



**TECNOLOGICO
DE MONTERREY**

Biblioteca
Campus Ciudad de México

**INSTITUTO TECNOLÓGICO Y DE ESTUDIOS
SUPERIORES DE MONTERREY
Campus Ciudad de México**

Escuela de Graduados en Ingeniería y Arquitectura
Maestría en Administración de las Telecomunicaciones

**“SISTEMA DE INFORMACIÓN PARA LA
ADMINISTRACIÓN DE EQUIPOS DE
TELECOMUNICACIONES”**

Autora: Ing. Erika Iliana Hernández Hernández
Asesor: Dr. Jose Martin Molina Espinosa
Sinodal: Dr. Víctor Manuel de la Cueva Hernández
Sinodal: Dr. Yoel Ledo Mezquita

México D.F., Febrero del 2011

Resumen

En el presente trabajo se muestra un problema de administración de los recursos tecnológicos, dentro de la infraestructura de telecomunicaciones del Tecnológico de Monterrey Campus Ciudad de México, por lo cual se implemento un sistema de administración que pudiera ayudar a llevar el control de un inventario tecnológico, así como desempeñar algunas tareas básicas de manera automatizada. El nuevo sistema de administración de las telecomunicaciones TelecomSist se puso en operación para dar solución al problema de la falta de inventario y cubrir algunos de los criterios más importantes según lo administradores de redes.

La solución planteada es una aplicación web, basada en el marco de trabajo MVC (modelo-vista-controlador), donde se separa la vista que se presenta al usuario del modelo y todo esto está coordinado a través de un director de orquesta conocido como controlador. Se utilizan diferentes librerías como: librerías de secure Shell, documentos de office, SNMP, correo electrónico, cuya integración permite el resultado final que se desarrolló.

Se realiza una encuesta para determinar la importancia que le dan los administradores de red a ciertos criterios y con ello se diseña un sistema básico de administración de las telecomunicaciones con el cual se pueda mejorar el desempeño de una red y hacer de manera más eficiente el trabajo como administrador de red.

Se instala el sistema en un servidor de aplicaciones y se crean cuentas de acceso para que los administradores de red y telefonía del campus ciudad de México puedan probar el sistema al final de un periodo de pruebas se encuestan a los participantes para comprobar el desempeño del mismo y saber si cumple con los criterios establecidos, así como si contiene funcionalidades que les ayuden a desempeñar mejor su trabajo.

Contenido

Capítulo 1 Introducción	9
1.1 Antecedentes	9
1.2 Definición del problema	13
1.3 Objetivos	14
1.4 Justificación	15
1.5 Hipótesis	16
1.6 Metodología	17
Capítulo 2 Marco Teórico	19
2.1 Importancia de las telecomunicaciones y su administración	19
2.2 Requerimientos de la administración de las telecomunicaciones	22
2.3 Estándares para la administración de las telecomunicaciones	24
2.4 Áreas funcionales de la administración de telecomunicaciones	24
2.4.1 Administración de las fallas	25
2.4.2 Administración de la contabilidad	25
2.4.3 Administración de la configuración	25
2.4.4 Administración del desempeño	25
2.4.5 Administración de la seguridad	26
2.5 SNMP	26
2.5.1 Elementos de un sistema de administración	27
2.5.2 Tipos de comandos	28
2.5.3 Tipos de mensajes	29
2.5.4 MIB	30
2.5.5 SMI	31
2.5.6 Tipos de SMI	31
2.5.7 Versiones de SNMP	31
2.6 CMIS y CMIP	32
2.6.1 Selección de objetos administrados	32
2.6.2 Servicios de CMIS	34
2.7 Telnet	35
2.7.1 Arquitectura de Telnet	36

2.8 SSH	36
2.8.1 Arquitectura de SSH	37
2.8.2 Arquitectura de encriptación.....	38
2.9 Lenguajes de Programación y Arquitectura.....	39
2.9.1 Java	39
2.9.2 MVC	40
2.10 Resumen.....	41
Capítulo 3 Sistema de Administración de Equipos de Red	43
3.1 Modelo de Factores Críticos	43
3.2 Propuesta de Arquitectura de un Sistema de administración de equipos de red.....	50
3.2.1 Arquitectura del sistema	50
3.2.2 Diseño de Procesos	52
Capítulo 4 Caso de estudio	56
4.1 Introducción	56
4.2 Funcionalidades del sistema implantado	56
4.3 Arquitectura específica del sistema	58
4.4 Tecnologías utilizadas.....	58
4.5 Vistas del sistema.....	62
4.6 Escenarios de Prueba	67
4.7 Encuestas de satisfacción.....	75
Capítulo 5 Conclusiones y Trabajo Futuro	78
5.1 Aportaciones de esta investigación.....	78
5.2 Trabajo Futuro	82
Referencias.....	83
Acrónimos.....	83
Anexo A.....	85
Anexo B	88
Anexo C	89

Lista de Figuras

Figura 2.1 Segmentación de mercado de la industria de Hardware (Data Monitor, 2008) .	19
Figura 2.2 Segmentación de Mercado de la industria de Software (Data Monitor, 2009) ..	20
Figura 2.3 Gastos en administración de redes (Stallings, 1993).....	21
Figura 2.4 Evolución del mercado de las TICs (Méndez, 2010)	22
Figura 2.5 Requerimientos para la administración de las Telecomunicaciones (Stallings, 1993)	23
Figura 2.6 Estructura del Protocolo SNMP (Cisco Systems, 1996)	28
Figura 2.7 Estructura mensaje de SNMP (Cisco Systems, 1996).....	29
Figura 2.8 SMI del protocolo SNMP (Cisco Systems, 1996).....	30
Figura 2.9 Establecimiento de conexión SSH (Himanshu, 2004)	37
Figura 2.10 Arquitectura MVC (Kassem, 2000)	41
Figura 3.1 Criterio de: Facilidad de Uso.....	44
Figura 3.2 Criterio de: Seguridad.....	44
Figura 3.3 Criterio de: Automatización Mejorada.....	45
Figura 3.4 Criterio de: Alta de usuarios.....	45
Figura 3.5 Criterio de: Reportes Mejorados	46
Figura 3.6 Criterio de: Capacidad de Restauración	46
Figura 3.7 Criterio de: Habilidad agregar o borrar	47
Figura 3.8 Criterio de: Monitoreo Disponibilidad.....	47
Figura 3.9 Criterio de: Re enrutamiento de Tráfico.....	48
Figura 3.10 Criterio de: Monitoreo del Tiempo de Respuesta.....	48
Figura 3.11 Importancia de los requerimientos del sistema para el usuario	50
Figura 3.12 Arquitectura de referencia propuesta para un sistema de información para la administración de equipos de red.....	51
Figura 3.13 Diagrama de casos de uso.....	53
Figura 4.1 Arquitectura específica del sistema	58
Figura 4.2 Diagrama Entidad-Relación de la Base de datos.....	61
Figura 4.3 Pantalla del Sistema funcionalidad Busca Mac.....	62
Figura 4.4 Pantalla del Sistema funcionalidad Busca Mac (Resultado).....	63
Figura 4.5 Pantalla del Sistema funcionalidad Ejecuta Comandos.....	64

Figura 4.6 Pantalla del Sistema funcionalidad Ejecuta Comandos (Histórico).....	64
Figura 4.7 Pantalla del Sistema funcionalidad Configura Perfiles	65
Figura 4.8 Pantalla del Sistema funcionalidad Configura Perfiles (Resultado Búsqueda)..	66
Figura 4.9 Pantalla del Sistema funcionalidad Configura Perfil (Resultado).....	66
Figura 4.10 Encuesta de satisfacción - Pregunta1	75
Figura 4.11 Encuesta de satisfacción - Pregunta 2	76
Figura 4.12 Encuesta de satisfacción - Pregunta 3	76
Figura 4.13 Encuesta de satisfacción - Pregunta 4	77
Figura 4.14 Encuesta de satisfacción - Pregunta 5	77
Figura C.1 Caso de Uso del Modulo de Monitoreo	89
Figura C.2 Caso de Uso del Modulo de Herramientas	92
Figura C.3 Caso de Uso del Modulo de Configuración.....	95
Figura C.4 Caso de Uso del Modulo de Administración.....	98
Figura C.5 Caso de Uso del Modulo de Manejo de Sesión	107

Lista de Tablas

Tabla 3.1 Resultados globales de la encuesta de criterios del sistema	49
Tabla 4.1 Funcionalidades del sistema	57
Tabla 4.2 Escenario de Prueba 1: Buscar Puertos.....	69
Tabla 4.3 Escenario de Prueba 2: Aislar Sala.....	70
Tabla 4.4 Escenario de Prueba 3: Heterogeneidad en las configuraciones.....	71
Tabla 4.5 Escenario de Prueba 4: Configuraciones Masivas	72
Tabla 4.6 Escenario de Prueba 5: Falta de Inventario Tecnológico	73
Tabla 4.7 Escenario de Prueba 6: Monitoreo de Equipos.....	74
Tabla C.1 Caso de Uso: Modulo Monitoreo-Monitoreo Enlaces	90
Tabla C.2 Caso de Uso: Modulo Monitoreo-Monitoreo Equipo.....	90
Tabla C.3 Caso de Uso: Modulo Monitoreo-Administración del Monitoreo.....	91
Tabla C.4 Caso de Uso: Modulo Herramientas-Busca Mac	93
Tabla C.5 Caso de Uso: Modulo Herramientas-Eventos	94
Tabla C.6 Caso de Uso: Modulo Configuración- Configura Perfiles.....	96
Tabla C.7 Caso de Uso: Modulo Configuración- Ejecuta Comandos	97
Tabla C.8 Caso de Uso: Modulo Administración-Alta Equipos.....	99
Tabla C.9 Caso de Uso: Modulo Administración-Baja Equipos	100
Tabla C.10 Caso de Uso: Modulo Administración-Cambios Equipos	101
Tabla C.11 Caso de Uso: Modulo Administración-Consulta Equipos	102
Tabla C.12 Caso de Uso: Modulo Administración-Alta Usuarios	102
Tabla C.13 Caso de Uso: Modulo Administración-Baja Usuarios	103
Tabla C.14 Caso de Uso: Modulo Administración-Cambios Usuarios	104
Tabla C.15 Caso de Uso: Modulo Administración-Consulta Usuarios	105
Tabla C.16 Caso de Uso: Modulo Administración-Respaldo.....	106
Tabla C.17 Caso de Uso: Modulo Administración-Restaurar	107
Tabla C.18 Caso de Uso: Modulo Manejo de Sesión-Login	108
Tabla C.19 Caso de Uso: Modulo Manejo de Sesión-Logout	109

Capítulo 1 Introducción

1.1 Antecedentes

Un sistema es un conjunto de elementos o componentes que interactúan entre sí para cumplir ciertas metas, existen una gran variedad de sistemas y una amplia gama de categorías, Stair y Reynolds (2000) propone algunas clasificaciones de los sistemas como: simple o complejo, abierto o cerrado, estable o dinámico, adaptable no adaptable, permanente o temporal. Por otro lado un sistema de información es un conjunto de elementos o componentes interrelacionados para recolectar (entradas), manipular (procesos) y diseminar (salidas) datos e información y para proveer un mecanismo de retroalimentación en pro del cumplimiento de un objetivo (Stair & Reynolds, 2000).

No es fácil medir el valor real de un sistema de información (Stair & Reynolds, 2000). Es difícil poder conocer el valor que nos da un sistema de información ya que una de las áreas que se ve más favorecida es la toma de decisiones, debido a que si se posee información adecuada y actualizada las decisiones que se toman basadas en esta información serán mejores a aquellas que se tomen sin ella.

Un problema que se tiene con el manejo de la información es que en algunos casos se genera información inexacta por que se insertan datos inexactos en el proceso de transformación por lo cual para poder garantizar un buen control se necesita tener información exacta y actualizada (Stair & Reynolds, 2000).

Como lo menciona Stair y Reynolds (2000) la información actualmente es uno de los activos más importantes de una organización, sin embargo esta información para ser útil debe cumplir ciertas características como son:

- Flexible, esto es, ser aprovechada para muchos propósitos.
- Completa, que contenga todos los datos importantes.
- Confiable, fuentes de datos sean fidedignas.
- Simple, ya que un exceso de información puede provocar sobrecarga.
- Oportuna, estar disponible justo cuando se necesita.
- Verificable, tener la posibilidad de comprobar que la información es correcta.

- Accesible, ser de fácil acceso a los usuarios autorizados.
- Segura, protegida contra el acceso de usuarios no autorizados.

En nuestros días los sistemas de información han llegado a ser muy importantes para la mayoría de las empresas. Estos sistemas se han utilizado en muchas ramas de la industria para una infinidad de de tareas que van desde hacer los procesos más eficientes y reducir costos, hasta para la toma de decisiones.

De igual forma las telecomunicaciones juegan un papel fundamental en el día a día de las empresas y es fundamental que estas puedan soportar el negocio principal de las mismas.

Para mejorar la administración de las áreas tecnológicas de una organización es necesario tener un mejor control dentro de estas áreas de apoyo, esto se puede lograr a través de sistemas de información que ayuden a hacer más eficientes los procesos y que lleven un inventario actualizado de los activos tecnológicos de la empresa, ya que “no puedes administrar lo que no puedes controlar, no puedes controlar lo que no puedes medir, no puedes medir lo que no defines”.

Existen varios sistemas que ayudan a la administración y monitoreo de los dispositivos de red entre algunos de los más grades encontramos:

CiscoWorks LMS (Lan Management solution)

Es un conjunto de funciones de administración que simplifican la configuración, administración, monitoreo y la resolución de problemas de redes Cisco. CiscoWorks LMS permite a los operadores de red administrar la red a través de una interfaz basada en web que puede ser accedida desde cualquier parte de la red.

CiscoWorks LMS posee las siguientes funcionalidades:

- Monitoreo y resolución de problemas: identificar y corregir problemas de red antes que impacten a los usuarios finales.
- Administración de la configuración: respaldos de la configuración, administración del sistema operativo de los equipos, y cambiar la administración necesaria para mantener y actualizar equipos de red.

- **Inventario:** inventario completo de todos los detalles de todo el equipo Cisco (Carcasas, módulos, interfaces).
- **Reportes:** todos los reportes son centralizados en un sólo menú simplificando el acceso.
- **Centros de Trabajo:** administración de tecnologías de valor agregado- implementación, monitoreo y administración.
- **Administración:** todas las funciones administrativas para configurar la aplicación estas centralizadas para fácil acceso.

Enterasys NMS (Network Management Suite)

Unifica todas las aplicaciones en una sola interface web, conocida como NMS OneView. Con NMS OneView la información crítica de la red está disponible y es fácil de usar. Esta herramienta permite a los administradores y personal técnico ser más eficiente en el monitoreo, análisis, reportes y solución de problemas.

Las características de NMS OneView son:

- **Descubrimiento de dispositivos:** este proceso descubre dispositivos conectados a la red, guarda los valores de los atributos de estos equipos y reporta el estado del dispositivo.
- **Mapas de topología de red:** es generada una representación visual de la conectividad de la red.
- **FlexViews y graficas:** permiten al personal de redes ver una amplia gama de parámetros de configuración de forma grafica.
- **Política de administración básica:** permite a los usuarios ver y configurar políticas por defecto a los puertos para los dispositivos de red conectados.
- **Brújula:** herramienta de búsqueda que permite al usuario obtener información de un usuario de red o un grupo de usuarios.
- **Alarmas y eventos:** reportan alarmas e información de eventos desde los dispositivos administrados.
- **Fácil instalación:** las aplicaciones cliente servidor se instalan en un solo paso y la llave de la licencia determina que características están permitidas.
- **Respaldo de la base de datos:** los administradores pueden calendarizar respaldos de la base de datos de NMS para fácil recuperación.

IBM Tivoli OMNibus y administrador de red

Provee descubrimiento en tiempo real, monitoreo de red y administración de eventos.

Algunas de sus funcionalidades principales son:

- Brindar un punto central para administrar todas las operaciones de red.
- Vistas en web de eventos en tiempo real.
- Descubre dispositivos y conectividad puerto a puerto, así como topologías lógicas.
- Administración de la configuración.
- Automatiza correlación y evita duplicidad de eventos para encontrar la raíz de la causa.

Sin embargo estas herramientas son caras y puede que no se adecuen al 100% a las necesidades de una empresa particular.

También existen utilidades gratuitas, pero son más limitadas en sus funcionalidades y generalmente solo cubren un modulo específico, es decir, una tarea de administración.

Nagios

Sistema de código abierto para monitoreo que permite a las organizaciones resolver problemas de infraestructura de TI (tecnologías de la información) antes de que afecten de manera critica los procesos de negocio. Algunas de sus funcionalidades son:

- Monitoreo de aplicaciones, servicios, sistemas operativos y protocolos de red.
- Vista centralizada de toda la infraestructura de TI.
- Detallada información del estado disponible a través de una interface web.
- Alertas enviadas por mail o sms.
- Reportes históricos.
- Acceso multiusuario vía web.
- Fácil integración con desarrollos en casa o de terceros.

Nets

Permite a administradores e ingenieros mantener de forma fácil y actualizada la información de la red. Algunas de sus características son:

- Habilidad de guardar información de compra.
- Completas preferencias y permisos por usuario.
- Reportes para extraer información de la base de datos.
- Auto descubrimiento basado en NMAP (aplicación de escaneo de puertos) .

Pancho

Programa basado en perl que permite a los administradores de red guardar configuraciones de dispositivos, así como realizar cambios a estos nodos remotos.

1.2 Definición del problema

Las áreas tecnológicas son el soporte de todas las áreas de la organización, sin embargo muchas veces por hacer más eficientes los procesos y administrar recursos utilizados en otros departamentos se pierde el control dentro de las áreas tecnológicas, un ejemplo claro de esto es el área de telecomunicaciones.

El administrar, configurar así como monitorear los equipos de red puede ser muy laborioso, repetitivo o inclusive salirse de control por la falta de modelos internos en la nomenclatura de estos activos, ya que la complejidad de administrar activos que no están estandarizados se vuelve extremadamente alta y el porcentaje de errores que se pueden presentar aumenta por estos problemas.

Por otro lado las telecomunicaciones al ser activos muy importantes para desempeñar las tareas diarias de la organización, no sólo deben estar estandarizados, sino que también se debe tener un control exhaustivo que incluya la administración de: configuraciones, monitoreo, inventario tecnológico entre otros.

Un problema común dentro de la administración de los activos, el cual puede provocar pérdidas de los mismos, es no tenerlos bajo un estricto control e inventario, de igual forma este descuido puede traer como consecuencia el uso ineficiente de los recursos, ya que si no se sabe que es lo que se tiene, no se puede aprovechar al máximo.

Un reto a su vez son las redes híbridas que ofrecen diferentes servicios para satisfacer a varios tipos de usuarios, a través de distintos dispositivos de red, ya que las configuraciones de cada tipo de equipo, o inclusive modelos del mismo, cambian.

1.3 Objetivos

El objetivo principal es realizar un sistema de información para la administración de las telecomunicaciones, el cual ayudará a agilizar y facilitar la configuración y monitoreo de equipos de redes.

Este sistema de información tiene como objetivos específicos:

1) Estandarizar la nomenclatura y configuraciones de los activos tecnológicos

Llegar a un modelo dentro de la nomenclatura de los activos tecnológicos, es decir, estandarizar nombres, procesos, configuraciones, información para garantizar el buen funcionamiento de los mismos, así como reducir el porcentaje de errores debidos a diferentes configuraciones en equipos que se usen para el mismo fin.

2) Crear una base de datos de los activos tecnológicos de una empresa

Para poder tener un control exhaustivo de los activos tecnológicos del área de telecomunicaciones, se necesita de la creación de una base de datos que integre todas las necesidades de la empresa.

3) Reducir el tiempo de configuración de equipos de red

Al tener un sistema de información que se pueda conectar de forma remota a los equipos y configure los parámetros necesarios puede reducir notoriamente el tiempo de configuración de los equipos.

4) Unificar las configuraciones en los dispositivos de red

Al tener configuraciones modelo para los diferentes tipos de dispositivos de red, se pueden homogeneizar las configuraciones necesarias los mismos, para con esto minimizar los errores que se puedan producir por errores dentro de las configuraciones.

5) Mantener una base de datos con la información de los activos tecnológicos actualizada

Al manejar un sistema de información, se podrá tener la información mucho más ordenada, así como exacta de los activos tecnológicos que posee una organización y de igual forma hacer un uso más eficiente de los mismos.

6) Monitorear los dispositivos de red y lanzar alarmas ante determinados eventos

El sistema de información podrá monitorear los dispositivos de red, así como lanzar alarmas de ciertos eventos, para mejorar el tiempo de respuesta de una falla en el servicio.

7) Automatización de procesos

El sistema se encargará de hacer muchas de las actividades que actualmente se hacen a mano de forma que se ahorrará tiempo y esfuerzo en la administración de los mismos.

1.4 Justificación

Los sistemas que actualmente existen en el mercado son pensados para la administración de redes corporativas o de proveedores de servicio y presenta algunas desventajas como son:

- **Costos del sistema:** el costo de estos sistemas es elevado y contienen muchos módulos que no se adecuan completamente a las necesidades del usuario.
- **Costos por licencia:** aparte del costo del sistema se debe de considerar el costo adicional de las licencias que se necesitan, en términos generales es una licencia por cada equipo a monitorear o configurar lo cual incrementa de manera excesiva los costos.
- **Mantenimiento:** estos sistemas tienen además un costo de mantenimiento y el mantenimiento muchas veces es realizado por expertos.

- **Configuración:** la administración de estos sistemas es complicada, ya que la configuración de los mismos es complicada y muchas veces requiere de un experto que configure dicho equipo.
- **Requerimientos mínimos de hardware y software:** los sistemas de caja, necesitan ciertos equipos, así como software especial para poder entrar a producción y se tiene que apearse a estas necesidades en lugar de poder disponer de una plataforma que se adecue al hardware y software ya existente dentro de una empresa.
- **Capacitación:** la complejidad de estos sistemas muchas veces también impacta cuando un sistema nuevo sale a producción y se necesita de una capacitación por parte de la empresa a la que se compro dicho sistema.
- **Tráfico excedente:** muchos de estos sistemas aumentan el trafico para monitorear los equipos, por lo cual se reduce el ancho de banda dedicado a dar servicios para usarse en la parte de monitoreo.
- **Módulos independientes:** los sistemas están formados por módulos independientes que tienen distintas funciones y dependiendo de las necesidades de dichas empresas se compran dichos módulos lo cual incrementa el costo final del sistema, en lugar de manejar una plataforma que integre todo.

1.5 Hipótesis

El principal problema dentro de la administración de los diferentes dispositivos es la heterogeneidad que puede existir en ellos al no tener modelos internos que provean una homogeneización de los mismos desde nomenclatura hasta configuración.

La falta de tiempo puede ocasionar que no se tenga un estricto control de dichos activos lo cual puede provocar que la complejidad para administrar, monitorear, detectar y corregir errores aumente, disminuyendo así el tiempo de respuesta para brindar una solución y un buen servicio.

Un sistema de información para la administración de los activos tecnológicos de una empresa podría corregir algunos de los problemas a través de:

- **Mejorar la calidad del servicio:** al ser más eficientes en la administración de los recursos se puede mejorar el servicio, así como el tiempo de respuesta ante una falla.

- **Automatizar procesos:** al automatizar procesos se puede ahorrar tiempo, dinero, esfuerzo, así como minimizar fallas.
- **Mayor control:** al tener un sistema de información con una base de datos actualizada se puede tener un mejor control de todos los activos tecnológicos de una organización.
- **Mejor tiempo de respuesta ante un evento:** al contar con un sistema de monitoreo, se puede detectar de manera más oportuna cualquier mal funcionamiento o cualquier detonante que indique que se puede presentar una falla o interrupción en el servicio.
- **Inventario actualizado de los activos tecnológicos:** se cuenta con una base de datos que contiene todo el inventario tecnológico la cual al mantenerse actualizada nos da información oportuna del estatus de dichos activos.

1.6 Metodología

Tomando como base la metodología de desarrollo de sistemas de Pressman (2010) se identifican las siguientes fases:

Fase de Investigación: En esta fase se recabará información necesaria para la realización del sistema de información, con esta información se podrá hacer una evaluación de las posibles tecnologías existentes en el mercado para desarrollar dicho sistema, entre las tareas que conforman esta fase se encuentran:

- Buscar información sobre temas relacionados con el problema: protocolos de conexión remota y administración de red, así como lenguajes de programación, concurrencia, recursión, multi-hilos, patrones de diseño, etc.

