ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO PARA LA IMPLEMENTACIÓN DE UN CENTRO NOC (NETWORK OPERATIONS CENTER) EN LA INTRANET DE PETROPRODUCCIÓN Y REALIZACIÓN DE UN PROYECTO PILOTO PARA LA MATRIZ QUITO

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

DANNY ALEXANDER BASTIDAS FLORES
dannydabf@hotmail.com

DANIEL SANTIAGO USHIÑA GUSQUE
saus_417@hotmail.com

DIRECTOR: ING. RODRIGO CHANCUSIG
rodrigch@panchonet.net

Quito, Septiembre 2010

DECLARACIÓN

Nosotros, Danny Alexander Bastidas Flores y Daniel Santiago Ushiña Gusque, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Danny Alexander Bastidas Flores Daniel Santiago Ushiña Gusque

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Danny Alexander Bastidas Flores y Daniel Santiago Ushiña Gusque, bajo mi supervisión.

_____

Ing. Rodrigo Chancusig
DIRECTOR DE PROYECTO

DEDICATORIA

El presente trabajo está dedicado primeramente a Dios todopoderoso que me ha dado la vida y salud para poder culminar una etapa muy linda de mi existencia, por permitir compartir de esta alegría con mi familia y las personas que han hecho posible este sueño.

A mi mamita Esperancita y mi padre Jaime Gustavo quienes me han dado su amor, confianza, esfuerzo y todo de ellos para que pueda salir adelante, siendo el ejemplo perfecto a seguir enseñándome lo valioso de la vida y como crecer con esfuerzo, respeto, sabiduría, abnegación y responsabilidad. A mis hermanos Fernando, David y Bryan que siempre me han apoyado y están conmigo en las buenas y las malas sobresaliendo juntos ante cualquier eventualidad, gracias ñañitos.

A mis abuelitos, PapaLucho y MamaLida que son un ejemplo de fuerza, constancia, sacrificio y amor. Igualmente a mi abuelita Inés que desde el cielo nos cuida y llena de bendiciones a mí y mi familia.

A María José quien ha estado conmigo durante el transcurso de mi carrera brindándome su cariño, respeto, confianza y amor siendo ayuda importante para lograr este objetivo, igualmente a su familia que me han dado apoyo incondicional en todos mis actos.

A mis amigos, primos, primas, tías y a todos por sus consejos, enseñanzas, experiencias, amistad, apoyo y ayuda.

Danny Alexander

AGRADECIMIENTO

Agradezco a Dios por darme la vida, salud, bendiciones y las facultades necesarias para poder culminar con cada etapa de mi vida.

A mis padres y hermanos por el apoyo y confianza puestos en mi persona convirtiéndose en un pilar indispensable siendo el motor para seguir adelante venciendo obstáculos a lo largo de la carrera y la vida.

A todos los profesores durante mi transcurso en la Escuela Politécnica Nacional por haber compartido sus conocimientos y prepararme a afrontar la vida profesional.

Al Ing. Rodrigo Chancusig quien como director de tesis nos supo guiar y colaborar con la realización del presente proyecto.

A Petroproducción especialmente al Ing. Pablo Simbaña e Ing. Mónica Sánchez que nos abrieron las puertas para poder realizar el proyecto en la empresa y brindarnos la ayuda necesaria para sacar adelante el trabajo.

A Santiago con quien enfrentamos este reto, por su amistad, compañerismo y ayuda en momentos difíciles durante la realización de la tesis y el paso por la universidad en general.

A nuestro grupo de amigos de la universidad (danny´s, vagos, guaiperos, etc), con quienes compartimos anécdotas, campeonatos, amanecidas, bielitas, bailes y que siempre nos apoyaron para seguir adelante y sobresalir ante las eventualidades durante el transcurso de la carrera.

Danny Alexander

DEDICATORIA

Todo este trabajo se lo dedico a la más hermosa familia que la vida pudo haberme dado. Para Ángel y Sarita unos padres de orgullo para mí, me han brindado el amor, apoyo y confianza, pilares en mi vida y en mis estudios.

A mis hermanos Javier y Ángel Fernando, con quienes he compartido mi vida en buenas y malas, gracias por apoyarme en todo momento.

Para mi familia con todo el cariño y amor del mundo, todo mi esfuerzo y dedicación. Los amo mucho

Santiago

AGRADECIMIENTO

A mi Dios por brindarme la fuerza para continuar día a día, por haberme dado una bella familia, y la oportunidad de vivir este momento.

A la Escuela Politécnica Nacional por verme crecer profesionalmente, a mis profesores por entregar parte de su conocimiento y sabiduría.

Al Ing. Rodrigo Chancusig por su tiempo y guía en la realización y culminación de este proyecto.

Al Departamento de Tecnologías de Petroproducción, por haberme dado la posibilidad de realizar este proyecto, en especial al Ing. Pablo Simbaña y a la Ing. Mónica Sánchez por su tiempo y apoyo.

A todos los amigos y amigas que han sabido compartir parte de su vida conmigo, gracias por su amistad, apoyo y confianza.

Santiago.

ÍNDICE DE CONTENIDOS

DECLARACIÓN ..... **II**

CERTIFICACIÓN ..... **III**

DEDICATORIA ..... **IV**

AGRADECIMIENTO ..... **V**

DEDICATORIA ..... **VI**

AGRADECIMIENTO ..... **VII**

ÍNDICE DE CONTENIDOS ..... **VIII**

ÍNDICE DE FIGURAS ..... **XV**

ÍNDICE DE TABLAS ..... **XVIII**

CAPÍTULO 1 ..... **1**

INTRODUCCIÓN Y MARCO TEÓRICO **1**

1.1. FUNDAMENTOS DE ADMINISTRACIÓN DE REDES 1

1.1.1. ADMINISTRACIÓN DE REDES. *1*

1.1.2. ELEMENTOS EN LA ADMINISTRACIÓN DE RED *1*

1.1.2.1. NMS (Network Management Station) 2

1.1.2.2. Agentes 2

1.1.2.3. Protocolo de Administración de Red 2

1.1.3. ARQUITECTURAS DE ADMINISTRACIÓN DE RED *3*

1.1.3.1. Arquitectura Centralizada 3

1.1.3.2. Arquitectura Distribuida 4

1.1.3.3. Arquitectura Jerárquica 5

1.2. MODELOS DE ADMINISTRACIÓN 6

1.2.1. ADMINISTRACIÓN OSI *6*

1.2.1.1. Arquitectura Funcional 6

1.2.1.1.1. Gestión de Fallas 7

1.2.1.1.2. Gestión de Configuración 8

1.2.1.1.3. Gestión de Análisis de datos (Accounting) 8

1.2.1.1.4. Gestión de Rendimiento 9

1.2.1.1.5. Gestión de Seguridad 9

1.2.1.2. Arquitectura Organizacional 10

1.2.1.3. Arquitectura de Comunicaciones 10

1.2.1.4. Arquitectura Informativa 11

1.2.2. ADMINISTRACIÓN INTERNET 11
1.2.3. ADMNISTRACIÓN TMN (TELECOMUNICATIONS MANAGEMENT NETWORK) 11
1.2.3.1. Arquitectura Funcional 12
1.2.3.2. Arquitectura Física 12
1.2.3.3. Arquitectura De Información 13
1.2.3.4. Arquitectura Organizativa 13
1.3. NOC (NETWORK OPERATIONS CENTER). 13
1.3.1. DEFINICIÓN 13
1.3.2. Objetivos de un NOC 13
1.3.3. Funciones de un NOC. 14
1.3.3.1. Gestión de Red 15
1.3.3.1.1. Despachador 16
1.3.3.1.2. Monitoreo 16
1.3.3.1.3. Análisis de Datos 16
1.3.3.2. Gestión de Configuración 17
1.3.3.2.1. Configuración 18
1.3.3.2.2. Inventario 18
1.3.3.2.3. Estado Operacional 18
1.3.3.3. Gestión de Fallos 18
1.3.3.3.1. Sistema de Gestión 19
1.3.3.3.2. Sistema de incidencias 20
1.3.3.3.3. Seguimiento de reportes 20
1.3.3.4. Gestión de Seguridad 20
1.3.3.4.1. Prevención de Ataques 20
1.3.3.4.2. Detección de Intrusos 20
1.3.3.4.3. Respuesta a Incidentes 21
1.3.3.4.4. Políticas de Seguridad 21
1.3.3.4.5. Servicios de Seguridad 21
1.3.3.4.6. Mecanismos de Seguridad 22
1.3.3.4.7. Procedimiento de Seguridad 22
1.3.3.5. Gestión de Análisis de Datos (Accounting) 22
1.4. PROTOCOLOS DE ADMINISTRACIÓN DE RED 23
1.4.1. CMIP (COMMON MANAGEMENT INFORMATION PROTOCOL) 23
1.4.2. CMOT (COMMON MANAGEMENT INFORMATION PROTOCOL OVER TCP/IP) 23
1.4.3. PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED (SNMP) 23
1.4.3.1. Definición 23
1.4.3.2. Partes 24
1.4.3.3. Funcionamiento de SNMP 24
1.4.4. SNMP VERSIÓN 1 25
1.4.4.1. Características 25

1.4.4.2. Comunidades SNMP 26
1.4.4.3. Mensajes SNMP v1 26
1.4.4.4. Políticas de Acceso 27
1.4.5. SNMP VERSIÓN 2 28
1.4.5.1. Características 28
1.4.5.2. Operaciones de Protocolo 29
1.4.5.3. Mensajes SNMP V2 29
1.4.5.4. Seguridad 29
1.4.6. SNMP VERSIÓN 3 30
1.4.6.1. Características 30
1.4.6.2. Arquitectura SNMPv3 30
1.4.6.2.1. Entidad NMS 30
1.4.6.2.2. Entidad Agente. 31
1.4.6.3. Seguridad SNMPv3 31
1.5. MIB (MANAGEMENT INFORMATION BASE) 32
1.5.1. CARACTERISTICAS 32
1.5.2. Árbol MIB 32
1.5.2.1. Identificadores de Objeto (OID) 32

CAPÍTULO 2 34

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE PETROPRODUCCION. 34

2.1. INTRODUCCIÓN 34
2.1.1. MISIÓN 34
2.1.2. VISIÓN 34
2.2. ANÁLISIS DE LA INFRAESTRUCTURA 35
2.2.1. INSTALACIONES 35
2.2.1.1. Instalaciones Quito 36
2.2.1.2. Instalaciones Distrito Amazónico D.A. 37
2.2.2. SERVIDORES 37
2.2.3. EQUIPOS DE INTERCONECTIVIDAD 56
2.2.4. DIRECCIONAMIENTO IP 56
2.2.5. TOPOLOGÍA DE LA RED 57
2.2.6. ENLACES INTERNOS 57
2.3. ANÁLISIS DE LA RED PASIVA 60
2.3.1. CABLEADO HORIZONTAL 60
2.3.2. CABLEADO VERTICAL 61
2.3.3. DISTRIBUCIÓN DE CUARTO DE EQUIPOS 61
2.4. ADMINISTRACIÓN DE LA RED 62
2.4.1. SEGURIDAD FÍSICA 62

2.4.1.1. Proxy-Firewall Astaro Security Gateway 62
2.4.1.2. Administrador de Ancho de Banda ALLOT ENFORCER 64
2.4.1.3. Políticas de Seguridad Manejadas 65
2.5. ENLACE A INTERNET 66
2.6. ANÁLISIS DE TRÁFICO 67
2.6.1. DETERMINACIÓN DE LAS FECHAS DE MEDICIÓN 67
2.6.2. CONEXIONES SIMULTÁNEAS a servicios 68
2.6.3. TRÁFICO INTERNO 69
2.6.4. TRÁFICO CNT-PETROPRODUCCIÓN 70
2.6.5. TRÁFICO POR SERVICIOS 71
2.6.5.1. Tráfico Mensual por Servicios 72
2.6.5.2. Tráfico Semanal por Servicios 74
2.6.5.3. Tráfico Diario por Servicios 75
2.6.6. TRÁFICO EN SERVIDORES 76
2.6.6.1. Tráfico servidor DNS 77
2.6.6.1.1. Tráfico diario del servidor DNS 77
2.6.6.1.2. Tráfico DNS semanal y mensual 78
2.6.6.2. Tráfico del Servidor Exchange 79
2.7. ESTABLECIMIENTO DE LÍNEA BASE 80
2.7.1. SERVICIOS FRECUENTES 81
2.7.2. EQUIPOS DE IMPORTANCIA 82
2.7.3. ANÁLISIS DE ROUTERS Y SWITCHES 83
2.7.3.1. Router Villafuerte 84
2.7.3.2. Router Principal del Edificio Tribuna 85
2.7.3.3. Switch de Núcleo Catalyst 4507 86
2.7.3.4. Switches de distribución Catalyst 2960G 87
2.8. REQUERIMIENTOS 87
2.8.1. RESPUESTA A FALLOS 88
2.8.2. CONFIGURACIÓN DE ELEMENTOS DE RED 88
2.8.3. REQUERIMIENTOS DE ANÁLISIS DE DATOS (ACCOUNTING) 88
2.8.4. RENDIMIENTO DE RED 89
2.8.5. REQUERIMIENTOS DE SEGURIDAD 89

CAPÍTULO 3 91

DISEÑO DEL CENTRO DE OPERACIÓN DE RED "NOC" 91

3.1. INTRODUCCIÓN 91
3.2. DISEÑO DE LAS AREAS FUNDAMENTALES DEL NOC 92
3.2.1. DISEÑO DE GESTION DE MONITOREO 92
3.2.1.1. Datos a ser Monitoreados 93

3.2.1.2. Definición de Umbrales 94
3.2.2. DISEÑO DE GESTION DE ANÁLISIS DE DATOS (ACCOUNTING) 96
3.2.2.1. Procedimiento para el manejo de Análisis de Datos (Accounting) 97
3.2.3. DISEÑO DE GESTION DE CONFIGURACION 97
3.2.3.1. Configuraciones de Monitoreo 98
3.2.3.1.1. Configuración del Agente Snmpd en Linux 98
3.2.3.1.2. Configuración de SNMP en Windows 2003 Server y Windows XP 98
3.2.3.1.3. Configuración del Agente SNMP en Windows Vista ó Windows 7 99
3.2.3.1.4. Configuración de SNMP en Router o Switch Cisco 100
3.2.3.1.5. Configuración de SNMP en Servidores AS400 100
3.2.3.2. Configuraciones de Conectividad 100
3.2.3.3. Configuraciones de Análisis de Datos (Accounting) 101
3.2.3.4. Configuraciones de Seguridad 101
3.2.4. MANUAL DE PROCEDIMIENTOS DE GESTIÓN DE FALLOS 102
3.2.4.1. Metodología - Troubleshooting 103
3.2.4.2. Proceso de Solución a Fallos 103
3.2.4.2.1. Monitoreo 104
3.2.4.2.2. Identificación del Problema 105
3.2.4.2.3. Aislamiento del problema o fallo 105
3.2.4.2.4. Resolución del Fallas 105
3.2.4.2.5. Documentación 110
3.2.4.3. Plan de Contingencia ante Fallos 114
3.2.4.3.1. Problemas de Conectividad 115
3.2.4.3.2. Procedimientos a ejecutar según el fallo 121
3.2.5. DISEÑO DEL COMITÉ DE SEGURIDAD 129
3.2.5.1. Descripción de la Problemática 130
3.2.5.2. Planeamiento del Comité de Seguridad 130
3.2.5.3. Factores de éxito del Sistema de Seguridad 132
3.3. ESTRUCTURA JERÁRQUICA DE RESPONSABILIDADES 132
3.3.1. RESPONSABILIDADES DEL PERSONAL 134
3.3.1.1. Directorio de Tecnologías 135
3.3.1.1.1. Vicepresidente 135
3.3.1.1.2. Coordinador del NOC 135
3.3.1.2. Área de Aplicaciones 136
3.3.1.2.1. Supervisor de Aplicaciones 136
3.3.1.2.2. Analista de Aplicaciones 136
3.3.1.2.3. Asistente de Aplicaciones 136
3.3.1.3. Área de Datos 136
3.3.1.3.1. Supervisor de Datos 136
3.3.1.3.2. Analista de Datos 137
3.3.1.4. Área de Infraestructura de Comunicaciones 137

3.3.1.4.1. Supervisor de Infraestructura de Comunicaciones 137
3.3.1.4.2. Analista de Infraestructura 138
3.3.1.4.3. Asistente de Infraestructura 138
3.3.1.5. Área de Redes 138
3.3.1.5.1. Administrador de la NMS 138
3.3.1.5.2. Soporte de Networking 139
3.3.1.6. Área de Seguridad 139
3.3.1.6.1. Supervisor de Seguridad 139
3.3.1.6.2. Analista de Seguridades 140
3.3.1.7. Comité de Seguridad 140
3.3.1.7.1. Roles del Responsable de Activos 141
3.3.1.8. Soporte al Usuario 142
3.3.1.8.1. Supervisor de Soporte al Usuario 142
3.3.1.8.2. Asistente de Soporte al Usuario 142
3.3.1.9. Roles de los Usuarios 142
3.3.2. PERFIL DEL PERSONAL DEL ÁREA DE REDES 143
3.4. DISEÑO DE INFRAESTRUCTURA 144
3.4.1. SELECCIÓN DE HERRAMIENTAS SOFTWARE 144
3.4.1.1. Selección de la Distribución Linux 145
3.4.1.2. Selección de la Herramienta de Monitoreo de Red 146
3.4.1.2.1. Requerimientos de la Herramienta 146
3.4.1.2.2. Selección de la Consola de Monitoreo. 147
3.4.2. EQUIPOS NECESARIOS PARA LA IMPLEMENTACIÓN DE LA NMS 150
3.4.2.1. Servidor de Monitoreo 150
3.4.2.2. Servidor de Notificaciones Logs 152
3.4.2.3. Equipos y Elementos de Conectividad 153
3.4.2.3.1. Switch Capa 2 153
3.4.2.3.2. Puntos de Red 153
3.4.3. EQUIPOS A SER MONITOREADOS 154
3.5. ANÁLISIS DE COSTOS DEL NOC 156
3.5.1. COSTOS DE INVERSIÓN 156
3.5.1.1. Activos Fijos 156
3.5.1.2. Activos Nominales 157
3.5.2. Costos de Operación 158
3.5.2.1. Costos de Producción 158
3.5.2.1.1. Mano de Obra 158
3.5.2.1.2. Capacitación 159
3.5.2.1.3. Insumo 160
3.5.2.2. Costos de Ventas 161
3.5.2.3. Gastos Administrativos 161
3.5.2.4. Gastos Financieros 161

3.5.3. Costo total *162*

CAPÍTULO 4 ..... **163**

PILOTO DEL CENTRO DE OPERACIONES DE RED "NOC" QUITO. **163**

4.1. INTRODUCCIÓN 163

4.2. SERVIDOR DE MONITOREO 164

4.3. ESPECIFICACIÓN DE EQUIPOS A MONITOREAR 165

4.4. CONFIGURACIÓN DEL SISTEMA 167

4.4.1. CONFIGURACIÓN DE AGENTES *167*

4.4.2. CONFIGURACION DNS *167*

4.4.3. CONFIGURACION DE NMS *168*

4.4.4. DEFINICIÓN DE USUARIOS *170*

4.4.5. ESPECIFICACIÓN DE ZONAS *172*

4.4.6. ESPECIFICACION DE HOSTS *174*

4.4.7. ESPECIFICACION DE MAPAS *178*

4.4.8. ESPECIFICACIÓN DE ALARMAS *179*

4.5. MONITOREO DE LA RED 181

4.5.1. PRUEBAS DE MONITOREO *185*

4.5.1.1. Caída de Interfaces en dispositivos de red 186

4.5.1.2. Alarmas en utilización de memoria Física. 188

4.5.1.3. Alarmas en utilización de disco Duro. 190

4.5.1.4. Comparación de datos y Veracidad de información capturada. 191

4.5.1.5. Monitoreo de equipos de Networking 197

4.5.1.5.1. Router 198

4.5.1.5.2. Switch de Core. 200

4.6. RESULTADOS DEL MONITOREO 201

4.7. APLICACIÓN DE SOLUCIONES 206

4.7.1. Monitoreo *206*

4.7.2. Seguridad *209*

CAPÍTULO 5 ..... **210**

CONCLUSIONES Y RECOMENDACIONES **210**

5.1. CONCLUSIONES 210

5.2. RECOMENDACIONES 214

GLOSARIO **216**

REFERENCIAS BIBLIOGRÁFICAS **220**

ÍNDICE DE FIGURAS

Figura 1-1.- Elementos en la Administración de Red. 3
Figura 1-2.- Arquitectura de Administración Centralizada 4
Figura 1-3.- Arquitectura de Administración Distribuida. 4
Figura 1-4.- Arquitectura de Administración Jerárquica. 5
Figura 1-5.- Áreas Fundamentales FCAPS. 7
Figura 1-6.- Áreas Funcionales del NOC. 15
Figura 1-7.- Gestión de Fallas del NOC. 19
Figura 1-8.- Partes de Administración de Red..... 24
Figura 1-9.- Ejemplo de Funcionamiento de SNMP 25
Figura 1-10.- Mensajes SNMPv1 entre NMS y Agentes. 27
Figura 1-11.- Entidades SNMPv3 según RFC 2571 31
Figura 1-12.- Árbol MIB 33
Figura 2-1.- Servidores en Cuarto de Equipos. 39
Figura 2-2.- Rack de servidores, Edificio Villafuerte. 43
Figura 2-3.- Distribución de los Equipos de interconexión, Edificio Villafuerte. 49
Figura 2-4.- Cuarto de Equipos – Piso 7 Edificio Tribuna..... 53
Figura 2-5.- Cuarto de Equipos Piso 12 – Edificio Tribuna..... 54
Figura 2-6.- Cuarto Equipos Piso 14 – Edificio Tribuna..... 55
Figura 2-7.- Enlaces Microonda 57
Figura 2-8.- Diagrama de la Red Actual de Petroproducción 59
Figura 2-9.- Rack de Fibra Óptica 60
Figura 2-10.- Diagrama de Conexión del firewall Astaro 63
Figura 2-11.- Detalles de Firewall Astaro Gateway 63
Figura 2-12.- Net-Enforcer Allot 404..... 65
Figura 2-13.- Enlaces a Internet de la red RRR 66
Figura 2-14.- Porcentaje de Utilización del enlace entre CNT y Petroproducción Quito..... 71
Figura 2-15.- Tráfico Mensual de los Principales Servicios 73
Figura 2-16.- Porcentaje de Tráfico Semanal por Servicios 75
Figura 2-17.- Tráfico Diario por Servicios 76
Figura 2-18.- Tráfico Diario DNS 78
Figura 2-19.- Tráfico DNS semanal - mensual 79

Figura 2-20.- Comparativa del Tráfico del Servidor Exchange 80
Figura 3-1.- Partes del Diseño del NOC. 91
Figura 3-2.- Diseño del NOC. 92
Figura 3-3.- Metodología Bottom-Up 103
Figura 3-4.- Proceso de solución de Problemas..... 104
Figura 3-5.- Proceso de Documentación 112
Figura 3-6.- Formato de Hoja de Control de Eventos 113
Figura 3-7.- Proceso de Troubleshooting 114
Figura 3-8.- Proceso para fallos en Hardware..... 120
Figura 3-9.- Proceso para fallos en Configuración 121
Figura 3-11.- Esquema Organizacional de Seguridad..... 131
Figura 3-12.- Estructura Jerárquica del NOC 133
Figura 3-13.- Selección de sistema Operativo Linux. 146
Figura 3-14.- Requerimientos de Hardware de JFFNMS. 150
Figura 3-15.- Infraestructura del NOC 155
Figura 4-1.- Identificación de Características del Servidor de monitoreo. 165
Figura 4-2.- Funcionamiento entrada DNS..... 168
Figura 4-3.- System Setup de JFFNMS. 169
Figura 4-4.- Login al sistema JFFNMS. 170
Figura 4-5.- Creación de Usuarios. 170
Figura 4-6.- Usuarios creados en JFFNMS. 171
Figura 4-7.- Perfil del usuario Admin. 171
Figura 4-8.- Perfil del usuario Monitor. 172
Figura 4-9.- Políticas de Autodescubrimiento de JFFNMS. 172
Figura 4-10.- Zonas creadas para Petroproducción en JFFNMS. 174
Figura 4-11.- Imágenes Cargadas..... 174
Figura 4-12.- Añadir un host al JFFNMS. 175
Figura 4-13.-Selección de interfaces de un host. 176
Figura 4-14.- Visor de interfaces seleccionadas para monitoreo..... 177
Figura 4-15.- Host a monitorear dentro de PPR QUITO..... 177
Figura 4-16.- Visualización de mapas. 178
Figura 4-17.- Mapa Enlaces Principales en vista DHTML Big. 179
Figura 4-18.- Mapa Enlaces Principales en vista Graphviz. 179

Figura 4-19.- Estado de Alarmas y Sonidos de JFFNMS. 180
Figura 4-20.- Definiciones de SLA en JFFNMS..... 181
Figura 4-21.- Opciones del Sistema JFFNMS. 181
Figura 4-22.- Pantalla de Hosts & Events. 183
Figura 4-23.- Monitorización con Performance de JFFNMS 184
Figura 4-24.- Monitoreo del Uso de CPU en servidor ASTARO. 184
Figura 4-25.- Captura de paquetes con Wireshark..... 185
Figura 4-26.- Prueba-Eventos lanzados por detección de alarma..... 187
Figura 4-27.- Formato de registro de prueba realizada. 188
Figura 4-28.- Utilización Memoria del Servidor ASTARO. 189
Figura 4-29.- Alarmas en utilización de memoria en servidor Astaro. 189
Figura 4-30.- Alarmas en utilización de disco duro de servidor de Correo. 191
Figura 4-31.- Utilización de las interfaces del Servidor Astaro, diario. 191
Figura 4-32.- Tráfico en Interfaces Ethernet servidor Astaro tomado del JFFNMS. 192
Figura 4-33.- Análisis de tráfico de la interfaz eth0 tomado del servidor Astaro. 192
Figura 4-34.- Análisis de tráfico de la interfaz eth4 tomado del servidor Astaro. 193
Figura 4-35.- Tráfico servidor Astaro semanal tomado del JFFNMS..... 194
Figura 4-36.- Tráfico servidor Astaro semanal tomado del Astaro. 194
Figura 4-37.- Promedio de Carga de CPU del Servidor ASTARO..... 196
Figura 4-38.- Agregación de Memoria del servidor ASTARO. 196
Figura 4-39.- Estado de las Conexiones TCP en el servidor ASTARO 197
Figura 4-40.- Paquetes Perdidos Servidor ASTARO..... 197
Figura 4-41.- Monitoreo de interfaces del router Villafuerte (Parte I)..... 198
Figura 4-42.- Monitoreo de interfaces del router Villafuerte (Parte II)..... 199
Figura 4-43.- Monitoreo de interfaces del router Villafuerte (Parte III)..... 199
Figura 4-44.- Monitoreo de interfaces del router Villafuerte (Parte IV) 200
Figura 4-45.- Imágenes de Monitoreo de Switch de Core Catalyst 4507 201

ÍNDICE DE TABLAS

Tabla 1-1.- Mensajes SNMPv1 27
Tabla 2-1.- Estructura Actual de la Coordinación TIC 36
Tabla 2-2.- Servidores Ubicados en el edificio Villafuerte 42
Tabla 2-3.- Servidores edificio Tribuna 45
Tabla 2-4.- Servidores Lago Agrio 46
Tabla 2-5.- Equipo Activo en Cuarto de Equipos Villafuerte 48
Tabla 2-6.- Equipo Activo Edificio Villafuerte 50
Tabla 2-7.- Equipo Activo Edificio Tribuna 52
Tabla 2-8.- Enlaces Microonda 58
Tabla 2-9.- Racks Instalados 61
Tabla 2-10.- Interfaces del Firewall Astaro Gateway 64
Tabla 2-11.-Periodos de Medición de Tráfico 67
Tabla 2-12.- Conexiones Simultáneas a Servicios. 68
Tabla 2-13.- Tráfico Interno 69
Tabla 2-14.- Tráfico entre CNT y Petroproducción 70
Tabla 2-15.- Grado Utilización del enlace CNT – Petroproducción Quito. 71
Tabla 2-16.- Tráfico Mensual por Servicios 72
Tabla 2-17.- Tráfico Semanal por Servicios 74
Tabla 2-18.- Muestras de Tráfico Diario por Servicios 75
Tabla 2-19.- Tráfico Diario del Servidor DNS 77
Tabla 2-20.- Tráfico DNS Semanal 78
Tabla 2-21.- Tráfico del Servidor Exchange 80
Tabla 2-22.-Servicios más usados en la Red 82
Tabla 2-23.- Equipos de Importancia a Monitorear 83
Tabla 2-24.- Tráfico Router Villafuerte 84
Tabla 2-25.- Uso de enlaces Router Villafuerte 85
Tabla 2-26.- Tráfico Router Tribuna 86
Tabla 2-27.- Tráfico Switch de Núcleo 86
Tabla 3-1.- Parámetros a Monitorizar por Dispositivo. 93
Tabla 3-2.- Umbrales Establecidos 95
Tabla 3-3.- Escala de Criticidad de la encuesta. 107
Tabla 3-4.- Nivel de Criticidad por Fallo según la encuesta. 107

Tabla 3-5.- Descripción de los niveles de criticidad a ser considerados. 108
Tabla 3-6.- Tiempos máximo de respuesta. 108
Tabla 3-7.- Tiempos óptimo esperado de respuesta. 110
Tabla 3-8.- Parámetros de Documentación 111
Tabla 3-9.- Componentes de Diagramación 111
Tabla 3-10.- Comandos de Troubleshooting en equipos Cisco. 118
Tabla 3-11.- Problemas de Cableado 119
Tabla 3-12.- Procedimiento ante Fallo en Enlace con la CNT 122
Tabla 3-13.- Procedimiento ante Fallo en Enlaces de Comunicación 123
Tabla 3-14.- Procedimiento ante Fallo en Administración Remota 123
Tabla 3-15.- Procedimiento ante Fallos en Switches 124
Tabla 3-16.- Procedimiento ante Fallo en Switch de Núcleo 125
Tabla 3-17.- Procedimiento ante Fallo en Routers 126
Tabla 3-18.- Procedimiento ante Robo de Equipos 127
Tabla 3-19.- Procedimiento ante Fallo Eléctrico 127
Tabla 3-20.- Procedimiento ante Fallo en Discos Duros 128
Tabla 3-21.- Procedimiento ante Problemas de Temperatura. 128
Tabla 3-22.- Procedimiento ante Ataques internos. 129
Tabla 3-23.- Perfil del Personal - Área de Redes 144
Tabla 3-24.- Características de Herramientas de Administración de Red. 149
Tabla 3-25.- Requerimientos Servidor de Monitoreo. 151
Tabla 3-26.- Requerimientos Servidor Logs. 152
Tabla 3-27.- Requerimientos de switch capa 2. 153
Tabla 3-28.- Costos de Equipos 157
Tabla 3-29.- Costos de Operación y Mantenimiento 159
Tabla 3-30.- Costos de Capacitación 160
Tabla 3-31.- Costos de Insumos 160
Tabla 3-32.- Costo Total de Implementación del Proyecto 162
Tabla 3-33.- Gastos Mensuales del Proyecto 162
Tabla 3-34.- Costo Anual del Proyecto 162
Tabla 4-1.- Características de Hardware del Servidor. 164
Tabla 4-2.- Características de Software del Servidor 165
Tabla 4-3.- Equipos Monitoreados 166

Tabla 4-4.- Zonas definidas para su monitoreo 173
Tabla 4-5.- Mapas Implementados 178
Tabla 4-6.- Comparación valores tomados de interfaces de servidor Astaro. 195
Tabla 4-7.- Resumen monitoreo de servidores 204
Tabla 4-8.- Resumen Switches críticos 205
Tabla 4-9.- Interfaces Switches Acceso (Villafuerte) 205
Tabla 4-10.- Resumen Routers Petroproducción. 206
Tabla 4-11.- Propuesta de Soluciones 207

RESUMEN

El proyecto de titulación trata el diseño de un Centro de Operaciones de Red “NOC” para Petroproducción, y la realización de un proyecto piloto en su matriz Quito, que conste en la implementación de un sistema de monitoreo en base al uso de software libre.

En el primer capítulo, se realiza una introducción a la administración de redes, describiendo los modelos de administración OSI, TMN e Internet haciendo énfasis en el modelo FCAPS. Posteriormente se da el concepto de un Centro NOC y se determina sus objetivos, funciones y elementos en base al modelo mencionado. Finalmente se realiza una descripción del protocolo SNMP caracterizando sus tres versiones.

En el segundo capítulo, se realiza una descripción de las instalaciones de Petroproducción recopilando datos de la infraestructura actual. Se efectúa una tabulación de los dispositivos activos, adjuntando diagramas de los racks existentes en los cuartos de equipos. Se analiza el tráfico circundante por la red para establecer una línea base de su funcionamiento. Finalmente se recopilan los requerimientos para el diseño del NOC.

En el tercer capítulo se centra en el diseño de un NOC para Petroproducción mediante el empleo de la metodología FCAPS tratando los temas de: monitoreo, guía de configuración de elementos, análisis de datos (Accounting), un manual de procedimientos de gestión de fallos y la propuesta de un Comité de Seguridad. Posteriormente se realiza un análisis de la plataforma, las herramientas software y hardware a utilizarse para el monitoreo de los equipos. Finalmente se presenta un análisis de costos para la implementación del NOC.

En el cuarto capítulo, se realiza el piloto del NOC consistente en el levantamiento de un servidor de monitoreo, describiendo la configuración de los

equipos. Se utiliza las herramientas de software seleccionadas en el capítulo anterior. A continuación se realizan las pruebas pertinentes, analizando los resultados obtenidos y presentando los problemas encontrados con soluciones factibles para corregirlos.

En el capítulo quinto, se presentarán las conclusiones y recomendaciones obtenidas en la realización del proyecto. Finalmente se presenta la referencia bibliográfica utilizada en este estudio y los Anexos con información que respalda lo expuesto en el proyecto.

PRESENTACIÓN

La Administración y Gestión de una Intranet empresarial debe estar adecuadamente estructurada y organizada con el fin de obtener niveles de disponibilidad óptimos en las comunicaciones y en los servicios prestados. Ante esto, un Centro de Operaciones de Red es importante para cumplir con este objetivo utilizando modelos de administración, políticas claras en la manejo de las tecnologías de la Información y herramientas que permiten un monitoreo preventivo de la infraestructura.

En la actualidad las empresas se encuentran geográficamente distribuidas como es el caso de Petroproducción que posee dependencias en varias ciudades del país y departamentos en dos edificios de Quito. Es importante disponer de normas de seguridad, planes de contingencia y un control centralizado tanto de los dispositivos de comunicación, permitiendo un buen manejo de recursos y servicios.

Un NOC tiene por responsabilidades el monitoreo del estado de la red, atención, resolución y análisis de incidentes que afecten la operatividad y disponibilidad de su infraestructura.

Con lo expuesto anteriormente, el presente proyecto abordara los elementos para el diseño de un NOC, contemplará un análisis para el desarrollo de un sistema de monitoreo y su posterior implementación utilizando software libre cumpliendo con las expectativas del alcance.

Capítulo 1

INTRODUCCIÓN Y MARCO TEÓRICO

1.1. FUNDAMENTOS DE ADMINISTRACIÓN DE REDES

1.1.1. ADMINISTRACIÓN DE REDES.

La administración de redes es un proceso de control, supervisión y toma medidas preventivas y correctivas para el óptimo funcionamiento de la red mediante el uso de herramientas de gestión para controlar degradaciones en su desempeño, a causa de posibles errores que puedan darse. Se diseña y ejecuta a la vez políticas para la optimización de la infraestructura existente, de las aplicaciones y de los servicios que se brindan.

Las redes corporativas por su gran crecimiento en tamaño y complejidad requieren la formulación de estrategias y modelos de administración de redes para un eficiente comportamiento. Para estandarizar el desarrollo de redes y esquemas de administración, la Organización Internacional de Estandarización ISO estableció el modelo OSI para la administración de redes, descrito posteriormente en el punto 1.2.1.

1.1.2. ELEMENTOS EN LA ADMINISTRACIÓN DE RED

La administración de red se basa en el modelo tradicional cliente-servidor compuesto por estaciones gestoras y dispositivos administrados o agentes conjuntamente con un protocolo de red.

1.1.2.1. NMS (Network Management Station)

Son dispositivos independientes que sirven como interfaz entre el administrador y la red. Poseen programas que reciben información de administración proveniente de los dispositivos gestionados. En una red administrada debe existir por lo menos un elemento NMS.

Sus principales características son:

- Aplicaciones de Administración donde se analizan los datos
- Interfaz que permite al Administrador gestionar la Red
- Control de los dispositivos remotos
- Una base de información extraída de las diferentes MIBs (Management Information Base).

1.1.2.2. Agentes

Son módulos que se encuentran en los dispositivos administrados, gestionados mediante un protocolo de administración como por ejemplo: servidores, routers, switches, computadores, impresoras, entre otros. Para poder administrar estos recursos se los representa como un conjunto de objetos conocidos como MIB[1].

1.1.2.3. Protocolo de Administración de Red

Es el encargado de la comunicación entre el gestor y el agente. Depende del modelo de gestión implementado.

[1] Colecciones de información organizada jerárquicamente, a las cuales se accede utilizando protocolos de administración de red.

La Figura 1-2, muestra la manera como se relacionan los elementos de gestión en una red.

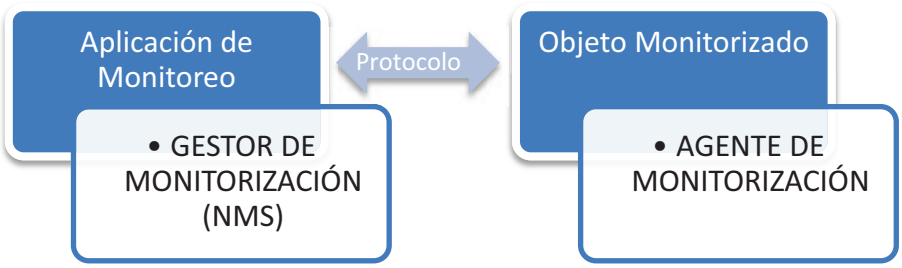


Figura 1-1.- Elementos en la Administración de Red.

1.1.3. ARQUITECTURAS DE ADMINISTRACIÓN DE RED

Se tienen tres arquitecturas fundamentales: centralizada, distribuida y jerárquica, las que se describen a continuación.

1.1.3.1. Arquitectura Centralizada

Aquí todas las consultas son enviadas a un sistema de administración simple. Las aplicaciones de administración son instaladas en la NMS, la cual responde a todos los avisos enviados desde los agentes.

Como se representa en la Figura 1-2, en un sistema de administración centralizado hay un único responsable de realizar consultas de información a los dispositivos. Si bien, su información es fácil de manejar, una NMS puede llegar a sobrecargarse fácilmente debido al número de traps[2] que los agentes pueden enviar al NMS.

[2] PDU generada por el agente para notificar determinadas condiciones y cambios de estado a una consola de administración.

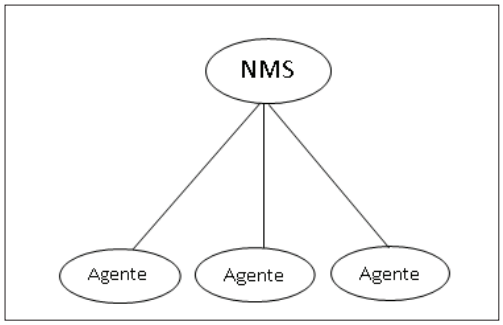


Figura 1-2.- Arquitectura de Administración Centralizada

1.1.3.2. Arquitectura Distribuida

Como se muestra en la Figura 1-3, hay dos puntos de administración del sistema que gestionan a los agentes. Se puede organizar una arquitectura distribuida basada en la geografía, o se puede asignar a cada NMS ser responsable de dispositivos específicos de la red.

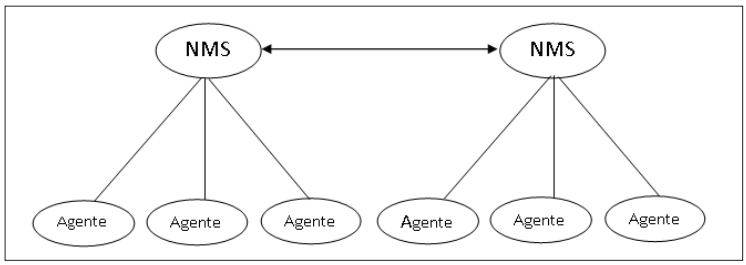


Figura 1-3.- Arquitectura de Administración Distribuida.

Debido a que las aplicaciones de administración están distribuidas en varios sistemas de administración, se puede asegurar que cada NMS no se sobrecargue. Este modelo tiende a limitar los beneficios de un modelo de administración de red centralizado, ya que las NMS pueden enviar solo mensajes entre ellas pero no pueden actualizar consultas o resultados de bases de datos de agentes administrados por otras NMS.

1.1.3.3. Arquitectura Jerárquica

Combina el sistema centralizado con el distribuido. Es la arquitectura más compleja, pero provee las fortalezas de las anteriores. Como se muestra en la Figura 1-4, se utiliza una NMS centralizada que solo coordina consultas enviadas de entidades NMS adicionales.

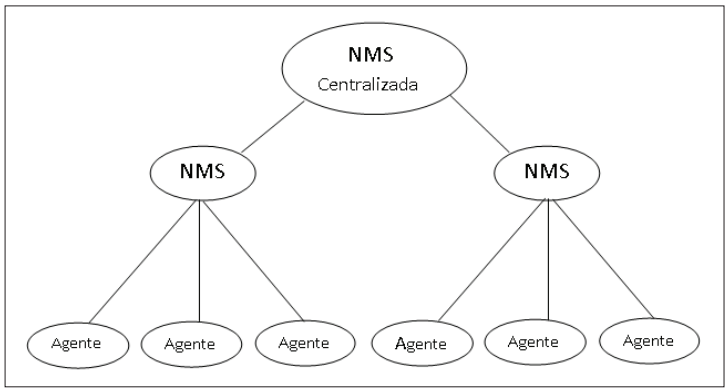


Figura 1-4.- Arquitectura de Administración Jerárquica.

Se puede delegar varias tareas y responsabilidades a varios sistemas en la red, de esta manera se mantiene y almacena la información de una manera centralizada y sin embargo asegura que los sistemas distribuidos sean responsables del procesamiento de consultas y respuestas.

Las aplicaciones de administración están distribuidas en varios sistemas, con un sistema central aceptando información de todas las aplicaciones de sub-administración.

Una desventaja de esta arquitectura es que más sistemas son involucrados. Además del crecimiento de requerimientos de administración, su complejidad también aumenta.

1.2. MODELOS DE ADMINISTRACIÓN

En la actualidad se tienen tres modelos fundamentales para una gestión integrada:

- **Administración OSI.-** *Open System Interconnection* (Interconexión de Sistemas Abiertos). Definido por OSI, tiene por objetivo lograr la gestión de los recursos siguiendo el modelo de referencia OSI.
- **Administración Internet.-** Basado en el protocolo SNMP y emplea el modelo gestor-agente.
- **Arquitectura TMN.-** *Telecommunications Management Network,* definida por la UIT-T.

1.2.1. ADMINISTRACIÓN OSI

Este modelo posee arquitecturas para definir sus características y son las siguientes:

1.2.1.1. Arquitectura Funcional

Define una serie de funciones descritas en la norma ITU-M.3400 llamadas Áreas Funcionales de los Sistemas de Gestión o SMFA (Systems Management Functional Areas)[3], más comúnmente conocido por FCAPS (Fault, Configuration, Accounting, Performance, Security).

