```

root@helpdesk: ~
GNU nano 2.2.6 Archivo: ...cal/nagios/etc/objects/timeperiods.cfg
# TIME PERIODS
#
#####
#####
# This defines a timeperiod where all times are valid for checks,
# notifications, etc. The classic "24x7" support nightmare. :-)
define timeperiod{
timeperiod_name 24x7
alias           24 Hours A Day, 7 Days A Week
sunday          00:00-24:00
monday          00:00-24:00
tuesday         00:00-24:00
wednesday       00:00-24:00
thursday        00:00-24:00
friday          00:00-24:00
saturday        00:00-24:00
}

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePÃ;g. ^K Cortar Tex ^C Pos actual
^X Salir    ^J Justificar ^W Buscar ^V PÃ;g. Sig. ^U PegarTxt ^T OrtografÃ-a

```

Figura 60. Ejemplo *script timeperiods.cfg*

3.3.7 Script localhost.cfg

Este *script* cuenta con información del servidor basado en Linux el cual contiene al sistema nagios, dentro del archivo se tiene parámetros de configuración para sistema operativo linux de cualquier distribución, debido a que comparten similares características en la ejecución interna de comandos en cada uno de ellos.

A continuación se detallara brevemente los campos que tiene el archivo:

Tabla 6. Campos a ser ingresados en el script localhost.cfg

Campo	Información a Completar	Descripción
use	linux-server	→ <i>Template</i> de archivo por defecto
host_name	Jupiter	→ Nombre del servidor
alias	Jupiter	→ Alias de servidor
address	172.22.2.5	→ Dirección IP
parents	DMZ	→ Pariente de equipo
icon_image	debian.gif	→ Imagen de dispositivo para map
statusmap_image	debian.gd2	→ Imagen para despliegue de map

```

GNU nano 2.2.6 Archivo: ...local/nagios/etc/objects/localhost.cfg Modificado
    address                127.0.0.1
    icon_image             debian.gif
    statusmap_image       debian.gd2
}

define host{
    use                    linux-server      ; Name of host template$
    host_name              Jupiter
    alias                  Jupiter
    address                172.22.2.5
    parents                DMZ
    icon_image             debian.gif
    statusmap_image       debian.gd2
}

define host{
    use                    linux-server      ; Name of host template$
    host_name              Ahorros
    alias                  Ahorros
    address                172.22.2.8
}
  
```

Figura 61. Ejemplo de *script localhost.cfg*

3.3.8 Script windows.cfg

En este archivo se definirán única y exclusivamente equipos con sistema operativo Windows. A continuación se detallara los campos que contiene el archivo.

Tabla 7. Campos a ser ingresados en el script *windows.cfg*

Campo	Información a Completar	Descripción
use	windows-server	→ Template de archivo por defecto
host_name	urano	→ Nombre de servidor
alias	urano	→ Alias de servidor
address	10.0.1.12	→ Dirección IP
parents	DMZ	→ Grupo al que pertenece
icon_image	windows_server.gif	→ Imagen de dispositivo paramap
statusmap_image	windows_server.gd2	→ Imagen para despliegue de map

```

root@helpdesk: ~
GNU nano 2.2.6 Archivo: ...r/local/nagios/etc/objects/windows.cfg Modificado

# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host{
    use                windows-server ; Inherit default values from a template
    host_name          urano           ; The name we're giving to this$
    alias              urano           ; A longer name associated with$
    address            10.0.1.12       ; IP address of the host
    parents            DMZ
    icon_image         windows_server.gif
    statusmap_image    windows_server.gd2
}

define host{
    use                windows-server ; Inherit default values from a template
    host_name          srvap101        ; The name we're giving$
    alias              srvap101        ; A longer name associa$
    address            172.22.4.17     ; IP address of the host
    parents            DMZ
}


^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePÃ;g. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V PÃ;g. Sig. ^U PegarTxt ^T OrtografÃ-a

```

Figura 62. Ejemplo de *script windows.cfg*

3.3.9 Script switch/router.cfg

Este archivo relaciona a los enlaces LAN y WAN, es aquí donde se defina el direccionamiento IP de cada dispositivo, los nombres de los componentes y al grupo que pertenecerán



```

root@helpdesk: ~
GNU nano 2.2.6 Archivo: /usr/local/nagios/etc/objects/switch.cfg Modificado

statusmap_image    router.gd2
}

define host{
use                 generic-switch ; Inherit default values from a template
host_name          Tulcan          ; The name we're giving to this$
alias              Tulcan          ; A longer name associated with$
address 10.0.34.1  ; IP address of the switch
hostgroups         switches        ; Host groups this switch is ass
parents R-C-AG-N
icon_image         router.gif
statusmap_image    router.gd2
}

define host{
use                 generic-switch ; Inherit default values from a template
host_name          Ibarra          ; The name we're giving to this$
alias              Ibarra          ; A longer name associated with the swi$
address 10.0.8.1   ; IP address of the switch
}

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePÃ;g. ^K Cortar Tex ^C Pos actual
^X Salir    ^U Justificar ^W Buscar  ^V PÃ;g. Sig. ^U PegarTxt ^T OrtografÃ-a

```

Figura 63. Ejemplo de *script switch.cfg*

Por último después de haber finalizado todas las configuraciones en los distintos componentes de red se obtendrá un entorno gráfico amigable y fácil de usar en la interface web del sistema.



Figura 64. Ejemplo de entorno web del sistema nagios

3.4 Interfaz web de Nagios

La interfaz web de nagios es fácil de utilizar y muy intuitiva, todos los módulos que posee el sistema se aloja en la parte izquierda en donde se puede encontrar las siguientes opciones: Mapa del diseño de red, Equipos, Servicios, Grupo de servicios, Grupo de equipos, Problemas de los servicios y equipos, Alertas, Histogramas, Contactos, etc.



Figura 65. Interfaz Web del sistema Nagios

3.4.1 Visión General

Finalizada la configuración de los script de cada módulo y reiniciado el sistema nagios, automáticamente se iniciara la ejecución de los comandos y servicios definidos y poco a poco se va ir dibujando el mapa con los componentes de red definidos.

La primera impresión del sistema es su módulo de mapa, es aquí donde se indicara el diseño y la forma de conexión entre los distintos dispositivos de red con sus respectivos iconos de simbología.

Dentro la interfaz web se podrá visualizar a manera general de todo lo que ocurre con cada uno de los equipos y servicios, permitiendo al administrador tomar decisiones rápidas en base a los datos obtenidos del sistema.



Figura 66. Visión general del sistema

3.4.2 Detalle de los Servicios

En este módulo se mostrara los servicios que se están monitorizando con una descripción del estado en que se encuentran cada uno de los ellos.



Figura 67. Estado de los servicio

En el detalle de los servicios se puede monitorear y visualizar los distintos servicios configurados que se ejecutan en cada uno de los equipos activos, como por ejemplo: en el servidor GUP-LATAACUNGA indica el nombre del servicio y el estatus en el que se encuentran los servicios de espacio en disco, carga del procesador, usuarios conectados, uso de memoria RAM, el protocolo *DHCP*. El estatus presentado es un *OK*, el cual nos da la interpretación de cada uno de los servicios están funcionando correctamente, si en caso de que uno de los servicios presenta alguna anomalía el color cambia a amarillo con la palabra *WARNING* o si hay un fallo completo el color cambia a rojo con la palabra *CRITICAL*. Estos tres estados se diferencian de la siguiente manera:

OK.- Cuando todos los servicios funcionan correctamente.

WARNING.- Indica una anomalía en uno de los servicios.

CRITICAL.- Cuando un equipo o servicio falla

3.4.3 Detalle de los equipos

Este módulo mostrara a cada uno de los distintos componentes de red que se encuentran monitoreados con sus estados e información detallada de cada uno de ellos.

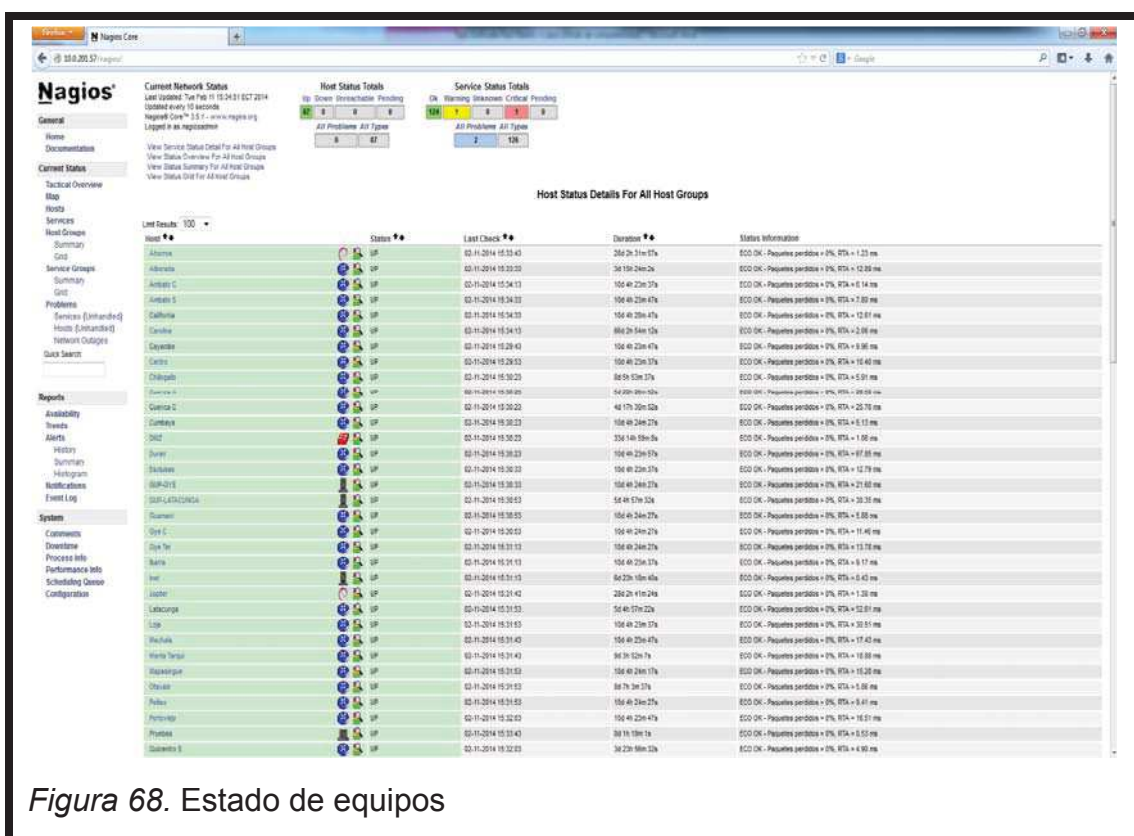


Figura 68. Estado de equipos

En detalle de los equipos se observa el estatus en que se encuentra cada uno de los equipos que están siendo monitoreados, teniendo como estados un *UP* o un *DOWN* en caso de fallos.

3.4.4 Estado detallado de equipos

Dentro de este módulo mostrara el estado en que se encuentra el equipo y los servicios asociados que tendrán configurado en cada uno de los dispositivos.