Fase de análisis del sistema: Buscar información referente a las necesidades de los administradores de red y de los criterios considerados como básicos para los sistemas de administración de equipos de red, para así poder establecer las funciones implementadas en dicho sistema y determinar el alcance del mismo. En esta fase se realiza lo siguiente:

- Buscar criterios para un sistema básico de administración de equipos de red.
- Proponer modelo de factores críticos para un sistema básico de administración de equipos de red.

Fase de Diseño del sistema: En esta fase realizamos el diseño necesario para poder brindar las funcionalidades básicas establecidas dentro del alcance del sistema. De igual manera se propone una arquitectura para los sistemas de información para la administración de equipos de red. Dentro de esta fase se realizan las siguientes actividades:

- Diseñar arquitectura del sistema.
 - Diseñar arquitectura del sistema.
 - Diseñar procesos a través de casos de uso.

Fase de Implementación del sistema: En esta fase se realiza el desarrollo del sistema, basado en el diseño de la arquitectura del sistema de la fase anterior y se implementa para el Campus Ciudad de México. Entre las tareas que conforman esta fase se encuentran:

- Diseño de la Base de datos.
- Diseño de procesos.
- Diseño de clases.
- Codificación de la solución propuesta.

Fase de pruebas: En esta fase se realizan las pruebas al sistema para garantizar el buen funcionamiento de éste, así como su aplicación en escenarios específicos dentro del Tecnológico de Monterrey Campus Ciudad de México y se presenta un comparativo de estos escenarios sin sistema y con sistema. Entre las tareas que conforman esta fase se encuentran:

- Realizar las pruebas al sistema en los distintos escenarios.
- Documentar los resultados.

Conclusiones y trabajo futuro: En esta fase se revisan los últimos detalles y se concluye con las aportaciones de esta tesis, así como el trabajo futuro con el que se podría continuar.

Capítulo 2 Marco Teórico

2.1 Importancia de las telecomunicaciones y su administración

Las inversiones en TI (Tecnologías de información) cada día son mayores, las empresas comienzan a ver los sistemas de información y las tecnologías de información y comunicaciones (TICs) como una necesidad para dar soporte a la estrategia del negocio. En estados unidos estas inversiones han crecido del 34% al 50% entre los años de 1980 y 2004 (Laudon, 2007).

Se invierte una cantidad importante en tecnología, el mercado de hardware en México creció 6.6% en el 2008, alcanzando un valor de \$6.2 billones (Data Monitor, 2008).

En la figura 2.1 se muestra la segmentación del mercado de la industria de hardware. En México el segmento de servidores y equipo de red muestra un mercado potencial del 19%.

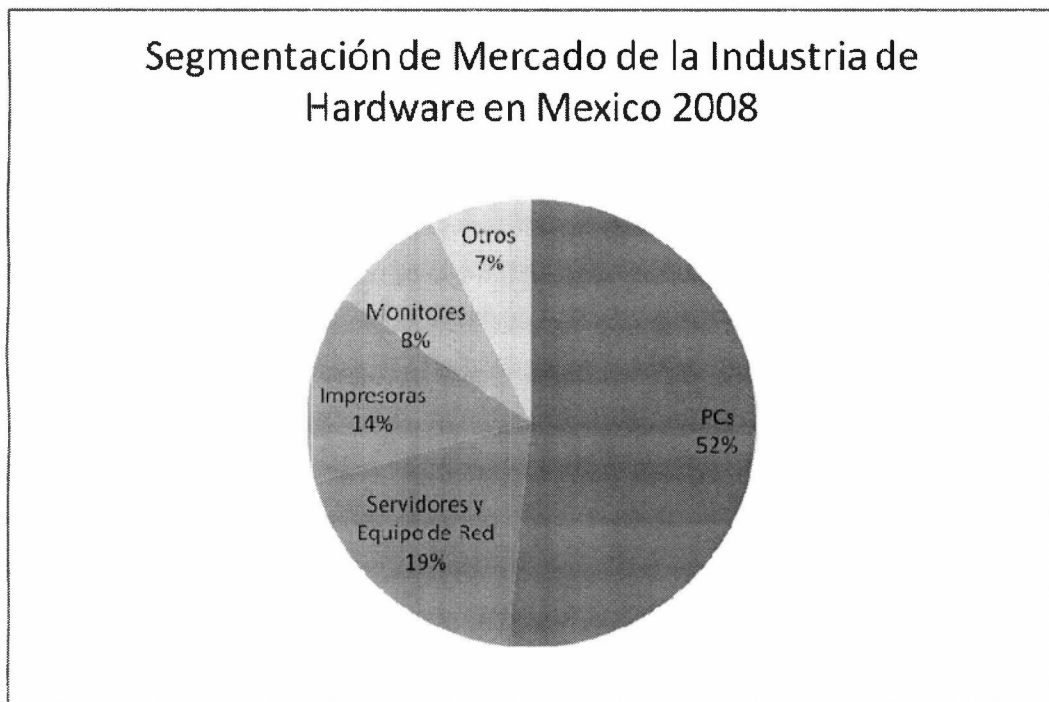


Figura 2.1 Segmentación de mercado de la industria de Hardware (Data Monitor, 2008)

Debido a la gran inversión que esto representa para las empresas, estos recursos deben estar controlados y administrados de forma eficiente para así poder apoyar a la estrategia del negocio y poder ofrecer un excelente servicio a las áreas que apoya.

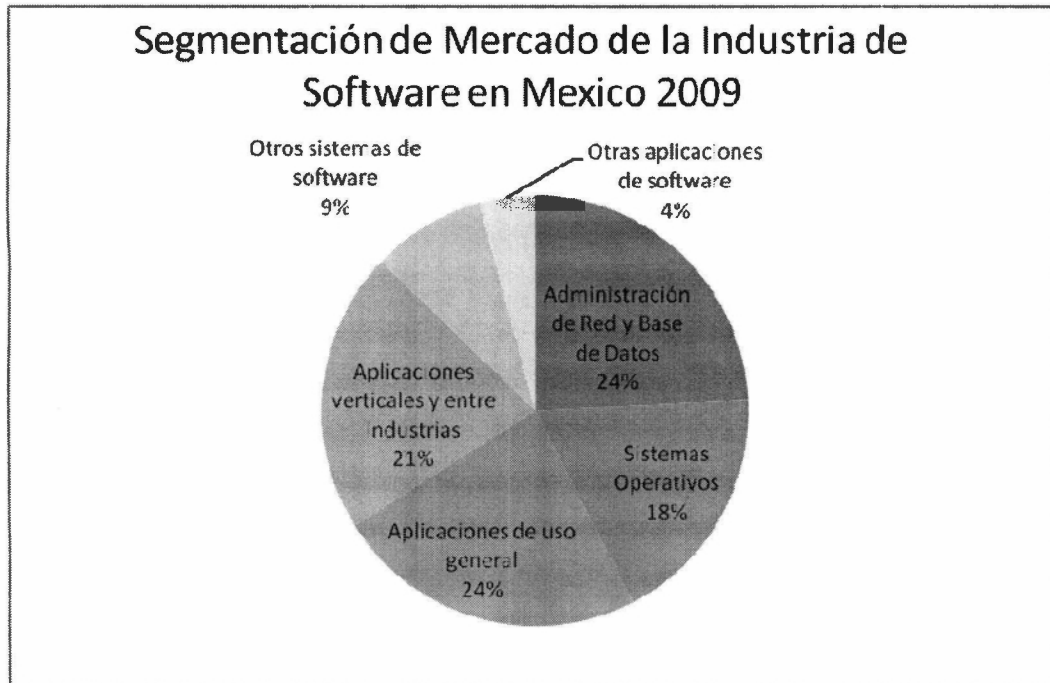


Figura 2.2 Segmentación de Mercado de la industria de Software (Data Monitor, 2009)

Por otro lado en la figura 2.2 se muestra la segmentación del mercado de software en México en el que podemos ver que la inversión que se hace en los sistemas para la administración de equipos de red es alta ya que esta dentro de los líderes del mercado de esta industria (Data Monitor, 2009).

El nicho de mercado de los sistemas de información para la administración de red es grande, ya que consiste de 24% del mercado de software en México. Por lo cual el sistema que se propone tiene un mercado potencial muy atractivo (Data Monitor, 2009).

Las telecomunicaciones han llegado a ser parte fundamental de nuestra vida, cada día éstas son más grandes y complejas para soportar mayor número de aplicaciones y un superior número de usuarios. Esto ha ocasionado que las redes al igual que los recursos tecnológicos se vuelvan indispensables para la organización. Sin embargo este mismo crecimiento ha traído como consecuencia que más cosas puedan salir mal dejando fuera de servicio una parte

de la red o degradando el desempeño a un nivel inaceptable. Por lo cual mejores sistemas de control deben de ser implementados para poder mantener un servicio de calidad para los usuarios (Stallings, 1993).

Una red de gran escala no se puede administrar a través del esfuerzo humano únicamente. Como podemos observar, la figura 2.3 muestra el dinero que destinan diferentes empresas a la administración de equipos de red, que van desde un monto de 0 a 5000 dólares hasta más de 500 000 dólares con el porcentaje más alto siendo de 31% con gastos entre 25 000 y 100 000 dólares. Esto muestra no sólo el nicho de mercado de un sistema de información para la administración de equipos de red, sino también la importancia que tienen estos sistemas para las empresas, ya que sus gastos en la administración de equipos de red son altos y la complejidad de su infraestructura requiere que se utilicen herramientas automatizadas para la administración de las redes. La necesidad de estas herramientas se ha incrementado, así como la dificultad de proveer dichas herramientas, sobre todo si se administran equipos de diferentes proveedores (Stallings, 1993).

Mientras las redes se vuelven más extensas y complejas los costos de administración se incrementan, para controlar costos, se necesitan herramientas estandarizadas que puedan ser utilizadas a través de una amplia gama de productos, incluyendo equipo de telecomunicaciones como *routers* o *switches*, dentro de un ambiente que involucra productos de varios proveedores (Stallings, 1993).

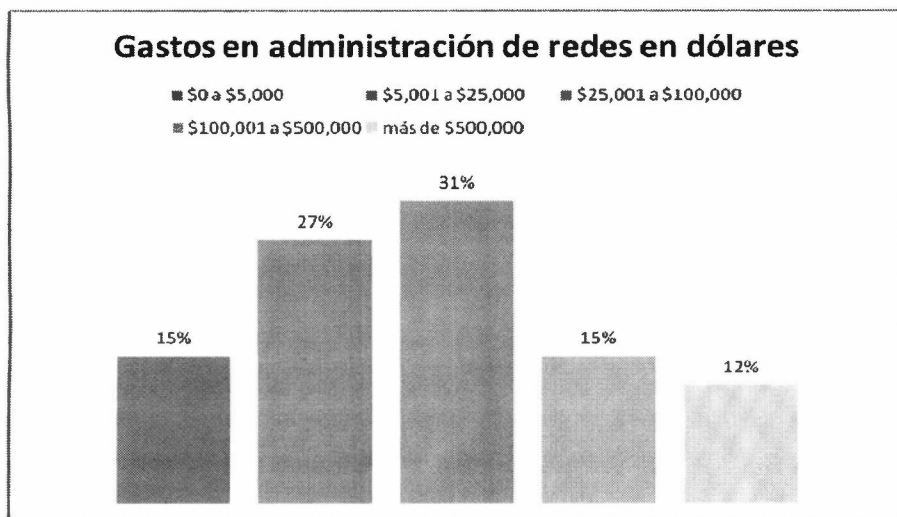


Figura 2.3 Gastos en administración de redes (Stallings, 1993)

En la figura 2.4 podemos ver la distribución del mercado de las TICs en México, donde se puede apreciar que el porcentaje más alto es ocupado por los servicios de telecomunicaciones, ya que la fuente no provee más detalles de esta distribución asumimos que este rubro contiene gastos como: conexión a internet, contratos de mantenimiento, herramientas de administración, entre otros. Es importante señalar la importancia que tienen todos estos servicios para las empresas ya que representan gastos significativos dentro de las mismas (Pineda, 2010).

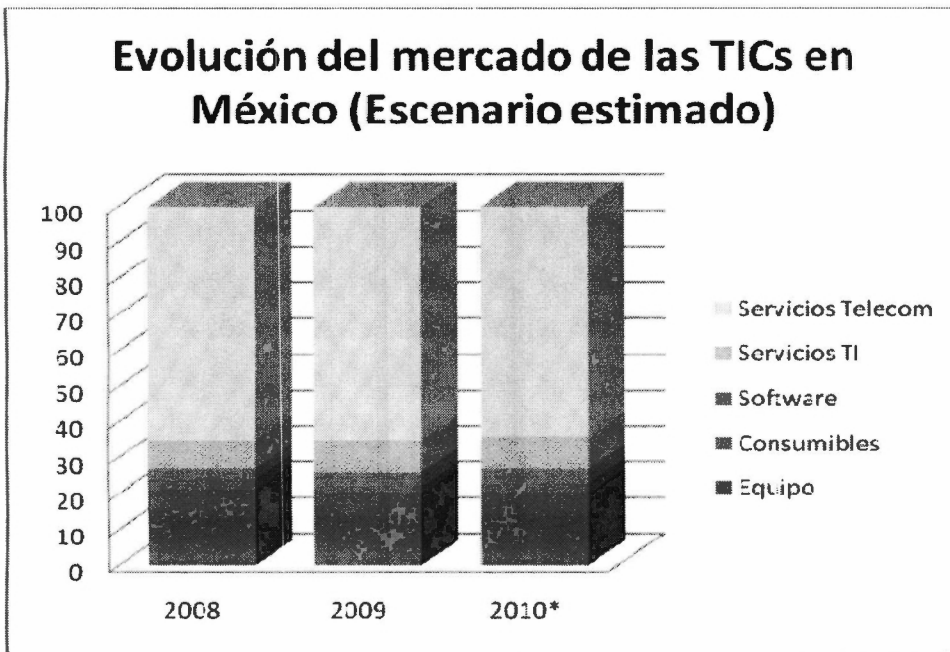


Figura 2.4 Evolución del mercado de las TICs (Pineda, 2010)

2.2 Requerimientos de la administración de las telecomunicaciones

Cuando se realiza un diseño. Lo primero que se debe hacer es conocer la definición de los requerimientos del usuario, esto es sumamente necesario en un ambiente tan complejo como lo es la administración de redes. Una forma de hacer esto es conocer las características más importantes que debe de tener un sistema según en punto de vista de los usuarios finales (Stallings, 1993).

En la figura 2.5 podemos ver la grafica de la importancia de los 10 criterios para sistemas de administración de equipos de telecomunicaciones que define Stallings (1993) evaluados por distintos administradores de red.

Requerimientos para la administración de las Telecomunicaciones

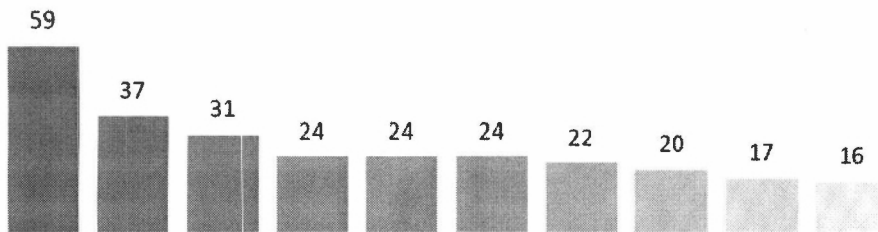
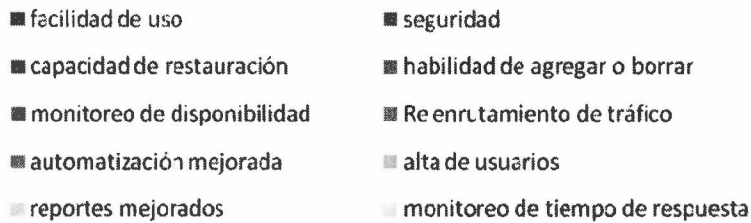


Figura 2.5 Requerimientos para la administración de las Telecomunicaciones (Stallings, 1993)

Según Stallings (1993) algunas de las características que se deben tomar en cuenta para la administración de las telecomunicaciones son:

- **Controlar los activos tecnológicos de una organización:** los recursos tecnológicos se han convertido en parte indispensables de las empresas, sin embargo sin el efectivo control, estos recursos no proveen a la organización su verdadero valor apoyando a las áreas corporativas que los requieren.
- **Controlar la complejidad:** el continuo crecimiento en el número de componentes de una red se convierte en una amenaza para la administración con la pérdida de control de lo que está conectado a red y como son usados estos recursos.
- **Mejorar el servicio:** los usuarios esperan que el servicio sea mejor mientras los sistemas de información o los recursos de red crecen.

- **Balancear varias necesidades:** los recursos de una organización deben satisfacer a una gama de usuarios con diferentes aplicaciones con requerimientos en áreas como desempeño, disponibilidad y seguridad.
- **Reducir tiempo de espera:** conforme los recursos de red se vuelven más importantes para una organización los requerimientos de disponibilidad se deben de aproximar cada vez más al 100%, con un adecuado diseño redundante para garantizar la alta disponibilidad de los mismos.
- **Controlar los costos:** la utilización de los recursos se debe monitorear y controlar para satisfacer las necesidades de los usuarios a un costo razonable.

2.3 Estándares para la administración de las telecomunicaciones

Según Mo (2005), la administración de las telecomunicaciones se puede separar en dos enfoques: el TMN (*Telecommunications Management Network*) y SNMP (*Simple Network Management Protocol*).

- El primer enfoque se define en 5 áreas: administración de la configuración, administración de las fallas, administración del desempeño, administración de la contabilidad y administración de la seguridad.
- El segundo enfoque por otro lado se basa en dos componentes lógicos: agente y administrador. Un agente reside en dispositivos administrados y tiene una base de administración del conocimiento para almacenar objetos administrados, mientras que el administrador es una entidad que interactúa con los agentes administrados. Este enfoque se utiliza en redes IP (*Internet Protocol*).

2.4 Áreas funcionales de la administración de telecomunicaciones

Las áreas clave de la administración de las redes definidas por ISO (*International Organization for Standardization*) fueron desarrolladas para el modelo OSI (*Open System Interconnection*) y están aceptadas por vendedores para sistemas de administración de red estándares y propietarios (Stallings, 1993).

2.4.1 Administración de las fallas

Cuando una falla ocurre es importante que, tan rápido como sea posible, se determine:

- Exactamente donde está la falla.
- Aislar el resto de la red de la falla para que la operación continúe sin interferencias.
- Reconfigurar o modificar la red para minimizar el impacto en la operación sin los componentes que fallaron.
- Reparar o reemplazar los componentes dañados para restaurar la red a su estado inicial.

2.4.2 Administración de la contabilidad

El administrador de red necesita ser capaz de monitorear el uso de los recursos de red por usuario o grupo de usuarios por las siguientes razones:

- Un usuario o grupo de usuarios pueden estar abusando de sus privilegios de acceso y sobrecargar la red a expensas de otros usuarios.
- Usuarios pueden estar haciendo un uso ineficiente de la red y el administrador de la red puede ayudar a cambiar procedimientos para mejorar el desempeño.
- El administrador de la red está en una mejor posición para planear un crecimiento en la red si conoce con suficiente detalle la actividad de los usuarios.

2.4.3 Administración de la configuración

Una vez que se ha decidido cómo se va a usar un dispositivo el administrador de la configuración puede escoger el software apropiado y el conjunto de atributos y valores para ese dispositivo. La reconfiguración de la red es frecuentemente deseada en respuesta a la evaluación del desempeño; para apoyar la mejora de la red, recuperación de una falla, o para un chequeo de seguridad.

2.4.4 Administración del desempeño

La administración del desempeño de una red involucra dos categorías funcionales:

- Monitoreo es la función que revisa la actividad de la red.

- Control habilita a la administración del desempeño a hacer ajustes a la red para mejorar el desempeño.

El administrador de la red debe enfocarse en algunos conjuntos de recursos que deben ser monitoreados para determinar el nivel de desempeño. Por otro lado, las estadísticas de desempeño pueden utilizarse para reconocer potenciales cuellos de botella antes de que estos causen problemas a los usuarios finales.

2.4.5 Administración de la seguridad

La administración de la seguridad se enfoca en generar, distribuir y almacenar llaves encriptadas, contraseñas y otra información para la autorización o control de accesos. Los registros son una importante herramienta de seguridad por lo tanto la administración de la seguridad involucra: recolectar, almacenar, examinar y auditar la información de los registros.

2.5 SNMP

Desde que fue desarrollado en 1988, el protocolo de administración de redes SNMP se ha convertido en el estándar más usado para administración de redes interconectadas. SNMP tiene varias ventajas que contribuyen a su popularidad. Ya que es una solución simple y requiere relativamente poco código para implementarse muchos vendedores pueden fácilmente construir agentes de SNMP en sus productos. SNMP es extensible, permitiendo así a los vendedores de equipo de red agregar funciones de administración de red de manera sencilla. SNMP separa la arquitectura de administración de la arquitectura del hardware de los dispositivos, lo cual amplía la base de soporte a varios vendedores. SNMP es más que solo una especificación en papel, es una implementación extensamente disponible hoy en día (Miller, 1993).

SNMP es un estándar ampliamente usado para la administración de dispositivos que funcionan en redes basadas en el protocolo IP. Parte de la importancia del protocolo SNMP es su simplicidad ya que toda la información administrada se guarda en su MIB (management information base), que puede ser accesible a través de consultas SNMP a algún agente de

software que se esté ejecutando en un dispositivo administrado y el estándar preferido sobre CMIS/CMIP (Breitgand, Raz, & Shavitt, 2002).

2.5.1 Elementos de un sistema de administración

Según Cisco Systems (1996) un sistema administración de la red contiene:

- **Elementos de red:** llamados dispositivos administrados, los elementos de red con dispositivos de hardware como: computadoras, ruteadores, servidores que están conectados a la red.
- **Agentes:** son módulos de software que residen en los elementos de red. Ellos colectan y almacenan información para la administración como el número de paquetes recibidos con error por un elemento de red.
- **Objeto administrado:** es una característica de algo que puede ser administrado, por ejemplo una lista de los circuitos TCP (*Transmission Control Protocol*) actualmente activos en una computadora en particular es un objeto administrado.
- **MIB:** es una colección de objetos administrados que viven dentro de un contenedor de información virtual. Colecciones de objetos administrados relacionados son definidos en módulos MIBs.
- **Notación sintáctica:** es un lenguaje que se usa para describir un MIBs de objetos administrados en un formato de maquina independiente. Uso consistente de la notación sintáctica permite que varios tipos de computadoras compartan información.
- **Estructura de la información administrada SMI (*Structure of management information*):** define las reglas para describir la información de administración, se define usando ASN.1.
- **Estaciones de administración de red NMS (*network management stations*):** llamadas consolas, estos dispositivos ejecutan aplicaciones de administración que monitorean o controlan los elementos de red.
- **Terceros (*Parties*):** es una entidad lógica que puede inicializar o recibir comunicación de SNMPv2.
- **Protocolo de administración:** es usado para transportar información para la administración entre agentes y NMSs SNMP es el estándar utilizado por la comunidad de Internet como protocolo de administración.

En la figura 2.6 podemos ver la interacción de los distintos componentes involucrados en el protocolo de SNMP. Los agentes tienen su selección de objetos administrados los cuales almacenan valores que los NMS obtendrán para monitorear dichos equipos de red.

