



**UNIVERSIDAD DE GUAYAQUIL**  
**Facultad de Ciencias Matemáticas y Físicas**  
**Carrera de Ingeniería en Sistemas**  
**Computacionales**

“Monitor de Red Seguro”

**PROYECTO DE TESIS DE GRADO**  
CURSO DE GRADUACIÓN

**Previo a la Obtención del Título de:**  
  
**INGENIERO EN SISTEMAS COMPUTACIONALES**

Autores:  
Camatón Zambrano Emma Geanina  
Flores Avelino Erik Alberto  
Mendoza Jácome Adela María

GUAYAQUIL-ECUADOR

Año: 2007

## **AGRADECIMIENTO**

Quiero agradecer a Dios por haberme permitido hacer de este sueño, una hermosa realidad, a la Universidad de Guayaquil, por todos los conocimientos adquiridos dentro de esta noble institución, a mis padres pilares de mi existencia por su apoyo incondicional desde el inicio de esta gran meta y a mis compañeros por sus conocimientos e inolvidables momentos de alegría, siempre los recordare.

Geanina Camatòn

Agradezco en primer lugar a Dios por todo lo que me ha dado, a mis padres por el esfuerzo y apoyo durante todo estos años de estudios y a mi grupo de tesis por los conocimientos compartidos.

Adela Mendoza

Ser agradecido es una virtud que pocos poseen. Por eso quiero dar las gracias primero a Dios que nos dio la fortaleza para seguir adelante, a mis padres por su apoyo incondicional, y en especial a mis compañeras de grupo de tesis por su gran aporte y por su paciencia.

Erik Flores A.

## DEDICATORIA

Quiero dedicar esta obra a mis padres Vitalia Zambrano V. y Jaime Camatòn B. fuente de mi inspiración constante y a quienes dedico mi mejor esfuerzo y mi mayor superación y a mi hermano Danny por su comprensión y colaboración incondicional

Geanina Camatòn

Dedico este trabajo a Dios por todas las oportunidades que me ha brindado, a mis padres en especial por todo su apoyo y a aquellas personas que hicieron que el transcurrir de todos estos años de estudios se convirtieran en un conjunto de sentimientos de alegrías y penas, que al culminar esta etapa de mi vida, me hicieran añorar el regresar a esos días que no volverán y poder vivir plenamente cada momento que pase.

Adela Mendoza.

Este trabajo esta dedicado a todas aquellas personas que en su momento nos dieron todo su apoyo y nos brindaron las facilidades para que cumplamos con este objetivo comun. Y dedicado a mis compañeras de grupo de tesis por su constante colaboración y apoyo.

Erik Flores A.

## **TRIBUNAL DE GRADUACIÓN**

---

Ing.  
Presidente del Tribunal

---

Ing.  
Primer Vocal

---

Ing.  
Segunda Vocal

---

Ing.  
Secretario

## **DECLARACION EXPRESA**

“La autoría de la tesis de grado corresponde exclusivamente a los suscritos, perteneciendo a la Universidad de Guayaquil los derechos que generen la aplicación de la misma”

(Reglamento de Graduación de la Carrera de Ingeniería en Sistemas Computacionales, Art.26).

---

CAMATON ZAMBRANO EMMA

---

FLORES AVELINO ERIK

---

MENDOZA JACOME ADELA

## **RESUMEN**

El Monitor de Red Seguro es una herramienta que fue desarrollada para que supervise los diferentes nodos conectados a la Red. En caso de fallos, esta aplicación alertará al administrador de la red mediante una ventana de aviso, ayudando de esta forma a proteger los equipos y datos, reduciendo la probabilidad de los fallos de la red que podrían ser costosos. Además de permitir guardar y revisar los reportes que se generen. Esta aplicación utiliza la arquitectura Cliente /Servidor, MySQL como base de datos, el Apache Tomcat como servidor Web y Java 1.5 como lenguaje de programación. Para utilizar esta aplicación deberá ingresar un usuario y password a través del browser conectado a la Intranet, permitiendo así consultar información en tiempo real, proporcionando una ayuda a la hora de realizar la selección de una máquina.

# CAPÍTULO 1

## 1. INTRODUCCIÓN

### 1.1 Antecedentes

En la actualidad, el manejo de la información constituye una de las principales preocupaciones de una organización. Las Empresas e Instituciones que cuentan con una red sea grande o pequeña deben garantizar la utilización de sus recursos, por lo que resulta necesario contar con herramientas que permitan conocer el estado de los nodos, aplicaciones de una red y cualquier información que me permita optimizar recursos y mejorar los servicios.

Teniendo los siguientes antecedentes, se decidió crear una aplicación mediante un browser que me permita visualizar, controlar y recopilar lo que sucede en cada uno de los nodos que pertenecen a una misma Red en tiempo como los recursos de software: aplicaciones, sistemas operativos, ip , etc. y la actividad de los servicios que cada uno utiliza.

Los factores que intervienen o que influyen en el tráfico de red son:

- El sistema operativo que tiene cada Pc
- Las aplicaciones que tienen instaladas
- El nombre del usuario
- Memoria utilizada

## **1.2 Problemática**

El gran crecimiento de las redes al igual que las aplicaciones de redes distribuidas, como la comunicación de datos se ha convertido en parte fundamental del desarrollo tecnológico, nos hemos visto en la necesidad de obtener de un modo rápido la información actualizada y precisa de cada uno de los nodos de la red.

## **1.3 Solución**

Para tener un control visual de lo que ocurre en la red se decidió realizar un MONITOR DE RED SEGURO el mismo que me permite visualizar la información más importante que genera el tráfico de red de cada uno de los nodos que se encuentren conectados a esta red y así evitar el mal uso de recursos (tiempo, red, etc...) por parte de los usuarios que usan la red, permitiendo además al administrador tomar decisiones y resolver problemas referentes al tráfico de red obteniendo así una red eficiente.



El Monitor de Red a implementarse es un software que podrá se utilizado en:

- Cyber
- Universidades
- Así, como Instituciones o Empresas que cuenten con una red LAN.

La aplicación ayudara a medir la utilización de los recursos de la red, además de guardar esta información para así obtener posteriormente reportes del monitoreo del tráfico de la Red.

## **1.4 Misión y Vision**

### **1.4.1 Misión**

Por medio de nuestro proyecto obtenemos información relevante para el control y visualización de lo que ocurre en la red y no solo se limita a esto sino que también protege los datos que llegan hacia el visualizador (MONITOR DE RED).

Es una aplicación que funciona en redes de área local (LAN), mostrando el tráfico que genere la red, es decir permite observar si esta activa o inactiva algún dispositivo.

### **1.4.2 Visión**

Este proyecto va dirigido para que en cada una de las empresas e instituciones que posean una red posean un monitor de red que permita a estas controlar y visualizar a través de una sola aplicación toda la red.

## **1.5 Objetivos del Proyecto**

### **1.5.1 Objetivos Generales**

Se implementará un software encargado de monitorear la red, los dispositivos conectados a ella, así como un visualizador que mostrara la información referente a cada computador conectado, nombres de usuarios, sistema operativo, estado, etc.

### **1.5.2 Objetivos Específicos**

- Implementar un software el cual se ejecutara en el servidor para ver el estado general de todas las PC`s de la red, tales como IP's, sistema operativo con el que están trabajando, estado (online /offline).
- Supervisar individualmente a cada uno de los nodos especificando los aplicaciones instaladas, servicios iniciados, dispositivos lógicos, etc.

- Generar reportes y almacenar en una bitácora todos los eventos tanto normales y no habituales al tráfico que genere la red.
- Desplegar una ventana de alerta indicando el numero de IP y nombre del computador cuando este abandona la red, así mismo indica si hay fallos o conexiones de otros dispositivos dentro de nuestra red.
- Generar reportes estadísticos del tráfico que genere la red.

### **1.6 Alcance del Proyecto**

- Desarrollar un software en Java que realice las funciones de un vizualizador de la red con protocolo SNMP.
- Generar un archivo que guarde un registro con toda la información de los dispositivos que el monitor encuentre activos en la red cada vez que este se ejecute.
- La supervisión de los nodos se va a implementar mediante una interfaz grafica general, donde se muestran todas los dispositivos en la red.
- La visualización de los nodos se podrá realizar de manera individual, pudiendo mostrar en una pantalla adicional la información de un nodo específico.

- Enviar un mail se surge algún problema al administrador, así como al usuario de la PC involucrada
- La información presentada de cada nodo será: sistema operativo, aplicaciones instaladas, servicios iniciados, dispositivos conectados, estado, nombre de usuario, memoria utilizada, capacidad del disco.
- Asegurarnos que toda la información proporcionada por el protocolo SNMP sea encriptada para evitar el mal uso de ella mediante algún protocolo de seguridad.
- Será parametrizable el tiempo de actualización del monitor de red, cada que tiempo va ha monitorear la red.

### **1.7 Beneficios del Proyecto**

Esta aplicación nos proporciona de una manera rápida lo que esta sucediendo en la red con los diferentes nodos. Permitiendo así controlar y visualizar los datos que se encuentra en el tráfico de toda la red.

### **1.8 Cronograma**

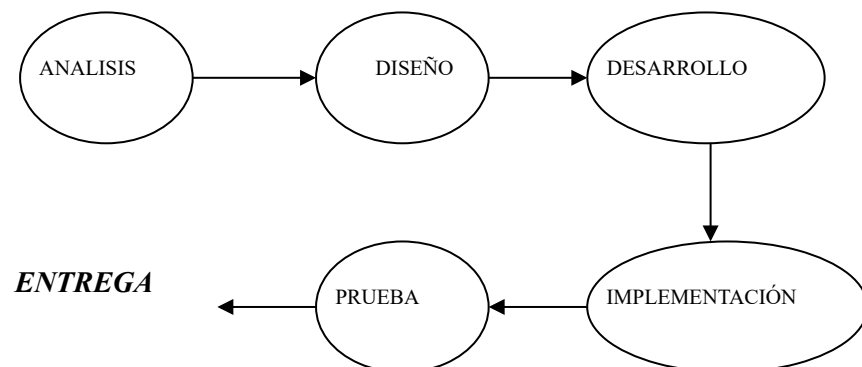
El cronograma se encontrará en el Anexo, en el cual se indicará el proceso de la elaboración del sistema a desarrollar.

## 1.9 Metodología

### 1.9.1 Modelo Secuencial

Este es un enfoque sistemático, secuencial de desarrollo del software que comienza en un nivel de sistemas y progresa con el análisis, diseño, codificación, pruebas y mantenimientos.

Es el adecuado para el desarrollo de esta aplicación debido a factores como el tiempo y recursos.



**Fig. 1.9.1**

## 1.10 Estudio de Viabilidad

El estudio que se realizará me indicará el funcionamiento, los alcances y los beneficios que me brindará este sistema.

El visualizador del Monitor de Red es el encargado de proporcionar la información al administrador de la red sobre el tráfico de la red o de una computadora específica conectada a la red, para así la persona encargada pueda verificar el estado y comportamiento de la red.

El Monitor de Red es un complemento para el encargado de administrar la red, a lo que se refiere a Sistemas o Plataformas de Gestión de Red. Debido a que el trabajo del administrador consiste en mantener el funcionamiento de los recursos que conforman la red, tanto Hardware como Software.

Un administrador de Red necesita monitorear la Red por las siguientes causas:

- Detectar los cuellos de botella.
- Resolver problemas con el cableado.
- Capacidad de los Disco cada Pc.
- Programas instalados en cada nodo.

Para el desarrollo de este sistema, se necesitaría un mínimo de tres computadoras con diversos sistemas operativos (LINUX y WINDOWS), en dos de los Pc's se instalará el agente SNMP trabajando como clientes y la tercera funcionará como servidor el cual se convertirá en un visualizador de toda la información (la más importante) que los dos primeros proporcionen (agentes SNMP).

El servidor funcionara en LINUX con FEDORA CORE 4, una de las funciones principales es organizar el tiempo que tiene el microprocesador para atender a cada uno de los procesos dependiendo de su prioridad, además de receptar toda la información y organizarla para visualizarla en pantalla. Este sistema operativo debe tener configurado el protocolo MRTG el cual me permitirá ver gráficamente las Pc que se están monitoreando. Además debe tener configurado lo siguiente:

- jakarta-tomcat-5.5.9.tar
- jakarta-tomcat-connectors-jk2-2.0.4-src.tar
- Apache
- Mysql-4.1.11-2.i386.rpm
- Sendmail
- DNS

Toda la información se almacenará en una Base de Datos (MYSQL), para posteriormente poder generar los reportes de todo el tráfico que ha sido generado en las fechas anteriores.

El cliente, representa todos los nodos de la red, en él se ejecutara constantemente una aplicación que obtendrá información como: número de IP, nombre de la máquina, usuario, estado on-line/off-line y toda la información existente (necesaria) de él, luego de recolectar todos estos datos se los enviará por el protocolo SNMP que es el encargado de enviar la información al Server para mostrada en el visualizador.

Este sistema nos dará la información en tiempo real de cada uno de los clientes (nodos) al momento de solicitarla. Así mismo indicará mediante alertas alguna situación anormal, teniendo así una red eficiente y accesible.



## **CAPÍTULO 2**

### **2. ANALISIS**

En este capitulo se lleva a acabo la fase de análisis del Sistema de Monitor de Red, como es la especificación de requerimientos, para ir desarrollando de forma gradual el sistema a desarrollar.

#### **2.1 Levantamiento de la Información**

Este proceso se lleva a cabo por medio de entrevistas y revisión de documentos. Referente a las entrevista, estas se realizaron con personal que tiene de alguna forma relación con los procesos de administración de redes.

Además se realizo investigaciones de aquellas aplicaciones, protocolos, puertos, etc., que son utilizadas para el monitoreo de una red.

Conociendo las necesidades del clientes, para mejorar la productividad y disminuir la vulnerabilidad de la Red.

### 2.1.1 Resultados de las entrevistas

A continuación detallaremos cada una de las diferentes respuestas que se obtuvo de las entrevistas realizadas.

1. Cuenta su empresa con algún sistema de monitoreo de red?

- a) Si 40 %
- b) No 60%

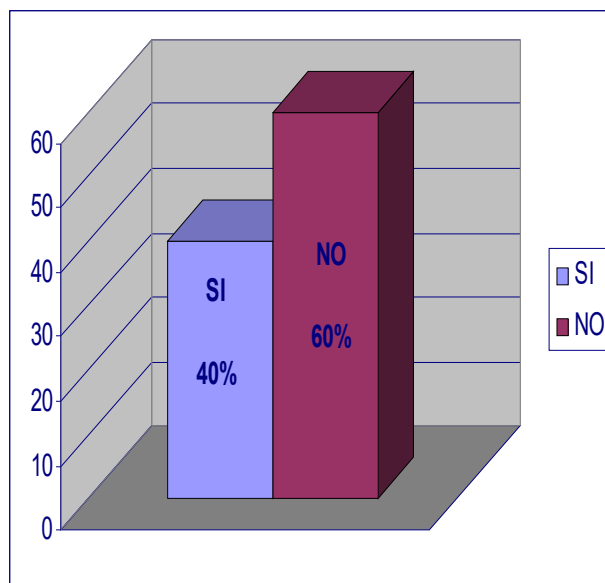


Fig. 2.1.1

2. Con que frecuencia los usuarios reportan problemas en la red?

- a) Nunca 30%
- b) Medianamente 40%
- c) Siempre 30%

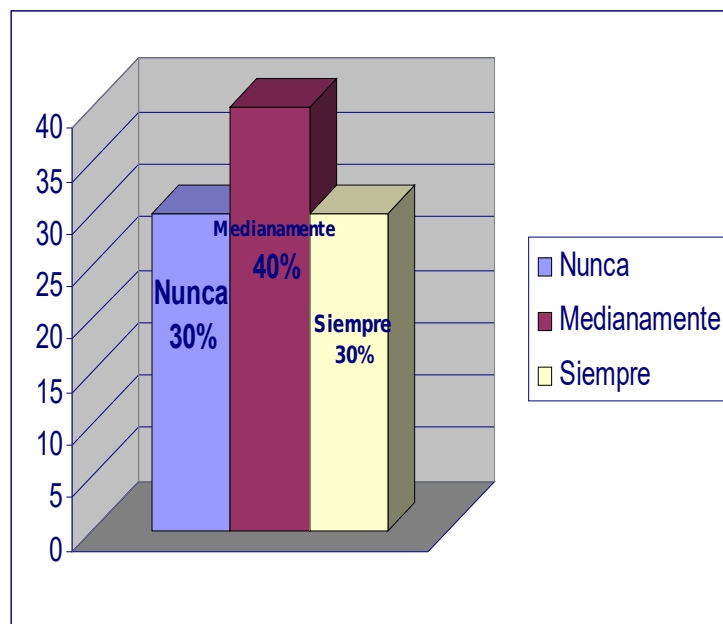


Fig. 2.1.1.2

3. Considera usted necesario que el administrador lleve el control de las Aplicaciones de la red?

- a) Si 80 %
- b) No 20%

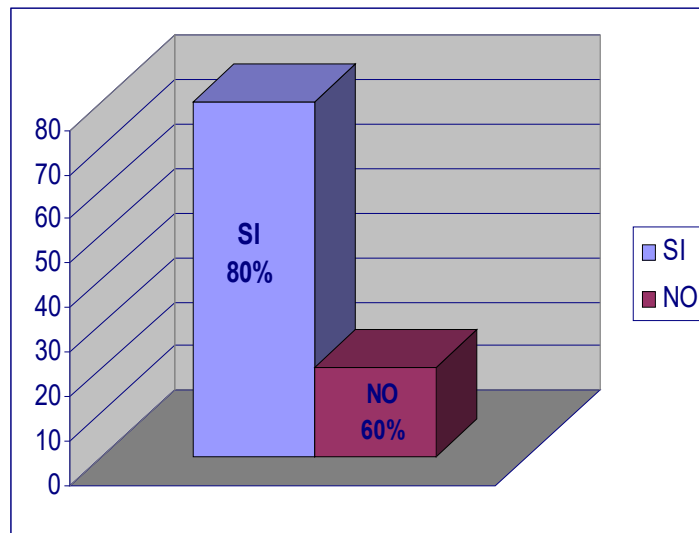


Fig. 2.1.1.3

4. Como considera el rendimiento de la red de su empresa?

- a) Bajo 30%
- b) Medio 30%
- c) Alto 40%

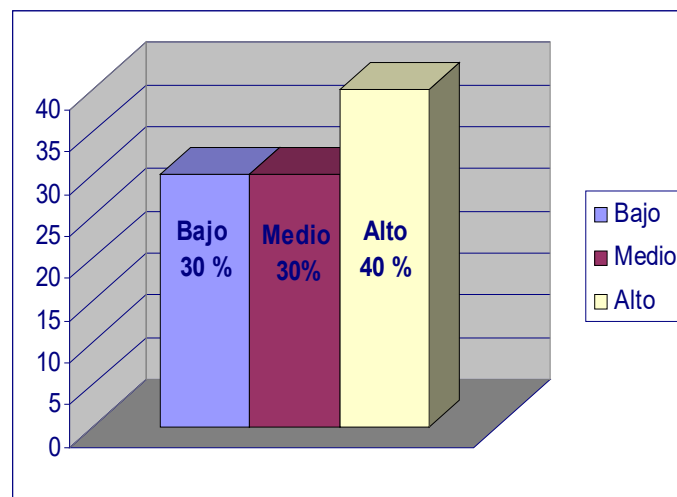


Fig. 2.1.1.4

5. Considera que una empresa cuente con un sistema de monitoreo de red?

- a) Si 80 %
- b) No 20 %

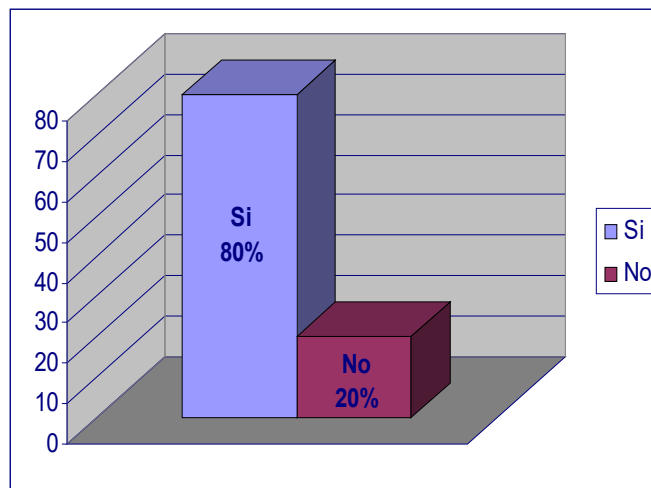


Fig. 2.1.1.5

## 2.2 Recursos

Para el desarrollo del proyecto

se hemos utilizado los recursos que se detallan a continuación:

### 2.2.1 Software

Para el desarrollo del proyecto se requieren los siguientes recursos de software:

- Windows XP
- Fedora Core 4 (Linux)
- VMware Workstation 5.5 (Maquina Virtual para Windows)
- Java (Herramienta de Desarrollo)
- Configuración de los agentes SNMP en Windows y Linux
- Configuración del MRTG (Multi Router Traffic Grapher)
- Servidor Tomcat 5.5.9
- Microsoft Project (Planificación Temporal del Proyecto)
- Base De Datos My SQL

### **2.2.2 Hardware**

Sistema Operativo	Procesador	Memoria RAM	Disco Duro	Monitor	Perifericos
Windows XP	Pentium IV 266Mhz	256 MB	80 GB	Mark Visio	mouse, teclado, unidad de CD-RW, UPS 1000v
Windows XP Profesional Service Pack 2y Windows 98	Pentium IV 2.8Mhz	512 MB	40 GB	Samsung 14"	Mouse óptico, teclado, unidad de CD-RW, UPS 1000v
Windows XP Profesional	Pentium IV 1.6Mhz	512 MB	40 GB	Samsung 17"	mouse, teclado, unidad de CD-R
Fedora 4-Linux	2.6 Mhz	512 MB	60 GB	Samsung 17"	mouse, teclado, unidad de CD-R

Tecnológico: Para el desarrollo del proyecto nos hemos provisto de los equipos con las siguientes características:

Además usamos otros Recursos:

- USB flash memorie <sup>Tabla 1</sup> 2 Mb)
- RED (LAN)

### **2.2.3 Humano**

El recurso humano que desarrolla el software “MONITOR DE RED SEGURO” son:

- Adela Mendoza Jácome
- Emma Camatón Zambrano
- Erik Flores Avelino

## **2.3 Costo**

Se realizará un análisis de los costos que implico en la realización del sistema denominado visualizador del Monitor de Red, el mismo que esta estimado en un valor aproximado de \$30, para lo cual se ha realizado un estudio con todos los recursos que se utilizaron tanto material como



egresos que tuvimos cada integrante del grupo para la realización del mismo, que a continuación detallamos:

<b>Insumos</b>			
Cuaderno			3
Lápiz			0,5
Rema	5		2,5
PenDrive	20		60
Cartucho color	35		35
Cartucho bn	20		20
Cd			10
			131
<b>* Para 8 meses</b>			
Sueldos	612		4896
Luz			8
Internet			50
Comunicación (teléfono)			20
Insumos			131
			5105

## 2.4 Estudio de Factibilidad

En el estudio de factibilidad para el Sistema de Monitor de Red, se basa en los siguientes aspectos: técnico, económico y operativo.