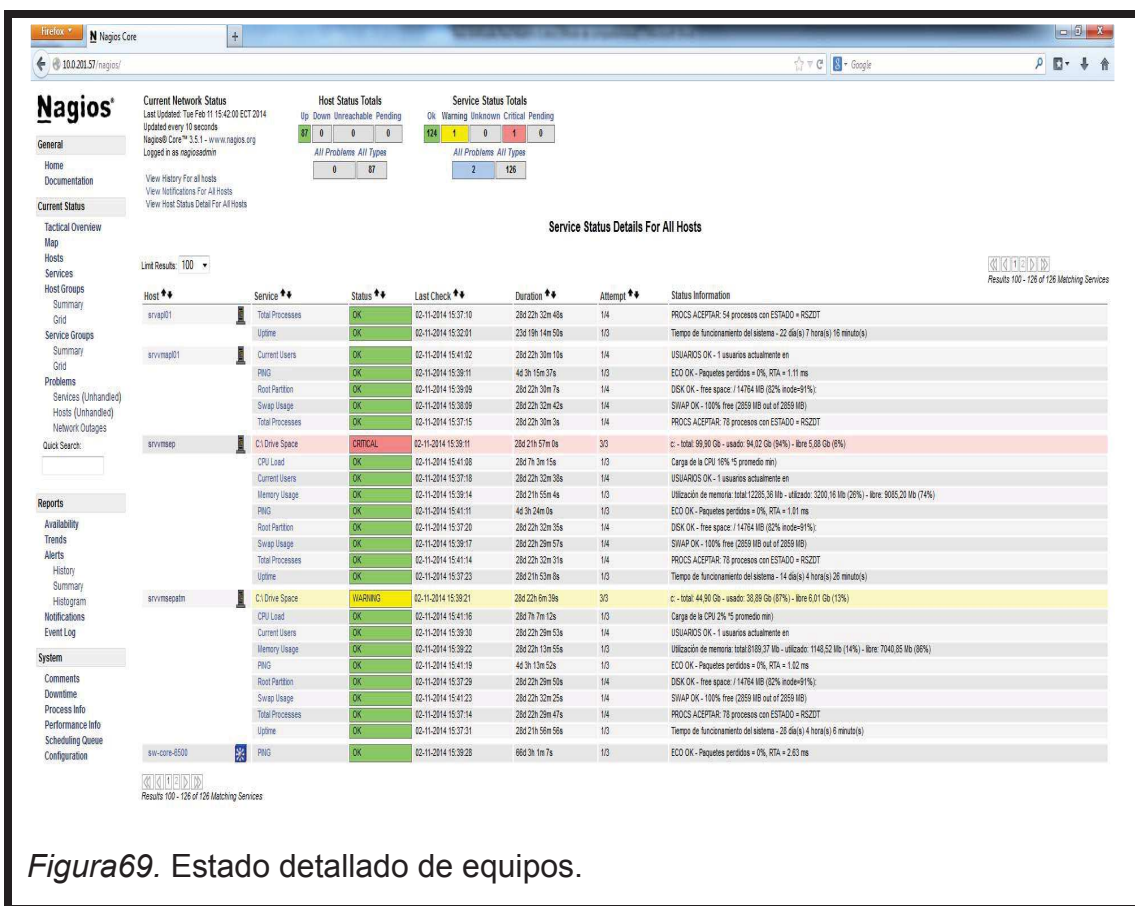


Figura69. Estado detallado de equipos.

En la gráfica 67 se evidencias una anomalía en uno de los servicios de dos servidores, este servicio pertenece al espacio en disco, como ya se mencionado para cada servicio se identifica con colores, donde se puede diferenciar entre un advertencia y una falla critica del mencionado servicio.

3.4.5 Problemas con los equipos y servicios.

En este módulo se encuentran exclusivamente los diferentes equipos que tienen problemas de funcionamiento de manera detallada. Este módulo será el más útil para el administrador ya que podrá verificar la falla generada por el o los equipos.

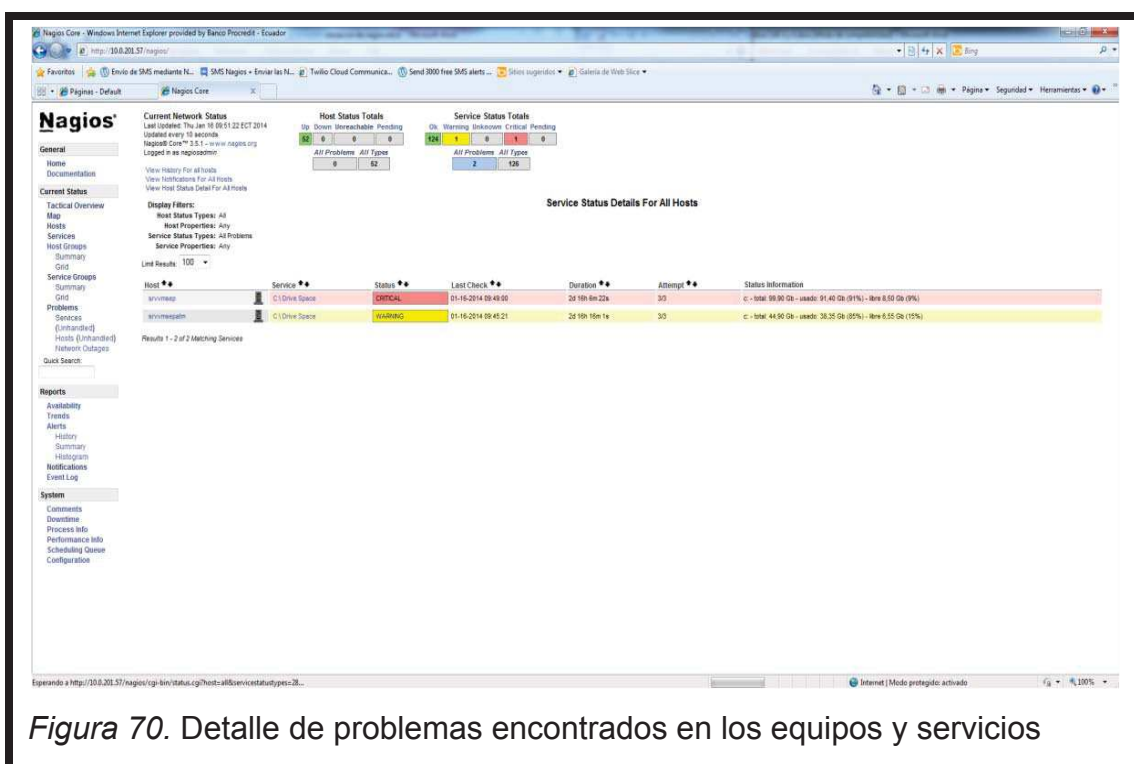


Figura 70. Detalle de problemas encontrados en los equipos y servicios

3.4.6 Grupo de equipos y servicios

Dentro de estos dos módulos se podrá apreciar de manera resumida todos los equipos y servicios con sus estados.



Figura 71. Grupos de equipos y servicios.

3.4.7 Informe de Disponibilidad.

En este módulo se presenta los resultados en porcentajes de tiempo de la disponibilidad que han tenido los equipos de red, además permite tener estadísticas de las fallas que con frecuencia un dispositivo sufre y tomar acciones sobre él.

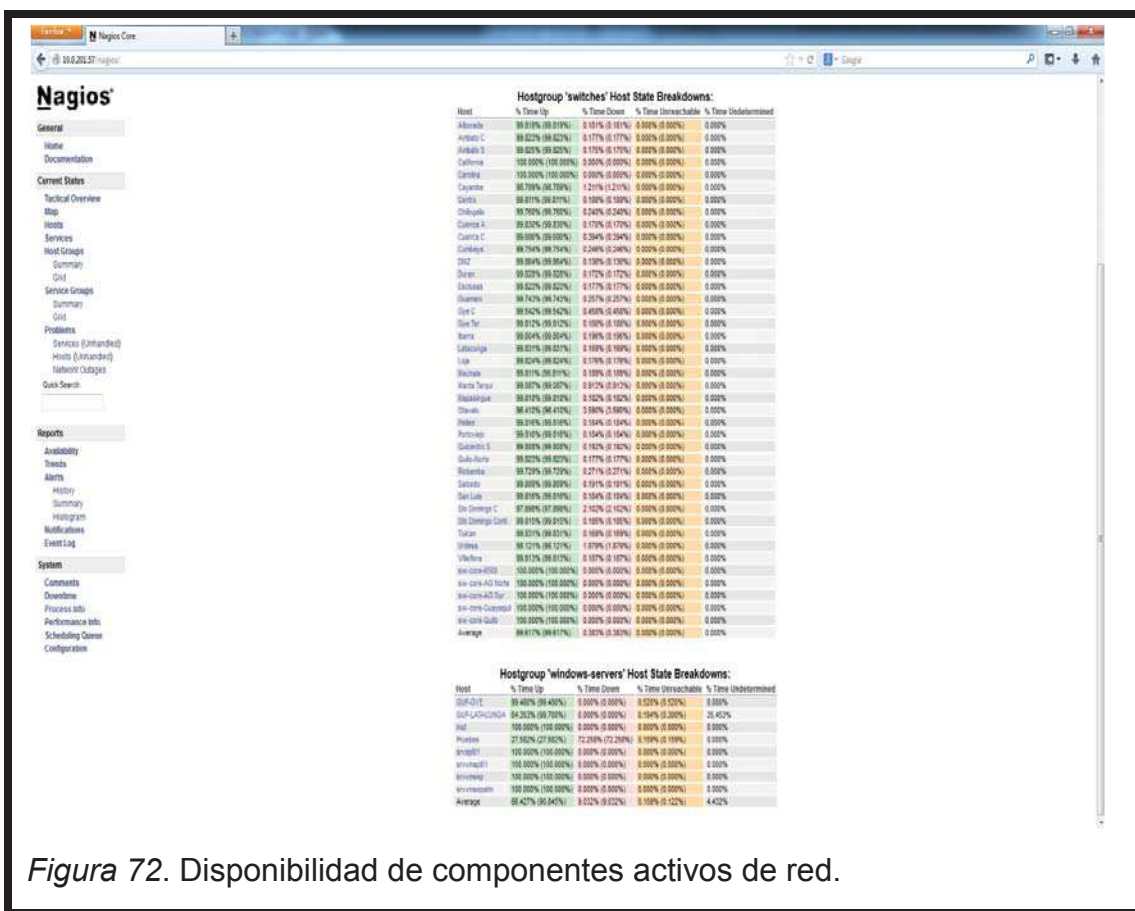


Figura 72. Disponibilidad de componentes activos de red.

3.4.8 Histograma

En este módulo permite ver de forma gráfica los cambios que hayan tenido un equipo o servicio monitoreado, además se utiliza para realización de informes ejecutivos

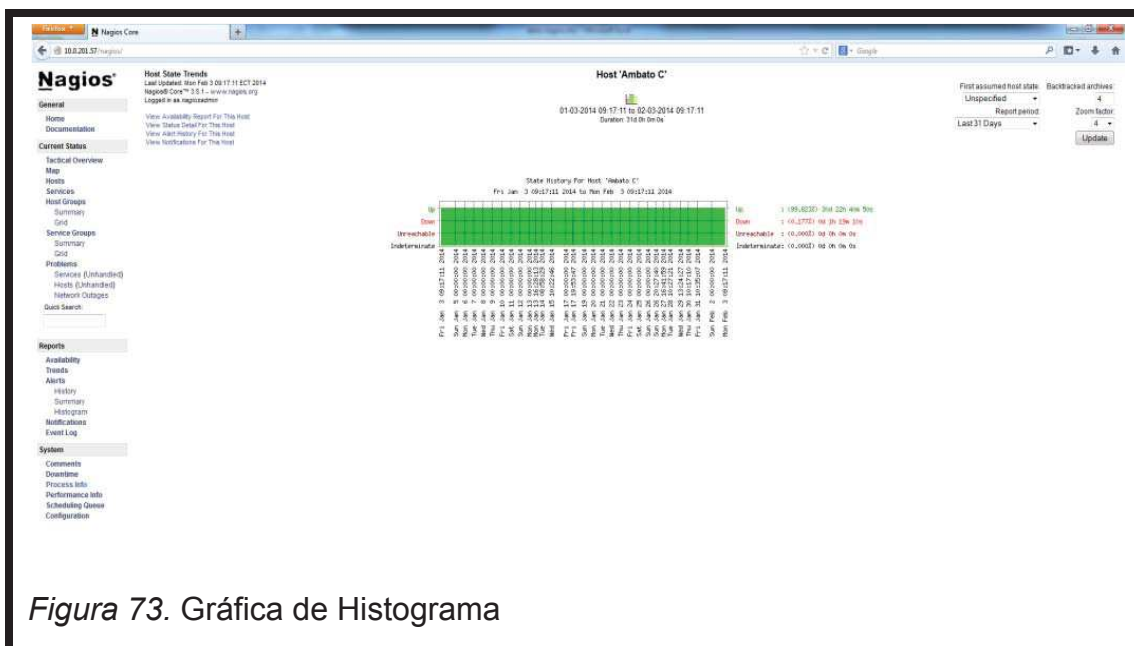


Figura 73. Gráfica de Histograma

3.4.10 Contactos

En esta opción permite ver los datos de configuración de cada contacto creado así como también el periodo con el cual se realiza la monitorización de los componentes activos, y el método que se utiliza para el envío de notificaciones, etc.