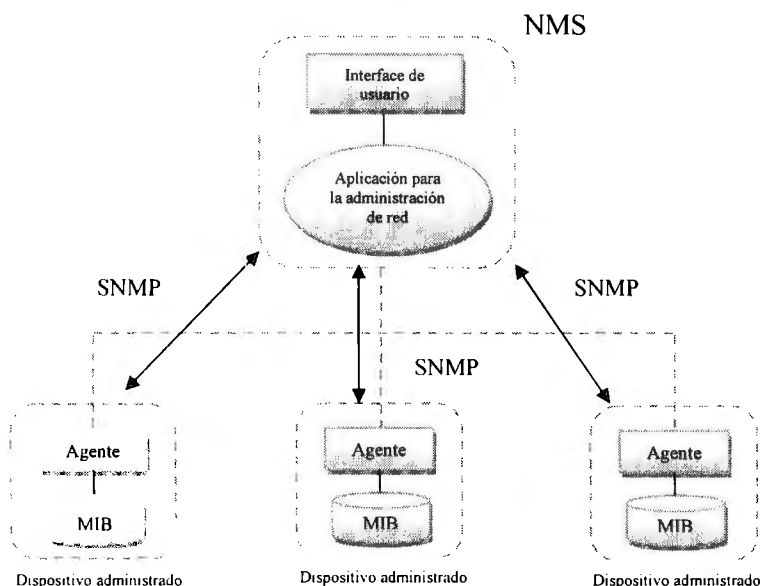


Figura 2.6 Estructura del Protocolo SNMP (Cisco Systems, 1996)

2.5.2 Tipos de comandos

Las interacciones entre NMSs y dispositivos administrados pueden ser de uno de los 4 tipos de comandos:

- **Lectura:** para monitorear a los dispositivos administrados los NMSs leen variables mantenidas por los dispositivos.
- **Escritura:** para controlar a los dispositivos administrados los NMS escriben variables almacenadas dentro de los dispositivos administrados.
- **Operaciones transversales:** NMSs usan estas operaciones para determinar que variables un dispositivo administrado soporta y secuencialmente obtiene información de las tablas de variables en los dispositivos administrados.
- **Trampas:** dispositivos administrados usan trampas para reportar determinados eventos a los NMSs de forma asíncrona.

2.5.3 Tipos de mensajes

Según Drake (1991) SNMP tiene 5 tipos de mensajes:

- **GET** sirve para obtener información de un objeto desde el servidor MIB.
- **GET NEXT** sirve para obtener información de un grupo de objetos desde el servidor MIB.
- **SET** sirve para poner información de un objeto en el servidor MIB.
- **GET RESPONSE** mensaje de respuesta del servidor que sigue a alguna de las operaciones antes mencionadas.
- **TRAP** un mensaje de alarma ante algún evento desde el servidor a un administrador.

Como podemos observar en la figura 2.7 los mensajes de SNMPv1 consisten de dos partes: la primera parte contiene la versión y el nombre de la comunidad, la segunda parte consiste de PDU (*protocol data unit*) de SNMP, que especifica la operación que va a ser efectuada (get, set, etc.) y las instancias de los objetos que están involucradas en la operación (Cisco Systems, 1996).

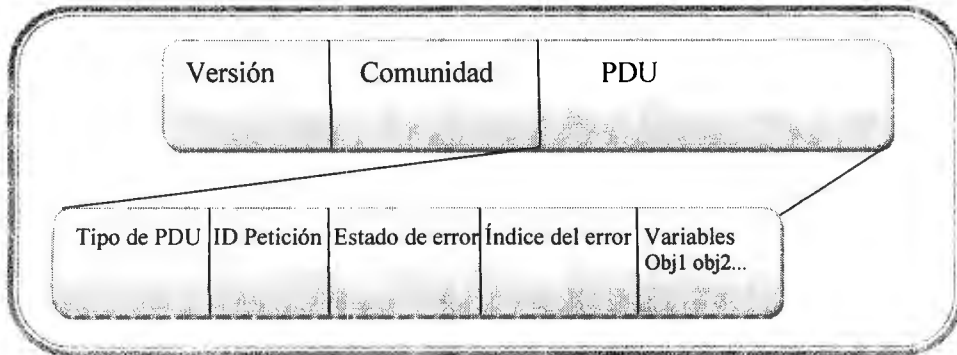


Figura 2.7 Estructura mensaje de SNMP (Cisco Systems, 1996)

La mayoría de las características de SNMP estas hechas para el monitoreo de los equipos, ya que la mayoría de los objetos SNMP son de sólo lectura, para obtener información acerca del estado de la red y determinar el funcionamiento de la misma. SNMP es menos poderoso cuando se requieren hacer modificaciones a la red a través de comando set (Stallings, 1993).

2.5.4 MIB

Un MIB puede ser visto como un árbol abstracto con una raíz sin nombre. Los datos individuales crean las hojas del árbol. Los identificadores de objeto identifican de forma única o los objetos MIB nombrados en el árbol, los identificadores de objetos son como números telefónicos, están organizados de forma jerárquica con dígitos específicos asignados por diferentes organizaciones. La estructura de los MIBs está definida por 3 ramas principales: CCITT, ISO y ISO/CCITT, estos valores se encuentran definidos en el estándar de Internet MIB definido en el RFC 1213 que contiene 171 objetos (Cisco Systems, 1996).

Para entender cómo funciona la nomenclatura de los MIB la figura 2.8 muestra la estructura de árbol del MIB desde la raíz hasta la rama de Cisco, por lo que cualquier MIB que pertenezca a Cisco estará precedido de la jerarquía 1.3.6.1.4.1.

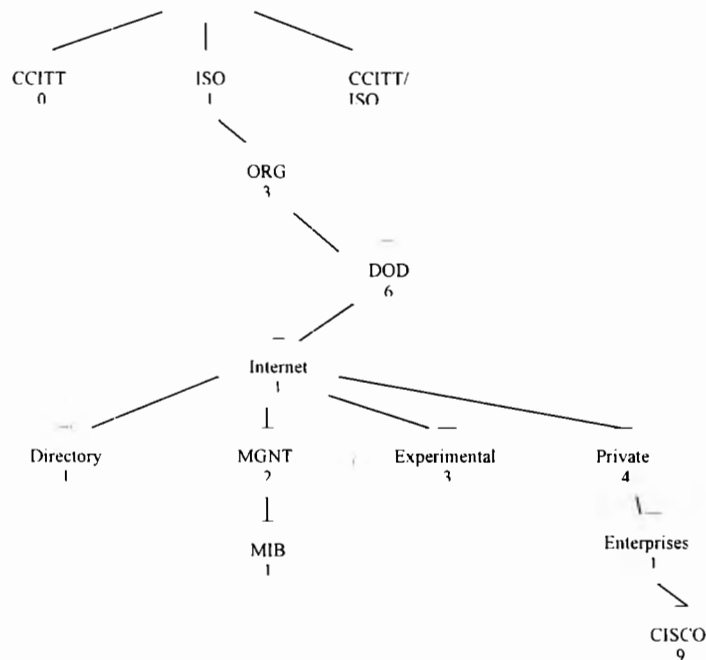


Figura 2.8 SMI del protocolo SNMP (Cisco Systems, 1996)

2.5.5 SMI

Los SMI especifican que todos los objetos administrados deben tener un nombre, una sintaxis y una codificación. El nombre es el identificador del objeto, la sintaxis define el tipo de dato del objeto, la codificación describe como la información asociada con los objetos administrados esta formateada como una serie de datos para transmitirse en la red (Cisco Systems, 1996).

2.5.6 Tipos de SMI

De acuerdo con Cisco Systems (1996), los tipos de datos de SMI están divididos en 3 categorías: tipos simples, tipos de aplicación y tipos simples construidos.

- Tipos simples
 - enteros
 - octetos de caracteres
 - identificadores de objetos
 - caracteres
- Tipos de aplicación
 - direcciones de red
 - contadores
 - calibradores
 - señales de tiempo
 - enteros con signo
 - enteros sin signo
- Tipos simples construidos
 - fila
 - tabla

2.5.7 Versiones de SNMP

SNMPv1 es la primera versión del protocolo de SNMP, definido en el RFC 1157 es un estándar de la IETF, la seguridad de este protocolo está basada en comunidades, que no son otra cosa que contraseñas, cadenas de caracteres en texto claro que permiten que cualquier

aplicación basada en SNMP que conozca esta contraseña pueda ganar acceso a información de los dispositivos administrados (Douglas & Schmidt, 2005).

SNMPv2 3s la segunda versión del protocolo, definida en los RFCs 3416, 3417 y 3418. Esta versión es conocida como SNMPSv2c, donde la “c” indica que se mantiene el esquema de seguridad basado en comunidades (Douglas & Schmidt, 2005).

SNMPv3 es la tercera y última versión del protocolo, definida en los RFCs 3410-3418. Su contribución más importante a la administración de redes es la seguridad ya que no hay operaciones nuevas y SNMPv3 soporta todas las operaciones definidas por las versiones 1 y 2. Esta versión agrega soporte para autenticación y comunicación privada entre las entidades administradas (Douglas & Schmidt, 2005).

2.6 CMIS y CMIP

La estructura del protocolo de administración de red de OSI está definida como un elemento de servicio de aplicación conocido como CMISE (*Common Management Information Service Element*). A pesar de los recursos manejados, el protocolo define un conjunto básico de operaciones aplicables a la administración de redes. Usando la estructura definida por el protocolo para las distintas funciones de administración, la información es modelada para representar los recursos administrados. Como parte de la administración de redes de OSI, se han usado principios orientados a objetos para definir modelos de información, los cuales se han desarrollado para representar entidades de comunicación (Raman, 1998).

CMIS (*Common Management Information Service*) esta es la interfaz con el usuario que especifica los servicios que se proveen (Stallings, 1993).

CIMP (*Common Management Information Protocol*) este es el protocolo que especifica el formato y los procedimientos asociados (Stallings, 1993).

2.6.1 Selección de objetos administrados

Stallings (1993) explica que el CMIS provee un conjunto de herramientas que permiten a un objeto o a un número de objetos ser el objetivo de una operación de administración.

- Alcance: se refiere a la identificación de un objeto u objetos a los cuales un filtro puede ser aplicado. El alcance se define con la referencia a una instancia específica de algún objeto administrado, referido como objeto administrado base. El objeto administrado base es el punto de partida para la selección de uno o más objetos a los cuales se les aplicarán un filtro. Existen cuatro especificaciones de nivel de alcance:
 - El objeto base solo
 - El nivel enésimo de subordinados del objeto base con el nivel base definido como nivel 0
 - El objeto base y todos sus subordinados hacia abajo incluyendo el nivel enésimo
 - El objeto base y todos sus subordinados, esto es, todo el subárbol

- Filtrado: Un filtro es una expresión booleana que consiste en una o más aseveraciones acerca de la presencia o valores de los atributos en el alcance de un objeto administrado. Las reglas a cumplir pueden ser:
 - Igualdad: un atributo sea igual que el que se quiere probar.
 - Mayor o igual: el valor del atributo del objeto sea mayor o igual que el valor del atributo.
 - Menor o igual: el valor del atributo del objeto sea menor o igual que el valor del atributo.
 - Presente: el atributo este presente.
 - Subcadena (substring): el valor del atributo incluya las subcadenas de texto en el orden especificado.
 - Subconjunto: todos los miembros confirmados están presentes en el atributo.
 - Superconjunto: todos los miembros del atributo están presentes en el atributo confirmado.
 - Ningún conjunto nulo en la intersección: por lo menos uno de los miembros está presente en el atributo.

- Sincronización: El parámetro de alcance puede resultar en la selección de uno o más objetos para ser objetivos del filtrado. Si más de un objeto esta en el alcance el parámetro de filtrado podría resultar en la selección de más de un objeto en el que se realizará la operación. En ese caso la pregunta importante es en cuanto al orden en

que los objetos serán procesados. Sin embargo CMIS incluye el concepto de sincronización, el usuario de CMIS puede pedir uno de dos tipos de sincronización.

- Atómico: todos los objetos administrados seleccionados para la operación son revisados para garantizar que se pueda realizar dicha operación de forma exitosa. Si uno o más objetos administrados no pueden hacerlo entonces nadie lo hace.
- Mejor intento: A todos los objetos administrados seleccionados para la operación se les indica realizar dicha operación.

2.6.2 Servicios de CMIS

Los servicios de CMIS están especificados en términos de primitivas que pueden ser vistas como comandos o llamadas a procedimientos con parámetros. Son relevantes tres categorías de servicio para CMIS: servicio de asociación, servicio de administración de notificaciones y servicio de administración de operaciones (Stallings, 1993).

Servicio de administración de notificaciones

La única primitiva definida para el servicio de administración de notificaciones es M-EVENT-REPORT. Esta primitiva es usada para reportar una notificación a un administrador que ha solicitado dicha notificación. A diferencia de todas las demás operaciones de administración el reporte de este evento es iniciado por el proceso agente y el proceso administrador es el que contesta (Stallings, 1993).

Servicio de administración de operaciones

Las primitivas utilizadas para realizar las demás operaciones de CMIS son:

- M-GET: pide información de administración de un usuario del servicio CMIS.
- M-SET: pide la modificación de información de administración por un usuario del servicio CMIS.
- M-ACTION: Pide que un usuario del servicio CMIS realice una acción.
- M-CREATE: pide que un usuario del servicio CMIS cree una instancia de un objeto administrado.
- M-DELETE: pide que un usuario del servicio CMIS borre una instancia de un objeto administrado.

- M-CANCEL-GET: pide que un usuario del servicio CMIS cancele una petición previa del servicio M-GET.

Servicios de asociación

Para que dos usuarios puedan utilizar operaciones de administración de CMIS, ellos primero deben establecer una asociación de aplicación (Stallings, 1993).

Primero se establece una asociación de aplicación que se pueda utilizar para intercambiar primitivas o servicios de CMIS. Segundo cuando se establezca la asociación, los dos usuarios convienen en que características de CMIS serán usadas en esa asociación (Stallings, 1993).

2.7 Telnet

Telnet es un protocolo que permite a un usuario en una terminal conectado a su propio equipo local controlar y usar procesos en un equipo remoto como si fuera un usuario local del equipo remoto. El propósito del protocolo de Telnet es proveer la facultad de una comunicación general, bidireccional y orientada a caracteres, Su meta principal es definir un método estándar para interconectar dispositivos terminales a los procesos de dicha terminal. Este protocolo puede ser usado para comunicación entre terminales o comunicación entre procesos (Davidson & Hathaway, 1977).

El protocolo Telnet está construido sobre tres ideas principales:

1. El concepto de una Terminal Virtual de red: Un NVT (Network Virtual Terminal) es un dispositivo imaginario que proporciona una representación estándar para toda la red de un terminal canónico.
2. El principio de negociación de opciones: tiene en cuenta el hecho de que muchos ordenadores querrán proporcionar servicios adicionales a los disponibles en un NVT. Hay "opciones" independientes del Protocolo TELNET que permiten a un usuario y a un servidor ponerse de acuerdo para usar convenciones más elaboradas (o tal vez sólo diferentes para sus conexiones TELNET).

3. La simetría de la sintaxis de negociación puede potencialmente llevar a ciclos infinitos de reconocimiento (cada parte viendo las órdenes que llegan no como reconocimientos sino como nuevas peticiones). Para evitar esto, existen las siguientes normas:
 - a. Las partes sólo pueden solicitar un cambio del estado de una opción.
 - b. Si una parte recibe lo que parece una petición para entrar en algún modo en el que ya está, la petición no debería reconocerse.
 - c. Siempre que una parte envíe una orden de opción a la otra, ya sea una petición o un reconocimiento, y el uso de la opción va a tener algún efecto en el procesado de los datos enviados de la primera parte a la segunda, dicha orden se debe enviar en el punto donde se desee que comience a tener efecto.

2.7.1 Arquitectura de Telnet

La conexión de telnet consiste en una conexión full-duplex a través de la cual se pasa información entremezclada con información de control de Telnet. Cuando una conexión de Telnet es establecida por primera vez se asume que cada punto es originado y terminado en un NVT. Esto elimina la necesidad de que el servidor y el cliente guarden información de las características mutuas de las convenciones manejadas en cada una de las terminales (Davidson & Hathaway, 1977).

NVT es un dispositivo de caracteres bidireccional con una impresora y un teclado. La impresora responde ante datos entrantes y el teclado produce datos salientes los cuales son enviados a través de la conexión de telnet. El código que se utiliza está fijado en 7 bits ASCII en un campo de 8 bits RFC 137.

2.8 SSH

SSH (*Secure Shell*) es un programa utilizado para comunicación segura entre dos entidades. SSH usa una arquitectura cliente/servidor, donde los clientes de SSH están disponibles en todas las versiones de Windows, Linux y Macintosh, quienes se conectan a servidores SSH que pueden correr en sistemas operativos como Sun Solaris, Windows, Linux o dispositivos como routers Cisco. En el sentido más simple SSH es usado para ejecutar comandos de

manera remota y segura en otra entidad, frecuentemente usado en lugar de los protocolos: Telnet, RSH (*Remote Shell*) o Rlogin (*Remote Login*). SSH provee métodos de encriptación entre las entidades, los métodos de encriptación y algoritmos que se utilizan son: 3DES, Blowfish, Twofish y AES (Himanshu, 2004).

Algunos de los usos de SSH son: seguridad, ejecución remota de comandos, transferencia remota de archivos, acceso remoto a la red, administración segura y servicios de proxy, mientras que las ventajas de utilizar SSH para la administración son: administración encriptada, significativo ahorro en costos, simplicidad, autenticación de 2 factores (Himanshu, 2004).

2.8.1 Arquitectura de SSH

SSH usa una arquitectura cliente/servidor en su implementación. Un servidor SSH puede permitir conectarse a varios clientes de SSH, la arquitectura no es diferente a otras arquitecturas cliente/servidor donde el servidor está corriendo un demonio. Un proceso demonio es un proceso que debe ejecutarse continuamente en modo *background* (en segundo plano), y generalmente se diseña para responder a peticiones de otros procesos a través de la red, este servicio usualmente escucha en el puerto TCP 22. SSH provee la habilidad de que el demonio o servicio escuche en cualquier otro puerto, sin embargo debe estar escuchando en una conexión TCP. SSH tiene un archivo de configuración donde se configuran diferentes opciones como: contraseña, puerto, directorio base. Los clientes de SSH solamente necesitan conocer la dirección IP del servidor SSH (o nombre del host) y el puerto en el que está escuchando, el cliente necesita autenticarse con el servidor con los requerimientos predefinidos para tener acceso a la sesión (Himanshu, 2004).

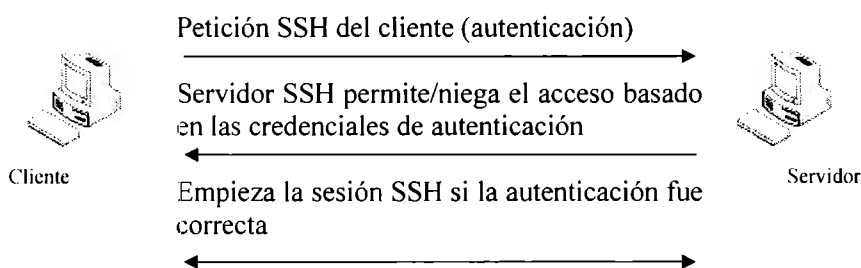


Figura 2.9 Establecimiento de conexión SSH (Himanshu, 2004)

En la figura 2.9 se muestra la secuencia de pasos que se sigue para poder crear una conexión segura a través del protocolo de SSH (Himanshu, 2004).

- El cliente de SSH pide la autenticación al servidor. En la conexión inicial el cliente recibe una llave del servidor, por lo tanto en las conexiones subsecuentes el cliente sabrá que se está conectando al mismo servidor de SSH.
- El servidor determina si el cliente está autorizado para conectarse a los servicios de SSH verificando su nombre de usuario y contraseña o la llave pública que el cliente haya presentado para autenticarse, este proceso está completamente encriptado.
- Si el servidor autenticó al cliente y el cliente está autorizado, la sesión de SSH comienza entre las dos entidades. Toda la comunicación está completamente encriptada.

2.8.2 Arquitectura de encriptación

Uno de los beneficios de SSH es que provee un protocolo encriptado para transferir la información. Las implementaciones de SSH utilizan en su mayoría los algoritmos de cifrado MD5 y SHA1. SSH ofrece algoritmos MAC (*Message Authentication Code*), estos algoritmos se usan para garantizar la integridad de los datos. A los datos que son transferidos de una entidad a otra, se les aplica una función hash con una firma criptográfica única, diferenciándola de los datos.

Una función hash es una función que hace posible obtener un hash (también llamado resumen de mensaje) de un texto, es decir, obtener una serie moderadamente corta de caracteres que representan el texto al cual se le aplica esta función hash. La función hash debe ser tal que asocie únicamente un hash con un texto plano (esto significa que la mínima modificación del documento causará una modificación en el hash). Además, debe ser una función unidireccional para que el mensaje original no pueda ser recuperado a partir del hash.

La firma criptográfica, es generada con funciones hash como MD5 o SHA1 y no cambia bajo ninguna circunstancia de una entidad a la siguiente. Esto garantiza que la entidad que recibe los datos ha obtenido la información sin ninguna modificación o abuso por entidades no autorizadas (Himanshu, 2004).

SSH utiliza autenticación de dos factores, esto quiere decir, que el cliente se debe autenticar con el servidor a través de su llave pública y una vez que es autenticado, se pide la contraseña que está dada de alta en el servidor para el usuario que esté intentando conectarse (Himanshu, 2004).

2.9 Lenguajes de Programación y Arquitectura

2.9.1 Java

Java es un lenguaje de programación orientado a objetos, esto significa que la programación está enfocada en crear clases que representen datos en una aplicación, más que en pensar en la solución del problema como un conjunto de procedimientos que deben ser ejecutados en un cierto orden, como se hace en los lenguajes como C y pascal (Holmes, 1998).

Java es un lenguaje fácil de aprender, utilizar y una de sus fortalezas más grandes es poseer una extensa librería de componentes de software que los programadores pueden utilizar. De igual forma Java no está restringido a desarrollar programas en un tipo de máquina específico o un sistema operativo en particular, ya que Java es portable. Esto quiere decir que un programa escrito y compilado en una PC funcionara sin modificaciones en una estación de trabajo de Sun (Holmes, 1998).

Java ofrece mejoras sobre otros lenguajes de programación como: robustez, seguridad y puede ser utilizado en aplicaciones de red (Holmes, 1998). Otras características y ventajas que hacen a Java diferente son: Lenguaje orientado a objetos, distribuido, portable, dinámico, incluye funciones de entrada y salida (I/O), sockets, ocultamiento de la información y soporta varios hilos de ejecución (*multi-threading*) (Sabharwal, 1998).

La plataforma J2EE soporta los siguientes tipos de componentes: applets, aplicaciones, componentes de enterprise JavaBeans, componentes web y componentes para adaptar recursos. Los applets y las aplicaciones corren en una plataforma de cliente, mientras que los EJBs, los componentes de web y para adaptar recursos, corren sobre una plataforma de servidor (Kassem, 2000).

Un componente web es una entidad de software que provee una respuesta a una petición. Un componente web típicamente genera una interfaz de usuario para una aplicación web. La plataforma J2EE especifica dos tipos de componentes web (Kassem, 2000):

- *Servlet* es un componente que provee al desarrollador de aplicaciones web un mecanismo simple y consistente para extender la funcionalidad de un servidor web con todas las características de Java. Los *servlets* son independientes de la plataforma y consumen menos recursos al ser cargados sólo la primera vez que se solicitan sus servicios. Las siguientes peticiones crearan hilos de ejecución. Un servidor web alberga clases de java *servlets* que se ejecutan dentro de un contenedor de *servlets*. El servidor web mapea un conjunto de direcciones URLs a un *servlet* para que peticiones por HTTP a estas direcciones invoquen al *servlet* mapeado. Cuando un *servlet* recibe un petición de un cliente, este genera una respuesta, posiblemente invocando lógica de negocios en un Enterprise bean o haciendo una búsqueda en una base de datos de forma directa. El *servlet* manda la respuesta como un documento HTML o XML a quien lo pidió.
- *JSP (JavaServer Pages)* provee una manera de generar contenido dinámico para un cliente web. Un JSP es un documento basado en texto que describe como procesar una petición para crear una respuesta. Un JSP contiene una plantilla de datos para dar formato al documento web con elementos HTML o XML y elementos de JSP o *scriptlets* para generar contenido dinámico en el documento web.

Los componentes web son albergados por: contenedores web y contenedores de JSPs, todos estos referidos colectivamente como contenedores web.

2.9.2 MVC

La arquitectura MVC (*Model, View, Controller*) se encarga de separar las cuestiones de diseño (persistencia de datos, presentación y control) centralizando el control y evitando duplicidad de código y nos permite hacer la aplicación más fácil de modificar (Kassem, 2000).