Aquí las tareas de administración son separadas en cinco categorías permitiendo una mejor organización. No requiere de la implementación de algún protocolo en específico, sin embargo SNMP y CMIP son los más comúnmente utilizados.

La Figura 1-5, muestra las distintas áreas que componen el modelo FCAPS.

[3] FUENTE: www.ciudadranelagh.com.ar/unlz/unocursada/Redes%20de%20Computadoras/ClaseAdmRedes_unlz.pdf

Figura 1-5.- Áreas Fundamentales FCAPS.

1.2.1.1.1. Gestión de Fallas

Una falla es un evento perjudicial que causa la anormalidad de un servicio y perjudica el rendimiento de la red, por lo que su detección y corrección inmediata son indispensables.

Su objetivo es reconocer, aislar, corregir y registrar los problemas que ocurren en la red, un monitoreo continuo, el establecimiento de alarmas y un análisis de tendencias que permitan predecir posibles errores garantizando la disponibilidad de la red y notificando de manera automática al administrador cuando exista algún problema.

El procedimiento para el manejo de fallas se puede establecer como el siguiente:

- Monitoreo continuo de componentes de red.
- Identificación exacta de la ubicación de la falla.
- Aislamiento de la falla para que la red opere sin interferencia.
- Reacción ante la falla estableciendo acciones para su resolución.
- Asignar los recursos suficientes para su resolución.

- Proveer una solución (probar en todos los subsistemas importantes y grabar esta solución para una futura referencia).
- Notificación, creación de reportes de estado y seguimiento de la reparación.

1.2.1.1.2. Gestión de Configuración

Proceso mediante el cual se inicializa, identifica, configura y se controla las operaciones diarias de los dispositivos que conforman la red. Su objetivo radica en obtener información para establecer ajustes y modificaciones de configuración tanto de hardware como software, nuevos elementos, modificaciones de sistemas existentes, eliminación de componentes obsoletos, generación de reportes y gestión de cambios dentro de la red.

Involucra también el entendimiento del contexto en el cual un dispositivo particular está operando, de los sistemas que trabajan en conjunto y el efecto que causa un sistema en otro. Se incluyen detalles de la topología de la red y un mapa físico de la misma.

En esta gestión se debe tener en cuenta los siguientes aspectos:

- Un acceso rápido a la información sobre configuraciones.
- Un inventario continuamente actualizado de los elementos de la red y de la configuración de los recursos.
- Facilidad en el acceso remoto a los dispositivos.
- Simplificación de la configuración de los equipos.

1.2.1.1.3. Gestión de Análisis de datos (Accounting)

Proceso de recolección de información proveniente de los recursos utilizados, desde equipos de interconexión hasta usuarios finales.

Se realiza con el fin de obtener los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación es muy común en ISPs[4]. Además permite obtener el tiempo que un administrador gasta ayudando a individuos o departamentos particulares.

Otros propósitos de Accountig son el analizar el tráfico, visualizar el porcentaje de utilización de la red globalmente o en forma individual de los diferentes dispositivos, lo que permite administrar los recursos y facilitar el planeamiento de capacidad de la red.

1.2.1.1.4. Gestión de Rendimiento

Provee información del desempeño y de la calidad del funcionamiento de la red actual, recolecta y analiza datos de rendimiento con el fin de asegurar que las prestaciones estén acorde con las necesidades de los usuarios.

La recolección de información permite establecer un historial estadístico de sucesos, permitiendo tomar medidas preventivas y correctivas ante posibles puntos conflictivos que degraden la calidad de los servicios prestados.

Umbrales de rendimiento son utilizados para el manejo de alarmas, habitualmente realizado por la gestión de fallas, otorga un nivel de severidad en función de la falla encontrada. Entre los parámetros que se analizan y controlan están: rendimiento, utilización, tráfico, tasa de error, tiempo de respuesta, cuellos de botella, latencia, entre otros.

1.2.1.1.5. Gestión de Seguridad

Proceso mediante el cual se controla el acceso a los recursos de la red y se protege la información para evitar alteraciones de cualquier índole. Puede ser

[4] FUENTE: UN MODELO FUNCIONAL PARA LA ADMINISTRACIÓN DE REDES, Carlos Vicente Altamirano, Centro de operación de RedUNAM (NOC-UNAM), Julio de 2003

conseguida mediante la implantación de controles, políticas, procedimientos o funciones de software, dividiendo a los recursos dentro de áreas autorizadas y no autorizadas.

La gestión de seguridad se ocupa de los siguientes puntos:

- Identificación de la información que se quiere proteger y su ubicación.
- Identificación de los puntos de acceso a la información.
- Protección y mantenimiento de los puntos de acceso a la información.

1.2.1.2. Arquitectura Organizacional

En esta área se definen los roles y formas de cooperación entre los elementos que forman parte de la administración de la red.

1.2.1.3. Arquitectura de Comunicaciones

Especifica características para el protocolo de comunicaciones a utilizar.

Los elementos que la componen son los siguientes:

- ASCE (Association Control Service Element).- Establece la conexión y liberación de las operaciones realizadas entre los elementos de la red.
- ROSE (Remote Operate Service Elelement).- realiza el control de las operaciones remotas.
- CMISE (Common Management Information Service Element).- brinda las características acerca del protocolo basadas en dos elementos que son: CMIP (Common Management Information Protocol) y CMIS (Common Management Information Services).

1.2.1.4. Arquitectura Informativa

Da las características de la forma en que se van a relacionar los diferentes elementos de la red a partir del concepto relacionado a un objeto.

1.2.2. ADMINISTRACIÓN INTERNET

Definido por el IETF (Internet Enginnering Task Force) y la IAB (Internet Activities Board), para la administración por medio de la arquitectura TCP/IP.

Utiliza los siguientes componentes para realizar su administración:

- Protocolo Simple de Gestión de Red (SNMP, Simple Network Management Protocol).
- Agentes SNMP.
- Estructura de Información y Gestión (SMI, Structure of Management Information), y
- Base de Información de Gestión (MIB, Management Information Base).

Este modelo depende de la existencia de agentes SNMP en cada dispositivo gestionado encargados de recolectar información sobre el estado, advertencias y alarmas de dicho elemento. Esta información es enviada a una aplicación central que controla el sistema compuesta por la base de datos MIB jerárquica y una consola de administración.

1.2.3. ADMNISTRACIÓN TMN (TELECOMUNICATIONS MANAGEMENT NETWORK)

Su objetivo es proporcionar una estructura de red organizada para interconectar distintos tipos de sistemas de administración y dispositivos de telecomunicación

haciendo uso de una arquitectura estándar e interfaces normalizados. Tiende a ser flexible, escalable y confiable.

Se orienta hacia la cooperación entre los sistemas de gestión individuales para conseguir un efecto coordinado en la red usando un conjunto de arquitecturas siguientes:

1.2.3.1. Arquitectura Funcional

Describe la funcionalidad del modelo TMN definiendo un conjunto de bloques funcionales que son los siguientes:

- Bloque Funcional de Sistema de Operación (OSF).- funciones típicas de una administración gestor-agente.
- Bloque Funcional de Elementos de Red (NEF).- Funciones de los dispositivos de red que les permiten funcionar como agentes de gestión.
- Bloque Funcional de Estación de Trabajo (WSF).- otorga los medios necesarios para conectar al usuario con el sistema de operaciones, permitiendo que pueda interpretar la información de gestión TMN.
- Bloque Funcional de Adaptador Q (QAF).- permite la administración de elementos de red que posean un sistema de gestión propietario.
- Bloque Funcional de Mediación (MD).- actúa sobre la información que llega de los NEF y de los QAF para adaptarla, filtrarla y condensarla al formato usado por los OSF.

1.2.3.2. Arquitectura Física

Muestra la manera en que los bloques funcionales definidos anteriormente se pueden implementar en dispositivos físicos interconectados mediante interfaces.

1.2.3.3. Arquitectura De Información

Está basada sobre un modelo orientado a objeto y define el formato de los datos que se transmite entre los bloques funcionales.

1.2.3.4. Arquitectura Organizativa

Introduce una relación jerárquica entre los diferentes sistemas de operación existentes en la red, de tal manera que existan gestores de bajo nivel orientados a la solución de problemas técnicos y gestores de alto nivel encargados de garantizar calidad de servicio. Para esto se divide en capas al bloque funcional OSF, la comunicación entre bloques se da mediante una relación gestor-agente.

1.3. NOC (NETWORK OPERATIONS CENTER).

1.3.1. DEFINICIÓN

Entidad de trabajo encargada de la administración de una red, de su infraestructura física y lógica, con la finalidad de mantener adecuados índices de rendimiento y disponibilidad.

Dentro del RFC 1302 (Building a Network Information Services Infrastructure), se define como: "*Un Centro de Operaciones de Red es una organización cuyo objetivo es supervisar y mantener las operaciones diarias de una red*."

1.3.2. OBJETIVOS DE UN NOC

Entre los objetivos que un NOC persigue se encuentran:

- Mantener la correcta operación de la red y de sus enlaces.

- Implementar herramientas que otorguen un adecuado funcionamiento de la red.
- Monitorear todos los enlaces de backbone y dispositivos de red.
- Monitorear, identificar y resolver irregularidades encontradas.
- Solucionar fallas de la red en el mínimo tiempo posible.
- Establecer normas y procedimientos para la gestión de la red.
- Implantar nuevas tecnologías dentro de la infraestructura de red.
- Verificar la continua operación de servidores y servicios.
- Operar las 24 horas del día, 7 días a la semana.
- Disponer de un personal adecuadamente preparado para su operación.
- Proveer soporte de calidad a los usuarios de la red.

1.3.3. FUNCIONES DE UN NOC.

Las diferentes áreas funcionales del NOC son determinadas en base a recomendaciones del modelo FCAPS y adaptadas según las necesidades y características de la red a fin de cumplir los objetivos de un NOC.

La Figura 1-6, muestra los distintos elementos existentes en un NOC dentro de cada área funcional

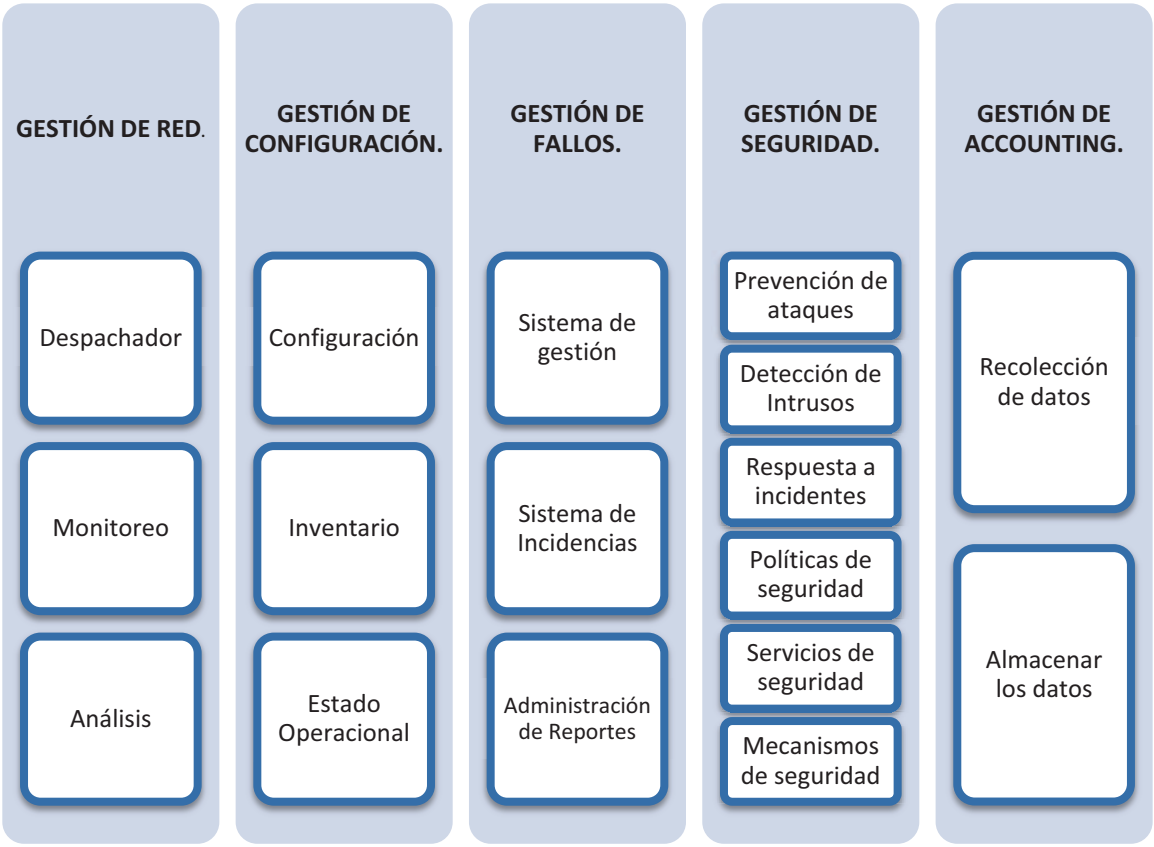


Figura 1-6.- Áreas Funcionales del NOC.

Siguiendo el modelo antes mencionado, se describen las siguientes áreas funcionales.

1.3.3.1. Gestión de Red

Dentro de las tareas que cumple se encuentran actividades proactivas y correctivas. Es el encargado de monitorizar el estado actual de la red asegurando su disponibilidad, un efectivo reconocimiento de fallas y la detección de posibles degradaciones en los servicios. Se la puede descomponer en sub-áreas operativas encargadas de realizar distintas funciones dentro de la gestión de la red.

1.3.3.1.1. Despachador

Establece el punto de ingreso de solicitudes y reportes para su posterior direccionamiento al área de operación correspondiente para su seguimiento y solución.

1.3.3.1.2. Monitoreo

Encargada de verificar el correcto funcionamiento y desempeño de la red y de sus enlaces en función de datos recolectados, además de los procesos y actividades que operan dentro de la administración de la red.

Sus tareas comprenden:

- Verificar alarmas provenientes de dispositivos monitoreados identificando puntos de falla.
- Realizar pruebas preliminares como método para el seguimiento del área operacional de la red.
- Interpretar datos provenientes del estado y desempeño de los dispositivos según un análisis de los registros históricos.
- Disponer de sistemas de monitoreo que trabajen con protocolos basados en SNMP y MIB.
- Realizar reportes acerca del estado actual de la red.
- Contar con un sistema de monitoreo operacional las 24 horas del día, 7 días a la semana los 365 días del año.

1.3.3.1.3. Análisis de Datos

La información recolectada en la etapa de monitoreo debe ser interpretada a fin de determinar el comportamiento de la red y tomar medidas que ayuden a mejorar su rendimiento. Se pueden detectar comportamientos relacionados a:

- **UTILIZACIÓN ELEVADA.-** Utilización en altos niveles de dispositivo o enlace.

- **TRÁFICO INUSUAL.-** El tráfico fuera de los patrones normales aporta elementos importantes en la resolución de problemas de rendimiento.

- **ELEMENTOS PRINCIPALES.-** Al identificar los elementos que más reciben y transmiten información se puede establecer un monitoreo más constante, debido a su importancia. La detección de elementos que generalmente no se encuentra dentro del patrón de equipos con más actividad ayuda a la detección de posibles ataques a la seguridad.

- **CALIDAD DE SERVICIO.-** Garantizar las condiciones necesarias a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP, entre otros.

- **CONTROL DE TRÁFICO.-** El tráfico puede ser reenviado o ruteado por otro camino cuando se detecte saturación en un enlace o al detectar que se encuentra fuera de servicio.

1.3.3.2. Gestión de Configuración

Encargado de mantener la información de diseño de la red y la configuración de los elementos integrantes, de cada equipo y nodo que se va a gestionar y de los enlaces necesarios para la comunicación interna y externa.

Es tarea de un NOC hacer que cada nodo esté bajo las configuraciones y el esquema topológico establecido, a fin de garantizar su operatividad. De no ser este el caso y al no cumplir las especificaciones requeridas se realizan los reportes necesarios para tomar medidas pertinentes.

Un NOC se maneja dentro de tres aspectos, configuración, inventario y el estado operacional de la red definiendo en cada uno de ellos temas que tratar.

1.3.3.2.1. Configuración

- El estado actual de la red de datos.
- Registro de la topología.
- Dispositivos instalados y su ubicación.
- Personal responsable.
- Estado operacional de los dispositivos gestionados.

1.3.3.2.2. Inventario

- Base de datos de los elementos de la red.
- Historial de fallas.
- Cambios realizados.
- Nodos y sus funciones.
- Mecanismos para la ubicación de información.

1.3.3.2.3. Estado Operacional

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

1.3.3.3. Gestión de Fallos

Se centra en la detección y corrección de fallos en base a alarmas generadas. Su control está a cargo del personal administrativo del NOC en turno que abre un proceso de seguimiento al problema para establecer una solución adecuada y su posterior notificación de estado del mismo.

Se posee dos métodos para la detección de problemas en la red: una proactiva y una reactiva.

- **La detección proactiva.-** aquella que mediante un monitoreo y análisis continuo de la red, permite visualizar un comportamiento que haga predecible algún problema en los servicios, enlaces o dispositivos.
- **La detección reactiva.-** reacciona ante una fluctuación en los servicios de la red o en cualquiera de sus elementos, afectando los niveles de correcto funcionamiento de los servicios brindados.

1.3.3.3.1. Sistema de Gestión

El proceso para la gestión de una falla viene dado por los pasos descritos en la Gestión de Fallos dentro del modelo FCAPS, en síntesis la Figura 1-7 muestra el procedimiento a seguir ante una eventual falla.

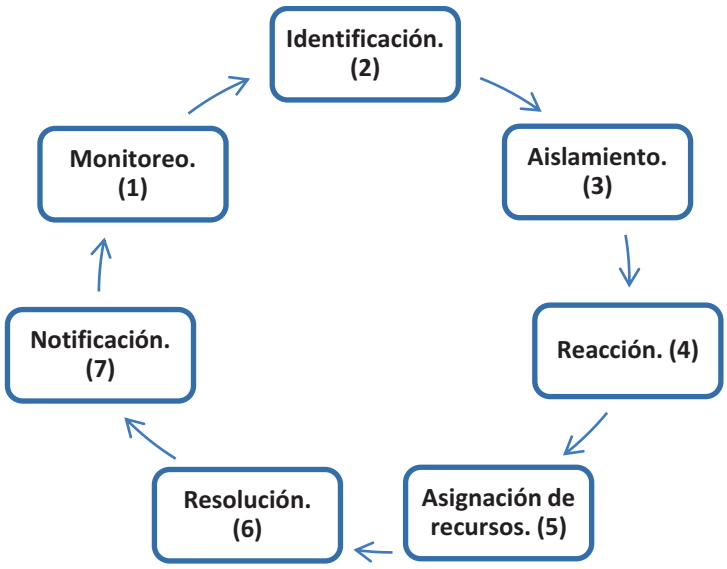


Figura 1-7.- Gestión de Fallas del NOC.

1.3.3.3.2. Sistema de incidencias

Se establece a fin de dar seguimiento a fallas detectadas. Programa y asigna tareas delegando responsabilidades, a su vez supervisa las actividades realizadas durante la resolución de la falla y realiza un análisis de los problemas surgidos.
Se da seguimiento a:

- El estado actual de la falla.
- El personal asignado.
- Actividades realizadas por el personal.
- Tiempo estimado para su resolución.

1.3.3.3.3. Seguimiento de reportes

Desde el ingreso de un reporte, éste es priorizado, notificado y atendido registrando las actividades realizadas para resolver el fallo. Posterior a su solución, es almacenado para usarlo en estadísticas e informes de operación.

1.3.3.4. Gestión de Seguridad

Su objetivo se centra en ofrecer la seguridad necesaria a la red y a cada uno de sus elementos, crea estrategias para la prevención, detección de ataques y una respuesta ante incidentes de seguridad.
Con el fin de cumplir este objetivo, un NOC debe incluir los siguientes aspectos:

1.3.3.4.1. Prevención de Ataques

Mantiene a usuarios mal intencionados fuera del alcance de recursos de la red implementando estrategias en el control de acceso.

1.3.3.4.2. Detección de Intrusos

Detecta el momento en que un ataque se está llevando a cabo. Se lo puede lograr mediante la implementación de un sistema de detección de intrusos que

monitoree el tráfico circulante por la red y se apoye en un esquema de alarmas indicando el momento de detección de una anomalía.

1.3.3.4.3. Respuesta a Incidentes

Toma las medidas necesarias para conocer las causas de un incidente de seguridad y tratar de eliminar las mismas.

1.3.3.4.4. Políticas de Seguridad

Establece requerimientos para la protección de la información e infraestructura de red, posterior a un análisis de necesidades de seguridad y especificando los mecanismos para su cumplimiento.
Algunas políticas necesarias son:

- Políticas de contraseñas
- Políticas de cuentas de usuario
- Políticas de respaldos
- Políticas de listas de acceso
- Políticas de configuración de dispositivos
- Políticas de acceso remoto, entre otros.

1.3.3.4.5. Servicios de Seguridad

Definen los objetivos específicos a ser implementados en los mecanismos de seguridad para satisfacer las políticas de seguridad establecidas.
Lo componen los siguientes servicios de seguridad:

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso

1.3.3.4.6. Mecanismos de Seguridad

Herramientas necesarias para poder implementar los servicios de seguridad, por ejemplo: cortafuegos, RADIUS, TACACS, Secure Shell, IPSec, entre otros.

1.3.3.4.7. Procedimiento de Seguridad

Acciones necesarias para llevar a cabo el objetivo perseguido por la Gestión de Seguridad. Un procedimiento de seguridad establecerá los siguientes pasos:

- Elaboración de las políticas de seguridad, reglas de administración de la infraestructura de red, de su buen uso, prevención y respuesta a incidentes de seguridad.
- Definición de servicios a ofrecer e implementar.
- Implementación de las políticas de seguridad.

1.3.3.5. Gestión de Análisis de Datos (Accounting)

Contabiliza el tráfico y los datos generados por elementos y enlaces de la red. Los sistemas de monitoreo recolectan a diario esta información para almacenarla en una base de datos que puede ser accesada por los sistemas de trabajo del NOC a fin de generar información útil y manejable para diferentes objetivos analíticos.

Los objetivos que persigue son:

- Identificar el uso ineficiente de la red.
- Evitar sobrecargas dentro de la red y perjuicios a otros usuarios.
- Planificar el crecimiento de la red.
- Verificar los servicios a los usuarios en función de sus necesidades.

1.4. PROTOCOLOS DE ADMINISTRACIÓN DE RED

1.4.1. CMIP (COMMON MANAGEMENT INFORMATION PROTOCOL)

El Protocolo de Administración de Información común (CMIP) se implementa sobre el modelo OSI y soporta CMIS (Common Management Information Services) que permite la colección y transmisión de Información de administración de red. Además este protocolo añade el servicio de petición/respuesta para el intercambio de información simétrica o asimétrica de control y mantenimiento de la red entre gestores y agentes, originando que sea uno de los primeros protocolos de Administración de Red, que en la actualidad prácticamente ya no es utilizado.

1.4.2. CMOT (COMMON MANAGEMENT INFORMATION PROTOCOL OVER TCP/IP)

La creciente acogida que tuvieron las redes de Internet basados en TCP/IP, generan la necesidad de la creación de un nuevo protocolo que permita la administración de estas redes. CMOT es simplemente una variante de CMIP implementado sobre un modelo de red TCP/IP, cumple las mismas funciones de intercambio de información de control y manteniendo de la Red pero sobre TCP/IP. CMOT y SNMP utilizan los mismos conceptos básicos en la descripción y definición de la administración de la información llamado Estructura e Identificación de Gestión de Información (SMI) descrito en el RFC 1155 y Base de Información de Gestión (MIB) descritos en el RFC 1156[5].

1.4.3. PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED (SNMP)

1.4.3.1. Definición

SNMP (Simple Network Management Protocol) fue creado para facilitar el intercambio de información administrativa entre los diferentes dispositivos que

[5] FUENTE: http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

componen una red, permitiendo a los administradores controlar, supervisar, gestionar y resolver problemas presentes, así como planificar el crecimiento futuro de la red.

Es un protocolo de capa aplicación de la arquitectura TCP/IP estandarizada y descrita en los RFC 1157. Hasta el momento existen tres versiones del protocolo: v1, v2c y v3. Las tres son muy parecidas, con la diferencia que SNMPv2 tiene algunas mejoras sobre la primera versión, y de la misma forma SNMPv3 tiene ciertas ventajas sobre la segunda versión pero no ha sido mayormente aceptado en la industria.

1.4.3.2. Partes

El protocolo SNMP se constituye de 2 elementos principales para que funcione: las Estaciones de Administración de Red (NMS) y los Agentes.

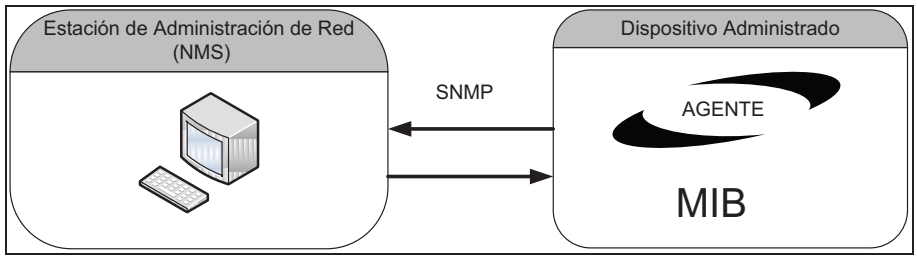


Figura 1-8.- Partes de Administración de Red.

1.4.3.3. Funcionamiento de SNMP

Consiste en el intercambio de mensajes entre la NMS y el agente del dispositivo administrado. Existen dos formas de empezar la comunicación; La primera cuando la NMS pide la información que requiere a un dispositivo administrado específico, el agente verifica el pedido si es autentico y responde con la información que le ha sido solicitada. La segunda forma es cuando el agente envía información de un evento suscitado en él sin que sea pedido con anterioridad por la NMS.

SNMP utiliza un servicio No Orientado a Conexión manejando el protocolo UDP (User Datagram Protocol), enviando mensajes con formatos ya establecidos que tienen información de seguridad y PDUs (Protocol Data Unit) especificas.
Los mensajes se envían a través de los puertos 161 (para mensajes de petición y repuesta) y 162 (para mensajes de notificación mediante traps). Cuando un agente envía una trap, la NMS envía un polling como respuesta.

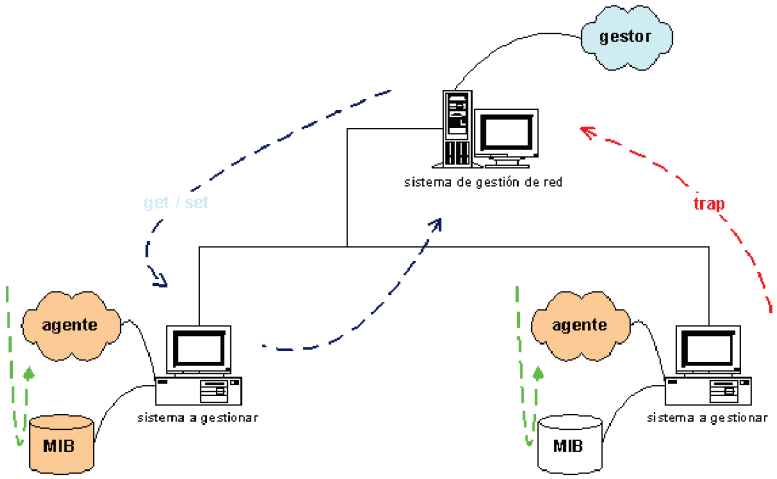


Figura 1-9.- Ejemplo de Funcionamiento de SNMP[6]

Como se menciona anteriormente SNMP alberga tres versiones, la comunicación descrita puede darse en función de cada una de ellas. A continuación se describen las tres versiones que se hacen referencia.

1.4.4. SNMP VERSIÓN 1

1.4.4.1. Características

Es la primera versión del protocolo SNMP, su principal objetivo era tener simplicidad en la administración de redes, para lo cual se definió ciertas características como los mensajes SNMP, generación de traps, formato de PDUs,

[6]FUENTE: SNMPv3 (Simple Network Management Protocol version 3). Autor: Ramón Jesús Millán Tejedor. Publicado en BIT Nº 139, COIT & AEIT, 2003.
http://www.ramonmillan.com/tutorialeshtml/snmpv3.htm

utilización de UDP en la capa transporte, entre otras. Se origina principalmente de SGMP (Simple Gateway Monitoring Protocol), el cual se utilizaba para una administración simple en redes pequeñas. A medida que éstas crecían considerablemente, existió la necesidad de crear un nuevo protocolo que permita gestionar las mismas, SNMP v1. Está descrito en las RFC 1155, 1157 y 1212 del IETF (Internet Engineering Task Force).

1.4.4.2. Comunidades SNMP

Comunidad es un conjunto de NMS con dispositivos administrados y la interrelación que existe entre ellos. A las comunidades se les asignan nombres, de tal forma que junto con información adicional sirva para validar el mensaje SNMP y al emisor del mismo definiendo características de autenticación y control de acceso.

El agente establece una comunidad para cada combinación deseada de autentificación. Para que una NMS pueda gestionar a un dispositivo debe tener el mismo nombre de comunidad para consultar y configurar un agente.

Los dispositivos pueden pertenecer a varias comunidades, todo con el fin de que se limiten el acceso a sus MIBs únicamente a sus respectivas NMS.

Cuando un NMS envía un comando SNMP, el nombre de comunidad es incluido en el mensaje que identifica al emisor y receptor de la información, el agente determina cual comunidad está en la lista de nombres aceptados y si éste no coincide, el paquete es descartado, permitiendo un nivel básico de autenticación.

1.4.4.3. Mensajes SNMP v1

El mensaje consiste de un Identificador de versión, un nombre de comunidad y una PDU SNMP. Los mensajes intercambiados entre una NMS y los agentes son independientes unos de otros. En SNMP v1 se tiene solo cinco tipos de mensajes con PDUs básicas que se utilizan para el intercambio de información mostrados en la Figura 1-10.

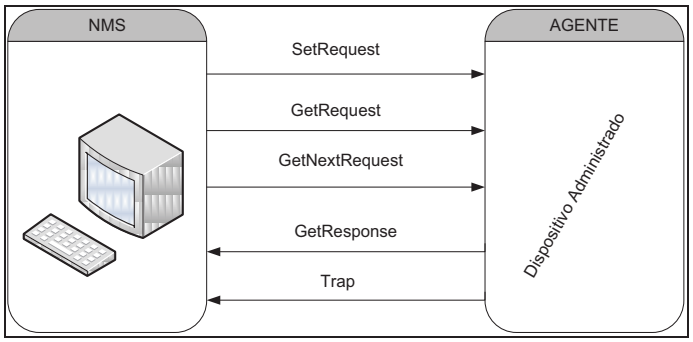


Figura 1-10.- Mensajes SNMPv1 entre NMS y Agentes.

Los mensajes de SNMP v1 se especifican en la siguiente tabla:

TIPO	MENSAJE	DESCRIPCION
1	GetRequest	Contiene una lista de variables que el administrador desea leer de una MIB, consulta a un agente sobre el estado de un objeto en particular.
2	GetNextRequest	Tiene el mismo funcionamiento que GetRequest pero provee un modo de lectura secuencial de datos de una tabla MIB.
0	SetRequest	Permite asignar o modificar valores de las variables que desee de un agente.
3	GetResponse	El agente envía este mensaje como respuesta a un mensaje de GetRequest, GetNextRequest o SetRequest.
4	Trap	Mensaje generado por el agente en respuesta a un evento o acontecimiento que afecte a la MIB o a los recursos gestionados, los cuales pueden ser fallas, caídas o subidas de enlace, mensaje de mala autenticación, entre otros.

Tabla 1-1.- Mensajes SNMPv1

1.4.4.4. Políticas de Acceso

Son una forma de brindar seguridad en la administración de redes. Básicamente existen 3 aspectos que se controlan:

- **Servicio de Autenticación:** El agente puede limitar el acceso a las MIB a las NMS.
- **Políticas de Acceso:** El agente da los permisos para acceder a ciertos objetos MIB por parte de las NMS
- **Servicios Proxy:** Un agente podría actuar como un proxy hacia otro agente.

Este control permite a un agente limitar el acceso a su información a un conjunto de NMSs. Utilizando varias comunidades, el agente puede proporcionar diferentes categorías de acceso a distintas estaciones de administración de red. Este control consta de dos aspectos:

- **Modo de acceso**: Acciones que se pueden realizar sobre la información, identificadas por RO (Read Only) y RW (Read-Write)
- **Vistas:** Se refiere a colecciones de información que están disponibles para que sean accedidas por las estaciones gestoras. Para cada comunidad pueden definirse diferentes vistas según se requiera.

1.4.5. SNMP VERSIÓN 2

1.4.5.1. Características

Es la segunda versión de SNMP que brinda algunas mejoras con respecto a la versión 1. Es compatible tanto para redes TCP/IP como para aquellas basadas en OSI. La especificación de SNMPv2 se encuentra definida en las RFC 1441-1452.
Entre las mejoras añadidas con respecto a la primera versión se destacan las siguientes:

- Se permite la comunicación entre NMSs,
- Se tiene un nivel de seguridad,
- Nuevas operaciones del protocolo,
- Permite lectura de tablas completas en una sola operación,
- Características adicionales de SMI (Structure and Identification of Management Information).

1.4.5.2. Operaciones de Protocolo

Proporciona tres tipos de acceso a la información de gestión:

- Petición/Respuesta NMS-Agente.
- Agente-NMS sin confirmación.
- Petición/Respuesta NMS-NMS.

A diferencia de SNMPv1 se incrementa el tercer tipo de acceso que permite la comunicación entre estaciones de administración permitiendo compartir información entre NMS. Descrito en RFC 3416.

1.4.5.3. Mensajes SNMP V2

Hereda los mensajes de la versión anterior conservando su formato de cabecera y añade otros mensajes para mejorar la administración. Estos son:

- **InformRequest**.- utilizado para compartir información de administración entre entidades NMS
- **GetBulkRequest**.- añadido para poder receptar todos los valores de una tabla con una sola petición permitiendo obtener información de forma más eficiente y reduciendo el número de peticiones.
- **Trap V2**.- Tiene la misma función que la PDU Trap de SNMPv1, pero con un formato diferente para facilitar la tarea de procesamiento del receptor.
- **Report.-** Respuesta a un inform request con valores correctos cuando se ha producido un error.

Conjuntamente con los nuevos tipos de mensajes, se añaden distintos de tipos de errores que se puedan presentar y ayudar la administración.

1.4.5.4. Seguridad

Se mantuvo el mismo concepto de comunidad que no brindaba el nivel deseado de seguridad pues era mínimo en las operaciones de administración. Para ésto, se plantearon tres tipos de SNMPv2 que son: v2c, v2u y v2*.

- **SNMPv2c**: está basado en comunidad y es el que se mantiene en mayor uso.
- **SNMPv2u** (basado en usuario) donde un usuario puede estar definido en varias entidades SNMP.
- **SNMPv2*:** proporciona mayores niveles de seguridad pero no fue aceptado por la IETF y no se estandarizó.

1.4.6. SNMP VERSIÓN 3

1.4.6.1. Características

Introduce seguridad basada en usuario, denominado el modelo USM (User-Based Security Model), un modelo de control de acceso basado en vistas VACM (View-based Access Control Model) y configuración remota. Además soporta el uso concurrente de diferentes seguridades, control de acceso y modelos de procesamiento del mensaje. Se encuentra definido en los RFC 1902-1908 y 2271-2275.

1.4.6.2. Arquitectura SNMPv3

Se desarrolló bajo el concepto de modularidad que no había en las versiones anteriores. Además añade el concepto de entidad que abarca tanto a los agentes como a las NMS. Las partes de las entidades se aprecian en la Figura 1-11.

1.4.6.2.1. Entidad NMS

- **Generador de Comandos:** Genera las PDU con que se trabaja.
- **Originador Notificaciones:** Responde al Inform Request.
- **Dispatcher:** Trabaja directamente con los mensajes recibidos y enviados.
- **Procesamiento de Mensajes:** Analiza el tipo de protocolo a ser utilizado.
- **Seguridad:** Trabaja con los diferentes modelos de seguridad según el protocolo.

1.4.6.2.2. Entidad Agente.

- **Control de acceso:** Controla el acceso de la información con VACM por ejemplo.
- **Respuesta de Comandos:** Responde peticiones de una entidad.
- **Proxy:** Interrelaciona en forma transparente diferentes entidades.

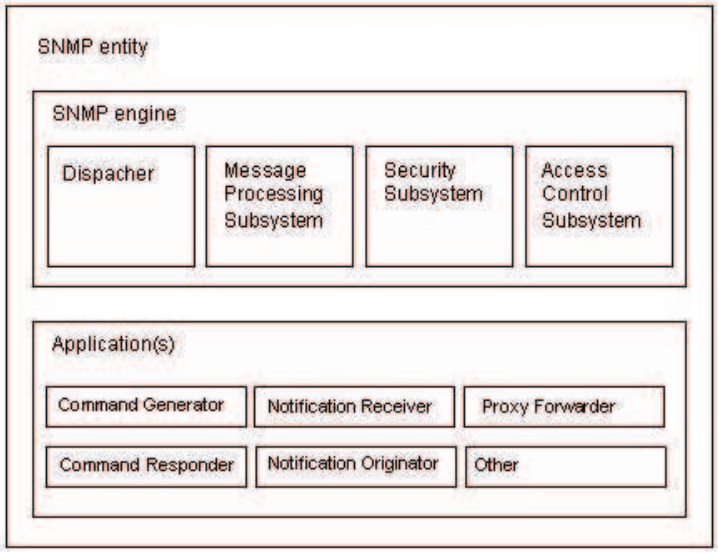


Figura 1-11.- Entidades SNMPv3 según RFC 2571[7]

1.4.6.3. Seguridad SNMPv3

Mantiene las PDUs de SNMPv1 y v2, pero define nuevas capacidades de seguridad. Trabaja con autenticación y/o encriptación, proporcionando protección contra amenazas como la modificación del flujo de mensajes, el enmascaramiento de información, violación de confidencialidad, entre otras.

[7] FUENTE: http://biblioteca.unitecnologica.edu.co/notas/2005-12-12/0032134.pdf

1.5. MIB (MANAGEMENT INFORMATION BASE)

1.5.1. CARACTERISTICAS

Es una base de datos bien definidos utilizados para manejar diversos grupos de objetos. Contiene información sobre variables que se pueden modificar o leer y una estructura de árbol jerárquica. Fueron creadas como parte de la gestión de red definida por OSI, definiendo las variables utilizadas por un protocolo de administración de red, permitiendo la administración y control de los dispositivos de una red. Las MIB-I y MIB-II se especifican en los RFC 1156 y RFC 1158 respectivamente.
Los objetos MIB se definen en las ASN.1 (Abstract Syntax Notation One), trabaja con reglas BER (Reglas de codificación Básica), y los tipos de datos con que puede trabajar se representan con SMI (Información para la administración estructurada).

Para definir una variable u objeto MIB se especifica lo siguiente:

- **Sintaxis:** Especifica el tipo de datos de la variable.
- **Acceso:** Especifica el tipo de permiso como: ro, rw, wo o no Access.
- **Estado**: Define si la variable es obligatoria u opcional.
- **Descripción:** Describe a la variable.

1.5.2. ÁRBOL MIB

Se definen grupos y dentro de ellos se sigue la jerarquía mencionada de la MIB con características propias. El espacio de Nombres del objeto identificador (Object ID) es administrado por la ISO y la ITU responsables de delegar y manejar el espacio de nombres a otras organizaciones.

1.5.2.1. Identificadores de Objeto (OID)

Nombre mediante el cual son identificados los objetos de los dispositivos administrados de manera única.

Este puede ser escrito textualmente en palabras, ejemplo (sysDescr), o siguiendo el árbol según sus números de identificación.

Por ejemplo: para obtener el sysContact de un objeto se utilizara 1.3.6.1.2.1.1.4 (Figura 1-17). O escribiendo toda la secuencia del árbol MIB según sus nombres, por ejemplo, para realizar petición del SysUptime de un agente: .root.iso.org.dod.internet.mgmt.mib2.system.SysUptime.

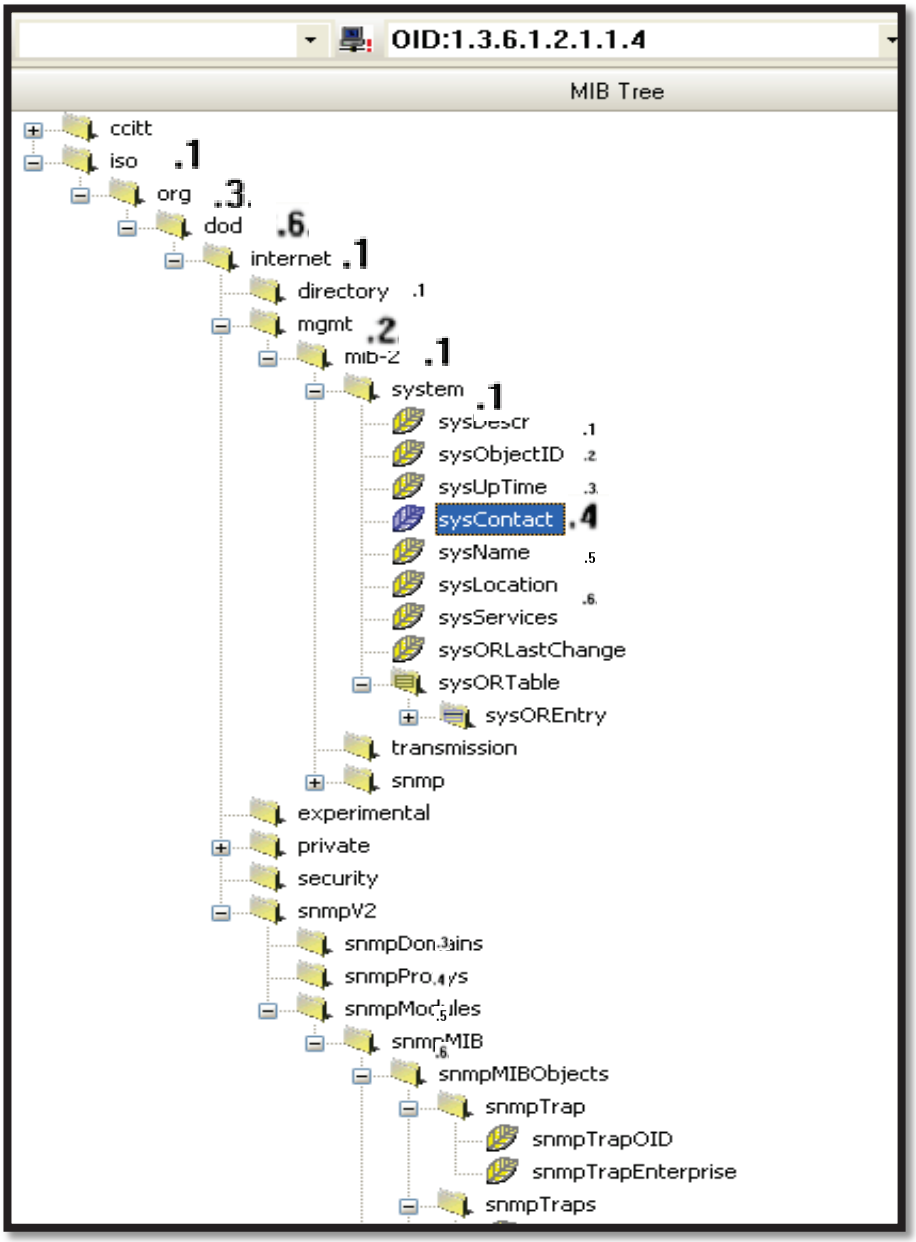


Figura 1-12.- Árbol MIB

Capítulo 2

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE PETROPRODUCCION.