Host Name	Alias/Description	Address	Parent Hosts	Max. Check Attempts	Check Interval	Retry Interval	Host Check Command	Check Period	Check Over	Enable Active Checks	Enable Passive Checks	Check Freshness	Freshness Threshold	Default Contacts/Groups	Notification Interval	First Notification Delay	Notification Options	Notification Period	Event Handler	Enable Event Handler	Dabling Options	Enable Flap Detection	Low Flap Threshold	High Flap Threshold
Atlanta	Atlanta	172.22.2.8	DRZ	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Unreachable, Recovery	30hours		Yes	None	Yes	Program-wide value	Program-wide value
Atlanta A	Atlanta A	10.0.17.1	10-1000-AG-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Atlanta C	Atlanta C	10.0.2.1	10-1000-AG-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Atlanta S	Atlanta S	10.0.24.9	10-1000-AG-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
California	California	10.0.12.1	10-1000-CA-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Carlsbad	Carlsbad	10.0.19.1	10-1000-CA-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Cayman	Cayman	10.0.1.1	10-1000-AG-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Centro	Centro	10.0.10.1	10-1000-CA-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Chicago	Chicago	10.0.16.1	10-1000-CA-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Cuenca A	Cuenca A	10.0.40.1	10-1000-AG-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Cuenca C	Cuenca C	10.0.18.1	10-1000-AG-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
Curitiba	Curitiba	10.0.30.1	10-1000-CA-Sur	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value
DRZ	DRZ	172.22.2.8	10-1000-1000	10	30 Sec	30 Sec	ifconfig -t	2x7	Yes	Yes	Yes	No	Auto-determined value	admins	30 Sec	30 Sec	Down, Recovery	2x7		Yes	None	Yes	Program-wide value	Program-wide value

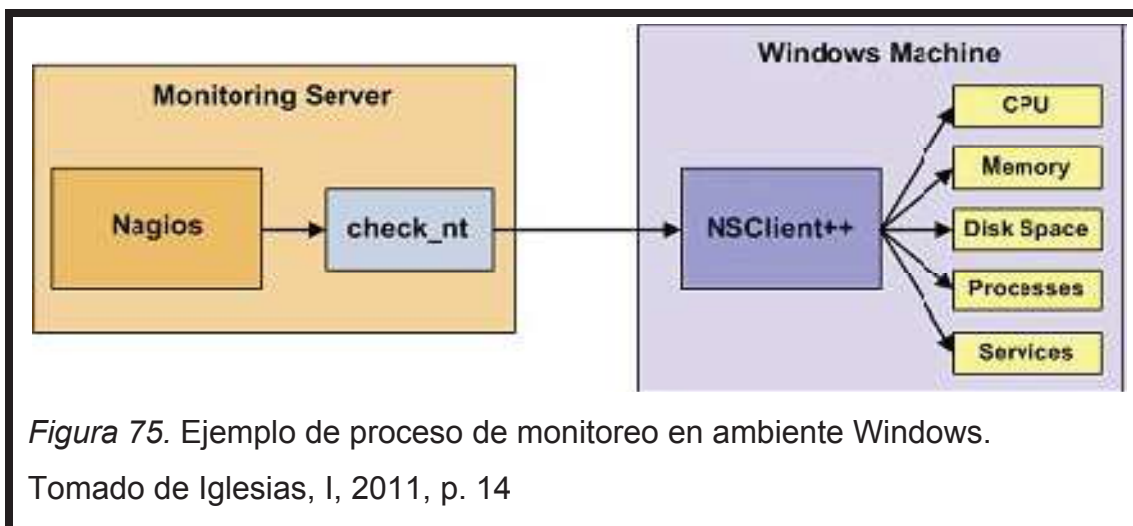
Figura 74. Módulos de contactos.

3.5 Instalación y Configuración de Clientes

3.5.1 Cliente Nagios para Windows

Para poder realizar una monitorización en equipos con sistema operativo Windows se debe instalar un agente dentro de ellos. El agente actuara como una pasarela entre los *plugins* de nagios los cuales se encargaran de realizar un seguimiento de los servicios definidos. Sin el agente instalado no se podrá monitorear de manera activa los servicios o parámetros de los computadores o servidores.

Se utilizara el agente *NSClient++*, este es el más utilizado y popular de lado del ambiente Windows junto con el complemento *check_nt* de Nagios.



Con el agente instalado es posible realizar la monitorización de los servicios y características tales como:

- Carga del CPU
- Uso de memoria RAM
- Espacio en disco duro
- Usuarios ingresados en el sistema
- Total de procesos en ejecución
- Ping
- HTTP
- DHCP

3.5.2 Cliente Nagios para GNU/Linux

Para servidores o computadores con sistema operativo Linux de igual o distinta distribución del servidor de monitoreo no será necesario la instalación de un agente, ya que comparte idénticos archivos en el cual nagios se podrá basar para la toma de información de los servicios y características siendo de esta manera fáciles de configuración, entre los cuales se tendrá:

- Carga del CPU
- Uso de Memoria
- Uso de Memoria *Swap*
- Espacio en discos duros
- Usuarios ingresados en el sistema
- SSH
- HTTP

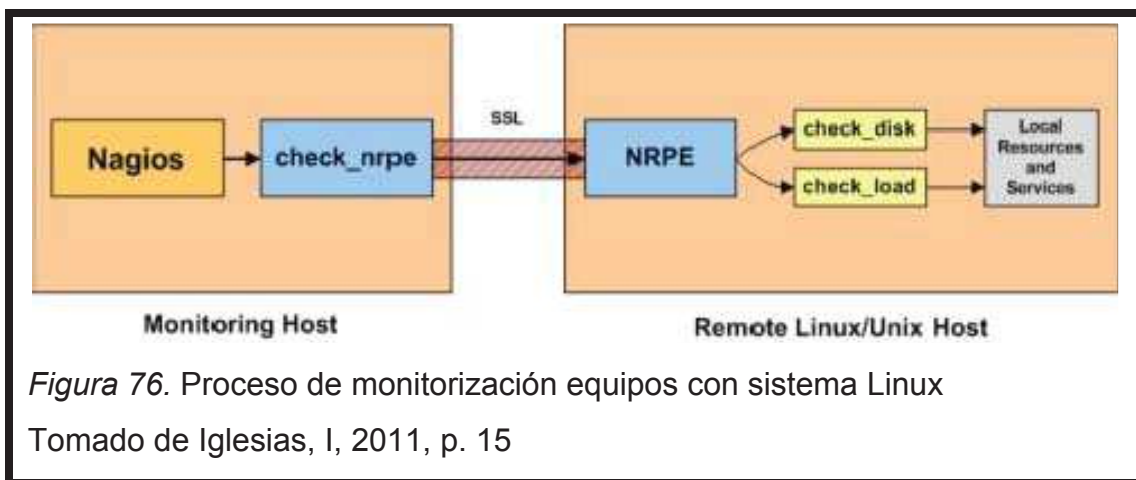


Figura 76. Proceso de monitorización equipos con sistema Linux

Tomado de Iglesias, I, 2011, p. 15

3.6 Instalación y configuración de *Postfix* para envío de correo electrónico

Instalación del agente de correo *Postfix*

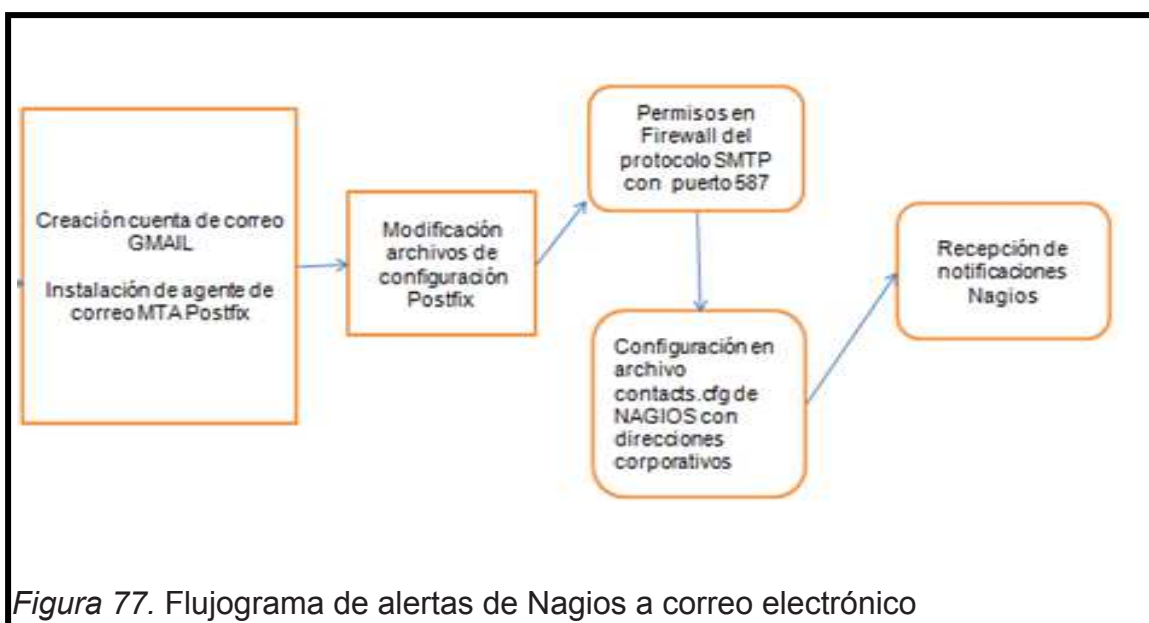
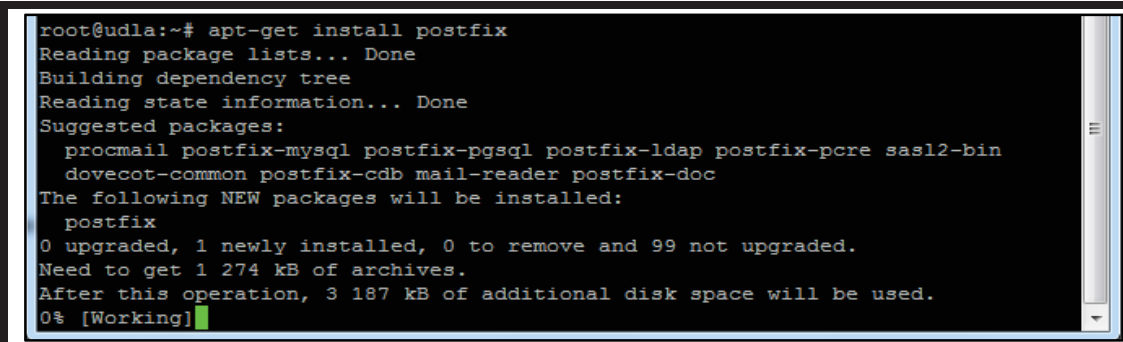


Figura 77. Flujograma de alertas de Nagios a correo electrónico

Como se explicó en el anterior capítulo es necesario utilizar un agente para el envío de correo electrónico hacia las cuentas corporativas indicadas en el archivo de configuración del sistema nagios, en esta ocasión se utilizara *Postfix* y su instalación y configuración se lo realiza mediante el uso de consola.

Como primer paso se debe estar con usuario *root* y se ejecuta el comando *apt-get install postfix*.



```
root@udla:~# apt-get install postfix
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre sasl2-bin
  dovecot-common postfix-cdb mail-reader postfix-doc
The following NEW packages will be installed:
  postfix
0 upgraded, 1 newly installed, 0 to remove and 99 not upgraded.
Need to get 1 274 kB of archives.
After this operation, 3 187 kB of additional disk space will be used.
0% [Working]
```

Figura 78. Instalación de *Postfix*

Un segundo paso a ejecutar es la selección con el cual se conectara el agente al servidor de correo, este caso se utiliza la opción: *Internet Site*.