La arquitectura MVC organiza una aplicación interactiva en tres módulos separados: uno para el modelo de la aplicación el cual provee representación de datos y lógica del negocio, el

segundo para las vistas que proveen la presentación de los datos y las entradas de información del usuario, y el tercero para el controlador que se encarga de despachar las peticiones y el flujo de control (Kassem, 2000).

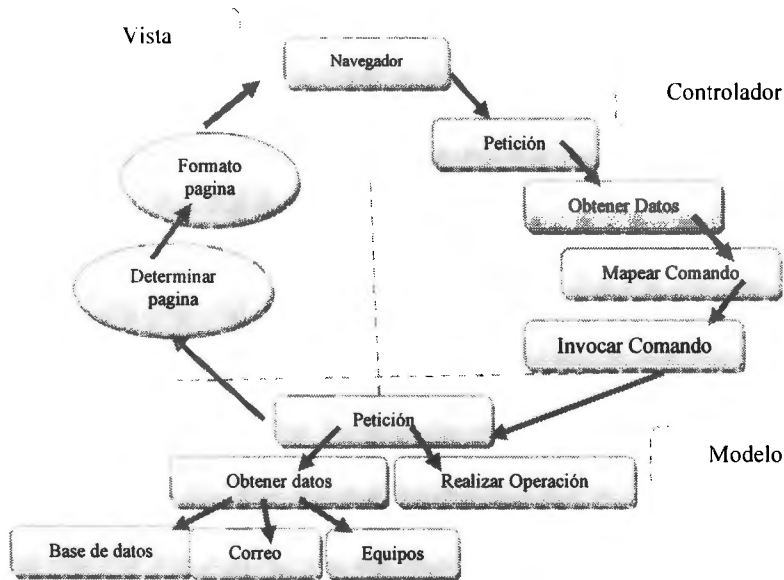


Figura 2.10 Arquitectura MVC (Kassem, 2000)

En la figura 2.10 se puede observar el ciclo de vida de una petición de un cliente en una arquitectura MVC desde que se hace una petición al navegador y el controlador obtiene, mapea e invoca un comando que genera una petición en el modelo ya sea para obtener datos o realizar alguna operación y entregar al usuario una nueva página (vista) con la respuesta de su petición.

2.10 Resumen

Para ofrecer una respuesta al problema planteado de la administración de equipos de red, se propone un sistema de información para la administración de equipos de red. Este sistema tomará en cuenta las áreas funcionales de la administración de las telecomunicaciones que son: administración de fallas, administración de la contabilidad, administración de la configuración, administración del desempeño y administración de la seguridad.

Las posibles tecnologías que se encontraron para construir el sistema de información se pueden dividir en 2 grupos dependiendo de su papel dentro del sistema: protocolos de administración de red y protocolos para conexión remota.

Los protocolos de administración de red discutidos en este trabajo son: SNNMP y CMIP. SNMP cuenta con cinco operaciones básicas: GET, GET NEXT, SET, GET RESPONSE y TRAP; Mientras que CMIP cuenta con 7 operaciones básicas: M-EVENT-REPORT, M-GET, M-SET, M-ACTION, M-CREATE, M-DELETE, M-CANCEL-GET. Las ventajas que presentan uno sobre otro son: SNMP es un protocolo más utilizado y del cual se cuenta con más información, sin embargo es un protocolo inseguro y las mejores prácticas dicen que solo sea usado como protocolo de lectura de datos. CMIS es un protocolo mucho más complejo y menos comúnmente utilizado, debido a la dificultad de su implementación.

Los protocolos para la conexión remota a equipos de red planteados en este trabajo son: Telnet y SSH, Las ventajas que presentan uno sobre otro son que SSH es un protocolo más seguro ya que utiliza encriptación y los datos enviados no viajan en texto claro como en telnet.

Java es un lenguaje de programación orientado a objetos, portable, robusto que soporta varios hilos de ejecución con la posibilidad de correr en un ambiente Web para poder ser utilizado por varios usuarios, brindando así la ventaja de disponibilidad y fácil acceso a través de un navegador web, sin la necesidad de instalar aplicaciones del lado del cliente. Para lograr conseguir un buen desarrollo se necesitan aplicar principios básicos de programación orientada a objetos para agregar flexibilidad y lograr un diseño fácil de mantener y reutilizar, a través del uso de una arquitectura, en este caso MVC, que nos permita una separación funcional del código.

Capítulo 3 Sistema de Administración de Equipos de Red

3.1 Modelo de Factores Críticos

Al hacer el análisis del sistema para la administración de equipos de red se buscó un modelo de factores críticos para este tipo de sistemas, sin embargo, no se encontraron referencias recientes que respondieran esta pregunta por lo que se propone un modelo de factores críticos para la administración de equipo de red basado en la propuesta de Stallings (1993).

Los 10 factores críticos propuestos son los siguientes:

- Facilidad de uso
- Seguridad
- Automatización mejorada
- Alta de usuarios
- Reportes mejorados
- Capacidad de Restauración
- Habilidad de agregar o borrar
- Monitoreo de la disponibilidad
- Re enrutamiento de tráfico
- Monitoreo del tiempo de respuesta

Para comprender la percepción de los administradores de red ante estos sistemas y la importancia que ellos le dan a estos 10 factores críticos, se realiza una encuesta de opinión de 10 preguntas, la cual se encuentra en el Anexo A.

Se realizan 18 encuestas a mexicanos de varios estados de la república con un perfil de administradores de red con una experiencia entre 2 y 10 años en el control y monitoreo de equipos de red y administrando un número considerable de equipos cuya administración se vuelve compleja. Los resultados de estas encuestas se describen y analizan a continuación:

En la figura 3.1 se muestra el criterio de facilidad de uso que toma en cuenta que tan amigable es para un usuario el uso de una herramienta de administración de telecomunicaciones. La importancia que tiene este criterio para los administradores de red es

alta ya que el 28% de los encuestados lo califica con 1 y 3 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

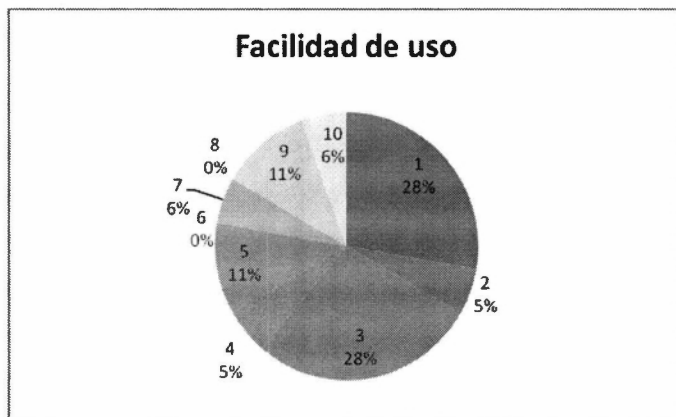


Figura 3.1 Criterio de: Facilidad de Uso

En la figura 3.2 se muestra el criterio de seguridad que toma en cuenta que tan confiable es el sistema permitiendo el acceso sólo a usuarios autorizados, así como una conexión segura a los equipos de red. La importancia que tiene este criterio para los administradores de red es alta, ya que el 33% lo califica con 1 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

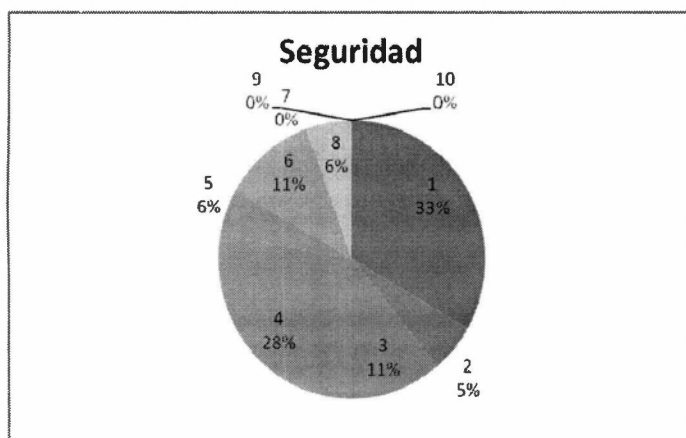


Figura 3.2 Criterio de: Seguridad

En la figura 3.3 se muestra el criterio de automatización mejorada el cual consiste en automatizar procesos de la administración de equipos de red para realizar tareas repetitivas de manera programada. La importancia que tiene este criterio para los administradores de red es

alta, ya que el 22% lo califica con 2 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

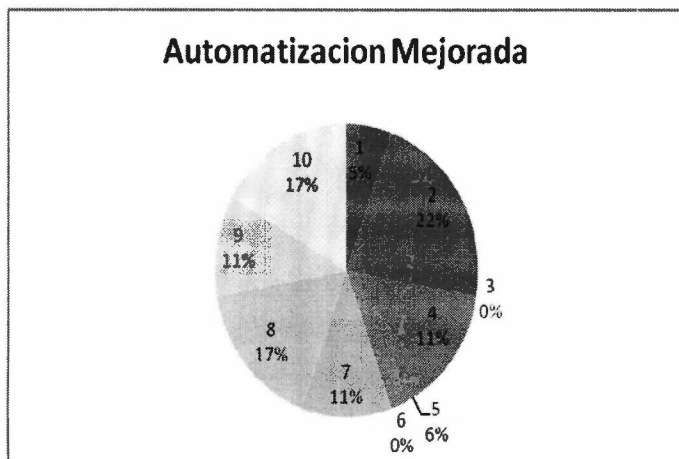


Figura 3.3 Criterio de: Automatización Mejorada

En la figura 3.4 se muestra el criterio de alta de usuarios el cual consiste en poder introducir un nuevo usuario capaz de hacer uso del sistema. La importancia que tiene este criterio para los administradores de red es baja, ya que el 28% lo califica con 9 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

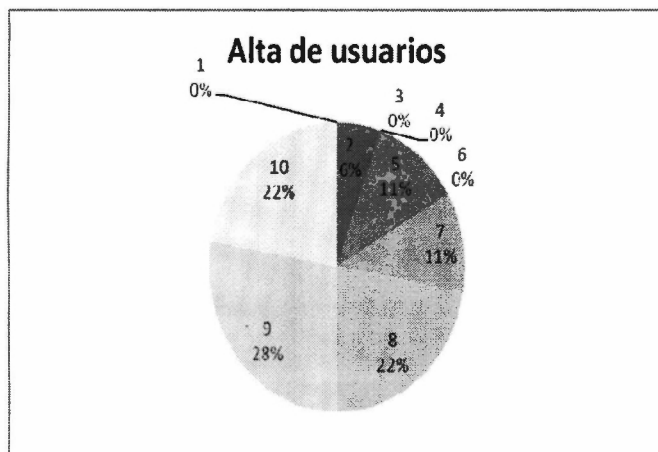


Figura 3.4 Criterio de: Alta de usuarios

En la figura 3.5 se muestra el criterio de reportes mejorados el cual consiste en presentar información útil para la toma de decisiones en reportes completos, claros y precisos. La

importancia que tiene este criterio para los administradores de red es media, ya que el 17% lo califica con 4 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

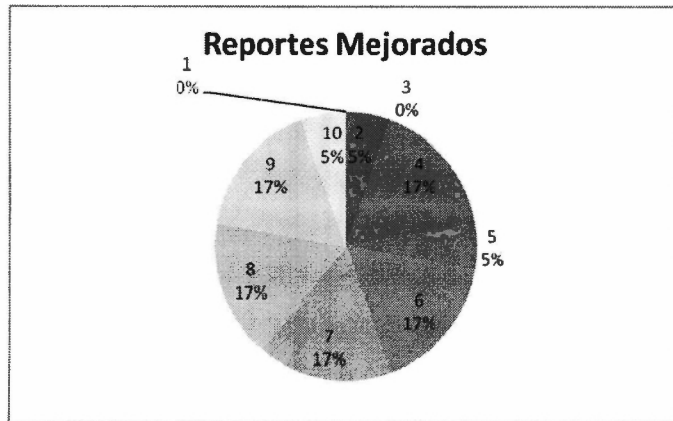


Figura 3.5 Criterio de: Reportes Mejorados

En la figura 3.6 se muestra el criterio de capacidad de restauración el cual consiste en poder regresar el sistema a su estado operacional, después de algún percance, desastre o pérdida de información. La importancia que tiene este criterio para los administradores de red es media, ya que el 22% lo califica con 5 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

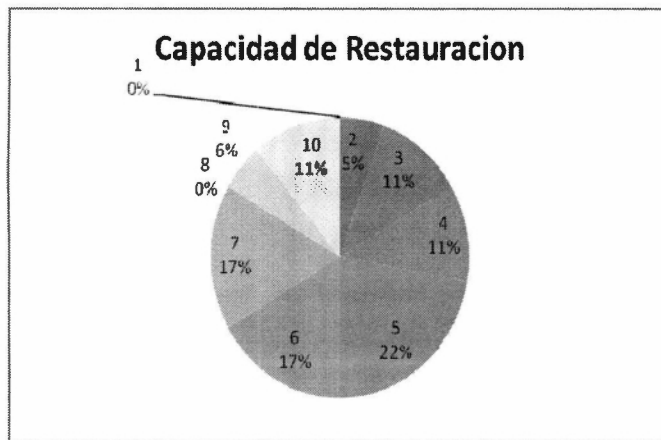


Figura 3.6 Criterio de: Capacidad de Restauración

En la figura 3.7 se muestra el criterio de habilidad de agregar o borrar que consiste en poder generar altas y bajas de dispositivos administrados dentro del sistema. La importancia que

tiene este criterio para los administradores de red es baja, ya que el 22% lo califica con 9 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

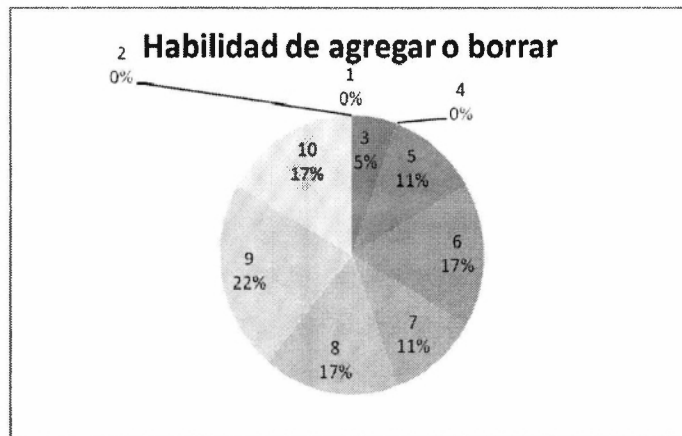


Figura 3.7 Criterio de: Habilidad agregar o borrar

En la figura 3.8 se muestra el criterio de monitoreo de la disponibilidad que consiste en reportar si algún dispositivo de red se encuentra fuera de operación para poder dar solución a este problema, así como la notificación adecuada cuando este equipo se encuentre de nuevo operacional. La importancia que tiene este criterio para los administradores de red es alta, ya que el 28% lo califica con 1 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

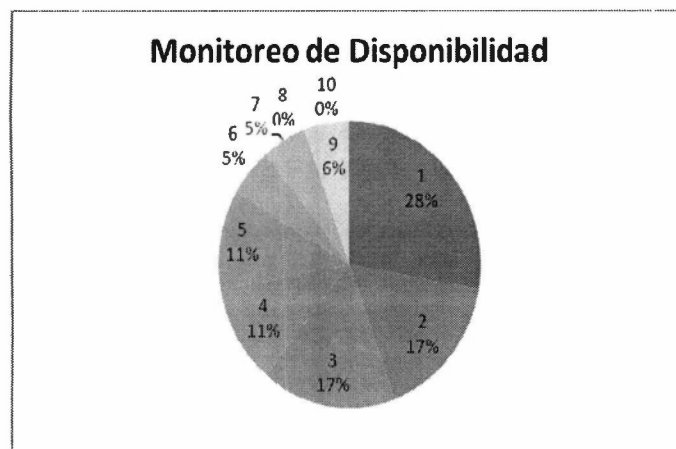


Figura 3.8 Criterio de: Monitoreo Disponibilidad

En la figura 3.9 se muestra el criterio de re enrutamiento de tráfico el cual consiste en poder reconfigurar los equipos para conmutar el tráfico por una ruta redundante. La importancia que tiene este criterio para los administradores de red es media, ya que el 33% lo califica con 6 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.



Figura 3.9 Criterio de: Re enrutamiento de Tráfico

En la figura 3.10 se muestra el criterio de monitoreo del tiempo de respuesta que toma en cuenta cuanto tiempo le toma a un dispositivo de red entregar la información que se le está solicitando. La importancia que tiene este criterio para los administradores de red es alta, ya que el 22% lo califica con 2 en la escala del 1 al 10 siendo 1 lo más importante y 10 lo menos importante.

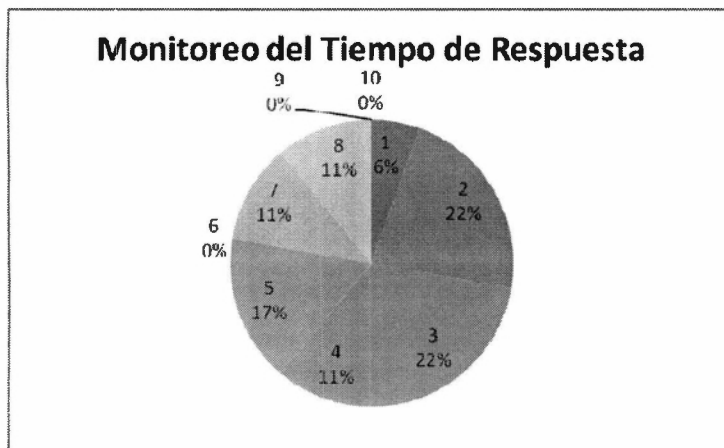


Figura 3.10 Criterio de: Monitoreo del Tiempo de Respuesta

Tomando en cuenta los 10 factores críticos se obtuvo un porcentaje global de importancia basado en la cantidad de usuarios y la calificación asignada. Debido a que no tienen la misma importancia un 33% que califico con 1, que un 33% que califico con 10, el 33% calificado con 1 tiene una importancia alta porque el 1 significa en la escala que es el más importante, mientras que el 33% que califico con 10 tiene una importancia baja, ya que el 10 en la escala es el menos importante con respecto a los demás factores críticos. En la tabla 3.1 se muestran estos porcentajes globales de importancia, ordenados de mayor a menor importancia.

Factor Crítico	Porcentaje Global	Importancia
Seguridad	77.22	1
Monitoreo de disponibilidad	76.67	2
Facilidad de uso	70.56	3
Monitoreo de tiempo de respuesta	68.89	4
Capacidad de restauración	52.22	5
Automatización mejorada	50.00	6
Re enrutamiento de tráfico	45.00	7
Reportes mejorados	43.89	8
Habilidad de agregar o borrar	35.00	9
Alta de usuarios	30.56	10

Tabla 3.1 Resultados globales de la encuesta de criterios del sistema

En la figura 3.11 se muestran gráficamente los factores críticos con sus porcentajes globales de importancia, tomando en cuenta no sólo el número de personas que los calificaron sino también la calificación asignada.

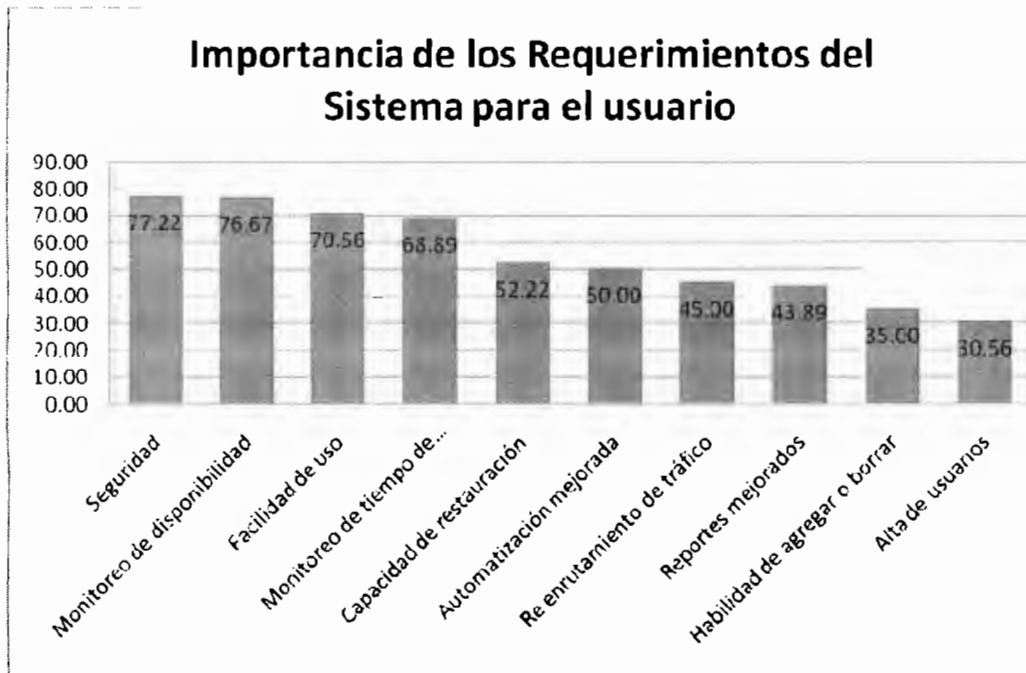


Figura 3.11 Importancia de los requerimientos del sistema para el usuario

3.2 Propuesta de Arquitectura de un Sistema de administración de equipos de red

3.2.1 Arquitectura del sistema

En la figura 3.12 se muestra la arquitectura propuesta para un sistema de información para la administración de equipos de red. Los componentes que lo forman son un subsistema web que permite que el sistema que pueda ser consultado por varios usuarios de forma web y un subsistema de interconexión que se encarga de comunicarse con el subsistema web para establecer comunicación con los equipos de red y servidores externos como servidor de correos y servidor de base de datos.

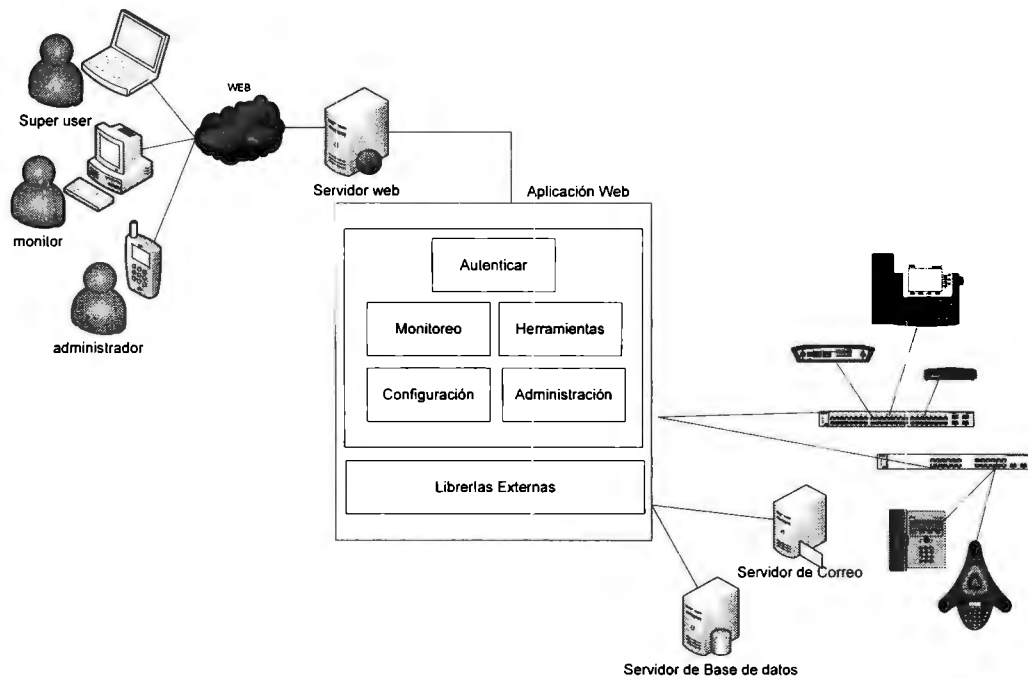


Figura 3.12 Arquitectura de referencia propuesta para un sistema de información para la administración de equipos de red

De acuerdo con el modelo de factores críticos para el sistema de administración de equipos de red, el producto consta de:

- Subsistema Web: para el acceso y la asignación de un perfil con el cual se podrá navegar por la aplicación principal, la cual consta de:
 - Módulo de monitoreo
 - Módulo de herramientas
 - Módulo de configuración
 - Módulo de administración del sistema

- Subsistema de Interconexión: referido de ahora en adelante como librerías de interconexión o librerías externas (la implementación de las cuales están fuera del alcance del proyecto, por lo cual se utilizarán librerías de interconexión existentes).