2.1. INTRODUCCIÓN

El presente capítulo mostrará el estado actual de la red de comunicaciones, sus elementos y la forma como ésta se encuentra administrada. Para tal efecto se tomarán datos en base a diversas metodologías de recolección de información.

Petroproducción es la Empresa Estatal de Exploración y Producción de Petróleos del Ecuador, filial de PETROECUADOR. Fue creada el 26 de septiembre de 1989 con el objetivo de explorar, explotar las cuencas sedimentarias o yacimientos hidrocarburíferos y operar los campos hidrocarburíferos asignados a PETROECUADOR.

2.1.1. MISIÓN

Realizar la exploración y explotación de hidrocarburos de manera sustentable, en armonía con los recursos socio-ambientales, para contribuir al desarrollo económico y al progreso social del Ecuador.

2.1.2. VISIÓN

Mantener y proyectar su liderazgo en el país con talento humano competitivo, motivado y comprometido que cumpla estándares internacionales de gestión y se apoye en la tecnología de punta y en los recursos provenientes de la comercialización de hidrocarburos.

2.2. ANÁLISIS DE LA INFRAESTRUCTURA

Se describirá la infraestructura actual de la red hasta finales del mes de Enero del 2010. Aquí se emplea como base de recolección de información el método de comunicación, basado en encuestas oral y escrita al personal de la COORDINACIÓN TIC[8], de igual manera se emplea información digital para su actualización conjuntamente con la revisión física de las instalaciones de la red.

Se hará mención a la red empresarial con las siglas PPR, utilizado actualmente para identificar la intranet de PETROPRODUCCIÓN.

2.2.1. INSTALACIONES

La empresa estatal PETROPRODUCCIÓN dispone de dos instalaciones en la ciudad de Quito ubicados en el sector norte de la ciudad, sus operaciones son realizadas a lo largo de la región Amazónica del Ecuador (Distrito Amazónico D.A.[9]) en campos ubicados en las siguientes localidades: Lago Agrio, Sacha, Coca, Auca, Cuyabeno, Guarumo, Shushufindi y Libertador. Además cuenta con dos Centros de Investigación Geológica, uno en el sector de San Rafael-Quito y otro en la ciudad de Guayaquil.

Dentro de la estructura interna de la empresa la Coordinación TIC es la encargada de gestionar la infraestructura informática, tanto en redes de datos, conexiones de microondas, telefónicas, información administrativa y técnica. Además administra las aplicaciones que Petroproducción dispone, garantizando la comunicación entre sus dependencias y empleados.

La organización de esta coordinación se presenta en la siguiente tabla:

[8] Tecnologías de Información y Comunicaciones

[9] D.A. Distrito Amazónico, se refiere a los distintos campos ubicados en el Oriente ecuatoriano

ESTRUCTURA ACTUAL	*SIGLAS* [10]	DEPARTAMENTO ANTERIOR[11]
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (Q[12] – D.A.)	*TIC*	INGENIERÍA DE PROCESOS TÉCNICOS, SISTEMAS, TELECOMUNICACIONES
COORDINACIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (Q)	*CTI*	
COORDINACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES QUITO (Q)	*TIQ*	
COORDINACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES D.A. (D.A.)	*TID*	
SUPERVISIÓN DE APLICACIONES (D.A.)	*SUA*	
SUPERVISIÓN DE DATOS (D.A.)	*SDD*	
SUPERVISIÓN DE INFRAESTRUCTURA DE COMUNICACIONES (D.A.)	*SIC*	
SUPERVISIÓN DE SEGURIDAD TECNOLÓGICA (D.A.)	*SST*	
SUPERVISIÓN DE SOPORTE AL USUARIO (D.A.)	*SSU*	

Tabla 2-1.- Estructura Actual de la Coordinación TIC

2.2.1.1. Instalaciones Quito

Petroproducción funciona en dos edificios que generan el mayor volumen de información desde y hacia el Distrito Amazónico. El edificio Villafuerte (Av. 6 de Diciembre N34-290 y Gaspar Cañero) es la matriz de la empresa, aquí se ubica la Coordinación TIC. El segundo edificio es denominado Tribuna (Av. De Los Shyris N34-382 y Portugal), aquí funcionan departamentos del área operativa y la Vicepresidencia de la empresa. La comunicación entre los dos edificios y con las restantes dependencias se da mediante enlaces de microonda. Esta interconexión esta prevista cambiarla a Fibra Óptica en el transcurso del presente año.

[10] Son usadas para el reconocimiento del departamento en aspectos administrativos internos.
[11] Petroproducción realizó una reestructuración interna en la cual unificó los departamentos de sistemas, telecomunicaciones e ingeniería de procesos técnicos en una sola coordinación.
[12] Ciudad de Quito

2.2.1.2. Instalaciones Distrito Amazónico D.A.

En la región oriental del país, se cuenta con campamentos asentados en cada población descrita anteriormente donde se desarrollan distintas tareas administrativas y operativas, cabe indicar que también se ubican instalaciones para el hospedaje del personal que labora en esta región.
Las instalaciones en la ciudad de Lago Agrio son las más importantes y constituyen el centro de enlace con las demás instalaciones dentro de la Amazonía, de aquí su importancia, debido al gran volumen de información que por ella circula.

2.2.2. SERVIDORES

Mediante un proceso de observación dentro de los cuartos de equipos de la empresa, inquietudes realizadas al personal de TIC respecto a los dispositivos e información digital otorgada, se identifica los diversos servicios que corren en la red, al igual que los servidores ubicados dentro de sus instalaciones.

- Servidor de Correo Electrónico.- Servidores de plataforma Microsoft Exchange Server. Los usuarios pueden acceder a su correo desde la intranet o desde internet mediante la página web de la empresa.

- Servidor DNS y Directorio.- Posee la plataforma Windows mediante un servidor Active Directory en conjunto con un Servidor de Nombres de Dominio DNS.

- Servidor Web.- Para la página web de intranet así como para la web externa. En estos sitios se brinda varios servicios y aplicaciones a los usuarios.

- Servidor FTP.- Principalmente destinado a la transferencia de programas y software para el uso de las estaciones de trabajo de los empleados.

- Servidor Proxy y Firewall.- se hace uso del *proxy-firewall Astaro Security Gateway*. Maneja filtrado de contenidos y paquetes de acuerdo a políticas de seguridad establecidas.

- Servidor Antivirus.- servidores *Kaspersky,* uno en cada edificio, proveen protección a servidores, estaciones de trabajo y computadores ante amenazas de virus y spyware.

- Servidor AS/400.- encargado de manejar gran parte de la información empresarial (facturas, documentos, roles de pago, entre otros). Se tienen tres servidores en Quito y dos en el Distrito Amazónico (Lago-Agrio).

- Servidor de Base de Datos.- servidor Oracle Enterprise 9G para el almacenamiento de datos.

- Servidor IBM Lotus Domino.- servicio de correspondencia interna para el manejo y control de la documentación entrante y saliente. Se cuenta con el sistema *Lotus Domino Server.*

- Servidor Bizagi BPM[13].- destinado al manejo de facturas, pagos y órdenes de pago. Dispone de una aplicación web para acceder al servicio.

- Servidor Citrix.- Solución para llevar aplicaciones Windows a los escritorios.

- Servidor Blackberry.- *BlackBerry® Enterprise Solution* usada como plataforma inalámbrica ofrece acceso a correo electrónico, calendario, contactos, mensajería instantánea, servicios y aplicaciones empresariales basados en web, ampliando los beneficios a usuarios móviles. [14]

[13] BPM *Bussiness Process Manager.*- herramienta para el manejo y gestión de procesos administrativos y financieros.

[14] http://mx.blackberry.com/services/server/

- Servidor DB2 y Business Objects.- permite el control y gestión empresarial sobre índices de avances de proyectos, indicadores de gestión, eficiencia y rendimiento.

La Figura 2-1 muestra algunos servidores montados sobre racks dentro del cuarto de equipos del edificio Villafuerte.

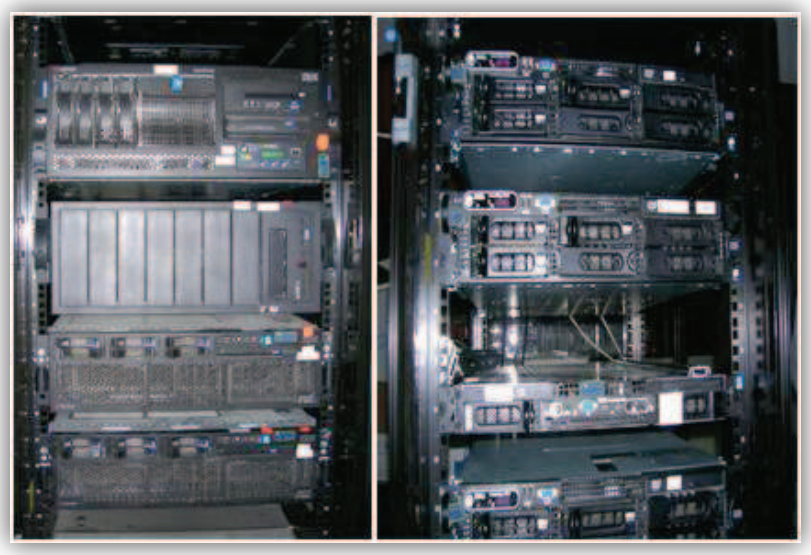


Figura 2-1.- Servidores en Cuarto de Equipos.

Las tablas: 2.2, 2.3 y 2.4 contienen un resumen de los distintos servidores de acuerdo a su ubicación física tanto para los edificios Villafuerte, Tribuna y el D.A. respectivamente.

SERVIDOR	HOSTNAME	SISTEMA OPERATIVO	DIRECCIÓN	CONSOLA - PUERTO	HARDWARE
RACK1					
BLADECENTER IBM MT-M / 8677-3X6	N.D. [15]	N.D.	172.16.x.x	N.D.	QC-28512 svr90022
Exchange Exchange.ppr.com	Exchange	Win2003S	172.16.x.x	BladeCeter Port:3 Pos:1	HS20 3.60GHZ Cuad Core, 2 GB
Active Directory y DNS	dc-vill01	Win2003S	172.16.x.x	BladeCeter Port:3 Pos:2	HS20 3.60GHZ Cuad Core, 2 GB
Web Interna Nueva Era www.ppr.com	Ppr	Red Hat E4	172.16.x.x	BladeCeter Port:3 Pos:3	JS21 2.2GHZ, 3GB
Kaspersky	Blade4hs21	Win2003S	172.16.x.x	BladeCeter Port:3 Pos:4	HS21 2.67 GHZ Dual Core, 1 GB
Bizagi BPM Base de Datos para desarrollo	Blade5hs21	Win2003S	172.16.x.x	BladeCeter Port:3 Pos:5	HS21 2.67 GHZ Dual Core, 1 GB
SMS	sms-vill01	Win2003S	172.16.x.x	BladeCeter Port:3 Pos:6	HS21 2.67 GHZ Dual Core, 1 GB
File Server	fs-vill01	Win2003S	172.16.x.x	BladeCeter Port:3 Pos:7	HS21 2.67 GHZ Dual Core, 1 GB
DataWareHouse y DB2	Srvdwh	RH E4 -	172.16.x.x	OPWarehouse Port:1	IBM eserver OpenPower S/N: 06-EF88F
Bussines Objects	Serverbo	Win2003S	172.16.x.x	Rack4 SERVERBO Port:7	IBM xSeries 366 3,16 GHZ Cuad Core 3 GB
Resolve IT Analyst (Soporte en Linea)	pprsvr366	Win2003S	172.16.x.x	ResolveIT Port:2	IBM xSeries 366 2 Procesadores de 3.16 GHZ Cuad Core
RACK2					
Consola de Administración del Servidor IBM System	Flujo de Facturación	IBM System x3550	172.16.x.x	N.D.	N.D.

[15] N.D. Información No Definida

Continúa en la página 41

SERVIDOR	HOSTNAME	SISTEMA OPERATIVO	DIRECCIÓN	CONSOLA - PUERTO	HARDWARE
p5	Bizagi				
AIX Linux 4 núcleos Power5		IBM System p5 6510 Express	N.D.	N.D.	N.D.
	Núcleo 1	Base de Datos de Producción	172.16.x.x	N.D.	N.D.
	Núcleo 2	Aplicaciones de Desarrollo (Bizagi)	172.16.x.x	N.D.	N.D.
	Núcleo 3	Aplicaciones de Producción desarrollo (Bizagi)	172.16.x.x	N.D.	N.D.
RACK3					
Aplicaciones Virtuales 1. WMware Capacity Planner x86 2. WMware Capacity Planner parisc		Win2003S	172.16.x.x	Ingreso por browser	DELL PowerEdge 2950
Astaro Security Gateway	Fwvill	Linux ASG V7.0	172.16.x.x	N.D.	DELL PowerEdge 1850
Servidor Citrix	N.D.	N.D.	172.16.x.x	N.D.	DELL PowerEdge 2950
Astaro Reporting Manager	N.D.	Win2003S y winXP	172.16.x.x	Astaro Repor Ma Port:4	WorkStation DELL PRECISION 690 3,0 GHZ Dual Core 4 GB
Servidor Lotus Notes	N.D.	Win2003S	172.16.x.x	Lotus	DELL PowerEdge 2950 CuadCore de 2,66 GHZ, 2GB
Servidor ONBASE	N.D.	Win2003S	172.16.x.x	SQLServer2005 Port:02	DELL PowerEdge 2950 CuadCore de 2,66 GHZ, 2GB
Trivoli Storage Manager (TSM Server) Controla la libreria LTO	N.D.	Win2003S	172.16.x.x	1TSM Port:01	IBM System x3650 DualCore de 3,0 GHZ, 1 GB
Web Externo	Webext	Red Hat E4	192.168.x.x/24	5WEBEX Port:05	IBM System x3550 3,60 GHZ Dual Core, 3 GB
WebMail Correo Web Access OWA	Webmail	Win2003S	172.16.x.x	6MAILEXT-7KASDA Port:07	IBM System X3550 3,73 GHZ Cuad Core, 3 GB

Continúa en la página 42

SERVIDOR	HOSTNAME	SISTEMA OPERATIVO	DIRECCIÓN	CONSOLA - PUERTO	HARDWARE
Control de Acceso de Personal por Sistema Biométrico	N.D.	Win2003S SQL Server 2000	172.16.x.x	Bizagi	DELL PowerEdge 2950, CuadCore de 2,66 GHZ
RACK4					
Microsoft Learning SQL, COMPERS	Pprsrvhp370	Win2003S	172.16.x.x	REVIT-SAVCE	HP ProLlant ML370
CALL MANAGER Y DHCP	SERVERCCM	Win2003S	172.16.x.x	CALLMANAGER Port:5	CISCO MCS 7800
WEB Interna RRHH	ftp	Red Hat E4	172.16.x.x	INTRANET WEB Port:4	IBM xseries 235 3 Procesadores 3,0 GHZ 3 GB
Lotus Domino Mail FUERA SERVICIO	Mail	Red Hat E4	172.16.x.x	N.D.	IBM eserver xseries 240
AS/400 PPRQ3A	pprq3a		172.16.x.x	N.D.	IBM e-server
PC VPN para router R.A.S	Router R.A.S	Red Hat E4	172.16.x.x	N.D.	COMPAQ DESKPRO
Server Blackberry	N.D.	N.D.	172.16.x.x	N.D.	DELL Optiplex GX280

Tabla 2-2.- Servidores Ubicados en el edificio Villafuerte

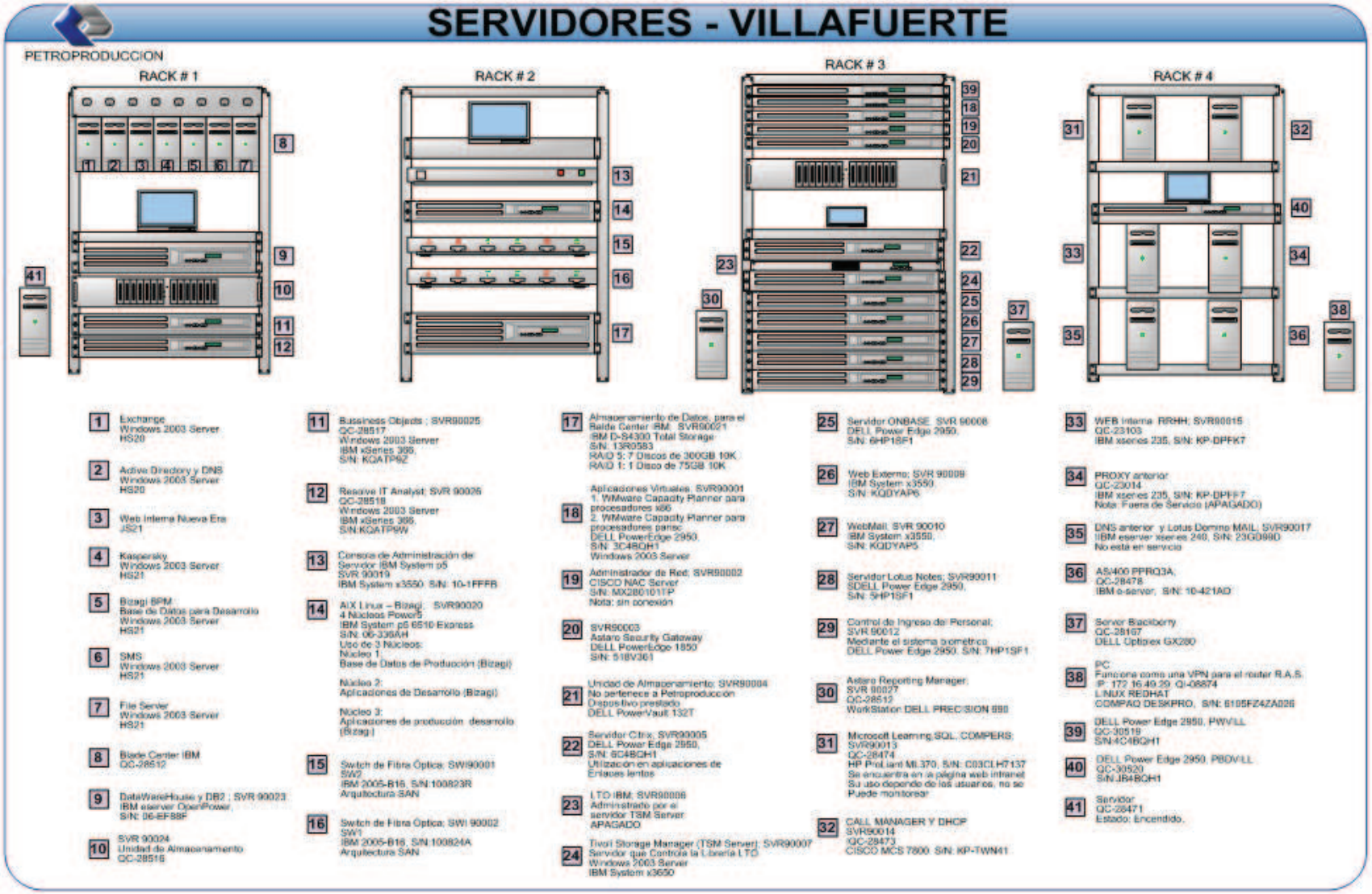


Figura 2-2.- Rack de servidores, Edificio Villafuerte.

SERVIDOR	HARDWARE	SISTEMA OPERATIVO	DIRECCION IP	COD.	OBSERVACIONES CAPACIDAD - PUERTO
PISO 2					
Almacenamiento de Datos	ONIX 3200		N.D.	Sin QC	Cable Fibra 10 discos, 146.8 Gb 10K
SUN microsystems	SUN microsystems T1000	UNIX	N.D.	QC-24419, QC-24418, QC-24417	Cable Fibra
SUN microsystems	SUN microsystems X4450	UNIX	N.D.	Sin QC	Cable Fibra
PISO 7					
Sistema de Reporte Mensual de Producción	DELL PowerEdge 2600	Win2003S	N.D.	QC-21681	SVR90043
AVOCET (Ambiente de Prueba)	IBM System X3650	RH E4	172.16.x.x	QC-29399 SVR90045	No está conectado a un storage
File de pozos	DELL PRECISION 360	N.D.	N.D.	QC-21628 SVR90044	Funciona como una workstation
PISO 12					
Servidor de LOTUS	DELL PowerEdge 2950	Win2003S	172.16.x.x	QC-29975 SVR90048	3 Discos, 300GB 10K 2 Seriales, 2 Gigabit, 2 USB
Servidor de Antivirus	DELL PRECISION 690	Win2003S	172.16.x.x	QC-29970 SVR90050	Cuad Core 3,20 GHZ, 4 GB

Continúa en la página 45.

SERVIDOR	HARDWARE	SISTEMA OPERATIVO	DIRECCION IP	COD.	OBSERVACIONES CAPACIDAD - PUERTO
Correo Electrónico	IBM System x3650	Win2003S	172.16.x.x	Sin QC SVR90048	2 Procesadores Cuad Core 3,20 GHZ 3 Discos, 300GB 10K
PISO 13					
Aplicación de información Legal y Update de Windows Generacion de Inventarios	DELL PRECISION 690	N.D.	172.16.x.x	QC-29186	Cuad Core de 3,20 GHZ 4 GB
PISO 14					
Componentes adicionales de Lotus	IBM System 3650	N.D.	172.16.x.x	Sin QC SVR90052	2 Discos, 300GB CuadCore 2,66GHz, 2GB
BLADE CENTER H	IBM	Win2003S y Win2008S		SVR90055	Ocupados: 3 slots

Tabla 2-3.- Servidores edificio Tribuna

MODELO	CAPACIDAD	DIRECCION IP	MEDIO ENLACE-BACKBONE	OBSERVACIONES
IBM System 3650	3.20GHZ, 3 GB	172.16.x.x	Active Directory, DNS, Correo	N.D.
IBM System x3550	3.72GHZ, 3 GB	172.16.x.x	Antivirus Kaspersky	Servidor primario de antivirus. Workstation.
HP XEON 5355	2.67GHZ, 2 GB	172.16.x.x	Antivirus Kaspersky	Administración de proyectos.
HP XEON 5355	2.67GHZ, 2 GB	172.16.x.x	Microsoft Project server SQLServer 2005 Visual Studio 2005 Apache Server 2.2	Administración de proyectos - Web Access
HP XEON E5420	2.50 GHZ. 2 GB	172.16.x.x	Integra: Lotus Notes, Bizagi, aplicación de facturación	Aplicación para enlaces lentos, ingresa a las aplicaciones Lotus Notes, Bizagi, aplicación de facturación
DELL PRECISION 650	2.80 GHZ, 2 GB	172.16.x.x	IIS, NetMeeting	N.D.
DELL Optiplex 170L	3.19 GHZ, 2 GB	172.16.x.x	Symantec Anti-virus	Workstation

Tabla 2-4.- Servidores Lago Agrio

EQUIPO	DIRECCIÓN IP	HOSTNAME	PUERTOS	DESCRIPCIÓN
RACK2				
Switch Fibra Óptica IBM 2005-B16	192.168.0.x	SW2	10X : Fibra	SWI90001, Arquitectura SAN
Switch Fibra Óptica IBM 2005-B16	192.168.0.x	SW1	10X : Fibra	SWI90002, ArquitecturaSAN
RACK5				
Router Cisco2600	172.16.x.x	N.D	8X: 100Base-T	ROU90002
Switch 3COM	DHCP	N.D.	8X :100Base-T	Switch para Pruebas
Switch CISCO Catalyst 2950	172.16.x.x	sissw02	48X: 10/100Base-T	SWI90004
Switch CISCO Catalyst 2950	172.16.x.x	sissw03	48X 10/100Base-T	SWI90005
Switch CISCO Catalyst 2950	172.16.x.x	sissw01	48X :100/1000Base-T	Conexión con switch de core
Switch CISCO Catalyst 2960G	172.16.x.x	N.D.	48X : 100/1000Base-T	N.D.
RACK6				
Switch CISCO Catalyst 2900XL	N.D.	N.D.	24X :100Base-T	SWI90008
Switch CISCO Catalyst 2950	172.16.x.x	Sissw04	24X :100Base-T	SWI90009
Switch CISCO Catalyst 2950	172.16.x.x	Sissw19	24X :100Base-T	SWI90010
Switch CISCO Catalyst 2950	172.16.x.x	Sissw17	24X :100Base-T	SWI90011
Switch CISCO Catalyst 2950	172.16.x.x	Sissw25	24X :100Base-T	SWI90012
Switch CISCO Catalyst 2950	N.D.	SWQ006	24X :100Base-T	SWI90013, Switch DMZ

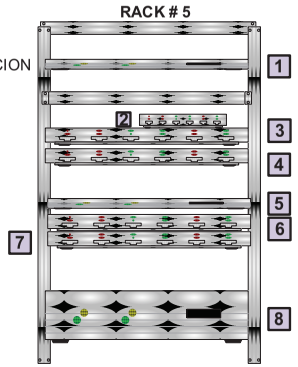
Continúa en la página 48.

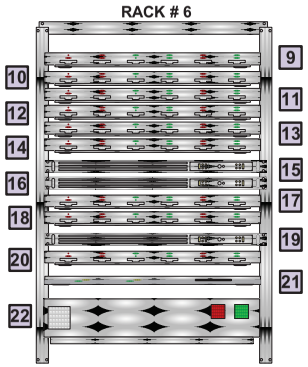
EQUIPO	DIRECCIÓN IP	HOSTNAME	PUERTOS	DESCRIPCIÓN
Switch 3COM X506	N.D.	N.D.	6X – FE/LAN-WAN	
Switch 3COM X506	N.D.	N.D.	6X – FE/LAN-WAN	SWI90006
Router CISCO 2800	N.D.	N.D.	2x - GE, 6x Seriales, 1x-FE	ROU90003 Telconet-Petroproducción
Switch CISCO Catalyst 4000	172.16.x.x	SW_Catalyst4000	124x - GE	SWI90018, Switch Capa 3
RACK7				
Switch CISCO Catalyst 2900XL	N.D.	N.D.	24X :100Base-T	SWI90018
Switch CISCO Catalyst 2950	N.D.	N.D.	24X :100Base-T	SWI90019
Switch CISCO Catalyst 2900XL	N.D.	N.D.	24X :100Base-T	SWI90020
Switch CISCO Catalyst 2900XL	N.D.	N.D.	24X :100Base-T	SWI90021
Switch CISCO Catalyst 2950	N.D.	N.D.	24X :100Base-T	SWI90022
Switch 3COM	N.D.	N.D.	24X :100Base-T	N.D.

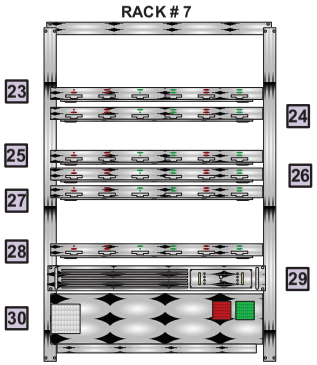
Tabla 2-5.- Equipo Activo en Cuarto de Equipos Villafuerte

SWITCHES Y ROUTERS - VILLAFUERTE

PETROPRODUCCION







1 Router R.A.S.; ROU90002
QC-28520
Cisco 2600, S/N: JMX0722L40N
8 Puertos FastEthernet
Cable UTP Categoría 6
Trabaja con el servidor Compaq Deskpro

2 QC-28522
3COM, S/N: 0200/2KG4Y0020146
8 Puertos FastEthernet
Cable UTP categoría 5
Switch para pruebas

3 Switch; SWI90004
QC-28521
CISCO Catalyst 2950
S/N: FOC1015Z2DA
Cascada con el Switch Catalyst 2950
IP: 172.16.X.X

4 Switch; SWI90005
QC-28523
CISCO Catalyst 2950
S/N: FOC1015Z2R3
Cascada con el Switch Catalyst
2950 IP: 172.16.X.X

5 ODF
Enlace de F.O 12 hilos
PETROECUADOR BACKBONE
La Paz – 6 de Dic. y Alpallana.

6 Switch SWI90007
QC-28524
CISCO Catalyst 2950
S/N: FOC1015Z2RJ
Conectado al Switch Catalyst
4507 "Core"

7 Switch; sissw01
Con: ---- Port: --
CISCO Catalyst 2960 G
48 Puertos:27 RJ45,
6 Telefono, 6 AP, 2 Giga
Cable UTP Categoría 6

8 Sin IP, QC-28527
NetEnfacer AC-202
S/N: 995698
FUERA DE SERVICIO

9 Swich SWI90008
CISCO Catalyst 2900XL
S/N:FAB0444N1EU
24 Puertos FastEthernet
Cable UTP categoría 5
Conectado al Switch Catalyst
4507 "Core"

10 Switch SWI90009
CISCO Catalyst 2950
S/N: FOC0751W2X2
Cable UTP categoría 5
24 Puertos FastEthernet
Conectado al Switch Catalyst
4507 "Core"

11 Switch SWI90010
CISCO Catalyst 2950
S/N: FOC0751X2H8
Cable UTP categoría 5
24 Puertos FastEtherne
Conectado al Switch Catalyst
4507 "Core"

12 Switch SWI90011
CISCO Catalyst 2950
S/N: FOC0751W2X
Cable UTP categoría 5
24 Puertos FastEthernet
Conectado al Switch Catalyst
4507 "Core"

13 Switch SWI90012
CISCO Catalyst 2950
S/N:FWK0719Y1A9
Cable UTP categoría 5
24 Puertos FastEtherne
Conectado al Switch Catalyst
4507 "Core"

14 Switch SWI90013
Switch DMZ
CISCO Catalyst 2950
S/N: FWK0719Y1AP
Cable UTP categoría 6
24 Puertos FastEthernet
Enlazado con el Firewall y
con el servidor web externo

15 Sin IP
QC30594
6 puertos FastEthernet/LAN-WAN
3COM X506

16 Switch SWI90006
QC30595
6 puertos FastEthernet /LAN-WAN
3COM X506

17 Conexión de Fibra
QC30594

18 Conexión de Fibra
QC30594

19 Sistema de Alimentación
APC Surge Arrest Network

20 CISCO Catalyst 2960G
S/N: FOC1224X7SJ
48 Puertos FatEthernet
2 Puertos GigabitEthernet

21 Router ROU90003
Cisco 2600
Enlace de Fibra de Telconet -
Petroproducción

22 CISCO Catalyst 4507R
Cable UTP Categoría 5 y 6
Switch Capa 3

23 Switch SWI90018
CISCO Catalyst 2900XL,
S/N: FAB0602Y2PU
24 Puertos FastEthernet
Cable UTP categoría 5

24 Switch SWI90019
QC-20350
CISCO Catalyst 2950
S/N: F0C0752Y279
Cable UTP categoría 5
24 Puertos FastEthernet

25 Switch SWI90020
CISCO Catalyst 2900XL,
S/N: FAB0602Y2P2
24 Puertos FastEthernet
Cable UTP categoría 5
Conectado al Switch Catalyst
4507 "Core"

26 Switch SWI90021
CISCO Catalyst 2900XL, S/N: FAB0502U4AP
24 Puertos FastEthernet
Deshabilitado por mal funcionamiento

27 Switch SWI90022
CISCO Catalyst 2950M, S/N: FHK0720W0W0
24 Puertos FastEthernet
Cable UTP categoría 5
Conectado al Switch Catalyst 4507 "Core"

28 Switch SWI90022
3COM,
S/N: CA/9URC90L9F0A61
24 Puertos FastEthernet
Cable UTP categoría 5
Conectado al Switch Catalyst 4507 "Core"

29 Sistema de Alimentación
APC Surge Arrest Network

30 Switch SWI90024
IBM W93/8274
S/N: 2313037
Cable UTP Categoría 6
Conectado al Switch Catalyst
4507 "Core"
Switch Capa 3 antiguo

Figura 2-3.- Distribución de los Equipos de interconexión, Edificio Villafuerte.

PISO	MODELO	DIRECCIÓN IP	PUERTOS	MEDIO	CONEXIÓN
MZ	CISCO Catalyst 2950	172.16.x.x	48X :100Base-T	UTP CAT6	Cascada con el Switch Catalyst 2950 IP: 172.16.48.x
MZ	CISCO Catalyst 2950	172.16.x.x	48X :100Base-T	UTP CAT6	Enlazada con el Piso 1 del Edificio Villafuerte
1	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T, 2X:1Gbps	UTP CAT6	Catalyst 4507 "Core"
2	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T, 2X:1Gbps	UTP CAT6	Catalyst 4507 "Core"
	3COM	N.D.	24X: 48X :100Base-T	UTP CAT5	Cascada con el switch Catalyst 2960G 48.x
3	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T 2X:1Gbps	UTP CAT6	Cascada con el switch Catalyst 2960G 48.x
4	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T 2X:1Gbps	UTP CAT6	Cascada con el switch Catalyst 2960G 48.x
5	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T 2X:1Gbps	UTP CAT6	Cascada con el switch Catalyst 2960G 48.x
6	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T 2X:1Gbps	UTP CAT6	Cascada con el switch Catalyst 2960G 48.x
7	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T 2X:1Gbps	UTP CAT6	Cascada con el switch Catalyst 2960G 48.x
8	CISCO Catalyst 2960G	172.16.x.x	48X : 100Base-T 2X:1Gbps	UTP CAT6	Cascada con el switch Catalyst 2960G 48.x
9	3COM	N.D.	24X :100Base-T	UTP CAT6	Catalyst 4507 "Core"
10	CISCO Catalyst 2950	172.16.x.x	48X :100Base-T	UTP CAT6	Cascada con el Switch Nortel ubicado en el mismo piso

Tabla 2-6.- Equipo Activo Edificio Villafuerte

PISO	MODELO	DIRECCIÓN IP	PUERTOS	MEDIO	CONEXIÓN
PB	3COM	N.D.	24X:100Base-T	UTP CAT6	Enlace con el primer piso
1	CISCO Catalyst 2960G	N.D.	48X:100Base-T 2X:1Gbps 4 Puertos de Fibra	UTP CAT6	Enlace con el Séptimo Piso
2	CISCO Catalyst 2960G	N.D.	48X:100Base-T 4X:1Gbps 4 Puertos de Fibra	UTP CAT6	N.D.
	SILKWORM 200E	N.D.	15X : 100Base-T	Cable de Fibra	N.D.
	3COM	N.D.	48X : 100Base-T	UTP CAT6	N.D.
3	CISCO LINKSYS	N.D.	8X : 100Base-T	UTP CAT6	Enlace con el doceavo piso
	3COM	N.D.	8X : 100Base-T	UTP CAT6	Enlace con el doceavo piso
6	3COM	N.D.	8X : 100Base-T	UTP CAT6	
7	INTEL Express 460T	N.D.	24X : 100Base-T	UTP CAT5	Cascada con switch 03 Catalyst 2950
	INTEL Express 460T	N.D.	24X : 100Base-T	UTP CAT5	Cascada con switch 03 Catalyst 2950
	INTEL Express 460T	N.D.	24X : 100Base-T	UTP CAT5	Cascada con switch 03 Catalyst 2950
	INTEL Express 460T	N.D.	24X : 100Base-T	UTP CAT5	Cascada con switch 04 Catalyst 2950
	CISCO Catalyst 2950	N.D.	12X : 100Base-TX	UTP CAT5	Cascada con el Switch 03 Catalyst 2950
	CISCO Catalyst 2950	N.D.	24X : 100Base-T	UTP CAT5	Décimo Piso y Cascada con el Switch 03 Catalyst 2950
	CISCO Catalyst 2950	N.D.	24X : 100Base-T	UTP CAT5	Onceavo Piso y Cascada con el Switch 03 Catalyst 2950
	CISCO Catalyst 2950	N.D.	24X : 100Base-T	UTP CAT5	Doceavo Piso y Cascada con CISCO

Continúa en la página 52.

PISO	MODELO	DIRECCIÓN IP	PUERTOS	MEDIO	CONEXIÓN
					Catalyst 12X:100Base-T
	CISCO Catalyst 2950	N.D.	24X : 100Base-T	UTP CAT5	Doceavo Piso y Cascada con el Switch 03 Catalyst 2950
	CISCO Catalyst 2950	N.D.	12X : 100Base-TX	UTP CAT5	N.D.
	3COM	N.D.	24X:100Base-T 2X:1Gbps	F.O.	Sexto piso y cascacada con Switch 2
	3COM	N.D.	24X:100Base-T 2X:1Gbps	F.O.	Sexto piso y cascacada con Switch 2, 3 y 4.
	3COM	N.D.	24X:100Base-T 2X:1Gbps	F.O.	Cascada con segundo piso
	3COM	N.D.	24X:100Base-T 2X:1Gbps	F.O.	cascada con Switch 2 y 3
12	**Rack1**				
	CISCO Catalyst 2950	N.D.	48X:100Base-T 2X:1Gbps	UTP CAT6	N.D.
	CISCO Catalyst 2950	N.D.	48X:100Base-T 2X:1Gbps	UTP CAT6	N.D.
	SW. CISCO 1800	190.95.245.x	8X: 100Base-T	UTP CAT6	EQUIPO DE TELCONET
	ROUTER CISCO 2600	172.16.49.x	2X: Seriales 2X: 1000Base-T	Serial UTP CAT6	N.D.
14	IBM 2005B16	N.D.	24X: 100BaseT	Cable- FO	FO
	IBM 2005B16	N.D.	24X: 100BaseT	Cable-FO	FO
	CISCO Catalyst 3560G	N.D.	48X: 100BaseT	UTP CAT5	Enlace con Router Full Data
	3COM	N.D.	8X: 100BaseT	UTP CAT5	Conectado a la SAN
	CISCO Catalyst 2950	N.D.	24X: 100Base-Tx	UTP CAT6	N.D.