### 2.4.1 Análisis beneficio costo

#### 2.4.1.1 Factibilidad Técnica

Este proyecto es realizable desde este punto de vista, debido a que la Carrera cuenta con los laboratorios a disposición de los alumnos, ya que estos poseen la infraestructura para la implementación y prueba del sistema a desarrollar.

Además de la tecnología con la que cuenta el grupo que se encuentra desarrollando el sistemas, consideramos que es factible la realización del software.

#### **2.4.1.2 Factibilidad Económica**

El costo que se va ha considerar son el tiempo del equipo, como es el costo estimado del hardware, software y desarrolladores del sistema.

Para el desarrollo del sistema, el costo que genera es económicamente factible, debido a que los programas a utilizarse son de libre distribución.

#### **2.4.1.3 Factibilidad operacional**

Esta factibilidad esta dada por los recursos humanos disponibles para el desarrollo del software, la operación del sistema y el uso del mismo.

Este sistema esta calculado para proporcionar una interfaz eficiente y accesible

Para lo cual se calcula que el Sistema de Monitor de Red será utilizado en un 100%.

$$\text{Indicador} = \frac{\text{Factibilidad Técnica}}{\text{Factiibilidad Económica}} = \frac{100}{100}$$

## 2.5 Análisis de Requerimientos

Para el análisis de Requerimientos del sistema que se muestra se han seguido los pasos que se detallan a continuación:

- Obtener información acerca de lo que los usuarios desean.
- Clasificar los deseos de los usuario para comenzar a estructurar requerimientos
- Identificar los niveles de jerarquía del sistema y empezar a alojar los ya clasificados requerimientos en cada nivel.

- Especificar formalmente los requerimientos de acuerdo al nivel de audiencia que se desea.

Los requerimientos son el punto de acuerdo entre el cliente y el sistema a desarrollarse, este entendimiento es necesario para poder construir el sistema y satisfaga las necesidades de nuestro cliente.

Las necesidades y/o requerimientos del cliente evolucionan con el tiempo y cada cambio involucra un costo. Por eso es necesario tener documentada toda la información sobre la revisión o cambio que se le realice al sistema. Para así evaluar los costos y beneficios de acuerdo a los diversos cambios realizados.

### **2.5.1 Clases de requerimientos**

El clasificar requerimientos es una forma de organizarlos, hay requerimientos que por sus características no pueden ser tratados iguales. Por ejemplo, los requerimientos de entrenamiento de personal no son tratados de la misma manera que los requerimientos de una conexión a Internet.

A continuación se detalla los diferentes tipos de requerimientos del software:

#### **2.5.1.1 Requerimientos del entorno**

El entorno es todo lo que rodea al sistema. El sistema usa el entorno y lo necesita para que funcione.

El entorno que necesita este sistema es como mínimo 3 computadoras conectadas a Red con diversos sistemas operativos (Windows y Linux).

El tráfico generado por la red, será almacenado en una base de datos (My SQL), para realizar consultas futuras, es decir tener un historial de todo el tráfico generado por la red.

#### **2.5.1.2 Requerimientos "ergonómicos"**

El requerimiento ergonómico es la interfaz con el usuario o GUI (Graphic User Interface). Es decir, es la forma en que el ser humano interactúa con el sistema, se cuenta con un software fácil de manejar y de interactuar entre páginas y amigable para el usuario.

### **2.5.1.3 Requerimientos funcionales**

Estos requerimientos al tiempo que avanza el proyecto de software son los algoritmos, la lógica y gran parte del código del sistema.

### **2.5.1.4 Requerimientos del Desempeño**

El requerimiento de desempeño nos informan las características de debe de tener el sistema, como es: ¿Que tan rápido?, ¿Cuántos recursos?.

Este tipo de requerimientos es de especial importancia en los sistemas de tiempo real en donde el desempeño de un sistema es tan crítico como su funcionamiento.

### **2.5.1.5 Disponibilidad**

Este tipo de requerimientos se refiere a la durabilidad, degradación, flexibilidad, contabilidad y capacidad de actualización. Este tipo de requerimientos es también muy importante en sistemas de tiempo real puesto que estos

sistemas manejan aplicaciones críticas que no deben de estar fuera de servicio por periodos prolongados de tiempo, como son los pedidos en línea del sistema que se está detallando.

#### **2.5.1.6 Requerimientos de Materiales**

Aquí se especifica en que medio se entregara el sistema y como esta empaquetado. Es importante para definir los costos de industrialización del sistema.

Se han seguido las siguientes actividades técnicas para poder realizar el análisis de requerimientos

#### **Actividades técnicas**

1. Identificar Casos de Uso del sistema
2. Dar detalle a los casos de uso descritos
3. Definir una interfaz inicial del sistema (si es aplicable)

## **2.6 Sistema Operativo (LINUX)**

El sistema operativo LINUX tiene características muy especiales que lo diferencian de los demás sistemas operativos, ya que es libre, es decir que no se debe pagar ninguna licencia por el uso del mismo, viene acompañado del código fuente. El [sistema](#) lo forman el núcleo del [sistema](#) (kernel) mas un gran numero de [programas](#) / librerías que hacen posible su utilización.

Características de Linux:

- Multitarea: varios programas ejecutándose al mismo [tiempo](#).
- Multiusuario: varios usuarios en la misma máquina al mismo [tiempo](#) (y sin licencias para todos).
- Multiplataforma: corre en muchas CPU's distintas, no sólo Intel.
- Funciona en modo protegido 386.
- Tiene protección de [la memoria](#) entre [procesos](#), de manera que uno de ellos no pueda colgar el sistema.
- Carga de ejecutables por [demanda](#): Linux sólo lee de disco aquellas partes de un [programa](#) que están siendo usadas actualmente

## **2.7 SNMP (Simple Network Managenet Protocol)**

El protocolo SNMP fue diseñado en los años 80, su principal objetivo fue el integrar la gestión de diferentes tipos de redes mediante un diseño sencillo que produjera poca sobrecarga en la red.



El Protocolo Simple de Gestión de Red (SNMP), es el encargado de intercambiar información en la red a través del protocolo UDP que envía y transforma el mensaje en un datagrama por medio del puerto 161.

El SNMP se basa en un conglomerado de agentes. Cada agente es un elemento de la red que ofrece unas determinadas variables al exterior, para ser leídas o modificadas.

El protocolo SNMP esta compuesto por dos elementos: el agente y el gestor.

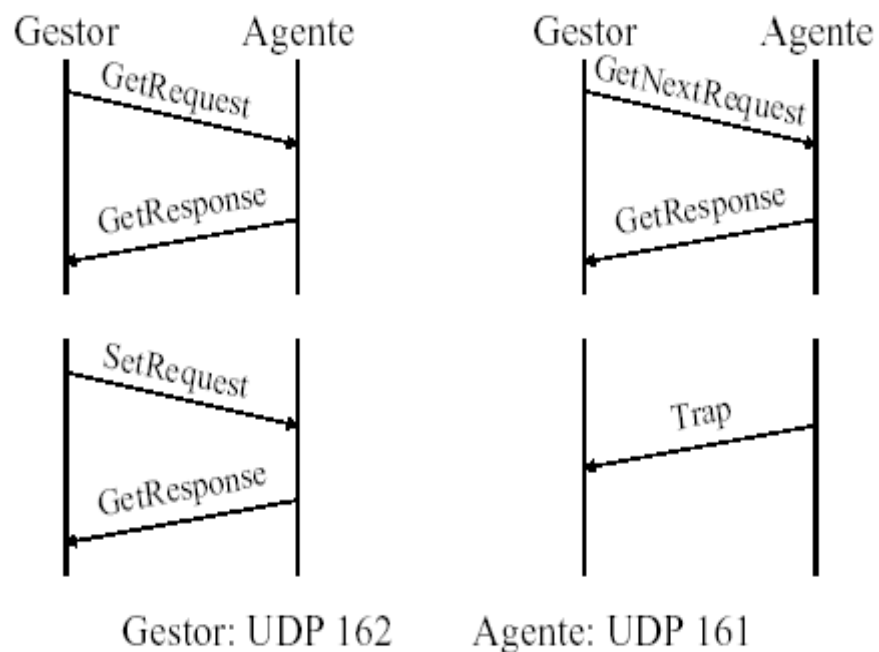


Fig. 2.7

- El gestor toma las decisiones de gestión

- El agente realiza localmente las acciones solicitadas por el gestor sobre un conjunto de objetos locales (MIB) que mantienen fundamentalmente información de estado

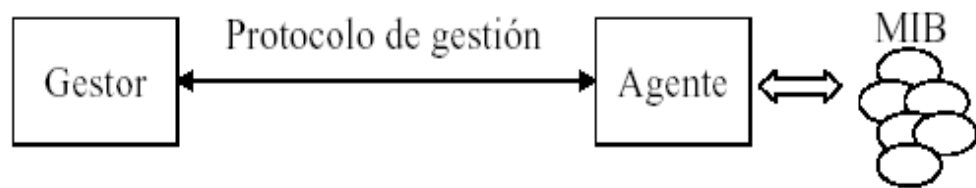


Fig. 2.7.1

SNMP tiene cinco modos de mensajes que se usan entre los Agentes y el Administrador son los siguientes:

- Get Request

Una petición del Administrador al Agente para que envíe los valores contenidos en el MIB (base de datos).

- Get Next Request

Una petición del Administrador al Agente para que envíe los valores contenidos en el MIB referente al objeto siguiente al especificado anteriormente.

- Get Response

La respuesta del Agente a la petición de información lanzada por el Administrador.

- Set Request

Una petición del Administrador al Agente para que cambie el valor contenido en el MIB referente a un determinado objeto.

- Trap

Un mensaje espontáneo enviado por el Agente al Administrador, al detectar una condición predeterminada, como es la conexión/desconexión de una estación o una alarma.

El protocolo de gestión SNMP facilita, pues, de una manera simple y flexible el intercambio de información en forma estructurada y efectiva, proporcionando significantes beneficios para la gestión de redes, aunque necesita de otras aplicaciones en el NMS que complementen sus funciones y que los dispositivos tengan un software Agente funcionando en todo momento.

### **2.7.1 Arquitectura del SNMP**

Utiliza una arquitectura cliente – servidor, en la cual el agente desempeña el papel del servidor y el gestor hace del cliente.

La arquitectura SNMP consta de los siguientes componentes:

- Gestores (NMS's)
- Agentes (nodos administrados)
- MIB (base de datos con información)

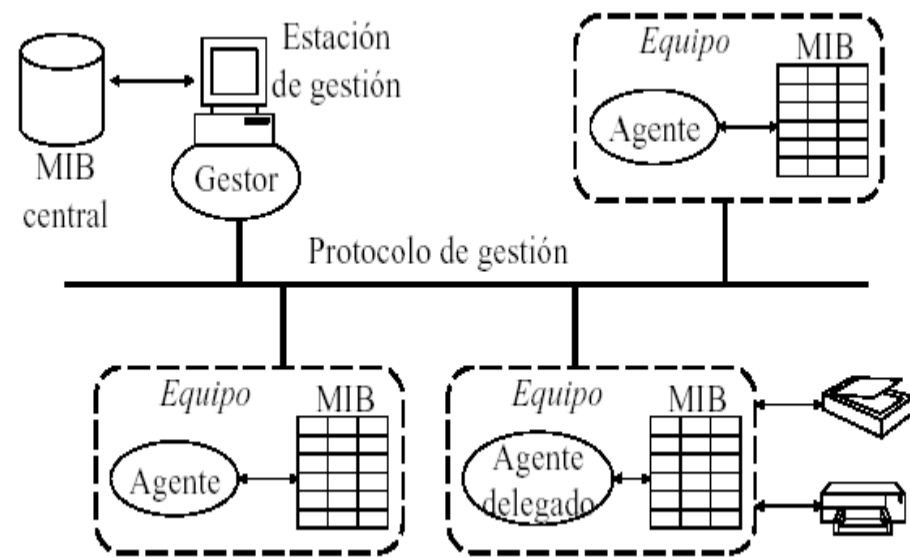


Fig. 2.7.1

### 2.7.2 MIB (Management Information Base)

El MIB está representado mediante la estructura de un árbol, un elemento del MIB es la especificación del tipo de dato que puede contener. Estos elementos usualmente son enteros, pero también pueden almacenar cadena de caracteres. A los elementos del mib toman el nombre de objetos.

Los objetos son los nodos hoja del árbol MIB. Dentro del espacio de nombres ISO hay una rama específica para la información MIB. Dentro de esta rama MIB, los objetos están a su vez jerarquizados en subárboles para los distintos protocolos y aplicaciones.

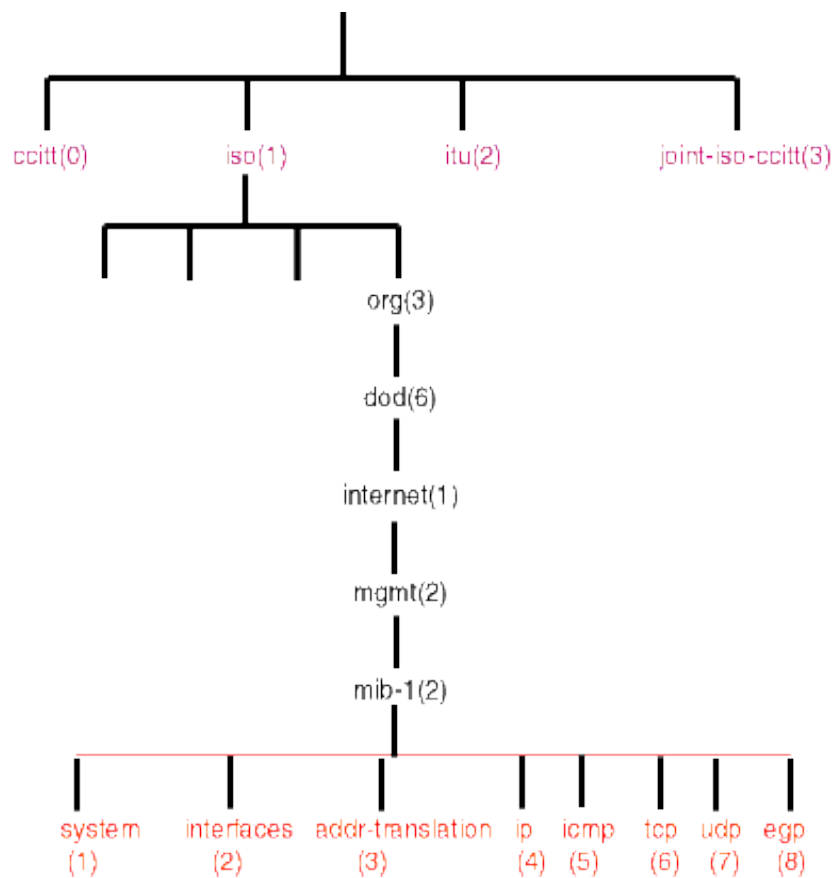


Fig. 2.7.2

A continuación detallaremos los objetos utilizados con su respectivo valor numérico.

OID	DESCRIPCION
1.3.6.1.2.1.1	system
1.3.6.1.2.1.1.1.0	sysDescr
1.3.6.1.2.1.1.2.0	sysObjectID
1.3.6.1.2.1.1.3.0	sysUpTime
1.3.6.1.2.1.1.4.0	sysContact
1.3.6.1.2.1.1.5.0	sysName
1.3.6.1.4.1.77.1.4.1.0	domPrimaryDomain
1.3.6.1.2.1.25.2.2.0	hrMemorySize
1.3.6.1.2.1.25.1.6	hrSystemProcesses
1.3.6.1.2.1.25.4.2.1.2	hrSWRunName
1.3.6.1.2.1.25.4.2.1.5	hrSWRunParameters
1.3.6.1.2.1.7.5.1.2.0.0.0.0	udpLocalPort
1.3.6.1.2.1.25.6.3.1.2	hrSWInstalledName
1.3.6.1.2.1.25.2.3.1.3	hrStorageDescr
1.3.6.1.2.1.25.2.3.1.6	hrStorageUsed
1.3.6.1.2.1.25.1.1.0	hrSystemUptime
1.3.6.1.2.1.4.20.1.1	ipAdEntAddr

Tabla. 2.7.2

**sysContact..-** Me especifica la información del contacto, es decir la persona responsable del host.

**sysName..-** Me indica el nombre del host, usualmente el nombre del dominio completo.

**sysObjectID.-** Contiene la identificación del subsistema de gestión de red que contiene el dispositivo, proporcionada por el fabricante.

**sysDescr.-** Especifica la descripción del host, es decir su nombre completo, descripción del hardware, sistema operativo y del software de red.

**domPrimaryDomain.-** Me indica el grupo de trabajo al cual pertenece el host.

**hrMemorySize.-** Me muestra el tamaño de la memoria física con la que cuenta el nodo.

**hrSystemProcesses.-** Me muestra la cantidad de procesos ejecutándose en el sistema.

**hrSWRunName.-** Me indica los programas que se están ejecutando en el sistema.

**hrSWRunParameters.-** Me muestra las aplicaciones que están abiertas en cada host.

**hrSWInstalledName.-** Me muestra los programas instalados de cada nodo.

**hrStorageDescr.-** Me indica la serie y el volumen de cada uno de los dispositivos de almacenamiento con que cuenta cada host.

**udpLocalPort.-** Me indica la cantidad de puertos abiertos en el host.

**hrStorageUsed.-** Me muestra la cantidad de memoria utilizada por el sistema.

**ipAdEntAddr.-** Me indica el numero de IP que tiene asignada cada PC en la red.

### **2.7.3 JSP (Java Server Pages)**

El código JSP es un lenguaje que permite desarrollar un código estructurado y orientado a objetos.



Este lenguaje genera archivos con extensión .jsp, que además incluyen etiquetas HTML. El motor JSP traduce esta página a un servlet, mediante un archivo class (Byte codes de Java).

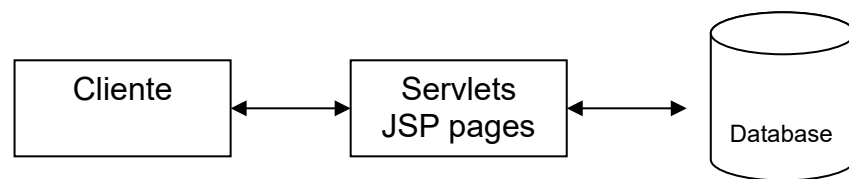


Fig. 2.7.3

El JSP utiliza los siguientes objetos:

Object	Type
request	javax.servlet.http.HttpServletRequest
response	javax.servlet.http.HttpServletResponse
out	javax.servlet.jsp.JspWriter
session	javax.servlet.http.HttpSession
application	javax.servlet.ServletContext
config	javax.servlet.ServletConfig
pageContext	javax.servlet.jsp.PageContext
page	javax.servlet.jsp.HttpJspPage
exception	java.lang.Throwable

Tabla. 2.7.3

**2.7.4 SSL (Secure Socket Layer)**

El SSL trabaja con la mayor parte de los browser, este protocolo es usado principalmente para cifrar datos confidenciales enviados sobre una red y brindar seguridad a la aplicación.

El SSL provee autenticación y privacidad de la información en Internet, mediante el uso de criptografía.

SSL contiene una serie de fases básicas:

- Negociar entre las partes el [algoritmo](#) que se usará en la comunicación
- Intercambio de [claves públicas](#) y autenticación basada en certificados digitales
- Cifrado del tráfico basado en [cifrado simétrico](#)

El protocolo de seguridad SSL/TLS, trabaja con la capa de protocolo de aplicación y la capa TCP/IP, donde esto puede asegurar y luego enviar datos de aplicación a la capa de transporte. Como esto trabaja entre la capa de aplicación y la capa TCP/IP, SSL/TLS puede apoyar múltiples protocolos de capa de aplicación.

Una página de Web asegurada con SSL/TLS tiene un URL que comienza con: `https: //` , además que en el navegador se mostrara un candado, en la parte inferior derecha del Explorer.

#### **2.7.5 MRTG (Multi RouterTraffic Graper)**

Es un protocolo que me permite representar gráficamente los datos que generen los agentes SNMP. La presentación la realiza

mediante páginas HTML, con gráficos GIF, sobre los datos que generen el SNMP sobre el tráfico de la red

El MRTG se base en Perl y en C, mientras que los gráficos con generados con la ayuda de la biblioteca GD.

El MRTG genera una página que contiene las imágenes junto con los detalles de cada interfaz, lo que permite tener una idea general de lo que esta sucediendo en la red.

El MRTG captura los datos de dos maneras:

- Mediante SNMP
- Mediante scripts de usuario

El método que estamos utilizando es nuestro sistema es mediante el uso del protocolo SNMP.