3.2.2 Diseño de Procesos

Para satisfacer el factor crítico de facilidad de uso, se diseñan interfaces gráficas concisas, sencillas e intuitivas.

Para satisfacer el factor crítico de seguridad y considerando que los roles de los distintos usuarios del sistema no son los mismos, se crean diferentes perfiles con diferentes niveles de autorización dentro del sistema para satisfacer distintas necesidades.

Tipos de usuarios del sistema:

El sistema se divide en 3 vistas principales, las cuales dependen del perfil que el usuario tenga dado de alta en la base de datos. Los perfiles permitidos son:

- **Monitor:** es el perfil de nivel de autorización menor, con el cual el usuario solo puede realizar consultas del sistema.
- **Administrador:** es el perfil de nivel de autorización medio, con el cual el usuario puede realizar consultas al sistema así como la configuración de activos fijos a través del mismo.
- **Super user:** es el perfil de nivel de autorización mayor, con el cual el usuario puede realizar todas las actividades, desde consultas al sistema, configuraciones de activos fijos y dar altas bajas modificaciones tanto de equipos como de usuarios.

Procesos del sistema

En la figura 3.13 se muestra el diagrama de casos de uso del sistema de información para la administración de equipos de red. En este diagrama se pueden observar los procesos que el sistema posee divididos en 4 módulos (monitoreo, herramientas, configuración y administración), así como los actores (o perfiles) que pueden usar el sistema.

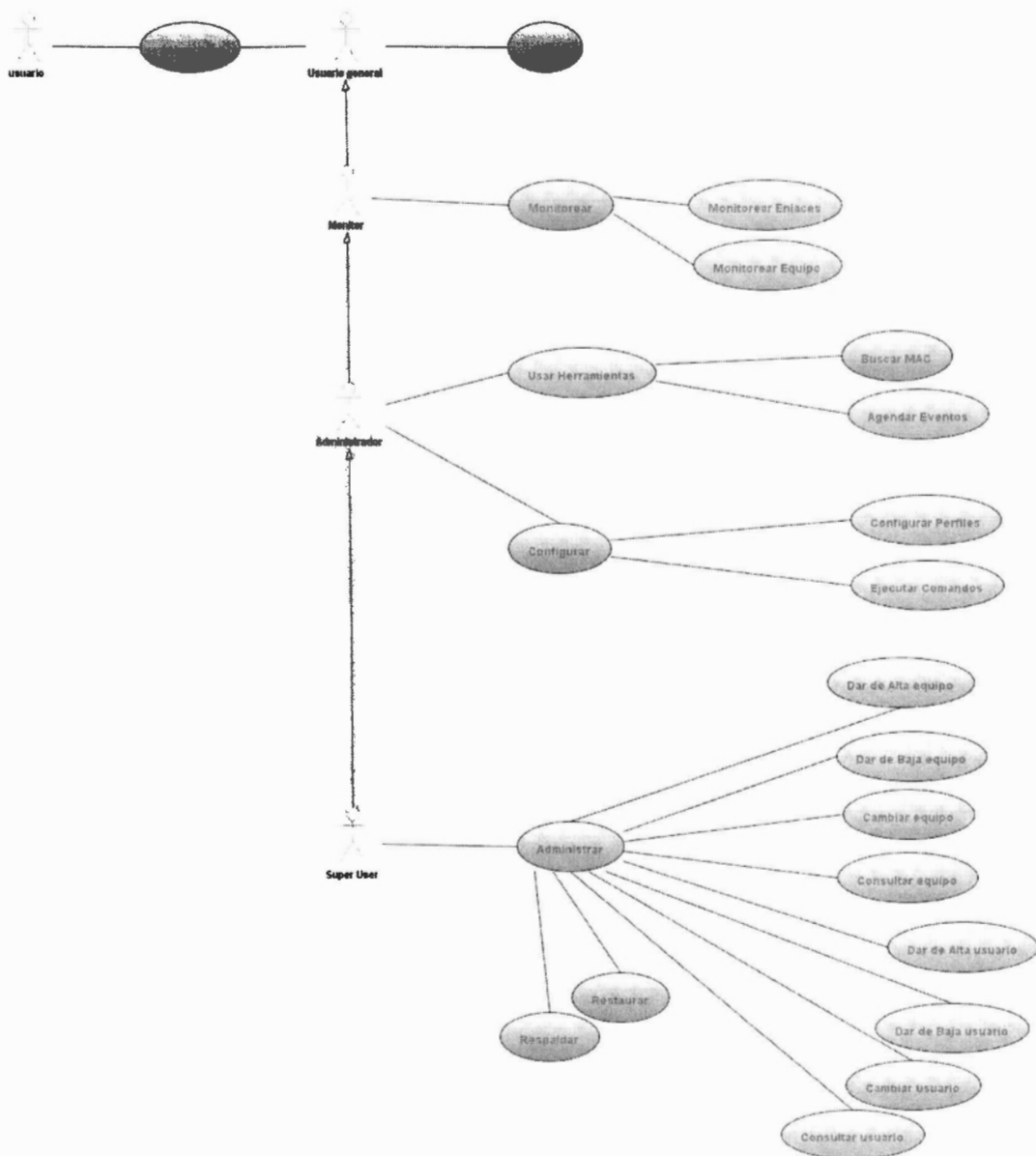


Figura 3.13 Diagrama de casos de uso

Descripción de los procesos del sistema representados por casos de uso del sistema:

El monitor administrador y super user se autentican a la aplicación a través de un navegador web.

El monitor, administrador y super user puede entrar al módulo de monitoreo en el cual se tienen los siguientes servicios:

- Monitoreo de enlaces: permite ver la carga de tráfico que posee cada enlace monitoreado.
- Monitoreo de equipos: permite ver el status de los equipos de red (apagado o encendido).

El administrador y super user pueden entrar al módulo de herramientas en el cual se pueden realizar las siguientes tareas:

- BuscaMac: permite encontrar un equipo que esté conectado a algún dispositivo de la red a través de su dirección física conocida como dirección mac.
- Agregar eventos: permite programar un evento en un equipo de red. Se le llama evento configurar un equipo de manera automática en un horario específico.

El administrador y super user pueden entrar al módulo de configuración en el cual se tienen los siguientes servicios:

- Configura Perfiles: permite configurar de manera automática un perfil determinado de algún dispositivo en la red. Ejemplo Si se tienen teléfonos IP se puede configurar un perfil de teléfono IP con una configuración específica para estos dispositivos que garantice la homogenización de las configuraciones y ayude a minimizar posibles errores en las mismas.
- Ejecuta Comandos: permite ejecutar una serie de comandos a varios equipos. Ejemplo obtener todas las configuraciones de los equipos de red. Se puede utilizar para configurar varios equipos, pero su uso está enfocado a obtener consultas de los equipos de red.

El super user es el único perfil que puede entrar al módulo de administración del sistema por cuestiones de seguridad. En este módulo se pueden realizar las siguientes tareas de administración:

- Alta Equipo: permite dar de alta un nuevo equipo de red en el sistema.
- Baja Equipo: permite dar de baja un equipo de red existente en el sistema.
- Cambio Equipo: permite realizar un cambio a un equipo de red existente en el sistema.
- Consulta Equipo: permite consultar equipo de red existente en el sistema.

- Alta Usuario: permite dar de alta un nuevo usuario y asignarle un perfil para acceder al sistema.
- Baja Usuario: permite dar de baja un usuario existente en el sistema.
- Cambio Usuario: permite realizar cambios de la información de un usuario existente en el sistema.
- Consulta Usuario: permite consultar la información de un usuario existente en el sistema.
- Respaldo: permite respaldar toda la base de datos del sistema.
- Restaurar: permite restaurar toda la base de datos del sistema (se necesita archivo de respaldo).

Capítulo 4 Caso de estudio

4.1 Introducción

El sistema de administración de las telecomunicaciones TELECOMSIST se implantó en el Tecnológico de Monterrey Campus Ciudad de México para ayudar a la administración de los dispositivos de red que ahí operan. Dentro del Campus se tienen alrededor de 900 teléfonos, 300 antenas y 160 switches en todo el campus.

Se dieron de alta los siguientes dispositivos para ser administrados a través del sistema:

- 408 Teléfonos (Representa el 45.33% del total)
- 129 Antenas (Representa el 43% del total)
- 160 Switches (Representa el 100% del total)
- 160 Monitores de los Switches (Representa el 100% del total)
- 2 Perfiles de configuración (antenas, teléfonos)

Se dieron de alta 5 cuentas con diferentes perfiles, para los empleados del área de telecomunicaciones. Dos cuentas de monitor, dos cuentas de administrador y una cuenta de super user.

4.2 Funcionalidades del sistema implantado

Todos los requerimientos arriba del 50% de importancia se incluyeron dentro de las funcionalidades del sistema, excepto el monitoreo del tiempo de respuesta, debido al alcance que se dio al proyecto, así como las necesidades actuales del Tecnológico de Monterrey Campus Ciudad de México.

Características

Facilidad de uso

Seguridad

Funcionalidad del sistema

El sistema posee una interface de usuario amigable y sencilla para realizar sus funciones.

El sistema garantiza la seguridad a través de

Capacidad de restauración	la implementación del protocolo SSH para la configuración de dispositivos y el protocolo SNMP solo para el monitoreo, así como perfiles de usuarios con diferentes permisos. El sistema posee la capacidad de respaldo de la base de datos con la cual se puede re configurar.
Capacidad de agregar o borrar	El sistema puede agregar o borrar entradas dentro de la base de datos para tener información actualizada.
Monitoreo de disponibilidad	El sistema tiene un modulo de monitoreo de disponibilidad de los equipos de red que estén dados de alta.
Re enrutamiento de tráfico	El sistema no posee un método de re enrutamiento de tráfico debido al alcance del proyecto, pero pueden integrarse como un trabajo futuro.
Automatización mejorada	El sistema cuenta con la funcionalidad de auto configuración de dispositivos con perfiles establecidos en el mismo, así como configuraciones programadas con fechas y horarios específicos.
Alta de usuarios	El sistema tiene una base de datos de usuarios con altas, bajas, modificaciones y consultas.
Reportes mejorados	El sistema no podrá generar reportes debido al alcance del proyecto, pero pueden integrarse como un trabajo futuro.
Monitoreo de tiempo de respuesta	El sistema no tendrá un modulo de monitoreo de tiempo de respuesta debido al alcance del proyecto, pero pueden integrarse como un trabajo futuro.

Tabla 4.1 Funcionalidades del sistema

4.3 Arquitectura específica del sistema

Integrando todo lo descrito anteriormente, la figura 4.1 muestra la arquitectura propuesta para el sistema de administración de equipos de red para el Tecnológico de Monterrey Campus Ciudad de México, en la cual un usuario puede conectarse ya sea a través de un equipo computacional o un dispositivo móvil con acceso a internet a la página web almacenada en el servidor y a través del subsistema web y el subsistema de interconexión podrá conectarse a diferentes dispositivos para obtener información o configurar algún parámetro de administración.

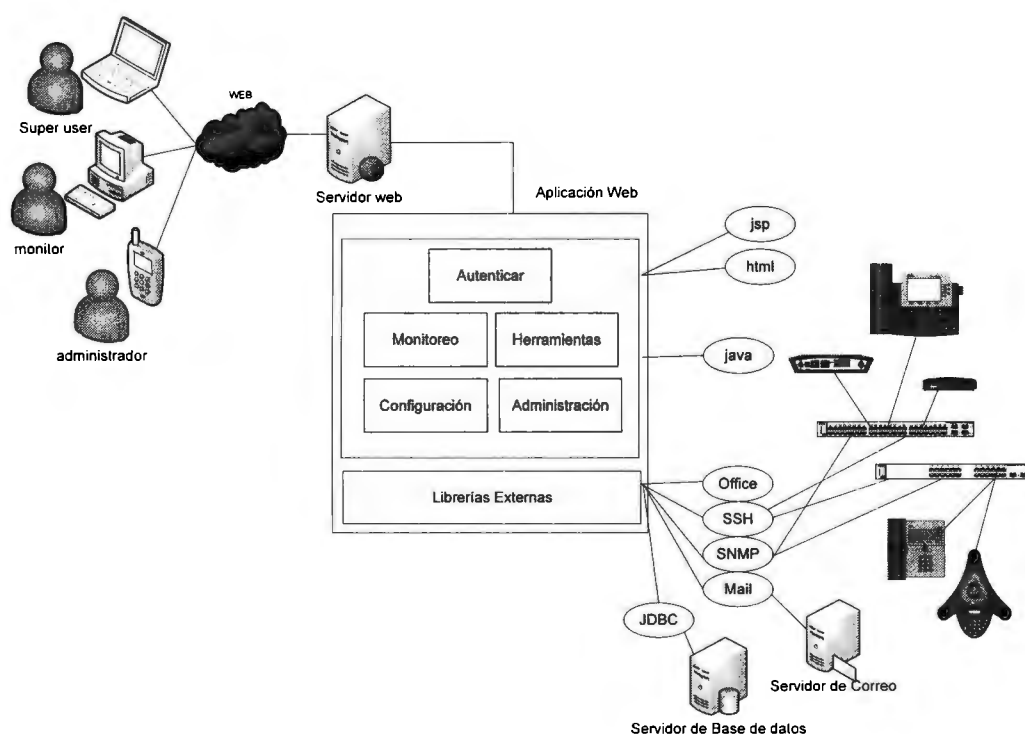


Figura 4.1 Arquitectura específica del sistema

4.4 Tecnologías utilizadas

El código de aplicación específico se encarga de la funcionalidad de la aplicación. En este caso se utilizó el lenguaje de programación Java para satisfacer los factores críticos descritos en el apartado anterior utilizando el patrón de diseño MVC. Para la representación de las vistas, se utilizaron JSP y páginas HTML, como controlador el patrón de diseño utiliza un

archivo de configuración conocido como struts-config.xml y para poder completar la funcionalidad del sistema se utilizaron las siguientes librerías de interconexión:

- SSH (Librería para el acceso a los equipos a través de SSH)
- SNMP (Librería para obtener valores a través de SNMP)
- Java Mail (Librería para mandar mails)
- POI (Librería para acceder ficheros con formato Microsoft)
- Struts (Librería para soportar el modelo MVC)
- JDBC (Librería para la conexión con la base de datos)

Durante la fase de migración se llevaron a cabo las tareas necesarias para poder poner en operación el sistema. Se instaló el sistema en un servidor de aplicaciones (Tomcat), se instaló la base de datos (My SQL) en un servidor alterno. Se pobló la base de datos con los datos necesarios de los equipos que compondrían el inventario tecnológico.

En la figura 4.2 se muestra el diagrama entidad-relación que conforma la base de datos del sistema, está compuesto de 7 tablas:

Edificios (que posee los campos: id_ed, descripción, vlanvoz, vlandatos, vlanwireless, vlandefault, campus). Con el identificador único (llave primaria) id_ed que también es utilizada para relacionar esta tabla con la tabla de switches (con los campos: idsw, ipsw, nombresw, modelosw, ossw, serialsw, descripcionsw, stacksw, id_ed) ya que con esto se pueden determinar los parámetros globales de configuración por edificio.

Cada switch a su vez tiene un monitor (que posee los campos: idsw, estados, cambiossw) por lo cual la tabla switches está relacionada con la tabla monitor y es a través de esta relación que se puede satisfacer el factor de monitoreo de la disponibilidad de los factores críticos propuestos.

Switches se relaciona a su vez con las tablas teléfonos (con los atributos: idtel, mactel, ided, puerto, serialtel, idsw, modelotel, responsable, dn) y antenas (con los campos: ipad, radioethernetap, radiomacap, primarycontroller, secondarycontroller, serialap, puertoap, idsw, nombreap, idperfil, ipap, ubicacionap, groupnameap, modeloap) para indicar que puerto de que switch corresponde a un teléfono ip o un antena. Para poder satisfacer el criterio de automatización mejorada y poder configurar dispositivos de forma automática, se crean en la tabla de perfiles (con los atributos: idperfiles, descripcionperfiles, tipoperfil, selectperfiles,

configperfiles, parametrosperfiles) plantillas de configuración y datos necesarios (de teléfonos o antenas en este caso ya que son los dos único perfiles existentes).

La tabla configuraciones (con los atributos: idconfig, descripcionconfig, fechaconfig, config, comandosconfig, equipoconfig, idusr) se utiliza para realizar configuraciones a los equipos a través del sistema, distintas de los perfiles ya establecidos y con ello guardar un histórico de los cambios aplicados a cada equipo y el usuario que realizó dicho cambio también para satisfacer el criterio de automatización mejorada y cuidar el factor de seguridad de la aplicación.

Por último la tabla de usuarios (con los atributos: ipusuario, passwordusr, nombreusr, apellidusr, emailusr, perfilusr) contiene a los usuarios autorizados a usar el sistema, así como los permisos que estos poseen dependiendo del perfil de usuario que se les asigne para satisfacer los criterios de seguridad y alta de usuarios.

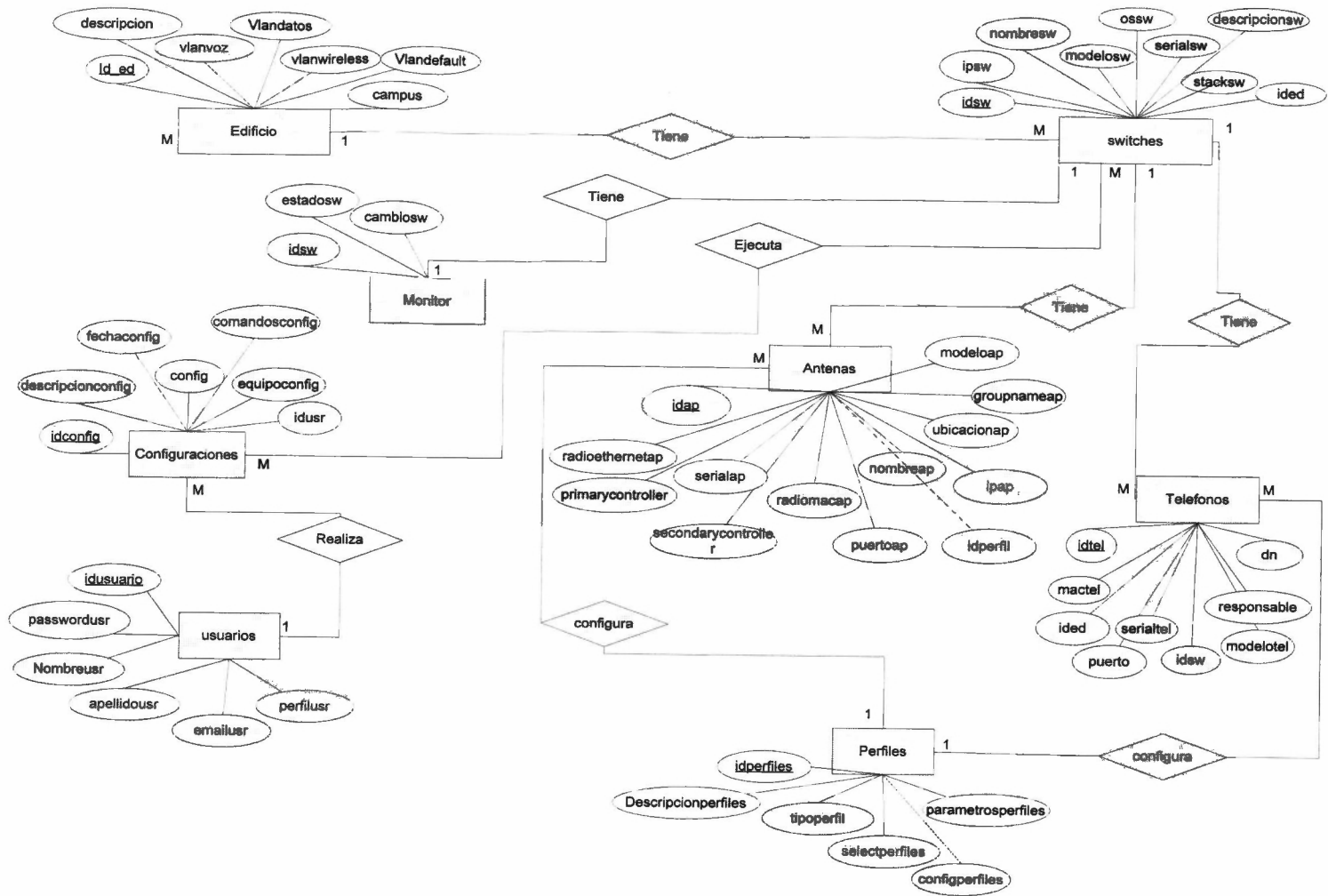


Figura 4.2 Diagrama Entidad-Relación de la Base de datos

4.5 Vistas del sistema

A continuación se describen 3 de las funcionalidades más utilizadas del sistema: Busca Mac, Configura Perfiles y Ejecuta Comandos. Para explicar mejor el funcionamiento estas tareas se muestran pantallas del sistema que describen el proceso que se sigue así como los datos de entrada y salida de cada una de ellas.

En la figura 4.3 se puede observar una de las vistas del sistema para buscar una dirección física (conocida como dirección mac) que esté conectada a la red a través del sistema de información para la administración de equipos de red. En esta primera pantalla se piden los datos necesarios para realizar la búsqueda como son: dirección mac y dependiendo del tipo de búsqueda (por árbol o por edificio) nos pide un segundo parámetro para la búsqueda por árbol la raíz del STP y para realizar la búsqueda por edificio podemos especificar el prefijo que identifica a cada edificio o si es su defecto no lo conocemos se hace la búsqueda en todos, dados estos parámetros se da click en el botón “Busca Mac”.

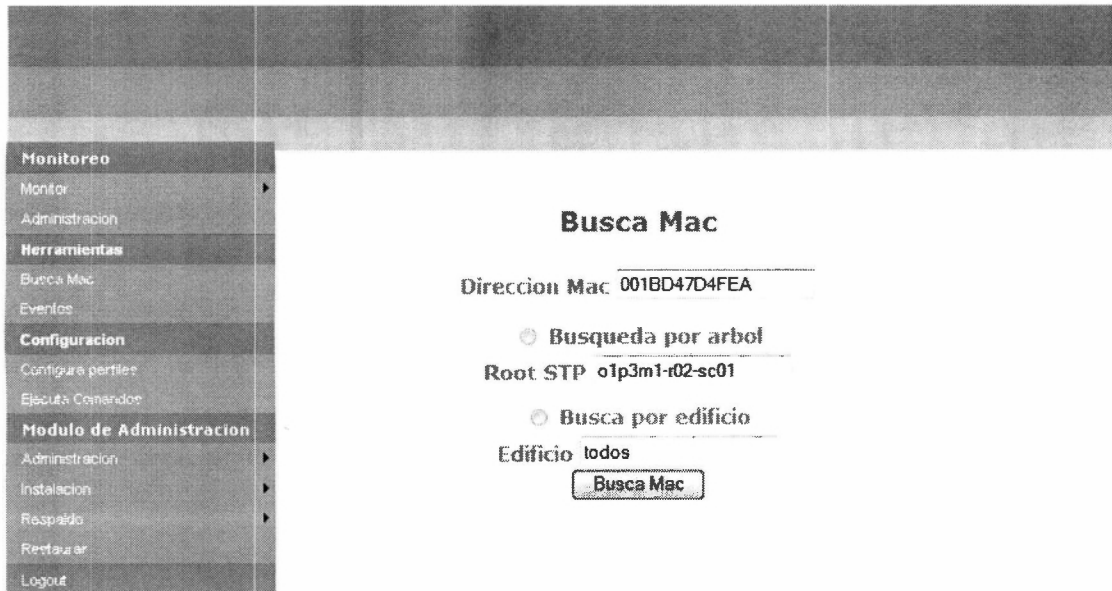


Figura 4.3 Pantalla del Sistema funcionalidad Busca Mac

Una vez que el sistema realice la búsqueda con los parámetros definidos, esta nos lleva a la siguiente pantalla (figura 4.4) en la cual se despliega el resultado de la búsqueda y nos da los

siguientes valores: *switch*, puerto y *vlan* de donde se encuentra conectado el equipo que se deseaba encontrar.