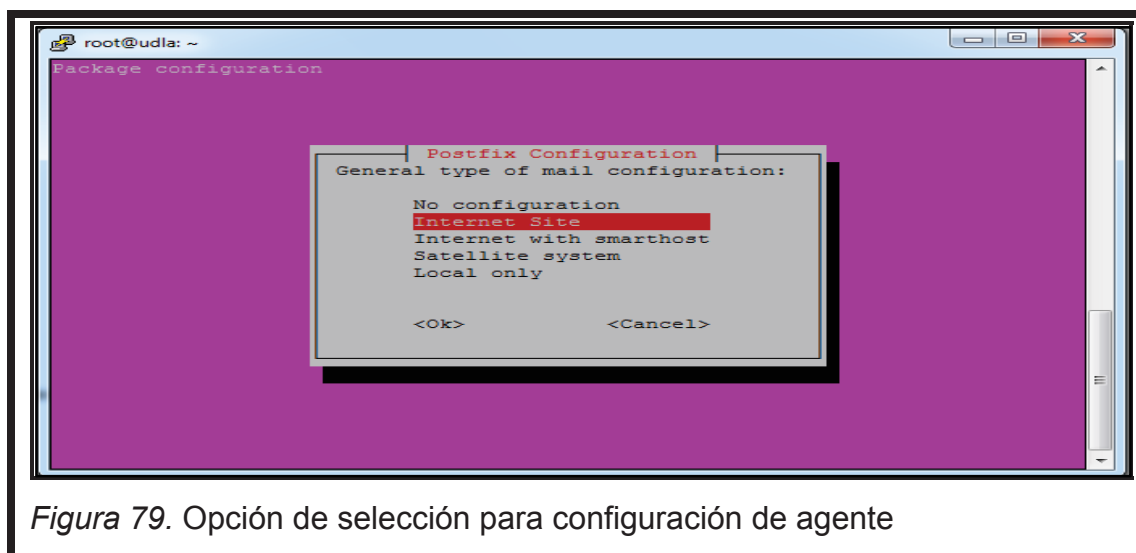


Figura 79. Opción de selección para configuración de agente

Una vez escogida la opción se presenta una tercera pantalla en el cual solicita ingresar un nombre del sistema de correo, al cual debe ser cancelado para que se cargue el agente a los valores por defecto.

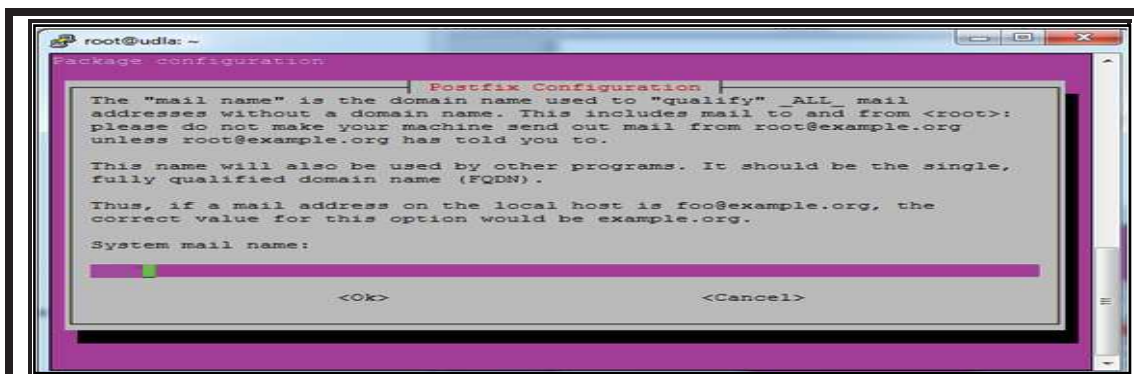


Figura 80. Ejemplo de configuración de Postfix

Por último indica que la instalación del agentes fue realizado exitosamente.

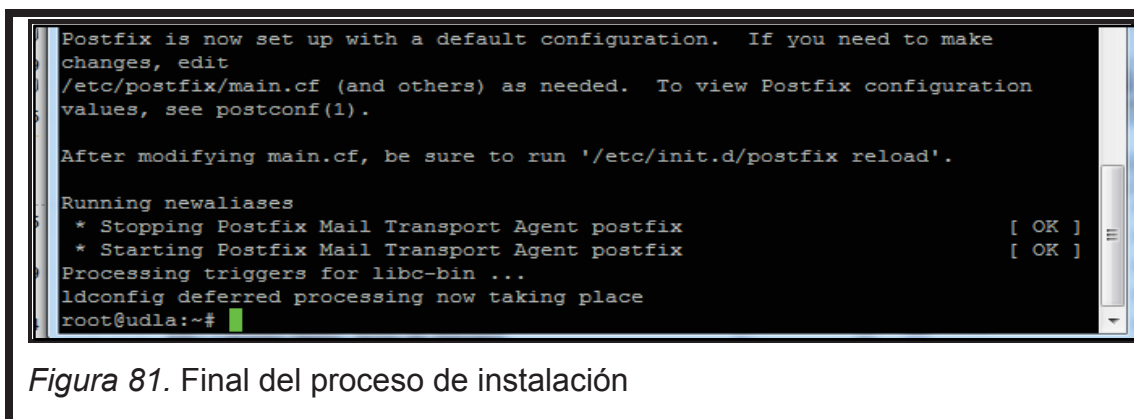


Figura 81. Final del proceso de instalación

Configuración del agente de correo *Postfix*.

La configuración se realiza mediante el método de reenvío de correo utilizando un servidor externo, como puede ser *Gmail*, *Hotmail*, *Yahoo*, etc., en este caso se utiliza *Gmail* en donde se ingresara las credencial dentro de los archivos de configuración del agente.



Figura 82. Archivo de configuración *main.cf*

En el siguiente directorio se indica el usuario y contraseña de la cuenta creada en los servidores de *Gmail*, esta información recibirá el servidor de forma encriptada.

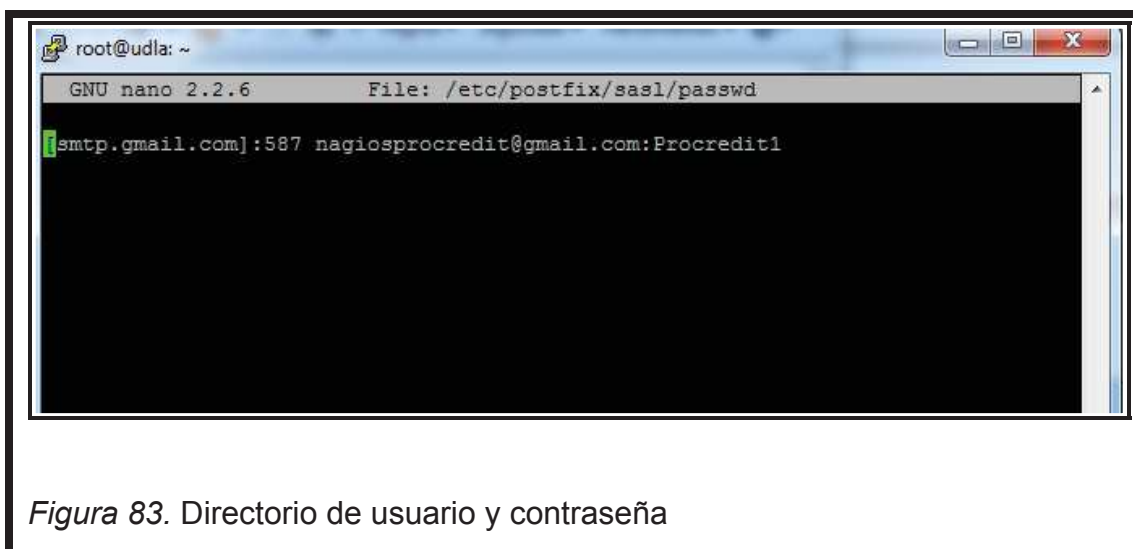


Figura 83. Directorio de usuario y contraseña

3.7 Instalación de aplicativo *Ozeki NG SMS Gateway* para el envío de SMS



Para el envío de mensajes cortos SMS, se utiliza la aplicación *Ozeki NG SMS Gateway*, esta aplicación tendrá una interface web para la administración y la configuración del envío de mensajería corta.

Esta aplicación será la más apropiada para la interacción entre el servidor del sistema nagios y el modem GSM debido a que tiene una gran versatilidad y compatibilidad con el dispositivo mencionado.

Para el proceso de instalación se requiere de los siguientes complementos que necesita la aplicación para su buen funcionamiento.

Como primer paso se tendrá que instalar las dependencias conocidas como *Mono Framework* para sistemas Linux

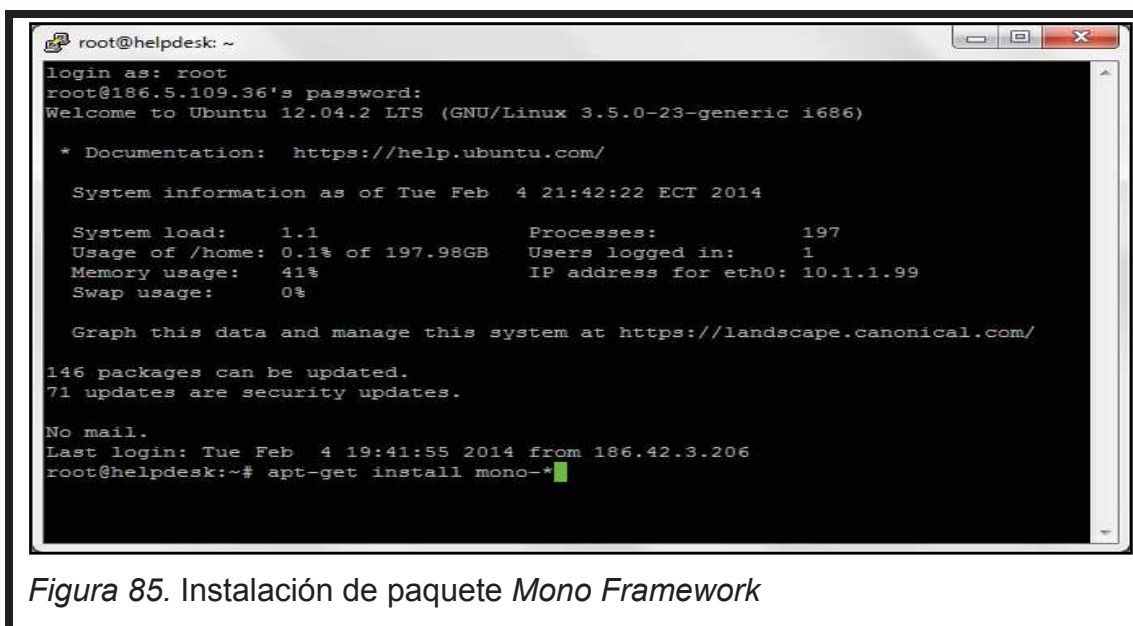


Figura 85. Instalación de paquete *Mono Framework*

Terminada la instalación se procede a instalar librerías especiales que utilizan las dependencias *Mono Framework* con el uso del siguiente comando: `apt-get install libmono-winforms2*`

Una vez instalada la dependencia con su respectiva librería se procede al cambio de directorio donde se descargara el sistema de mensajería corta