Otra característica del MRTG es que me detalla gráficamente la información del tráfico de la red en:

- Por día

- Por semana
- Mensualmente
- Anualmente

Además genera una página principal de las imágenes estadística de lo que esta sucediendo en la red. Permitiendo de esta forma al administrador tomar decisiones sobre el uso de la red.

### **2.7.6 Apache**

El Apache es un servidor HTTP (Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertext), de código abierto que funciona en Linux, Windows y otras plataformas. Es uno de los servidores http más utilizados. Las principales ventajas de la utilización de Apache son:

- Corre en una multitud de Sistemas Operativos, lo que lo hace prácticamente universal.
- Apache es una tecnología gratuita de código fuente abierto. Esto le da una transparencia a este software de manera que si queremos ver que es lo que estamos instalando como servidor, lo podemos saber.
- Apache es un servidor altamente configurable de diseño modular. Es muy sencillo ampliar las capacidades del servidor Web Apache. Actualmente existen muchos módulos

para Apache que son adaptables a este, y están ahí para que los instalemos cuando los necesitemos. Otra cosa importante es que cualquiera que posea una experiencia decente en la programación de C o Perl puede escribir un modulo para realizar una función determinada.

- Apache trabaja con gran cantidad de Perl, PHP y otros lenguajes de script.
- Apache te permite personalizar la respuesta ante los posibles errores que se puedan dar en el servidor. Es posible configurar Apache para que ejecute un determinado script cuando ocurra un error en concreto.
- Tiene una alta configurabilidad en la creación y gestión de logs. Apache permite la creación de ficheros de log a medida del administrador, de este modo puedes tener un mayor control sobre lo que sucede en tu servidor

## **2.8 Diccionario de Datos**

El Diccionario de Datos me permite describir el contenido de los objetos definidos durante el análisis.

Es el listado organizado de todos los elementos de datos que son pertinentes para el sistema, con definiciones que permiten al usuario una comprensión de las entradas y salidas de los componentes.

El diccionario de datos contiene lo siguiente:

- Nombre: El nombre del elemento de datos o de control, del almacén de datos o de una entidad externa.
- Alias: otros nombres usados.
- Donde se usa/Como se usa: Un listado de los procesos que se usan.
- Descripción: El contenido representado mediante una notación.

### 2.8.1 Estructura de las Tablas

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: Usuarios			Tipo: Maestra
Descripción: En esta se almacenara los usuarios que tendrán acceso al sistema del Monitor de Red			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
ID_USUARIO	Numero de Identificación	int	11
NOMBRES	Nombre del Uusario	varchar	200
APELLIDOS	Apellidos del Usuario	varchar	200
TELEFONO	Teléfono del Usuario	varchar	15
NOMBRE_USUARIO	Nombre que distingue al usuario	varchar	20
EMAIL	Correo electrónico	varchar	200
TIPO_USUARIO	Tipo de usuario (Administrador /Usuario)	varchar	3
ESTADO	Si se encuentra activo o inactivo	varchar	1
OBSERVACION	Tipo de usuario (Administrador /Usuario)	varchar	2000

Tabla 2.8.1

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: Usuario_dat		Tipo: Maestra	
Descripción: Se almacenará los usuarios con su respectiva clave encriptada para validar el ingreso al sistema.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
ID_USUARIO	Numero de Identificación	varchar	50
ID_CLAVE	Clave de acceso al sistema	varchar	200
TIPO_USUARIO	Tipo de usuario (Administrador /Usuario)	varchar	3
FEC_CREACION	Fecha de Creación del Usuario	datetime	
FEC_REGISTRO	Fecha de registro	datetime	
N_INTENTOS	Intentos de Ingreso al sistema	int	11

Tabla 2.8.2

MONITOR DE RED
----------------



Base de Datos:			
Nombre de la Tabla: IP			Tipo: Maestra
Descripción: Se ingresan las Ip con su respectivo sistema operativo de las Pc que se encuentran conectadas en la Red.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	Numero de IP	varchar	15
DESCRIPCION	Descripción	varchar	45
ESTADO	Tipo de usuario (Administrador /Usuario)	varchar	1
SISTEMA_OPERATIVO	Sistema Operativo que tiene instalado la PC	varchar	20

Tabla. 2.8.3

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: IF_NODOS			Tipo: Maestra
Descripción: Almacena la información que se muestra en la pantalla principal de todos los nodos que se encuentran en la red.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
ID_DISPOSITIVO	Número de identificación	varchar	20
IP	IP que tiene cada nodo	varchar	15
SIST_OPERATIVO	Sistema Operativo instalado en PC	varchar	20
ID_USUARIO	Nombre del usuario	varchar	15
ESTADO	Si se encuentra activo o inactivo	varchar	1

Tabla. 2.8.4

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: COMANDOS_SNMP			Tipo: Maestra
Descripción: Tiene almacenado OID de los comandos que utiliza el snmpwalk para capturar la información del tráfico de red.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
NOMBRE	Nombre del Comando	varchar	50
DESCRIPCION	Descripción de la función del comando	varchar	260
ID_COMANDO	Número que identifica al comando	varchar	50
ESTADO	Estado	varchar	1
TABLA		varchar	20

Tabla 2.8.5

MONITOR DE RED	
Base de Datos: MySql	
Nombre de la Tabla: APLICACIONES	Tipo: Maestra

<b>Descripción:</b> Se registrarán las aplicaciones que se muestran en el sistema de cada nodo, y que se utilizarán para los reportes posteriormente.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	IP del nodo	varchar	15
DESCRIPCION	Aplicaciones que se mostraron	varchar	100
FECHA	Fecha en que se monitoreo	datetime	

Tabla 2.8.6

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: ICONO_APLICACIONES		Tipo: Maestra	
Descripción: Contiene los iconos de las aplicaciones para presentarlos en el sistema.			
Tabla 2.8.7			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
APLICACIÓN	Nombre de la Aplicación	varchar	30
Base de Datos: MySql			
DESCRIPCION	Descripción de Aplicación	varchar	45
Nombre de la Tabla: SERVICIOS			
ICONO	Gráfico de la Aolicación	varchar	30
Tipo: Maestra			
Descripción: Contiene los servicios que se encuentran iniciados en cada Pc cuando fueron monitoreados.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	IP de la máquina monitoreada	varchar	15
DESCRIPCION	Descripción de los servicios	varchar	300
FECHA	Fecha en que fue monitoreada la máquina	datetime	

Tabla 2.8.8

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: DISPOSITIVOS_LOGICOS		Tipo: Maestra	
Descripción: Contiene los dispositivos lógicos que se encuentran conectados a su respectiva Pc.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	IP de la máquina monitoreada	varchar	15
NOMBRE	Dispositico (A:, C:, E:, etc)	varchar	20
DESCRIPCION	Nombre del Dispositivo (A:, C:, E:, etc)	varchar	30
VOLUMEN	Volumen del Dispositivo	varchar	40
TAMAÑO	Capacidad de cada dispositivo.	varchar	15
ESPACIO_LIBRE	Capcidad libre del dispositivo	varchar	15
FECHA	Fecha en que fue monitoreada la máquina	datetime	

Tabla 2.8.9

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: SISTEMA			Tipo: Maestra
Descripción: Contiene los datos del sistema como nombre del sistema operativo, numero de aplicaciones, Memoria, Capacidad del Disco Duro, etc.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	IP de la máquina monitoreada	varchar	15
NOMBRE_EQUIPO	Nombre del Dispositico (A:, C:, E:, etc)	varchar	200
DESCRIPCION	Fecha en que fue monitoreada la máquina	varchar	40
SISTEMA_OPERATIVO	Sistema Operativo Instalado (Linux, Windows)	varchar	40
NUM_PROGRAMA	Número de Programas Abiertos	varchar	3
TIEMPO	Tiempo que esta el servicio SNMP iniciado	varchar	30
FECHA	Fecha en que fue monitoreada la máquina	datetime	

Tabla 2.8.10

## **2.9 Análisis de la Estructura de un Objeto (AEO)**

El análisis de la estructura de los objetos (AEO) define las categorías de los objetos que percibimos y las formas en que lo asociamos. Este análisis identifica lo siguiente: ¿Qué son tipos de objetos y como se asocian?, Como se organizan? y ¿Cuál es la composición?.

### **2.9.1 Tipos de Objetos**

A continuación detallamos los tipo de objetos que nuestro sistema requiere:

- Administrador
- Visualizador
- Agente
- Pc
- Usuario
- Red

### **2.9.2 Diagrama de Relación entre los objetos**

Este Diagrama me indica los tipos de objetos que están relacionados con otros tipos de objetos:



Fig. 2.9.2

### 2.9.3 Diagrama de Generalización

La generalización es el acto o el resultado de distinguir un concepto que es más general que otro.

Esto nos permite comprender el mismo objeto dentro del contexto de una jerarquía. La generalización se aplica a las extensiones de un objeto, esto nos indica que el conjunto de uno de los tipos incluye al otro.

En este diagrama tenemos 4 objetos, no relacionados entre sí, aunque varios de estos son similares. Esto nos indica que

PERSONA es un tipo de objeto más general que USUARIO y este a su vez es un supertipo de *usuario normal* y *administrador*.

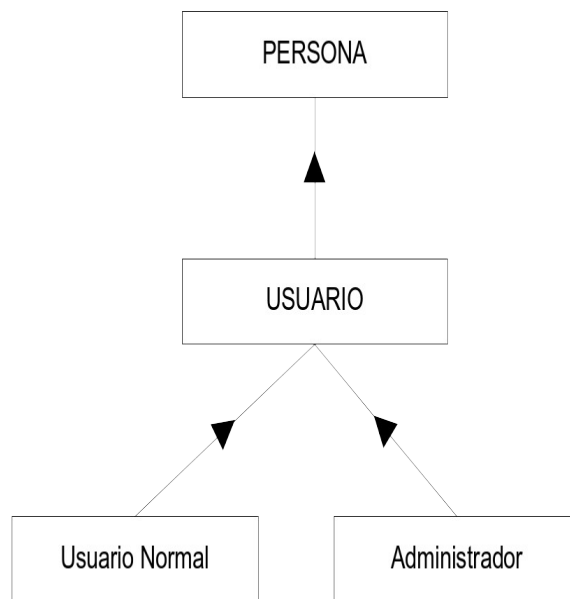


Fig. 2.9.3

Este diagrama nos indica que DISPOSITIVOS es un supertipo de *routers, impresora y switch*.

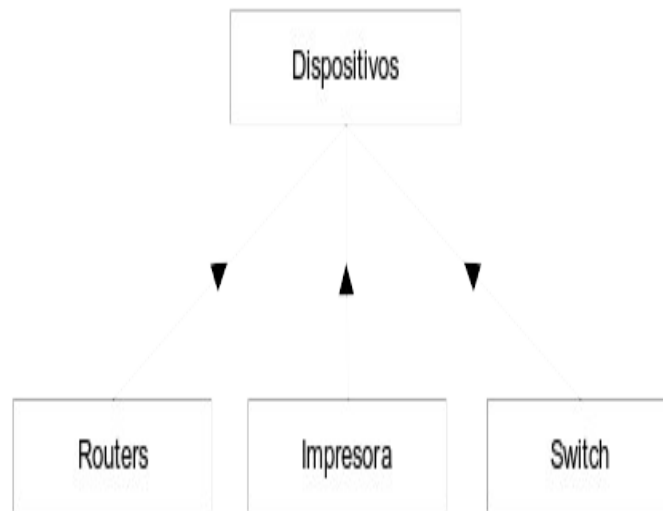


Fig. 2.9.3.1

#### 2.9.4 Diagrama de Componentes

La composición es el acto o el resultado de formar un objeto configurado mediante sus partes componentes. La composición reduce la complejidad al tratar muchas cosas como una sola.

A continuación el diagrama nos indica que el objeto Red esta compuesta por Pc's y dispositivos y cada Pc por un Agente y Usuario.



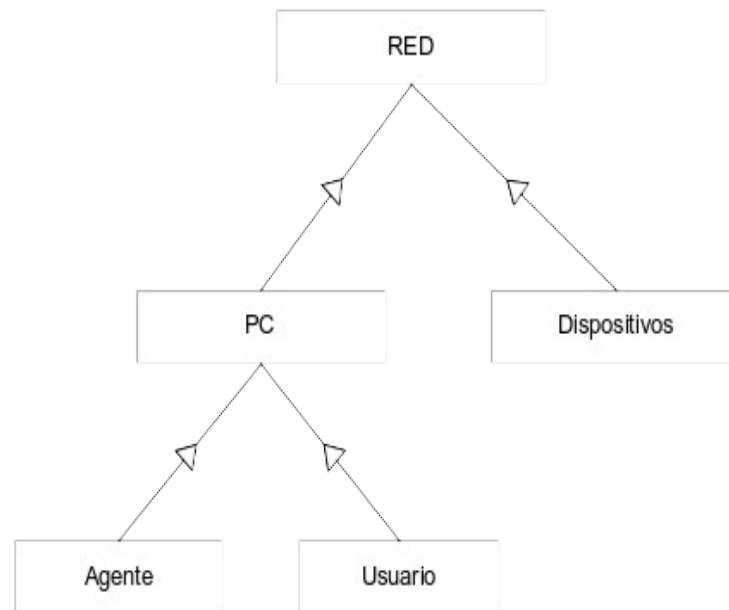


Fig. 2.9.4

### 2.10 Análisis del Comportamiento de los Objetos (ACO)

En el análisis de comportamiento de objetos (ACO), realizamos esquemas de eventos que muestran eventos, la secuencia en que ocurren y como los eventos cambian el estado de los objetos.

Aquí identificamos lo siguiente: ¿En que estado puede estar un objeto?, ¿Qué transiciones de estados se puede dar?. ¿Que eventos ocurren?, ¿Qué operaciones se llevan acabo?, ¿Que interacciones ocurren entre objetos? Y ¿Cuáles son las reglas de activación que se utilizan para reaccionar ante el evento?.

### 2.10.1 Diagrama de Flujo de Objetos

Este diagrama nos indica los objetos que se producen y las actividades que los producen e intercambian. Es donde se detalla el proceso del sistema.

Uno de los primeros pasos es que La Pc proporciona datos al Agente para que esta información se a procesada y enviada al visualizador y por otro extremo el CLIENTE solicita información de la Red a través del visualizador.

El diagrama de Flujo objetos se lo realiza con las siguientes figuras.

**Tipos de Objetos.-** Un objeto es cualquier cosa, real o abstracta, acerca de la cual almacenamos datos, los métodos que controlan dichos datos. El objeto se representa mediante un triángulo.



**Tipos de Objetos externos.-** Este tipo de objeto externo se representa mediante una caja sombreada.



**Comunicación.-** Se representa por medio de una flecha.

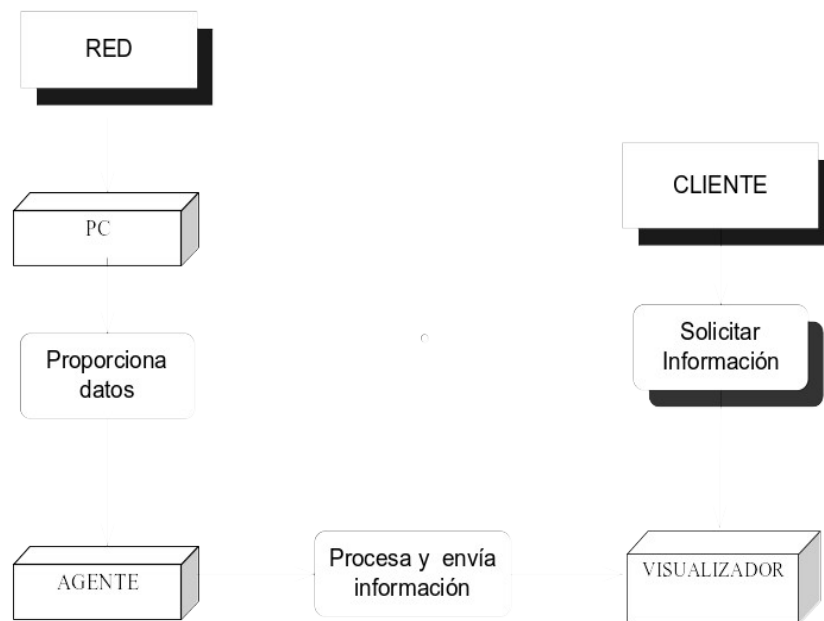
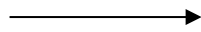


Fig. 2.10.1

## 2.10.2 Diagrama de Eventos

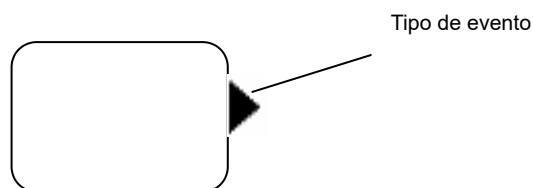
En el diagrama de Eventos se indican las operaciones que se realizan. Un evento se representa mediante un triángulo sólido.

En el análisis necesitamos conocer cada evento que ocurra. Así como hablamos anteriormente de tipos de objetos, podemos hablar de tipos de eventos e instancias de tipos de eventos. Los tipos de eventos indican los cambios sencillos de un objeto. El diagrama de eventos de este proyecto se lo encuentra en la Fig. 2.10.2

Los tipos de eventos describen las siguientes formas de cambios de estado:

A continuación detallamos los estándares de diagramación:

**Eventos** .- Estos se representa, mediante cuadros con esquinas redondeadas . Los tipos de eventos se representan mediante triángulos negros conectados a la caja.



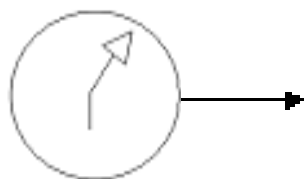
**Eventos Externos.-** El símbolo de operación se dibuja con una caja sombreada con esquinas redondeadas.



**Reglas de Activación.-** Las líneas de activación indican dos cosas.



**Eventos del Reloj.-** Este tipo de evento se dibuja como una carátula de reloj.



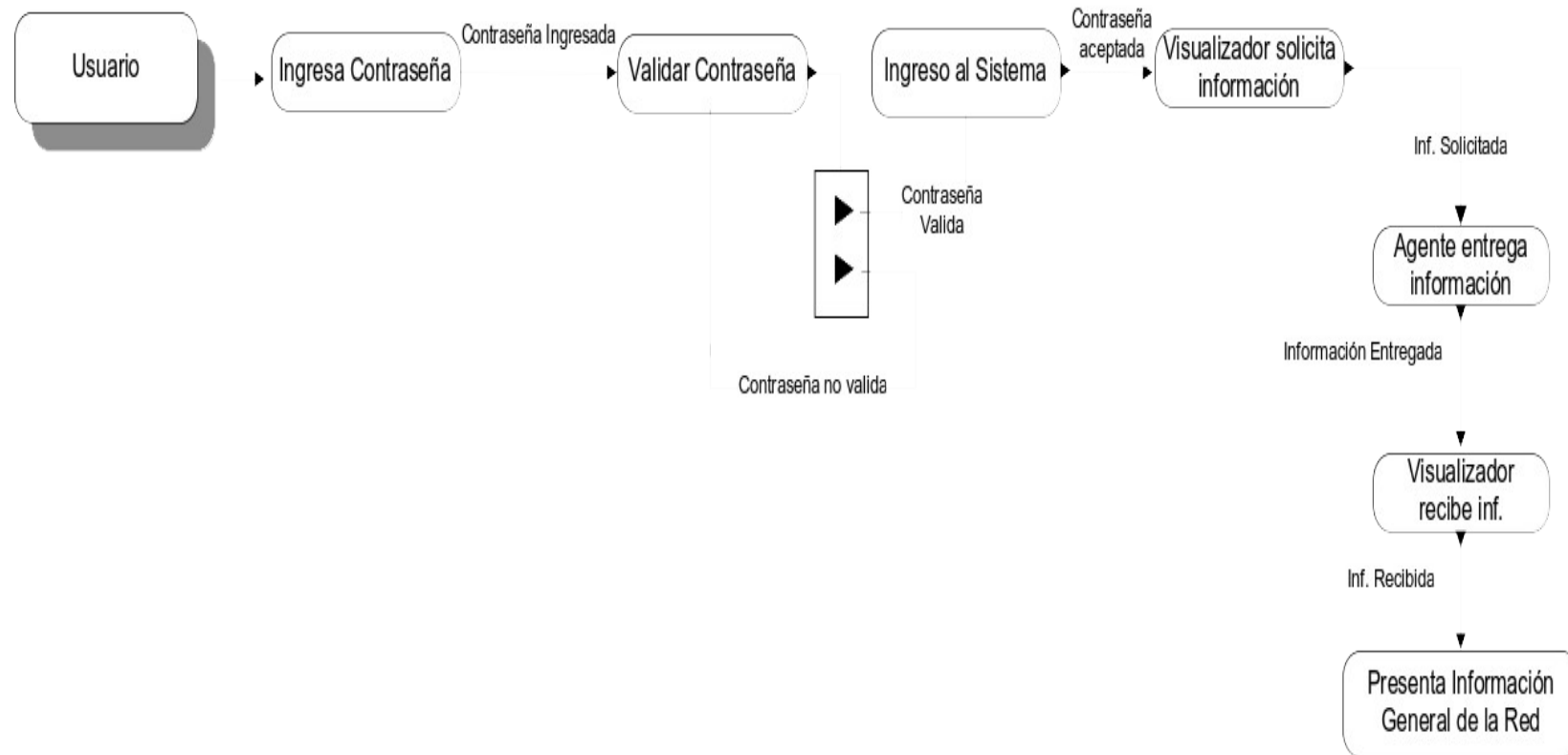


Fig. 2.10.2

### **2.10.3 Diagrama de Eventos Específico**

Aquí se detallará más específicamente los eventos que realicen los usuarios cuando ingresen al sistema, activándose de esta manera la reglas de activación en el momento en que decida de visualizar la información o generarlos reportes.

Además se detallara el evento del reloj, el cual indica el tiempo en el cual el Monitor de Red va ha solicitar información al protocolo SNMP de los agentes para presentar la información actualizada en el visualizador de la red.