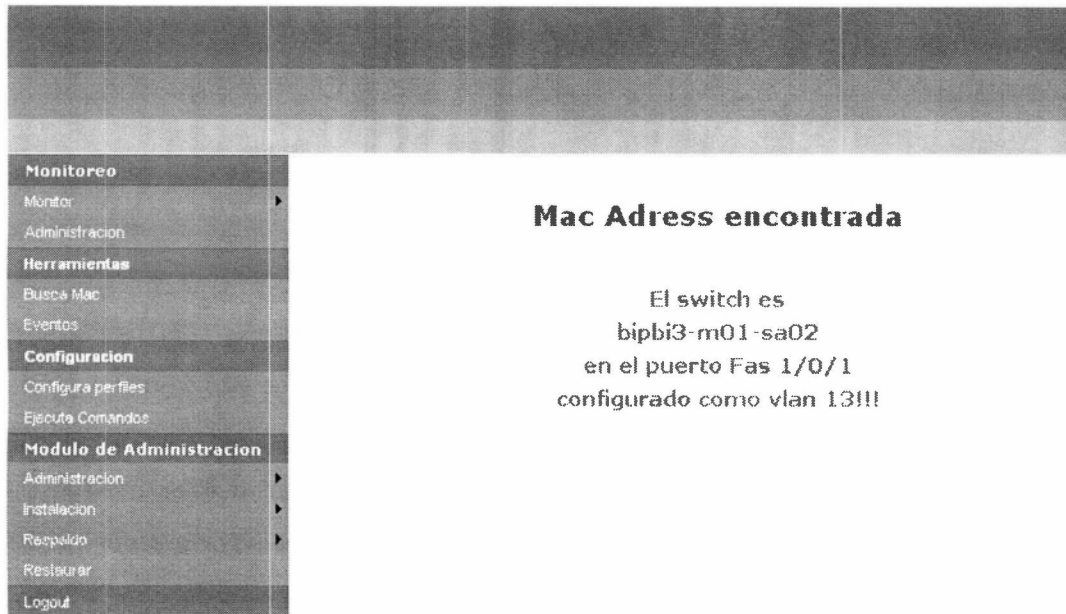


Figura 4.4 Pantalla del Sistema funcionalidad Busca Mac (Resultado)

En la figura 4.5 se muestra la funcionalidad de “Ejecuta Comandos” en la cual se pueden realizar configuraciones específicas a uno o más equipos a través del nombre de los mismos. Por ejemplo si se desea configurar todo un edificio se antepone el prefijo del edificio, o si se desea una configuración más específica por piso o *switch* se va agregando mayor detalle del nombre del *switch*.

Ya que el sistema está programado para poder utilizar comodines y configurará todos los equipos que hagan match con el prefijo del nombre, aprovechando la nomenclatura de los mismos, la cual está basada en su ubicación geográfica. En la primera pantalla el sistema nos pide los datos del equipo (o prefijo del equipo o equipos) que se van a configurar así como los comandos que se ejecutaran (separados por una coma) y una descripción de por qué se ejecuta este comando para guardar un histórico y en la parte inferior podemos ver dicho histórico.

Si queremos ejecutar el o los comandos damos click en el botón de “Ejecutar” y por otro lado si sólo queremos consultar alguna configuración realizada anteriormente la seleccionamos de la parte inferior de la ventana y le damos click al botón de “Desplegar”. Todo esto está dentro

de una misma vista para ser más amigable y presentar la información de manera más rápida y sin que el usuario tenga que dar demasiados clicks para obtener la información que necesita y así cumplir con el criterio de facilidad de uso.

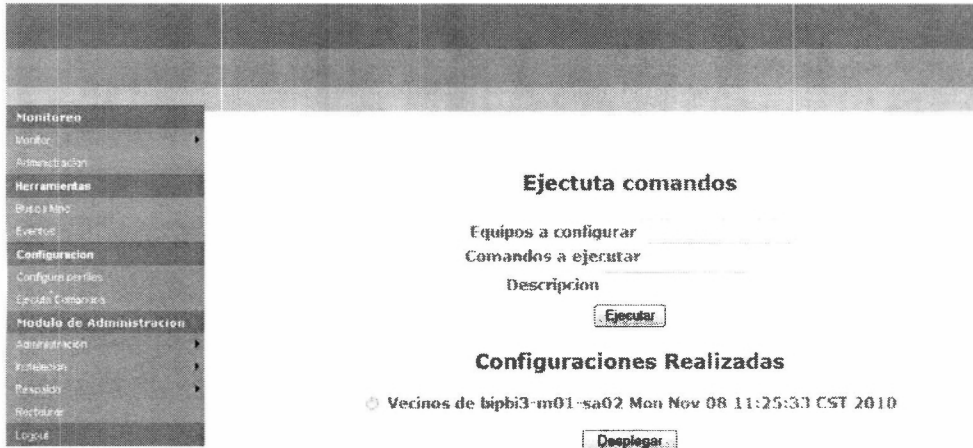


Figura 4.5 Pantalla del Sistema funcionalidad Ejecuta Comandos

Una vez que el sistema realice la configuración que se le solicito este mostrará la misma ventana con las nuevas entradas de dicha configuración en la parte inferior de la pantalla como parte del histórico, así que seleccionamos la configuración que deseamos ver y le damos click al botón “Desplegar”. En la figura 4.6 podemos observar un ejemplo de histórico con los datos que son guardados cada que se realiza una configuración desde el sistema.

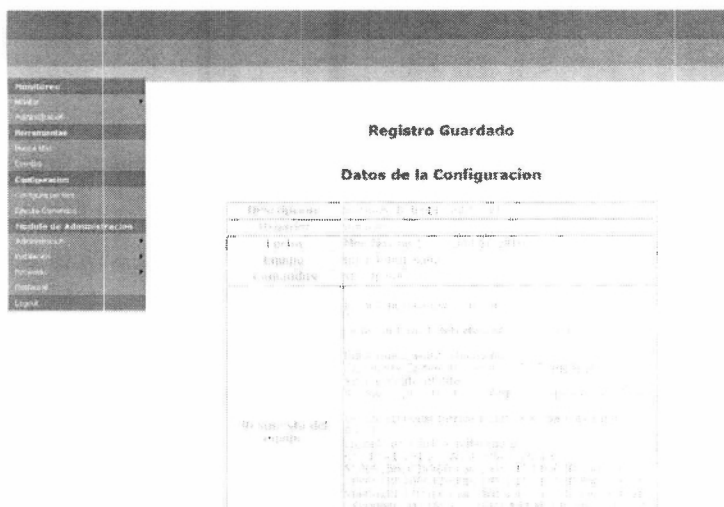


Figura 4.6 Pantalla del Sistema funcionalidad Ejecuta Comandos (Histórico)

Otra funcionalidad del sistema es “Configura Perfiles”, se muestra en la figura 4.7 la pantalla principal donde se piden los datos del tipo de perfil que se va a utilizar y algún dato que se conozca del mismo, se puede utilizar la dirección mac o el serial o una extensión o algún dato que se recuerde del equipo que se desea configurar, se recomienda usar datos únicos para reducir las búsquedas y que nos entregue menos resultados pero si no se puede poner un dato más general o incluso dejar vacío para consultar todos.

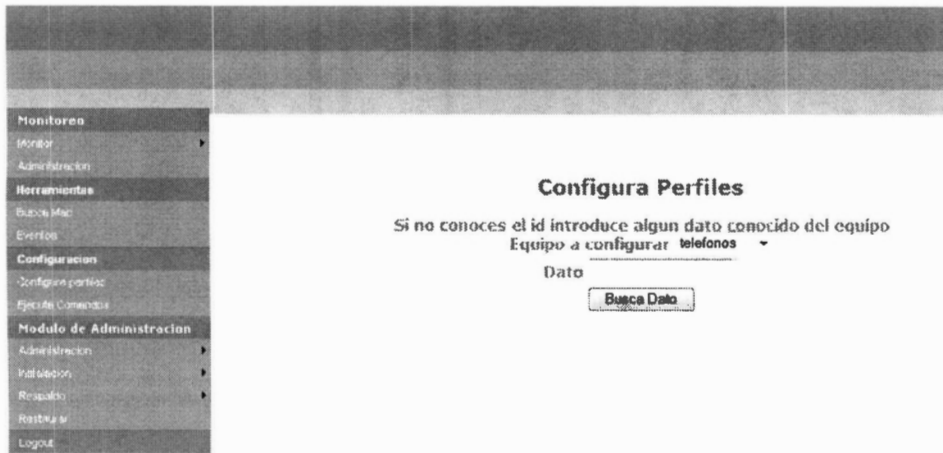


Figura 4.7 Pantalla del Sistema funcionalidad Configura Perfiles

Ya que hemos dado click en “Consultar” nos aparece la siguiente ventana con los resultados, así como la opción de redefinir la búsqueda si no se arroja el dispositivo que queremos configurar. En la figura 4.8 se muestra el resultado de una búsqueda de una antena inalámbrica para ser configurada. Una vez localizado el dispositivo a configurar este se selecciona y se da click en el botón de “Configura perfil” para que el sistema configure el puerto con los parámetros necesarios para este dispositivo.

4.6 Escenarios de Prueba

Se desarrollaron algunos escenarios de prueba para documentar como se realizaban determinados procesos sin el sistema propuesto y después como cambio dicho proceso una vez implantado el sistema de información para la administración de equipos de red. Cada uno de estos se explica a continuación:

Escenario de Prueba 1: Buscar puertos	
<p>Descripción del problema: Debido a la falta de documentación en la estructura de la red, la búsqueda de un puerto para poder configurarlo de manera adecuada para soportar un dispositivo en particular se vuelve muy laboriosa y tardada.</p>	
<p>Situación de uso: Cuando se necesita ubicar un nodo de red para realizar una configuración específica en dicho nodo. Por ejemplo:</p> <ul style="list-style-type: none"> • Dar de alta/Cambiar/Dar de baja una nueva impresora • Dar de alta/Cambiar/Dar de baja una nueva antena • Dar de alta/Cambiar/Dar de baja un teléfono IP • Dar de alta/Cambiar/Dar de baja un nodo para un usuario de SAP • Alguna configuración muy específica de algún dispositivo 	
<ul style="list-style-type: none"> • ¿Cómo se realizaba el proceso? 	<p><u>Opción 1:</u></p> <p>Se busca el puerto de forma manual a través de un dispositivo conocido como generador de tonos, que emite un tono y del otro extremo un segundo dispositivo recibe el tono y emite un sonido para poder ubicar los puertos a los que está conectado un equipo. Por lo cual una persona debe de estar en el cuarto de telecomunicaciones con el dispositivo receptor y la otra en el nodo que se quiere encontrar.</p> <p>La primera opción es muy tardada y requiere de al menos dos personas que se encuentren en los extremos uno con un dispositivo y el otro con el otro. De igual forma se requiere que el personal tenga acceso a los cuartos de telecomunicaciones para poder utilizar esta técnica. Si el nodo se encuentra en un cuarto de telecomunicaciones que no se había contemplado puede tomar mucho más de tiempo</p>

	<p><u>Opción 2:</u></p> <p>Se conecta una computadora o dispositivo (del cual se conozca la dirección física o dirección mac) Se busca de forma manual la dirección mac en los equipos en los que podría estar ese nodo</p> <p>Esta opción es un poco menos tardada pero requiere de personal con acceso a los equipos de red para poder utilizar esta técnica. Si el nodo se encuentra en un cuarto de telecomunicaciones que no se había contemplado puede tomar un poco más de tiempo</p>
<ul style="list-style-type: none"> • ¿Quién lo realizaba? 	<p>Personal de telecomunicaciones de diferentes áreas:</p> <ul style="list-style-type: none"> • Telefonía • Redes
<ul style="list-style-type: none"> • ¿Cómo se realiza el proceso con el sistema? 	<p><u>Opción 1:</u></p> <p>Se conecta un equipo con dirección mac conocida se introduce la dirección mac en el sistema, se escoge la opción de búsqueda por árbol y se introduce la raíz de STP (<i>spanning tree protocol</i>) y el sistema se encarga de buscar esa mac aprovechando la estructura que crea el protocolo de STP, al buscar el camino más corto del árbol que se genera con STP y entregándonos como resultado el switch en el que se encuentra el nodo, así como numero de puerto donde está conectado y la vlan en la que está configurado.</p> <p><u>Opción 2:</u></p> <p>Se conecta un equipo con dirección mac conocida se introduce la dirección mac en el sistema, se escoge la opción de búsqueda por edificio y se introduce el edificio en el que se quiere buscar o la palabra clave todos si no se conoce la ubicación del nodo y el sistema se encarga de buscar esa mac preguntado en todos los switches que se tienen dados de alta en la base de datos de activos tecnológicos, entregándonos como resultado el switch en el que se encuentra el nodo, así como numero de puerto donde está conectado y la vlan en la que está configurado.</p> <p>Las ventajas que presenta es que no se necesita que el usuario conozca de redes o dispositivos cisco, ni que tenga autorización dentro de estos equipos</p>

	para poder localizar una dirección mac utilizando dentro del sistema el modulo de herramientas y de ahí la opción de Busca mac.
<ul style="list-style-type: none"> • ¿Quién lo realiza? 	<p>Usuarios dados de alta en el sistema</p> <p>Perfiles que lo pueden utilizar:</p> <ul style="list-style-type: none"> • Monitor • Administrador • Super user

Tabla 4.2 Escenario de Prueba 1: Buscar Puertos

Escenario de Prueba 2: Aislar Sala	
<p>Descripción del problema: Debido a las diferentes necesidades de red algunas salas de computo requieren de alguna configuración especifica por algún evento como es aislar las salas de la red para impartir cursos de seguridad que podrían afectar la operación normal de la red si no se tomará esta precaución, pero por el uso de las mismas estas se desocupan después de las 10 por lo cual la configuración de las misma se puede necesitar en horario no laborales.</p>	
<p>Situación de uso: Cuando se necesita realizar alguna configuración especial en la salas de computo debido a algún evento. Por ejemplo:</p> <ul style="list-style-type: none"> • Aislar de la red una sala de computo • Regresar a la red una sala de computo 	
<p>1. ¿Cómo se realizaba el proceso?</p>	<p><u>Opción 1:</u></p> <p>Se accede al equipo para configurarlo de acuerdo al evento que se necesitara de forma remota en el horario requerido ya sea tarde o en sábados (horarios no laborales para el personal de redes) una vez realizado el cambio se debía revisar que la configuración se hubiera ejecutado de manera correcta</p> <p>Es la única opción para realizar un cambio para un evento en horario no laboral lo cual se complica debido a la disponibilidad del personal.</p>
<p>2. ¿Quién lo realizaba?</p>	<p>Personal de redes con acceso a los equipos de red únicamente</p>

<p>1. ¿Cómo se realiza el proceso con el sistema?</p>	<p><u>Opción 1:</u></p> <p>Se introduce la configuración específica y el nombre del switch que se verá afectado por dicha configuración y la hora después de la cual se deberá de ejecutar el evento y el comando de verificación.</p> <p>Las ventajas que presenta es que no se necesita entrar en horas no laborales y de forma remota a los equipos sino que se pueden dejar programados eventos que el sistema realizará de forma automática utilizando dentro del sistema el modulo de herramientas y de ahí la opción de Eventos. Una vez que el evento sea configurado se nos notificará a través de un correo con la salida de un comando de verificación.</p>
<p>2. ¿Quién lo realiza?</p>	<p>Usuarios dados de alta en el sistema</p> <p>Perfiles que lo pueden utilizar:</p> <ul style="list-style-type: none"> • Administrador • Super user

Tabla 4.3 Escenario de Prueba 2: Aislar Sala

<p align="center">Escenario de Prueba 3: Heterogeneidad en las configuraciones</p>	
<p>Descripción del problema: Debido a las diferentes necesidades de red algunos dispositivos que deberían tener la misma configuración de red no la tienen.</p>	
<p>Situación de uso: Cuando se necesita realizar alguna configuración de algún dispositivo específico anexado a la red. Por ejemplo:</p> <ul style="list-style-type: none"> • Agregar un dispositivo nuevo a la red (teléfono, antena, impresora, etc.) • Quitar un dispositivo nuevo de la red (teléfono, antena, impresora, etc.) • Cambiar un dispositivo nuevo de la red (teléfono, antena, impresora, etc.) 	
<p>1. ¿Cómo se realizaba el proceso?</p>	<p><u>Opción 1:</u></p> <p>Se accede al equipo para configurarlo de acuerdo al dispositivo que se quiere agregar a la red, ya sea teléfono, antena, impresora, etc. Se configura el puerto donde se conectará dicho dispositivo se prueba que el equipo funcione de manera adecuada.</p> <p>Es la única opción para realizar un cambio en la configuración de los equipos pero esta es realizada por diferentes personas por lo cual se puede</p>

	esto puede generar una diversidad en las configuraciones lo cual nos trae problemas como que algún comando este faltando y después se levanten reportes ya que no hay buen servicio.
2. ¿Quién lo realizaba?	Personal de redes con acceso a los equipos de red únicamente
1. ¿Cómo se realiza el proceso con el sistema?	<p><u>Opción 1:</u></p> <p>Se introduce algún dato para encontrar el dispositivo que se verá afectado, el sistema tomará los datos de la base de datos del equipo que se va a configurar y con las plantillas establecidas se generará la configuración necesaria y se configurará el equipo con esos datos.</p> <p>Las ventajas que presenta es que no se necesita conocer de memoria las configuraciones específicas, sino establecer una plantilla la primera vez, la cual se utilizará como un estándar y que el sistema las configura de forma automática con esa plantilla y los datos necesarios de la base de datos. También nos ayuda a garantizar la homogeneidad de las configuraciones evitando de igual forma errores por parte de los administradores.</p>
2. ¿Quién lo realiza?	<p>Usuarios dados de alta en el sistema</p> <p>Perfiles que lo pueden utilizar:</p> <ul style="list-style-type: none"> • Administrador • Super user

Tabla 4.4 Escenario de Prueba 3: Heterogeneidad en las configuraciones

Escenario de Prueba 4: Configuraciones Masivas	
Descripción del problema: Debido a las diferentes necesidades de la red, cuando se requiere hacer un cambio a nivel de toda la red este trabajo se vuelve muy pesado y difícil ya que hay que reconfigurar algún valor en todos los equipos de red (switches).	
Situación de uso: Cuando se necesita realizar un cambio a toda la red. Por ejemplo:	
<ul style="list-style-type: none"> • Actualización de IOS • Respaldo de todas las configuraciones de red • Cambio de contraseña 	
Cuenta nueva de administración	

<p>1. ¿Cómo se realizaba el proceso?</p>	<p><u>Opción 1:</u> Se realiza el cambio de forma manual en todos y cada uno de los equipos de red (switches). Hay que autenticarse en cada equipo, realizar el cambio y validarlo.</p> <p>Esta única opción es muy tardada y cansada ya que se debe hacer lo mismo muchas veces.</p>
<p>2. ¿Quién lo realizaba?</p>	<p>Personal de telecomunicaciones del área de redes únicamente</p>
<p>1. ¿Cómo se realiza el proceso con el sistema?</p>	<p><u>Opción 1:</u> Se establece que equipos serán configurados, por edificio o edificio y piso o edificio piso y cuarto de telecomunicaciones o el prefijo todos para toda la red y se establecen los comandos a ejecutar. El sistema se encarga de entrar en cada equipo y ejecutar los comandos que se establecieron al terminar queda guardado en la base de datos todo lo que se hizo en cada equipo para validación.</p> <p>Las ventajas que presenta es que no se necesita que el usuario realice todas estas tareas repetitivas y nos presenta un gran ahorro de tiempo para poder enfocarnos en tarea más importantes.</p>
<p>2. ¿Quién lo realiza?</p>	<p>Usuarios dados de alta en el sistema</p> <p>Perfiles que lo pueden utilizar:</p> <ul style="list-style-type: none"> • Administrador • Super user

Tabla 4.5 Escenario de Prueba 4: Configuraciones Masivas

Escenario de Prueba 5: Falta de inventario tecnológico

Descripción del problema: No se tiene un inventario actualizado de los equipos de red, y actualmente se utiliza Excel como base de datos de los activos tecnológicos, por lo cual solo la persona que posee ese archivo conoce la información y esta no está centralizada ya que hay diferentes tecnologías con diferentes administradores de las mismas y son ellos los únicos que tienen la información de dicha tecnología. De igual forma obtener reportes es muy difícil con la información en este formato.

<p>Situación de uso: Cuando existe algún reporte o se necesita dar de alta algún nuevo dispositivo. Por ejemplo:</p> <ul style="list-style-type: none"> • Dar de alta/Cambiar/Dar de baja una nueva impresora • Dar de alta/Cambiar/Dar de baja una nueva antena • Dar de alta/Cambiar/Dar de baja un teléfono IP 	
<p>1. ¿Cómo se realizaba el proceso?</p>	<p><u>Opción 1:</u></p> <p>Se da de alta el equipo en Excel en los diferentes archivos dependiendo de la tecnología a la que pertenezca (Telefonía IP, redes inalámbricas y red alamburada) y solo el administrador de la tecnología es quien posee y modifica el archivo.</p> <p>Esta única opción es problemática ya que solo se tiene el archivo de Excel y no es compartido y estos se encuentran en computadoras no en un servidor que se respalde, este centralizado y esté disponible para todos los administradores.</p>
<p>2. ¿Quién lo realizaba?</p>	<p>Personal de telecomunicaciones de diferentes áreas:</p> <ul style="list-style-type: none"> • Telefonía • Redes
<p>1. ¿Cómo se realiza el proceso con el sistema?</p>	<p><u>Opción 1:</u></p> <p>Se especifican los datos y se pueden realizar altas, bajas, cambios y consultas de la información la cual es guardada en la base de datos.</p> <p>Las ventajas que presenta es que no se tiene el un archivo sino en un servidor esta información y nos permite que esté disponible para quienes la necesitan, de igual forma se mantiene centralizada y se puede respaldar así como restaurar si algo se daño.</p>
<p>2. ¿Quién lo realiza?</p>	<p>Usuarios dados de alta en el sistema</p> <p>Perfiles que lo pueden utilizar:</p> <ul style="list-style-type: none"> • Super user

Tabla 4.6 Escenario de Prueba 5: Falta de Inventario Tecnológico

Escenario de Prueba 6: Monitoreo de equipos	
Descripción del problema: Se cuenta con un sistema de monitoreo gratuito que se encarga de ver que los equipos estén encendidos dando servicio a la red y en cuanto el equipo se apaga o prende nuevamente el sistema lo reporta, sin embargo cuando se va la luz el sistema manda un correo por cada equipo prendido/apagado lo cual satura los correos y nos presenta la información de manera inadecuada.	
Situación de uso: Cuando se necesita revisar algún cambio o identificar los edificios que presentan problemas. Por ejemplo: <ul style="list-style-type: none"> • Si se va la luz encontrar los edificios con problemas • Si algún equipo se daña o es apagado que el sistema lo notifique 	
1. ¿Cómo se realizaba el proceso?	<p><u>Opción 1:</u></p> <p>El sistema anterior monitorea los equipos pero presenta la información de manera inadecuada ya que con la cantidad masiva de correos que este manda la información se presenta de manera abrumadora y difícil de entender.</p> <p>La única opción presenta la información de manera inadecuada</p>
2. ¿Quién lo realizaba?	Personal de telecomunicaciones del área de redes únicamente
1. ¿Cómo se realiza el proceso con el sistema?	<p><u>Opción 1:</u></p> <p>El nuevo sistema nos envía un correo por todos los cambios detectados presentando la información de manera adecuada así como más fácil de entender y presentable.</p> <p>Las ventajas que presenta es que la información de este sistema no es abrumadora y nos permite tener una mejor respuesta ante este incidente.</p>
2. ¿Quién lo realiza?	<p>Usuarios dados de alta en el sistema</p> <p>Perfiles que lo pueden utilizar:</p> <ul style="list-style-type: none"> • Administrador • Super user

Tabla 4.7 Escenario de Prueba 6: Monitoreo de Equipos

4.7 Encuestas de satisfacción

Después de un periodo de prueba del sistema de 6 meses se encuesta a los usuarios para evaluar la satisfacción de los mismos ante el uso del nuevo sistema.