Tabla 2-7.- Equipo Activo Edificio Tribuna

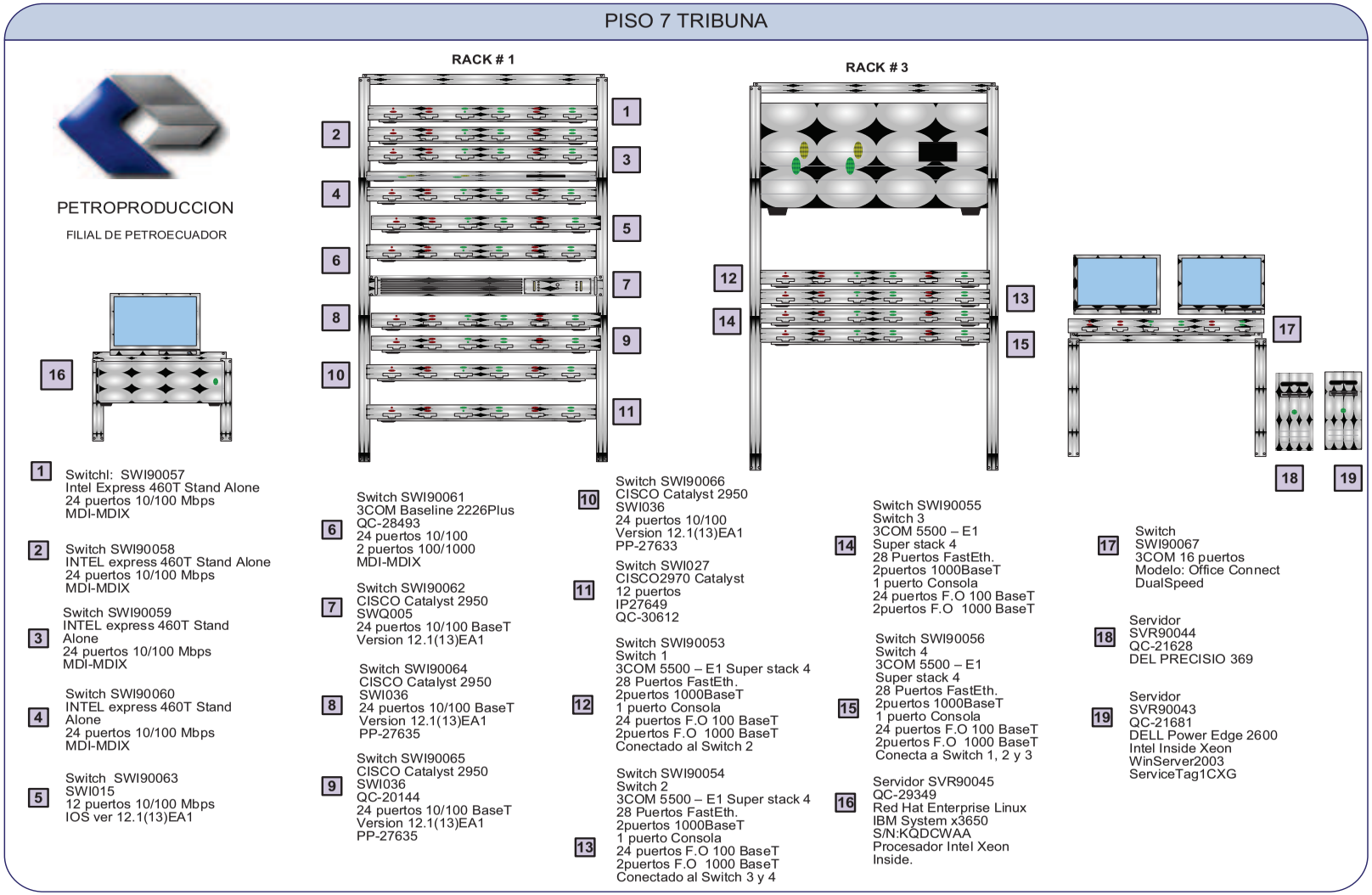


Figura 2-4.- Cuarto de Equipos – Piso 7 Edificio Tribuna

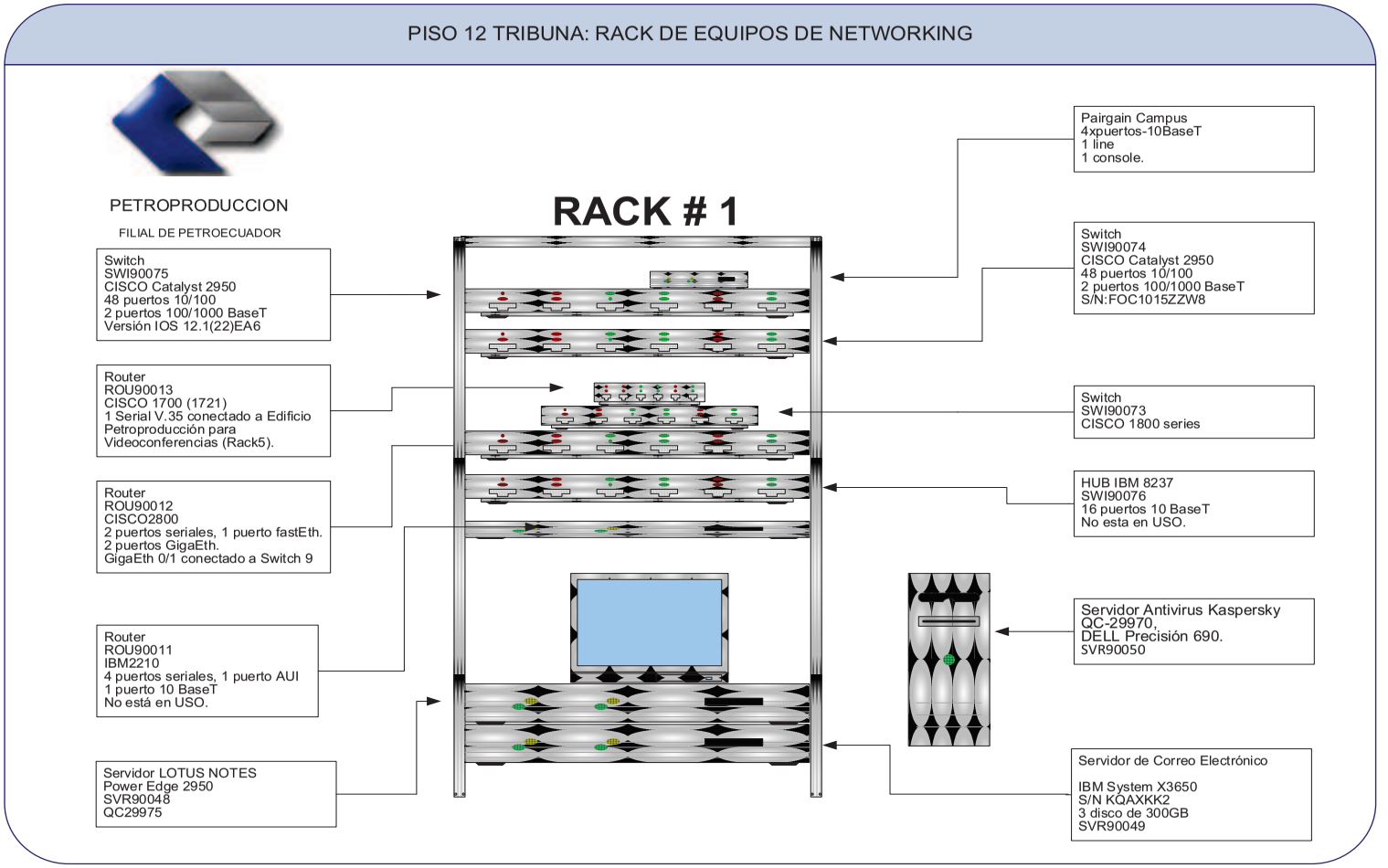


Figura 2-5.- Cuarto de Equipos Piso 12 – Edificio Tribuna[16]

[16] Se presenta solo el rack usado para los dispositivos de Networking, la demás infraestructura del cuarto de equipos corresponde a dispositivos de Telefonía Analógica

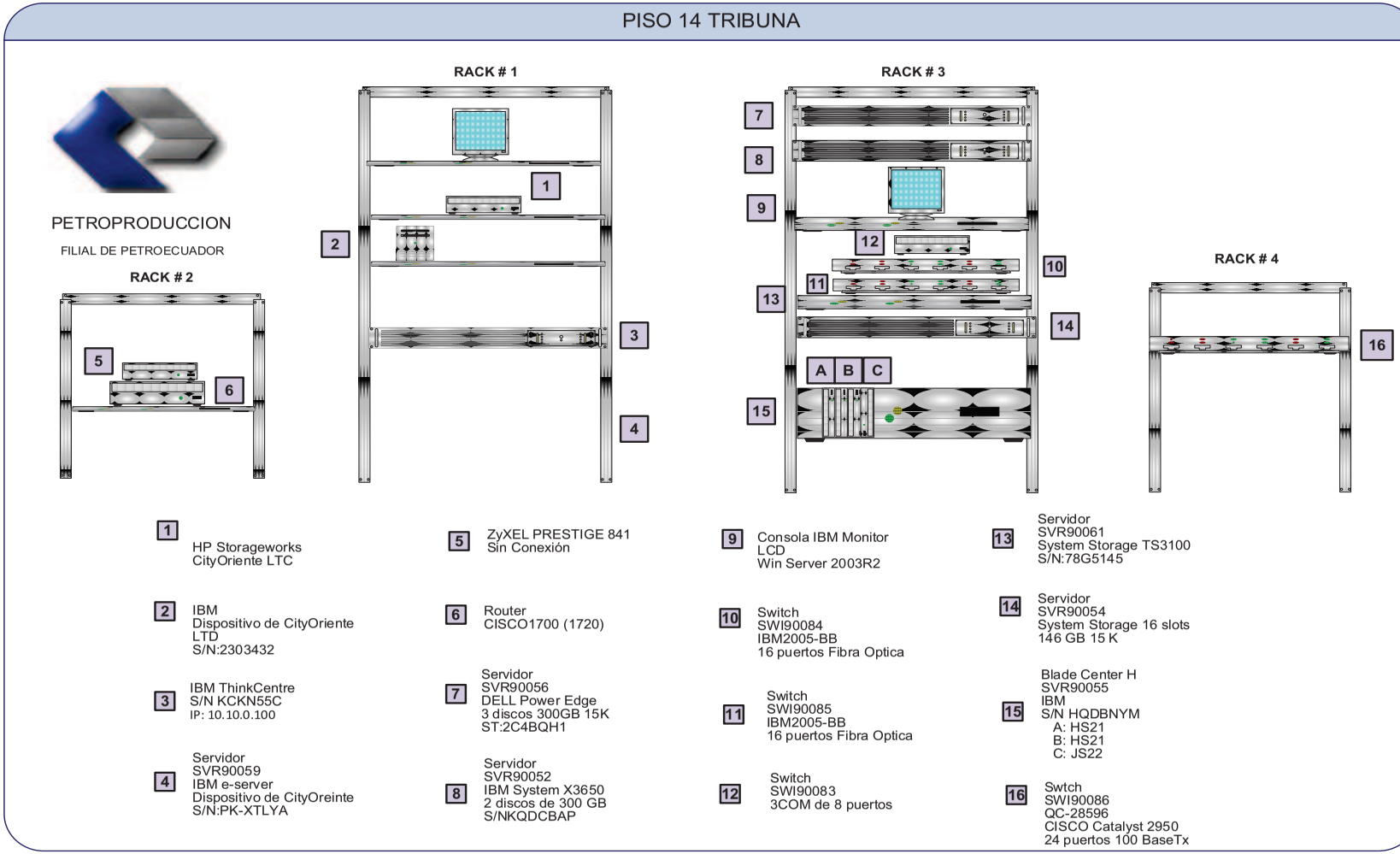


Figura 2-6.- Cuarto Equipos Piso 14 – Edificio Tribuna

2.2.3. EQUIPOS DE INTERCONECTIVIDAD

Se dispone de un Switch Cisco Catalyst 4507 como núcleo, switches de distribución Cisco Catalyst de la familia 2900 a velocidades de 100 - 1000 Mbps y switches de acceso (2950 y 2960G Cisco Catalyst) distribuidos en cada piso. Además existen varios Puntos de Acceso Cisco Aironet 1200 conectados a switches de acceso que brindan comunicación inalámbrica a determinados departamentos según las necesidades que estos presenten.

Los principales dispositivos se ubican en cuartos de equipos ubicados en áreas de la Coordinación TIC, son montables sobre racks y disponen de un sistema de aire acondicionado para regular la temperatura. Su distribución se presenta en los diagramas anteriores junto con sus principales características.

2.2.4. DIRECCIONAMIENTO IP

Debido a su gran extensión, Petroproducción hace uso de una red privada clase B para direccionar sus departamentos, estaciones de trabajo, servidores y equipos activos. La red utilizada es la 172.16.0.0 /16, de la cual se derivan diferentes subredes para separar sus dependencias. Cada subred abastece a una sucursal de la empresa empleando hasta dos subredes en determinadas instalaciones dependiendo del número de equipos existentes.

Para los enlaces entre sucursales se emplea una red privada clase C 192.168.X.X/24 dividida en subredes con máscara /30 para asignar únicamente una dirección lógica a cada interfaz de router extremo.

Los equipos del personal de la empresa disponen de una dirección estática dentro de su subred, otorgada por la Coordinación TIC. Existe a la vez un servidor DHCP principalmente destinado a usuarios temporales de la red como visitantes y personal de empresas privadas que realizan trabajos en las instalaciones, el ámbito DHCP destinado para tal efecto otorga direcciones en el rango 172.16.53.x

2.2.5. TOPOLOGÍA DE LA RED

La red cuenta con una topología tipo Estrella siendo su principal nodo el edificio Villafuerte en Quito, se tiene un switch de núcleo Catalyst 4507 y un proxy-firewall Astaro Gateway, además la granja de servidores se enlaza al núcleo para formar la capa jerárquica superior. Para los niveles de Distribución y Acceso se utilizan Switches descritos en la Tabla 2-5, Tabla 2-6 y Tabla 2-7, formando así una red de datos jerárquica. En la Figura 2-8 se puede apreciar el diagrama de red actual de Petroproducción.[17]

2.2.6. ENLACES INTERNOS

Para la comunicación dentro de la ciudad de Quito se dispone de enlaces de Fibra Óptica que comunica a Petroproducción – Petroecuador – Lago Agrio recientemente implementado, sin embargo existe una ruta alterna de microonda con el cerro Pichincha desde y hacia los edificios Villafuerte, Tribuna y el Distrito Amazónico identificados en la siguiente Figura:

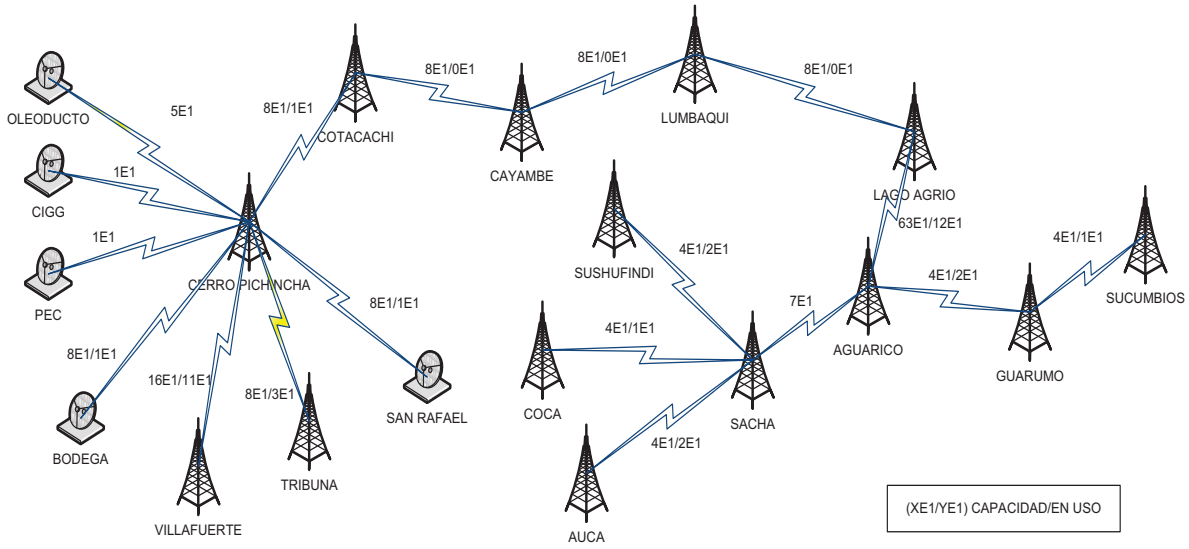


Figura 2-7.- Enlaces Microonda

[17] Coordinación de Tecnologías de Información Quito - PETROPRODUCCIÓN, modificación del original Autor: Emilio Bolaños

La siguiente tabla muestra las capacidades de los distintos enlaces de microonda entre las dependencias de Petroproducción.

Enlace	Capacidad
CP[18] - Villafuerte	16 E1
CP - Tribuna	8 E1
CP - San Rafael	8 E1
CP - Guayaquil	1 E1
CP – Oleoducto	5 E1
CP - PEC	1 E1
Villafuerte - L.A.	1 E1[19]
L.A. - Aguarico	12 E1
Aguarico - Guarumo	4 E1
Aguarico - Sacha	7 E1
Sacha - Sushufindi	4 E1
Sacha - Coca	4 E1
Sacha - Auca	4 E1

Tabla 2-8.- Enlaces Microonda

[18] Cerro Pichincha
[19] Real Usada

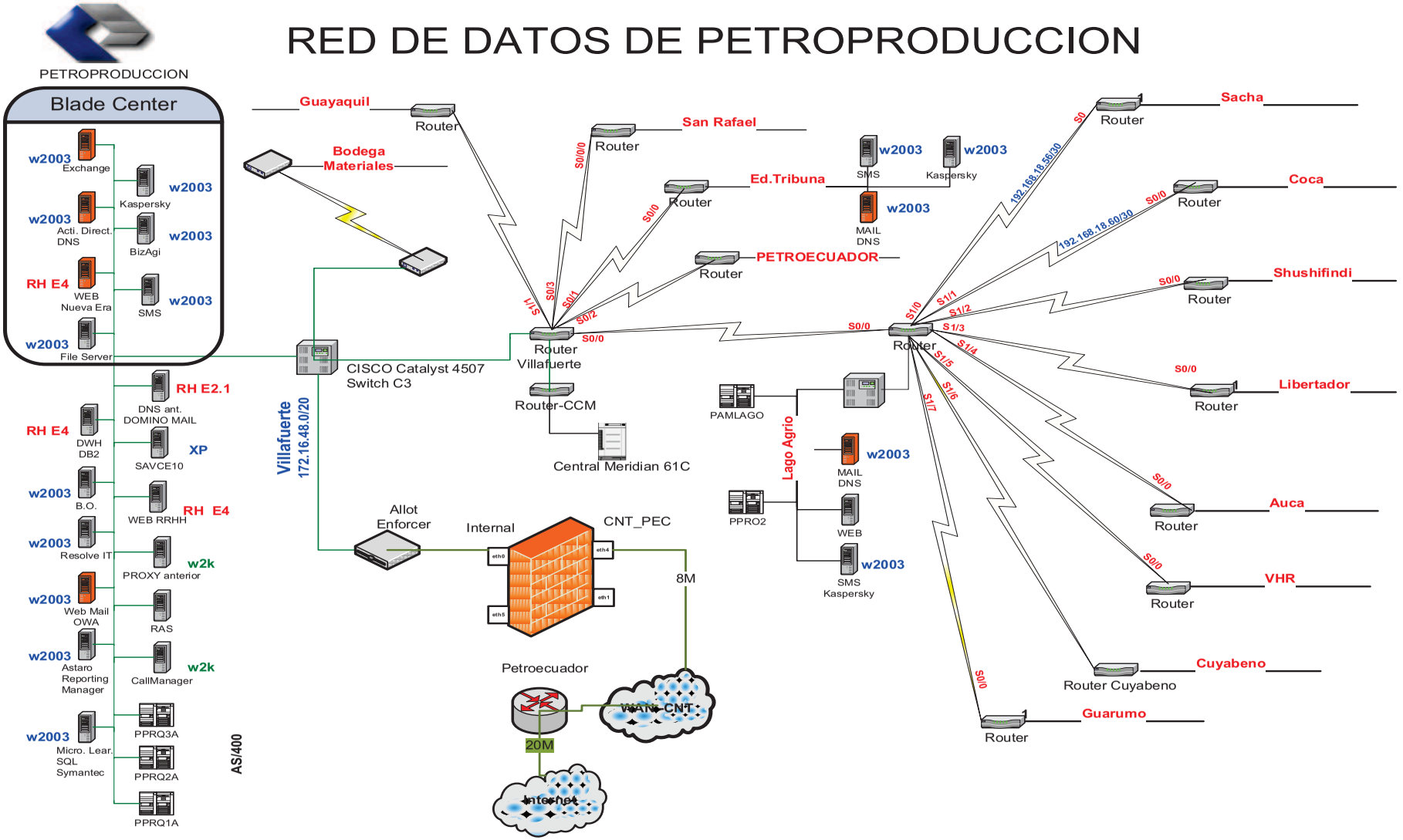


Figura 2-8.- Diagrama de la Red Actual de Petroproducción

2.3. ANÁLISIS DE LA RED PASIVA

2.3.1. CABLEADO HORIZONTAL

El edificio Villafuerte cuenta con 12 pisos, mientras que el edificio Tribuna posee 14 pisos, es el único que cuenta además de un cableado UTP de cobre con un cableado de fibra óptica multimodo para los departamentos de la Subgerencia de Exploración y Desarrollo. El cableado es de tipo par trenzado de cobre categoría 6 y 5e, se ha implementado UTP CAT6 sobre todo en el backbone, y en la conexión de servidores.

Figura 2-9.- Rack de Fibra Óptica

Cada punto de red es de salida doble, una del tipo RJ-45 y otra salida para voz analógica. Los racks ubicados en cada piso disponen de Patch Panels independientes para voz y datos respectivamente etiquetados al igual que las salidas en cada estación de trabajo. Todas las instalaciones poseen cielo raso, por donde el cableado es transportado.

La Tabla 2-10, resume el número de racks instalados en la red, la categoría de cableado estructurado y sus dimensiones.

2.3.2. CABLEADO VERTICAL

Consiste en tendidos de cable UTP CAT6 desde el cuarto de equipos hasta los racks de distribución instalados en cada planta. Su desplazamiento se lo realiza por ductos del edificio destinados para tal efecto.

INSTALACIONES	CATEGORIA MARCA	# DE RACKS INSTALADOS/TAMAÑO
EDIF. VILLAFUERTE	CAT. 6 R&M	12/1,20m + 7 Rack de2,10
EDIF. LA TRIBUNA	CAT 5E	4/1,20m + 5/2,10ab.+ 1/ab.
SAN RAFAEL	CAT 5E	1/1,20m
GUAYAQUIL	CAT 5E	1/84"
LAGO AGRIO	CAT 5E	5 Rack de 2,10 m

Tabla 2-9.- Racks Instalados

2.3.3. DISTRIBUCIÓN DE CUARTO DE EQUIPOS

El Cuarto de equipos principal se encuentra en planta baja del edificio Villafuerte, aquí se encuentran los servidores descritos anteriormente en la Tabla 2-2 y Tabla 2-5. Éste es el punto donde los switches de acceso se interconectan al backbone de la empresa. Mientras que en el Edificio Tribuna se cuenta con tres cuartos de equipos, ubicados en el séptimo, doceavo y catorceavo piso.

Los equipos se encuentran montados sobre racks estándares de diecinueve pulgadas numerados. Los cuartos son administrados por la Coordinación TIC, encargado de prestar sus servicios ante alguna circunstancia o problema que requiera de pronta solución.

2.4. ADMINISTRACIÓN DE LA RED

2.4.1. SEGURIDAD FÍSICA

La empresa maneja políticas básicas de seguridad, gestionadas por el personal de vigilancia en el ingreso y salida de equipos, y por los administradores de las distintas áreas de TIC, encargados del correcto manejo y funcionamiento de equipos y servicios de red, así como de la información que por ella circula.

En base a las obligaciones asignadas a cada integrante de TIC, se establece la responsabilidad de brindar seguridad en el manejo de los dispositivos de la empresa, las cuentas de usuario, contraseñas, bases de datos, respaldos de información y demás aplicaciones que corren en la red, garantizando la confidencialidad de datos y la integridad de los mismos.

Los dispositivos de seguridad manejados son:

2.4.1.1. Proxy-Firewall Astaro Security Gateway

Dispositivo proxy y firewall, provee protección ante una serie de amenazas de internet incluyendo gusanos, troyanos o manipulación de aplicaciones. Además un filtrado del tráfico de correo electrónico y previene la intercepción no autorizada del mismo, filtra todo el tráfico desde y hacia Internet, controla el acceso de los usuarios a Internet, el uso de aplicaciones de mensajería instantánea y P2P[20]. Todo esto a través de una administración vía web.

La empresa dispone de la versión V7 release 7.501 siendo esta actualizada mediante el servicio Up2Date de Astaro Security. Todos los resultados son presentados en forma de reportes y enviados al correo electrónico del personal de TIC a cargo. Los parámetros de configuración son amplios, y abarcan: Administración, Manejo de Usuarios, Servicios de Red, Seguridad de Red,

[20] Point to Point.- transferencia de archivos entre usuarios de una red

Web, Mail y VoIP, además manejo de Acceso Remoto, VPN, Logging y Reportes.

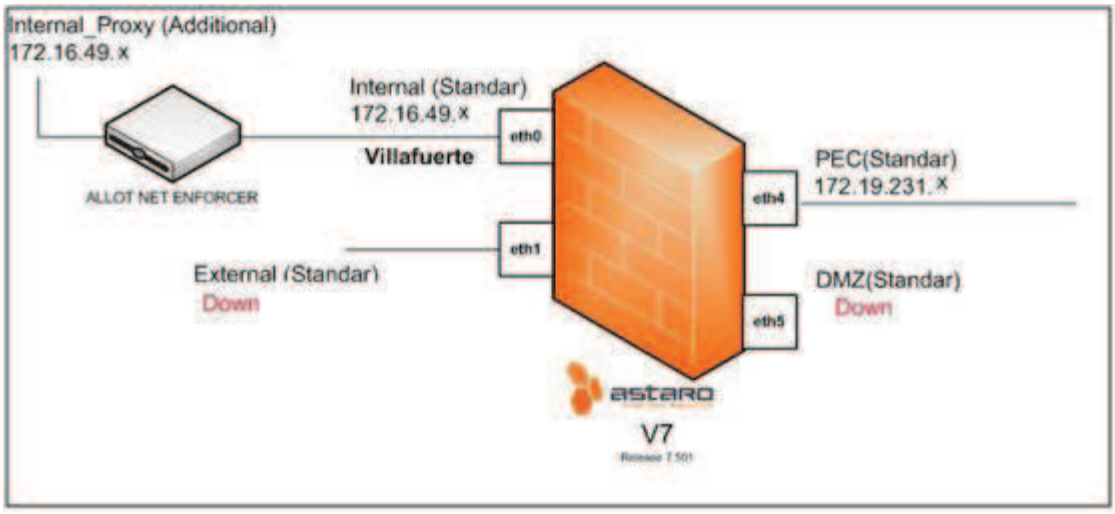


Figura 2-10.- Diagrama de Conexión del firewall Astaro[21]

Actualmente el dispositivo dispone de dos interfaces levantadas (Figura 2-10), una interna conectada a la red empresarial y una conexión externa correspondiente al enlace hacia Internet a través del proveedor CNT cursando por las dependencias de Petroecuador.

La zona DMZ[22] se encuentra desactivada pues dejó de funcionar al entrar en ejecución el enlace CNT-Petroecuador-Petroproducción, todo el tráfico desde y hacia el exterior de la red circula por este enlace.

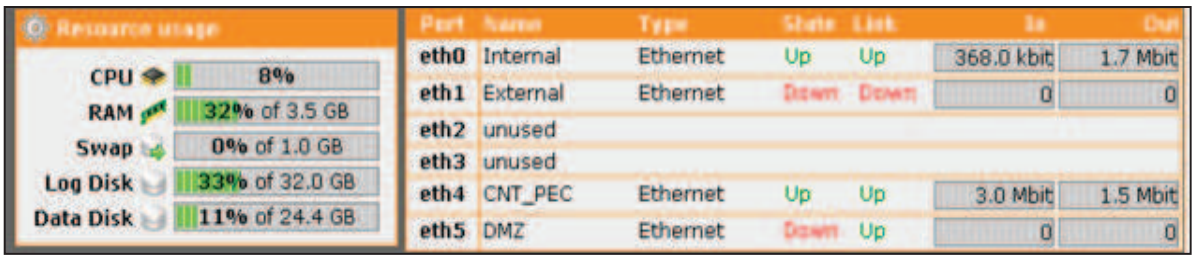


Figura 2-11.- Detalles de Firewall Astaro Gateway

[21] Coordinación de Tecnologías de Información Quito - PETROPRODUCCIÓN

[22] DMZ: Zona DesMilitarizada, se define como una red perimetral entre la red interna de una organización y una red externa (Internet).

Interfaz	Nombre	Dirección IP	Estado	Detalle
eth0	Internal	172.16.x.x /20	Up	Interfaz interno de la red PPR
eth1	External	IP pública[23]	Down	Down
eth4	CNT_PEC	172.19.x.x /29	Up	Enlace a la CNT a través de Petroecuador
eth5	DMZ	192.168.x.x /24	Down	Down

Tabla 2-10.- Interfaces del Firewall Astaro Gateway

2.4.1.2. Administrador de Ancho de Banda ALLOT ENFORCER

Actualmente se dispone de un manejador de Ancho de Banda Enforcer modelo ALLOT 404. Su función es generar datos estadísticos del uso de la capacidad del canal de la empresa y establecer un control para la optimización del mismo. Posee tres puertos para realizar sus funciones, un puerto interno, otro externo y una de administración. El externo se encuentra enlazado a la interfaz eth0 del proxy Astaro, mientras que el interno se enlaza a la intranet de la empresa. La Figura 2-12 presenta la conexión actual del administrador de Ancho de Banda dentro de la red interna. El dispositivo fue montado recientemente como una necesidad de Petroecuador impuesta a sus filiales. Debido a la imposibilidad de acceso a la información al mismo, no se recogen datos de esta fuente para el presente capítulo.

[23] La dirección no ha sido presentada por razones de seguridad

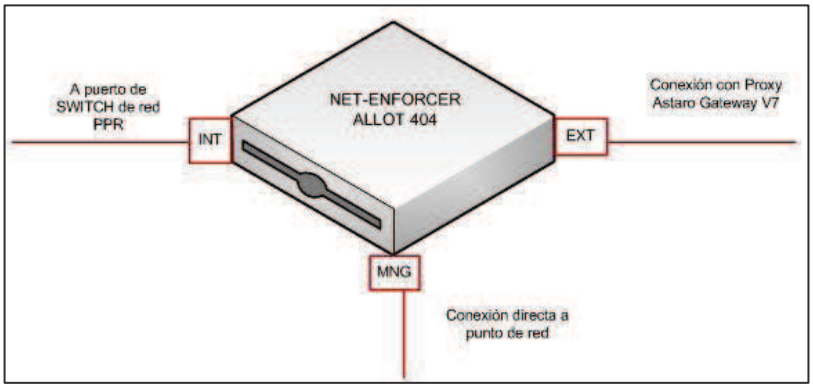


Figura 2-12.- Net-Enforcer Allot 404

2.4.1.3. Políticas de Seguridad Manejadas

La seguridad física está a cargo el personal de vigilancia de cada edificio, la empresa maneja reglas para precautelar la misma, de las cuales se puede resumir las siguientes:

- Para el ingreso particular a las instalaciones se requiere de una identificación otorgada por el personal de seguridad de la empresa. Sus empleados deben llevar su identificación a la vista.
- Todo equipo tecnológico que ingresa o sale del edificio es registrado.
- Cámaras de seguridad se encuentran ubicadas tanto en el ingreso a las instalaciones así como en el acceso a cada uno de los pisos.
- El acceso a cuartos de equipos, dispositivos de núcleo y distribución está restringida al personal autorizado del departamento de TIC.
- Se asigna a los empleados un usuario y una contraseña para el acceso a su estación de trabajo con una dirección IP estática.
- Los racks en cada piso de las instalaciones son bastidores bajo llave evitando la manipulación por parte de personas no autorizadas.
- Los dispositivos de interconectividad disponen de un usuario y una contraseña para su acceso y administración remota.
- El acceso inalámbrico requiere de una contraseña WPA-PSK.
- Se lleva un registro de la ubicación y función de cada dispositivo instalado mediante la realización de inventarios como documentación necesaria, la última ejecutada a mediados del año 2009.

2.5. ENLACE A INTERNET

PETROPRODUCCIÓN cuenta con una salida al exterior por medio de un enlace directo por fibra óptica con Petroecuador en Quito, este enlace es proveído por la Corporación Nacional de Telecomunicaciones y tiene una capacidad de 8 Mbps. Todo el tráfico saliente va por este canal y llega a Internet pasando primero por Petroecuador poseedor de un canal de 20 Mbps con el proveedor CNT y que lo distribuye entre sus filiales a lo largo del territorio ecuatoriano.

El laboratorio de Geología en San Rafael posee la misma estructura de conexión que la matriz en Quito pero con una capacidad de 3 Mbps en su enlace. Para las instalaciones del Distrito Amazónico se cuenta igualmente con un enlace de 6 Mbps de capacidad y una conexión directa a Internet de 8 Mbps.

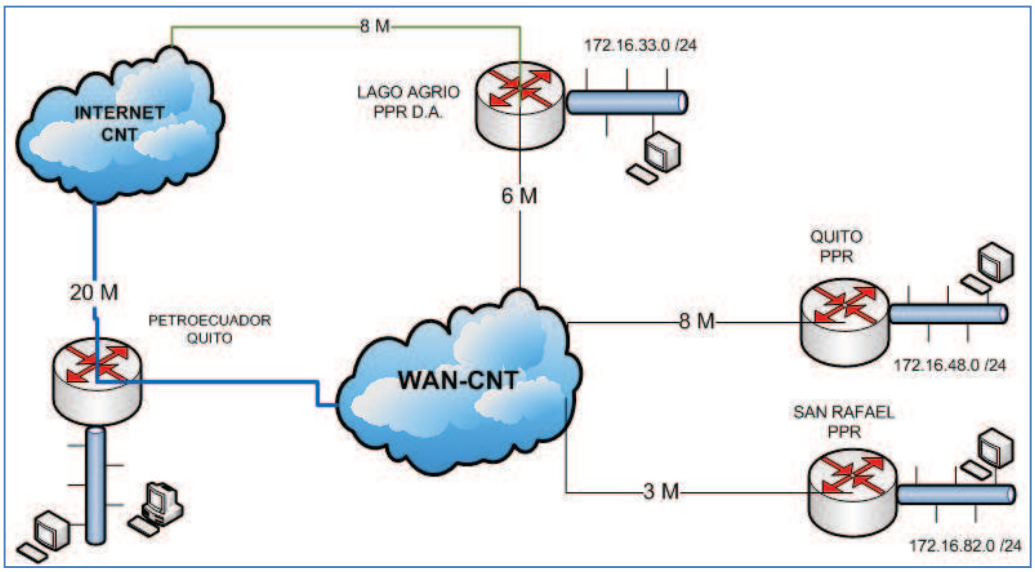


Figura 2-13.- Enlaces a Internet de la red RRR

2.6. ANÁLISIS DE TRÁFICO

2.6.1. DETERMINACIÓN DE LAS FECHAS DE MEDICIÓN

Para el análisis se recopiló tráfico dentro de un periodo mensual otorgado por el dispositivo firewall ASTARO, de esta forma se procede a tomar las muestras respectivas y realizar los análisis correspondientes. Las mediciones realizadas se encuentran agrupadas en el anexo A, donde se presentan gráficas y reportes recopilados.

Se realizaron tomas del tráfico global de la empresa de manera mensual, semanal y diaria tanto de los principales enlaces de la red y de algunos servidores importantes (escogidos en base a la cantidad de tráfico que manejan y por la capacidad del dispositivo de medición para monitorearlos). Debido a la gran cantidad de información solo se incluyeron los datos más relevantes de las mediciones en el presente Capítulo (en detalle presentado en el anexo A). Se establecieron tres fechas de medición diarias, con el objetivo de tener una mejor precisión.

Las fechas correspondientes se muestran en la Tabla 2-11. Dependiendo de las necesidades de este capítulo, se incluyó en ciertos casos días extra de medición, que se especifican en los resultados mostrados.

MUESTRAS	PERIODOS DE MEDICIÓN
MEDICIÓN MENSUAL	12 Diciembre 2009 – 12 Enero 2010
MEDICIÓN SEMANAL	6 - 12 de Enero 2010
MEDICIÓN DIARIA 1	8 de Enero 2010
MEDICIÓN DIARIA 2	11 de Enero 2010
MEDICIÓN DIARIA 3	12 de Enero 2010

Tabla 2-11.-Periodos de Medición de Tráfico

Las tomas gráficas realizadas por el servidor Astaro presenta tres tipos de datos: Current (valor actual) que muestra el valor del dato tomado en el mismo momento de realizada la medición; Average (Promedio) realiza un promedio de los datos medidos en el intervalo de tiempo; y Maximum (Máximo) que especifica el valor máximo que ha tomado la medición dentro del período que se realiza el análisis.

2.6.2. CONEXIONES SIMULTÁNEAS A SERVICIOS

Desde la Figura A-1 hasta la Figura A-5 (Anexo A) del análisis de conexiones diarias simultáneas a los diferentes servicios que corren en la red de Petroproducción se obtuvieron los resultados presentados en la Tabla 2-12. El valor Actual, es aquel tomado en el instante de captura de cada figura, por lo que se considera únicamente los valores promedio y máximo para el análisis.

Toda petición de servicio pasa a través del servidor Astaro, siendo éste un punto vital dentro de la red empresarial, como resultados de las muestras recogidas se observa un elevado número de conexiones de acceso simultáneas a los servicios, en promedio estas conexiones no afectan al rendimiento de la red pero incrementan el procesamiento del proxy a medida que su número crece.

CONEXIONES SIMULTÁNEAS			
	Actual	**Promedio**	**Máximo**
Muestra Mensual	1782	1095.68	15227
Muestra Semanal	2273	900.68	4792
Muestras Diarias			
MEDICIÓN 1	410	1105.92	3820
MEDICIÓN 2	331	1146.88	3338
MEDICIÓN 3	280	1140	5250

Tabla 2-12.- Conexiones Simultáneas a Servicios.

2.6.3. TRÁFICO INTERNO

La Tabla 2-13 sintetiza las mediciones de tráfico y permite la realización del análisis respectivo. Las mediciones correspondientes a tráfico entrante (Inbound) corresponden a un tráfico de subida de clientes y usuarios, mientras que el tráfico saliente (Outbound) es el tráfico de bajada hacia los usuarios de la red.

TRAFICO INTERNO						
	ENTRANTE (Mbps)			SALIENTE (Mbps)		
	Actual	Promedio	Máximo	Actual	Promedio	Máximo
Muestra Mensual	0.538	0.248	11.03	2.33	1.07	36.06
Muestra Semanal	0.351	0.307	11.03	3.84	1.43	8.68
Muestras Diarias						
MEDICIÓN 1	0.045	0.329	5.72	0.914	1.65	8.68
MEDICIÓN 2	0.691	0.389	4.09	0.044	2.03	8.27
MEDICIÓN 3	0.034	0.327	5.82	0.005	1.52	8.18

Tabla 2-13.- Tráfico Interno

La tabla anterior muestra en el canal de comunicación un tráfico entrante con un valor máximo de 11.03 Mbps, y un valor promedio que bordea los 0.36 Mbps entre todas las mediciones realizadas siendo este un valor bajo. De igual manera el tráfico saliente presenta un máximo de 36.06 Mbps que es un valor pico inusual (aproximadamente tres veces en valor de inbound), teniendo en consideración los valores máximos del resto de mediciones que están alrededor de los 8 Mbps, y valores promedio salientes que bordean 1.5 Mbps siendo también valores relativamente bajos teniendo en cuenta la cantidad de usuarios de la empresa. Considerando lo enunciado anteriormente se pronostica una baja probabilidad de congestión en el canal de transmisión por tráfico entrante o saliente.

2.6.4. TRÁFICO CNT-PETROPRODUCCIÓN

Primeramente se debe tener en cuenta que el canal proveído por la CNT presta una capacidad de 8 Mbps tanto para los sentidos de transmisión (subida) como de recepción (bajada) para el tráfico entre la CNT y Petroproducción Quito. Se tienen los siguientes resultados:

TRÁFICO CNT-PEC						
	ENTRANTE (Mbps)			SALIENTE (Mbps)		
	Actual	Promedio	Máximo	Actual	Promedio	Máximo
Muestra	2.15	0.961	8.01	0.479	0.391	9.35
Muestra	3.76	1.38	7.97	1.11	0.806	9.35
Muestras Diarias						
MEDICIÓN 1	0.904	1.58	7.95	0.024	0.613	6.69
MEDICIÓN 2	0.061	1.94	7.93	1.04	1.14	8.18
MEDICIÓN 3	0.070	1.47	7.70	2.82	0.902	8.07

Tabla 2-14.- Tráfico entre CNT y Petroproducción

La Tabla 2-14 presenta en síntesis el análisis del tráfico entrante y saliente de Petroproducción hacia la CNT, se puede apreciar que los valores promedios tanto de bajada como de subida están entre 0.391Mbps (medición mensual saliente) y 1.94 Mbps (medición 2 diaria entrante), en promedio de las 2 medidas se tiene el valor de 1.165 Mbps correspondiente a un 14.56 % de la capacidad total del enlace.

En la Figura A-13 hasta la Figura A-17 del anexo A se aprecia que el tráfico es elevado en el horario de 8:00 a 18:00 horas de lunes a viernes, en los cuales hay valores pico que sobrepasan el valor máximo del canal en pocas ocasiones, principalmente en sentido saliente como se aprecia en la medición mensual máxima con un valor 9.35 Mbps que correspondería a un 116% de la capacidad del canal, esto se explica debido a la limitación del canal brindado por la CNT no es exacta a los 8 Mbps.

De las tomas se puede concluir el grado de utilización del enlace que se presenta en la Tabla 2-15.

Grado Utilización del enlace CNT –PPR UIO	
HORARIO	**Porcentaje Utilización**
0:00 a 8:00	< 30 %
8:00 a 12:00	30 – 70 %
12:00 a 18:00	> 50 %
18:00 a 23:59	< 30 %

Tabla 2-15.- Grado Utilización del enlace CNT – Petroproducción Quito.

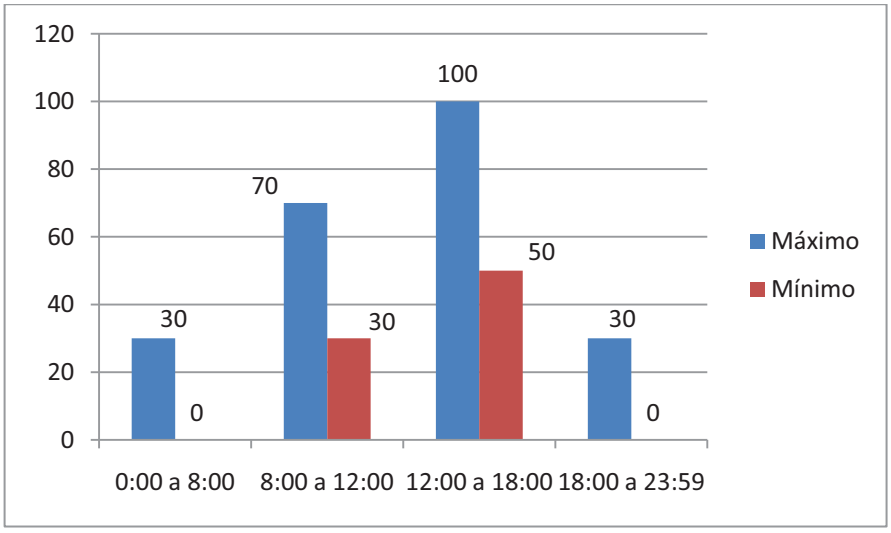


Figura 2-14.- Porcentaje de Utilización del enlace entre CNT y Petroproducción Quito.

2.6.5. TRÁFICO POR SERVICIOS

Es medido con el objetivo de apreciar cuáles son los servicios comúnmente requeridos por los usuarios de la red, de manera que queden en relevancia los más importantes y críticos según la cantidad de tráfico que manejen. Se presentan los datos más relevantes obtenidos de reportes de medición regidas a las fechas especificadas en la Tabla 2-11. Los reportes de las mediciones en detalle se muestran en el Anexo A del presente trabajo.

Conjuntamente con estos resultados tabulados se adjuntan gráficas comparativas, donde se podrá apreciar de mejor manera las características del flujo de datos a través de la red. Se usa un método deductivo partiendo desde estadísticas mensuales hasta diarias con el objetivo de buscar tendencias que justifiquen los datos mensuales.

2.6.5.1. Tráfico Mensual por Servicios

Para la toma de esta medida se estableció un periodo de muestra del 6 de diciembre de 2009 al 12 de enero del 2010. Mediante datos obtenidos de los reportes mostrados en las figuras desde A-44 hasta A-54, se especifican los diez servicios con mayor cantidad de tráfico total (entrante y saliente) ordenados de forma descendente según este parámetro.
Los resultados se muestran en la tabla siguiente.

Top	Servicio	Tipo	In	%	Out	%	Tráfico	%	Port
1	HTTP	TCP	24.2 GB	10.71	288.4 GB	48.02	**312.6 GB**	37.82	80
2	HTTP-ALT	TCP	25.5 GB	11.27	277.7 GB	46.23	**303.1 GB**	36.68	8080
3	SMTP	TCP	164.9 GB	73.02	5.8 GB	0.96	**170.6 GB**	20.65	25
4	HTTPS	TCP	3.1 GB	1.36	17.2 GB	2.86	**20.3 GB**	2.45	443
5	DOMAIN	UDP	1.7 GB	0.75	4.5 GB	0.75	**6.2 GB**	0.75	53
6	TINCAN[24]	TCP	49.5 MB	0.02	2.4 GB	0.41	**2.5 GB**	0.30	1935
7	MS-WBT-SERVER	TCP	152.9 MB	0.07	1.9 GB	0.31	**2.0 GB**	0.24	3389
8	0	GRE[25]	1.4 GB	0.61	333.4 MB	0.05	**1.7 GB**	0.21	0
9	MS-SQL-S	TCP	832.3 MB	0.36	779.5 MB	0.13	**1.6 GB**	0.19	1433
10	WEBADMIN	TCP	33.3 MB	0.01	257.3 MB	0.04	**290.6 MB**	0.03	4444
Totals	-	-	225.8 GB	-	600.6 GB	-	**826.4 GB**	-	

Tabla 2-16.- Tráfico Mensual por Servicios

[24] TINCAN: protocolo utilizado para stream de datos multimedia.

[25] Generic Routing Encapsulation: protocolo para el establecimiento de túneles a través de Internet. Definido en RFC 1701 y RFC 1702,

Se puede apreciar que el tráfico HTTP[26] tiene el mayor grado de utilización dentro de la empresa aproximadamente un 75% del total de tráfico generado (porcentaje en conjunto de los servicios HTTP y HTTP-ALT[27]) se evidencia como el servicio esencial en las transacciones empresariales diarias.

Por otro lado la importancia del servicio web para acceso a Internet se ve reflejada en la cantidad de tráfico obtenido en la muestra, constituyéndose en un servicio de relevancia para los empleados de la empresa. La consulta en línea, entretenimiento, educación, entre otros, son posibles usos de esta conexión al exterior.

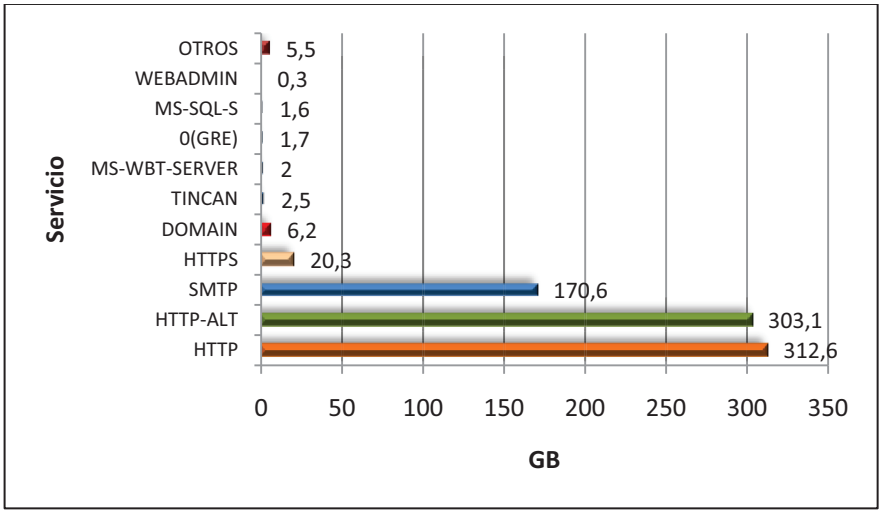


Figura 2-15.- Tráfico Mensual de los Principales Servicios

Mediante la observación de la Figura 2-15 se aprecia la gran diferencia existente entre los tres primeros servicios que abarcan un total del 95.15% del tráfico circulante en comparación con los restantes.

El servicio de correo electrónico ocupa el tercer puesto dentro de la muestra, notoriamente separado de los dos primeros sin dejar de ser menos importante. A pesar de su ubicación, este servicio que hace uso del Protocolo SMTP[28] es vital para las operaciones empresariales, el envío y recepción de documentos,

[26] Protocolo de Transferencia de Hypertexto
[27] HTTP-ALT: Protocolo HTTP alternativo que trabaja en el puerto 8080.
[28] Protocolo Simple de Transferencia de Correo

comunicados, reportes, datos, informes y demás documentos son anexados en gran cantidad varias veces al día por los usuarios, de ahí su cantidad alta dentro de esta muestra mensual.