Fig. 2.10.3



### **2.11 Diagrama de Casos de Usos**

El Diagrama de Casos de Uso es aquel que me muestra la relación entre los actores y los casos de uso del sistema. Representa la funcionalidad que ofrece el sistema en lo que se refiere a su interacción externa. En el diagrama de casos de uso se representa por un elipse con el nombre en su interior. Los casos de uso están en el interior de la caja del sistema, y los actores fuera, y cada actor está unido a los casos de uso en los que participa mediante una línea. En la Figura

Los elementos que se encuentran en un diagrama de casos de uso son: actores, casos de uso y las relaciones entre los casos de usos.

**Actor.-** Un actor puede ser una persona (identificada por un rol), un sistema u organización y que realiza algún tipo de interacción con el sistema.

**Casos de Uso.-** Un caso de uso es una descripción de la secuencia de interacciones que se produce entre un actor y un sistema para llevar a cabo una tarea específica.

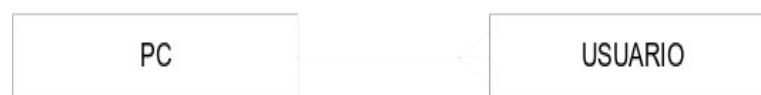
Es importante diferenciar que actor y usuario no es lo mismo. Un usuario desempeña ciertos números de roles cuando usa el sistema, mientras que el actor representa una clase de entidades eternas que desempeña un papel.

## 2.12 Cardinalidad

La cardinalidad nos indica la instancia de un tipo de objeto asociado con la instancia de otro tipo de objeto.

A continuación se detalla cada una de las cardinalidades que posee nuestro proyecto:

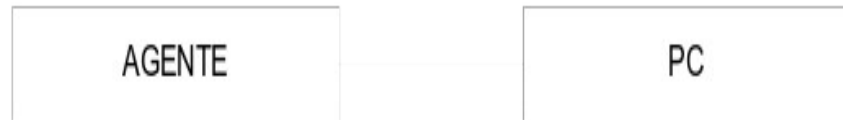
### PC y Usuario



#### Cardinalidad de uno a muchos

La línea de relación Pc-Usuario nos indica que un Pc puede más de un usuario .

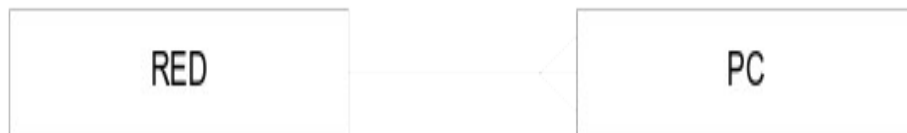
### Agente y Pc



#### Cardinalidad de uno a uno

La línea de relación Agente-Pc nos indica que un Pc tiene un Agente y un Agente esta en PC.

### Red y Pc



#### Cardinalidad de uno a muchos

La línea de relación Red-Pc nos indica que una Red tiene una o más Pc y una Pc debe pertenecer a una Red.

### Visualizador y Pc



#### Cardinalidad de uno a muchos

La línea de relación entre Visualizador y Pc nos indica que un Visualizador tiene o muestra una o más Pc y un Visualizador necesita por lo menos una Pc para funcionar.

### Visualizador y Administrador



#### Cardinalidad de uno a uno

La línea de relación entre Visualizador y Administrador nos indica que un Visualizador tiene un Administrador y un administrador un visualizador.

Nota: En los diagramas de cardinalidad explicados anteriormente están sujetos dentro del contexto del sistema a desarrollarse.

### **2.13 Esquema de Actividades**

Un esquema de actividad es un diagrama de flujos del proceso que se usa para mostrar el comportamiento del sistema, mediante una secuencia de operaciones. Una actividad es el proceso cuya producción y consumo están especificados. En otras palabras las actividades son procesos cuya dinámica no está especificadas.

Este diagrama es parecido a un diagrama de flujo, la diferencia en que mediante este diagrama se pueden mostrar procesos paralelos y además de hilos en los programas concurrentes. La desventaja es que no mediante este diagrama no se muestra los enlaces existentes entre las acciones y los objetos.

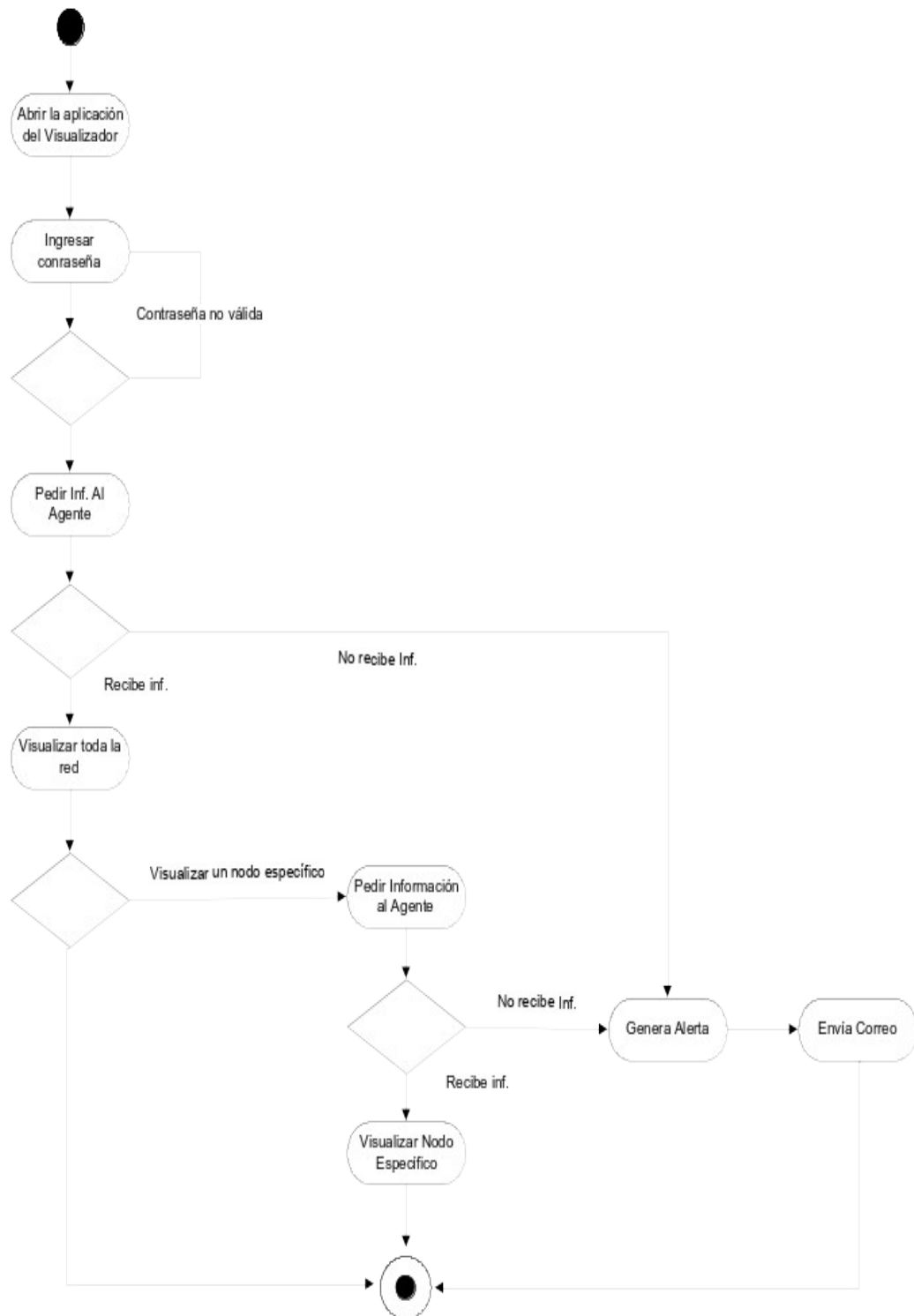


Fig. 2.13

## 2.14 Diseño de Componentes

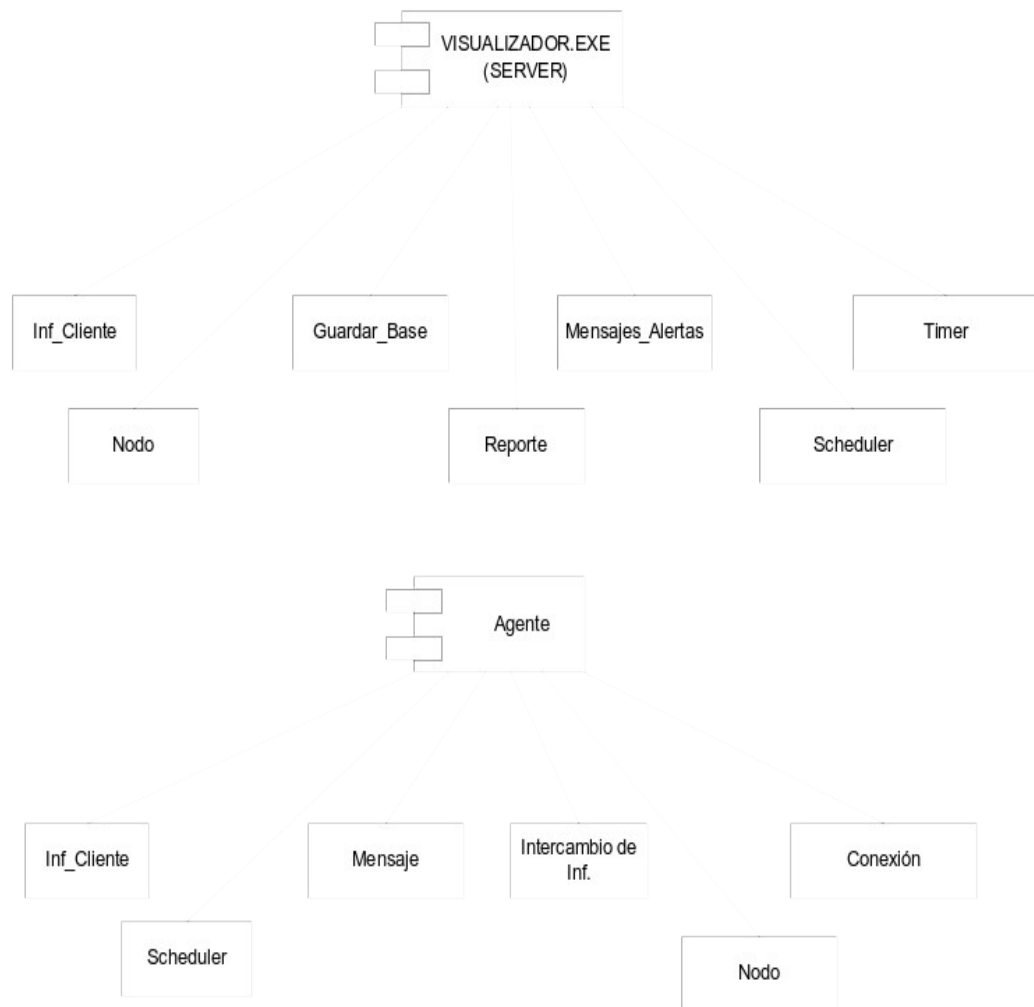


Fig. 2.14

## CAPÍTULO 3

### 3. DISEÑO

En este capítulo se lleva a acabo la fase del diseño del Sistema de Monitor de Red, es un proceso mediante el cual se realiza la transformación de los requisitos en los datos y arquitectura del software como es la arquitectura del sistema, la interfaz gráfica,etc.

#### 3.1 Arquitectura del Sistema

El sistema a implantar utiliza la arquitectura Cliente – Servidor, es decir la comunicación entre el cliente y servidor es a través de un puerto de comunicación.



Fig. 3.1



Este sistema realiza las funciones de gestión y control mediante el intercambio de mensajes con el protocolo SNMP v1.y SNMP v2.

### 3.2 Esquema de la descripción funcional del sistema

El propósito del sistema, es ofrecer servicio de gestión y control. Este servicio esta basado en una interfaz Web, ofrece al usuario el acceso al sistema dentro de un entorno navegador.

El sistema utiliza el protocolo SNMP v1 y SNMP v2 para el intercambio de mensajes. Los agentes SNMP proceso los datos que se requieren de acuerdo a las opciones del sistema actualizando la presentación de las páginas. El SNMP utiliza el TCP como el protocolo de transporte de mensajes.

El depositario de los datos se encuentra en una Base de Datos de MYSQL, esta base de datos es rápida y confiable en el entorno Open Source, esta base de datos provee de una interfaz para el intercambio masivo de datos,

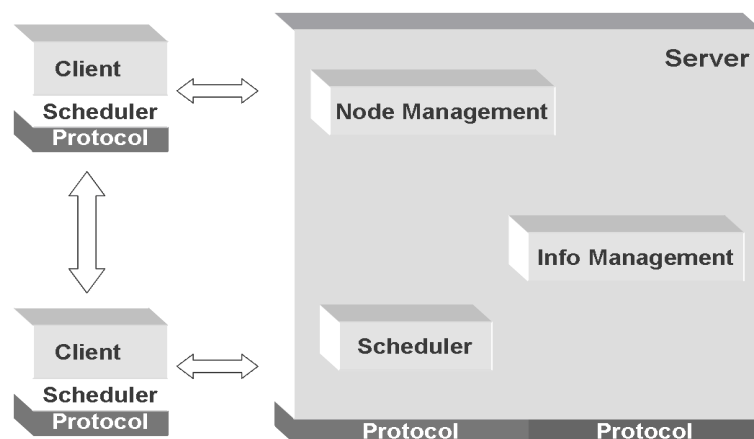


Fig. 3.2

La interfaz Web del sistema esta manejada por un Servido Web Apache Tomcat 5. y la herramienta de desarrollo que se esta empleado es Java. La elección de este lenguaje se la realizó.

El software se encuentra en JSP. La elección de este lenguaje se basa que es un lenguaje multiplataforma, Las páginas JSP están compuestas de código HTML/XML y Java mezclado con etiquetas especiales para programar scripts ejecutables. Por lo tanto, las JSP podremos escribirlas con nuestro editor HTML/XML habitual.

Se utiliza además el protocolo MRTG, que es aquel que me permite mostrar gráficamente el tráfico de la red, este protocolo trabaja junto con el protocolo SNMP que es el encargado de enviar la información de los nodos al Monitor de Red.

### **3.3 Diseño de Datos**

El diseño aplicado al sistema del Monitor de Red es Orientado a Objetos. Es de mencionar que los datos bien diseñados conducen a una mejor estructura del programa

### **3.3.1 Estructura de la Base de Datos**

En la estructura de datos se detallara las relaciones entre las entidades de un sistema que el sistema utilizará con sus respectivos campos como claves primarias y foráneas.

#### **3.3.1.1 Tablas**

Las tablas son aquellas que contienen los atributos de una entidad, las cuales se detallaran a continuación:

#### **USUARIOS**

Esta tabla almacenará la información de cada uno de los usuarios que tendrán acceso al sistema.

Tabla. 3.3.1.1

**USUARIOS\_DAT**

<b>CAMPOS</b>	<b>TIPO DE DATO</b>	<b>NULL</b>
ID_USUARIO	int(11)	NOTNULL
NOMBRES	varchar (200)	NOTNULL
APELLIDOS	varchar (200)	NOTNULL
TELEFONO	varchar (15)	NULL
NOMBRE_USUARIO	varchar (20)	NULL
EMAIL	varchar (200)	NULL
TIPO_USUARIO	varchar (3)	NULL
ESTADOO	varchar (1)	NULL
OBSERVACAION	varchar (2000)	NULL

Esta tabla me permite guardar la clave para posteriormente realizar su respectiva validación ingreso al sistema.

CAMPOS	TIPO DE DATO	NULL
ID_USUARIO	varchar (50)	NULL
ID_CLAVE	varchar (200)	NULL
TIPO_USUARIO	varchar (3)	NULL
FEC_CREACION	datetime	NULL
FEC_REGISTRO	datetime	NULL
N_INTENTOS	int (11)	NULL

Tabla. 3.3.1.2

## IP

Esta tabla almacenara cada una de las Ip de las máquinas que ingresaran a la red.

CAMPOS	TIPO DE DATO	NULL
IP	varchar (15)	NOTNULL
DESCRIPCION	varchar (45)	NOTNULL
ESTADO	varchar (1)	NOTNULL
SISTEMA_OPERATIVO	varchar (20)	NOTNULL

Tabla. 3.3.1.3

### IF\_NODOS

Esta tabla guarda la información enviada por el snmp de los campos que se mostrara en la pantalla principal del sistema.

CAMPOS	TIPO DE DATO	NULL
ID_DISPOSITIVO	varchar (20)	NOTNULL
IP	varchar (15)	NOTNULL
SIST_OPERATIVO	varchar (50)	NOTNULL
ID_USUARIO	varchar (15)	NOTNULL
ESTADO	varchar (1)	NOTNULL

Tabla. 3.3.1.4

### COMANDOS\_SNMP

Contiene el OID de los comandos con sus respectivas descripciones, los cuales van ha ser utilizados para obtener los datos que se presentaran en la aplicación.

CAMPOS	TIPO DE DATO	NULL
NOMBRE	varchar (50)	NULL
DESCRIPCION	varchar (260)	NULL
ID_COMANDO	varchar (50)	NULL
ESTADO	varchar (1)	NULL
TABLA	varchar (20)	NULL

Tabla. 3.3.1.5

### ICONO\_APLICACIONES

En esta tabla se almacenara los gráficos de las aplicaciones que contiene cada PC y que se mostraran en la aplicación.

CAMPOS	TIPO DE DATO	NULL
APLICACIÓN	varchar (30)	NULL
DESCRIPCION	varchar (45)	NULL
ICONO	varchar (30)	NULL

Tabla. 3.3.1.6

### APLICACIONES

Esta tabla almacenará las aplicaciones que se muestran en el sistema y que se utilizará para los reportes que se generarán posteriormente.

CAMPOS	TIPO DE DATO	NULL
IP	varchar (15)	NULL
DESCRIPCION	varchar (100)	NULL
FECHA	datetime	NULL

Tabla. 3.3.1.7

## SERVICIOS

Esta tabla almacenará los servicios que se muestran en el sistema y que se utilizará para los reportes que se generarán posteriormente.

CAMPOS	TIPO DE DATO	NULL
IP	varchar (15)	NULL
DESCRIPCION	varchar (300)	NULL
FECHA	datetime	NULL

Tabla. 3.3.1.8

## DISPOSITIVOS\_LOGICOS

Esta tabla contendrá la descripción, capacidad, volumen de los dispositivos que se encuentran conectados en la PC, y que se utilizará para los reportes que se generarán posteriormente.

CAMPOS	TIPO DE DATO	NULL
IP	varchar (15)	NOTNULL
NOMBRE	varchar (20)	NULL
DESCRIPCION	varchar (30)	NULL
VOLUMEN	varchar (40)	NULL
TAMAÑO	varchar (15)	NULL
ESPACIO_LIBRE	varchar (15)	NULL
FECHA	datetime	NULL



Tabla. 3.3.1.9

**SISTEMA**

Esta tabla guarda la información más relevante del sistema operativo que tiene instalado la PC que se encuentra monitoreada., como es el nombre del sistema, número de aplicaciones, el tiempo desde cuando esta ejecutando el snmp, etc.

CAMPOS	TIPO DE DATO	NULL
IP	varchar (15)	NOTNULL
NOMBRE_EQUIPO	varchar (200)	NULL
DESCRIPCION	varchar (40)	NULL
SISTEMA_OPERATIVO	varchar (40)	NULL
NUM_PROGRAMA	varchar (3)	NULL
TIEMPO	varchar (30)	NULL
FECHA	datetime	NULL

Tabla. 3.3.1.10

### 3.4 Funcionamiento de los Agentes

En este esquema se podrá observar que los agentes (Clientes), de cada una de las Pcs que se encuentra conectadas en la red obtiene información por medio de su BD llamada MIB.

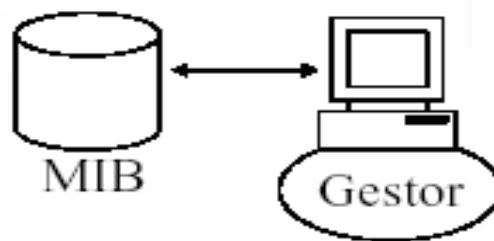


Fig. 3.4

Este solicita la información a los agentes mediante el protocolo SNMP como es: el sistema operativo, ip, usuario, etc).

### 3.5 Módulos del Sistema

Se detallan cada uno de los módulos con los que cuenta el sistema con sus respectivas funciones. Como se muestra en la Fig,

#### 3.5.1 Módulo Principal

Es el módulo principal de la aplicación es donde se realizan las siguientes acciones:

- Conexión de los Agentes (Clientes) que se encuentran en la Red.
- El servidor solicita la información de los agentes
- Captura los datos enviados por el SNMP
- Envía alertas si se encuentra inactivas la Pc's.
- Guarda la información en la Base de Datos.

Se necesita una red de área local (LAN) y se utiliza la herramienta jsp junto con código HTML. Además de la Base de Datos MySql.

Este proceso se ejecuta en el servidor y se conecta a los agentes que se encuentran configurados en cada PC por medio del protocolo SNMP de los OID que van ha ser supervisados.

Después de capturar la información que nos envía cada nodo estás son mostradas en el visualizador del Monitor de Red.