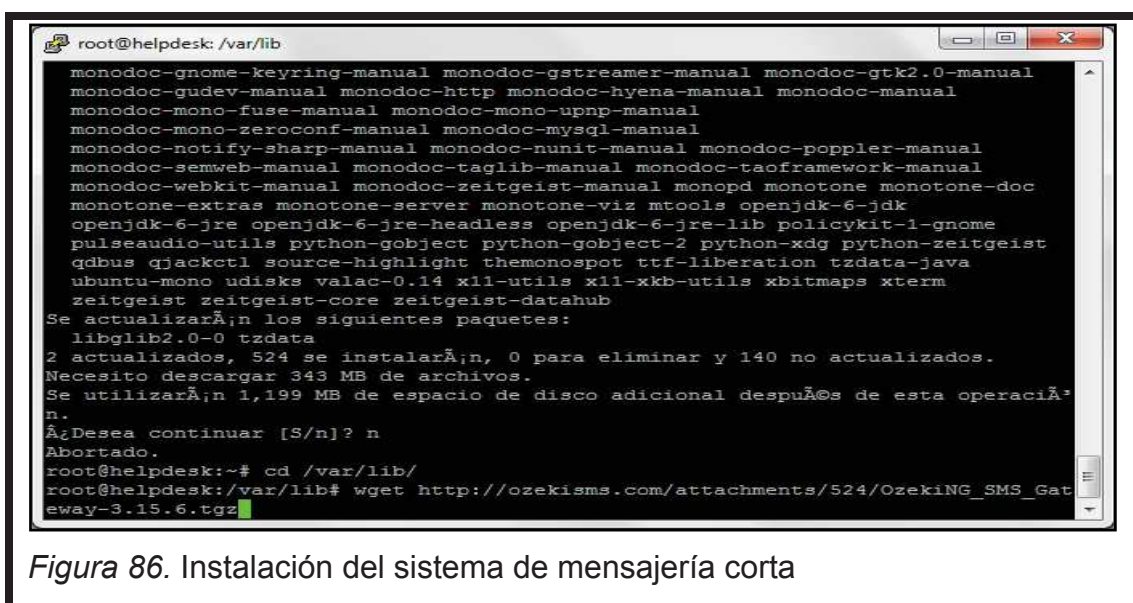


Figura 86. Instalación del sistema de mensajería corta

Por último compilado y ejecutado todos los complementos se obtiene la siguiente información acerca de la instalación de la aplicación.

```

root@nagios-server: /var/lib/OzekiNG_SMS_Gateway-3.15.6
03/02/2014 18:16:33 - 0 rows in set
Connecting to service providers...
03/02/2014 18:16:33 -
03/02/2014 18:16:33 - Inbound routing
03/02/2014 18:16:33 - +-----+-----+-----+-----+-----+-----+
03/02/2014 18:16:33 - | | Name | Operator | Originator | Recipient | Keyw
03/02/2014 18:16:33 - +-----+-----+-----+-----+-----+-----+
03/02/2014 18:16:33 - | 1 | defaultin | ANY | ANY | ANY | ANY
03/02/2014 18:16:33 - +-----+-----+-----+-----+-----+-----+
03/02/2014 18:16:33 - 1 rows in set
03/02/2014 18:16:33 -
03/02/2014 18:16:33 - Outbound routing
03/02/2014 18:16:33 - +-----+-----+-----+-----+-----+-----+
03/02/2014 18:16:33 - | | Name | User | Originator | Recipient | Keyword
03/02/2014 18:16:33 - +-----+-----+-----+-----+-----+-----+
03/02/2014 18:16:33 - | 1 | defaultout | ANY | ANY | ANY | ANY
03/02/2014 18:16:33 - +-----+-----+-----+-----+-----+-----+
03/02/2014 18:16:33 - 1 rows in set
Connecting to users/applications...
Opening GUI to accept connections on http port...
Ozeki NG SMS Gateway Service started. Open http://127.0.0.1:9501 to configure!
Type 'x' to stop OzekiNG
03/02/2014 18:16:33 - INFO 3014: Service initialized successfully.

```

Figura 87. Finalización de instalación

Por medio de un explorador de internet se ingresa a la interfaz web de la aplicación donde el usuario y la contraseña vienen predefinidos en la configuración, para el acceso se digita la siguiente dirección:
http://10.0.201.57:9501



Figura 88. Interfaz web de autenticación del sistema Ozeki NG SMS Gateway

Autenticados con las credenciales correctas se accede a la parte de administración y configuración de la aplicación.



Figura 89.- Consola de administración y configuración del sistema

Luego accedemos a las formas de conexión que el programa puede realizar para la conexión con el modem GSM, ahí escogemos la opción “*GSM Modem Connection Install*”.

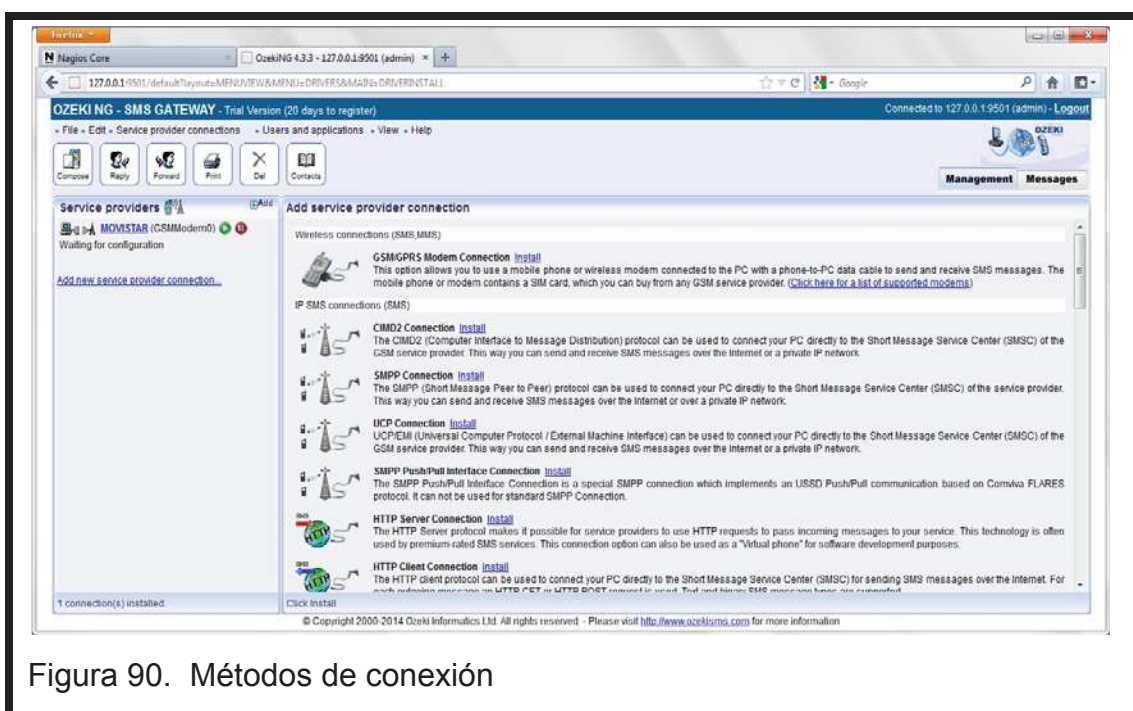


Figura 90. Métodos de conexión

Se crea el usuario NAGIOS para realizar modificación en las opciones de mensajes de entrada y de salida

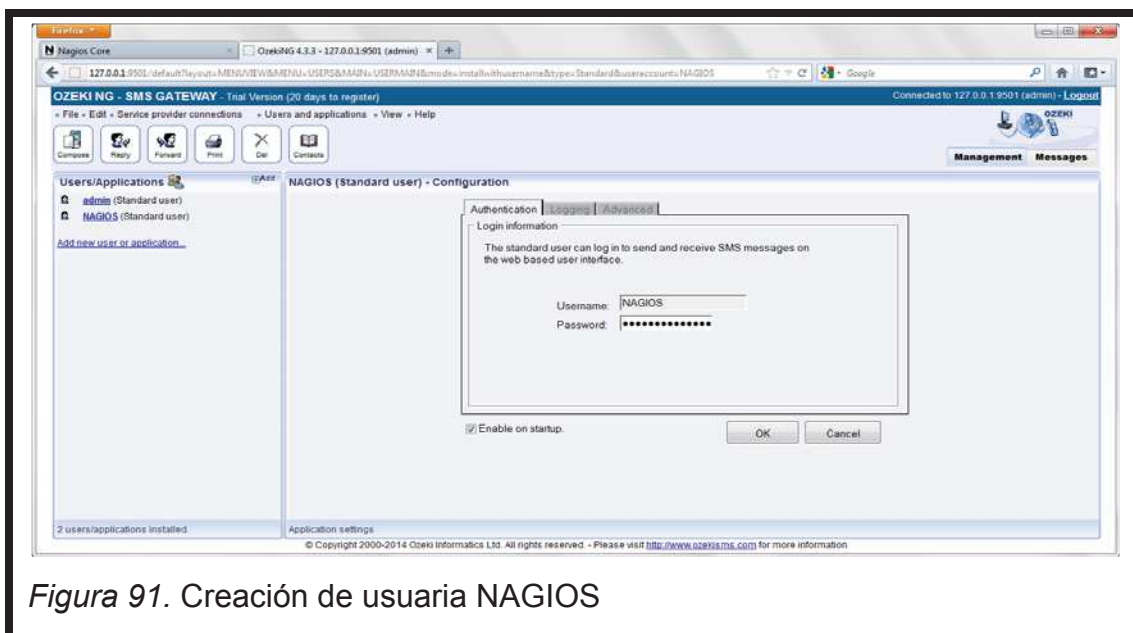


Figura 91. Creación de usuario NAGIOS

Seguidamente se inicia con la configuración del ruteo de mensajes tanto de entrada como de los de salida, en donde se debe tener cuidado con el ingreso de los números celulares a los cuales llegarán los mensajes del sistema, los números son ingresados en formato internacional.



Figura 92. Ruteo de mensajes entrantes

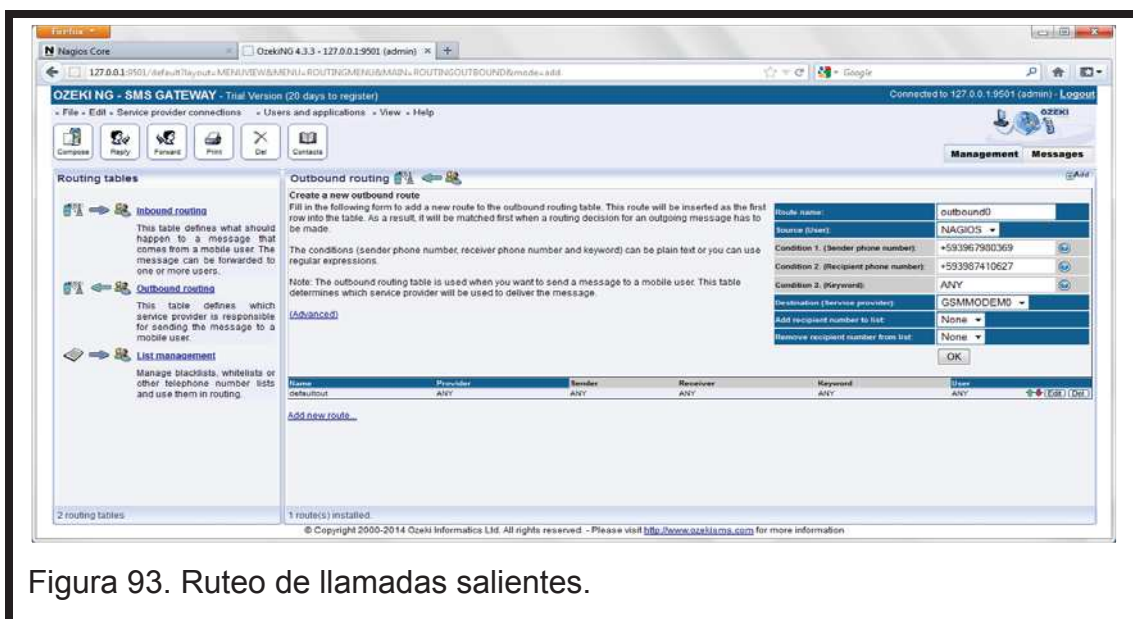


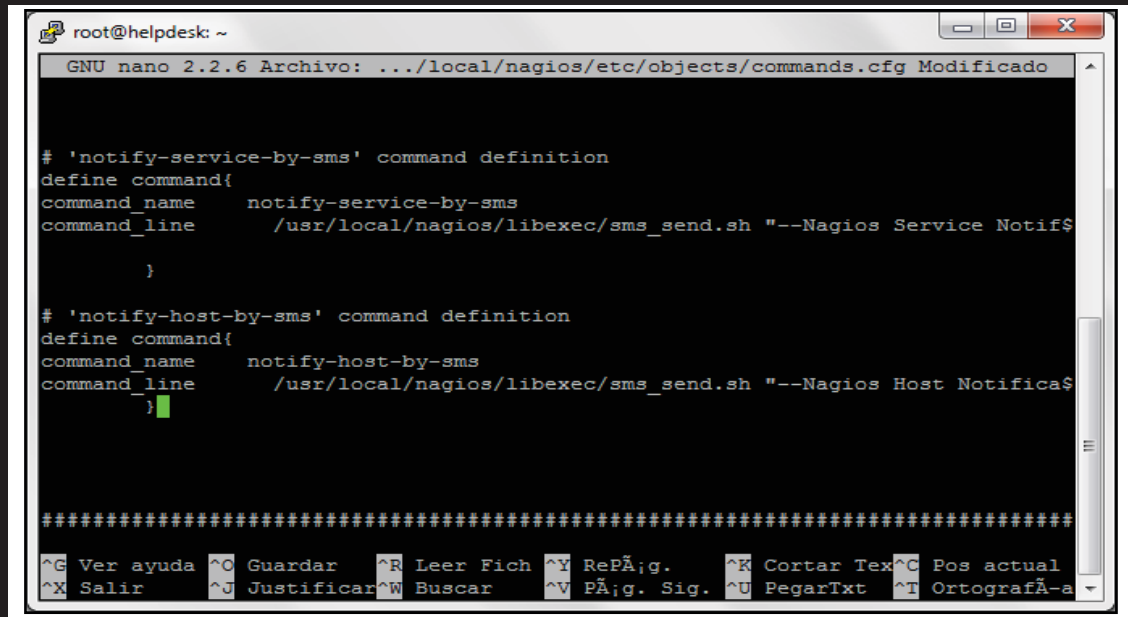
Figura 93. Ruteo de llamadas salientes.