2.6.5.2. Tráfico Semanal por Servicios

La muestra semanal arroja los resultados en la Tabla 2-17, al igual que en el punto anterior se presentan los diez primeros servicios organizados según su tráfico total de forma descendente.

Top	Servicio	Tipo	In	%	Out	%	Tráfico	%	Port
1	HTTP	TCP	5.4 GB	7.94	78.6 GB	47.98	**84.0 GB**	36.16	80
2	HTTP-ALT	TCP	4.5 GB	6.61	77.7 GB	47.44	**82.3 GB**	35.39	8080
3	SMTP	TCP	56.6 GB	82.45	1.6 GB	0.99	**58.2 GB**	25.04	25
4	HTTPS	TCP	757.1 MB	1.08	4.1 GB	2.49	**4.8 GB**	2.07	443
5	DOMAIN	UDP	198.4 MB	0.28	566.7 MB	0.34	**765.1 MB**	0.32	53
6	0	GRE	456.8 MB	0.65	82.1 MB	0.05	**538.9 MB**	0.23	0
7	MS-WBT-SERVER	TCP	39.0 MB	0.06	330.8 MB	0.20	**369.9 MB**	0.16	3389
8	TINCAN	TCP	4.5 MB	0.01	238.2 MB	0.14	**242.7 MB**	0.10	1935
9	DYNAMID	TCP	2.2 MB	0.00	140.4 MB	0.08	**142.6 MB**	0.06	9002
10	WEBADMIN	TCP	8.2 MB	0.01	131.3 MB	0.08	**139.5 MB**	0.06	4444

Tabla 2-17.- Tráfico Semanal por Servicios

No existe mayor variación en cuanto al porcentaje de información que estos servicios manejan. Para el servicio HTTP y HTTP-ALT se nota la existencia de tráfico saliente mucho mayor que el entrante, por el contrario en cuanto SMTP, existe un flujo mayor en el sentido de entrada.

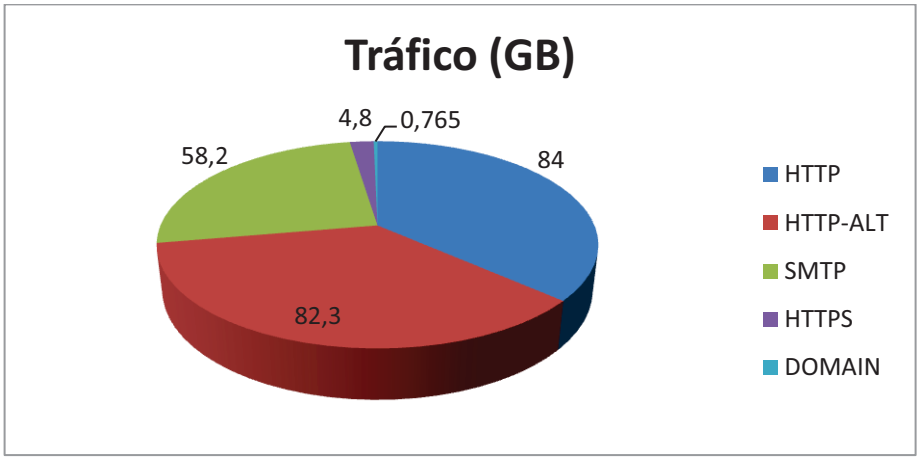


Figura 2-16.- Porcentaje de Tráfico Semanal por Servicios

2.6.5.3. Tráfico Diario por Servicios

Para una observación clara del comportamiento del tráfico diario, ha sido necesario la incorporación de dos muestras adicionales (13 y 14 de enero) a las especificadas en la Tabla 2-11, de esta manera se tendrá un mayor número de muestras con el fin de presentar una gráfica que presente las variaciones de cantidad de tráfico en función del tiempo.

Debido a que muestras anteriores (semanal y mensual) presentan claramente los servicios de mayor peso en cantidad de datos, se escogen los tres primeros para su tabulación, adicionalmente se incorpora el servicio de Dominio debido a su influencia en la resolución de nombres para los servicios tanto web como de correo electrónico.

	08-Ene	11-Ene	12-Ene	13-Ene	14-Ene
HTTP-ALT	16.50 GB	19.40 GB	14.40 GB	15 GB	17 GB
HTTP	15.80 GB	19.20 GB	15.60 GB	15.2 GB	17 GB
SMTP	7.60 GB	10.30 GB	25.60 GB	10.4	12.7 GB
DOMAIN	0.11 GB	0.12 GB	0.20 GB	0.133 GB	0.118 GB

Tabla 2-18.- Muestras de Tráfico Diario por Servicios

Los resultados presentan leves variaciones para el tráfico diario HTTP, HTTP-ALT y DOMAIN, los dos primeros se comportan de manera similar y con cantidades de datos muy cercanas la una con la otra, lo que justifica que la muestra mensual tenga una diferencia de apenas un 1.14% entre estos dos servicios. Sin embargo se tiene mayores variaciones y un pico pronunciado para el tráfico de correo electrónico, las irregularidades en la cantidad de datos tabulados se podrían justificar en las actividades operativas y productivas de Petroproducción en fechas específicas.

La Figura 2-17 muestra el comportamiento descrito anteriormente.

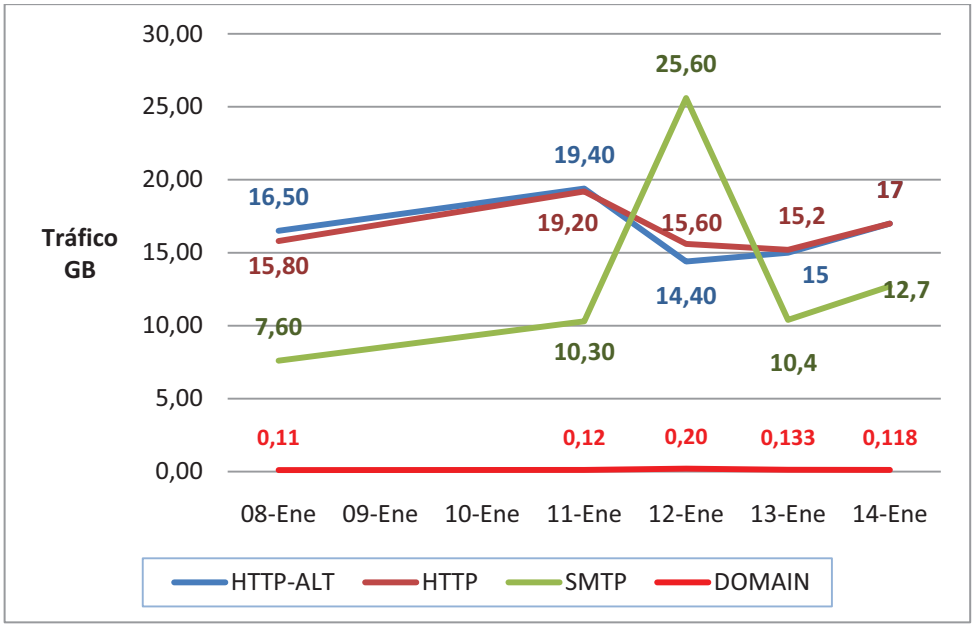


Figura 2-17.- Tráfico Diario por Servicios

SMTP muestra un pico de 25GB para el día 12 de enero, si bien esta cantidad es mayor al tráfico generado por HTTP, sucede de forma poco usual sin afectar la tendencia a nivel semanal ni mensual de este servicio.

2.6.6. TRÁFICO EN SERVIDORES

Los servidores han sido elegidos en función de dos premisas esenciales.

A. La capacidad de recoger datos de un servidor específico por parte del módulo configurable “Reporting” del dispositivo Astaro Gateway en su monitoreo.
B. Servidores esenciales para el funcionamiento de una red de datos empresarial.

Su presentación se hará de forma inductiva desde reportes diarios a mensuales para observar la tendencia y el comportamiento de su tráfico.

2.6.6.1. Tráfico servidor DNS

Este servidor ha sido elegido debido a la función que desempeña dentro de red al establecer la resolución de nombres para que los usuarios puedan ingresar a sitios web o conectarse con otros dispositivos dentro de la intranet. Aquí se sitúa el servidor Active Directory conteniendo el dominio PPR y todos los usuarios que pertenecen a la red. Debido a esto se recogen datos de este dispositivo presentados a continuación. Los resultados arrojados muestran la cantidad de tráfico generado o recibido por el dispositivo.

2.6.6.1.1. Tráfico diario del servidor DNS

Principalmente se maneja tráfico del tipo Dominio diferenciando los protocolos de capa transporte TCP y UDP. Los datos tabulados se presentan a continuación.

DIA	Servicio	Protocolo	In	%IN	Out	%OUT	Tráfico
8 Enero	DOMAIN	UDP	9.5 MB	98.08	35.7 MB	99.48	45.1 MB
		TCP	190.3 kB	1.92	190.3 kB	0.52	380.7 kB
11 Enero	DOMAIN	UDP	10.5 MB	98.20	43.3 MB	99.56	53.9 MB
		TCP	192.3 kB	1.75	194.4 kB	0.44	386.7 kB
12 Enero	DOMAIN	UDP	9.9 MB	98.11	37.9 MB	99.50	47.8 MB
		TCP	190.6 kB	1.84	196.0 kB	0.50	386.6 kB

Tabla 2-19.- Tráfico Diario del Servidor DNS

El tráfico diario es bajo en comparación con servidores como correo o web, se puede identificar que en el sentido de salida se maneja la mayor parte de los datos Domino, es decir, el servidor es el que da la mayor cantidad de información ante peticiones de clientes.

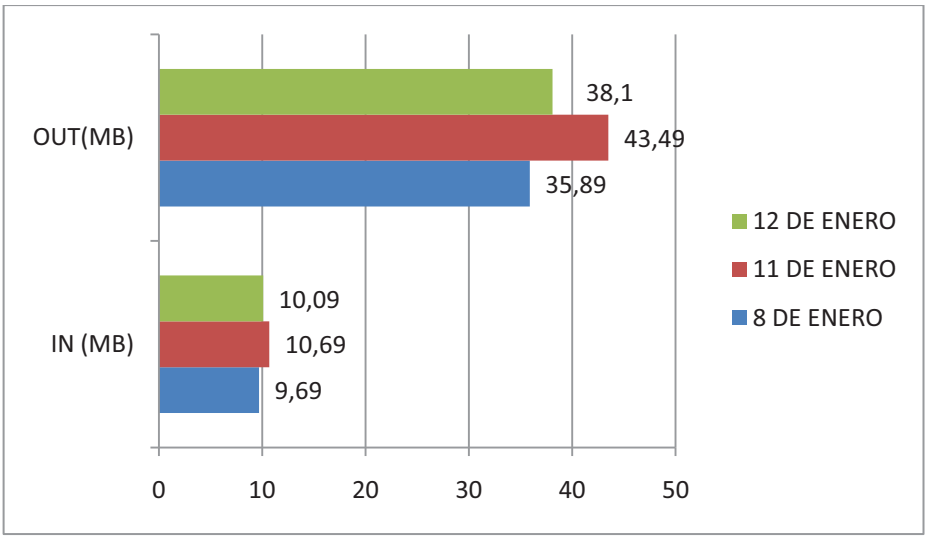


Figura 2-18.- Tráfico Diario DNS

2.6.6.1.2. Tráfico DNS semanal y mensual

Semanalmente este servidor maneja alrededor de 319 MB de tráfico del tipo Domain, el restante tráfico manejado por éste es despreciable, pues se encuentra por debajo del 1% del total y no requieren de mayor comentario. La Figura 2-19 presenta que la cantidad de información que genera el servidor es mucho mayor a la recibe de los clientes.

	Protocol	In	%	Out	%	Traffic	Packets	%
MENSUAL								
DOMAIN	UDP	760.5 MB	99.22	1.9 GB	99.44	2.6 GB	21847783	99.35
DOMAIN	TCP	2.9 MB	0.38	3.8 MB	0.20	6.7 MB	108369	0.49
SEMANAL								
DOMAIN	UDP	65.0 MB	98.02	251.6 MB	99.49	316.6 MB	2009774	97.60
DOMAIN	TCP	1.3 MB	1.96	1.3 MB	0.51	2.6 MB	49198	2.39

Tabla 2-20.- Tráfico DNS Semanal

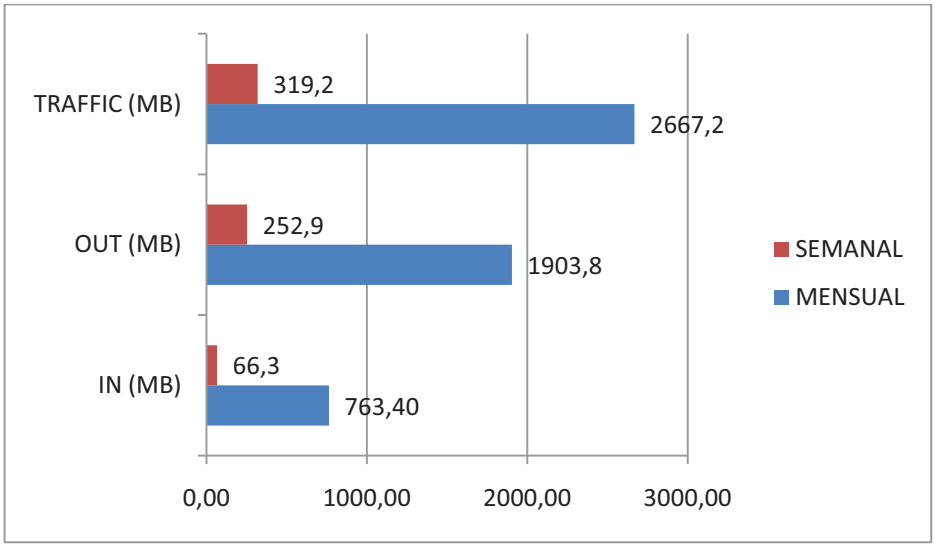


Figura 2-19.- Tráfico DNS semanal - mensual

De acuerdo a resultados se puede observar que el total semanal es menor que el esperado, la semana de toma de datos ha tenido un 11,5% del tráfico total del mes, lo que demuestra que las solicitudes y respuestas de este servicio se generan en mayor proporción las últimas semanas de cada mes.

2.6.6.2. Tráfico del Servidor Exchange

Los resultados obtenidos de todas las muestras se presentan en conjunto debido al tamaño del tráfico SMTP sobre los otros protocolos presentes en el servidor, los considerados irrelevantes para este caso (En detalle se muestran los reportes en el Anexo A). Este servicio realiza sus conexiones con el puerto 25 y representa uno de los dispositivos que maneja un gran volumen de información, se nota un gran volumen de tráfico de entrada, si bien existen volúmenes de tráfico saliente, éstos son pequeños en comparación con el primero.

La siguiente tabla muestra las cantidades de tráfico recopiladas del tipo SMTP.

Periodo	Fecha	Protocolo	In	Out	Tráfico	Conns
Mensual	12 dic- 12 ene	TCP	35.1 GB	1.4 GB	36.4 GB	665886
Semanal	07-12 ene	TCP	6.5 GB	279.3 MB	6.8 GB	152066
Diario	08-Ene	TCP	1.1 GB	46.2 MB	1.2 GB	23782
	11-Ene	TCP	1.3 GB	45.1 MB	1.3 GB	21622
	12-Ene	TCP	1.2 GB	45.8 MB	1.3 GB	22905

Tabla 2-21.- Tráfico del Servidor Exchange

La Figura 2-20 presenta una perspectiva del comportamiento de tráfico SMTP para este servidor, tanto mensual, semanal como un promedio diario. Teniendo en cuenta que en la empresa la mayoría de trabajo se realiza cinco días a la semana, y alrededor de cinco semanas por mes, las muestras siguen una proyección acorde a este enunciado.

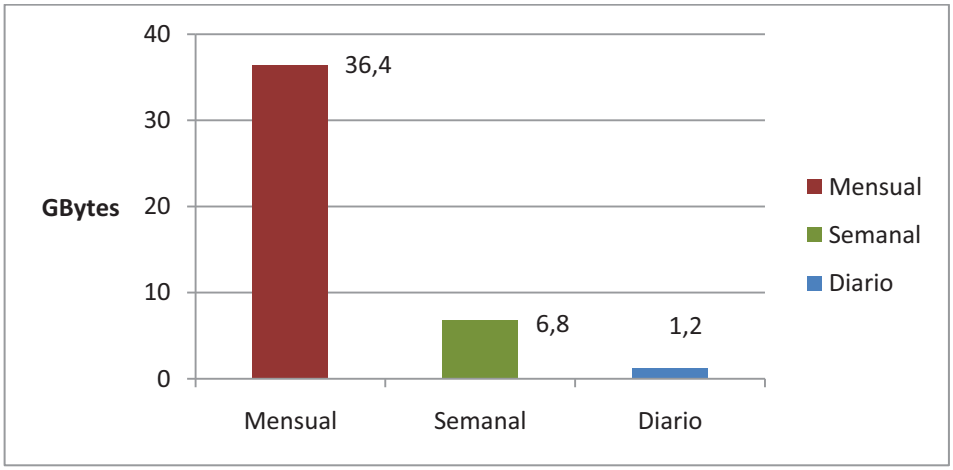


Figura 2-20.- Comparativa del Tráfico del Servidor Exchange

2.7. ESTABLECIMIENTO DE LÍNEA BASE

Con el fin de identificar anormalidades en el comportamiento de la red, una línea base se constituye en la descripción de parámetros habituales de la intranet, del tráfico y de equipos influyentes.

Las funciones y obligaciones del TIC se distribuyen de acuerdo con la nueva organización de departamentos presentada en la Tabla 2-1.

Para la administración de red, el personal de TIC es responsable de una serie de funciones (ver tablas del Anexo C), en relación al cargo que ocupan dentro de la empresa. La seguridad depende tanto de procedimientos cotidianos dentro de las instalaciones y de dispositivos firewall instalados

2.7.1. SERVICIOS FRECUENTES

Dentro de los servicios más comunes y con mayor generación de tráfico dentro de la red, se eligen los de mayor importancia y se los clasifica de acuerdo al volumen de información que manejan mensualmente.

El grado de utilización, permite identificar los servicios siguientes como los de mayor frecuencia:

- Servicio de Correo Electrónico.- mediante Microsoft Exchange
- Servicio de Internet.- mediante la conexión a la CNT por medio de Petroecuador
- Servicio de Web Interno.- con aplicaciones ejecutadas desde el browser del equipo del usuario con servidores de la empresa.
- Servicio Lotus Domino.- presente en el seguimiento de toda documentación ingresada al archivo de Petroproducción.

El resto de servicios al estar por debajo del 1% de tráfico manejado, no se los presenta a excepción del servicio de resolución de nombres, necesario para la comunicación entre dispositivos de una red.

SERVICIO	DETALLE
HTTP	Representa el 37,8 % del total de tráfico utilizado, junto con HTTP-ALT generan las tres cuartas partes del tráfico circulante.
HTTP-ALT	Tiene el 36% del total de tráfico mensual, representa una ruta alterna para el tráfico web hacia el puerto 8080. Junto con HTTP manejan alrededor de 300GB de información cada uno.
SMTP	Tiene el 20,65% del tráfico total, provee el envío y recepción de archivos, documentos e información a través de los servidores de correo Microsoft Exchange y el servidor de correspondencia interna Lotus Domino. Se convierte en un servicio de gran importancia dentro de la empresa. Maneja aproximadamente 170 GB de información durante el mes.
HTTPS	Representa el tráfico seguro existente en varias aplicaciones utilizadas como VPN´s, acceso remoto a servidores por parte del personal de TIC, entre otros. Representa un 2,45% del tráfico circulante con alrededor de 20,3 GB en datos.
DOMAIN	A través de la resolución de nombres DNS y con el servidor Active Directory ocupa apenas el 0,75% del tráfico.

Tabla 2-22.-Servicios más usados en la Red

2.7.2. EQUIPOS DE IMPORTANCIA

Si bien toda la infraestructura de la empresa tiene importancia en la red, se destacan para efectos de este estudio equipos considerados críticos para las operaciones empresariales. Algunos de estos corresponden a dispositivos que ofrecen los servicios de mayor tráfico en la red, otros son considerados por aplicaciones cruciales que manejan de acuerdo al personal de la Coordinación de TIC. Así se mencionan además de servidores, dispositivos de networking que poseen la mayor carga de información.

EQUIPO	DETALLE
BIZAGI	Plataforma para la automatización de procesos
LOTUS DOMINO	Maneja la correspondencia interna de la empresa y envío de documentos.
CORREO	Servidor mail, necesario para la transferencia de archivos y documentos.
WEB	Sistema web, encargado de interactuar con usuarios finales y conector hacia servicios informáticos empresariales.
DNS Y ACTIVE DIRECTOTY	Equipo poseedor del directorio empresarial
PROXY-FIREWALL	Sistema Linux ASG V7, responsable de la seguridad de la red.
SWITCHES DE ACCESO	Equipos que brindan conectividad a cada departamento de la empresa
SWITCH DE NÚCLEO	Equipo Central de información donde circula todo el tráfico generado.
RUTEADORES	Dispositivos de interconectividad entre dependencias y hacia el exterior.

Tabla 2-23.- Equipos de Importancia a Monitorear

2.7.3. ANÁLISIS DE ROUTERS Y SWITCHES

La toma de datos de estos dispositivos se lo realizó en distintos días según necesidades encontradas para este proyecto, las horas de medición estuvieron entre la 8:00 – 9:00 horas y entre 16:00 – 17:00 horas. Cabe mencionar que en el caso de los Ruteadores de la empresa, sus relojes se encuentran seteados con cinco horas de adelanto respecto a la hora actual.

Los métodos empleados fueron:

- Sesiones Telnet a dispositivos
- Sesiones web vía browser (Internet Explorer)
- Uso de SDM Security Device

2.7.3.1. Router Villafuerte

La Figura A-37 del ANEXO A, nos muestra un resumen del estado del router, aquí el porcentaje utilizado del procesador es de un 2% y de la memoria de un 8%. La Figura A-31 nos presenta un seguimiento del uso de la CPU del dispositivo a lo largo del tiempo, podemos destacar un pico inusual de 60% del procesador durante la última hora de monitoreo, este se lo puede explicar debido a la gran cantidad de información que soporta a la hora de la medición (16:15 horas). Sin embargo en promedio su uso no sobrepasa del 20% siendo un valor bajo y o representa peligro de sobrecarga, garantizando la capacidad operativa del router.

En cuanto al tráfico que soporta el dispositivo se tiene:

Tráfico	Total Paquetes	Paquetes Errados	% de Error
IP	2163363076 Recibidos 3159171057 Enviados	9682640 Encapsulación 205 Sin resolver 1243615 No ruteados	0,2 %
TCP	32146 Recibidos 29998 Enviados	2 Sin puerto	> 0,1 %
UDP	26485129 Recibidos 150 Enviados	13 Errores de checksum	> 0,01 %

Tabla 2-24.- Tráfico Router Villafuerte

De acuerdo al cuadro anterior, se presentan paquetes perdidos mínimos en comparación con la información procesada, el detalle de estadísticas se muestran en la Figura A-32 del respectivo anexo. El uso de memoria es muy bajo para el equipo, con un 6,85% de memoria en uso estando a plenas capacidades de procesar información. Para el tráfico, se pueden destacar las siguientes estadísticas, basadas en las gráficas de cada enlace presentadas en el Anexo A.

Enlace hacia:	Actual	Pico	Promedio Aprox.
Interno	1%	1%	1%
Tribuna	18%	95%	20%
Lago Agrio	45%	98%	40%
San Rafael	1%	1%	1%

Tabla 2-25.- Uso de enlaces Router Villafuerte

Cabe mencionar que los enlaces con mayor uso de su capacidad pertenecen a enlaces seriales o de radio-enlace entre los dispositivos ruteadores.

2.7.3.2. Router Principal del Edificio Tribuna

La figura A-37 y la figura A-38 del Anexo A presentan las capturas realizadas del Router principal del edificio Tribuna, el cual se conecta directamente con Villafuerte. Se realizó el análisis de la interfaz serial 0/0/0 que es la conexión con el Router Villafuerte donde se aprecia la variación de la utilización del ancho de Banda. Considerando que la toma se realizó a las 16:00 horas determinada como hora pico por estar cerca de la hora de salida de los empleados. Se puede ver el mayor grado de utilización del ancho de banda con un 85% en uso, este valor duró 10 segundos aproximadamente estabilizándose nuevamente a un valor cercano al promedio de alrededor del 30 % de su capacidad lo que significa que el Router está en buen funcionamiento sin la presencia de errores.

El cuanto al uso del procesador del equipo, se nota un 40% de uso en horas pico, mientras que el resto del día, el procesamiento es bajo. Igualmente con un 6,58% de uso de la memoria el router tiene suficiente espacio para almacenar actualizaciones de IOS en caso de necesitarlo.

Tráfico	Total Paquetes	Paquetes Errados	% de Error
IP	3370414466 Recibidos 2954222 Enviados	5481511 Encapsulación 145 Checksum 568 No ruteados 42978 bad hop count	0,16 %
TCP	5725472 Recibidos 2882691 Enviados	Sin errores	0 %
UDP	12198375 Recibido 12 Enviado	2 Errores de checksum	> 0,01 %

Tabla 2-26.- Tráfico Router Tribuna

2.7.3.3. Switch de Núcleo Catalyst 4507

El dispositivo de núcleo presenta los datos más elevados en cuanto al uso del procesador y memoria dentro de la red soportando toda la carga informática de la empresa. Podemos apreciar en la Figura A-39 el grado de uso del procesador en un 53% para cargas picos, aunque en promedio su uso está en el rango del 20% al 30%, estos picos frecuentes afectan el rendimiento del dispositivo.

El tráfico circulante por el switch es el siguiente:

Tráfico	Total Paquetes	Paquetes Errados	% Error
IP	22034069 Recibidos 153907 Enviados	83455 Errores de encapsulación 385 No ruteados	0,37 %
TCP	7695 Recibidos 9760 Enviados	2 Sin puerto	0,01 %
UDP	21684312 Recibidos 3 Enviados	13 Errores de checksum	>0,01 %

Tabla 2-27.- Tráfico Switch de Núcleo

La pérdida de paquetes es mínima garantizando la comunicación entre la red de la empresa. El detalle de los datos obtenidos se encuentran en las Figuras A-30, A-40 y A-41. En cuanto a memoria, el equipo posee un porcentaje de memoria en uso del 27.73%, valor relativamente bajo y con suficiente espacio para actualizaciones de IOS.

2.7.3.4. Switches de distribución Catalyst 2960G

Se tomó uno de los switch de distribución de la red para su análisis en función de la mayor cantidad de interfaces troncales activas, estas al interconectar switches, tendrán una mayor carga informativa que dispositivos con un menor número de troncales.

El dispositivo analizado es el switch de dirección 172.16.48.x ubicado en el cuarto de equipos del edificio Villafuerte. La Figura A-44 presenta un uso promedio del procesador del 12% al 14%, la existencia de un pico del 90% en la toma de los últimos sesenta minutos no es preocupante pues es una muestra aislada que no se ve reflejada en el monitoreo de las últimas 72 horas. Respecto al tráfico que procesa, las pérdidas son casi nulas, lo que garantiza la correcta operación del switch (datos detallados en la figura A-45). El espacio de memoria utilizado es bajo, con un 18,23% en uso el dispositivo funcionará correctamente.

2.8. REQUERIMIENTOS

Para la recopilación de los requerimientos dentro del diseño del NOC se utilizó el método de entrevistas, diálogos verbales y encuestas a distintos miembros del departamento de TIC, estas recogen necesidades en áreas como administración de recursos, políticas de gestión de seguridad y rendimiento de la red. Los elementos tomados en cuenta se orientan a las cinco áreas funcionales (FCAPS) de la recomendación ITU-T M.3400[29], presentados a continuación.

[29] UIT-T M.3400 Funciones de gestión de la red de gestión de las telecomunicaciones.

2.8.1. RESPUESTA A FALLOS

- Dar solución en el menor tiempo posible a problemas que se presenten dentro de la red PPR tanto en las instalaciones Quito como en el D.A.

- Llevar un control de los activos informáticos, elementos y servicios de red que sufren de algún tipo de desperfecto.

- Los problemas presentados deben tener un margen de tiempo para su resolución y prioridad para ser atendidos. La respuesta oportuna ante eventualidades debe estar ligada a la monitorización continua de los equipos de networking en operación, las alarmas y logs serán los primeros pasos para responder al problema.

2.8.2. CONFIGURACIÓN DE ELEMENTOS DE RED

Con la finalidad de atender de manera oportuna incidentes que degraden la operación normal de la red se requiere:

- Los agentes a ser monitoreados deben brindar la información suficiente para llevar un control del estado de funcionamiento del equipo.

- Los distintos elementos deben alertar a la NMS de la presencia de anormalidades en su operación.

- Únicamente los administradores deben tener acceso a los parámetros configurables de los equipos.

2.8.3. REQUERIMIENTOS DE ANÁLISIS DE DATOS (ACCOUNTING)

- Los datos a contabilizar de los agentes por parte de la NMS deben ser: capacidades de disco, utilización de memoria, uso del procesador, estados de las interfaces de red, procesos en ejecución considerados importantes, entre otros.

- Establecer márgenes de correcto funcionamiento de los dispositivos y umbrales máximos que alerten y sean el inicio de medidas preventivas ante posibles errores y fallas dentro de la red.

- Determinar el costo que implica a la red el uso de recursos por parte de un equipo.

2.8.4. RENDIMIENTO DE RED

- Monitorear el rendimiento, utilización y funcionamiento de los distintos elementos de red, teniendo una visión global de servidores, switches y routers que se encuentran activos dentro de Petroproducción, principalmente de los que manejan un mayor volumen de información.

- De igual manera se pueden monitorear hosts que muestren una gran utilización de recursos de la red, permitiendo el control y restricción de tráfico que él esté utilizando.

- La Coordinación TIC encargada de gestionar estos recursos necesita disponer de mecanismos que permitan comprobar su estado de funcionamiento actual, al igual que establecer premisas para su administración y mantenimiento.

- Disponer de herramientas que permitan llevar un control preventivo de los servidores y equipos de conectividad, garantizando la comunicación entre los distintos departamentos de la empresa.

2.8.5. REQUERIMIENTOS DE SEGURIDAD

Petroproducción se encuentra en proceso de elaboración de un plan de seguridad que incorpore aspectos de manejo de recursos, protección de información e infraestructura con políticas claras y controles que garanticen la

seguridad de sus recursos. Se ha podido establecer ciertos requisitos que en un principio se esperan obtener, como una base para el continuo desarrollo de la seguridad.

Los requerimientos son los siguientes:

- Establecer una base para la elaboración de un Plan de Seguridad que defina los pasos a seguir por el departamento de TIC y por el personal de la empresa.

- Establecer a la seguridad como un campo importante dentro de las operaciones empresariales definiendo los objetivos que persigue y determinando controles que aseguren la infraestructura física y la información empresarial.

- Identificar los principales riesgos y amenazas que afecten a la seguridad informática. Establecer recomendaciones que permitan la correcta utilización de los recursos de red existentes, sobretodo de los servidores más críticos.

- Controlar el acceso a las instalaciones del área de TIC dentro del edificio, a los cuartos de equipos y a los racks de distribución ubicados en cada planta.

- Definir funciones de administrador de seguridad dentro del departamento a un funcionario en particular.

Capítulo 3

DISEÑO DEL CENTRO DE OPERACIÓN DE RED "NOC"

3.1. INTRODUCCIÓN

Este capítulo contempla el diseño de un NOC en cinco áreas primordiales que permitan mantener un control centralizado de toda la red en base a necesidades y requerimientos recogidos durante el análisis del Capítulo anterior. El sistema centralizado permite simplificar la administración e implementación del NOC brindando una visión global de la red y reduciendo costos operacionales.

Se determinará los procedimientos que se deberán ejecutar para la administración del NOC mediante la elaboración de manuales de procedimientos de gestión y que destaquen procedimientos de contingencia ante eventuales fallos en las comunicaciones. Finalmente se presentará un análisis de costos para la implementación del NOC dentro de la empresa.

La Figura 3-1 presenta las fases consideradas para el Diseño.

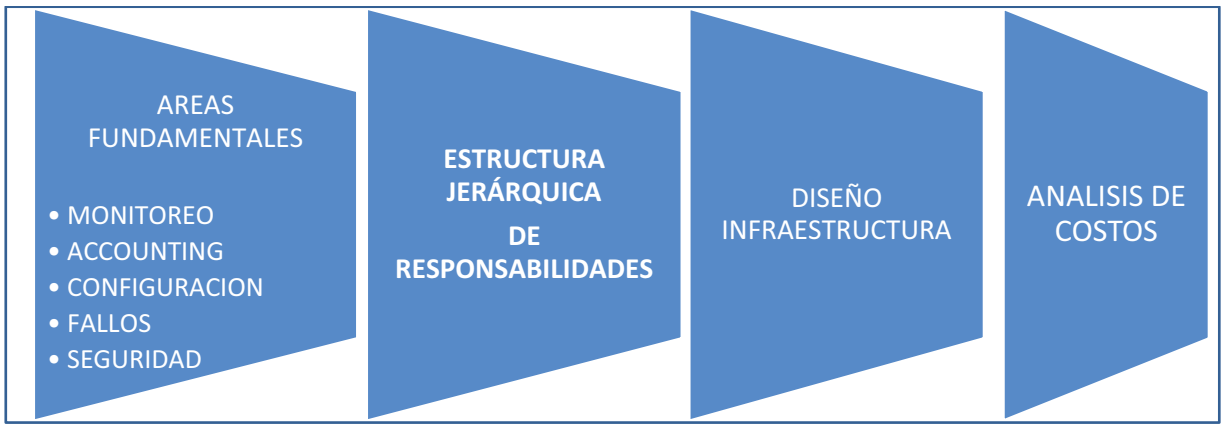


Figura 3-1.- Partes del Diseño del NOC.

Para una eficaz administración del NOC, su desarrollo será enfocado en cinco áreas con un diseño en base al modelo FCAPS,

3.2. DISEÑO DE LAS AREAS FUNDAMENTALES DEL NOC

La Figura 3-2 presenta cinco áreas fundamentales consideradas para el diseño del NOC en función del modelo FCAPS, las cuales ayudarán a segmentar el diseño en distintas partes permitiendo un adecuado desarrollo de los mismos.

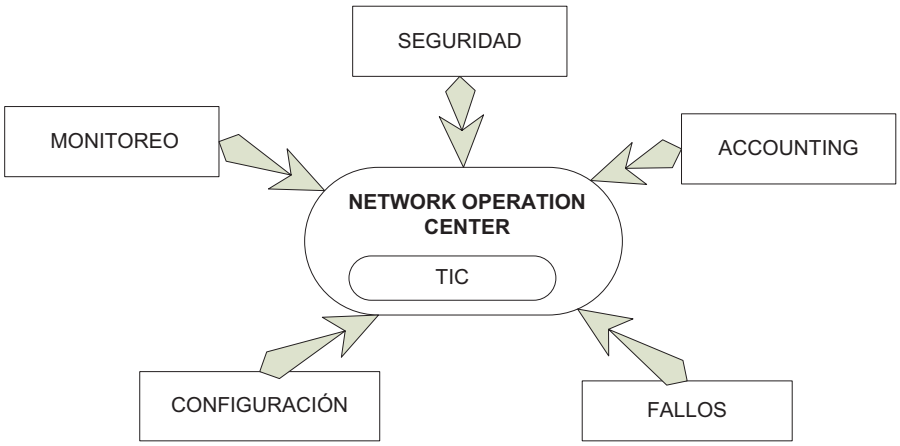


Figura 3-2.- Diseño del NOC.

3.2.1. DISEÑO DE GESTION DE MONITOREO

Una vez configurado todos los equipos (descritos en el punto 3.2.3), se procede al monitoreo de la red. Éste deberá ser realizado durante las 24 horas del día, los 7 días de la semana, el administrador debe estar en constante revisión de la consola JFFNMS para proceder a tomar acciones en caso de presencia de alarmas o eventos.

Se procede a definir los datos a monitorizar en los distintos dispositivos y especificar los umbrales para la gestión de alarmas.

3.2.1.1. Datos a ser Monitoreados

Los datos deben estar de acuerdo a las características propias del equipo gestionado, por ejemplo: memoria, puertos, interfaces, procesador, entre otros. De esta manera se presenta el siguiente cuadro que recoge los parámetros que se tomarán en cuenta en este proceso.

	Parámetro	Especificación
Servidor	Estado	Actividad del servidor, si posee o no conectividad.
	Memoria	Capacidad de memoria utilizada y libre, (RAM y discos duros).
	Procesamiento	Estadísticas de uso de la CPU.
Router	Interfaces	Estado actual de las interfaces utilizadas, tanto seriales como ethernet y módulos de red.
	Utilización	Porcentaje de ocupación del canal de transmisión en función de los datos procesados.
	Memoria	Memoria RAM y cantidad de disco utilizable para futuras actualizaciones.
	Procesador	Historial del uso de la CPU.
Switch	Interfaces	Estado y número de puertos utilizados. Protocolos en funcionamiento. Estado de puertos troncales.
	Errores	Porcentaje del tráfico procesado con error.
	Procesamiento	Uso del procesador.
	Dashboard	Información general del dispositivo: SNMP, ubicación, descripción, administrador, entre otros.
Enlace	Estado	Actividad del enlace, activo o inactivo
	Promedio Utilizado	Cantidad de tráfico promedio que cursa por el enlace.
	Máximo Utilizado	Pico más alto que ha cursado por el enlace en un tiempo determinado.

Tabla 3-1.- Parámetros a Monitorizar por Dispositivo.

Cualesquier otro parámetro de interés será añadido a la configuración de los dispositivos según las exigencias del NOC.

3.2.1.2. Definición de Umbrales

El rendimiento a nivel de servidor individual es afectado por los servicios en ejecución y los recursos que estos consumen en relación con su capacidad de procesamiento y memoria. Esto también se aplica a los dispositivos de conectividad. Los umbrales a establecerse se encuentran en función de las características propias del dispositivo, por esta razón es preferible otorgar un margen o porcentaje referencial.

Puesto que las recomendaciones las da cada casa fabricante y ante la falta de un estándar que defina estos parámetros, se toma en consideración el siguiente criterio dado por Microsoft: "*El uso del procesador de un servidor debe mantener una carga del 60 por ciento aproximadamente durante las horas de máxima actividad. Este porcentaje admite períodos de carga muy elevada. Si el uso del procesador está por encima del 75 por ciento de manera continua, el rendimiento del procesador se considera un cuello de botella*"[30].

Teniendo en cuenta esta recomendación, se considera que en promedio los equipos no deben sobrepasar el **75%** de la capacidad operativa por periodos de tiempo largos para mantener el rendimiento óptimo del equipo y la red en general. En caso de que el elemento de red trabaje sobre este porcentaje se recomienda tomar acciones correctivas que eviten la degradación de la red.

La memoria de un servidor sirve para atender las solicitudes a servicios de red, si se encuentra en uso casi en su totalidad, el servidor no atenderá nuevas peticiones, denegará aplicaciones que consumen memoria, y las solicitudes que están siendo atendidas demorarán más tiempo en completarse. Así el servidor se torna lento en responder, implicando retardos y un rendimiento por debajo de su comportamiento normal. Por esta razón se establece que la

[30] FUENTE: http://technet.microsoft.com/es-es/library/bb124583%28EXCHG.65%29.aspx

memoria no debe estar en utilización sobre el 75% en periodos largos y continuos en el tiempo, es recomendable ampliar la memoria RAM del servidor.

Para el caso de eventos referentes a la capacidad de discos duros, se recomienda establecer un umbral del 80%. Ésta premisa justificada en la rápida respuesta que se puede otorgar ante sobrecargas de información en memoria. Posibles soluciones como inserción de discos extras, respaldos o liberación de espacio en disco conllevará un tiempo de solución menor a problemas de procesador o memoria RAM, así se considera un evento menos crítico y con un umbral mayor.

En base a los criterios mencionados, se especifican los siguientes Umbrales:

Elemento	Parámetro	Umbral
Servidor	CPU	75 %
	RAM	75 %
	DISCO	80 %
Enlaces	CNT_PEC	75 %
	Backbone	75 %
Routers y Switches	CPU	75 %
	Memoria	75 %
Umbral de prevención		60 – 75%
Funcionamiento óptimo		< 60%

Tabla 3-2.- Umbrales Establecidos

Por otra parte se considera umbrales de prevención, que implican un trabajo de entre el 60% y 75% por periodos continuos. Los administradores deben prestar mayor atención a elementos dentro de este rango para prevenir que no sobrepase el límite establecido.

Cuando los dispositivos se encuentren trabajando por debajo del 60% de su capacidad operativa se considera que el mismo funciona de manera óptima.

3.2.2. DISEÑO DE GESTION DE ANÁLISIS DE DATOS (ACCOUNTING)

Permitirá la medición del uso de los recursos y servicios de la red empresarial, para lo cual se establece un proceso que permita obtener datos estadísticos de los distintos elementos de red a controlar. Para llevar su contabilidad se definen parámetros que permitan tener una noción clara del funcionamiento de la red:

- Tráfico entrante y saliente en enlaces importantes y de interés entre dispositivos de conectividad y/o servidores.
- Cantidad de ocupación de los discos duros de servidores, permitirá identificar el momento de inserción de nuevos módulos de almacenamiento para la información.
- Porcentaje de uso del procesador del equipo, permitirá especificar si el equipo está en óptimas condiciones para soportar la carga informática actual. Al mismo tiempo será una herramienta de planificación en la adquisición de dispositivos que remplacen aquellos que no soporten la carga actual.
- Cantidades de paquetes caídos o errados en interfaces monitoreadas. Éstos detonarán en la realización de un análisis y búsqueda de soluciones que detengan y eviten la pérdida de datos.
- Tasa de errores en los canales e interfaces de transmisión de la información.
- Permite el llevar un registro de alarmas (logs) generadas por dispositivo de red, los recursos necesarios para atenderlos y el tiempo que el personal invierte en solucionar los eventos.
- En aspectos de seguridad permite contabilizar las entradas de cada miembro del NOC a los servidores o cuarto de equipos y el tiempo que se demora dentro del mismo.
- RADIUS y TACACS son ejemplos de protocolos comúnmente utilizados para gestión de contabilidad en acceso de usuarios además de brindar seguridad.
- Establecer los límites de uso de recursos en planificación de capacidad de ancho de banda por grupo de usuarios.

- Reportes automáticos de eventos sucedidos por dispositivo o por periodos de tiempo.

Las estadísticas, reportes y gráficas serán de gran utilidad para el administrador; Podrá observar y contabilizar qué servidores o dispositivos en general están consumiendo grandes cantidades de recursos, dando lugar, en caso de ser necesaria una re-planeación de la capacidad de servidores que estén trabajando sobre los umbrales pre-establecidos.
Herramientas como Astaro Gateway y Allot Enforcer pueden ser utilizadas en conjunto para controlar el uso de recursos de aquellos elementos que generen problemas.

3.2.2.1. Procedimiento para el manejo de Análisis de Datos (Accounting)

Los siguientes pasos presentan un proceso para contabilizar parámetros de interés para los administradores del NOC dentro de la red.

a) Fijar los distintos parámetros que serán contabilizados.
b) Crear un proceso de recolección de datos.
c) Fijar una base de tiempo en el cual los valores serán recolectados.
d) Recolectar datos mediante herramientas a agentes.
e) Finalizar del proceso de recolección.
f) Clasificar valores y datos obtenidos según los criterios de contabilidad que se utilicen.
g) Obtener y respaldar un registro de la contabilidad realizada.
h) Evaluar los resultados obtenidos.