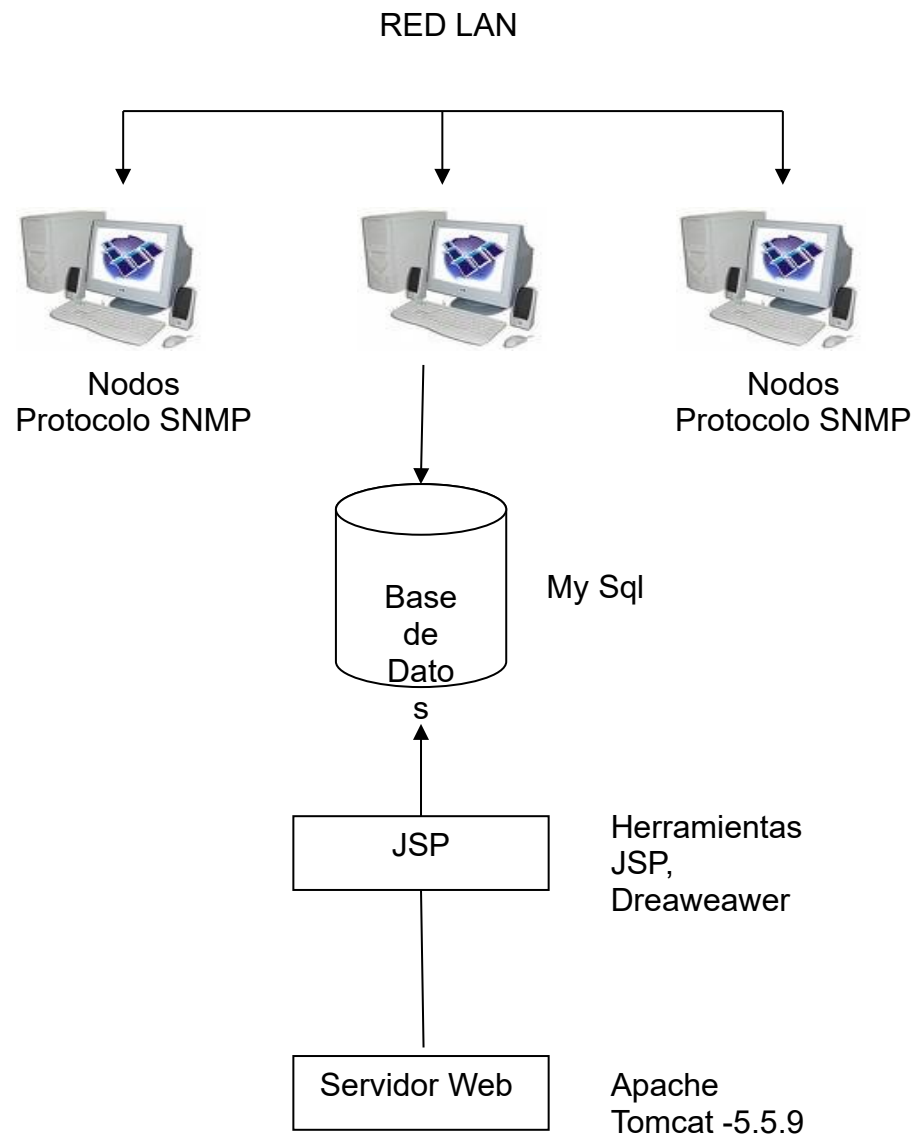


Fig. 3.5.1

### **3.6 Alertas**

Las alertas se generarán de acuerdo a los eventos que se generen, por ejemplo, cuando algún dispositivo se encuentre en estado inactivo, presentará un mensaje indicando la Ip, con el estado actual del dispositivo.

### **3.7 Ingreso del Usuario**

Este esquema nos indica como el usuario realiza el ingreso al servidor donde se encuentra instalada la aplicación. Cada usuario ingresara su username y su password.. Como se muestra en la Fig. 3.7



## Esquema para la validación de Usuarios

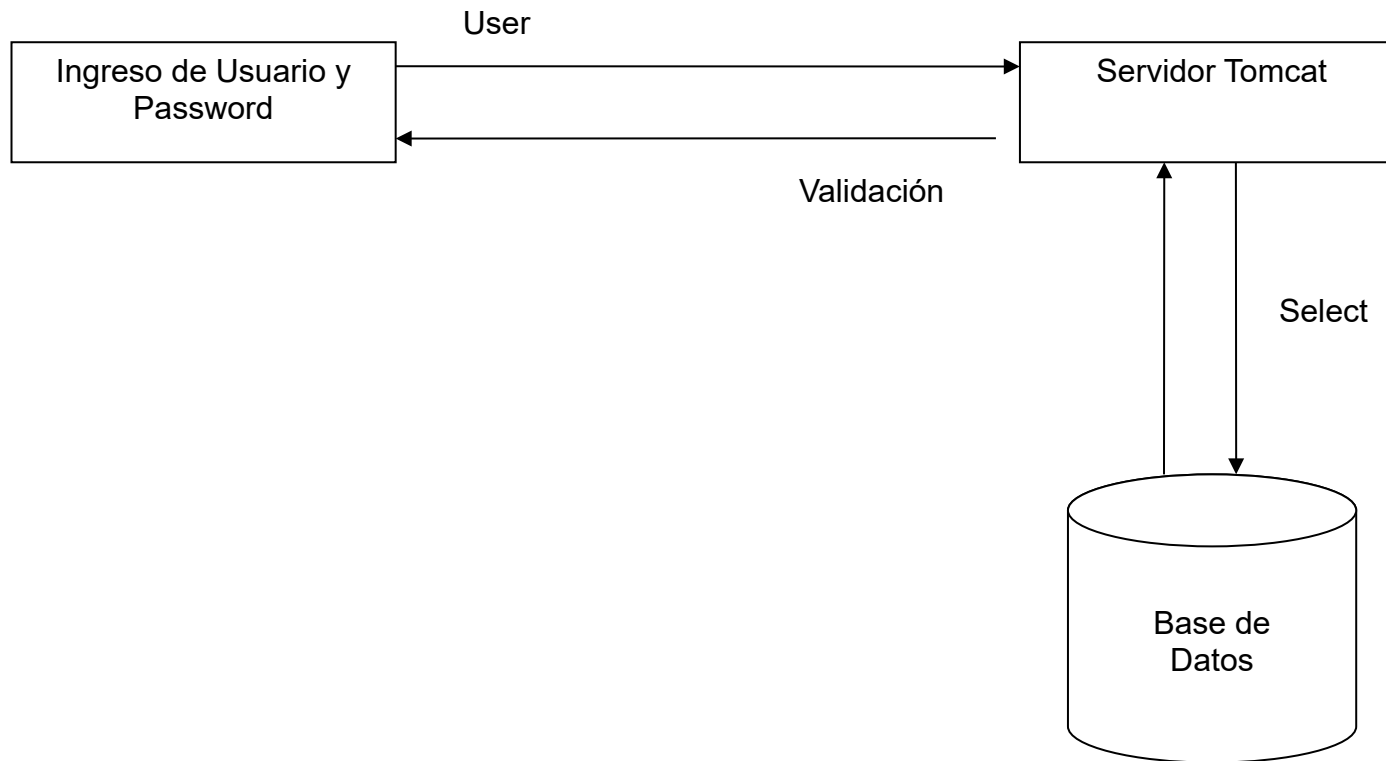


Fig 3.7

### **3.8 Funcionamiento del Sistema**

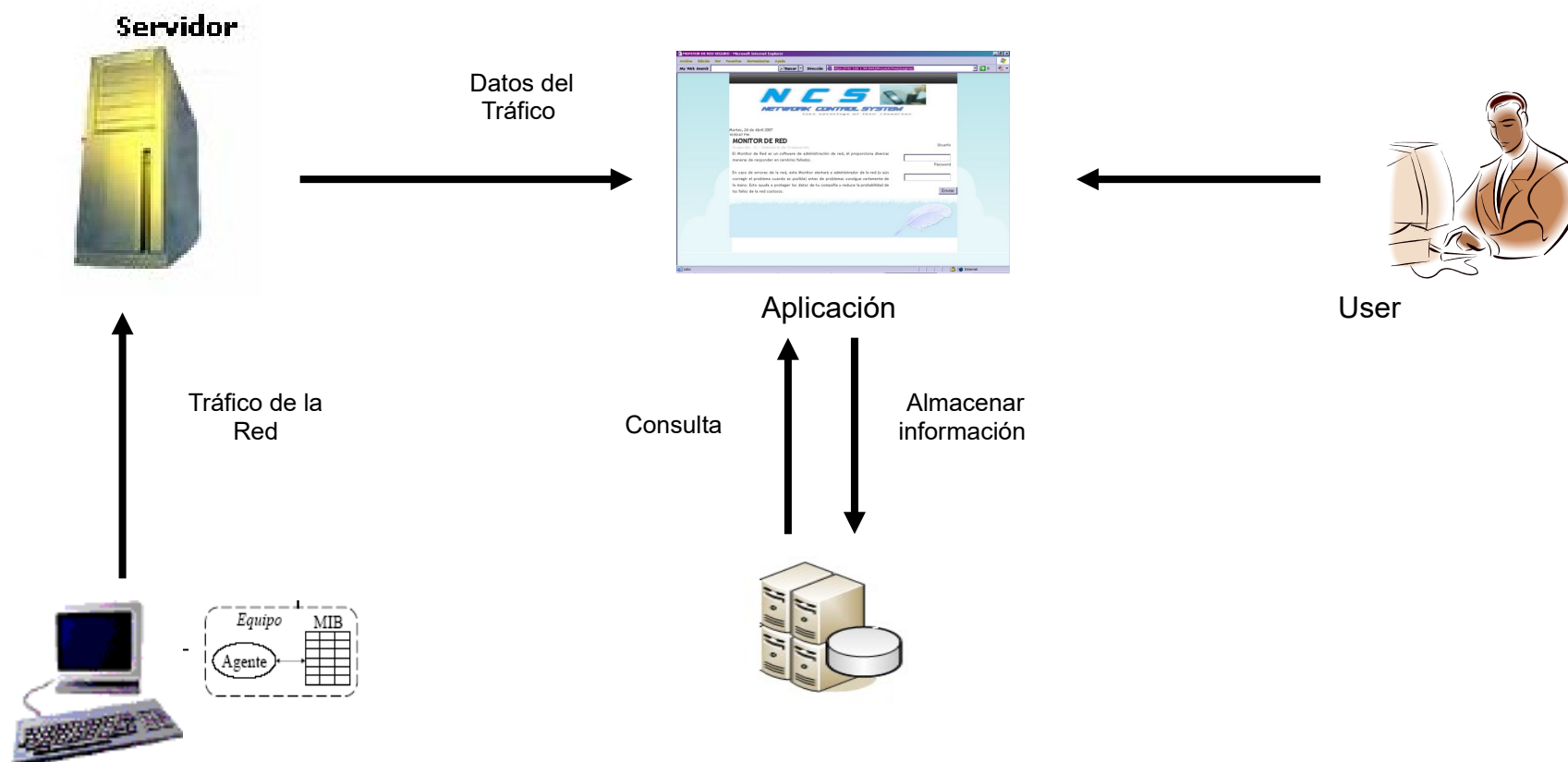
El servidor obtendrá la información de cada uno de los agentes que son enviados por el protocolo SNMP que será el encargado de capturar el tráfico de la red y presentarlos en la Aplicación, para que luego estos sean almacenados en Base de Datos y puedan ser consultados por medio de reportes. Además el ingreso del usuario a la aplicación que será la encargada de monitorear la red. Ver (Fig. No. 3.8)

### **3.9 Diagrama de Entidad-Relación**

En el Diagrama de Entidad-Relación definiremos las entidades por las que va ha estar constituido nuestro sistema y el tipo de relación que existe entre ellas. Ver (Fig. 3.9)



## FUNCIONAMIENTO DEL SISTEMA



NCS_IP			
Column	Type	Nullable	Default
<b>IP</b>	<b>VARCHAR2(15)</b>		
DESCRIPCION	VARCHAR2(45)	Y	
ESTADO	VARCHAR2(1)	Y	
SISTEMA_OPERATIVO	VARCHAR2(20)	Y	
Key		Column(s)	Type
NCS_IP_PK	IP	P	
Index		Column(s)	Type
NCS_IP_PK	IP	unique	

NCS_INF_NODOS			
Column	Type	Nullable	Default
<b>IP</b>	<b>VARCHAR2(15)</b>	Y	
<b>ID_DISPOSITIVO</b>	<b>VARCHAR2(20)</b>		
SIST_OPERATIVO	VARCHAR2(50)	Y	
ID_USUARIO	VARCHAR2(15)	Y	
ESTADO	VARCHAR2(1)	Y	
FEC_REGISTRO	DATE	Y	
Key		Column(s)	Type
NCS_INFNODES PK	ID_DISPOSITIVO	P	
NCS_INFNODES FK1	IP	R	
NCS_INFNODES FK2	ID_USUARIO	R	
Index		Column(s)	Type
NCS_INFNODES PK	ID_DISPOSITIVO	unique	

NCS_USUARIOS	
Column	Type
<b>ID_USUARIO</b>	<b>NUMBER(3)</b>
NOMBRES	VARCHAR2(200)
APELLIDOS	VARCHAR2(200)
DIRECCION	VARCHAR2(500)
TELEFONO	VARCHAR2(15)
<b>NOMBRE_USUARIO</b>	<b>VARCHAR2(20)</b>
EMAIL	VARCHAR2(200)
EMAIL_ALTERNO	VARCHAR2(200)
TIPO_USUARIO	VARCHAR2(3)
ESTADO	VARCHAR2(1)
OBSERVACION	VARCHAR2(2000)
Key	
NCS_USUARIOS PK	NOMBRE_USUARIO
Index	
NCS_USUARIOS IDX1	TIPO_USUARIO, ESTADO, NOMBRE_USUARIO
NCS_USUARIOS PK	NOMBRE_USUARIO

NCS_USUARIOS_DAT			
Column	Type	Nullable	Default
<b>ID_USUARIO</b>	<b>VARCHAR2(50)</b>	Y	
<b>ID_CLAVE</b>	<b>VARCHAR2(200)</b>	Y	
<b>TIPO_USUARIO</b>	<b>VARCHAR2(3)</b>	Y	
FEC_CREACION	DATE	Y	
FEC_REGISTRO	DATE	Y	
<b>N_INTENTOS</b>	<b>NUMBER(3)</b>	Y	
Key		Column(s)	Type
NCS_USUARIOSDAT FK	ID_USUARIO	R	
Index		Column(s)	Type
NCS_USUARIOSDAT IDX	TIPO_USUARIO		

### 3.10 Diseño de Interfaz

#### 3.10.1 Acceso al Sistema

Mediante esta pantalla se ingresa el username y el password respectivo de los usuarios autorizados para manejar el sistema.

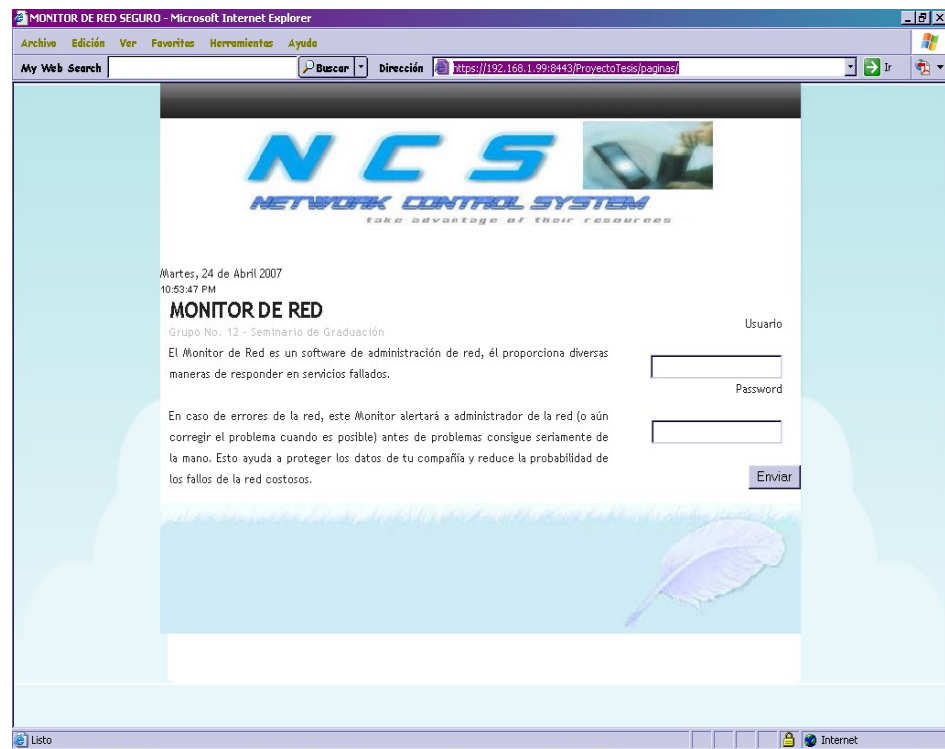


Fig. 3.10.1

Mediante esta pantalla se puede visualizar la encriptación de la clave



Fig. 3.10.1.1

3.10.2 Detalle de Nodos

Esta pantalla mostrará cada una de las Pc's que se encuentran conectadas en la red, con sus respectivas ip, así como: nombre, sistema operativo y estado.



Fig. 3.10.2

### 3.10.3 Aplicaciones y Servicios

Esta página muestra las aplicaciones que se encuentran instaladas en cada nodo y los servicios que se encuentran iniciados.

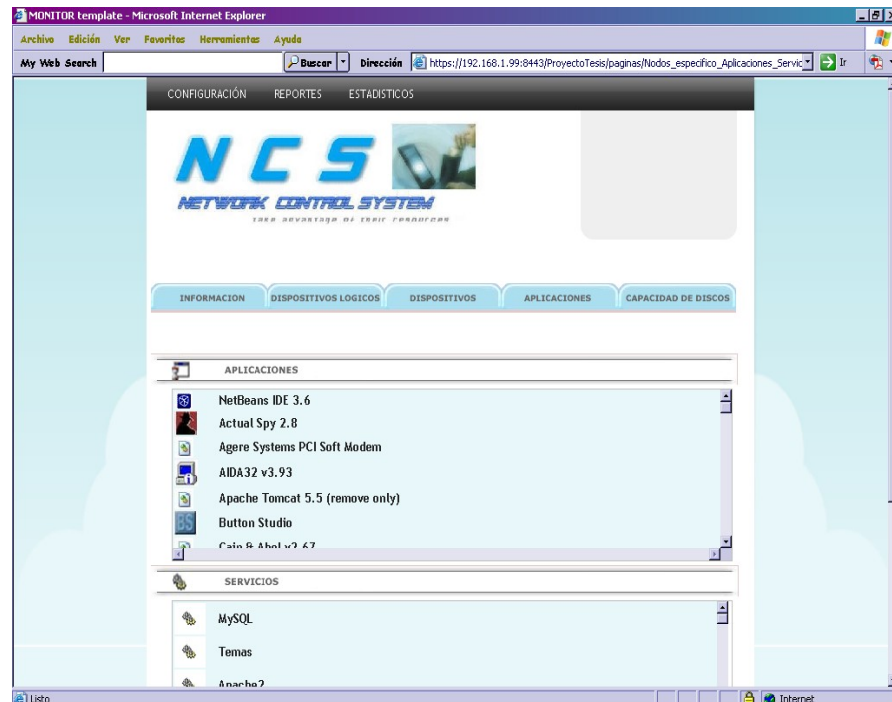


Fig. 3.10.3

### 3.10.4 Dispositivos Lógicos

En esta página se muestra los dispositivos conectados a la PC que se encuentra monitoreando con sus respectivos label, memoria, etc.

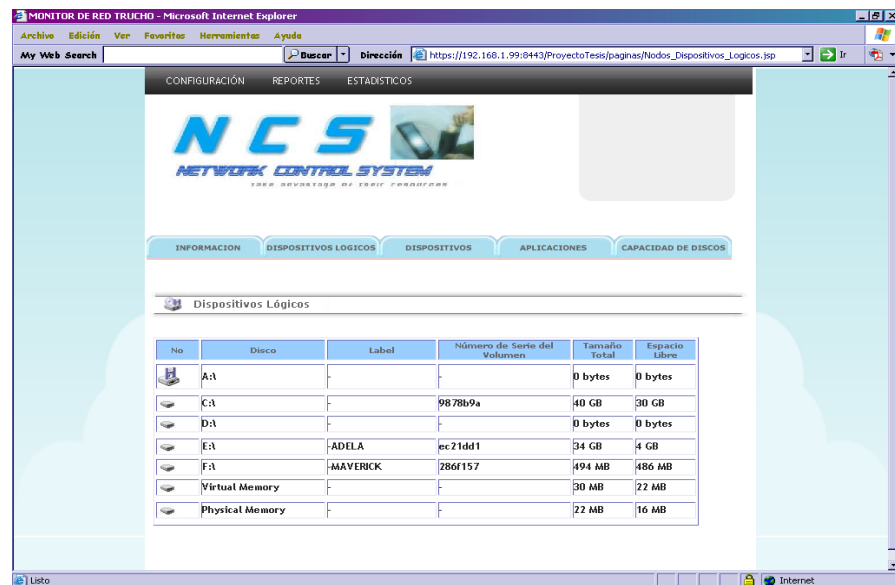


Fig 3.10.4

### 3.10.5 Capacidad de Dispositivos

Nos muestra la capacidad de los dispositivos que se encuentra conectados a la Pc, en forma numérica como gráfica.

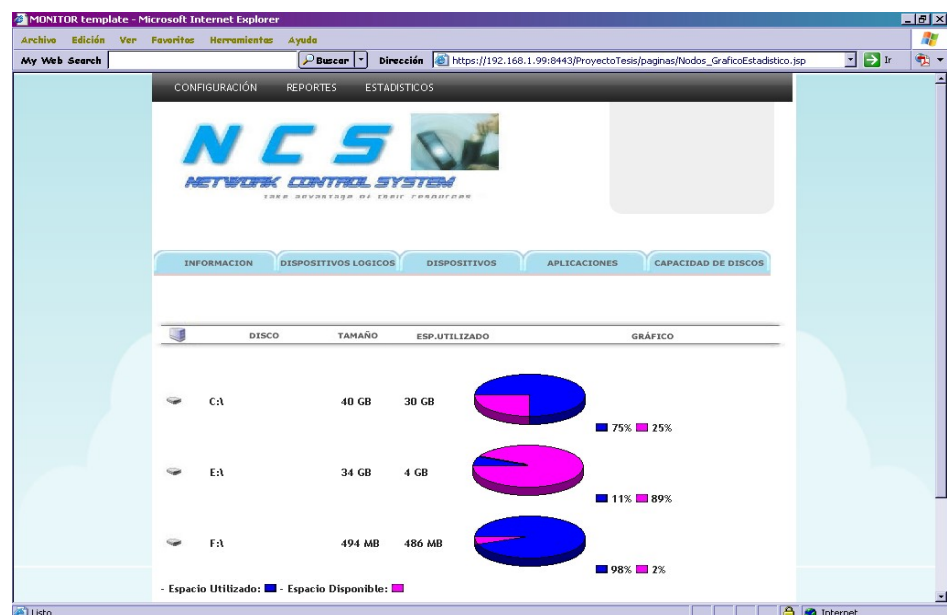


Fig. 3.10.5

### 3.10.6 Información del Sistema

Mediante esta pantalla se mostrará los usuarios, nombre, sistema operativo, etc. , es decir información general del sistema operativo que tiene la Pc que se encuentra monitoreada.