Culminada con las configuraciones en el aplicativo de administración de mensajería corta, se procede a realizar la descarga del archivo para el sistema de monitoreo, este archivo tiene la función de hacer el envío hacia el aplicativo de las alertas generadas por nagios, en dicho archivo se pone el número del teléfono del modem GSM, el directorio que contiene el archivo es “/usr/local/nagios/libexec”, para acceder al archivo y realizar la modificación mencionada se utiliza el editor de texto mencionado en capítulos anteriores ejemplo: “*nano /usr/local/nagios/libexec/sms_send.sh*”



Figura 94. Modificación archivo sms_send.sh

El último paso es definir en el archivo *commands* el segundo método que tendrá el sistema para realizar el envío de las notificaciones al o a los usuarios configurados para el recibo mediante SMS



```
root@helpdesk: ~
GNU nano 2.2.6 Archivo: .../local/nagios/etc/objects/commands.cfg Modificado

# 'notify-service-by-sms' command definition
define command{
command_name    notify-service-by-sms
command_line    /usr/local/nagios/libexec/sms_send.sh "--Nagios Service Notif$
}

# 'notify-host-by-sms' command definition
define command{
command_name    notify-host-by-sms
command_line    /usr/local/nagios/libexec/sms_send.sh "--Nagios Host Notifica$
}

#####
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePÃ¡g. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V PÃ¡g. Sig. ^U PegarTxt ^T OrtografÃ-a
```

Figura 95. Agregación del segundo método de envío de alertas

Terminada con las configuraciones correctas el sistema automáticamente iniciará el proceso de envío de mensajes del sistema nagios cuando se presenten anomalías en el comportamiento de los equipos y servicios monitoreados.

4. Pruebas del sistema de Monitoreo Nagios

4.1 Pruebas de funcionalidad

A partir de su instalación y configuración, el sistema de monitoreo Nagios ha mantenido un óptimo funcionamiento como en su rendimiento en los distintos entornos presentados, sean estos equipos con sistema operativo Windows y Linux.

Cada uno de sus módulos ha mantenido una constante supervisión sobre los equipos y servicios definidos para la monitorización, actuando sin inconveniente en alertar sobre alguna falla presentada dentro de la empresa al personal de TI, además cabe mencionar su óptimo acople con el agente *NSClient++* tanto en computadoras de escritorio y en servidores con Windows.

En la parte de notificaciones por medio de correo electrónico el agente de transporte no ha tenido dificultades en realizar el reenvío de alertas de fallas presentadas dentro de los componentes de red como en sus enlaces de comunicación a las cuentas corporativas del personal de infraestructura tecnológica.

A continuación se presentan los siguientes gráficos del sistema implementado con sus distintos módulos y componentes activos, además se muestra una falla de dos componentes en dos servidores con su respectivo envío de notificaciones al correo electrónico informando el problema que se está suscitando en cada uno de ellos.

Los problemas que indica el sistema de monitoreo son los siguientes:

En el servidor *srvvmsepatm* es el poco espacio que tienen en disco duro en la actualidad, he indica con color amarillo con un 14% de disponibilidad, convirtiéndose así un peligro para un óptimo funcionamiento del servidor.

En el otro caso en el servidor srvvmsep indica con color rojo que tiene un 7% de espacio en disco duro el cual se convierte en un problema crítico para el funcionamiento del servidor.

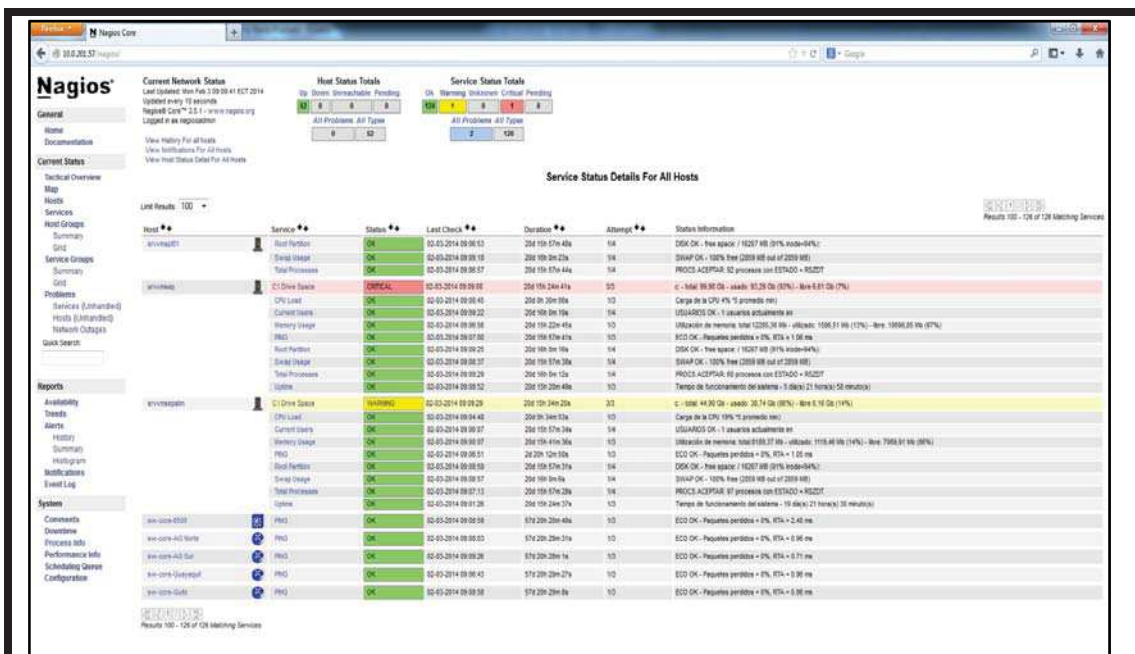


Figura 96. Módulo de equipos y servicios de los componentes activos de red.