3.2.3. DISEÑO DE GESTION DE CONFIGURACION

Dentro de esta área se considera los parámetros a ser configurados para el monitoreo de dispositivos, implicando la instalación de agentes en los diferentes sistemas operativos y la consola de administración del NOC (NMS). De igual manera se reseñan criterios a tener en cuenta en el funcionamiento diario de la red.

3.2.3.1. Configuraciones de Monitoreo

Para el correcto funcionamiento de SNMP v2c se definen los siguientes parámetros:

- COMUNIDAD de Lectura y Escritura: **sec_tic_ppr.**
- COMUNIDAD de Solo Lectura: **sec_tic_public.**
- GRUPO de Escritura y Lectura: **nocrw.**
- GRUPO únicamente de Lectura: **nocro.**
- MIBs permitidas para las Vistas: **MIB-2, cisco, snmpv2**.

3.2.3.1.1. Configuración del Agente Snmpd en Linux

Linux utiliza el demonio snmpd para enviar información de administración de los dispositivos. Para su activación se realizan los siguientes pasos:

1. Instalar el demonio snmpd.
2. Modificar los archivos de configuración snmpd.conf y snmpdtrap.conf.
   - Configuración de comunidades y vistas.
   - Habilitación del monitoreo del agente
3. Iniciar el servicio SNMP.

El Anexo D muestra en detalle la configuración del agente en Linux.

3.2.3.1.2. Configuración de SNMP en Windows 2003 Server y Windows XP

Se debe instalar el servicio con el siguiente procedimiento:

1. En el panel de control dirigirse a *Herramientas Administrativas* y entrar a la ventana *Agregar y Quitar Programas*.
2. Se selecciona los detalles de *Herramientas de administración y Supervisión* dentro del apartado *Agregar o Quitar Componentes de Windows*.
3. Escoger el protocolo SNMP y aceptar.

Nota: el sistema pedirá el CD de instalación para poder copiar en disco los paquetes necesarios para el funcionamiento del agente.

4. Se finaliza la instalación y se configura el agente ingresando en la ventana servicios de Herramientas Administrativas del sistema.
5. En propiedades del agente, agregamos el nombre de la comunidad (en la pestaña *capturas)*, para nuestro casó será **"sec_tic_ppr"** y el destino de la información recogida "172.16.X.X" (dirección IP del servidor).
6. Definir el nombre de administrador del equipo (Contacto) y la ubicación física del equipo (Ubicación).
7. En la pestaña Servicio, activar las casillas de verificación situadas junto a los servicios proporcionados por el equipo según las necesidades.

Desde la Figura D-1 a la Figura D-8 del Anexo D, se muestra el procedimiento de configuración del agente SNMP en Windows Server de manera gráfica.

3.2.3.1.3. Configuración del Agente SNMP en Windows Vista ó Windows 7

Al igual que en Windows XP se procede con pasos similares el procedimiento de configuración del agente:

1. Dentro del *Panel de Control,* ingresar en "*Programas y características"*
2. Escoger la opción activar o desactivar las *características de Windows*. Y buscar característica *SNMP*, activarla y aceptar.
3. Seleccionar *Herramientas Administrativas*, e ingresar en el ícono de *Servicios y* seleccionar el servicio SNMP**.**
4. En la ventana de propiedades de SNMP, agregamos la comunidad "sec_tic_ppr" y el destino de la captura "172.16.X.X"
5. En la pestaña seguridad, en el apartado nombre de comunidad añadimos la comunidad "sec_tic_ppr".
6. Luego activar la opción Aceptar paquetes SNMP de cualquier host, o en su defecto la configuración que los administradores del NOC crean más conveniente para su gestión.
7. Finalmente se reinicia el servicio SNMP.

3.2.3.1.4. Configuración de SNMP en Router o Switch Cisco

Para la activación del agente SNMP se ejecutan comandos en modo de configuración global, estableciendo:

- Configuración de comunidad.
- Habilitación de traps y logs.
- Información del dispositivo (contacto, locación y descripción).
- Destino de las traps.
- Configuración de vistas a las cuales se tendrá acceso.

En la configuración en detalle se muestra en el Anexo D con los comandos a ser ejecutados en los dispositivos Cisco.

3.2.3.1.5. Configuración de SNMP en Servidores AS400

Se la realiza mediante el ingreso de comandos propios de estos servidores:
Se modifica la configuración del servicio SNMP: CFGTCPSNMP, donde se establecerán los siguientes parámetros:

- Nombre de Comunidad
- Valor de ASCIICO, conversión del nombre de comunidad a ASCII para atender a peticiones SNMP, pues este sistema maneja lenguaje EBCDIC.
- Dirección IP de la estación NMS.
- Habilitación de traps y logs

3.2.3.2. Configuraciones de Conectividad

Los dispositivos de conectividad deber garantizar la comunicación entre los usuarios y los servicios que se ofrece dentro de la intranet. Hay que tomar en cuenta ciertos parámetros que permitan optimizar su interconexión.

A continuación se mencionan puntos a considerar dentro de la configuración en switches y routers.

- Uso de puertos troncales y de acceso en modo de auto-negociación en cuanto a velocidad y modo de puerto (dúplex).

- Uso de protocolos de enrutamiento dinámico y rutas estáticas en caso de ser necesarias.
- Empleo de protocolos que eviten lazos y rutas redundantes entre dispositivos de red, por ejemplo STP.
- Para enlaces WAN empresariales, la multiplexación de canales si se manejan E1 o T1.
- Comunicación permanente con el proveedor de enlaces WAN de fibra.

3.2.3.3. Configuraciones de Análisis de Datos (Accounting)

Con el fin de llevar un registro contable de protocolos, alarmas y eventos que se generen con los elementos de red será necesario habilitar ciertos servicios en los dispositivos de interés.

- Habilitar logs y traps del equipo redirigiéndolos al servidor de logs.
- Habilitar únicamente los tipos de traps de interés para el departamento.
- Uso de SNMP en cada uno de los elementos.
- Herramientas de captura de información del tráfico circulante en la red y un trabajo en conjunto con servidores de seguridad y monitoreo para su análisis.
- Permitir presentación estadística del análisis de datos.
- Configuración de protocolos que permitan la gestión de accounting como RADIUS o TACACS.

3.2.3.4. Configuraciones de Seguridad

Dentro de la infraestructura existente, se debe poseer mecanismos que brinden seguridad tanto a la información como a los equipos de red. El uso de firewalls y demás dispositivos protegerán de ataques internos y externos (esto manejado por la solución Astaro). Sin embargo se deben establecer lineamientos que aseguren el acceso a equipos responsables de la comunicación entre los usuarios.

Se enumeran los parámetros a seguir para evitar accesos no autorizados:

- Configuración de una VLAN de administración de dispositivos y seteo de direcciones IP estáticas a cada dispositivo administrable.
- Creación de un direccionamiento de red exclusivo para dispositivos de interconectividad cuyos valores sean conocidos solamente por el personal a cargo.
- Uso de usuarios y contraseñas encriptados en el acceso local y vía remota, realizando cambios periódicamente.
- Usar SSH para el ingreso y configuración remoto de dispositivos. No habilitar su acceso desde redes externas.
- Establecer seguridades por puertos en switches que se considere pertinentes, sobretodo en la capa núcleo y distribución.
- Eliminar los permisos de acceso a usuarios que han sido separados del personal de la empresa o que han sido trasladados a otro sitio de trabajo.
- Limitar el número de veces por sesión que un usuario trata de ingresar una contraseña incorrecta.
- Creación y gestión de listas de acceso para restringir o permitir trafico a las diferentes dependencias según las necesidades de la empresa.
- Configuraciones periódicas de los dispositivos de seguridad para tener actualizadas sus reglas y restricciones.
- Aplicar las políticas de seguridad en los servidores correspondientes conforme se van estableciendo en la empresa.

3.2.4. MANUAL DE PROCEDIMIENTOS DE GESTIÓN DE FALLOS

Petroproducción otorga importancia relevante a las tareas informáticas que se realizan dentro de sus dependencias, por tanto los equipos deben mantener altos niveles de operatividad. El resultado de esta etapa es la estructuración de un “Manual de Procedimientos de Gestión de Fallos”, que remite de:

- Metodología de Troubleshooting[31]
- Proceso de Solución a Fallos

[31] Proceso a seguir para la solución de problemas.

- Monitoreo
- Identificación del Problema
- Aislamiento del problema
- Resolución de fallos
- Documentación

- Plan de contingencia ante fallos

El manual tiene como objetivo diagnosticar y corregir problemas en la red de comunicaciones.

3.2.4.1. Metodología - Troubleshooting

La asociación con un modelo de capas (OSI o TCP/IP) garantizará un apropiado orden en busca de causas a fallos acontecidos. El empleo de la metodología Bottom-up para la resolución de problemas empieza por la capa inferior desde los componentes físicos de la red y asciende gradualmente por las capas superiores hasta identificar la causa del fallo.

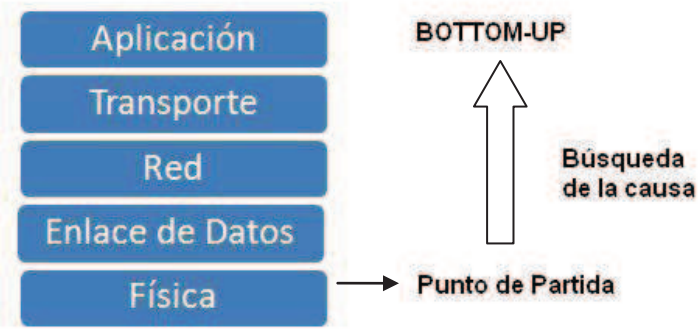


Figura 3-3.- Metodología Bottom-Up

Bottom-up será implementado en el tratamiento a problemas informáticos con la finalidad de resolverlos en el menor tiempo posible.

3.2.4.2. Proceso de Solución a Fallos

De igual manera, con el fin de obtener un proceso organizado que garantice soluciones eficaces a fallos, se presentan puntos importantes considerados

para atacar un problema, desde su descubrimiento hasta la evaluación de su solución, como se muestra en la Figura 3-4.

Figura 3-4.- Proceso de solución de Problemas

3.2.4.2.1. Monitoreo

Se realiza a través de la consola JFFNMS (detallada en el punto 3.2.1 de la Gestión de Monitoreo). Los problemas que no se vean alertados en la herramienta serán sujetos de atención inmediata ante una eventual llamada al área de soporte a usuarios y reflejadas en la herramienta "Resolve It"[32], el administrador deberá integrar la nueva falla para hacerla visible por la consola de monitoreo dependiendo de qué tan crítico sea el problema.
A continuación se establecen los siguientes pasos a seguir:

1. Monitorear en la pantalla principal de la consola que todos los dispositivos se encuentren activos y sin alarmas (color verde).
2. En caso de que en la herramienta exista la presencia de una alarma, se navegará dentro del segmento de red alertado, identificando el dispositivo afectado.
3. Verificación de la fecha y hora que se produjo la falla.

[32] Sistema implementado para la asignación de técnicos en soporte a usuarios

La revisión de la pantalla principal de la NMS tiene que ser continua, En caso que el monitoreo no pueda ser permanente se recomienda cada determinado intervalo de tiempo identificando cualquier indicio de fallo. El tiempo es de 5 a 10 minutos, para una detección rápida de eventos y apertura del proceso de troubleshooting.

3.2.4.2.2. Identificación del Problema

Mediante el mensaje de alarma generado se identifica el dispositivo problemático, se procede a realizar lo siguiente:

- Verificación de conectividad con el dispositivo.
- Su respuesta a peticiones SNMP.
- Su respuesta a administración remota vía CLI.
- Logs lanzados por el dispositivo.

Si no se pudiese identificar el problema, el acceso físico al dispositivo será usado como último recurso para encontrar una falla.

3.2.4.2.3. Aislamiento del problema o fallo

Se debe aislar el problema o la causa del mismo, recomendando empezar eliminando los problemas más críticos y posteriormente continuar con los demás. El usuario puede ayudar dando detalles de sus actividades antes y durante el error. Puede ser útil pedir al usuario que no trate de hacer nada con el equipo cuando se produzca el problema, salvo llamar a los administradores, quienes verificarán lo que está sucediendo.

3.2.4.2.4. Resolución del Fallas

Una vez aislado el problema, se procederá con las soluciones más sencillas, continuando con las más complejas. Todo proceso que involucre la solución de un problema debe ser notificado y documentado.

Se deberá identificar puntos críticos y niveles de criticidad para dar prioridad de atención al dispositivo con fallo. Los administradores son los encargados de

resolver el problema, reparar los dispositivos defectuosos y en última instancia sustituirlos. En caso de ser problemas a nivel de software se debe detallar específicamente los cambios y configuraciones que se realicen antes y después de atacar el problema.

Para la resolución de fallos se presenta el Plan de Contingencia descrito a continuación en el punto 3.2.4.3.

I. Puntos Críticos

En base a resultados de la encuesta realizada en las instalaciones de Quito y presentada en las figuras B-1 y B-2 del Anexo B, se establecen los siguientes como puntos críticos dentro del funcionamiento de la red PPR.

- Servidores de aplicaciones relacionadas con el área operativa de Petroproducción.
- Servidor de Correo Electrónico, Lotus Domino y Web.
- Enlace de fibra Petroproducción – Petroecuador.
- Dispositivos de Core: Switch Catalyst 4507, Switches de Distribución, Routers Cisco 2800 y 2600.
- El hardware y software en la red de backbone.
- Servicio de Internet.
- Enlaces Troncales entre las capas de núcleo, distribución y acceso.

II. Niveles de Criticidad

La Tabla 3-4 presenta el nivel de criticidad a considerar en presencia de un fallo, los datos fueron obtenidos en base a la encuesta realizada al personal de TIC (ANEXO B). Si dos problemas tuviesen el mismo nivel de criticidad y se presentasen al mismo tiempo, queda a consideración del administrador su atención teniendo en cuenta el grado de afectación dentro de la red.
La Tabla 3-3 muestra la escala de criticidad considerada para la encuesta realizada.

1	2	3	4	5
Poco crítico	Algo crítico	Crítico	Muy crítico	Extremadamente crítico

Tabla 3-3.- Escala de Criticidad de la encuesta.

	Criticidad					Responsable
FALLA	**1**	**2**	**3**	**4**	**5**	
Caída de un enlace WAN interno de la Red (Dentro de Quito).				X		Supervisión de Infraestructura
Caída de un enlace WAN de la Red (Fuera de Quito).					X	Supervisión de Infraestructura
Caída del enlace a Internet					X	Coordinación, Supervisión de Infraestructura
Caída de un servidor de área operativa. Ejm: Bizagi.					X	Supervisión de Aplicaciones
Caída del servidor Active Directory					X	
Caída de un servidor de uso general Ejm: Mail, Antivirus, Lotus, Web					X	
Problemas en la red de transporte.			X			Departamento Redes Supervisión de Infraestructura
Fuera de servicio de Hardware o Software del backbone.					X	
Problemas con un Switch de acceso.			X			Área de Redes Supervisión de Infraestructura
Problemas con un Switch de distribución.				X		
Problemas con un Switch de Core.					X	
Problemas con un Router					X	
Problemas con puntos de red y cableado estructurado			X			Supervisión de Infraestructura y Soporte de Usuario
Problemas software o hardware en equipos de usuarios normales.			X			Soporte de Usuario
No se pueden leer las MIBs de un equipo.			X			Área de Redes
Equipo no responde a SNMP pero si a Ping.			X			
No existe conectividad alguna sobre el dispositivo			X			Área de Redes, Soporte Usuario
El dispositivo a sufrido un problema eléctrico y deja de funcionar			X			Soporte de Usuario

Tabla 3-4.- Nivel de Criticidad por Fallo según la encuesta.

Los resultados de la encuesta permiten tener una visión global de la experiencia de la Coordinación TIC acerca de los problemas presentados en la

red. Por medio de los resultados obtenidos, se establece en la Tabla 3-5 la escala de criticidad necesaria para la gestión de fallos.

NIVEL	DESCRIPCIÓN
Extremadamente crítico (5)	Afectación en el tráfico de la red debido a avería en hardware, software o configuración.
Muy crítico (4)	Afectación de servicios. Problemas que impidan la gestión de la red.
Crítico (3)	Afectan a la operación de equipos, mantenimiento y/o gestión.
Algo crítico (2)	Problemas tolerables durante el funcionamiento de la red
Poco crítico (1)	Asesoría sobre detalles técnicos.

Tabla 3-5.- Descripción de los niveles de criticidad a ser considerados.

III. Tiempos de Solución a Fallos

Se definen tiempos de solución de fallos en base a su severidad descritos en la Tabla 3-5. Se tiene en cuenta los siguientes conceptos:

- TIEMPO DE ATENCIÓN: Es el considerado en que el personal del NOC debe llegar a atender un fallo.
- TIEMPO DE NEUTRALIZACIÓN: El máximo para aislar el problema y dar soluciones.
- TIEMPO DE RECUPRACIÓN: El tiempo máximo en que el fallo debe ser resuelto desde su aparición.

Estos tiempos involucran el llamar a personal experto en los equipos afectados en caso que así se requiera.

	NIVEL 1 Y 2	NIVEL 3	NIVEL 4 Y 5
TIEMPO DE ATENCIÓN	4 horas	1 hora	30 minutos
TIEMPO DE NEUTRALIZACIÓN	2 días	8 horas	4 horas
TIEMPO DE RECUPERACIÓN	15 días	2 días	1 día

Tabla 3-6.- Tiempos máximo de respuesta.[33]

[33] Basado en Documentación confidencial de DIGITEC S.A.

En casos extraordinarios de problemas con equipos que requieran ser importados o aplicación de garantías y se necesite un tiempo mayor para el proceso de solución de fallos, se debe proporcionar soluciones temporales para que la red no se vea gravemente afectada hasta que se levante nuevamente el servicio.

Con el fin de obtener tiempos referenciales que permitan una ágil atención y solución a percances dentro de la red se establecen los siguientes criterios:

1. Se genera un reporte que permite realizar un seguimiento detallado de la falla, con un tiempo entre 5 y 10 minutos para dar inicio a la evaluación del problema después de ser detectado.
2. La identificación del problema y sus causas conllevarán un tiempo de 25 minutos.
3. Él o los responsables del seguimiento del fallo, se comunicarán con el área afectada en un tiempo no mayor a los 10 minutos, informando el estado del problema presente. Es obligatorio registrar cada actividad realizada para su resolución.
4. El tiempo de resolución de fallos estimado será de 2 horas para devolver el servicio afectado.
5. Él o los responsables estarán en continua comunicación con su superior inmediato informando la totalidad de las actividades realizadas hasta la solución definitiva del fallo. También se considerará los tiempos de traslado hacia los dispositivos problemáticos.
6. Se deberá realizar pruebas de verificación del correcto funcionamiento con un tiempo estimado de 30 minutos para esta tarea.
7. Una vez solucionado el problema se documentará el proceso de resolución.

La Tabla 3-7 resume los tiempos a ser considerados en la resolución de fallos.

PROCESO	TIEMPO ÓPTIMO ESPERADO
Detección – inicio del proceso(registros)	5 a 10 min
Detección de causas	25 min
Comunicación con el área afectada	10 min
Traslado	Quito: 15 min D.A. dentro de instalaciones: 20 min D.A. fuera de instalaciones: 2 horas San Rafael: 1 hora 30 min Sitios Remotos: 3 horas
Solución al Fallo	2 horas a partir de la apertura del registro.
Prueba de verificación	30 min
Notificación y Reporte	30 min

Tabla 3-7.- Tiempos óptimo esperado de respuesta.

3.2.4.2.5. Documentación

Petroproducción cuenta con una amplia y variada lista de equipos de comunicaciones, que van desde switches básicos hasta complejos servidores de aplicaciones, por lo que la correcta documentación de los mismos es necesaria. Con este propósito se deberán registrar los siguientes parámetros mínimos por cada dispositivo en operación.

	PARÁMETRO	DETALLE
Equipo	Equipo: Marca y Modelo	Tipo de Equipo (Switch, Router o Servidor)
	Características de Hardware	Memoria y Procesador
	Características de Software	Sistema Operativo Versión
	Etiquetado	Etiquetas existentes
	Código QC	Inventario Petroproducción
Ubicación Física	Instalación	Edificio (Quito) Campo (D.A.)
	Ubicación	Piso en donde se encuentra ubicado.
	Número de Rack	Etiqueta del rack
	Conexión del Dispositivo	Identificar el dispositivo al cual se conecta (enlace troncal).
Configuración	Dirección IP	IP y máscara, gateway y DNS
	Acceso y Seguridad	Passwords de acceso y usuarios.
	SNMP	Comunidad, usuarios, contacto de administración.

Continúa en la página 111.

	PARÁMETRO	DETALLE
	Configuración de Interfaces	Puertos de acceso, troncales y características particulares.
	Tablas de Enrutamiento	Rutas estáticas, dinámicas y protocolos de enrutamiento.
	Aplicaciones y Servicios	Servicios activos y principales aplicaciones en ejecución.
Registros	Fallos anteriores	Descripción del problema, sus causas y afectados.
	Soluciones aplicadas	Procedimiento y acciones que se tomaron hasta restablecer el servicio.
	Características del fallo	Criticidad, tipo y tiempo de solución

Tabla 3-8.- Parámetros de Documentación

Conjuntamente con la recopilación de datos de los elementos, se encuentra la elaboración de diagramas de topología y elementos de red representando una necesidad para el personal del NOC. El acceso ágil y un entendimiento rápido del estado de la intranet son premisas para la localización y prevención de fallos. A continuación se identifican elementos que deberán estar presentes en los distintos diagramas realizados por el departamento de Redes.

No.	ITEM	DIAGRAMACIÓN
1	**Componentes**	Solamente equipo en Funcionamiento
2	**Símbolo Gráfico**	Normalizado por el departamento
3	**Interfaces**	En funcionamiento y estado activo
4	**Direccionamiento**	Último digito de su dirección IP
5	**Conexiones**	A dispositivos de Networking de Backbone
6	**Identificación**	Acorde a su etiquetado.
7	**Descripción**	Según la importancia dentro del diagrama y para el usuario.

Tabla 3-9.- Componentes de Diagramación

El proceso de documentación logrará identificar soluciones efectivas a problemas similares que se tuvieron en el pasado, ahorrando y disminuyendo el tiempo de respuesta ante la eventualidad y dando una solución comprobada.

Los Registros serán documentados tanto por dispositivos como por servicio interrumpido en la empresa. Los responsables del proceso se asignan en función de la criticidad del problema y de las funciones que desempeñan dentro del NOC. Se debe notificar y detallar lo más exactamente posible los siguientes puntos, estableciendo un nuevo registro de la incidencia:

- Problema o falla surgida.
- Antecedentes
- El lugar donde ocurrió.
- Cuáles fueron las causas que lo ocasionaron.
- Precauciones a tener en cuenta.
- Actividades realizadas para solucionar el problema.
- Si quedó totalmente controlado y corregido.
- Recomendaciones para evitar su reincidencia.

Una exploración rápida debería incluir una revisión del historial documentado de la red para determinar si el problema ha ocurrido antes, y si es así, dónde se anotó la solución. El procedimiento para la documentación de nuevos dispositivos integrantes de la red se presenta en el siguiente diagrama:

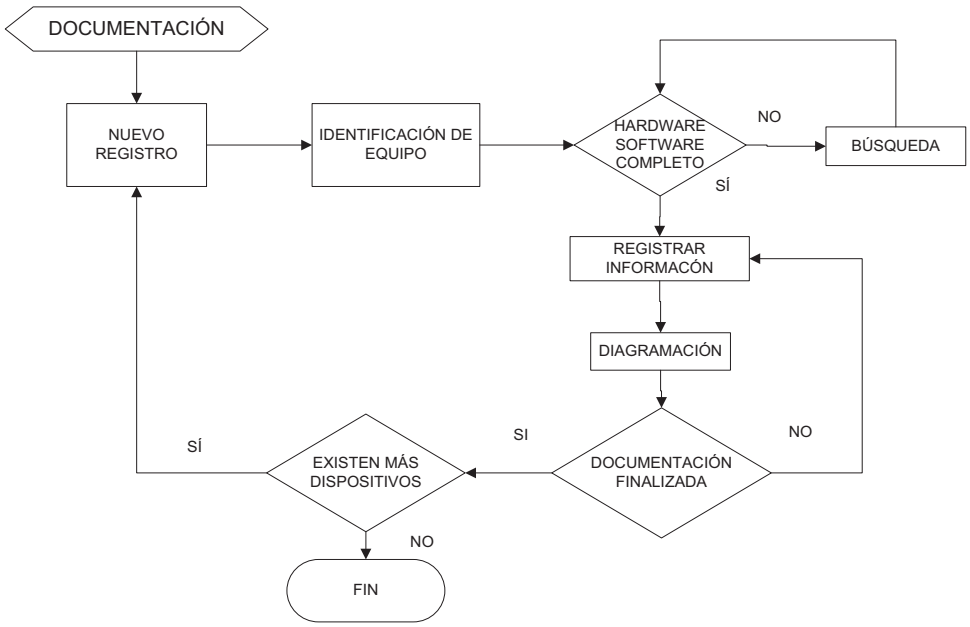


Figura 3-5.- Proceso de Documentación

Para llevar el control de estos parámetros se propone la elaboración de planillas de control y seguimiento a fallas, con tal propósito la Figura 3-6 presenta un modelo de hoja de control.

CONTROL DE EVENTOS - PETROPRODUCCIÓN **No.**

PETROPRODUCCION
FILIAL DE PETROECUADOR

Fecha: Hora:
Realizado por:

Solicitado por: Teléfono:
Instalación:
Ubicación:

Descripción del Problema:

Posibles Causas:

Tipo de Fallo: Red ◯ Servicios ◯ Seguridad ◯ PCs ◯ Otro ◯

Equipo(s) Afectados: _____

Hora Asignada: _____

Criticidad: Ninguna ☐ Baja ☐ Media ☐ Alta ☐ Extrema ☐

Estado: Iniciado ☐ Pendiente ☐ Finalizado ☐

Personal Asignado: _____

Solución:

Hora de Finalización: _____ Tiempo de Solución: _____

Sugerencias:

Firma: _____

Figura 3-6.- Formato de Hoja de Control de Eventos

Una vez establecido el procedimiento de seguimiento a fallos, la **Figura 3-7** presenta el proceso general de resolución de problemas desde su notificación hasta su resolución y posterior documentación.

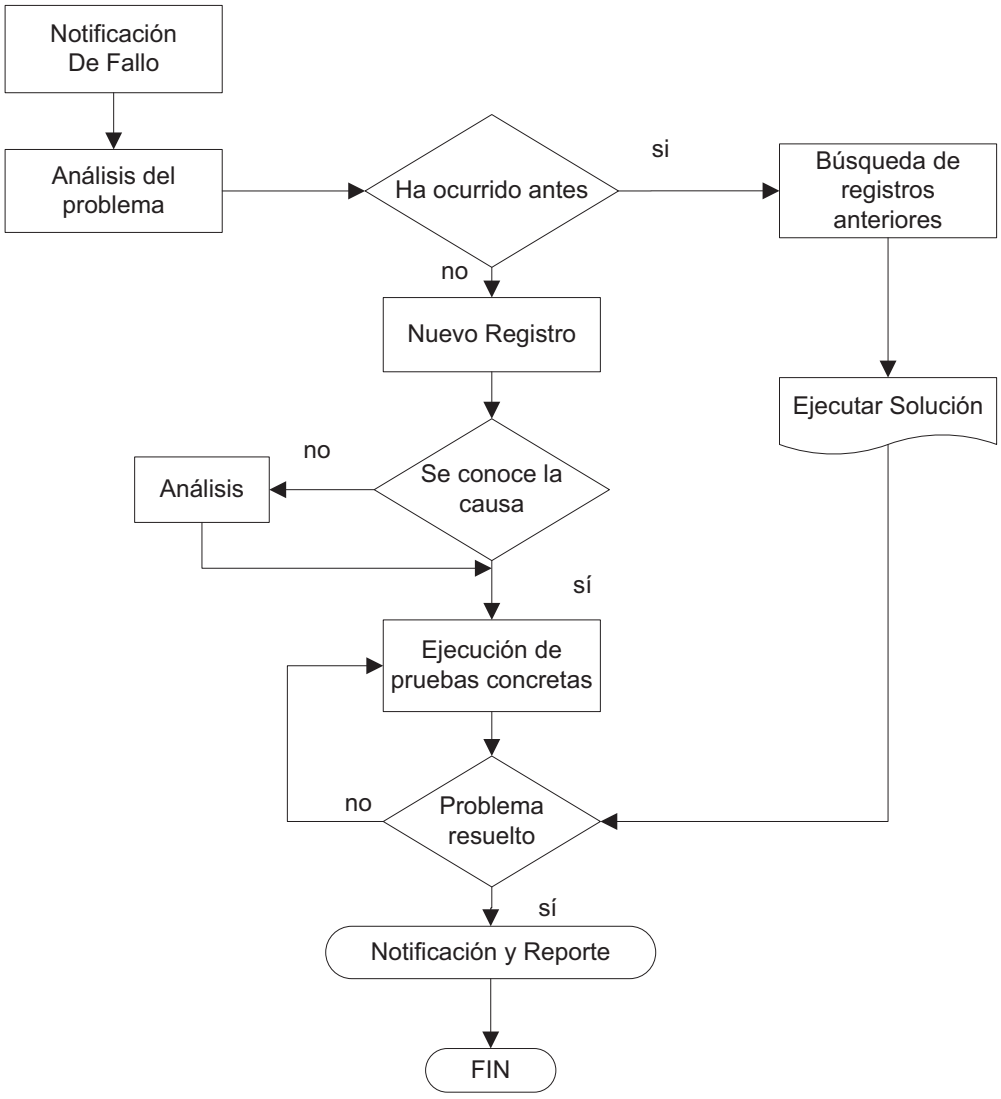


Figura 3-7.- Proceso de Troubleshooting

3.2.4.3. Plan de Contingencia ante Fallos

Uno de los requisitos para resolver problemas en cualquier dispositivo es conocer las reglas bajo las cuales está operando. Se sugiere acciones que pueden ser de gran ayuda ante la presencia de fallas dentro de la red, basados en recomendaciones de casas fabricantes y en función de las características

de la empresa. Al encontrarse la organización bajo una solución basada en switches, se han considerado las siguientes recomendaciones.

a. Tomar el tiempo suficiente para familiarizarse con la operación normal de los dispositivos. Las guías de configuración de los productos son de gran ayuda, muchos casos son resueltos en base a información ya existente.
b. Para fallos más complejos es recomendable disponer del mapa físico y lógico de la red. Permiten mostrar la manera como los cables se encuentran conectados, los segmentos existentes en nuestra red y los routers que brindan enrutamiento. Otros mapas recomendables son: VLANs, STP, entre otros.
c. Algunos problemas y soluciones son obvias, pero otras no. Los síntomas presentes en un área en particular pueden ser el resultado de fallos en otra área. Antes de sacar conclusiones hay que examinar y verificar de una manera estructurada que es lo que trabaja y lo que no. Muchos de los problemas que se presentan están relacionados con la capa física.
d. No asumir que un dispositivo trabaja correctamente, esta premisa puede ahorrar mucho tiempo desperdiciado. No saltarse factores básicos y asumir que algo funciona, alguien pudo haber cambiado algo y no decirlo al personal encargado de resolver la falla.

3.2.4.3.1. Problemas de Conectividad

Los puertos son la base de una red basada en switches, siendo primordial el diferenciar puertos troncales y puertos de acceso. A continuación se describen procedimientos para encarar problemas de conectividad entre dispositivos dependiendo de la clase de fallo que se presente.

i. Fallas de Hardware

a. Identificar el color de luz que corresponde a cada puerto, luz verde corresponde a un puerto funcional y de correcta operación.

b. Revisar los dos extremos de conexión, verificando que el estado de los puertos se encuentre arriba, si un extremo se encuentra arriba y el otro no, el estado del puerto se mostrará cómo no conectado.
c. Revisar la utilización de cables adecuados para conexión entre dispositivos. cable directo, cruzado y fibra monomodo o multimodo, para este último verificar la correcta ubicación de los hilos de recepción-transmisión y estar seguro del tipo de conector en ambos extremos. Con su revisión la luz indicadora es verde y el estado del puerto es *up.*
d. Si el problema no es resuelto se debe verificar otros componentes como:
   - Conversores de medios entre fibra y cobre, pueden estar funcionando indebidamente o generando mucho ruido
   - Chequear el estado de los cables, si están correctamente insertados en los puertos, si poseen suciedad o p*ine*s dañados.
   - Si el cable se encuentra conectado en el puerto incorrecto.
e. Para determinar si el cable es la causa, intercambiar por uno que se esté seguro que funciona correctamente. Para enlaces de larga distancia, disponer de un *cable tester*.

ii. Fallas de Configuración

Se lo identifica por la luz naranja indicativa que el software dentro del equipo ha bajado su puerto de conexión. Se procederá de la siguiente manera:

a. Estar seguro que el administrador no ha bajado el estado del puerto en uno de los extremos.
b. En algunos dispositivos el estado de error se da debido a una falla interna del equipo, se lo puede arreglar levantando la interfaz manualmente.
c. Verificar la correspondiente configuración en cada extremo del enlace, estas deben ser las mismas en velocidad, dúplex, modo troncal, entre otros.
d. Colisiones tardías son generadas por una NIC defectuosa, cables de red demasiados largos y problemas de dúplex (modo de puerto), que es la causa más común. Tener en cuenta la configuración full dúplex y half dúplex.

e. Si se verifica que el enlace es correcto y los puertos muestran conexión pero no existe comunicación con otro dispositivo, el problema excede la capa física, la causa podría encontrarse en capa dos o tres, se recomienda:
   - Chequear que el modo troncal sea el mismo a cada lado del enlace.
   - Verificar protocolos como STP, VTP, entre otros.
   - Asegurarse que el direccionamiento de capa tres se encuentre correctamente configurado.

iii. Fallas del equipo físico

Si se ha realizado todos los procedimientos y la falla persiste, se considerarán desperfectos en el hardware o software del equipo

a. Puertos dañados por electricidad estática.
b. Problemas con el Sistema Operativo del equipo, considerar su reiniciación, actualización o cambio si el dispositivo no funciona adecuadamente.
c. Si las luces del switch son de color naranja, es un indicativo de existencia de problemas en hardware. Antes de cambiar cualquier componente intentar:
   - Resetear el módulo del switch.
   - Reiniciar el equipo.
   - Chequear el software (si hubo nuevas instalaciones).
d. Finalmente remplazar el componente problemático.
e. Para todo esto se debe consultar la guía de configuración del componente.

Debido a que en su mayoría la conectividad de la red se encuentra bajo una solución Cisco, se presenta comandos útiles para la verificación de configuración y funcionamiento de estos dispositivos.

	COMANDO	DETALLE
1	`show versión`	Muestra que versión de software se encuentra en ejecución.
2	`show module`	Muestra los módulos instalados.
3	`show port`	Permite determinar el estado de los puertos, su velocidad y la configuración *duplex*.
4	`Ping`	test de conectividad con otros equipos
5	`show port channel`	Otorga una vista detallada del estado del canal o

Continúa en la página 118.

	COMANDO	DETALLE
	mod/port	de un Puerto en particular.
6	**show spanning-tree**	Verificar la configuración del protocolo STP en el enlace.
7	**show trunk**	muestra el estado de los puertos troncales
8	**show mac**	Permite observar la cantidad de paquetes recibidos y enviados por el Switch.
9	**clear counters**	Encera el contador de paquetes del Switch.
10	**show runing-config**	Permite visualizar la configuración actual del dispositivo.
11	**show interfaces**	Muestra en detalle parámetros de funcionamiento por interfaz.
12	**show post**	Muestra cualquier tipo de error de hardware encontrado.
13	**show interface fa0/0 counters**	Estadísticas de los paquetes enviados y recibidos según el puerto especificado.
14	**show logging**	Vista de los mensajes log almacenados
15	**show cdp neighbors**	Muestra información de los dispositivos vecinos mediante el protocolo propietario de cisco CDP
16	**Show tech-support**	Despliega información técnica de soporte para un proceso de troubleshooting.

Tabla 3-10.- Comandos de Troubleshooting en equipos Cisco.[34]

iv. Problemas de cableado

La Tabla 3-11 hace referencia a diversos problemas que pudiesen estar presentes en los medios de transmisión de la red.

POSIBLE CAUSA	ACCIÓN A TOMAR
Cable no conectado	Conectar el cable en el puerto del switch, router o NIC a un dispositivo bien conocido.
Puerto equivocado	Verificar que los dos extremos se encuentren en los puertos correctos (troncales, para PC´s o para AP´s) y conectados adecuadamente

Continúa en la página 119.

[34]FUENTE:http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015bfd6.shtml

POSIBLE CAUSA	ACCIÓN A TOMAR
Dispositivo sin fuente de poder	Asegurar la conexión a alimentación de energía
Tipo de cable incorrecto	Verificar el tipo de cable utilizado. Solicitar uno de repuesto al área de soporte al usuario.
Cable defectuoso	Remplazar por un nuevo cable. Verificar los daños en el cable remplazado
Patch Panels	Eliminar conexiones que hayan sufrido desperfectos en algún momento.
Conversores de medio	Remplazo, verificación de conexión y puertos. En lo posible evitar el uso de estos dispositivos.
Conectores de interfaces gigabit errados	Cambiar el conector problemático por uno en buenas condiciones. Verificar si el software y hardware del equipo soportan esta clase de conectores.
Puerto o módulo defectuosos	Probar con otros puertos del equipo Usar comandos de diagnóstico para verificar el estado de los puertos. Ver Tabla 3-10.

Tabla 3-11.- Problemas de Cableado

Debido a que el edificio Tribuna dispone también de un cableado de fibra óptica, ante posibles percances se recomienda primero verificar ambos extremos de los enlaces el uso del mismo tipo de conector Gigabit, para ello tener en cuenta que los tipos 1000BASE-T soportan UTP Categoría 5, 5E y 6, mientras que los 1000BASE-SX son destinados para Fibra Multimodo, en este caso es muy importante que los conectores estén correctamente limpios.

A continuación, la Figura 3-8 y la

Figura **3-9.- Proceso para fallos en Configuración**

se modela procesos de resolución a diversos tipos de fallos que puedan presentarse.

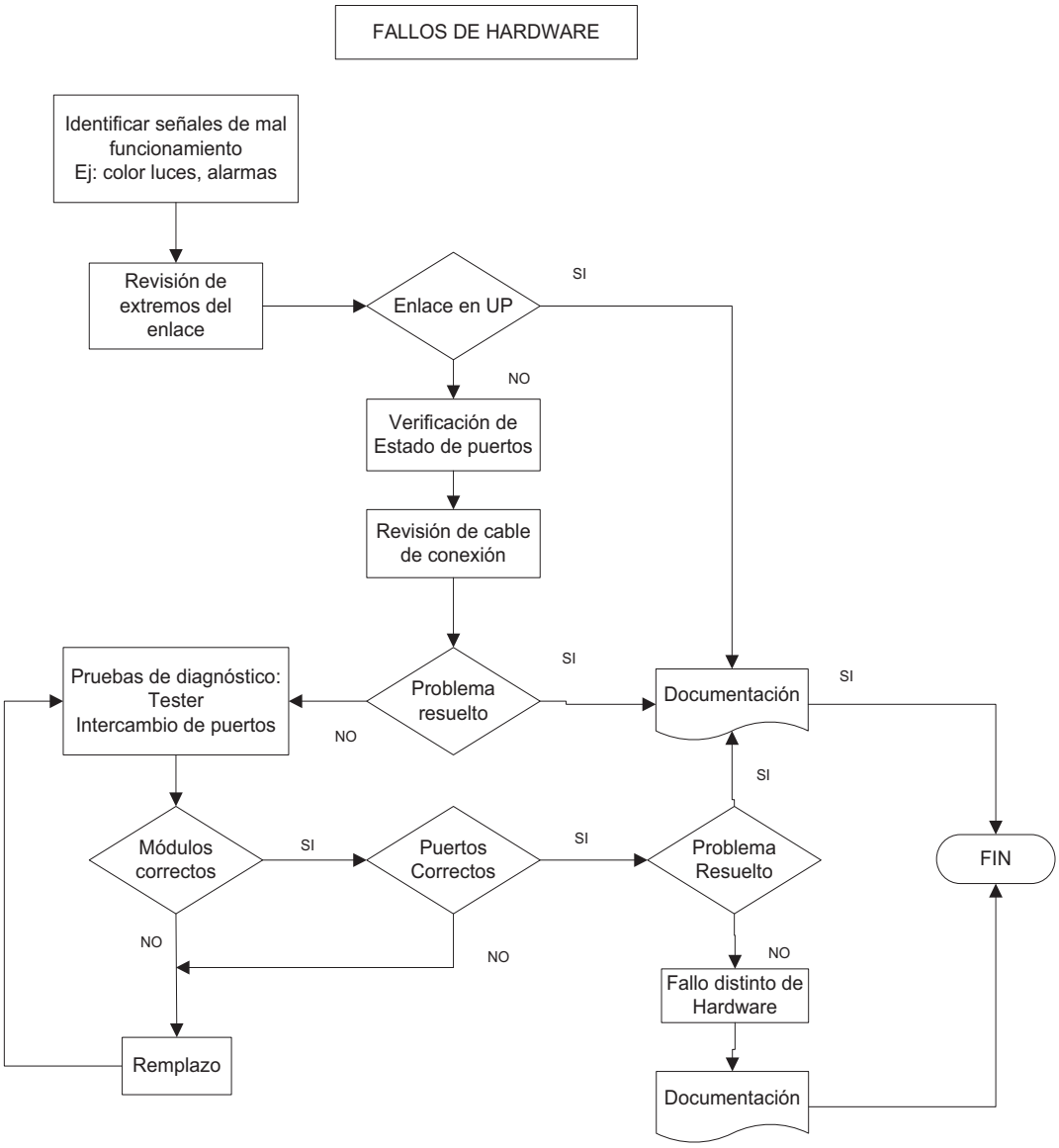


Figura 3-8.- Proceso para fallos en Hardware

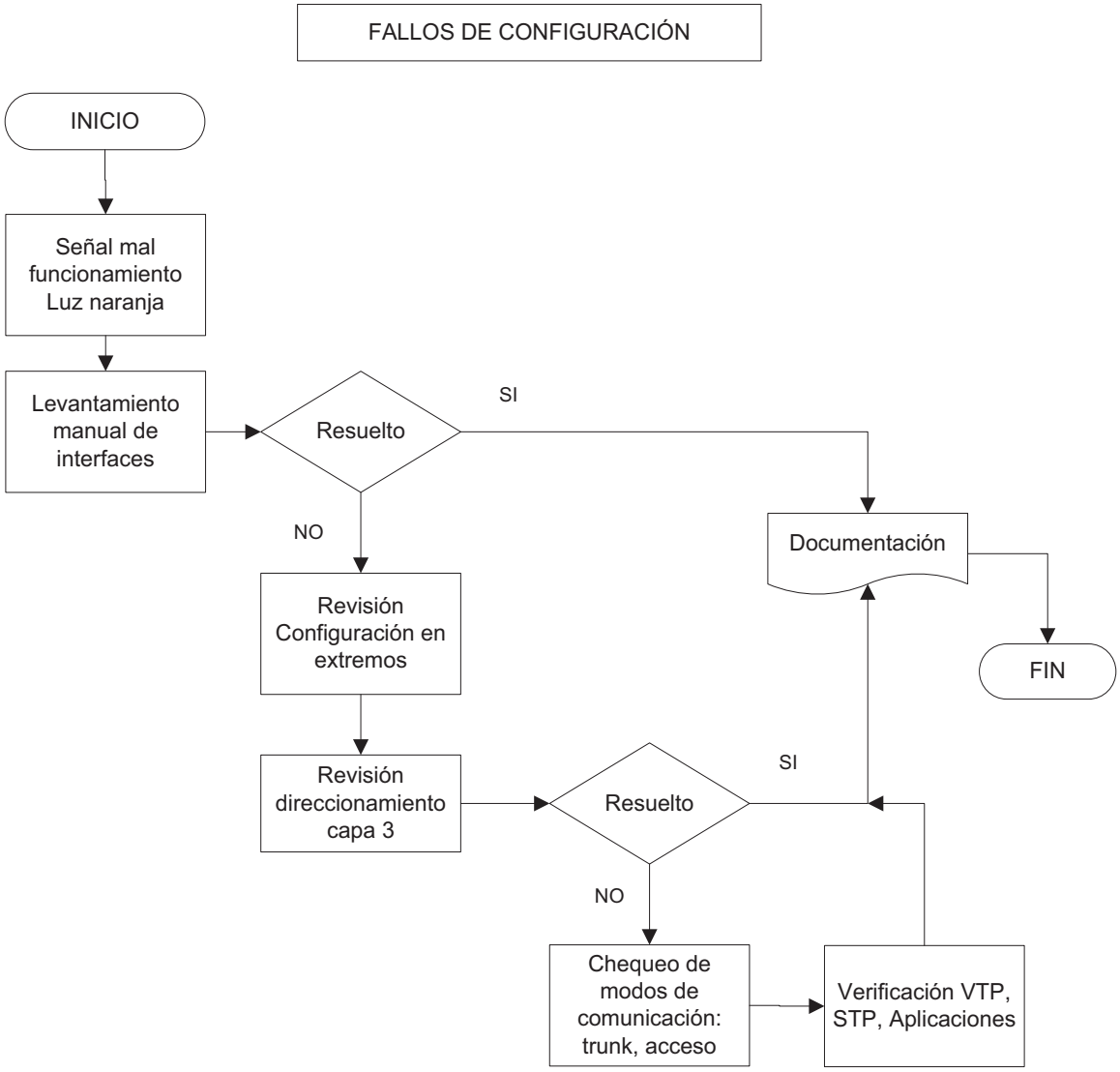


Figura 3-9.- Proceso para fallos en Configuración

3.2.4.3.2. Procedimientos a ejecutar según el fallo

A continuación se establecen procedimientos a seguir por parte del personal del NOC ante la presencia de fallos en distintos elementos de red:

- Ante la presencia de algún fallo, revisar los registros existentes en busca de soluciones comprobadas para dicho problema. De esta manera se ahorrará tiempo valioso en su solución.
- Todas las decisiones y actividades realizadas por el personal a cargo de la solución deben ser notificadas a su superior de manera continua y con la autorización respectiva.
- Después de solucionado el problema, su documentación es indispensable. detallando los parámetros descritos en el punto 0

Se detallan a continuación distintos tipos de fallos que se pudiesen generar, estableciendo su tiempo de solución, responsables y demás características de interés.[35]

Fallo	Fallo de enlace CNT-PEC		
Descripción	Fallo en las comunicaciones hacia el exterior a través del enlace de fibra con la CNT y Petroecuador		
Área afectada	Toda la instalación	**Responsable(s)**	Coordinador NOC Supervisor de Infraestructura
Criticidad	5	**Tiempo Óptimo Solución**	4 horas
Procedimiento a efectuar	a. Verificación del ODF y equipos de CNT. Encendido, tarjetas de red, cable de fibra y transceiver. b. Realizar pruebas de fibra del enlace. c. Comunicación inmediata con el proveedor. d. Establecer un tiempo estimado de recuperación del enlace. e. Informar al personal el tiempo fuera de servicio del enlace.		
Sugerencias	• Verificación continua de logs • Comunicación permanente con Petroecuador, encargada de los contratos con la CNT		

Tabla 3-12.- Procedimiento ante Fallo en Enlace con la CNT

[35] Basado en: NORMA TÉCNICA PERUANA 2007 NTP-ISO/IEC 17799, EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. (EQV. ISO/IEC 17799:2005 Information technology. Code of practice for information security management)

Fallo	Fallo de enlaces de comunicaciones		
Descripción	Fallo en las comunicaciones entre departamentos de Petroproducción		
Área afectada	Departamentos	**Responsable**	Supervisor de Infraestructura Analista de Infraestructura Área de Redes
Criticidad	4	**Tiempo Óptimo Solución**	30 min
Procedimiento a efectuar	a. Comunicación con el área afectada b. Verificación de los extremos del enlace. c. Revisión de los equipos de networking, en cada piso y en cuartos de equipos. d. Identificar posibles causas eléctricas, de configuración, cables entre otros. e. Informar al área afectada el tiempo necesario para la recuperación del enlace. Ver punto 3.2.4.3.1		
Sugerencias	• Revisión continua de la herramienta de monitoreo. • Realización de mantenimiento continuo de enlaces principales.		