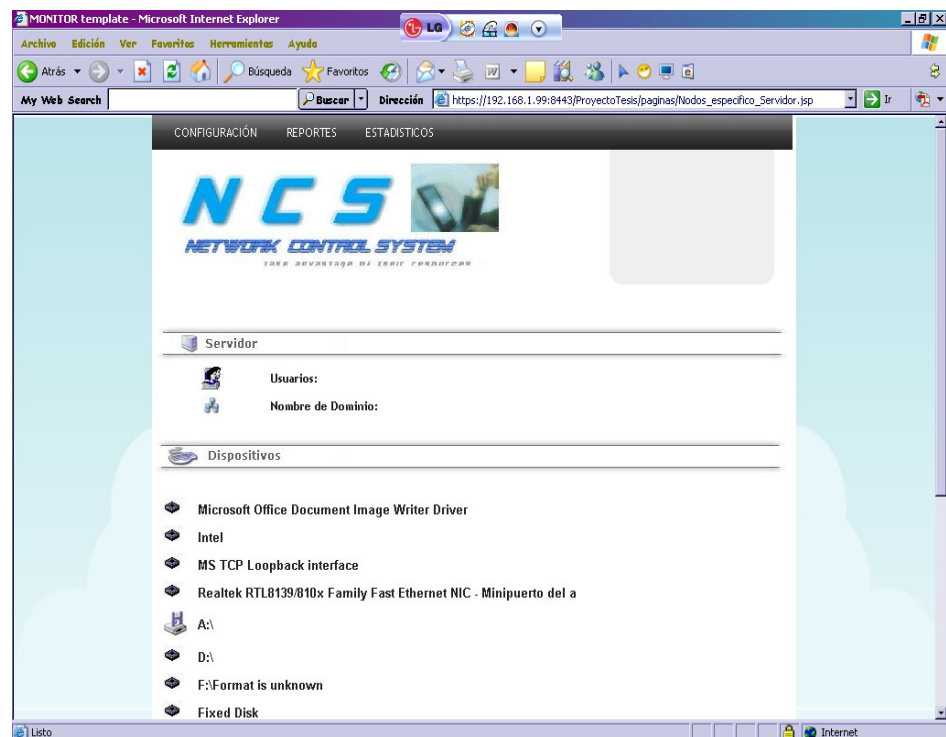


Fig . 3.10 .6

# CAPÍTULO 4

## 4. DESARROLLO Y PRUEBA DEL SISTEMA

En este capítulo se lleva a cabo la fase del desarrollo en la cual se verifica el sistema de acuerdo al alcance, cumplimiento de los requerimientos, así como su instalación y funcionamiento

### 4.1 Creación de la Base de Datos

En esta etapa se realiza una lista de las entidades y de las relaciones existentes entre cada una de ellas. Se identifica cada uno de los datos requeridos para que luego estos sean analizados, que consiste en la definición que se representa mediante el diccionario de datos

#### 4.1.1 Diseño Lógico de la Base de Datos

El objetivo del diseño lógico es convertir los esquemas conceptuales a locales en un esquema lógico global que se ajuste



al modelo de la base sobre la que se vaya a implementar el sistema.

#### **4.1.2 Metodología del Diseño lógico**

La metodología que se va a seguir para el diseño lógico del modelo relacional consta de dos fases, cada una de ellas compuesta por varios pasos:

1. Convertir y Validar los esquemas lógicos locales para cada vista de usuario
  - Convertir los esquemas conceptuales locales en esquemas lógicos locales, aquí se eliminan de cada esquema conceptual las estructuras de datos que los sistemas relaciones no modelan directamente: eliminar las relaciones muchos a muchos, revisar las relaciones uno a uno, eliminar las relaciones redundantes
  - Derivar un conjunto de relaciones y tablas para cada esquema lógico
  - Validar cada esquema mediante la normalización
  - Validar cada esquema frente a las transacciones
  - Dibujar el Diagrama de Entidad Relación
  - Definir las restricciones de Integridad

- Revisar cada esquema lógico

## 2. Convertir y evaluar el esquema lógico global

### **4.1.3 Metodología del Diseño Físico**

El objetivo de esta etapa es producir una descripción que incluye las estructuras de almacenamiento y los métodos de acceso que se utilizarán para conseguir un acceso eficiente a los datos. El diseño físico se divide en 4 fases cada uno de ellas compuestas por una serie de pasos.

#### 1. Traducir el esquema lógico global para el DBMS especificado

- Diseñar las relaciones y tablas para el DBMS específico
- Diseñar las reglas de negocio

#### 2. Diseñar la representación física

- Analizar las transacciones
- Escoger las organizaciones de tablas
- Escoger índices
- Considerar la introducción de redundancia
- Estimar la necesidad de espacio en disco duro

### 3. Diseñar los mecanismos de seguridad

- Diseñar la vista de los usuarios
- Diseñar la reglas de acceso

### 4. Monitorizar y afinar el sistema

## **4.2 Diccionario de Datos**

Es el encargado de reunir la información sobre los datos almacenados, sus descripciones, significados, restricciones, usos, etc.

## **4.3 La entidad –relación**

Se toma como punto inicial la existencia de entidades, que representa objetos, personas, etc, sobre las cuales se va almacenar información.


Las entidades con sus mismas características forman una entidad y las características para describir una entidad se les denomina atributo.

Con estos conceptos y la identificación de las entidades graficamos el modelo entidad/relación.

## **4.4 Seguridad**

Un sistema de monitoreo de red debe ser seguro, debido a que los administradores de la red tiene el control sobre la misma , es decir, si existe algún atacante y este tiene acceso al sistema, este tendrá acceso y control sobre toda la red,.

Por lo tanto, se hace imprescindible contar con un mecanismo en el que se pueda confiar a la hora de transmitir la información. Para brindar esta seguridad en el sistema se está utilizando el protocolo SSL permitiendo una autenticación, aislamiento de mensaje, e integridad Interoperabilidad. SSL/TLS, este protocolo trabaja con la mayor parte de browsers de Web.

Se sabe que el servidor está seguro porque en nuestro navegador se mostrará una llave o un candado , en la parte inferior derecha del Explorer.

## **4.5 Sistema**

Este sistema funciona sobre LINUX e interactúa con otros sistemas operativos con Windows, además de utilizar los protocolos SNMP y los servidores Sendmail, Apache, Tomcat .

## **4.6 Calidad del Sistema**

### **4.6.1 Calidad del Diseño**

El diseño del sistema se realizó con la participación del usuario, de tal forma permitiendo que el sistema se adapte a las necesidades

del usuario. La interfaz que se uso como botones y gráficos se la realizó con la finalidad de que esta sea amigable para el usuario.

El sistema va dirigido a usuarios expertos, ya que este debe tener conocimiento de administración de redes.

#### **4.6.2 Requerimientos**

1. Se realizo la Instalación de Linux (Fedora Core 4), en un computador el cual hará la función de Servidor. Además de instalar Linsux en un máquina virtual para que realice las funciones de cliente.
2. Se realizo las configuraciones de las interfaces de red tanto del Servidor (Linux), como en las Pc's que funcionaran como clientes en Windows y Linux, paras así poder tener una conexión que conforman la red.
3. Se procedió a realizar la configuración del protocolo SNMP, tanto en el servidor como en los clientes, logrando la arquitectura cliente /servidor con los elementos que maneja este protocolo. Esta configuración se la realiza tanto al servidor (Linux), como a los clientes (Windows y Linux).

4. En el servidor se deberá además configurar el DNS, Sendmail, Dovecot, MySQL, MRTG, Jdk para poder instalar el Apache con el Tomcat.
5. La Base de Datos que se utilizo para almacenar la información que genera el tráfico de red es MySQL, con la finalidad que esta información se guarde en las tablas correspondientes, para posteriormente acceder a ellas en el momento que se la solicite como es, cuando se generan los reportes.
6. Además debemos generar un certificado para brindar seguridad a la aplicación que se levanta en el browser.
7. A continuación se realiza la configuración del Servidor Web (Apache y Tomcat) en el Servidor (linux) para subir en un browser la aplicación.

## **4.7 Prueba del Sistema**

Para el buen funcionamiento del sistema se ha realizado una variedad de pruebas las cuales se explicara detalladamente a continuación:

### **4.7.1 Pruebas Técnicas**

- Realizar pruebas a través de ping para verificar la conexión entre las máquinas.
- Realizar prueba a través de la función snmpwalk para el envío y recepción de paquetes.
- Realizar pruebas a través de los diferentes comandos del protocolo snmp tanto en Windows Linux, para verificar las diferentes respuestas del sistema.
- Realizar pruebas a través del servidor sendmail, para verificar el envío de correo electrónico.

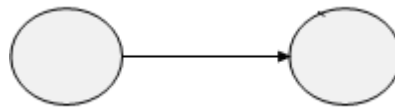
### **4.7.2 Prueba del Camino Básico**

Este modelo permite al diseñador obtener una visión de la complejidad lógica del diseño procedimental del sistema y obtener una guía para la definición de un conjunto básico de caminos de ejecución.

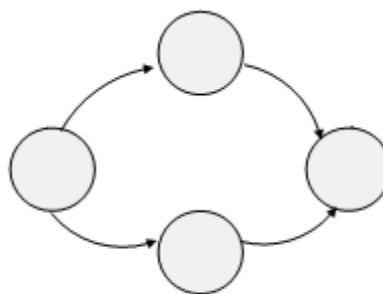
#### 4.7.2.1 Notación Gráfica de Flujo

Representa el flujo del control lógico del sistema.

**Secuencia.-** Es aquella en que una acción sigue a otra secuencia. Las tareas se suceden de tal modo que la salida de una es la entrada de la siguiente y así sucesivamente hasta el final del proceso. La Figura. , representa una estructura secuencial.

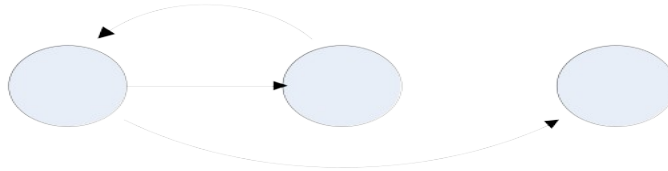


**If.-** Esta estructura, ejecuta una determinada acción cuando se cumple una determinada condición, si no se cumple no se realiza ninguna acción.

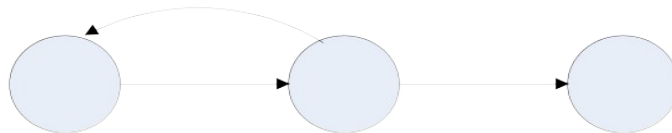




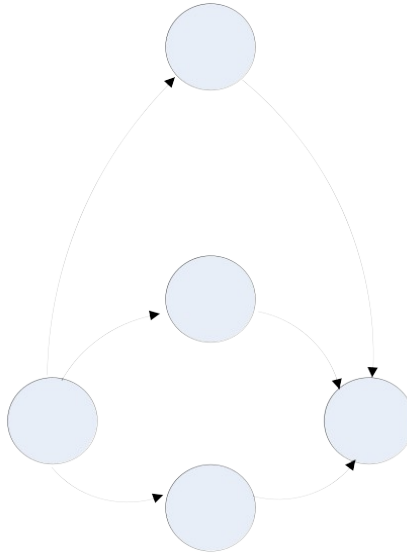
**While.-** El bloque de instrucciones se repetirá mientras que la condición sea cierta.



**Bucle (Hasta).-** En este tipo, el bloque de acciones se repetirá hasta que la condición sea cierta. La condición se evalúa al final de la estructura. Esto implica que el bloque de instrucciones se ejecutará al menos una vez, aunque la condición de salida ya sea cierta al entrar a dicha estructura.



**Case.-** La estructura de decisión múltiple evaluará una expresión que podrá tomar n valores distintos. Según elija uno de estos valores es la condición se realizará una acción.



#### **4.7.3 Prueba de la Base de Datos**

Nos permite ver si la Base de Datos satisface las necesidades de la aplicación, es decir, revisando los datos ingresados por la página o la información que se encuentra almacenada en ella para luego ser mostrada.

#### **4.7.4 Prueba de Acceso**

Se mide el nivel de seguridad del acceso al sistema con la validación del usuario con su respectiva clave que es encriptada, permitiendo de esta manera el acceso al sistema.

## **4.8 Riegos**

### **4.8.1 Riegos de gestión**

- Resultados no esperados en las pruebas.
- Atrasos en la implementación de las pruebas y desarrollo del sistema.

### **4.8.2 Riegos Técnicos**

- Instalación de Fedora Core 4 (LINUX) en la maquina virtual.
- Posibles fallas en la tarjeta de Red.
- Fallas al configurar el protocolo SNMP en Linux.
- Fallas al configurar el protocolo SNMP en Windows.
- Fallas en el cableado de la Red.
- Fallas al configurar el protocolo de seguridad SSL.
- Fallas al interactuar con la Base de Datos.
- Fallas al interactuar con el servidor Web Apache Tomcat 5

### **4.8.3 Riesgos enfocado al recurso humano**

- Los integrantes del grupo no cuentan con el mismo tiempo para desarrollar el software.
- Los desarrolladores deben capacitarse en las herramientas que deben utilizar.

# CAPITULO 5

## 5. IMPLEMENTACION

Para utilizar este sistema para monitorear el tráfico de red., es necesario que posea ciertos requerimientos para el funcionamiento del mismo. A continuación detallaremos el Hardware, Software y Recursos Humanos que debe de tener para la implementación del sistema.

En la pirámide se ilustra los recursos que intervienen en la implementación del sistema. En la base se encuentra Hardware y Software, que proporciona la infraestructura de soporte al esfuerzo de desarrollo, en el otro nivel se encuentra los componentes de software reutilizables, en la parte más alta las personas.

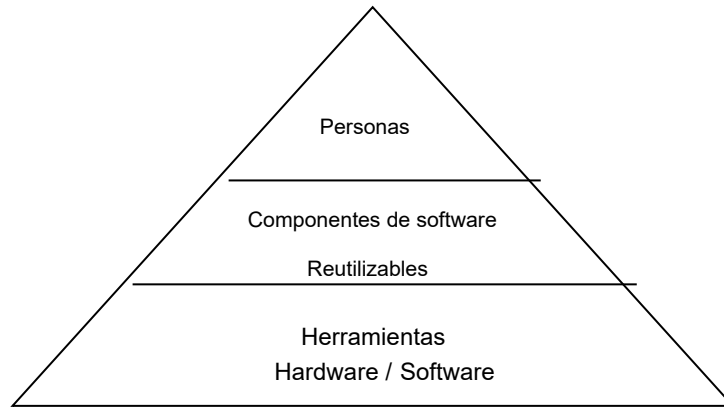


Fig. 5

### 5.1 Hardware

El Sistema a instalarse deberá contar con los siguientes equipos que tengan las siguientes características:

1. Si el servidor se instala en Windows:

- Pentium 3 o superior.
- Memoria Ram 512 MB
- Disco Duro de 80 GB
- Teclado
- Mouse

2. Si el servidor se instala en LINUX:

- Memoria Ram 256 MB
- Disco Duro como mínimo de 20 GB

- Teclado
- Mouse

## **5.2 Software**

### **1. Si el servidor se instala en Windows**

- Windows 2000 y XP
- Configuración del Servidor Web (Tomcat-5.59)
- Configuración de los Protocolos SNMP y MRTG
- Base de Datos MySql
- Java
- Configuración del Sendmail (Servidor de Correo)
- Configuración del DNS
- Configuración Apache y Tomcat
- Configuración del SSL.

### **2. Si el servidor se instala en LINUX**

- Fedora Core 4
- Configuración del Servidor Web (Tomcat-5.59)
- Configuración de los Protocolos SNMP y MRTG
- Base de Datos MySql
- Java
- Configuración del Sendmail (Servidor de Correo)

- Configuración del DNS
- Configuración del Apache y Tomcat
- Configuración del SSL

Cada uno de los clientes tiene que tener configurado el protocolo SNMP.

### **5.3 Humano**

El sistema para su utilización requiere del siguiente recurso humano:

- Usuarios que estén ingresado al sistema.
- Administrador de la red: responsable directo del buen funcionamiento del sistema

Tipo de información que manejan:

- Usuarios: ingresa al sitio web, con su respectiva clave y podrán visualizar el tráfico de la red.
- Administrador de la Red: Persona responsable de la información que genera el Monitor de Red, como de los dispositivos que se encuentran conectados en la Red.

Es de indicar que el administrador de la red debe ser un usuario experto ya que este debe tener conocimientos de administración de redes.

#### **5.4 Infraestructura**

La infraestructura con que se debe de contar para el buen funcionamiento del sistema, es tener una red de área local (LAN).

Esta Red debe de estar conformada como mínimo de tres computadoras, una de ellas cumpliendo la función de servidor en la cual estará instalado el Monitor de Red que permitirá visualizar el tráfico de red que generen las otras.



# CAPITULO 6

## 6. CONCLUSIONES Y RECOMENDACIONES

### 6.1. Conclusiones

Las conclusiones que se llegaron al término del proyecto fueron:

- La implementación del software desarrollado deberá ser utilizado en una red de área local, permitiendo tener en el menor tiempo posible resultados sobre el tráfico que genera la red.
- El Monitor de Red nos dará información en tiempo real de cada uno de los clientes (nodos) al momento de solicitarla.
- Este software va dirigido a usuarios expertos que tengan conocimiento sobre administración de redes.
- El Monitor de Red cuenta con mensajes de alertas en el momento en que se encuentra inactiva alguna nodo de la red.
- La utilización de este software permitirá al administrador de la red, tomar decisiones y resolver problemas referentes al tráfico de red obteniendo así una red eficiente.

## **6.2. Recomendaciones**

Entre las recomendaciones hechas en este proyecto son:

- Promocionar este software a las Empresas e Instituciones que cuenten con una red.
- A los administradores de una red, deben contar con un software que lo mantenga informado sobre los dispositivos de la red para mantener una red eficiente.
- La computadora que funcione como servidor de preferencia debe tener sistema operativo LINUX.

## GLOSARIO DE TERMINOS

**Agente.-** Software que ejecuta una serie de tareas automáticamente sin necesidad que el usuario esté presente. Proceso de comunicación cliente/servidor que maneja la negociación entre cliente y el servidor.

**Protocolo.-** Un protocolo es un método establecido de intercambiar datos en Internet. Un protocolo es un método por el cual dos ordenadores acuerdan comunicarse, una especificación que describe cómo los ordenadores hablan el uno al otro en una red.

**SNMP.-** (Protocolo Simple de administración de redes). Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la suite de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

**MIB.-** (Management Information Base). Base de información de administración. Grupo de elementos nombrados que entiende un agente SNMP. Para supervisar o controlar una computadora remota, el administrador debe obtener o almacenar valores en variables MIB.

## BIBLIOGRAFIA

1. Sistema Linux  
[www.linuxparatodos.net/](http://www.linuxparatodos.net/) -
2. Funcionamiento y Configuración de SNMP en Linux  
[www.linuxparatodos.net/portal/staticpages/index.php?page=como-linux-snmp](http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-linux-snmp)
3. Funcionamiento y Configuración de SNMP en Windows  
[www.microsoft.com/windows/windows2000/es/server/help/snmp\\_service\\_start\\_stop.htm](http://www.microsoft.com/windows/windows2000/es/server/help/snmp_service_start_stop.htm)
4. Funcionamiento y Configuración del MRTG  
[www.mrtg.jp/en/es\\_es/](http://www.mrtg.jp/en/es_es/) - 26k
5. Funcionamiento de la Base (MIB)  
[http://es.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol)
6. MySql  
<http://dev.mysql.com/doc/refman/5.0/es/index.html>

# **MANUAL TECNICO**

## 1. CONFIGURAR SNMP

### 1.1. En Linux

#### Listas de Control de Acceso

Se deben crear las listas de control de acceso (ACL) correspondientes en el fichero `/etc/snmp/snmpd.conf` y que servirán para definir quien tendrá acceso hacia el servicio `snmpd` que se instala por defecto. Lo más recomendable es crear un fichero nuevo y cambiarle el contenido.

Se debe crear un lista de control de acceso en la que se definirá quien tendrá acceso al servicio `snmpd`. A una de estas listas se le otorgará permiso de acceso de lectura y escritura para lo que sea necesario y a la otra de solo lectura. Por razones de seguridad solo la interfaz `127.0.0.1` será la de lectura escritura. Se otorgará permiso de acceso de solo lectura a una red o bien a una IP en la otra lista de control de acceso (ACL).

```
com2sec local      localhost      public
com2sec redlocal  192.168.1.0/24 public
```

En lo anterior la primera línea significa que habrá una lista de control de acceso denominada «local» y que corresponderá solo a 127.0.0.1/32, asignando publica como clave de acceso. La segunda línea hace lo mismo pero definiendo a la red 192.168.1.0/24. Se puede definir lo que uno guste mientras no sea la clave de root, esto porque dicha clave se transmite a través de la red en forma de texto simple (es decir, sin cifrar).

### **Definición de Grupos**

Se van a crear dos grupos: MyRWGroup y MyROGroup. El primero será un grupo al que se asignarán más adelante permisos de lectura escritura y el segundo será un grupo al que posteriormente se asignarán permisos de solo lectura. Por cada grupo se asignan tres líneas que especifican el tipo de acceso que se permitirá en un momento dado a un grupo en particular. Es decir, MyRWGroup se asocia a local y MyROGroup a miredlocal.

```
#Se asigna local al grupo de lectura escritura
##group.name sec.model sec.name
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
```

```
#Se asigna redlocal al grupo de solo lectura
##group.name sec.model sec.name
group MyROGroup v1 redlocal
group MyROGroup v2c redlocal
group MyROGroup usm redlocal
```

### **Ramas Predeterminadas**

Se especifican las ramas que se van a permitir ver a través del servicio.