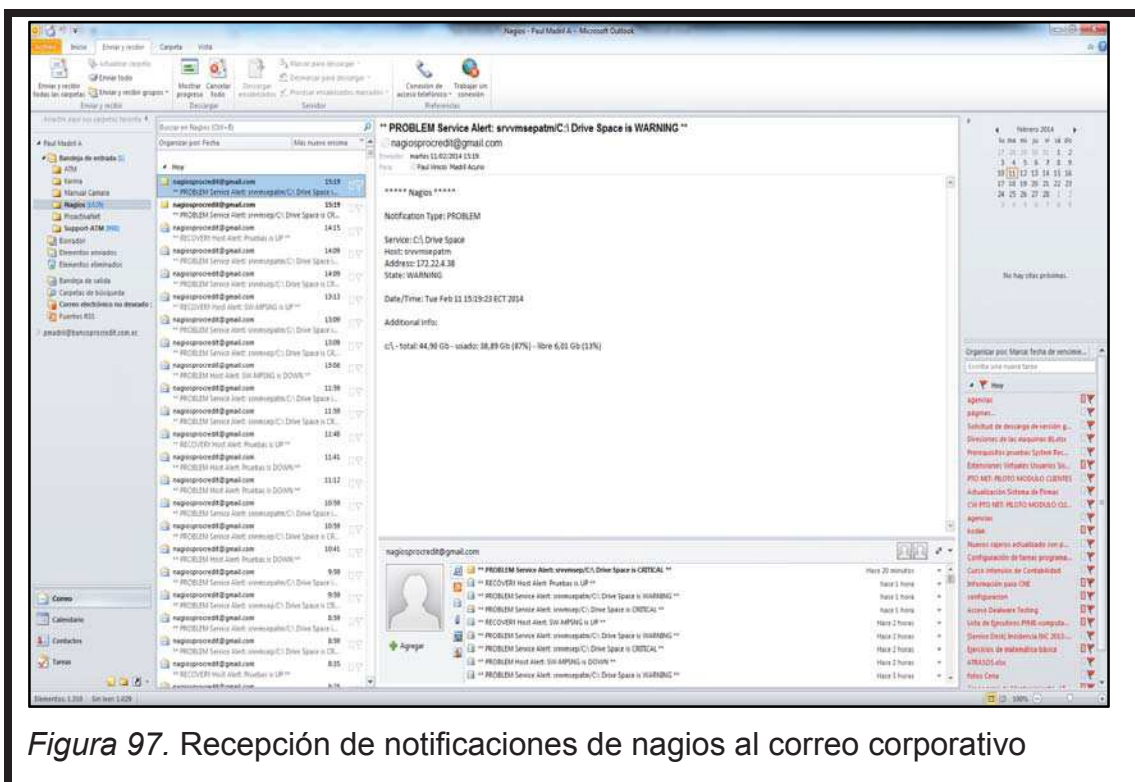


Figura 97. Recepción de notificaciones de nagios al correo corporativo

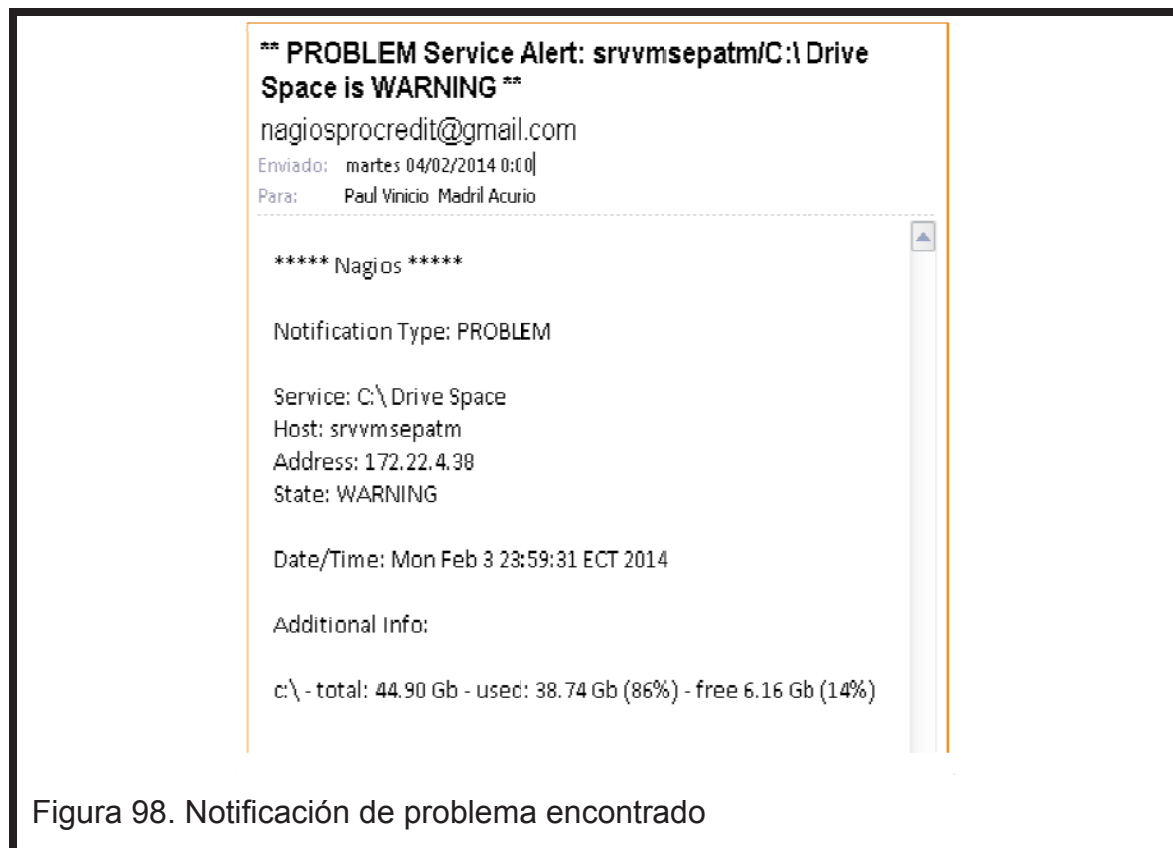


Figura 98. Notificación de problema encontrado

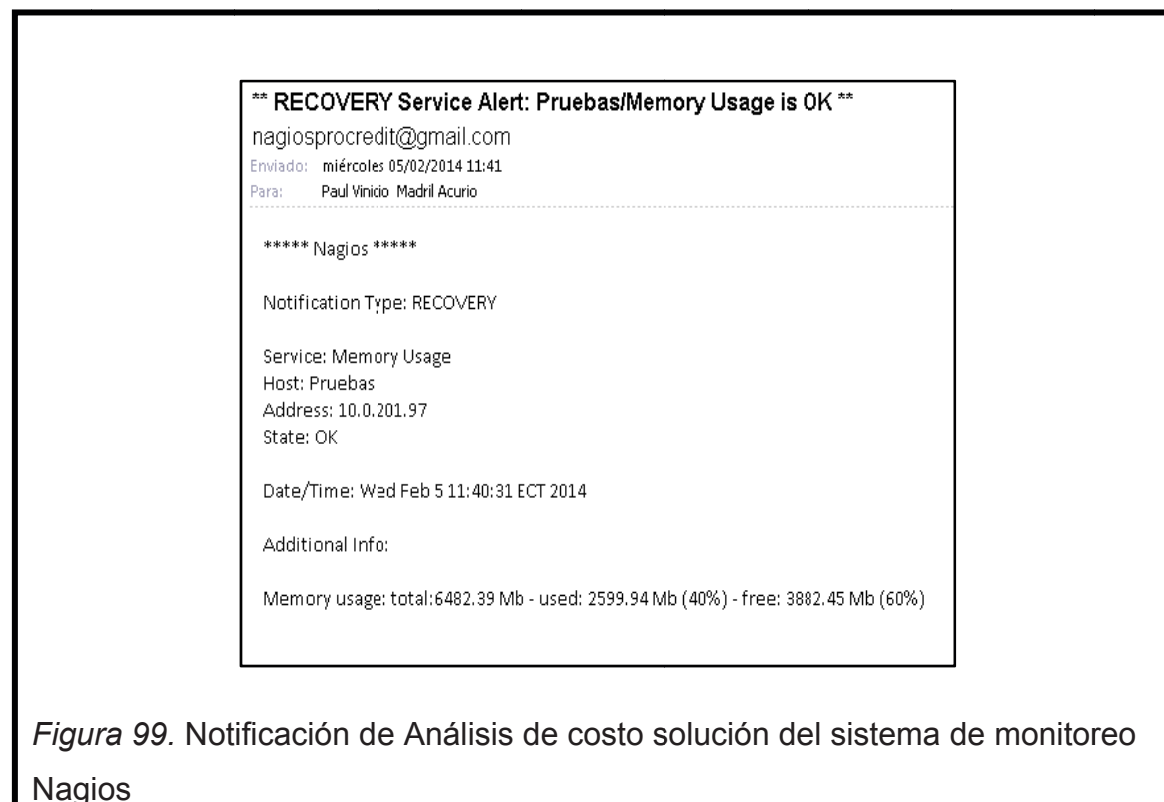


Figura 99. Notificación de Análisis de costo solución del sistema de monitoreo Nagios

La inversión a realizarse para el sistema de monitoreo realmente es mínima debido a que el sistema operativo Linux como el sistema de monitoreo Nagios tienen licencia GNU y por ende no se pagara ningún costo. Adicional los gastos incurridos son relacionados al computador y al modem GSM que se utiliza para llevar a cabo la implementación.

Para un sistema operativo baso en Linux no se necesario contar con un potente equipo sino más bien se utiliza un computador de escritorio con características medianas tanto en memoria, espacio en disco y procesador que cubran los requerimientos indicados en capítulos anteriores.

Tabla 5. Características y costos de equipos

NOMBRE	CARACTERÍSTICAS	VALOR
<p data-bbox="327 1055 683 1088">CPU HP COMPAQ 5700</p> 	<p data-bbox="810 1055 1158 1200">Memoria Ram 2GB Disc0 Duro de 150GB Procesador Core 2 Duo</p>	<p data-bbox="1190 1167 1305 1200">300,00\$</p>
<p data-bbox="228 1335 778 1424">MODEM GSM Fast Track Wavecom Q2303A</p> 	<p data-bbox="810 1279 1158 1648">Case de aluminio Cable RS 232 Antena Adaptador de corriente Frecuencia GSM Dual 850/1900MHz Soporta comando AT</p>	<p data-bbox="1190 1447 1289 1480">60,00\$</p>

El valor total de la inversión será de 360,00\$, este valor corresponderá únicamente a la parte de hardware.

4.2 Costo Beneficio de solución

El costo del sistema de monitoreo será bastante accesible para cualquier empresa sea esta mediana o grande, la inversión es únicamente en hardware y por el pago de licencias del sistema no tendrá que preocuparse debido q que es un software gratuito y se encuentra bajo la licencia GNU.

Los beneficios que obtendrá con el sistema Nagios son muchos más que otros sistemas pagados, debido a su gran versatilidad, acople y a una comunidad entera de desarrolladores a nivel mundial, tendrá soporte para cualquier inconveniente que se presente a futuro, contar con actualizaciones que son fáciles de implementar y lo que es mejor sin costo alguno.

4.3 Costo Mantenimiento Servidor

El costo del mantenimiento del servidor será variable ya que se dependerá de las partes de hardware que posea, puede ser desde un cambio de fuente de poder hasta el cambio de tarjeta de red, los montos de estas piezas se indicara la siguiente tabla de valores

Tabla 6. Costo de servidor

Tipo de Hardware	Precio
Fuente de Poder	20,00\$
Tarjeta de Red 10/100/1000	15,00\$
Memoria RAM de 2GB	15,00\$

Para realizar los cambios de hardware el personal de TI lo podrá realizarlo sin inconveniente.

4.4 Costo Mantenimiento Plataforma Nagios

El costo de mantenimiento de la plataforma se realiza dependiendo de los requerimientos indicados por el personal a cargo, en este caso deberán ser personal que está involucrada al área de tecnología.

El personal que tendrá contacto en la plataforma debe tener un conocimiento previo del sistema operativo en el cual se encuentre instalado el sistema nagios también debe conocer los archivos y parámetros de configuración, por tal motivo el costo será por horas por un monto aproximado de 60,00\$ hora, dando un total de 2374,40\$





















Tabla 7. Precios Mantenimiento e Implementación









Tiempo	P. Mantenimiento	P. Implementación	Precio Total
1 H	30,00\$ Trimestral		120,00\$
40 H		50,00\$	2000,00\$
			Sub Total
			2120,00\$
			IVA:12%
			TOTAL: 2374,40\$

4.5 Tiempo puesto operativo sistema Nagios

Una vez obtenido todos los implementos necesarios y el conocimiento adecuado, el tiempo de duración en la implementación del sistema llevara de tres a cuatro meses con las siguientes fases las cuales se detallaran a continuación:

Tabla 8. Tiempos de preparación, ejecución e instalación del NAGIOS

Id		Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1			Descarga de sistema operativo linux	1 día?	vie 30/08/13	vie 30/08/13	
2			Grabación de DVD Bootable del SO	1 día	lun 02/09/13	lun 02/09/13	1
3			Proceso de instalación del sistema Linux	1 día?	mar 03/09/13	mar 03/09/13	2
4			Actualización de paquetes y librerías del servidor	1 día?	mié 04/09/13	mié 04/09/13	3
5			Instalación de servidor web con paquetes y librerías del sistema Nagios	1 día?	jue 05/09/13	jue 05/09/13	4
6			Recopilación de información del número de Agencias del Banco Procredit	1 día	vie 06/09/13	vie 06/09/13	5
7			Recopilación de información del direccionamiento IP de Agencias	1 día	lun 09/09/13	lun 09/09/13	6
8			Proceso de configuración de script en el modulo de switch/router	2 días	mié 05/02/14	jue 06/02/14	
9			Descarga de imágenes con simlogía de equipos	1 día	mar 10/09/13	mar 10/09/13	7
10			Recopilación de información de servidores a monitorear	1 día	mié 11/09/13	mié 11/09/13	9
11			Información de direccionamiento IP de servidores	1 día	jue 12/09/13	jue 12/09/13	10
12			Diseño de sistema de Monitorización Nagios	2 días	vie 13/09/13	lun 16/09/13	11
13			Proceso de configuración de script en el modulo de windows	2 días	mar 17/09/13	mié 18/09/13	12
14			Instalación de Agente NSClient++ en servidores	5 días	jue 19/09/13	mié 25/09/13	13
15			Investigación sobre formas de envío de correo con notificaciones del sistema Nagios	7 días	jue 26/09/13	vie 04/10/13	14
16			Proceso de instalación del MTA Postfix	1 día	lun 07/10/13	lun 07/10/13	15
17			Configuración de archivos de Postfix	3 días	mar 08/10/13	jue 10/10/13	16
18			Permisos en firewall para protocolo smtp	9 días	vie 11/10/13	mié 23/10/13	17

19		Configuración de direcciones de correo en el módulo de contacts del sistema Nagios	4 días	jue 24/10/13	mar 29/10/13	18
20		Pruebas de funcionalidad de envío de correo	4 días	mié 30/10/13	lun 04/11/13	19
21	 	Investigación sobre métodos y programas para envío de mensajes cortos SMS	1 día	mar 05/11/13	mié 13/11/13	20
22	 	Compra de equipo GSM	8 días	jue 14/11/13	lun 25/11/13	21
23		Pruebas de funcionalidad de SMS	4 días	mar 26/11/13	vie 29/11/13	22
24		Pruebas de funcionalidad de todos los módulos y sistemas integrados	10 días	lun 02/12/13	vie 13/12/13	23

5. Conclusiones y Recomendaciones

5.1 Conclusiones

- Tener una red monitoreada hoy en día se ha convertido en una de las tareas más importantes y primordiales para empresas que trabajan con redes de datos, VoZIP, Video conferencia, etc., la monitorización es uno de los avances tecnológicos que permite tener y mantener una red con alta disponibilidad, estable y eficiente para el avance económico y productivo de una empresa en general.
- El desarrollo y la implementación del sistema de monitoreo Nagios se encuentra bajo la plataforma GNU/Linux con distribución Ubuntu Server 12.04 LTS por ser un sistema estable y estar orientado al ambiente servidor.
- El sistema de monitoreo Nagios es uno de los más completos y lo mejor de todo es un *software* gratuito y libre, lo que le convierte en un sistema robusto ideal para ser implementado en cualquier empresa como herramienta de gestión de red.
- Nagios es un sistema que todo administrador de servicios red y/o sistemas debería conocer pues es una de las alternativas para productos excesivamente costosos, es un sistema probado por miles de compañías a nivel mundial, escalable, robusto, etc., y lo más importante es que permite el ahorro en licencias de *software* para las empresas.
- Nagios es una poderosa herramienta de monitoreo la cual proporciona una gran cantidad de información tanto en sus archivo de *log* como en cada uno de sus módulos, permitiéndole al

administrador identificar de manera rápida y oportuna los problemas presentados dentro de la red.