Tabla 3-13.- Procedimiento ante Fallo en Enlaces de Comunicación

Fallo	Problemas de Monitoreo Remoto del Dispositivo		
Descripción	El equipo a monitorear no responde a pruebas y peticiones SNMP y no se lo ve desde la consola NMS.		
Área afectada	Administración NMS	**Responsable(s)**	Administrador NMS Soporte de Redes
Criticidad	3	**Tiempo Óptimo Solución**	8 horas
Procedimiento a efectuar	a. Revisión de configuración SNMP del dispositivo: Comunidad, permisos, entre otros. b. Verificación de la consola NMS hacia el equipo defectuoso. Revisión de logs. c. Ejecución de peticiones MIB por medio de consola. d. Reinicio del servicio (agente) SNMP. e. Intentar el reconocimiento manual del agente en la NMS. f. Reconfiguración completa del equipo. (ver Gestión de Configuración)		

Tabla 3-14.- Procedimiento ante Fallo en Administración Remota

<table>
<tr><td>Fallo</td><td colspan="4">Fallo en Switches</td></tr>
<tr><td>Descripción</td><td colspan="4">Anomalías en equipos de switching tanto acceso como distribución provocando pérdida de conectividad con la red.</td></tr>
<tr><td>Área afectada</td><td>Departamento conectado</td><td>Responsable</td><td colspan="2">Supervisión de Infraestructura de Comunicaciones
Área de Redes</td></tr>
<tr><td>Criticidad</td><td>4</td><td colspan="2">Tiempo Óptimo Solución</td><td>1 hora</td></tr>
<tr><td>Procedimiento a efectuar</td><td colspan="4">a. Revisión del enlace en los extremos
b. Revisión general del dispositivo, conexión y fuente de energía. Estado de luces del módulo principal
c. Verificación del estado de los puertos
Luces indicativas
Chequeo de cables y conectores
Chequeo de configuración de puertos troncales y de acceso, protocolo STP, dúplex, entre otros. (Ver punto 3.2.4.3.1)
d. Monitoreo y verificación de la configuración actual
Ejecución de comandos de troubleshooting
(Ver Tabla 3-10). Consulta en guías del fabricante.
e. Pruebas de diagnóstico.- intercambio de puertos, comprobación de enlace mediante Tester.
f. Reinicio de Switch.
g. Remplazo del equipo por uno totalmente probado y configurado.</td></tr>
<tr><td>Sugerencias</td><td colspan="4">• Disponer de acceso restringido a estos dispositivos para evitar cualquier alteración de los mismos.
• Poseer archivos de configuración de respaldo para cargar al dispositivos de remplazo.
• Disponer del software propio del switch, en caso de recarga del IOS.
• Disponer de las guías de configuración dadas por el fabricante.</td></tr>
</table>

Tabla 3-15.- Procedimiento ante Fallos en Switches

<table>
<tr><td>Fallo</td><td colspan="4">Fallo en Switch de Núcleo</td></tr>
<tr><td>Descripción</td><td colspan="4">Anomalías o alarmas generadas en el switch de núcleo de la dependencia, que puedan generar dificultades en el sistema de comunicaciones.</td></tr>
<tr><td>Área afectada</td><td>Toda la Instalación</td><td colspan="2">Responsable(s)</td><td>Coordinador TIC
Supervisor y Analista de Infraestructura de Comunicaciones.</td></tr>
<tr><td>Criticidad</td><td>5</td><td colspan="2">Tiempo Óptimo Solución</td><td>30 min.</td></tr>
<tr><td>Procedimiento a efectuar</td><td colspan="4">a. Revisión general del dispositivo,
Conexión y fuente de energía.
Estado de luces del módulo principal.
b. Verificación del estado de los puertos,
Luces indicativas,
Chequeo de cables y conectores,
Chequeo de configuración de puertos troncales y de acceso, protocolo STP, dúplex, entre otros. (Ver punto 3.2.4.3.1)
c. Monitoreo y verificación de la configuración actual.
Ejecución de comandos de troubleshooting (Ver Tabla 3-10).
Consulta en guía del fabricante.
d. Pruebas de diagnóstico
e. Reinicio de Switch fuera de las horas laborables
f. Si fuese el caso: evaluación de la capacidad operativa del Switch y análisis de la adquisición de componentes nuevos.</td></tr>
<tr><td>Sugerencias</td><td colspan="4">• Disponer de acceso restringido a estos dispositivos para evitar cualquier alteración de los mismos.
• Poseer archivos de configuración de respaldo para cargar al dispositivo.
• Actualización periódica de sistema operativo del equipo.
• Mantenimiento preventivo permanente.</td></tr>
</table>

Tabla 3-16.- Procedimiento ante Fallo en Switch de Núcleo

Fallo	Fallo en Routers			
Descripción	Anomalías en equipos de enrutamiento que provocan pérdidas de información			
Área afectada	Instalación	**Responsable(s)**	Supervisión de Infraestructura de Comunicaciones. Área de Redes	
Criticidad	5	**Tiempo Óptimo Solución**		30 min
Procedimiento a efectuar	a. Diagnóstico físico del dispositivo Interfaces, conexiones seriales y Ethernet, conexión a fuente de energía. Chequeo de cables, conectores y estado de luces indicativas b. Monitoreo y verificación de la configuración actual Ejecución de comandos de troubleshooting (Ver Tabla 3-10) Consulta en guías del fabricante. c. Verificación de tablas de enrutamiento y protocolos usados. d. Pruebas de diagnóstico e. Reinicio del Router. f. Remplazo del equipo por uno totalmente probado y configurado fuera del horario laboral.			
Sugerencias	• Disponer seguridad de acceso al equipo. • Poseer archivos de configuración de respaldo. • Disponer del IOS de respaldo del switch. • Disponer de las guías de configuración dadas por el fabricante. • Adquirir módulos de repuesto (Tarjetas seriales, tarjetas Gigabit Ethernet, FXS, FXO, entre otros.)			

Tabla 3-17.- Procedimiento ante Fallo en Routers

Fallo	Robo de equipos Informáticos			
Descripción	Pérdidas de equipos informáticos y dispositivos de comunicación a cargo del NOC.			
Área afectada	NOC	**Responsable**	Coordinador de NOC Supervisión de Seguridad Tecnológica Asistente de Seguridad tecnológica	
Criticidad	5	**Tiempo Ópt. Solución**		48 horas para su reposición
Procedimiento a efectuar	a. Dependiendo del caso, informar a los usuarios el tiempo de suspensión del servicio afectado.			

Continúa en la página 127.

	b. Instalar equipos de respaldo. c. Restaurar la información de respaldos existente. d. Restablecer los servicios. e. Informar a los usuarios los acontecimientos y la fecha hasta la cual se recuperó la información. f. Comunicación con Activos para la adquisición de nuevos equipos.
Sugerencias	• Cumplir con las políticas y controles de seguridad. • Verificación continua del sistema de respaldos de la empresa • Restringir el acceso de personas no autorizadas.

Tabla 3-18.- Procedimiento ante Robo de Equipos

Fallo	Problema Eléctrico			
Descripción	Corte del suministro eléctrico en las instalaciones			
Área afectada	Toda la instalación	**Responsable(s)**	Coordinador del NOC.- Encargado de coordinar el procedimiento	
Criticidad	5	**Tiempo Ópt. Solución**		10 min
Procedimiento a efectuar	a. Comunicación con el encargado del suministro eléctrico. b. Verificar el estado de carga de los UPS. c. Apagar los equipos que no son indispensables. d. No encender dispositivos que son poco cruciales y no indispensables. e. Verificar el suministro eléctrico alterno. • Comunicación al personal • Encendido			
Sugerencias	• Verificar continuamente el estado de los UPS aunque no sean utilizados • Disponer de sistemas de energía de respaldo en cada piso de las instalaciones.			

Tabla 3-19.- Procedimiento ante Fallo Eléctrico

Fallo	Fallo en discos duros de servidores			
Descripción	Reporte de anomalía en el disco duro de un servidor Al tener arreglos de discos RAID, los datos se pueden recuperar.			
Área afectada	Integridad de Información	**Responsable(s)**	Supervisor de Datos Analista de Datos	
Criticidad	5	**Tiempo Ópt. Solución**		24 horas
Procedimiento a efectuar	a. Solicitar al departamento de adquisiciones la compra de discos de similares características. b. Establecer un horario para el cambio de discos. c. Informar al personal sobre la suspensión del servicio (si fuese el caso) para efectuar el remplazo. d. Verificar el correcto funcionamiento			
Sugerencias	• Revisión continua de logs del sistema • Mantenerse en contacto con los proveedores de servidores para contratos de mantenimiento. • Sacar respaldo continuamente de los servidores.			

Tabla 3-20.- Procedimiento ante Fallo en Discos Duros

Fallo	Problemas de temperatura en cuartos de equipos			
Descripción	Fallo en el sistema de aire acondicionado ocasionando dificultades en servidores y dispositivos del cuarto de equipos.			
Área afectada	NOC	**Responsable**	Supervisor - Analista de Seguridad Tecnológica Supervisor – Analista de Infraestructura	
Criticidad	3	**Tiempo Ópt. Solución**		2 días
Procedimiento a efectuar	a. Comunicación con el encargado del mantenimiento del aire acondicionado. b. Disponer de ventiladores temporales que proporcionen ventilación a equipos críticos. c. Comunicación con Adquisiciones para la compra de un nuevo equipo si fuese el caso.			
Sugerencias	• Mantenimiento constante del equipo de aire acondicionado. • Tener a disposición equipos de repuesto en bodega y ventiladores convencionales en caso de emergencia. • Disponer de garantía para posibles equipos afectados.			

Tabla 3-21.- Procedimiento ante Problemas de Temperatura.

Fallo		Ataques internos	
Descripción		Ataques de usuarios mal intencionados que provoquen pérdida de información o la baja de un servidor.	
Área afectada	Servicios de red	**Responsable(s)**	Coordinador del NOC Supervisión de Seguridad Tecnológica.
Criticidad	4	**Tiempo Ópt. Solución**	1 día
Procedimiento a efectuar	a. Informar a los usuarios del tiempo de suspensión del servicio en cuestión. b. Restaurar el último respaldo de información. c. Dar seguimiento a logs y datos recogidos por equipos de seguridad y control de tráfico. d. Dar seguimiento hasta encontrar la causa del percance. e. Cubrir la seguridad afectada.		
Sugerencias	• Cumplir con las políticas y controles de seguridad. • Verificación continua del sistema de respaldos de la empresa • Dar a conocer a los usuarios sobre sus responsabilidades, obligaciones en el manejo de su información y de las sanciones existentes si se incumplen las mismas.		

Tabla 3-22.- Procedimiento ante Ataques internos.

3.2.5. DISEÑO DEL COMITÉ DE SEGURIDAD

El presente apartado, tiene como objetivo ser una guía para la implantación de un Comité de Seguridad de la Información que dé comienzo al desarrollo de normativas organizacionales y prácticas efectivas de seguridad. Las recomendaciones que se establecen en este capítulo serán de libre elección y uso de acuerdo a las pretensiones del personal integrante del NOC. Se presentan puntos a considerarse basados en la norma 17799:2005 (ISO 27002) como:

- Descripción de la problemática.
- Planeamiento del comité de seguridad.
- Factores de éxito del sistema de seguridad.

3.2.5.1. Descripción de la Problemática

Un lineamiento base para un Sistema de Seguridad se justifica en la presencia de fallos tanto en la red como en su infraestructura. El desarrollo de normas de seguridad será beneficioso y eficaz si es sustentado en base a una normativa adecuada. Petroproducción actualmente presenta inconvenientes en el área de gestión de seguridad, algunos de los problemas que presenta son:

- No se cuenta con políticas de seguridad establecidas ni algún tipo de documentación que permita gestionar y definir lineamientos base en la gestión de seguridad en la empresa.
- El acceso a espacios de importancia para las comunicaciones como cuartos de equipos y racks de distribución no cuenta con una restricción formal, haciéndolos susceptibles a accesos no autorizados.
- La documentación de aspectos como manejo de contraseñas, direccionamiento de equipos, usuarios, restricciones y políticas normativas es escasa.
- No se cuenta con alguna herramienta de administración que permita el monitoreo de los dispositivos integrantes de la red, detección de fallas, anomalías en equipos y posibles ataques en un tiempo oportuno.
- No se toma a la información como un activo empresarial que merece la suficiente protección.

3.2.5.2. Planeamiento del Comité de Seguridad

La información es un activo crítico en el funcionamiento de la institución, su cuidado y protección deben ser tomados en cuenta desde los niveles gerenciales hasta los operativos.

"La información es un activo, que tal como otros importantes activos del negocio, tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente"[36].

Desde este punto de vista se propone establecer un marco organizacional a través de un Comité de Seguridad para iniciar, controlar e implementar un Sistema de Seguridad de la Información dentro de la empresa. La Figura 3-10 muestra la propuesta definiendo sus integrantes que garanticen la dirección, el apoyo y una apropiada asignación de recursos al Sistema de Seguridad.

Figura 3-10.- Esquema Organizacional de Seguridad

Supervisor de Seguridad.- Elaborará la documentación pertinente en aspectos de seguridad, coordinará su implementación y realizará una evaluación de la misma.

Coordinador NOC.- Encargado de la gestión de equipos y aplicaciones de la red interna de la empresa, presta su apoyo al Área de Seguridad para la elaboración y ejecución de lineamientos básicos.

Responsable de Activos.- Encargado de velar por la seguridad física de los activos informáticos dentro de las instalaciones de la empresa. Está representada por el área de activos y el servicio de vigilancia y seguridad.

[36] ISO/IEC 17799:2005 (ISO/IEC 27002:2005)

3.2.5.3. Factores de éxito del Sistema de Seguridad.

El éxito en la implementación de la seguridad estará ligado a:

- Apoyo y compromiso de la Vicepresidencia y de los niveles gerenciales.
- Comunicación eficaz con todas las gerencias.
- Distribución de políticas y normas de seguridad a todos los empleados.
- Buscar el compromiso, la cooperación y colaboración de gerentes, usuarios, administradores, auditores y personal de seguridad, además de expertos en áreas como seguros y administración de riesgos.
- Iniciar programas de concientización e Información a los usuarios.
- Comunicación ágil y eficaz por parte de usuarios de los eventos y debilidades en la seguridad de la información.
- Dar a conocer a los usuarios los puntos de contacto donde pueden reportar los incidentes de seguridad.
- Dar mantenimiento en periodos determinados a los equipos de networking.

Los roles de cada miembro del comité se describen más adelante en el punto “Roles de los Integrantes del Comité de Seguridad” (Página 139).

3.3. ESTRUCTURA JERÁRQUICA DE RESPONSABILIDADES

Con la finalidad de establecer los roles que desempeñará el personal del NOC, es necesario saber la estructura organizativa que tendrá el Centro, la propuesta planteada se exhibe en la Figura 3-11.

A partir de su estructura, cada elemento del NOC cumple con una asignación de funciones y responsabilidades (complementarias a las existentes en la actual Coordinación TIC, detalladas en las tablas del ANEXO C).

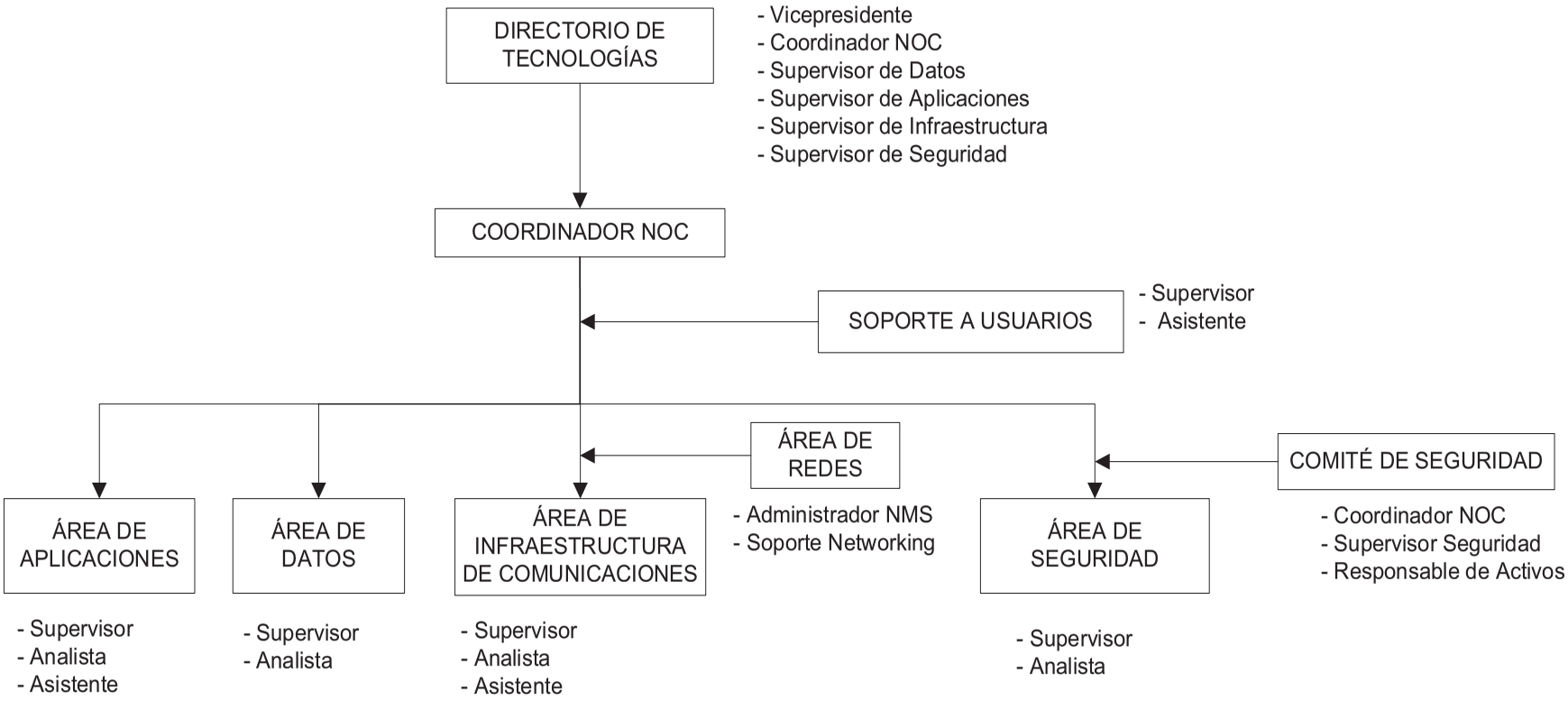


Figura 3-11.- Estructura Jerárquica del NOC

Se propone una adaptación a la estructura ya existente (presentada en el ANEXO C) donde se incorpore las funciones de los Administradores del NOC, esto debido a la reciente reestructuración administrativa y organizacional de la empresa y del personal en el área de TIC.

La gestión del NOC abarca nuevas responsabilidades y un conjunto de obligaciones actualmente repartidas dentro de los diferentes cargos que existen en cada área, las responsabilidades que tiene el personal actualmente se pueden apreciar en el anexo antes mencionado.

La implantación del NOC implica un trabajo en equipo para la gestión del Centro. Es así que éste abarcará las mismas áreas establecidas actualmente para la Coordinación TIC e incorporará un nuevo segmento que complementará la gestión de la red denominada “Área de Redes”, necesaria para el manejo, monitoreo de la consola NMS y que garantice la funcionalidad del equipamiento de networking existente.

Además para tratar temas y decisiones referentes a seguridad, un comité de seguridad es planteado a fin de brindar apoyo al Área de Seguridad. Como ente jerárquico superior se encuentra el Directorio de Tecnologías que es la cabeza del NOC en todo aspecto administrativo. A continuación se detallan las funciones de cada integr6ante dentro del Centro

.

3.3.1. RESPONSABILIDADES DEL PERSONAL

En referencia a la Figura 3-11 se plantea la creación del “Área de Redes”, encargada de administrar y controlar el funcionamiento, configuración, estado de los elementos de networking de la empresa y gestión del sistema de monitoreo de red. A continuación se especifican las distintas funciones que deberá cumplir el personal integrante del centro NOC.

3.3.1.1. Directorio de Tecnologías

Toma decisiones de gran relevancia dentro de las Tecnologías de la Información de la empresa. Los integrantes que lo conforman son:

3.3.1.1.1. Vicepresidente

Autoridad de nivel superior encargada de cumplir y hacer cumplir las normativas tecnológicas desarrolladas para Petroproducción.

Como máximo ente gerencial, está a cargo de las direcciones administrativas y del recurso humano, brindando apoyo activo que demuestre su compromiso y enfoque empresarial hacia la gestión de seguridad.

3.3.1.1.2. Coordinador del NOC

Las funciones desempeñadas y asignadas actualmente se encuentran detalladas en la tabla C-1 del Anexo C.

- Coordinar y administrar todas las áreas que pertenezcan al Centro de Operaciones de Red en función de las necesidades tecnológicas de la empresa.
- Gestionar la administración del NOC haciendo cumplir las responsabilidades del personal
- Planificar y someter a aprobación las políticas para el desarrollo e implementación de sistemas de información, sistemas de comunicaciones y la adquisición e implementación de software, así como del fortalecimiento de la infraestructura computacional y de comunicaciones.
- Establecer y mantener actualizados políticas, normas y estándares de tecnologías de información y comunicaciones para Petroproducción.
- Gestionar la capacitación integral y profesional del personal del NOC.

3.3.1.2. Área de Aplicaciones

3.3.1.2.1. Supervisor de Aplicaciones

- Analizar las necesidades de aplicaciones informáticas de los diferentes departamentos y ejecutar proyectos que den solución a las mismas.
- Implantar planes de seguridad en aplicaciones.
- Estudiar, establecer y evaluar las pruebas a realizarse para detectar posibles problemas de funcionamiento.
- Cumplir con la gestión de fallos de la empresa, en aplicaciones y servicios que corren en la red.
- Establecer reglas y derechos de cada usuario o grupo de usuarios, sus requisitos de seguridad y asignación de privilegios.

3.3.1.2.2. Analista de Aplicaciones

- Diseñar, programar e implementar aplicaciones informáticas.
- Ejecutar planes de seguridad de la información de las aplicaciones.
- Analizar y ejecutar pruebas para detectar los problemas de funcionamiento de servicios empresariales.
- Mantener el control de software y servicios que corren y funcionan en la red, dando a cada usuario solo las aplicaciones necesarias para la realización de su trabajo con su respectiva licencia de funcionamiento.

3.3.1.2.3. Asistente de Aplicaciones

- Llevar el control de las incidencias de las diferentes aplicaciones y notificarlas a su superior.
- Implementar aplicaciones y capacitar a los usuarios en las mismas.

3.3.1.3. Área de Datos

3.3.1.3.1. Supervisor de Datos

- Coordinar, implementar y ejecutar proyectos de expansión de bases de datos y respaldos de información.
- Implantar planes de seguridad para datos
- Estudiar, establecer y evaluar las pruebas a realizarse para detectar posibles inconsistencias en la información.
- Analizar y especificar el alcance, factibilidad e implantación de nuevas herramientas para el almacenamiento y administración de datos.
- Administrar y optimizar las bases de datos.

3.3.1.3.2. Analista de Datos

- Administrar, crear y mantener las bases de datos empresariales aplicando políticas de seguridad de información
- Ejecutar planes de seguridad de la administración de los datos.
- Analizar y ejecutar pruebas para detectar los problemas de integridad y consistencia de la información.
- Realizar periódicamente respaldos de la información que permitan a la empresa recuperarse tras un fallo, realizando pruebas de restauración junto con registros de copias de seguridad y un sistema de documentación.
- Capacitar, asesorar y asistir en la organización de los datos.

3.3.1.4. Área de Infraestructura de Comunicaciones

3.3.1.4.1. Supervisor de Infraestructura de Comunicaciones

- Identificar y brindar soluciones a necesidades de comunicaciones asegurando la disponibilidad y confiabilidad de servicios que corren en Petroproducción.
- Establecer, evaluar y ejecutar las pruebas para detectar problemas de funcionamiento en infraestructura.
- Cumplir y hacer cumplir las políticas de buen uso de la infraestructura de red.

- Implantar los planes de seguridad y contingencia elaborando planes de mantenimiento preventivo y correctivo

3.3.1.4.2. Analista de Infraestructura

- Implantar y documentar soluciones de infraestructura.
- Diseñar y ejecutar sistemas de pruebas para detectar problemas de funcionamiento y analizar los resultados.
- Ejecutar planes de mantenimiento preventivo y correctivo.
- Garantizar la disponibilidad y confiabilidad de los servicios de infraestructura.

3.3.1.4.3. Asistente de Infraestructura

- Implantar las diferentes soluciones de infraestructura y brindar mantenimiento a las mismas.
- Llevar el control de las incidencias de los equipos y reportar a su superior.
- Ejecutar planes de mantenimiento preventivo y correctivo de la infraestructura.

3.3.1.5. Área de Redes

3.3.1.5.1. Administrador de la NMS

- Administrar y coordinar el proceso de monitoreo de la red empresarial.
- Asegurar el correcto funcionamiento de la NMS.
- Programar nuevas alarmas necesarias para el control de la red.
- Adecuar la NMS según los protocolos que se requieran para controlar un nivel aceptable de performance de la red.
- Añadir nuevos dispositivos a la herramienta de administración en función de su ingreso a la intranet y habilitar las interfaces a ser monitoreadas.
- Monitorear constantemente la capacidad operativa de la red y de sus elementos asegurando su correcto funcionamiento.

3.3.1.5.2. Soporte de Networking

- Realizar una evaluación del funcionamiento de la red actual, sus características y brindar soluciones de mejoramiento.
- Establecer actualizaciones y nuevas soluciones de infraestructura, de acuerdo al avance de la tecnología y de los cambios informáticos.
- Configurar equipos de networking que se añaden a la red, corroborando su buen funcionamiento, seguridad y monitoreo remoto desde la NMS.
- Mantener el cableado estructurado de la organización en excelente estado, con referencia a normas internacionales, como EIA 568 B y EIA 606.
- Mantener actualizado el inventario de equipos de infraestructura
- Implantación de nuevos puntos de red según la necesidad.
- Implantar los planes de seguridad y contingencia de la sección.
- Realizar un mantenimiento continuo de los equipos de Red.
- Gestionar las garantías de los equipos de networking de la organización en caso que se requieran.

3.3.1.6. Área de Seguridad

3.3.1.6.1. Supervisor de Seguridad

- Coordinar y diseñar políticas de seguridad de información y planes de contingencia para las comunicaciones empresariales.
- Identificar riesgos y amenazas para la información. Además definir qué información debe ser protegida y el uso de la misma.
- Definir los controles necesarios para protección de información (gestión de contraseñas, métodos de autenticación apropiados, entre otros).
- Definir Acuerdos de confidencialidad con términos legales ejecutables que protejan la información crítica necesaria para la empresa.
- Estudiar el mercado informático en referencia a nuevas herramientas que puedan ser implantadas en Petroproducción.

- Asegurarse que el usuario tenga conocimiento de los temas y responsabilidades de la seguridad de la información y dar a conocer los puntos de contacto donde se reporten los incidentes.
- Establecer responsabilidades y procedimientos que aseguren una respuesta óptima a los incidentes de seguridad.
- Verificar los perímetros de seguridad que protegen los recursos y activos, cuenten con barreras, restricciones y mecanismos de acceso adecuados.
- Conservar la integridad y seguridad de la información de la organización siguiendo recomendaciones de estándares como ISO 27000 o mediante guías COBIT o ITIL y en base a objetivos previamente establecidos por el NOC.

3.3.1.6.2. Analista de Seguridades

- Realizar pruebas para detectar posibles fallas de seguridad tecnológica, evaluar los incidentes reportados y preparar informes de resultados.
- Implantar, administrar y dar mantenimiento a las herramientas para seguridad tecnológica en su ámbito de acción (firewalls, sistemas de detección de intrusos, entre otros) así como sus licencias, elaborando la documentación inherente.
- Controlar el acceso a sitios restringidos y puntos críticos de la red, además gestionar los permisos y accesos a la información.
- Ejecutar las políticas de seguridad establecidas.
- Analizar los requerimientos de seguridad tecnológica.
- Implantar medidas para la mitigación de software malicioso, política de licencias de software y prohibición del uso de software no autorizado.

3.3.1.7. Comité de Seguridad

Para su establecimiento, es necesaria la definición de funciones de cada integrante. Para tal propósito se propone lineamientos en base a la normativa ISO 27002 que enumera clausulas y roles que se deberán seguirse.
Las cláusulas tienen referencia a temas tratados en el estándar como:

a. Organización de seguridad de información.
b. Gestión de activos.
c. Seguridad en recursos humanos.
d. Seguridad física y ambiental.
e. Control de acceso.
f. Gestión de incidentes de los sistemas de información.

Al ser un ente conformado por varios integrantes, todos ellos coordinarán y darán cumplimiento en conjunto a las siguientes premisas:

- Definir los objetivos y el alcance de la Seguridad de la Información y su importancia dentro de Petroproducción.
- Formular, revisar, aprobar y evaluar políticas, dando direcciones claras y un apoyo visible en la asignación de recursos.
- Determinar necesidades de asesoría externa a una fuente de consulta especializado en materia de seguridad de la información.
- Definir responsabilidades claras de cada integrante dentro del plan de seguridad y de las políticas establecidas.
- Proponer y coordinar la realización de un análisis de riesgos formal en seguridad de la información.
- Generar Políticas de seguridad para usuarios, manejo de información en la empresa y nuevos Planes de Respuesta a Incidentes.
- Establecer reuniones regulares de todas las áreas integrantes del NOC.

3.3.1.7.1. Roles del Responsable de Activos

- Definir responsabilidades de los usuarios con los activos informáticos que se les entregue y que el individuo haga uso.
- Determinar el cumplimiento o no de las responsabilidad delegadas.
- Nombrar responsable(s) de cada activo quien responderá por su utilización o negligencia con el dispositivo.
- Documentar los detalles de asignación de responsabilidad y autorización.
- Realizar el inventario de los activos informáticos.

3.3.1.8. Soporte al Usuario

3.3.1.8.1. Supervisor de Soporte al Usuario

- Definir niveles de acuerdo de servicio (SLA) para los diferentes reportes de incidentes.
- Supervisar la actualización de la base del conocimiento generada por los reportes de incidentes.
- Informar a la sección de infraestructura cambios en la red (traslado de equipos, equipos sin inventariar, entre otros).

3.3.1.8.2. Asistente de Soporte al Usuario

- Monitorear el estado operativo de equipos tecnológicos de oficina.
- Atender los incidentes reportados por los usuarios.
- Instalar, configurar y actualizar las aplicaciones de computadores personales.
- Instalar, configurar y dar soporte de periféricos y dispositivos tecnológicos.

3.3.1.9. Roles de los Usuarios

- Asegurar que el activo entregado esté acorde con las instalaciones y el trabajo desempeñado.
- Aceptar los términos y condiciones que establecerán sus obligaciones dentro del Sistema de Seguridad.
- Aceptar los acuerdos de confidencialidad y de no divulgación antes de obtener acceso a recursos que lo ameriten.
- Retornar todos los activos de su posesión en la finalización de su contrato, de igual forma sus derechos de acceso, documentación, equipos y otros activos empresariales.
- Cambiar periódicamente todo tipo de contraseña de acceso.
- Cumplir con sus responsabilidades en el mantenimiento de las medidas de control de acceso y seguridad puestos a su disposición.

3.3.2. PERFIL DEL PERSONAL DEL ÁREA DE REDES

Ante la presencia de una nueva área dentro de la estructura de la actual Coordinación TIC, será necesaria la presencia de nuevos integrantes que conformarán en conjunto con el personal existente el Centro NOC. De esta manera se determinan las aptitudes y habilidades que deberán cumplir los candidatos a integrantes del Área de Redes.

Los criterios de selección son elaborados según requerimientos actuales en el sector de tecnologías de la información y apoyados en el "Manual de Clasificación de Cargos"[37] de la empresa.

APTIDUDES	
Administrador de Red (Administrador de la NMS)	**Soporte de Networking (Técnico de Redes)**
Instrucción Formal	
• Título en Ingeniería de Sistemas o Electrónica.	• Título de Tecnólogo en Computación, Informática o Electrónico
Conocimientos Técnicos	
• Conocimientos en Sistemas Operativos Linux y Windows a nivel de administrador. • Conocimientos en bases de datos y lenguajes de programación. • Conocimientos en redes LAN, WAN y WLAN. • Manejo de stack de protocolos de comunicación TCP/IP. • Conocimientos en configuración y gestión de equipos de Networking. (Certificación Cisco CCNA, deseable CCNP). • Inglés técnico	• Conocimiento en Sistemas Operativos Linux y Windows a nivel de usuario. • Mantenimiento y ensamblaje de computadores y periféricos. • Conocimientos en redes LAN, WAN y WLAN. • Manejo de stack de protocolos de comunicación TCP/IP. • Conocimientos en configuración de equipos de Networking. (Deseable certificación CCNA Cisco). • Cableado estructurado. • Inglés

Continúa en la página 144.

[37] RRHH Petroecuador: Instrumento Administrativo que contiene las áreas de gestión, grupos ocupacionales y cargos, que describen las funciones y el perfil requerido para el desempeño de cada uno de los cargos, acorde a la realidad ocupacional, avance tecnológico y proyección de la empresa.

APTIDUDES	
Administrador de Red (Administrador de la NMS)	**Soporte de Networking (Técnico de Redes)**
Habilidades Personales	
• Capacidad de resolución a problemas y evaluación de soluciones. • Pro actividad, habilidades de planeación y organización. • Trabajo en equipo y bajo presión. • Manejo de grupos. • Habilidades de comunicación y negociación.	• Excelentes habilidades técnicas. • Capacidad de resolución a problemas. • Pro actividad, habilidades de organización y comunicación. • Trabajo bajo presión y en equipo.
Experiencia	
• Experiencia en el Área de 3 años • Administración de redes empresariales. • Manejo de servidores en plataformas Windows y Linux. • Dirección de equipos de trabajo. • Gestión de equipos switches, routers, firewalls, entre otros.	• Experiencia en el Área de 2 años • Trato con usuarios finales. • Soporte técnico. • Configuración de equipos de conectividad como Switches, Routers, Access Points.

Tabla 3-23.- Perfil del Personal - Área de Redes

3.4. DISEÑO DE INFRAESTRUCTURA

Para la implementación del NOC se requieren elementos adicionales a la infraestructura actual, que permitan la gestión de red y herramientas eficaces para administrarlo.

3.4.1. SELECCIÓN DE HERRAMIENTAS SOFTWARE

Como muestra de la tendencia existente a la incorporación de software libre por parte de las entidades públicas del Ecuador, proponemos el empleo del mismo para este proyecto, aprovechando las facilidades que ofrece como: robustez, soporte, flexibilidad y seguridad a bajos costos.

Con el fin de brindar una solución con software libre, se empleará el sistema operativo Linux, lo que conlleva a la realización de un estudio con el objetivo de encontrar la distribución más conveniente para este proyecto, así como la herramienta de monitoreo que cumpla con los requerimientos de la red.

3.4.1.1. Selección de la Distribución Linux

En base a la encuesta detallada en el Anexo B y recogiendo el estudio en base a la norma IEEE 830 para la selección de software realizada en el proyecto de titulación referenciado[38], se requiere un sistema operativo con las siguientes características:

- Posea funcionalidades propias del sistema Linux.
- Robusto y estable basado en software OPEN SOURCE, de acuerdo con la licencia GNU-GPL o similar.
- Posea un gran repositorio y amplias fuentes de soporte.
- Permita la instalación, configuración e implementación de herramientas para gestión de la red.
- Posea un nivel de seguridad, que garantice un acceso restringido al núcleo del sistema.
- El software debe tener versiones estables distribuidas públicamente.

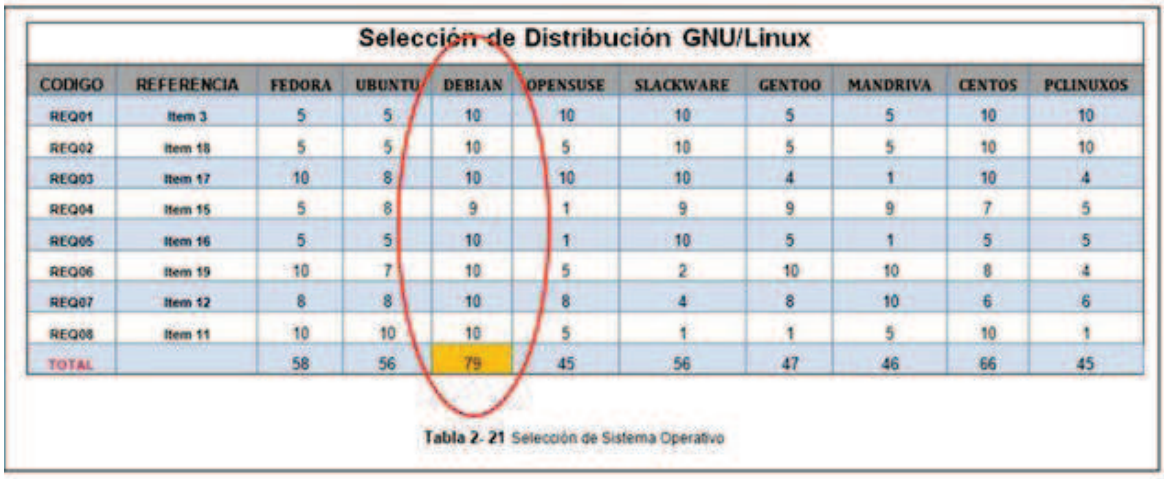
Se escoge la distribución **DEBIAN 5.0.4** en base a las siguientes premisas:

a. Cumple con los requerimientos antes enunciados para la instalación de herramientas de gestión de red.
b. El estudio en base a la norma IEEE 830 (Figura 3-12) lo ubica como una de las distribuciones de mejores características en Open Source.
c. Se establece como un sistema orientado a la implementación de servidores.

---

[38] JIMÉNEZ GLADYS, PAZMIÑO CARLOS, “Análisis, implementación y evaluación de un prototipo ruteador dual IPv4/IPv6 con soporte de QoS e IPsec sobre Linux, usando AHP para la selección del hardware e IEEE 830 para la selección del Software”, Proyecto de Titulación de Ingeniería, Escuela Politécnica Nacional, Quito, Agosto 2009.

d. Es una distribución Linux estable con facilidad de ejecución de comandos a través de la consola de texto y posee un amplio número de paquetes necesarios para la implementación de la NMS.
e. Amplia y disponible documentación.