La encuesta consistió en 7 preguntas (ver Anexo B) aplicada a los 5 usuarios del sistema, a continuación se muestran y analizan los resultados:

En la figura 4.3 se muestra la grafica de la pregunta “El sistema te ayuda a realizar tus labores de forma eficiente” de la encuesta de satisfacción, en la cual 100% de los usuarios es decir, todos los usuarios contestaron que estaban totalmente de acuerdo. Esto quiere decir que el sistema es útil para todos los administradores de red que lo usan.

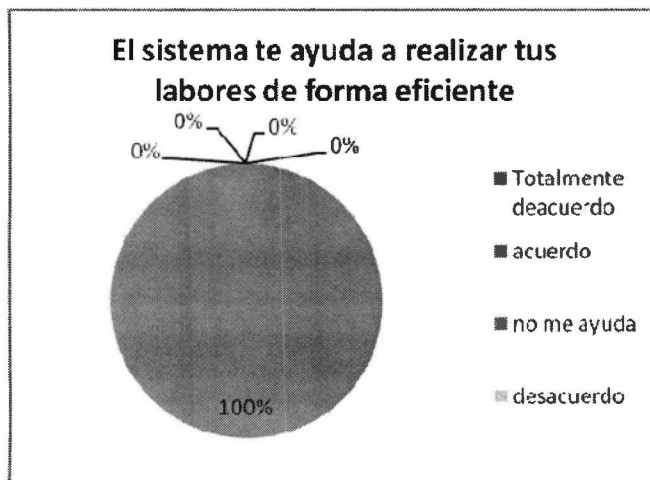


Figura 4.10 Encuesta de satisfacción - Pregunta1

En la figura 4.4 se muestra la grafica de la pregunta “El sistema te ahorra tiempo en tus labores” de la encuesta de satisfacción, en la cual 100% de los usuarios es decir, todos los usuarios contestaron que estaban totalmente de acuerdo. Esto quiere decir que el sistema minimiza el tiempo de respuesta para los usuarios finales.

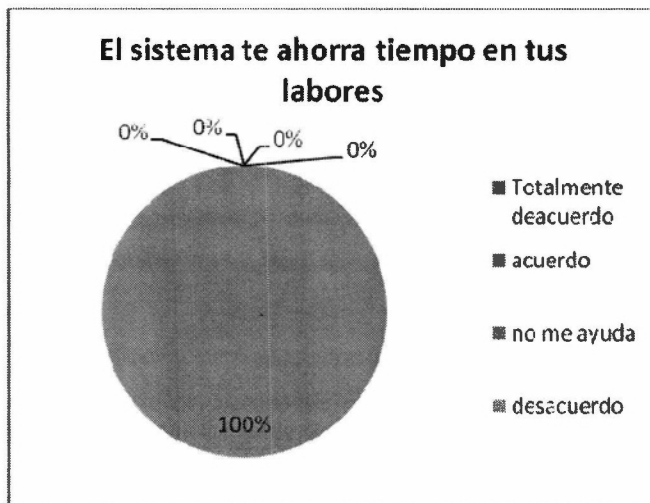


Figura 4.11 Encuesta de satisfacción - Pregunta 2

En la figura 4.5 se muestra la grafica de la pregunta “El sistema es amigable y entendible” de la encuesta de satisfacción, en la cual 100% de los usuarios es decir, todos los usuarios contestaron que estaban totalmente de acuerdo. Esto quiere decir que el sistema es fácil de usar por los administradores de red y cumple el criterio de facilidad de uso.

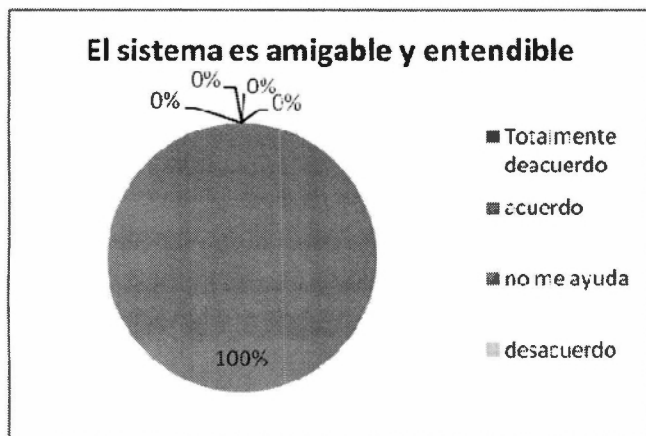


Figura 4.12 Encuesta de satisfacción - Pregunta 3

En la figura 4.6 se muestra la grafica de la pregunta “El sistema presenta información adecuada y valiosa” de la encuesta de satisfacción, en la cual 100% de los usuarios es decir, todos los usuarios contestaron que estaban totalmente de acuerdo. Esto quiere decir que el sistema ayuda a la toma de decisiones de los administradores de red y directivos con respecto a los activos fijos de la empresa y los servicios que ofrecen.

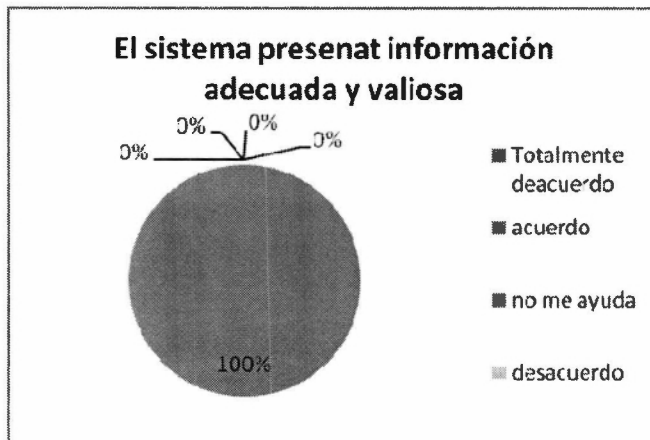


Figura 4.13 Encuesta de satisfacción - Pregunta 4

En la figura 4.7 se muestra la grafica de la pregunta “El sistema contiene la funcionalidades básicas de un sistema de administración de las telecomunicaciones” de la encuesta de satisfacción, en la cual 100% de los usuarios es decir, todos los usuarios contestaron que estaban totalmente de acuerdo. Esto quiere decir que el sistema contiene todas las funcionalidades que los administradores de red consideran más básicas dentro de un sistema de administración de equipos de red.

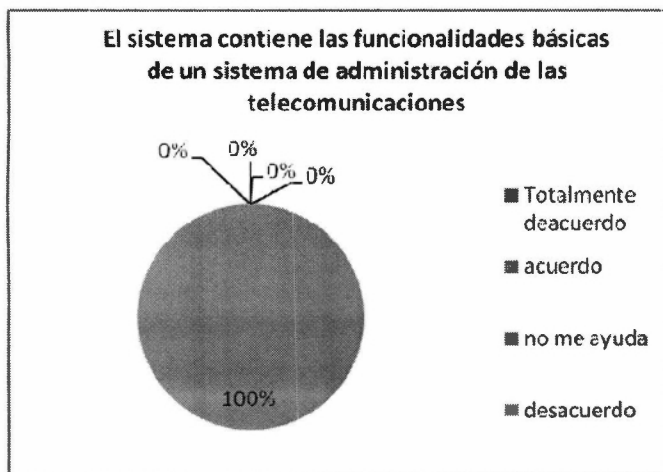


Figura 4.14 Encuesta de satisfacción - Pregunta 5

Capítulo 5 Conclusiones y Trabajo Futuro

En este trabajo se definieron las actividades básicas de un sistema de información para la administración de equipos de red, basadas en la importancia que le dan los administradores de red a dichas actividades obteniendo un modelo de factores críticos.

Una vez determinadas las funcionalidades del sistema se propuso una arquitectura general para los sistemas de información para la administración de equipos de red y basada en esta arquitectura se realizó la implementación de un sistema de información específico para la red del Tecnológico de Monterrey Campus Ciudad de México, donde se probó y evaluó dicha implementación en un caso de estudio.

Debido a las crecientes necesidades de los nuevos servicios que se ofrecen día a día, la rapidez de los avances tecnológicos es cada vez mayor. Las redes no están exentas a esto, al contrario con la convergencia de servicios la capa de red se ve constantemente afectada, por lo cual un sistema como este tiene que seguirse actualizando y requiere de un trabajo futuro continuo para poder estar al nivel de los servicios que los usuarios requieren, obteniendo un mejor desempeño.

5.1 Aportaciones de esta investigación

Modelo de Factores Críticos

En este trabajo se detectaron las necesidades de distintos administradores de red a través de un modelo de factores críticos propuesto por Stallings en 1993, sin embargo al no encontrar información más reciente se encuestó a administradores de red para evaluar estos criterios y así establecer una nueva escala de importancia de los mismos.

Los tres factores críticos más importantes: seguridad, monitoreo de la disponibilidad (criterio que cumple el objetivo específico 6: Monitorear los dispositivos de red y lanzar alarmas ante determinados) y facilidad de uso marcaron los parámetros más importantes a considerar en la implementación de este sistema, ya que muchos sistemas de información para administración

de equipos de red son muy complejos en su uso diario, instalación o requieren demasiados recursos incluyendo equipos dedicados que elevan mucho su costo y mantenimiento.

Arquitectura de un sistema de información para administrar equipos de red

La importancia que le dieron los usuarios finales a los factores críticos, mencionados anteriormente, sirvió para proponer una arquitectura de un sistema de información básico, así como base de los módulos funcionales que se plantearon tanto para el diseño de la arquitectura como para la implementación de este sistema.

En base al modelo de factores críticos obtenido se pudo proponer una arquitectura para sistemas de información para la administración de equipos de red. Tomando en cuenta estos factores se detectaron cuatro módulos funcionales: monitoreo, herramientas, configuración y administración del sistema.

Se identificaron diferentes roles capaces de hacer uso del sistema, por lo cual se proponen 3 perfiles de usuarios (monitor, administrador y super user), estos perfiles no sólo ayudan a delegar tareas, sino a mejorar la seguridad de la aplicación con diferentes niveles de autorización.

Implementación de un sistema básico de información para administrar equipos de red

Para garantizar el criterio de seguridad en la implementación del sistema se prefirió el protocolo de SSH sobre el protocolo de telnet para la conexión a equipos de forma remota, tanto para la obtención de datos, como para la configuración de los equipos y se utilizó el protocolo de SNMP únicamente para lectura de datos como se indica dentro de las mejores prácticas de SNMP, ya que este es menos seguro, debido a que los datos viajan en texto claro, es decir, sin ningún método de encriptación.

Se encontró que la forma de garantizar la facilidad de uso, fue utilizar vistas sencillas con un solo menú del lado izquierdo, donde se puede acceder a cualquier componente de la aplicación. El sistema está separado por módulos funcionales para hacer la navegación más rápida e intuitiva, así como presentar solo la información necesaria.

Se escogió el lenguaje de programación Java, ya que es un lenguaje portable que nos permite mantenernos independientes del hardware en la fase de implementación, también este lenguaje nos ofrece una amplia gama de librerías de terceros existentes para poder ser utilizadas en el proyecto y brindar servicios base como la interconexión con bases de datos, servidores de correo o equipos de red.

En este sistema se utilizaron principios básicos de programación orientada a objetos como: polimorfismo, interfaces, encapsulación entre otros.

Al trabajar en un ambiente con muchos equipos de red el tiempo de respuesta de la aplicación puede verse afectado de manera importante; ya que cada equipo tiene a su vez un tiempo de respuesta, así que para aprovechar el procesamiento del lado del servidor y tratar de minimizar tiempos muertos o tiempos de espera se utilizaron multihilos para poder ofrecer una mayor velocidad.

Se creó una base de datos para guardar toda la información referente a los dispositivos de red cumpliendo así con el objetivo específico 2 (Crear una base de datos de los activos tecnológicos de una empresa). De igual forma cumpliendo el objetivo específico 1 se estandarizó la nomenclatura y las configuraciones de los activos tecnológicos, utilizando un nombre compuesto de un identificador y/o la ubicación física de cada uno de los activos. También se crearon plantillas de configuraciones básicas para cada tipo de dispositivo de red.

La mejor forma de obtener un control sobre el funcionamiento de algunas clases específicas como: eventos y monitoreo de la disponibilidad se logro al utilizar el patrón de diseño singleton para garantizar una sola instancia de estos componentes, aunque fueran utilizados por varios usuarios al mismo tiempo.

Java también nos ofrece un marco de trabajo probado para el modelo MVC conocido como struts, que nos permite separar los componentes para tener un mejor control ofreciendo un código flexible y de fácil mantenimiento.

Caso de estudio con escenarios de prueba de la implementación del sistema de información para administrar equipos de red

El uso de multihilos realmente mejora el desempeño como se puede constatar en el sistema por el usuario final, ya que en las encuestas de opinión se obtuvo una calificación sobresaliente acerca de la velocidad y el ahorro de tiempo que el sistema ofrece a los administradores de red. Antes se tenía un script en bash que tenía la funcionalidad de una de las herramientas del nuevo sistema de administración de equipos de red (busca mac) el cual revisaba todos los equipos con un tiempo de respuesta alto entre 3 y 4 minutos por mac, mientras que el nuevo sistema logro reducir ese tiempo de respuesta a menos de un minuto.

El sistema ayuda a los administradores de red en sus labores diarias, esta herramienta resulta muy valiosa para minimizar tiempo y esfuerzos al realizar tareas de administración de redes, con esto también se ve alcanzado el objetivo específico 3 (Reducir el tiempo de configuración de equipos de red).

Al utilizar un sistema de información para la administración de equipos de red, no sólo se posee un inventario actualizado de los activos tecnológicos de una empresa (objetivo específico 5), sino que también se garantiza un mayor control en las configuraciones de los mismos y se minimizan los errores al realizar configuraciones de forma manual, al establecer configuraciones homogéneas para dispositivos específicos dentro de la red (objetivo específico 4).

Se ofrece una mayor flexibilidad al poder programar eventos de forma automática en un horario específico, ya que algunas de las tareas realizadas por administradores de red deben de ser en un horario que no afecte el servicio a los usuarios, todo esto de forma segura y fácil de usar, para ayudar a brindar un mejor servicio así como un menor tiempo de respuesta para los usuarios finales (objetivo específico 7 Automatización de procesos).

Se puede brindar acceso al sistema a usuarios con conocimientos básicos de red para realizar tareas de operación diaria, incluso si estos no poseen conocimientos especializados en el área de redes, ya que el sistema hará de forma automática configuraciones o tareas preestablecidas.

A pesar de que pueden usarse varias arquitecturas para resolver esta necesidad se observó que la arquitectura implementada proporcionó un mantenimiento más cómodo. El Campus Ciudad de México está iniciando una migración de equipos de red y las modificaciones del sistema para acoplarse a los equipos de la nueva infraestructura, son mínimas y controladas gracias a la encapsulación, polimorfismo y marco de trabajo utilizados en la implementación.

5.2 Trabajo Futuro

Los objetivos logrados en este trabajo nos permiten visualizar nuevas oportunidades de mejora dentro del sistema como la implementación de las funcionalidades faltantes (monitoreo de tiempo de respuesta, re enrutamiento de tráfico y reportes mejorados) que se dejaron fuera debido al tiempo y alcance dedicados a este trabajo de tesis.

Por otro lado se pueden implementar nuevas funcionalidades que se observen en el Campus Ciudad de México para realizar actividades más complejas que ayuden a tener un diagnóstico de los problemas a los que los administradores de red se enfrentan o puedan ayudar a realizar un mantenimiento preventivo a través de alertas en los equipos de red antes de que surjan los posibles problemas.

Referencias

- Breitgand, D., Raz, D., & Shavitt, Y. (2002). SNMP GetPrev: An Efficient Way to Browse Large MIB Tables. *IEEE Journal On Selected Areas In Communications* , 656 - 667.
- Cisco System. (2006). SNMP: Simple Network Management Protocol. Recuperado el 2010, de <http://www.cisco.com/warp/public/535/3.html>
- Data Monitor. (2008). Computer Hardware in Mexico. Data Monitor.
- Data Monitor. (2009). Software in Mexico. Data Monitor.
- Davidson, J., & Hathaway, W. (1977). The Arpanet Telnet Protocol: Its purpose, principles, implementation, and impact on host operating system design SIGCOMM '77. *Proceedings of the fifth symposium on Data communications* .
- Douglas, M., & Schmidt, K. (2005). *Essential SNMP*. Sebastopol CA: O'Reilly.
- Drake, P. (1991). Using SNMP to manage networks, *Designing Resilient Architectures*. IEE Colloquium , 1-4.
- Himanshu, D. (2004). *Implementing SSH: Strategies for Optimizing the Secure Shell*. Indianapolis, Ind.: John Wiley & Sons.
- Holmes, B. (1998). *Programming With Java*. Sudbury, Mass.: Jones & Bartlett Publishers.
- Kassem, N. (2000). *Designing Enterprise applications with the Java 2 Platform*. Boston: Addison-Wesley.
- Laudon, k. (2007). *Management Information Systems: Managing the Digital Firm*. N.J: Prentice Hall.

Miller, M. (1993). *Managing internetworks with SNMP: the definitive guide to the Simple Network Management Protocol (SNMP) and SNMP version*. New York: M & T Books.

Mo, L., & Sandrasegaran, k. (2005). *Network management challenges for next generation networks*. *Local Computer Networks* , 6.

Pineda, S. (2010). *Entorno macroeconómico de México e industria TIC Anual 2009*. Recuperado el 08 de Febrero de 2011, de AMITI: http://www.cysp.com.mx/Ima/Amiti/Documentos%20Descargables/2010_Entorno_macro_económico_Mexico-industria_TIC.pdf

Pressman, R. (2010). *Ingeniería del Software: un enfoque práctico*. México: McGraw-Hill.

Raman, L. (1998). *OSI Systems and Network Management*. *IEEE Communications Magazine* , 46 - 53.

Sabharwal, C. (1998). *Java, Java, Java. Potentials* , 33-37.

Stair, R., & Reynolds, G. (2000). *Principios de Sistemas de Información*. International Thompson.

Stallings, W. (1993). *SNMP, SNMPv2, and CMIP: The Pratical Guide to Network-Management Standards*. Reading, Mass: Addison-Wesley Pub. Co.

Acrónimos

AES	Advanced Encryption Standard
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
DES	Data Encryption Standards
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology (TIC Tecnologías de Información y Comunicaciones)
JDBC	Java Data Base Connectivity
JSP	Java Server Pages
MAC	Message Authentication Code
MD5	Message-Digest Algorithm 5
MIB	Management Information Bus
MVC	Model - view - controller
NMS	Network Management System
NVT	Network Virtual Terminal
OSI	Open System Interconnections
PDU	Protocol Data Unit
RLOGIN	Remote Login
RSH	Remote Shell
SHA1	Secure Hash Algorithm 1
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SSH	Secure shell
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TMN	Telecommunications Management Network
URL	Uniform Resource Locator
XML	eXtensible Markup Language

Anexo A

Encuesta

A continuación se presenta un cuestionario compuesto, el cual tiene como finalidad identificar su percepción en cuanto al uso de sistemas de administración de equipos de red. Estos resultados son totalmente confidenciales y servirán para la realización de una tesis de maestría.

¿Ha trabajado con sistemas de administración de redes?

Si No

Porque:

¿Qué opina de esos sistemas?

¿Qué requerimientos considera usted más importante? (Ordene del 1 al 10, siendo 1 el más importante)

- | | | | |
|-------------------------|--------------------------|----------------------------------|--------------------------|
| Facilidad de uso | <input type="checkbox"/> | Capacidad de restauración | <input type="checkbox"/> |
| Seguridad | <input type="checkbox"/> | Habilidad de agregar o borrar | <input type="checkbox"/> |
| Automatización mejorada | <input type="checkbox"/> | Monitoreo de disponibilidad | <input type="checkbox"/> |
| Alta de usuarios | <input type="checkbox"/> | Re enrutamiento de tráfico | <input type="checkbox"/> |
| Reportes mejorados | <input type="checkbox"/> | Monitoreo de tiempo de respuesta | <input type="checkbox"/> |
| Otro: _____ | <input type="checkbox"/> | | |

¿Qué equipos controla con este tipo de sistemas?

Mencione que funcionalidades cree usted básicas para un sistema de administración de redes

¿En que se basa para escoger un sistema de administración de equipos de red?

¿Compraría o no compraría para su empresa un sistema de administración de equipos de red?

Si No

Porque:

Anexo B

Encuesta de opinión

1) Totalmente de acuerdo

2) De acuerdo

3) No me ayuda

4) Desacuerdo

5) Totalmente desacuerdo

El sistema te ayuda a realizar tus labores de forma eficiente

1	2	3	4	5
---	---	---	---	---

El sistema te ahorra tiempo en tus labores

1	2	3	4	5
---	---	---	---	---

El sistema es amigable y entendible

1	2	3	4	5
---	---	---	---	---

El sistema de presenta información adecuada y valiosa

1	2	3	4	5
---	---	---	---	---

El sistema contiene las funcionalidades básicas de un sistema de administración de las telecomunicaciones

1	2	3	4	5
---	---	---	---	---

Que funcionalidad es la que mas ocupas del sistema y porque:

Que funcionalidades crees que hacen falta si es que hay alguna:

Anexo C

Descripción de casos de uso utilizados para la implementación dividida por módulos funcionales: Monitoreo, Herramientas, Configuración y Administración del sistema.

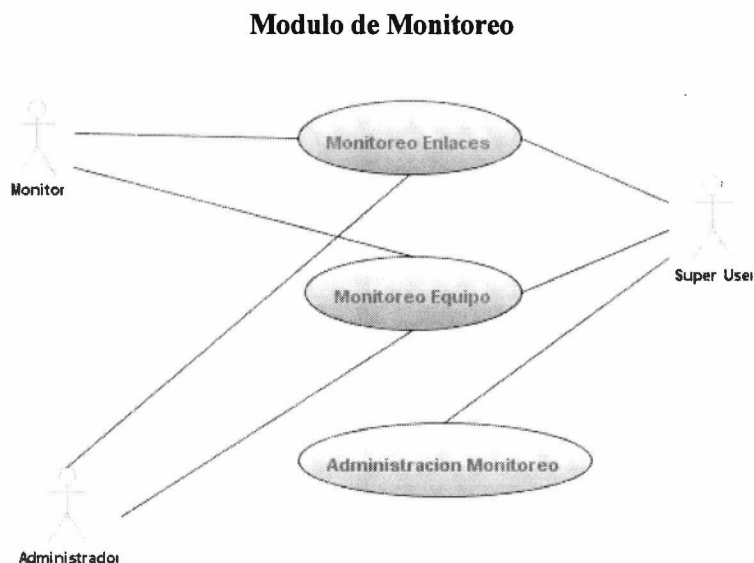


Figura C.1 Caso de Uso del Módulo de Monitoreo

Dentro del modulo de Monitoreo se encuentran tres casos de uso: Monitoreo enlaces, Monitoreo Equipo y Administración Monitoreo, los cuales se explican a continuación

Nombre:	Monitoreo Enlaces
Autor:	Erika Hernández
Fecha:	18/06/2010
Descripción:	Permite ver la carga de trafico que posee cada enlace monitoreado
Actores:	Usuario de Internet autenticado. (Monitor, Administrador, o super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema.