- El sistema se desarrolló en base a las necesidades y los requerimientos solicitados por el administrador de red, el cual cubre la monitorización de los servicios de servidores, disponibilidad de los equipos, enlaces de comunicación con agencias.
- Una de las funcionalidades más relevantes del sistema de monitoreo son los envíos de mensajes de alertas o notificaciones mediante SMS y correo electrónico, estas funcionalidades permitirá alertar al personal de TI sobre algún comportamiento o anomalía suscitada con los diferentes componentes activos de red.
- Mediante las notificaciones enviadas por el sistema el personal de TI, tendrán la posibilidad de realizar las debidas correcciones de manera que los problemas puedan ser resueltos en el menor tiempo posible.
- Las notificaciones mediante SMS generada por el sistema de monitoreo depende de la ubicación del equipo y de las características técnicas que posea así como también del tráfico de la red GSM, estos factores impactaran en el nivel de señal que reciba el modem y como consecuencia la demora en la recepción del mensaje.

5.2 Recomendaciones

- Debido a que el sistema de monitoreo se encuentra instalado en ambiente GNU/Linux y este a su vez no tiene instalado una interfaz gráfica es de vital importancia realizar la instalación del protocolo *ssh* para tener acceso remoto a los archivos y directorios del sistema.
- Dentro de los ambientes GNU/Linux se recomienda no hacer uso del usuario *root* por personas que no posean el conocimiento necesario del sistema, debido a que si lo hacen uso tendrá todos los privilegios y accidentalmente podrán modificar o eliminar archivos de configuración ocasionando fallas perjudiciales.
- Cuando se trabaja con ambientes GNU/Linux puede aparecer errores al momento de ejecutar comandos, por tal motivo se recomienda hacer uso del comando *man* para obtener mayor información y ayuda.
- Es recomendable la revisión de los *log* generados por el sistema, ya que la información proporcionada por el sistema ayudara en gran medida al personal de TI mitigar y solventar errores presentados en los equipos.
- Se recomienda tener mucho cuidado con los archivos de configuración de los módulos de equipos Windows, *Switch* y *Router's*, debido a que si en algún momento deseen ingresar otro componente de red a ser monitorizado este deberá ser ubicado dentro de la descripción correcta del equipo como en el grupo con el nombre correcto.

- Para la instalación del agente en equipos con sistema operativo Windows se deberá verificar las características, es decir ver si el sistema es de 32 *bits* o de 64 *bits*.
- Se recomienda realizar un backup de todo el sistema nagios debido a que en un futuro puedan haber fallos en el disco duro o como también realizar un snapshot de todo el sistema operativo así se evitaría la pérdida parcial o total del sistema.
- También es recomendable tener el servidor de monitoreo conectado a las tomas eléctricas del ups, porque si existe un corte eléctrico, el sistema no sufra un apagado total y deje de realizar el monitoreo y el envío de las alertas de fallos en los componentes red.
- Como última recomendación es la colocación de una tarjeta de red adicional por razones de mantener al servidor con conexión redundante debido a que si la tarjeta principal falla, la segunda entra en funcionamiento sin perder la disponibilidad del sistema.

Referencias

- Fedora Project (Guía de usuario p.11.2.2), Recuperado el 14 de diciembre de 2013 de http://nagios.sourceforge.net/docs/3_0/quickstart.html
- Montoro, A. (2011), Recuperado el 14 de noviembre de 2013 de ebooks.google.com.ec/books?isbn=8493831255
- Moran, A. (2009), Recuperado el 3 de Diciembre de 2013 de <http://gsync.es/~mortuno/lagsr/editores.pdf>
- Nagios Enterprise (2011, pp.1-3), Recuperado el 17 de noviembre de 2014 de http://assets.nagios.com/downloads/nagioscore/docs/Installing_Nagios_Core_From_Source.pdf,
 Recuperado el 13 de noviembre de 2013 de <http://histinf.blogs.upv.es/2011/12/23/historia-de-linux/>
- Recuperado el 18 de noviembre de 2013 de <http://www.nagios.org/about/history>
- Rivas, J. (2009), Recuperado el 20 de noviembre de 2013 de <http://www.nagios.org/projects/nagioscore/history/core-3x>
- Recuperado el 10 de diciembre de 2013 de http://docs.fedoraproject.org/es-ES/Fedora/14/html/User_Guide/sect-User_Guide-Office_Applications-Word_Processing.html
- Recuperado el 16 de diciembre de 2013 de <http://library.nagios.com/>
- Recuperado el 20 de diciembre de 2014 de <http://library.nagios.com/library/products/nagioscore/manuals/>
- Recuperado el 7 de enero de 2014 de http://nagios.sourceforge.net/docs/3_0/monitoring-windows.html
- Recuperado el 14 de enero de 2014 de http://nagios.sourceforge.net/docs/3_0/monitoring-routers.html
- Recuperado el 21 de enero de 2014 de http://nagios.sourceforge.net/docs/3_0/monitoring-publicservices.html
- Recuperado el 28 de enero de 2014 de http://nagios.sourceforge.net/docs/3_0/monitoring-linux.html
- Recuperado el 5 de febrero de 2014 de <http://definicion.de/red/>

Recuperado el 10 de febrero de 2014 de <http://unesr-grupo4-internet-extranet.blogspot.com/2011/01/definicion-de-internet-y-intranet.html>

Recuperado el 26 de febrero de 2014 de <http://www.sms-integration.com/>

Toranzo, F. (2010), Recuperado el 18 de noviembre de 2013 de http://www.forpas.us.es/aula/hardware/dia4_redes.pdf

Universidad Rey Juan Carlos (2013) Editor de texto vs Procesador de palabras 6 (17-31). Madrid, España.

Universidad San Francisco de Quito (2013) Academia de Linux Red Hat (RHA 030). Quito, Ecuador.

ANEXOS

ANEXO 1. CERTIFICADO DEL BANCO PROCREDIT S.A.



Banco ProCredit

Ecuador

CERTIFICADO

A quien corresponda.

Mediante el presente certificado, quien suscribe Edison Tito Lucero, en calidad de Jefe del Área de Infraestructura del Banco Procredit S.A, empresa que se encuentra ubicada en la Avenida Amazonas y Av. Atahualpa Esquina, CERTIFICO que la señor MADRIL ACURIO PAÚL VINICIO, con Cédula de Identidad N° 050316125-9, ha realizado su correspondiente trabajo de titulación en la empresa a la cual represento

Siendo los 21 días del mes de Febrero del 2013, firmo dando conformidad a lo expuesto anteriormente.

Atentamente

Banco ProCredit S.A.

Edison Tito

Edison Tito

**Jefe de Infraestructura
BANCO PROCREDIT S.A.**

ANEXO 2. AUSPICIO DEL PROYECTO DE TITULACIÓN



Banco ProCredit

Ecuador

Quito, 21 de febrero de 2014

Señor Ingeniero

Julio Freire

**Coordinador de la Carrera de Ingeniería en Redes y Telecomunicaciones
Universidad de las Américas**

Presente.

De nuestra consideración

Por medio de la presente, queremos comunicar a su distinguida institución educativa nuestro compromiso de auspiciar el proyecto de trabajo de titulación del señor: MADRIL ACURIO PAÚL VINICIO; que consiste en el Diseño e Implementación de un sistema de monitoreo de red y mensajes de alerta basado en la plataforma NAGIOS, bajo las siguiente condiciones:

- Nuestra empresa se compromete a proveer los dispositivos y materiales que constituirán el sistema de monitoreo y facilitara los trabajos de estudio de funcionamiento, instalación y pruebas de nuestras instalaciones.
- La propiedad intelectual del software y el diseño del sistema será de la Universidad de las Américas , sin embargo Banco Procredit S.A., en su calidad de auspiciante y propietario del equipo en el que se realizara la implementación, tiene el derecho de realizar en el futuro las modificaciones y ampliaciones que considere convenientes.
- La información que se entregue será clasificada por la empresa y podrá ser divulgada solo con autorización expresa de nuestra parte.

Atentamente

Banco ProCredit S.A.

Edison Tito
Edison Tito

Jefe de Infraestructura

BANCO PROCREDIT S.A.

ANEXO 3. Problema critico de servidor srvvmsep

srvvmsep
(srvvmsep)

Member of
No servicegroups.

172.22.4.54


Service State Information

Current Status:	CRITICAL (for 31d 23h 31m 18s)
Status Information:	c: - total: 99.90 Gb - used: 94.23 Gb (94%) - free 5.67 Gb (6%)
Performance Data:	"c:\ Used Space"=94.23Gb;79.92;89.91;0.00;99.90
Current Attempt:	3/3 (HARD state)
Last Check Time:	02-14-2014 17:15:23
Check Type:	ACTIVE
Check Latency / Duration:	0.220 / 0.007 seconds
Next Scheduled Check:	02-14-2014 17:25:23
Last State Change:	01-13-2014 17:45:00
Last Notification:	02-14-2014 16:45:28 (notification 7 14)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	02-14-2014 17:16:08 (0d 0h 0m 10s ago)


Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

ANEXO 4. Notificación Nagios

**** PROBLEM Service Alert: srvvmsep/C:\ Drive Space is CRITICAL ****

 nagiosprocredit@gmail.com

Enviado: viernes 14/02/2014 16:45

Para:  Paul Vinicio Madril Acurio

***** Nagios *****

Notification Type: PROBLEM

Service: C:\ Drive Space
Host: srvvmsep
Address: 172.22.4.54
State: CRITICAL

Date/Time: Fri Feb 14 16:45:28 ECT 2014

Additional Info:

c:\ - total: 99.90 Gb - used: 94.22 Gb (94%) - free 5.68 Gb (6%)

ANEXO 5. Problema servidor srvmsep

Service State Information

Current Status:	WARNING (for 31d 23h 46m 32s)
Status Information:	c: - total: 44.90 Gb - used: 38.82 Gb (86%) - free 6.08 Gb (14%)
Performance Data:	'c:\ Used Space'=38.82Gb;35.92;40.41;0.00;44.90
Current Attempt:	3/3 (HARD state)
Last Check Time:	02-14-2014 17:12:34
Check Type:	ACTIVE
Check Latency / Duration:	0.018 / 0.008 seconds
Next Scheduled Check:	02-14-2014 17:22:34
Last State Change:	01-13-2014 17:35:21
Last Notification:	02-14-2014 16:42:38 (notification 716)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	02-14-2014 17:21:48 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

ANEXO 6. Notificación Nagios

**** PROBLEM Service Alert: srvmsep/ C:\ Drive Space is WARNING ****

nagiosprocredit@gmail.com

Enviado: viernes 14/02/2014 16:43

Para: Paul Vinicio Madrid Acurio

***** Nagios *****

Notification Type: PROBLEM

Service: C:\ Drive Space
Host: srvmsep/ atm
Address: 172.22.4.38
State: WARNING

Date/Time: Fri Feb 14 16:42:38 ECT 2014

Additional Info:

c:\ - total: 44.90 Gb - used: 38.82 Gb (86%) - free 6.08 Gb (14%)

ANEXO 7. Equipos para envío de mensajes SMS



ANEXO 8. Ingreso de tarjeta SIM



ANEXO 9. Conexión de modem a CPU



ANEXO 10. Notificación de SMS a celular

```
***** Nagios *****  
  
Notification Type: RECOVERY  
Host: SW-SLDO  
State: UP  
Address: 10.0.45.2  
Info: PING OK - Packet loss = 16%, RTA = 23.80  
ms  
  
Date/Time: Fri Feb 14 08:22:21 ECT 2014
```

```
***** Nagios *****  
  
Notification Type: PROBLEM  
  
Service: C:\ Drive Space  
Host: srvvmsepatm  
Address: 172.22.4.38  
State: WARNING  
  
Date/Time: Fri Feb 14 08:32:41 ECT 2014  
  
Additional Info:  
  
c:\ - total: 44.90 Gb - used: 38.82 Gb (86%) - free  
6.08 Gb (14%)
```

ANEXO 11. Diagrama de conectividad de red física enlaces wan e internet