Lo más común, para, por ejemplo, utilizarse con MRTG, es lo siguiente:

```
#Ramas permitidas para ver a traves del servicio
## name incl/excl subtree mask(optional)
view all included .1 80
```

### **Permisos a los grupos**

Se debe especificar que permisos tendrán los dos grupos, MyROGroup y MyRWGroup. Son de especial interés las últimas columnas.



```
#Permisos a los grupos

## group      context sec.model sec.level prefix read write notif
access MyROGroup ""    any    noauth    exact  all  none  none
access MyRWGroup ""    any    noauth    exact  all  all   all
```

### Parámetros de carácter informativo

Se definen dos parámetros de carácter informativo para que cuando utilicen aplicaciones cliente como MRTG se incluya algo de información acerca de que sistema se está accediendo

```
#Parametros de caracter informativo

syslocation Servidor Linux Adela_linux
syscontact  Administrador (adela_mj@hotmail.com)
```

**Si es necesario añadir más equipos para que accedan al servicio snmp, solo hay que hacer lo siguiente:**

1. Agregar una ACL con un nombre único. Ejemplo

```
com2sec micuenta 192.168.1.251 public
```

2. Agregar un juego reglas que asignen al grupo, en este caso **micuenta**, con lo siguiente:

```
group    otrogrupo v1    local
group    otrogrupo v2c   local
group    otrogrupo usm   local
```

3. Agregar una línea donde se establece que permisos tendrá el grupo **otrogrupo**. Va a ser de solo lectura:

```
access MyROGroup "" any noauth exact all none none
```

### **Iniciar el servicio y añadirlo a los servicios de arranque del sistema**

Inicie el servicio de SNMP y añada éste al resto de los servicios que arrancan junto con el sistema:

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

## Comprobaciones

Suponiendo que sea signó como clave de acceso public en un sistema cuya dirección IP es 192.168.1.8, para probar si la configuración funciona, solo hay que ejecutar los dos siguiente mandatos a fin verificar que devuelvan información acerca del sistema consultado.

```
snmpwalk -v 2 192.168.1.8 -c public system  
snmpwalk -v 2 192.168.1.8 -c public interfaces
```

### 1.2. En Windows

#### Para instalar el servicio SNMP

Se debe abrir el Asistente para componentes de Windows, se debe dar clic en Inicio, Panel de Control, doble clic en Agregar o Quitar Programas y a continuación en Agregar o Quitar componentes de Windows.

1. Asistente para **componentes** de Windows.
2. En la pantalla de componentes hacer clic en **Herramientas de administración y supervisión**, luego en **Detalles**.
3. Activar la casilla de verificación **Protocolo simple de administración de redes**, clic en aceptar.
4. Dar clic en siguiente

### **Configurar las propiedades del Agente**

Se debe ingresar al Administrador de Equipos, dar clic en **Inicio, Panel de Control**, doble clic en **Herramientas administrativas**, y luego en **Administración de Equipos**.

1. Abrir el administrador de equipos
2. Dar clic en Servicios y Aplicaciones
3. Luego en Servicios
4. Dar clic en **Servicios SNMP**
5. En el menú **Acción**, clic en **Propiedades**
6. En la ficha **Agente**, en el **Contacto**, escribir el nombre del usuario.
7. En **Ubicación**, escribir la ubicación física del equipo.
8. En **Servicio** activar las casillas de verificación y dar clic en **Aceptar**.

### **Configurar capturas**

Para ingresar en Administración de Equipos, dar clic en **Inicio, Panel de Control**, doble clic en **Herramientas Administrativas** y luego en **Administración de Equipos**.

1. Abrir Administrador de Equipos.
2. Dar clic en **Servicios y Aplicaciones**

3. Dar clic en **Servicios**.
4. En el menú **Acción**, clic en Propiedades.
5. En **Capturas, Nombre de Comunidad**, escribir el nombre de comunidad a la que el equipo enviará los mensajes de captura, luego dar clic en **Agregar a la lista**.
6. **Destinos de capturas**, hacer clic en Agregar.
7. En **Nombre, Dirección IP o IPX del host**, escribir la información del host y hacer clic en Agregar.
8. Realizar los mismos pasos si se desea ingresar más comunidades.

## 2. CONFIGURACION DEL DNS

- rpm – qa bind
- cd /etc/
- vi named.conf

Copiar el bloque que a continuación se detalla zone “localhost”,l luego editar zone “ncs.com”

```
zone "ncs.com" IN {

    type master;

    file "ncs.com.zone";
```

```
allow-update { none ;};
```

```
};
```

```
wq
```

- slocate localhost.zone
- / var/named/chroot/var/named/localhost.zone
- /var named/localhost.zone
- cd /var/named/:

Copiar el contenido del al destino sino existe se lo crea

- cp localhost.zone ncs.com.zone
- vi ncs.com.zone

Se edita el bloque que a continuación se detalla:

```
IN SOA www.ncs.com. Root.ncs.com.(
```

```
42 ; serial (d.adams)
```

```
3H ; refresh
```

```
15M ; retry
```

1W ; expiry

1D) ; minimum

IN NS ncs.com

Localhost IN A 127.0.0.1

Ncs IN A 192.168.1.1

www IN CNAME ncs

wq:

- name ] cp ncs.com.zone /var/named/chroot/var/named
- name ] cd /etc/
- etc ] resolv.conf

Se edita lo siguiente

nameserver 192.168.1.1

search localhostdomain

.wq

- etc ] service network restart
- etc ] service named Stara

- etc ] service named status
- etc ] ping [www.ncs.com](http://www.ncs.com)
- etc ] netconfig

Dirección IP

192.168.1.1    Mascara de Red : 255.255.255.0

Puerta de enlace predeterminada (IP): .....

Servidor de nombre primario:                    192.168.1.1.

- etc ] service network restart
- etc ] service named restart
- etc ] ping [www.ncs.com](http://www.ncs.com)

### 3. CONFIGURACION DEL SERVIDOR

Crear la carpeta:

- mkdir /var/www/sitio
- rpm -qa httpd
- cd /etc/
- etc ] cd /httpd/conf
- etc ] vi httpd.conf

Descomentar las siguientes lineas



Listen 80

ServerAdmin root@localhost

DocumentRoot “ /var/www/html/ ”

DirectoryIndex index.html index.html.var

Copiar el ultimo bloque y modificarlo:

</ VirtualHost \*: 80>

ServerAdmin [root@localhost.localdomain](mailto:root@localhost.localdomain)

ServerName [www.ncs.com](http://www.ncs.com)

</VirtualHost>

wq:

- conf ] service httpd start
- conf ] service httpd status

Probar el buscador del servidor

http:// [www.ncs.com](http://www.ncs.com)

Configurar la conexión de red, puerta de enlace y el DNS con e IP del servidor de LINUX.

En el navegador cambiar en herramientas, opciones de Internet, conexiones, configuraciones LAN, marcar la opción detectar automáticamente IP y cargar el sitio [http:// www.ncs.com/](http://www.ncs.com/)

#### 4. CONFIGURACION DE SENDMAIL

- etc ] rpm -qa sendmail

La instrucción que a continuación se detalla nos permite ver todos los puerto abiertos en el servidor, en este caso el puerto 53 DNS.

- etc ] netstat -an | more
- etc ] rpm -qa dovecot
- etc ] vi dovecot.conf

En el archivo se procede a descomentar la linea siguiente:

```
Protocols = imap imaps pop3
```

```
wq:
```

- etc ] service dovecot start
- etc ] netstart -an | more
- etc ] vi rc.local
- cd /mail/
- mail ] vi sendmail.cf

- Buscar la linea # local info #
- Insertar la linea gmail.com
- Buscar la linea # Cw localhost
- Editar la linea:
- Cwgmai.com
- Modificar O DaemonPortOptions = Port = smtp.Addr= 127.0.0.1, Name = MTA por O DaemonPortOptions = Port = smtp.Addr= 0.0.0.0, Name = MTA

wq:

- mail ] service sendmail start
- mail ] service xinetd restart
- Me permite levantar los subsistemas actualizando todos los servicios y protocolos del servidor.
- cd /etc/sysconfig/
- sysconfig ] vi network

working = yes

hostname = gmail.com

- netstat -an | more
- service xinetd restart
- service sendmail restart

- vi host

Modificar el siguiente bloque

```
127.0.0.1    localhost.localdomain localhost
```

```
127.0.0.1    gmail.com    gmail
```

- cd /etc/xinetd.d/
- vi krb5-telnet

Modificar: disable = no

wq:

- xinetd ] service xinetd restart
- adduser grupo12
- passwd grupo12
- mail grupo12.
- Subjetc: Prueba.
- Cc:
- enter
- reboot

## **5. INSTALAR TOMCAT- 5.59**

El Tomcat es un servidor de aplicaciones que sirve como contenedor de servlets y JavaServerPages. El Tomcat necesita del JDK, para lo cual detallamos a continuación su instalación:

### 5.1. Instalar JDK

Descargamos la versión jdk-1.5.bin

La copiamos dentro de Linux en /tmp/

Damos permiso de ejecución :

```
chmod +x jdk-1_5-linux- i586.bin
```

Se crea una estructura jdk1.5.0 la cual se la mueve a:

```
mv jdk-1.5_04/ /usr/local/jdk1.5
```

Se configura las variables de entorno y se las agrega /etc/profile:

```
export JAVA_HOME=/usr/local/jdk1.5  
export JRE_HOME=${JAVA_HOME}/jre  
export PATH=$PATH:${JAVA_HOME}/bin
```

### 5.2. Instalar Tomcat

Descargar Tomcat-5.59

Se copia el archivo dentro de /tmp/

Descomprimir la estructura:

```
tar xvfz jakarta-tomcat – 5.59.tar.gz
```

Se mueve dentro de /usr/local como el JDK

```
mv jakarta-tomcat5.59 /usr/local/tomcat-5.5.9
```

Ejecutamos el tomcat

```
/usr/local/tomcat-5.5.9/bin/startup.sh
```

Se asignas variables de entorno dando como resultado:

```
Using CATALINA_BASE: /usr/local/tomcat5.5.11  
Using CATALINA_HOME: /usr/local/tomcat5.5.11  
Using CATALINA_TMPDIR: /usr/local/tomcat5.5.11/temp  
Using JRE_HOME: /usr/local/jdk1.5/jre
```

Se procede abrir el navegador por el puerto 8080

### 5.3. Tomcat con Apache

Para que apache sea el que reciba las peticiones de JSP y servlets hay que agregar un modulo dentro de apache, el cual estará encargado de realizar la comunicación con el Tomcat :

Se descarga la versión jakarta-tomcat-connectors-jdk-2.2.0.4 –src.tar .gz

Se copia el archivo dentro de /tmp/

Descomprimos el archivo:

```
tar xvfz jakarta-tomcat-connectors-jk2-2.0.4-src
cd jakarta-tomcat-connectors-jk2-2.0.4-src/
cd jk/
cd native2/
```

Se realiza la siguiente configuración para su ejecución:

```
LDFLAGS= -lc ./configure --with-apache2=/usr/local/http --with-
apxs2=/usr/local/http/bin/apxs --with-java-home=/usr/local/jdk1.5
```

/usr/local/http	Aqui se encuentra instalado el apache
/usr/local/jdk1.5	Aquí se instala el jdk

Se procede a compilar

```
make
```

Se copia el modulo que esta en la siguiente ruta de la cual es el resultado de la compilación:

```
jakarta-tomcat-connectors-jk2-2.0.4-src/jk/ build/jk2
/apache2/mod_jk2.so
```

Se copia en la siguiente carpeta:

```
cp mod_jk2.so /usr/local/http/modules
```

```
S LoadModule jk2_module modules/mod_jk2.so

<IfModule mod_jk2.c>
    JkSet2 channe.socket:localhost:8009 info "socket de  AJP13"
    JkSet2 status: info "Status"
    JkSet2 workerEnv: logger loger.file:0

    <Location "/jsp/examples">
        JkUriSet group lb:lb
        JkUriSet info "Ejemplos de  jsp"
    </Location >

    Location "tomcat-docs">
        JkUriSet group lb:lb
        JkUriSet info "Documentación de tomcat"

    </Location >
```



Se prueba en la dirección que se detalla:

<http://192.168.1.1/jsp-examples/>

## 6. INSTALAR MYSQL

Verificar en Linux si se encuentra instalado el MySql con el siguiente comando:

```
rpm -qa mysql
```

Si no se encuentra instalado, descargar el archivo e instalarlo.

```
rpm -hiv mysql-4.1.11-2.i386.rpm
```

Se procede agregar a MySql a los niveles de corrida 3. 4 y 5.

```
/sbin/chkconfig --level 345 mysqld on
```

Procedemos a ingresar al shell del mysql con la siguiente instrucción:

```
mysql
```

Se ingresa a la Base de Datos a utilizar.

```
> use mysql;
```

Se muestran la tablas existentes

```
> show tables;
```

Se muestra el contenido de la tabla user

```
> select * from user;
```

Se asigna una contraseña al usuario root

```
> update user set Password=PASSWORD ('nuevo_password') where  
user= 'root';
```

Se ejecuta el siguiente comando para visualizar el usuario con su respectiva clave.

Se refrescan los privilegios para que se actualicen los cambios.

```
> flush privileges
```

Se procede a salir del shell para comprobar los datos ingresados

```
> quit
```

Se ingresa a un nuevo shell

```
mysql
```

Al momento de volver ingresar se mostrara un mensaje de error

```
ERROR 1045: Access denied for user: 'root@localhost' (Using  
password: NO)
```

A continuación se añade el usuario (-u root), solicitando una contraseña (-p).

```
mysql -u root -p
```

Luego le solicitara ingresar una contraseña, con la cual ingresara al shell de Mysql.

Se procede a crear la Base de Datos que se utilizara.

Para crear la base de datos se utiliza el mandato mysqladmin con el parámetro create.

```
mysqladmin -u root -p create dbejemplo
```

Para eliminar la Base de Datos se utiliza el parámetro drop.

```
mysqladmin -u root -p drop dbejemplo
```

Para otorgar permisos a otros usuarios se realiza la siguiente instrucción:

Se ingresa a la base de datos

```
mysqladmin -u root -p create dbejemplo
```

Se ingresa al shell de Mysql y se ejecuta la instrucción que se detalla a continuación en la que se indicara los permisos que tendrá cada usuario.

```
GRANT select, insert, update, create, alter, delete, drop ON directorio.*  
TO jbarrios@localhost IDENTIFIED BY 'password_del_usuario_jbarrios';
```

Al concluir se tendrá una Base de Datos desde otro equipo que podrá ser utilizada y modificada por el usuario que cuente con los permisos indicados.

## 7. GENERAR UN CERTIFICADO

Generar un almacén de firmas, denominado jvstore, con una entrada denominada firma1 que será la que servirá

Se solicitarán dos claves: una para el almacén de firmas y la otra como clave secreta de la firma.

Pueden ser ambas la misma. También se solicitarán los datos personales del firmante.

```
keytool -gentey -alias firma1 -keystore jvstore
```

Extraer el certificado del almacén de firmas (exportar) y depositarlo en un fichero .cer.

Este certificado contiene la clave pública del emisor de la firma.

```
Keytool -export -keystore jvstore -alias firma1 -file GRUPO12 cer
```

## 8. CONFIGURACION DEL MRTG

El primer paso es verificar que están instalados los paquetes del mrtg, lo hacemos con la siguiente instrucción:

```
rpm -aq mrtg
```

Si no aparece nada procedemos a buscar en los cd's de instalación o descargar el paquete mrtg de Internet en la página [www.rpmfind.com](http://www.rpmfind.com)

Luego de esto nos dirigimos a la ruta `cd /etc/mrtg` y observaremos que se ha creado un archivo `mrtg.cfg` el mismo que vamos a modificar pero primero debemos respaldarlo:

```
cp mrtg.cfg mrtg.cfg.resp
```

Luego, dentro del mismo directorio de mrtg procedemos a ejecutar lo siguiente pero primero deberemos crear el directorio en donde se guardaran las paginas html (Workdir):

```
cfgmaker \
--global "workdir:
/usr/local/tomcat-5.5.9/webapps/paginas/estadistica/maq_linux.htm" \
--global "Options [ ]: bits, growright" \
--output /etc/mrtg/mrtg192.168.1.1.cfg \ public@192.168.1.1
```

A continuación ejecutamos la siguiente línea:

```
env LANG=C mrtg /etc/mrtg/mrtg192.168.1.1.cfg
```

Para comprobar si esta todo correcto nos dirigimos a la dirección que hemos puesto en el Workdir y ejecutamos la pagina `maq_linux.htm` y podremos observar que se ha creado 4 gráficos en la cual se pueden ver el tráfico de nuestra máquina, pero esperar 5 minutos para ver los resultados.

Ahora, si queremos añadir varios gráficos entramos en el archivo `mrtg192.168.1.1.cfg`

y ponemos las siguientes líneas en el caso de supervisar una máquina en Linux:

```
### TCP ABIERTOS ###  
Target[arpanet.tcp]: .1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:public@192.16  
8.0.5  
RouterUptime[arpanet.tcp]: public@192.168.0.5  
Options[arpanet.tcp]: nopercent,growright,gauge  
Title[arpanet.tcp]: Conexiones TCP abiertas  
PageTop[arpanet.tcp]: <h1>Conexiones TCP abiertas</h1>  
MaxBytes[arpanet.tcp]: 1000000  
YLegend[arpanet.tcp]: Conexiones  
ShortLegend[arpanet.tcp]: Conexiones  
LegendI[arpanet.tcp]: Conexiones:  
LegendO[arpanet.tcp]:  
Legend1[arpanet.tcp]: Conexiones TCP abiertas
```



### ### MEM LIBRE INFO ###

Target[arpanet.mem]: .1.3.6.1.4.1.2021.4.6.0&.1.3.6.1.4.1.2021.4.6.0:public@192.168.0.5

RouterUptime[arpanet.mem]: public@192.168.0.5

PageTop[arpanet.mem]: <h1>RAM Libre</h1>

Options[arpanet.mem]: nopercent,growright,gauge

Title[arpanet.mem]: RAM Libre

MaxBytes[arpanet.mem]: 1000000

kMG[arpanet.mem]: k,M,G,T,P,X

YLegend[arpanet.mem]: bytes

ShortLegend[arpanet.mem]: bytes

LegendI[arpanet.mem]: RAM libre:

LegendO[arpanet.mem]:

Legend1[arpanet.mem]: RAM libre, no incluye la swap, en bytes

### ### SWAP INFO ###

Target[arpanet.swap]:

memAvailSwap.0&memAvailSwap.0:public@192.168.0.5

RouterUptime[arpanet.swap]: public@192.168.0.5

PageTop[arpanet.swap]: <h1>Swap Libre</h1>

Options[arpanet.swap]: nopercent,growright,gauge

Title[arpanet.swap]: Swap Libre

MaxBytes[arpanet.swap]: 1000000

kMG[arpanet.swap]: k,M,G,T,P,X

YLegend[arpanet.swap]: bytes

ShortLegend[arpanet.swap]: bytes

LegendI[arpanet.swap]: Swap Libre:

LegendO[arpanet.swap]:

Legend1[arpanet.swap]: Swap libre, en bytes

Y ejecutamos el indexmaker

```
indexmaker /etc/mrtg/maq_linux.cfg >  
/usr/local/tomcat-5.5.9/webapps/paginas/estadisticas
```

## 9. Casos de Uso

El caso de uso es una estructura que ayuda a los analistas a trabajar con los usuarios para determinar la forma en que se usará el sistema. Con una colección de casos de uso se puede hacer el bosquejo de un sistema en términos de lo que los usuarios intenten hacer con él. Este tipo de análisis es importante para la fase de análisis y desarrollo de un sistema. La forma en que los usuarios utilicen un sistema le da la pauta para lo que diseñara y creara.

Un caso de uso es una manera específica de utilizar el sistema que se está analizando.

Los elementos que intervienen en el caso de uso son:

**Usuario:** Es una casuística concreta dentro de un caso de uso

**Actor:** Representa un papel interpretado por una persona o cosa que interactúa con el sistema.

**Relaciones:** Interacciones entre los distintos elementos

## Usuario



Fig. 1

Cada escenario describe una secuencia de eventos. Cada secuencia se inicia por una persona.

El actor en este caso es el usuario que desea visualizar la Red. Esto iniciará cuando el usuario ingrese al sistema, ingrese la contraseña y visualice la información. Además también puede solicitar información específica o generar reportes.

## Visualizador



Fig. 2

El actor es el visualizador que me permitirá validar la contraseña, generar alertas, generar reportes, enviar correos al generarse alertas, presentar la información y guardarla.

## Agente

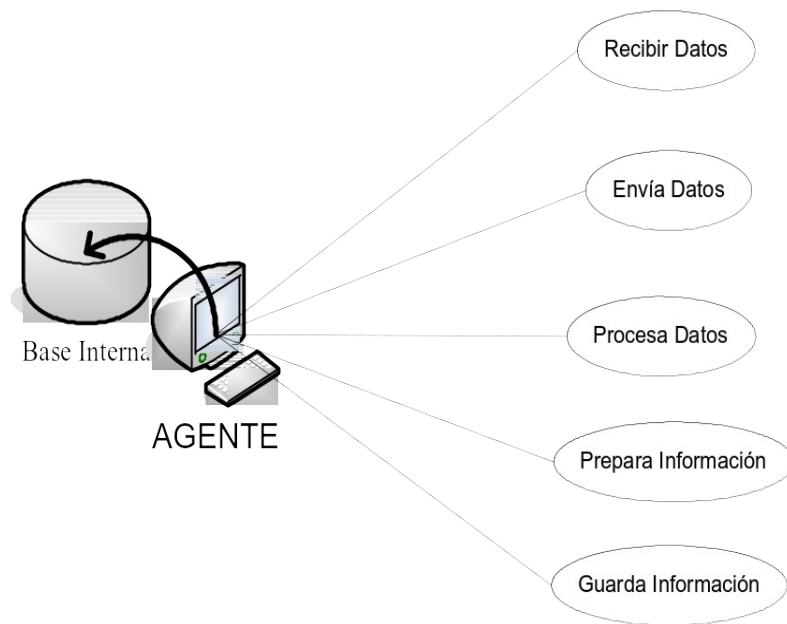


Fig. 3

El actor es el agente que me permitirá recibir, enviar y procesar los datos en la Pc que esta instalado además de preparar y guardar la información de la misma.