<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El actor escoge en el menú la opción de monitor y posteriormente enlace. 2. El actor escoge el enlace que desee ver 3. El sistema despliega la carga del enlace seleccionado en una nueva pantalla
<p>Flujo Alternativo:</p>
<p>Poscondiciones:</p> <p>El sistema despliega la información solicitada por el usuario acerca de la carga de los enlaces de red.</p>

Tabla C.1 Caso de Uso: Modulo Monitoreo-Monitoreo Enlaces

Nombre:	Monitoreo Equipo
Autor:	Erika Hernández
Fecha:	18/06/2010
<p>Descripción:</p> <p>Permite ver el status de los equipos en la red (encendido o apagado).</p>	
<p>Actores:</p> <p>Usuario de Internet autenticado. (Monitor, Administrador, o super user)</p>	
<p>Precondiciones:</p> <p>El usuario debe haberse autenticado en el sistema.</p>	
<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El actor escoge en el menú la opción de monitor y posteriormente equipo. 2. El actor escoge la opción que desee: ver todos los equipos, solo los encendidos o solo los apagados 3. El sistema despliega el status de los equipos en la red 	
<p>Flujo Alternativo:</p>	
<p>Poscondiciones:</p> <p>El sistema despliega la información solicitada por el usuario acerca del status de los equipos de red.</p>	

Tabla C.2 Caso de Uso: Modulo Monitoreo-Monitoreo Equipo

Nombre:	Administración Monitoreo
Autor:	Erika Hernández
Fecha:	18/06/2010
Descripción:	Permite encender/apagar el modulo que se encarga de monitorear los equipos de red
Actores:	Usuario de Internet autenticado. (solo super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema y ser super user
Flujo Normal:	<ol style="list-style-type: none"> 1. El actor escoge en el menú la opción de Administración en el modulo de Monitoreo. 2. El actor solo tiene la opción de prender el monitoreo si este está apagado o apagarlo si se encuentra prendido. 3. El actor prende/apaga el monitoreo 4. El sistema comienza o detiene este servicio según lo haya solicitado el actor
Flujo Alternativo:	
Poscondiciones:	<p>El sistema prendió/apago el servicio.</p> <ul style="list-style-type: none"> • Si el servicio se apago: el monitoreo se detiene una vez que haya terminado su ciclo normal. • Si el servicio se prendió: el sistema se encarga de consultar el estatus de cada equipo dado de alta en el monitoreo y estará revisando los equipos cada 15 minutos (o como se haya establecido la ventana de tiempo) para corroborar el estatus de los mismos.

Tabla C.3 Caso de Uso: Modulo Monitoreo-Administración del Monitoreo

Modulo de Herramientas

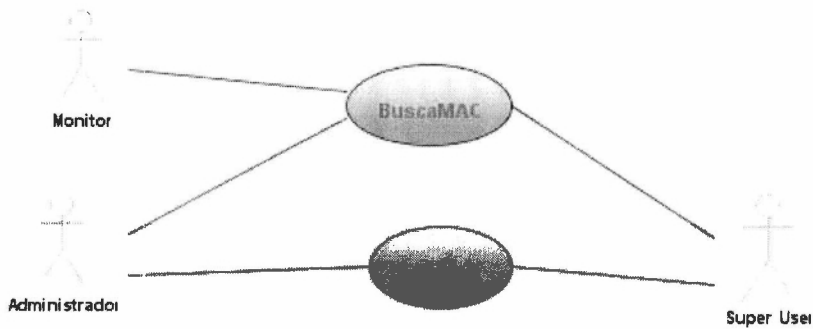


Figura C.2 Caso de Uso del Modulo de Herramientas

Dentro del modulo de Herramientas se encuentran dos casos de uso: Busca Mac y Eventos

Nombre:	Busca Mac
Autor:	Erika Hernández
Fecha:	18/06/2010
Descripción:	Permite encontrar un equipo que se encuentre conectado a algún dispositivo de la red a través de su dirección mac.
Actores:	Usuario de Internet autenticado. (Monitor, Administrador, o super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema El equipo que se quiera encontrar debe de estar conectado a la red
Flujo Normal:	<ol style="list-style-type: none"> 1. El actor escoge en el menú la opción de Busca Mac en el menú de Herramientas. 2. El actor debe introducir la dirección mac del equipo que desee encontrar en la red 3. El actor escoge el método de búsqueda: por árbol o por edificio <ul style="list-style-type: none"> o Si se busca por árbol el sistema hace el recorrido de menor longitud para encontrar el equipo con la dirección mac. El actor necesita introducir el

<p>nombre o la dirección ip de la raíz de STP (<i>spanning tree protocol</i>) de la red.</p> <ul style="list-style-type: none"> o Si se busca por edificio el sistema hace el recorrido más largo para encontrar el equipo con la dirección mac. El actor necesita introducir el identificador del edificio o la palabra clave todos (Si el actor introduce el identificador del edificio se buscara solo en ese edificio o si se introduce la palabra clave todos el sistema buscará en todos los equipos dados de alta) <p>4. El sistema comienza la búsqueda del equipo al tratar de ubicar la dirección mac</p>
<p>Flujo Alternativo: Si no está conectada el equipo el sistema nos desplegará que no se encontró la dirección mac.</p>
<p>Poscondiciones:</p> <p>El sistema encuentra la ubicación del equipo y nos despliega el equipo en el que se encontró la dirección maca si como el puerto en el que está conectado y la vlan a la que pertenece.</p>

Tabla C.4 Caso de Uso: Modulo Herramientas-Busca Mac

Nombre:	Eventos
Autor:	Erika Hernández
Fecha:	18/06/2010
Descripción:	Permite programar un evento en un equipo de red. Se le llama un evento a configurar un equipo de manera automática en un horario específico.
Actores:	Usuario de Internet autenticado. (Administrador, o super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema (solo usuarios administrador o super user) El equipo que se quiera configurar debe de estar conectado a la red
Flujo Normal:	

1. El actor escoge en el menú la opción Eventos del menú Herramientas.
2. El actor debe introducir el nombre o la dirección ip del equipo que se configurará de manera automática
3. El actor debe introducir la configuración que desee ingresar al equipo
4. El actor introduce una descripción del evento para poder distinguirlo de otros eventos programados.
5. El actor introduce un comando de verificación para poder corroborar la configuración que se ingreso al equipo
6. El actor introduce la fecha y hora después de la cual quiere que se configure el equipo
7. El sistema espera hasta que se cumpla la fecha y hora y configura el equipo con los comandos especificados

Flujo Alternativo: Si el equipo no está conectado el sistema no podrá configurar dicho equipo.

Si se desea cancelar el evento se podrá deshabilitar desde la página de eventos con el botón cancelar.

Poscondiciones:

El sistema configura el equipo a la fecha y hora indicada y al término del evento nos manda un correo con el comando de verificación al actor que programo dicho evento.

Tabla C.5 Caso de Uso: Modulo Herramientas-Eventos

Modulo de Configuración

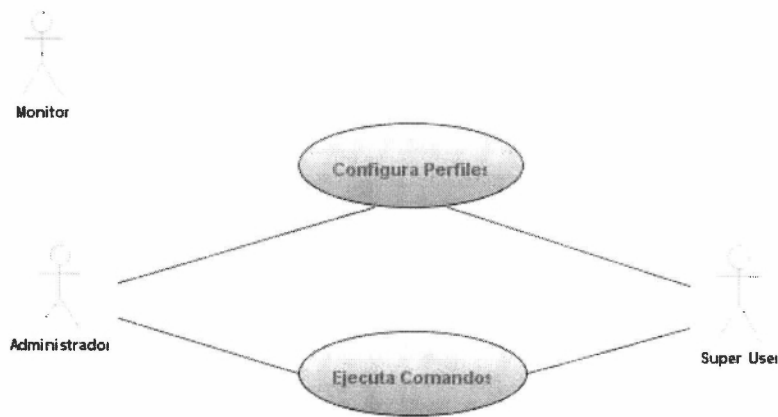


Figura C.3 Caso de Uso del Modulo de Configuración

Dentro del modulo de Configuración se encuentran dos casos de uso: Configura Perfiles y Ejecuta Comandos.

Nombre:	Configura Perfiles
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite configurar de manera automática un perfil determinado de algún dispositivo en la red. Ejemplo: Si se tienen teléfonos ip se puede configurar un perfil de teléfono ip con una configuración específica para teléfono ip que garantice la homogenización de las configuraciones.
Actores:	Usuario de Internet autenticado. (Administrador, o super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema (solo usuarios administrador o super user) El equipo que se quiera configurar debe de estar conectado a la red

Flujo Normal:

1. El actor escoge en el menú la opción Configura Perfiles del menú Configuración.
2. El actor debe introducir el tipo de equipo que va a configurar con un perfil
3. El actor debe introducir algún dato conocido de ese equipo para encontrar el equipo que se va a configurar y obtener todos los datos necesarios para la configuración
4. El actor debe escoger el dispositivo que va a configurar con un perfil de la lista de resultados
5. El sistema configura el equipo de red donde se conectara este dispositivo con la configuración del perfil

Flujo Alternativo: Si el equipo no está conectado el sistema no podrá configurar dicho equipo.

Poscondiciones:

El sistema configura el equipo con el perfil necesario para que el dispositivo que se conectara a la red funcione de manera adecuada y se mantenga estandarizada la configuración de estos dispositivos.

Tabla C.6 Caso de Uso: Modulo Configuración- Configura Perfiles

Nombre:	Ejecuta Comandos
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite ejecutar una serie de comandos a varios equipos. Ejemplo obtener todas las configuraciones de los equipos de red. Se puede utilizar para configurar varios equipos, pero su uso es esta enfocado a obtener consultas de los equipos.
Actores:	Usuario de Internet autenticado. (Administrador, o super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema (solo usuarios administrador o super user)

El equipo o los equipos que se quiera configurar deben de estar conectado a la red

Flujo Normal:

1. El actor escoge en el menú la opción Ejecuta Comandos del menú Configuración.
2. El actor debe introducir los equipos a configurar (ya sea la palabra clave todos, o por edificio o el nombre de un equipo en particular)
3. El actor debe introducir los comandos que se ejecutaran en cada equipo separados por comas
4. El actor debe de introducir una descripción que le ayude a identificad la configuración que será almacenada en la Base de datos
5. El sistema ejecutara los comandos en cada uno de los equipos
6. El sistema desplegará en la parte inferior las configuraciones que se llevaron a cabo en el o los equipos y las almacenará en la base de datos como histórico para corroborar lo que se hizo en cada equipo
7. Si el usuario quiere ver lo que se configuro así como la salida que entrego el equipo deberá escoger la configuración que quiere ver y presionar el botón despliega

Flujo Alternativo: Si el equipo no está conectado el sistema no podrá configurar dicho equipo.

Poscondiciones:

El sistema configura el equipo con los comandos establecidos y nos desplegará los registros de la base de datos que el usuario acaba de realizar así como los que ese mismo usuario hizo en el pasado.

Tabla C.7 Caso de Uso: Modulo Configuración- Ejecuta Comandos

Modulo de Administración

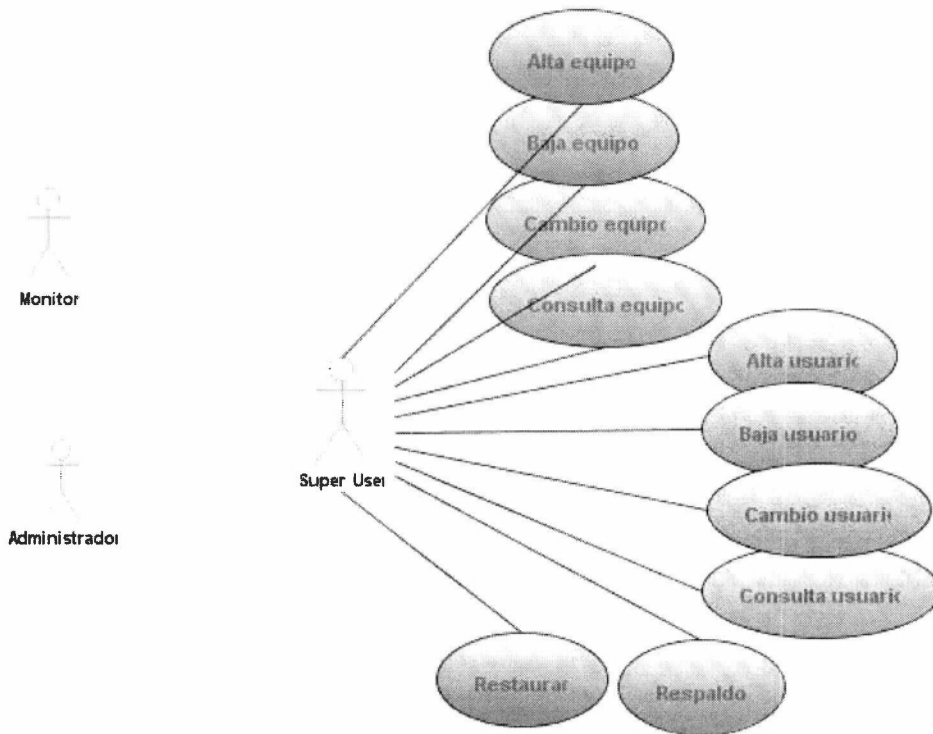


Figura C.4 Caso de Uso del Modulo de Administración

Dentro del modulo de Administración se encuentran diez casos de uso: Alta equipo, Baja equipo, Cambio equipo, Consulta equipo, Alta usuario, Baja usuario, Cambio usuario, Consulta usuario, Respaldo, Restaurar.

Nombre:	Alta Equipo
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite dar de alta un nuevo equipo de red en el sistema.
Actores:	Usuario de Internet autenticado. (Super user)
Precondiciones:	

El usuario debe haberse autenticado en el sistema (solo usuarios super user)
<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente equipos y de ahí escoge la opción de alta. 2. El actor debe escoger el tipo de equipo que dará de alta. 3. El actor debe introducir todos los datos de ese equipo que serán almacenados en la base de datos 4. El sistema guardará los datos proporcionados en la base de datos del sistema
<p>Flujo Alternativo: Si datos únicos como el serial, dirección mac u otros se repiten el sistema marcara error y los datos no serán almacenados.</p>
<p>Poscondiciones:</p> <p>El sistema almacenará los datos del nuevo activo fijo en la base de datos del sistema para después poder ser utilizados por el sistema.</p>

Tabla C.8 Caso de Uso: Modulo Administración-Alta Equipos

Nombre:	Baja Equipo
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite dar de baja un nuevo equipo de red en el sistema.
Actores:	Usuario de Internet autenticado. (Super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema (solo usuarios super user)
Flujo Normal:	<ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Administración del menú Administración y

<p>posteriormente equipos y de ahí escoge la opción de baja.</p> <ol style="list-style-type: none"> 2. El actor debe escoger el tipo de equipo que dará de baja. 3. El actor debe introducir algún dato de ese equipo para buscarlo en el sistema y poderlo dar de baja en la base de datos 4. El sistema borrara el equipo especificado en la base de datos del sistema
<p>Flujo Alternativo:</p>
<p>Poscondiciones:</p> <p>El sistema borrará los datos del activo fijo que se haya escogido de la base de datos del sistema.</p>

Tabla C.9 Caso de Uso: Modulo Administración-Baja Equipos

Nombre:	Cambio Equipo
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	
Permite realizar alguna modificación a algún equipo de red en el sistema.	
Actores:	
Usuario de Internet autenticado. (Super user)	
Precondiciones:	
El usuario debe haberse autenticado en el sistema (solo usuarios super user)	
Flujo Normal:	
<ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente equipos y de ahí escoge la opción de cambios. 2. El actor debe escoger el tipo de equipo que cambiará. 3. El actor debe introducir los datos de ese equipo que serán cambiados en la base de datos 4. El sistema guardará los datos proporcionados en la base de datos del sistema 	

Flujo Alternativo: Si datos únicos como el serial, dirección mac u otros se repiten el sistema marcara error y los datos no serán almacenados.

Poscondiciones:

El sistema almacenará los datos modificados del activo fijo en la base de datos del sistema para después poder ser utilizados por el sistema.

Tabla C.10 Caso de Uso: Modulo Administración-Cambios Equipos

Nombre:	Consulta Equipo
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite consultar algún equipo de red en el sistema.
Actores:	Usuario de Internet autenticado. (Super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema (solo usuarios super user)
Flujo Normal:	<ol style="list-style-type: none">1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente equipos y de ahí escoge la opción de consultas.2. El actor debe escoger el tipo de equipo que quiere consultar.3. El actor debe introducir algún dato que conozca de ese equipo para poderlo localizar en la base de datos.4. El sistema desplegará los todos los datos del equipo solicitado haciendo una consulta a la base de datos del sistema
Flujo Alternativo:	
Poscondiciones:	El sistema desplegará los datos del activo fijo obtenidos de la base de datos del sistema

para después poder ser utilizados por el sistema.

Tabla C.11 Caso de Uso: Modulo Administración-Consulta Equipos

Nombre:	Alta Usuario
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite dar de alta un nuevo usuario en el sistema.
Actores:	Usuario de Internet autenticado. (Super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema (solo usuarios super user)
Flujo Normal:	<ol style="list-style-type: none">1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente usuarios y de ahí escoge la opción de alta.2. El actor debe escoger el tipo de usuario que dará de alta.3. El actor debe introducir todos los datos de ese usuario que serán almacenados en la base de datos4. El sistema guardará los datos proporcionados en la base de datos del sistema
Flujo Alternativo:	Si datos únicos como identificador del usuario o correo electrónico u otro se repiten el sistema marcara error y los datos no serán almacenados.
Poscondiciones:	El sistema almacenará los datos del nuevo activo usuario en la base de datos del sistema para después poder ser utilizados por el sistema.

Tabla C.12 Caso de Uso: Modulo Administración-Alta Usuarios

Nombre:	Baja Usuario
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción: Permite dar de baja un usuario en el sistema.	
Actores: Usuario de Internet autenticado. (Super user)	
Precondiciones: El usuario debe haberse autenticado en el sistema (solo usuarios super user)	
Flujo Normal: <ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente usuarios y de ahí escoge la opción de baja. 2. El actor debe introducir algún dato de ese usuario para buscarlo en el sistema y poderlo dar de baja en la base de datos 3. El sistema borrará el usuario especificado en la base de datos del sistema 	
Flujo Alternativo:	
Poscondiciones: El sistema borrará los datos del usuario que se haya escogido de la base de datos del sistema. Este usuario ya no podrá acceder al sistema una vez borrado	

Tabla C.13 Caso de Uso: Modulo Administración-Baja Usuarios

Nombre:	Cambio Usuario
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción: Permite realizar alguna modificación a algún usuario en el sistema.	

Actores:
Usuario de Internet autenticado. (Super user)
Precondiciones:
El usuario debe haberse autenticado en el sistema (solo usuarios super user)
Flujo Normal:
<ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente usuarios y de ahí escoge la opción de cambios. 2. El actor debe escoger el tipo de equipo que cambiará. 3. El actor debe introducir los datos de ese usuario que serán cambiados en la base de datos 4. El sistema guardará los datos proporcionados en la base de datos del sistema
Flujo Alternativo: Si datos únicos como el identificador del usuario o correo electrónico u otro se repiten el sistema marcara error y los datos no serán almacenados.
Poscondiciones:
El sistema almacenará los datos modificados del usuario en la base de datos del sistema para después poder ser utilizados por el sistema.

Tabla C.14 Caso de Uso: Modulo Administración-Cambios Usuarios

Nombre:	Consulta Usuario
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite consultar algún usuario en el sistema.
Actores:	Usuario de Internet autenticado. (Super user)
Precondiciones:	El usuario debe haberse autenticado en el sistema (solo usuarios super user)

<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente usuarios y de ahí escoge la opción de consultas. 2. El actor debe introducir algún dato que conozca de ese usuario para poderlo localizar en la base de datos. 3. El sistema desplegará los todos los datos del usuario haciendo una consulta a la base de datos del sistema
<p>Flujo Alternativo:</p>
<p>Poscondiciones:</p> <p>El sistema desplegará los datos del usuario obtenidos de la base de datos del sistema para después poder ser utilizados por el sistema.</p>

Tabla C.15 Caso de Uso: Modulo Administración-Consulta Usuarios

Nombre:	Respaldo
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	
Permite hacer un respaldo de toda la base de datos del sistema, así como de las configuraciones de los equipos.	
Actores:	
Usuario de Internet autenticado. (Super user)	
Precondiciones:	
El usuario debe haberse autenticado en el sistema (solo usuarios super user)	
Flujo Normal:	
<ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente respaldo 	

<p>Existen dos formas de respaldo Base de Datos y Configuración Equipos:</p> <ul style="list-style-type: none"> ○ El respaldo de la base de datos nos creará una copia de seguridad de toda la base de datos que opera el sistema ○ El respaldo de la configuración equipos nos creará una copia de seguridad de todas las configuraciones de los equipos administrados por el sistema <p>2. El actor debe escoger el tipo de respaldo que desea</p> <p>3. El sistema obtendrá toda la información de la base de datos o todas las configuraciones de todos los equipos según haya escogido el usuario</p>
<p>Flujo Alternativo:</p>
<p>Poscondiciones:</p> <p>El sistema guardará una copia de seguridad de las configuraciones o de la base de datos del sistema para poder utilizarla si la original se pierde o se daña.</p>

Tabla C.16 Caso de Uso: Modulo Administración-Respaldo

Nombre:	Restaurar
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite restaurar toda la base de datos del sistema.
Actores:	Usuario de Internet autenticado. (Super user)
Precondiciones:	<p>El usuario debe haberse autenticado en el sistema (solo usuarios super user)</p> <p>El usuario debe haber hecho una copia de seguridad (Respaldo) de la base de datos con anterioridad y conocer la ubicación del archivo de respaldo.</p>
Flujo Normal:	<p>1. El actor escoge en el menú la opción Administración del menú Administración y posteriormente restaurar</p>

2. El actor debe introducir la ruta del archivo de respaldo
3. El sistema podrá volver a crear y poblar la base de datos dañada o perdida

Flujo Alternativo: Si el archivo de respaldo está dañado no se podrá regresar la base de datos a su estado funcional.

Poscondiciones:

El sistema podrá restaurar la base de datos a través de un archivo de respaldo.

Tabla C.17 Caso de Uso: Modulo Administración-Restaurar

Modulo de Manejo de sesión

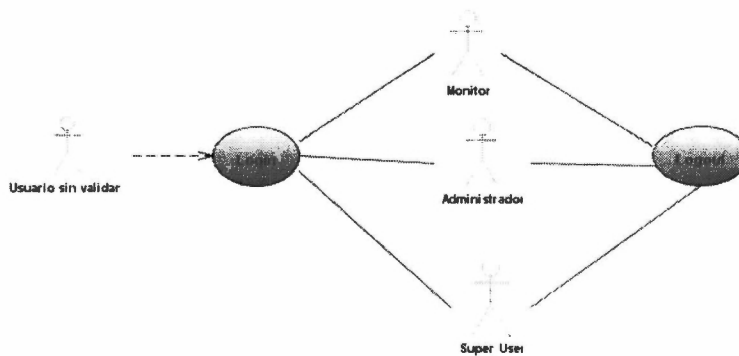


Figura C.5 Caso de Uso del Modulo de Manejo de Sesión

Dentro del modulo de manejo de sesión se encuentran dos casos de uso: login y logout.

Nombre:	Login
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	Permite a un usuario autenticarse como usuario valido y asignarle el perfil que le corresponda para hacer uso del sistema.
Actores:	Usuario de Internet sin autenticar.

<p>Precondiciones:</p> <p>El usuario debe de estar dado de alta como usuario valido en la base de datos del sistema</p>
<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El actor entra a la página de bienvenida del sistema 2. El actor introduce su nombre de usuario y contraseña 3. El sistema coteja que los datos del usuario sean correctos y sea un usuario valido del sistema
<p>Flujo Alternativo: Si el usuario no provee las credenciales validas el sistema regresará a la página de bienvenida.</p>
<p>Poscondiciones:</p> <p>El sistema validó al usuario y creó una sesión dependiendo de los privilegios que este tenga dentro del sistema.</p>

Tabla C.18 Caso de Uso: Modulo Manejo de Sesión-Login

Nombre:	Logout
Autor:	Erika Hernández
Fecha:	21/06/2010
Descripción:	
Permite a un usuario autenticado como usuario valido salir de su sesión.	
Actores:	
Usuario de Internet autenticado. (monitor, administrador, super user)	
Precondiciones:	
El usuario debe haberse autenticado en el sistema (monitor, administrador, super user)	
Flujo Normal:	
<ol style="list-style-type: none"> 1. El actor escoge en el menú la opción Logout 2. El sistema destruye la sesión activa del usuario para que nadie más la pueda utilizar 	

de manera inapropiada

3. El actor sale del sistema

Flujo Alternativo:

Poscondiciones:

El sistema destruye la sesión activa del usuario para que no se utilice por algún usuario no autenticado.

Tabla C.19 Caso de Uso: Modulo Manejo de Sesión-Logout