## 10. Diccionario de Datos

El Diccionario de Datos me permite describir el contenido de los objetos definidos durante el análisis.

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: Usuarios			Tipo: Maestra
Descripción: En esta se almacenara los usuarios que tendrán acceso al sistema del Monitor de Red			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
ID_USUARIO	Numero de Identificación	int	11
NOMBRES	Nombre del Uusario	varchar	200
APELLIDOS	Apellidos del Usuario	varchar	200
TELEFONO	Teléfono del Usuario	varchar	15
NOMBRE_USUARIO	Nombre que distingue al usuario	varchar	20
EMAIL	Correo electrónico	varchar	200
TIPO_USUARIO	Tipo de usuario (Administrador /Usuario)	varchar	3
ESTADO	Si se encuentra activo o inactivo	varchar	1
OBSERVACION	Tipo de usuario (Administrador /Usuario)	varchar	2000

Tabla. 1.

MONITOR DE RED	
Base de Datos: MySql	
Nombre de la Tabla: Usuario_dat	Tipo: Maestra

<b>Descripción:</b> Se almacenará los usuarios con su respectiva clave encriptada para validar el ingreso al sistema.			
<b>Descripción de los Registros</b>			
<b>Campo</b>	<b>Descripción</b>	<b>Tipo de Dato</b>	<b>Longitud</b>
ID_USUARIO	Numero de Identificación	varchar	50
ID_CLAVE	Clave de acceso al sistema	varchar	200
TIPO_USUARIO	Tipo de usuario (Administrador /Usuario)	varchar	3
FEC_CREACION	Fecha de Creación del Usuario	datetime	
FEC_REGISTRO	Fecha de registro	datetime	
N_INTENTOS	Intentos de Ingreso al sistema	int	11

Tabla 2.

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: IP			Tipo: Maestra
Descripción: Se ingresan las Ip con su respectivo sistema operativo de las Pc que se encuentran conectadas en la Red.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	Numero de IP	varchar	15
DESCRIPCION	Descripción	varchar	45
ESTADO	Tipo de usuario (Administrador /Usuario)	varchar	1
SISTEMA_OPERATIVO	Sistema Operativo que tiene instalado la PC	varchar	20

Tabla. 3

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: IF_NODOS		Tipo: Maestra	
Descripción: Almacena la información que se muestra en la pantalla principal de todos los nodos que se encuentran en la red.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
ID_DISPOSITIVO	Número de identificación	varchar	20
IP	IP que tiene cada nodo	varchar	15
SIST_OPERATIVO	Sistema Operativo instalado en PC	varchar	20
ID_USUARIO	Nombre del usuario	varchar	15
ESTADO	Si se encuentra activo o inactivo	varchar	1

Tabla. 4

MONITOR DE RED	
Base de Datos: MySql	
Nombre de la Tabla: COMANDOS_SNMP	Tipo: Maestra



<b>Descripción:</b> Tiene almacenado OID de los comandos que utiliza el snmpwalk para capturar la información del tráfico de red.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
NOMBRE	Nombre del Comando	varchar	50
DESCRIPCION	Descripción de la función del comando	varchar	260
ID_COMANDO	Número que identifica al comando	varchar	50
ESTADO	Estado	varchar	1
TABLA		varchar	20

Tabla 5.

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: APLICACIONES		Tipo: Maestra	
Descripción: Se registrarán las aplicaciones que se muestran en el sistema de cada nodo, y que se utilizarán para los reportes posteriormente.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	IP del nodo	varchar	15
DESCRIPCION	Aplicaciones que se mostraron	varchar	100
FECHA	Fecha en que se monitoreo	datetime	

Tabla 6.

MONITOR DE RED	
Base de Datos: MySql	
Nombre de la Tabla: ICONO_APLICACIONES	Tipo: Maestra
Descripción: Contiene los iconos de las aplicaciones para presentarlos en el sistema.	

Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
APLICACIÓN	Nombre de la Aplicación	varchar	30
DESCRIPCION	Descripción de Aplicación	varchar	45
ICONO	Gráfico de la Aplicación	varchar	30

Tabla. 7.

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: SERVICIOS			Tipo: Maestra
Descripción: Contiene los servicios que se encuentran iniciados en cada Pc cuando fueron monitoreados.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	IP de la máquina monitoreada	varchar	15
DESCRIPCION	Descripción de los servicios	varchar	300
FECHA	Fecha en que fue monitoreada la máquina	datetime	

Tabla. 8

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: DISPOSITIVOS_LOGICOS		Tipo: Maestra	
Descripción: Contiene los dispositivos lógicos que se encuentran conectados a su respectiva Pc.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud

IP	IP de la máquina monitoreada	varchar	15
NOMBRE	Dispositico (A:, C:, E:, etc)	varchar	20
DESCRIPCION	Nombre del Dispositico (A:, C:, E:, etc)	varchar	30
VOLUMEN	Volumen del Dispositivo	varchar	40
TAMAÑO	Capacidad de cada dispositivo.	varchar	15
ESPACIO_LIBRE	Capacidad libre del dispositivo	varchar	15
FECHA	Fecha en que fue monitoreada la máquina	datetime	

Tabla. 9

MONITOR DE RED			
Base de Datos: MySql			
Nombre de la Tabla: SISTEMA			Tipo: Maestra
Descripción: Contiene los datos del sistema como nombre del sistema operativo, numero de aplicaciones, Memoria, Capacidad del Disco Duro, etc.			
Descripción de los Registros			
Campo	Descripción	Tipo de Dato	Longitud
IP	IP de la máquina monitoreada	varchar	15
NOMBRE_EQUIPO	Nombre del Dispositico (A:, C:, E:, etc)	varchar	200
DESCRIPCION	Fecha en que fue monitoreada la máquina	varchar	40
SISTEMA_OPERATIVO	Sistema Operativo Instalado (Linux, Windows)	varchar	40
NUM_PROGRAMA	Número de Programas Abiertos	varchar	3
TIEMPO	Tiempo que esta el servicio SNMP iniciado	varchar	30
FECHA	Fecha en que fue monitoreada la máquina	datetime	

Tabla. 10

# **MANUAL DE USUARIO**

A continuación se mostrará un manual en el cual se indicará el manejo del Monitor de Red Seguro, es decir, el funcionamiento de los botones y accesos a las páginas de consulta.

### Pantalla Principal (Acceso al Sistema)

Es la primera pantalla que se muestra cuando se accesa al sistema, aquí se ingresará el username y el password respectivo, de los usuarios autorizados para manejar el Monitor de Red

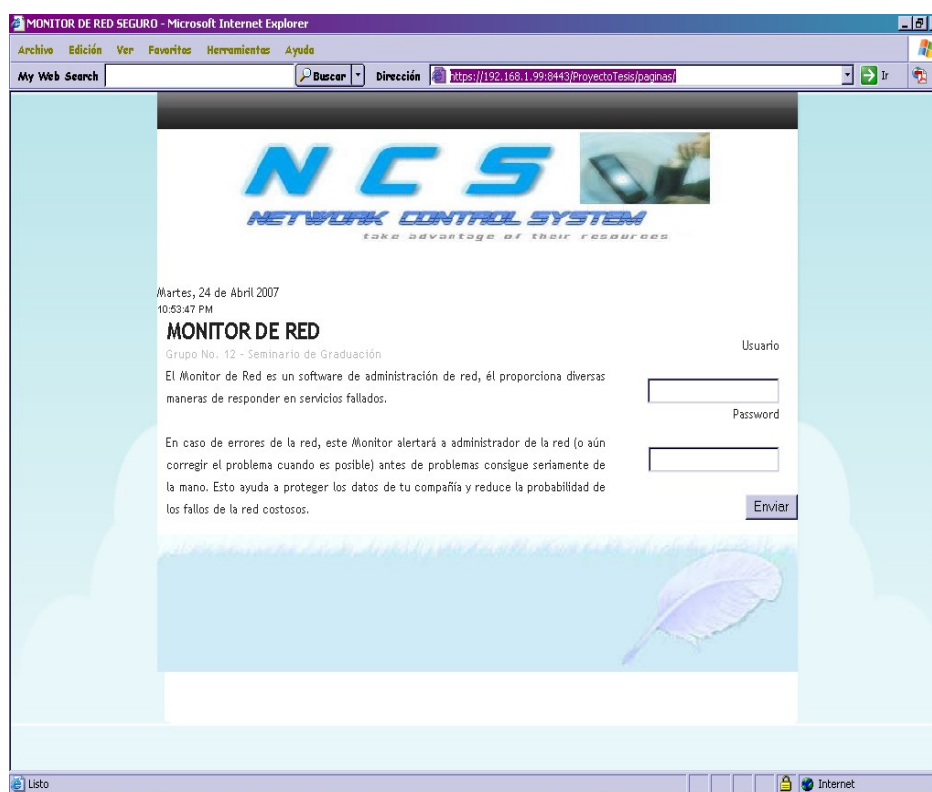


Fig. 4

En esta pantalla se podrá apreciar que la clave ha sido encriptada para el respectivo ingreso al sistema, brindando seguridad al acceso de la aplicación.

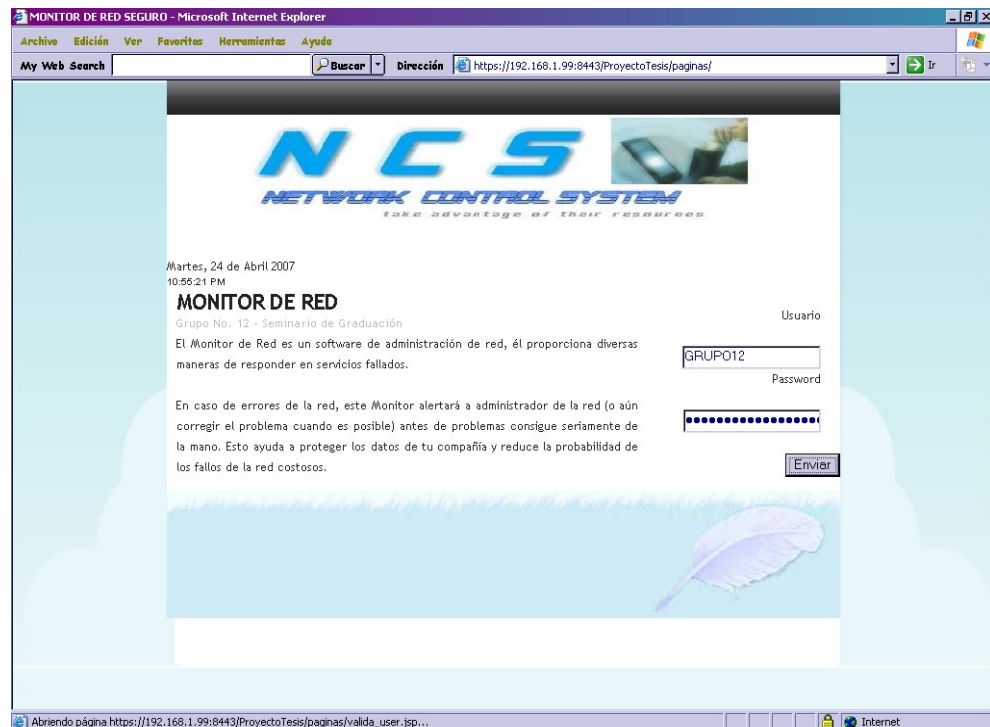


Fig. 5

## Barra de Menú

Se podrá apreciar un barra de menú en la cual se mostrará el acceso a la configuración donde se desplazara un submenu, par el ingreso de la IP de los dispositivos que conformarán parte de la red, como de los usuarios que tendrán acceso al sistema. Además del ingreso a los reportes y gráficos estadísticos del tráfico que genera de la red.



Fig. 6

### **Pantalla General de Nodos**

En esta pantalla se mostrara todos los dispositivos que se encuentran conectados a la red, con su respectiva ip, estado y sistema operativo que tiene instalado.

Además por medio de esta pantalla se podrá tener acceso a cada uno de los nodos para visualizar posteriormente de una manera más detallada la información de cada dispositivo, esta acción se la realiza dando clic sobre el número de ip del dispositivo que va hacer consultado.



Fig. 7

### Menú de los Nodos Específicos

Por medio de estas pestañas podemos visualizar la información detallada de cada nodo consultado como son: información general, los dispositivos lógicos, Aplicaciones instaladas, servicios iniciados y capacidad de los discos conectados.

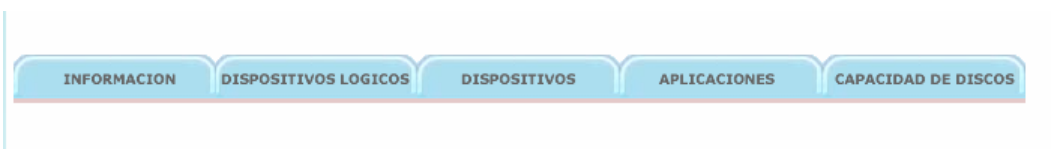


Fig. 8



## Información del Sistema

Mediante esta página se mostrará los usuarios, nombre, sistema operativo, memoria, capacidad del disco, etc., es decir información general del sistema del nodo que se encuentra en ese momento consultado.

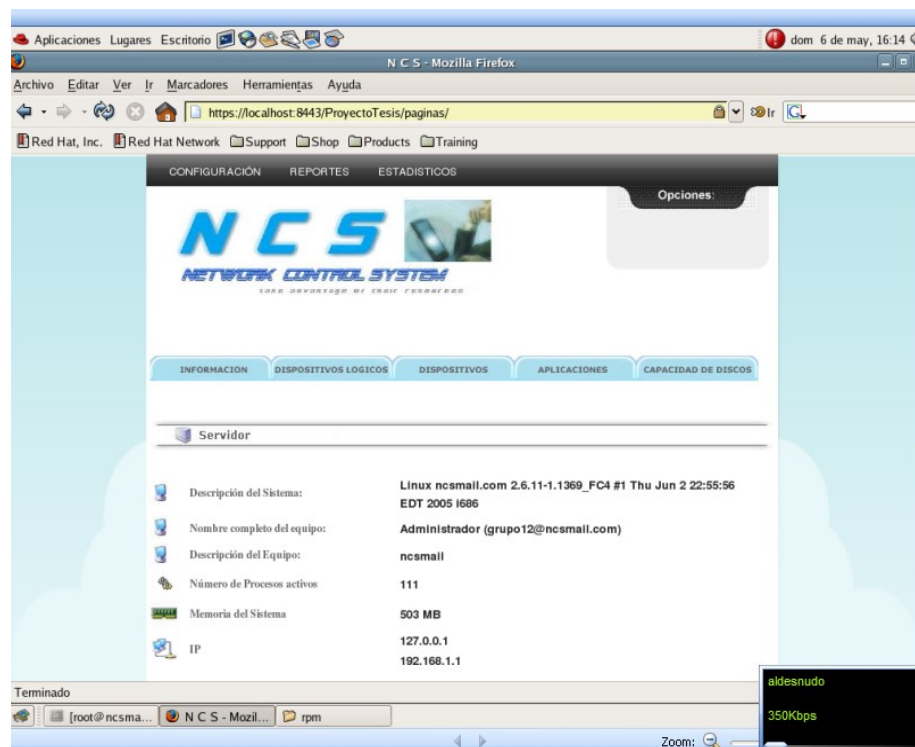


Fig . 9

## Dispositivos Lógicos

En esta página se muestra los dispositivos conectados a la PC que se encuentra monitoreando con sus respectivos label, tamaño y espacio libre con que tiene el dispositivo.

No	Disco	Label	Número de Serie del Volumen	Tamaño Total	Espacio Libre
A:	-	-	-	0 bytes	0 bytes
C:	-	-	9878b9a	40 GB	30 GB
D:	-	-	-	0 bytes	0 bytes
E:	-	ADELA	ec21dd1	34 GB	4 GB
F:	-	MAVERICK	286f157	494 MB	486 MB
Virtual Memory	-	-	-	30 MB	22 MB
Physical Memory	-	-	-	22 MB	16 MB

Fig. 10

## Aplicaciones y Servicios

Esta página muestra las aplicaciones que se encuentran instaladas en cada nodo y los servicios que se encuentran iniciados para visualizar con mejor detalle se podrá desplazar en cada una de las opciones por medio de la barra scroll.

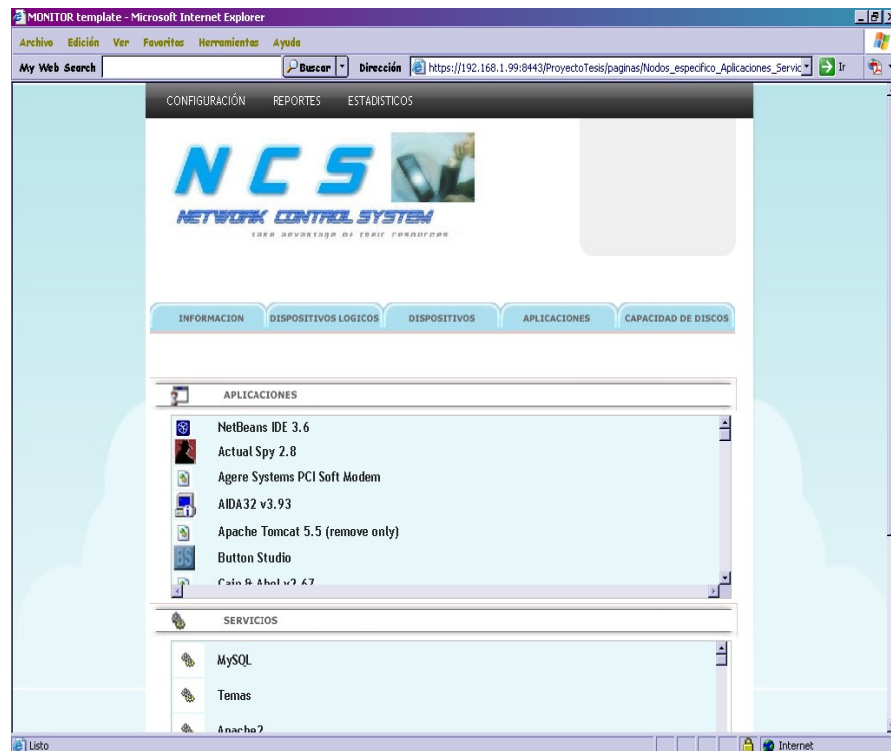


Fig. 11.

### Capacidad de Dispositivos

Mediante esta página se podrá visualizar cada uno de las unidades de almacenamiento conectados al nodo, mostrando la capacidad y el espacio utilizado tanto en gigabyte, porcentaje y gráficamente.

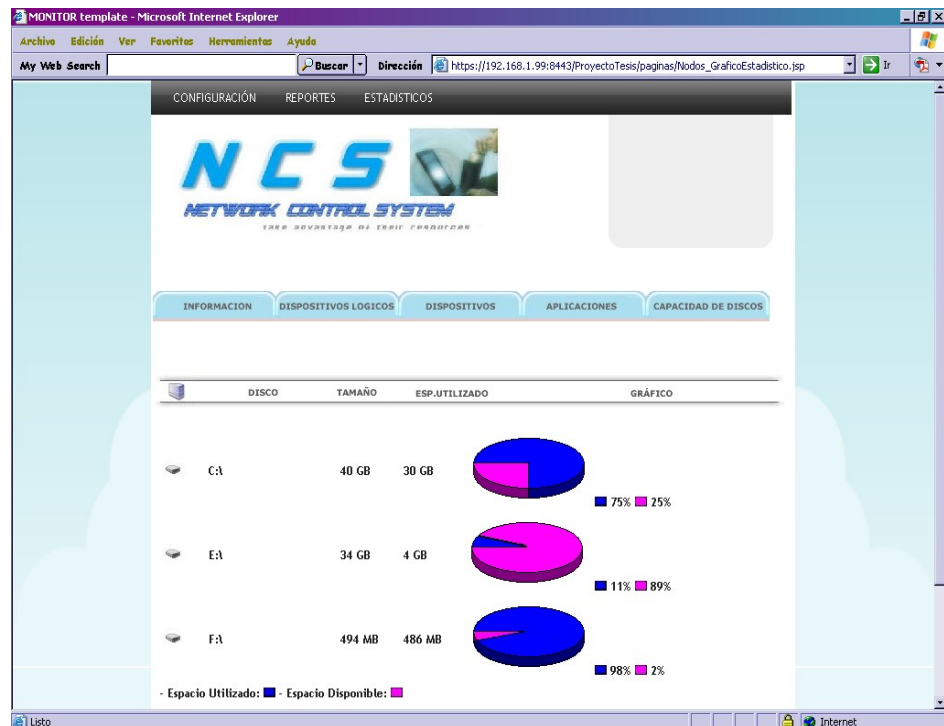


Fig. 12


## Ingreso de Usuario

Por medio de esta página se podrá ingresar los usuarios que tendrán acceso al sistema, mediante la cual ingresara sus datos como: nombres apellidos, número de teléfono, email y clave.

https://192.168.1.99:8443/ProyectoTesis/paginas/ - Microsoft Internet

Archivo Edición Ver Favoritos Herramientas Ayuda

My Web Search Buscar Dirección https://192.168.1.99:8443/ProyectoTesis/paginas/ Ir



USUARIO

Datos personales del Usuario:

Nombre	<input type="text"/>
Teléfono	<input type="text"/>
Nombre de Usuario	<input type="text"/>
Clave	<input type="text"/>
Confirmar Clave	<input type="text"/>
Email	<input type="text"/>

Grabar

NOTE:

Listo Internet