Selección de Distribución GNU/Linux

CODIGO	REFERENCIA	FEDORA	UBUNTU	DEBIAN	OPENSUSE	SLACKWARE	GENTOO	MANDRIVA	CENTOS	PCLINUXOS
REQ01	Item 3	5	5	10	10	10	5	5	10	10
REQ02	Item 18	5	5	10	5	10	5	5	10	10
REQ03	Item 17	10	8	10	10	10	4	1	10	4
REQ04	Item 15	5	8	9	1	9	9	9	7	5
REQ05	Item 16	5	5	10	1	10	5	1	5	5
REQ06	Item 19	10	7	10	5	2	10	10	8	4
REQ07	Item 12	8	8	10	8	4	8	10	6	6
REQ08	Item 11	10	10	10	5	1	1	5	10	1
TOTAL		58	56	79	45	56	47	46	66	45

Tabla 2-21 Selección de Sistema Operativo

Figura 3-12.- Selección de sistema Operativo Linux.[39]

3.4.1.2. Selección de la Herramienta de Monitoreo de Red

3.4.1.2.1. Requerimientos de la Herramienta

Se desea un software que permita monitorear los distintos equipos y dispositivos de red con las siguientes características:

- Monitoreo de utilización de cada interfaz de los equipos.
- Permita el monitoreo personalizado en función del tiempo.
- Muestre información gráfica y tablas de datos de los últimos minutos, horas, días y meses de monitoreo.
- Permita la utilización del protocolo SNMP en sus versiones v1, v2c y v3.
- Monitoreo de la conectividad de los equipos en tiempo real.

[39] JIMÉNEZ GLADYS, PAZMIÑO CARLOS, "Análisis, implementación y evaluación de un prototipo ruteador dual IPv4/IPv6 con soporte de QoS e IPsec sobre Linux, usando AHP para la selección del hardware e IEEE 830 para la selección del Software", Proyecto de Titulación de Ingeniería, Escuela Politécnica Nacional, Quito, Agosto 2009.

- Permita un monitoreo mínimo de 200 sensores.
- Permita monitorear la utilización de red en tráfico entrante y saliente.
- Posea un registro de eventos.
- Posibilidad de formar grupos para los sensores monitoreados.
- Permita la exportación de reportes en xls.

3.4.1.2.2. Selección de la Consola de Monitoreo.

En función de los requerimientos para la gestión de los dispositivos y las ventajas ofrecidas por varias herramientas de administración analizadas (Anexo E), se selecciona la consola "JFFNMS" (Just For Fun Network Management System), que proporcionará facilidad a los administradores de Petroproducción en el monitoreo de red de una manera sencilla y amigable. La Tabla 3-24 presenta el resumen de las características de diferentes herramientas estudiadas.

Las características tomadas en cuenta para su selección son:

- Su desarrollo es constante, posee una comunidad que apoya al proyecto JFFNMS.
- Software libre bajo la licencia GPL[40].
- Monitoreo de una red IP mediante SNMP y Syslog[41].
- Posee características orientadas a dispositivos Cisco.
- Escrito en PHP y funcional en ambientes GNU/Linux, FreeBSD y Windows.
- Modular y extensible.
- Soporte de datos MySQL o PostgreSQL.
- Estadísticas muy visuales gracias al uso de RRDTool.
- Los agentes no necesitan de software adicional.

La herramienta ayudará a mantener un correcto funcionamiento de la red a través de la detección de errores presentes en un tiempo mínimo, brindando la

[40] Licencia Pública General de GNU
[41] Estándar de facto para el envío de mensajes de registro en una red informática IP.

oportunidad al personal del NOC de implementar acciones preventivas y correctivas. Además con soporte SNMP v1, v2c y v3 brinda una fácil implementación de la consola y gestión de los equipos, siendo útil al momento de administrar la red.

CARACTERISITICAS	NAGIOS	ZENOSS	JFFNMS	PANDORA FMS	OPENNMS	ZABBIX
GRÁFICAS	SI	SI	SI	SI	SI	SI
ESTADÍSTICAS	SI	SI	SI	SI	SI	SI
AUTODESCUBRIMIENTO	NO	SI	SI	SI	SI	SI
SNMP	SI, con plugins	SI	SI	SI	SI	SI
SYSLOG	SI	SI	SI	SI	SI	SI
SCRIPTS EXTERNOS	SI	SI	SI	SI	SI	SI
ALERTAS	SI	SI	SI	SI	Algunas	SI
INTERFAZ WEB	Sólo Visualización	Control Total	Control Total	Control Total	Control Total	Control Total
BDD (ALMACENAJE)	SQL	RRDTool y MySQL	RRDTool, MySQL y PostgreSQL	SQL	RRDTool	SQL
EVENTOS	SI	SI	SI	SI	SI	SI
LICENCIA	GPL	GPL	GPL	GPL2	GPL	GPL
COMPLEMENTOS	SI	SI	SI	SI	SI	SI
SEGURIDAD	NO	SI	SI	SI	Pantallas con Dashboard	SI

Tabla 3-24.- Características de Herramientas de Administración de Red.

3.4.2. EQUIPOS NECESARIOS PARA LA IMPLEMENTACIÓN DE LA NMS

Se requerirá un servidor de monitoreo, servidor de logs (destinado a almacenar grandes cantidades de información proveniente de los eventos en los agentes) y la consola NMS, juntos estos elementos permitirán a los administradores sondear la red y gestionar su administración, en mayor detalle descritos posteriormente.

El desarrollador del software JFFNMS otorga un cuadro guía de requerimientos en hardware en función del número de hosts e interfaces a ser monitoreadas, la siguiente tabla señala de entre las distintas opciones la más cercana a lo requerido para el NOC. En función de esto se procede a detallar los distintos elementos que serán necesarios para la implementación de la consola.

Table 3.1: Example hardware requirements

Hosts	*Interfaces*	*CPU*	*Memory*	*Disk*	OS	*Notes*
15	125	PII 266MHz	128MB	SCSI	RedHat9	5avg 3 slow
38	660	Xeon 3.4GHz	512MB	SCSI	Debian sarge	5avg 1.72
41	1531	P4 2.8Ghz	1GB	SCSI	Slackware	5avg 5.0
55	920	Cel 1.6 Gz	512MB	IDE	Windows?	35-65%
67	2017	Dual 3GHz	2GB	SCSI RAID0	RedHat ES4	5avg 45.78
Database		Sunfire V110			RedHat	unknown
69	1210	P4 1.7GHz	768M	IDE	FreeBSD 4.11	55% avg
72	1100	Dual Xeon 2GHz	4GB	SCSI RAID5	RedHat ES4	5avg 0.45
82	989	Dual Xeon 3.4 GHz	2GB	SCSI	Debian Sarge	5avg 0.13
Database		Dual Xeon 3.4 GHz	2GB	SCSI	Debian Sarge	5avg 0.13
95	624	Dual 1.2 GHz	1.25GB	?	Windows 2000	22%
119	1700	Dual P4 3GHz	1GB	SATA	Windows 2003	bit slow
150	2000	P4 2.8 GHz	1GB	SATA	Debian Sarge	5avg 2
Database		P4 2.8 GHz	1GB	SATA	Debian Sarge	5avg 2
362	4570	Dual Xeon 2.8 GHz	2GB	SCSI RAID0	Freebsd 4.11	5avg 4.5
Database		Dual Xeon 2.8 GHz	2GB	SCSI RAID0	Freebsd 4.11	5avg 4.5

Figura 3-13.- Requerimientos de Hardware de JFFNMS.[42]

3.4.2.1. Servidor de Monitoreo

Si bien las características mencionadas en la Figura 3-13 (detallada en el manual de administración oficial[43]), no aseguran el óptimo funcionamiento de la

[42] FUENTE: http://www.scribd.com/doc/18110697/Jffnms-Manual
[43] FUENTE: http://www.jffnms.org/docs/jffnms.html

herramienta, son una pauta para identificar los requerimientos en hardware necesarios para la NMS. Por conveniencia a requerimientos empresariales y por tiempos de respuesta en actividades de monitoreo, se necesitarán dos equipos con similares características destinados uno para la matriz Quito y otro para su operación en el Distrito Amazónico – Lago Agrio.

El servidor requerido para el monitoreo debe poseer características superiores a las recomendadas anteriormente, existen también parámetros a tener en consideración que formarán parte del equipo como por ejemplo: interfaces de red, fuentes de poder, entre otros. La siguiente tabla muestra las características del servidor requerido.

ÍTEM	DESCRIPCIÓN
Procesador	Intel familia 5500, frecuencia mínima 2GHz
Memoria RAM	Capacidad de memoria por encima de los 6GB expansible
Memoria Cache	Caché de nivel 3 por cada procesador
Interfaz de Red	Puerto Ethernet a velocidad de transferencia de 1Gbps.
Disco Duro	Gran capacidad de almacenamiento mínima de 500GB con posibilidades de expansión.
Unidad de DVD	Unidad óptica integrada con soporte para DVD-RW.
Tarjetas de video	2 tarjetas Quadro NVS 420 pci-e x16, cables y adaptadores para los monitores
Monitor	Monitor 27" LCD Wide screen compatibles con las tarjetas de video,
Fuente de Poder	Fuente de alta eficiencia, redundante.
Otros	Teclado, Mouse, Lector de memorias. Conexión redundante de poder.

Tabla 3-25.- Requerimientos Servidor de Monitoreo.

3.4.2.2. Servidor de Notificaciones Logs

Se necesitará de un equipo servidor encargado de almacenar y procesar los distintos archivos logs (como un dispositivo únicamente de registros) que serán enviados por todos los equipos e interfaces monitoreados. Serán requeridos dos equipos de este tipo uno con destino para la matriz e instalaciones en la ciudad de Quito y otro para su operación en el Distrito Amazónico debido a la extensión de la empresa.

ÍTEM	ESPECIFICACIÓN
Procesador	Alto procesamiento debido a la cantidad de información que genera una red corporativa, como mínimo 2.5GH de procesamiento
Memoria RAM	Cantidad de memoria considerable para crecimiento futuro por encima de 1GB.
Disco Duro	Discos de gran capacidad que recojan todo log entrante de 1TB, que sean capaces de recuperarse ante algún desperfecto y que se encuentren siempre en funcionamiento. Presencia de formaciones RAID[44].
Tarjeta de red	Puertos de red de alta velocidad para su comunicación. Puertos gigabit
Sistema Operativo	Capacidad de albergar distintos sistemas operativos en función de los requerimientos del NOC. Debian 5.0, Red Hat ES 5.0, CentOS 5.0, Windows 2003 Server Enterprise
Unidad Óptica	Almacenamiento en dispositivos ópticos mediante la incorporación de unidad de DVD-ROM.
Otros	Registro de eventos de fallas

Tabla 3-26.- Requerimientos Servidor Logs.

[44] Redundant Array of Independent Disks: Arreglo redundante de discos independientes, hace referencia a un sistema de almacenamiento que usa múltiples discos duros.

FUENTE: http://es.wikipedia.org/wiki/RAID.

3.4.2.3. Equipos y Elementos de Conectividad

Para albergar los nuevos dispositivos, es necesario considerar los medios de transmisión que permitan la comunicación entre éstos y la red empresarial. Así se requerirá los siguientes elementos en la actual infraestructura de red.

3.4.2.3.1. Switch Capa 2

Permitirá la interconexión de servidores y de sus administradores con la red PPR, permitiendo la recolección de datos y el monitoreo de los dispositivos. Para nuestro caso, es suficiente con un switch de acceso ubicado en el cuarto de equipos que brinde conectividad a los nuevos equipos y sirva como reserva ante el crecimiento de la red. A continuación se detalla las características necesarias del dispositivo.

CARACTERÍSTICA	DETALLE
Tipo	Montable en Rack
Puertos	24 x Ethernet 10/100 Base-T
Estándares Compatibles	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Fuente de Poder	Power supply – internal, AC 120/230 V (50/60 Hz)

Tabla 3-27.- Requerimientos de switch capa 2.

Se ha escogido un dispositivo Cisco 2960 TTL, por ser un equipo administrable y de la misma plataforma de los equipos existentes dentro de la organización.

3.4.2.3.2. Puntos de Red

Debido a la instauración de nuevos puestos de trabajo y de equipamiento adicional en el centro de datos, se requiere puntos de interconexión a la red (categoría 6 certificados).

Debido al poco número de equipos adicionales, se estima que se necesitarán ocho puntos de red adicionales (3 en Quito y 5 en Distrito Amazónico – Lago Agrio). La Figura 3-14 muestra la infraestructura adicional necesaria para el funcionamiento del NOC.

3.4.3. EQUIPOS A SER MONITOREADOS

Petroproducción cuenta con un considerable número de dispositivos de networking a lo largo de su red, su infraestructura es propensa a cambios, reconfiguraciones, actualizaciones y demás tareas técnicas para su correcto funcionamiento.

La monitorización se debe realizar a todos los equipos de la red (Descritos desde la tabla 2.2, hasta la tabla 2.7) para tener una administración completa y detallada, así como proporcionar seguridad a los dispositivos en cuestión.

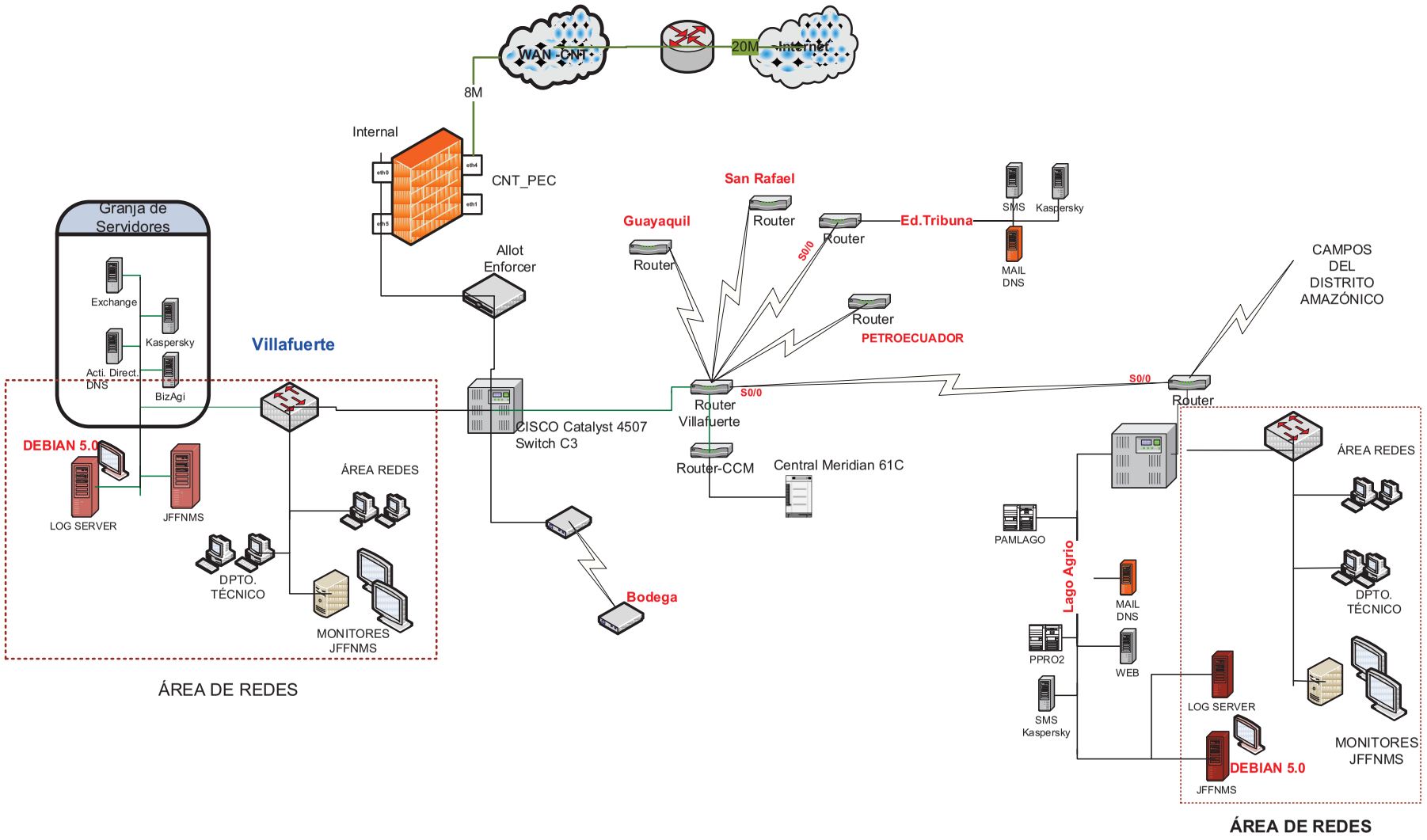


Figura 3-14.- Infraestructura del NOC

3.5. ANÁLISIS DE COSTOS DEL NOC

Para la estimación de los costos, se toma en cuenta los recursos necesarios para la implementación de la nueva área planteada para la conformación del NOC. Los elementos tomados en cuenta son: recursos para su diseño, instalación, capacitación al personal y mantenimiento de la red, distribuidos y separados en costos de inversión, operación y mantenimiento como se describen a continuación.

Los precios de referencia han sido basados en la cotización de una empresa de servicios tecnológicos.[45]

3.5.1. COSTOS DE INVERSIÓN

Se refieren a los recursos en que se invierten para poner en marcha el proyecto. Se clasifican en:

- Activos Fijos
- Activos Nominales

3.5.1.1. Activos Fijos

Comprenden la inversión de dispositivos físicos como servidores y equipos de conectividad:

- Servidor de Monitoreo, NMS
- Servidor de Logs
- Monitores para administración de la NMS
- Switch capa 2 para incorporación de nuevos elementos
- CATALYST 2960 24 PORT 10/100 (Switch Catalyst de 24 puertos)

[45] Cotización realizada por una empresa de servicios Tecnológicos y de Comunicaciones: Andean-Trade S.A., tecnological business.

Los servidores que han sido elegidos para este proyecto por sus características y han sido cotizados de manera individual.

Además incluye:

- Configuración de elementos de red para ser administrados por el sistema de monitoreo.
- Pruebas de funcionamiento efectuadas una vez realizada la configuración de los equipos.
- Instalación y certificación de los puntos de cableado categoría 6A.

ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO USD $	PRECIO TOTAL USD $
1	Servidor NMS	2	2.381,91	4.763,82
2	Servidor de logs	2	796,81	1.593,62
3	Monitor de Consola DELL 27”	2	1.119,00	2.238,00
4	Switch 2960	2	870,00	1.740,00
5	Configuración de equipos	1	5.000,00	5.000,00
6	Pruebas de Funcionamiento	1	1.000,00	1.000,00
7	Instalación de los puntos de datos cat 6A	8	30,00	240,00
8	Certificación de puntos de datos cat 6A	8	5,00	40,00
			TOTAL	**$ 16.615,44**

Tabla 3-28.- Costos de Equipos

3.5.1.2. Activos Nominales

Se refiere a la inversión de recursos no tangibles como licencias, patentes, permisos de operación, membrecías, franquicias, entre otros.

Para el presente proyecto se plantea la utilización de software libre de la herramienta a ser utilizada por lo que se estima el valor de cero en activos nominales.

3.5.2. COSTOS DE OPERACIÓN

Son los que se utilizan para poner en marcha el proyecto, se clasifican en:

- Costos de Producción
- Costos de Ventas
- Gastos Administrativos
- Gastos Financieros

3.5.2.1. Costos de Producción

Son los gatos necesarios para mantener en ejecución el proyecto y se clasifican en:

- Mano de Obra
- Capacitación
- Insumos

3.5.2.1.1. Mano de Obra

Tienen que ver con el funcionamiento y gestión de la red. Debe incluir un mantenimiento preventivo periódico y correctivo en caso de presencia de fallos lo que involucra un suministro de repuestos y equipos de respaldo según sea el caso.

Para realizar el mantenimiento propuesto se requerirá del siguiente personal

- 2 Analistas (se harán cargo de las NMS en los puntos de mayor concentración, el edificio Villafuerte y las instalaciones de Lago Agrio)
- 3 Asistentes (Dos en el Área en el Distrito Amazónico y uno en la Ciudad de Quito).

El personal ha sido designado para laborar en los dos puntos centrales de datos, debido a la extensión de la empresa y a la conveniencia en cuestiones de respuesta a fallos.

El cálculo de costos es tomado en base a los cuadros remunerativos de la LOSCCA[46] 2010 y utilizados por el departamento de Recursos Humanos para la contratación de personal.

PERSONAL	CANTIDAD	REMUNERACIÓN USD $	OTROS VALORES USD $[47]	COSTO EMPRESA USD $	TOTAL USD $
ANALISTAS	**2**	1.150,00	988,36	2.138,36	4.276,72
ASISTENTES	**3**	775,00	672,59	1.447,59	4.342,77
				TOTAL	**$ 8.619,49**

Tabla 3-29.- Costos de Operación y Mantenimiento

3.5.2.1.2. Capacitación

La capacitación tendrá una duración de 10 horas teórico práctico para el personal que estará a cargo de la administración del NMS y el área de redes y deberá tratar los siguientes temas:

- Generalidades del equipo de monitoreo, consola JFFNMS.
- Monitoreo de equipos y dispositivos de red.
- Gestión de reportes.
- Usar el equipo de monitoreo para investigar incidentes y evitar fallas.
- Troubleshooting del equipo de monitoreo.

[46] Ley Orgánica de Servicio Civil y Carrera Administrativa y de Unificación y Homologación de las Remuneraciones del Sector Público.

[47] Se considera valores adicionales basados en el cuadro remunerativo LOSCCA 2010 como décimo tercer y cuarto sueldo, aporte IESS, vacaciones, entre otros, por mes.

Además se abarcará la capacitación de temas:

- Administración de redes empresariales.
- Configuración y mantenimiento de dispositivos de red.

ITEM	DESCRIPCIÓN	PRECIO CURSO USD $
1	Capacitación en NMS JFFNMS y Server de logs	600,00
2	Curso de administración y mantenimiento de Redes	1.200,00
3	Capacitación en configuración de equipos de networking	1.500,00
	TOTAL	**$ 3.300,00**

Tabla 3-30.- Costos de Capacitación

3.5.2.1.3. Insumo

- Cableado estructurado categoría 6 más accesorios.

ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO USD $	PRECIO TOTAL USD $
1	CABLE UTP CAT 6A	1	150,00	150,00
2	Patch Cord UTP Cat. 6 a de 10 pies color blanco	8	17,01	136,10
3	Face Plate Ejecutivo de 1 salidas	8	1,67	13,33
4	Cajas Sobrepuestas	8	1,79	14,36
5	Jack CAT 6A	8	14,62	116,92
6	Canaletas y accesorios de instalación	1	200,00	200,00
			TOTAL	**$ 630,71**

Tabla 3-31.- Costos de Insumos

3.5.2.2. Costos de Ventas

Para el proyecto no existe este valor puesto que no será un producto que se comercialice, será de uso exclusivo para Petroproducción. No existe ningún tipo de publicidad, promoción ni marketing.

3.5.2.3. Gastos Administrativos

Se consideran los gastos necesarios para la planificación, coordinación y control del Centro NOC. Abarca los sueldos mensuales de los Supervisores de cada área, del Coordinador y del personal de planta de Petroproducción.

PERSONAL	CANTIDAD	REMUNERACIÓN USD $	OTROS VALORES[48] USD $ / MES	COSTO EMPRESA USD $	TOTAL USD $
SUPERVISOR	5	1.670,00	1.426,23	3.096,23	15.481,15
COORDINADOR	1	2.505,00	2.129,35	4.634,35	4.634,35
ANALISTA	4	1.150,00	988,36	2.138,36	8.553,44
ASISTENTE	3	775,00	672,59	1.447,59	4.342,77
				TOTAL	**$ 33.011,71**

3.5.2.4. Gastos Financieros

Estos gastos implican los intereses a pagar por préstamos y recursos ajenos a la empresa, al ser una empresa pública, estos valores son nulos debido a que no se requiere un financiamiento externo a lo otorgado por el Estado.

[48] Se considera valores adicionales según el cuadro remunerativo LOSCCA 2010 como décimo tercer y cuarto sueldo, aporte IESS, vacaciones, entre otros

3.5.3. COSTO TOTAL

La Tabla 3-32 muestra el costo referencial de puesta en marcha el Centro de Operaciones de Red en Petroproducción, dicho costo aunque puede ser variable, presenta una referencia a tomar en consideración.

DESCRIPCIÓN	COSTO TOTAL USD $
Costos de Inversión	**16.615,44**
Costos de Operación	**12.550,20**
TOTAL	**$ 29.165,64**

Tabla 3-32.- Costo Total de Implementación del Proyecto

COSTOS DE MANTENIMIENTO Y GASTOS ADMINISTRATIVOS	
Mantenimiento **MENSUAL**	**$ 8.619,49**
Gastos Administrativos **MENSUAL**	**$ 33.011,71**
TOTAL	**$ 41.631,2**

Tabla 3-33.- Gastos Mensuales del Proyecto

COSTO ANUAL DEL PROYECTO	
Costos de Inversión	**$ 16.615,44**
Costos de Operación	**$ 12.550,20**
Mantenimiento	**$ 103.433,88**
Gastos Administrativos	**$ 396.140,52**
TOTAL	**$ 528.740,04**

Tabla 3-34.- Costo Anual del Proyecto

Capítulo 4

PILOTO DEL CENTRO DE OPERACIONES DE RED "NOC" QUITO.

4.1. INTRODUCCIÓN

El presente capitulo abarca la implementación del plan de monitoreo del NOC, implicando la recolección de datos de los principales equipos activos de Petroproducción. En su realización se emplea el protocolo SNMP con la versión 2c, y de la consola de monitoreo como servidor de Administración. Se podrá apreciar los distintos acontecimientos de los equipos en la red y la realización de pruebas funcionales con la consola JFFNMS previamente escogida en el Capítulo 3 como herramienta de gestión.

Puntos importantes a perseguir en este piloto son:

- Cada nuevo dispositivo ingresado a la intranet debe sujetarse a las configuraciones descritas en el punto 3.3.3 y serán acordes al servidor JFFNMS.
- Monitorear los parámetros de funcionamiento del dispositivo en base a la Tabla 3.1.
- Llevar un registro del equipo monitoreado, estado de su funcionamiento y demás características que permitan identificar de manera rápida y ágil a los dispositivos.
- Establecer alarmas que indiquen el momento de fallo o funcionamiento anormal de los elementos, mostrándolo con prontitud al administrador e identificando la causa del error ocurrido.
- Tener una visión global del desempeño y utilización de los dispositivos dentro de la red.
- Minimizar tiempos de actuación ante la presencia de un fallo.

4.2. SERVIDOR DE MONITOREO

Para la puesta en marcha del piloto, la empresa supo facilitar un equipo que estaba en desuso debido a la inexistencia de equipos nuevos disponibles. Sus características en hardware se especifican a continuación en la Tabla 4-1.

ITEM	DETALLE
MARCA:	HP Compaq d35cmt
Procesador:	Intel Inside Pentium IV, 2.8 GHz
Memoria RAM:	512 MB, expandible según la necesidad (4 slots)
Disco Duro:	80 GB
Discos:	Unidad de CR-R, Floppy
Características:	Puerto de Red: 10/100 Mbps Tarjeta de Video 6 puertos USB 1 puerto Serial 1 puerto Paralelo

Tabla 4-1.- Características de Hardware del Servidor.

Durante el proceso de instalación del sistema operativo Debian 5.0.4 se eligen características y parámetros a implantarse en el servidor, mostradas en el siguiente cuadro:

CONFIGURACIÓN DEL SISTEMA OPERATIVO	
ITEM	**DETALLE**
IDIOMA	Inglés
HOSTNAME	NOClinux
DOMAIN	ppr.com
TIME ZONE	Guayaquil-Ecuador
DISCO	Uso de toda su capacidad de la siguiente manera:
/	Primario: 75GB
swap	Pri/log: 3 GB
free	Primary: 2 GB

Continúa en la página 165.

ROOT PASSWORD	******
USER	Guest
PASSWORD	*******
SOFTWARE INSTALADO	Sistema estándar más un ambiente de escritorio KDE

Tabla 4-2.- Características de Software del Servidor

La siguiente gráfica confirma las características del equipo utilizado, una vez instalado el sistema Debian y mediante el comando *cat /proc/cpuinfo que* despliega la información del CPU utilizado.

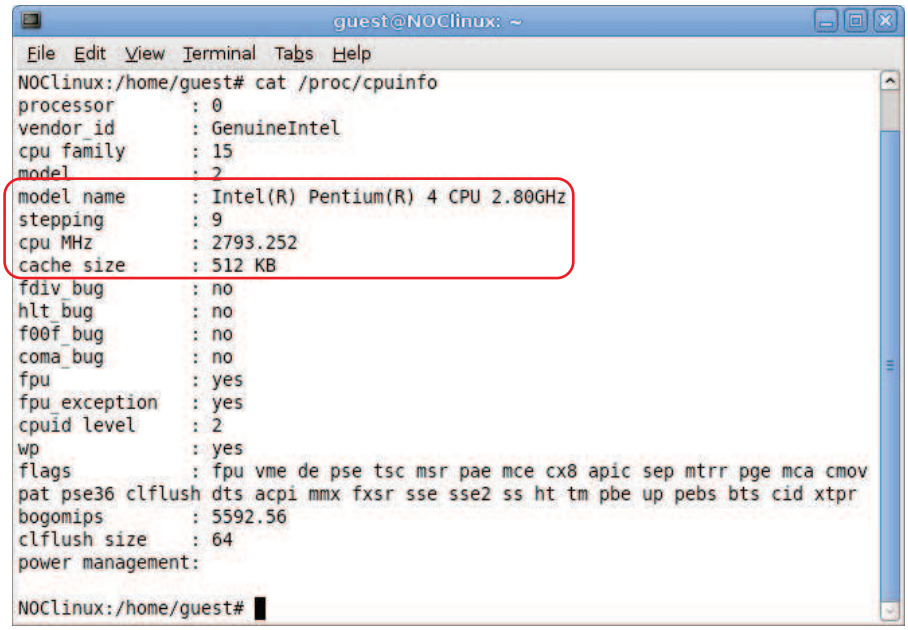


Figura 4-1.- Identificación de Características del Servidor de monitoreo.

4.3. ESPECIFICACIÓN DE EQUIPOS A MONITOREAR

Si bien el monitoreo por parte de la consola de administración debe ser de todo equipo activo dentro de la red PPR y pertenecientes a la empresa, para la implementación se escogerán los equipos más relevantes (autorizados por el departamento TIC para su acceso y configuración) que soporten el protocolo SNMP. Para la elección se consideró aquellos dispositivos con mayor carga de

información, procesamiento, ocupación y permisos de manipulación, tanto del edificio Tribuna como Villafuerte.

La Tabla 4-3 muestra los principales dispositivos gestionados durante el proceso de monitoreo mediante la consola JFFNMS.

DISPOSITIVOS	DETALLE
SERVIDORES	
Lotus	Necesario para llevar control de la documentación interna, procesos legales y demás. Edificio Villafuerte.
File Server	Servidor de archivos (Edificio Villafuerte).
Correo Electrónico	Indispensable para el envío y recepción de documentación entre departamentos.
DNS y Active Directory	Resolución de nombres de Dominio y directorio PPR.
ASTARO	Servidor de seguridad (Proxy y Firewall) (Ed. Villafuerte)
JFFNMS	Servidor de Monitoreo (Edificio Villafuerte)
AS400	Encargado de manejar información empresarial (facturas, documentos, roles de pago, entre otros) (2 de Quito y 2 de D.A)
SWITCHES	
Catalyst 4507	Switch de Core. (Edificio Villafuerte)
Catalyst 2960G	Switches de acceso y distribución dentro del cuarto de equipos del Edificio Villafuerte.
Catalyst 2950	Switches de acceso en ambas instalaciones
ROUTERS	
Cisco 2800	Router Villafuerte
Cisco 2600	Router Tribuna
Cisco 2600	Router Lago Agrio (monitoreo de Conectividad)

Tabla 4-3.- Equipos Monitoreados

4.4. CONFIGURACIÓN DEL SISTEMA

4.4.1. CONFIGURACIÓN DE AGENTES

La consola de administración posee comandos previamente configurados con peticiones de OID definidos y específicos que sirven para la gestión de los equipos. Por lo tanto, solo se debe configurar y permitir la ejecución del protocolo SNMP en los dispositivos para la recolección de la información de interés dentro del piloto.

Además se realiza la instalación del protocolo SNMP en servidores autorizados mediante sesiones de escritorio remoto y a dispositivos de interconectividad por medio de sesiones telnet y vía browser.

La configuración se muestra en detalle para los diferentes sistemas operativos y dispositivos en el ANEXO D.

4.4.2. CONFIGURACION DNS

La consola de monitoreo es una aplicación vía Web por lo que es de suma importancia la creación de una entrada DNS en el servidor de Nombres de Dominio, para que los administradores de la red y encargados del monitoreo puedan ingresar al sistema por medio de su navegador web sin necesidad de aprender la dirección IP del servidor de monitoreo.

La entrada creada es: ***jffnms*** en el dominio ***ppr.com***

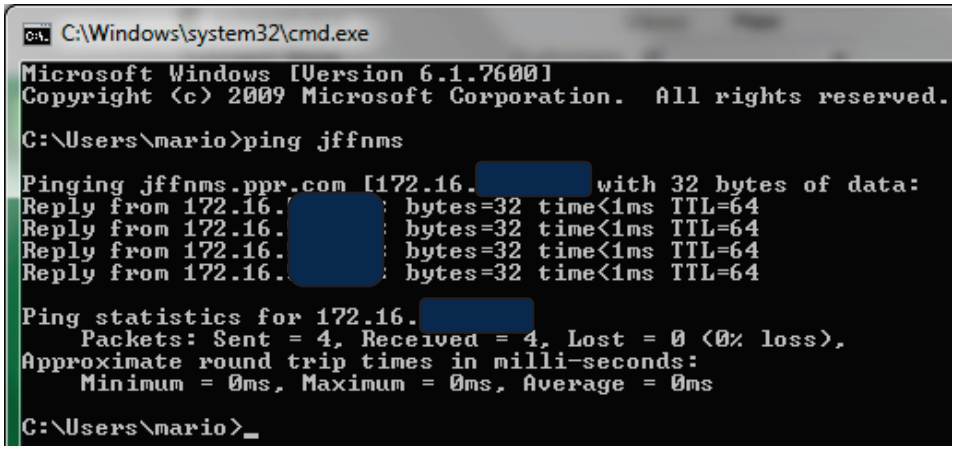


Figura 4-2.- Funcionamiento entrada DNS

La Figura 4-2 presenta la ejecución del comando ping al nombre “jffnms” desde una máquina dentro de la red, y se puede apreciar que se realiza la resolución del nombre a la dirección IP del servidor correctamente.

4.4.3. CONFIGURACION DE NMS

Se instala la herramienta JFFNMS en el servidor como se describe en el ANEXO D y se procede a configurarlo para la visualización de los equipos. Se deben tener dos conceptos claros que la consola maneja:

- **Host.-** se considera como host a los distintos dispositivos que pueden ser monitoreados como switches, ruteadores, servidores o PC´s.
- **Interfaz.-** parámetro o característica propia de cada host que es monitoreado como por ejemplo: tarjetas de red, discos duros, memorias, procesos en ejecución, entre otras.

La configuración requiere definir ciertos parámetros tanto para la administración del propio servidor como para la organización y poleo de los distintos elementos de red. Los parámetros a definirse son:

a. **USUARIOS.-** Personas con privilegios de acceso definidos.
b. **ZONAS.-** Grupos de host con características similares para el administrador.
c. **HOSTS.-** Dispositivos a ser monitoreados.

d. MAPAS DE MONITOREO.- Rápido acceso a host o interfaces de interés.

e. ALARMAS ó SLA.- Especificación de eventos que deberán generarse.

De los elementos anteriormente mencionados cada uno tiene parámetros propios que deben ser especificados según lo que se requiera.

Se verifica la correcta instalación de la consola JFFNMS. Con tal objetivo se visualiza el apartado *"System Setup"* al momento del primer ingreso al sistema, se comprueba que los distintos parámetros se encuentren en estado "OK", mientras que los estados "ERROR" deben ser corregidos para un óptimo funcionamiento.

La Figura 4-3 muestra la correcta instalación de JFFNMS al encontrar los apartados en estado "OK".

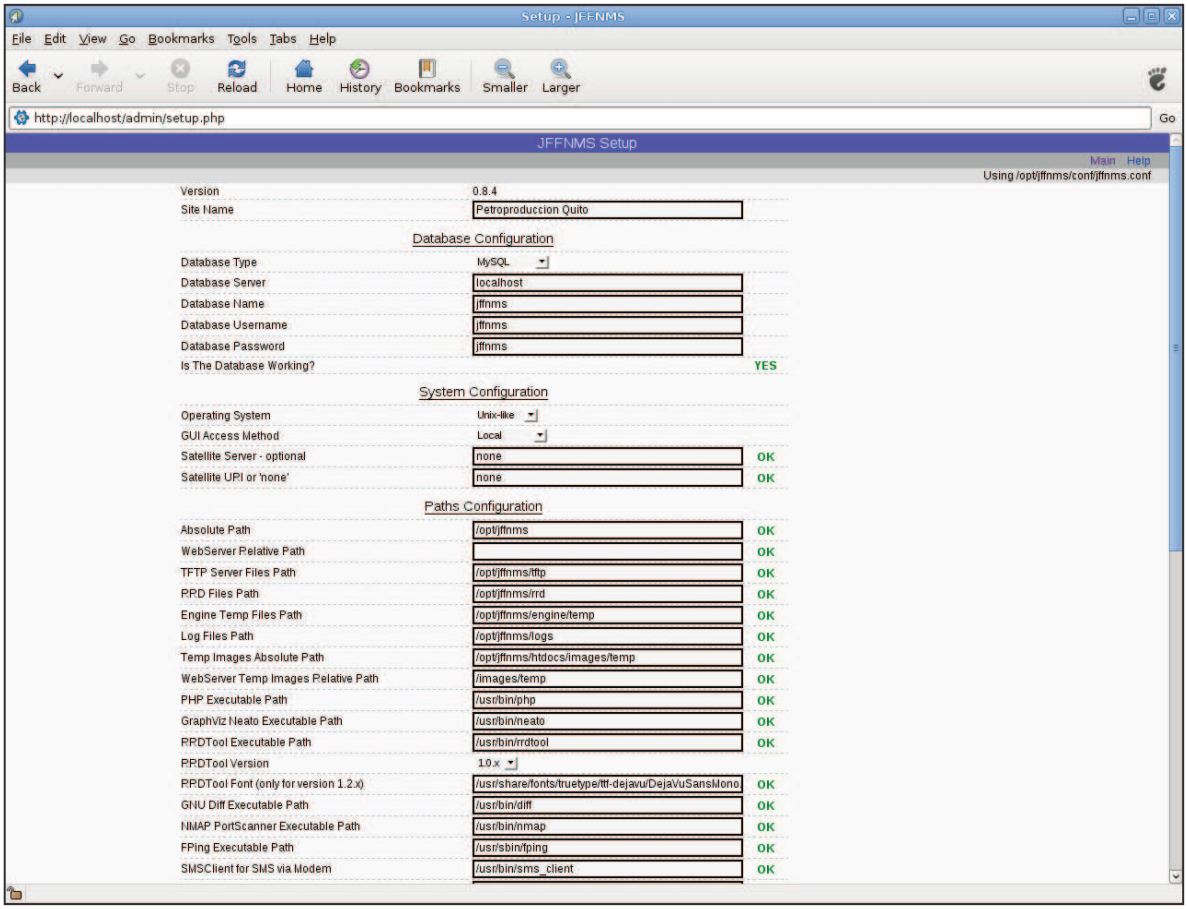


Figura 4-3.- System Setup de JFFNMS.

4.4.4. DEFINICIÓN DE USUARIOS

Consiste en la creación de USERS con su respectiva contraseña y permisos para el ingreso al sistema de monitoreo JFFNMS de la red PPR a través de la pantalla de login que se presenta en la Figura 4-4.

Figura 4-4.- Login al sistema JFFNMS.

La administración del sistema solo puede hacerla inicialmente el usuario Administrador "***admin"*** quien posee todos los privilegios de configuración. Se recomienda que una vez ingresado al sistema se cambie el password del administrador, se creen nuevos usuarios para la gestión y monitoreo de la red.

Para la creación de nuevos usuarios se dirige al módulo **Administración**, dentro del apartado *Users and Customers*, elegir la opción *Add*. En este caso se crea el usuario "***monitor"*** con los permisos básicos únicamente de visualización de la red, sin ningún tipo de privilegio de administración como se muestra en la Figura 4-5.

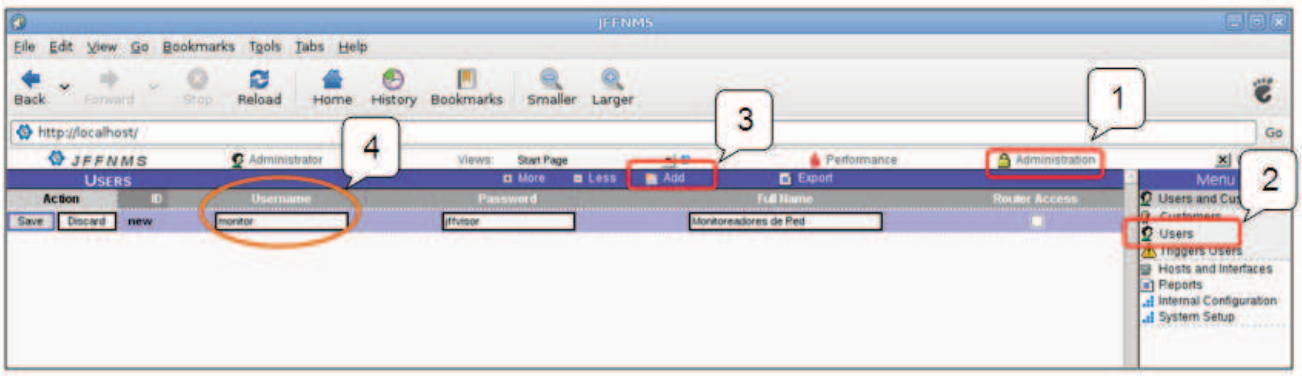


Figura 4-5.- Creación de Usuarios.

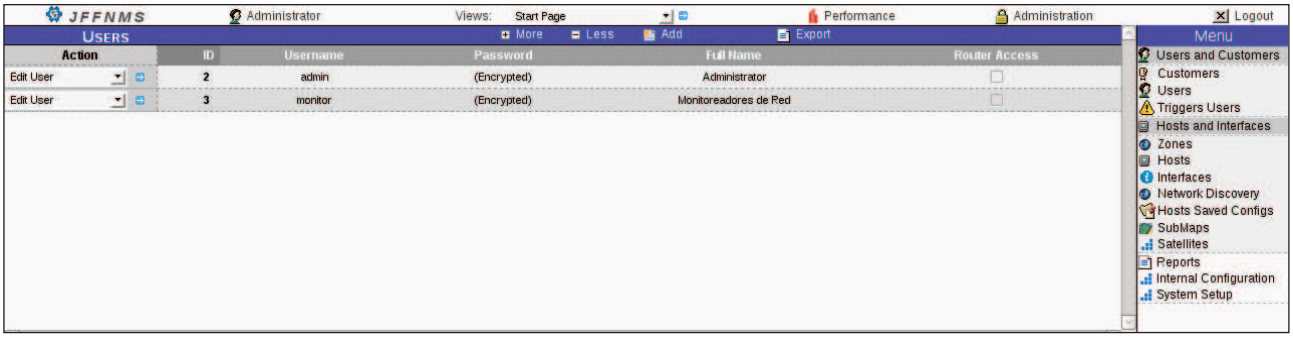


Figura 4-6.- Usuarios creados en JFFNMS.

La Figura 4-7 y Figura 4-8 la muestran los perfiles y permisos para los usuarios "Admin" y "Monitor" respectivamente. El usuario "Admin" tiene todos los permisos para modificar, crear, borrar y administrar la consola JFFNMS, mientras que "Monitor" puede solo visualizar los eventos y gráficas generadas, sacar reportes, pero no crea ni borra elementos en la consola. Esta seguridad permite que otros usuarios autorizados también puedan observar lo que sucede en la red, sin alterar la configuración.

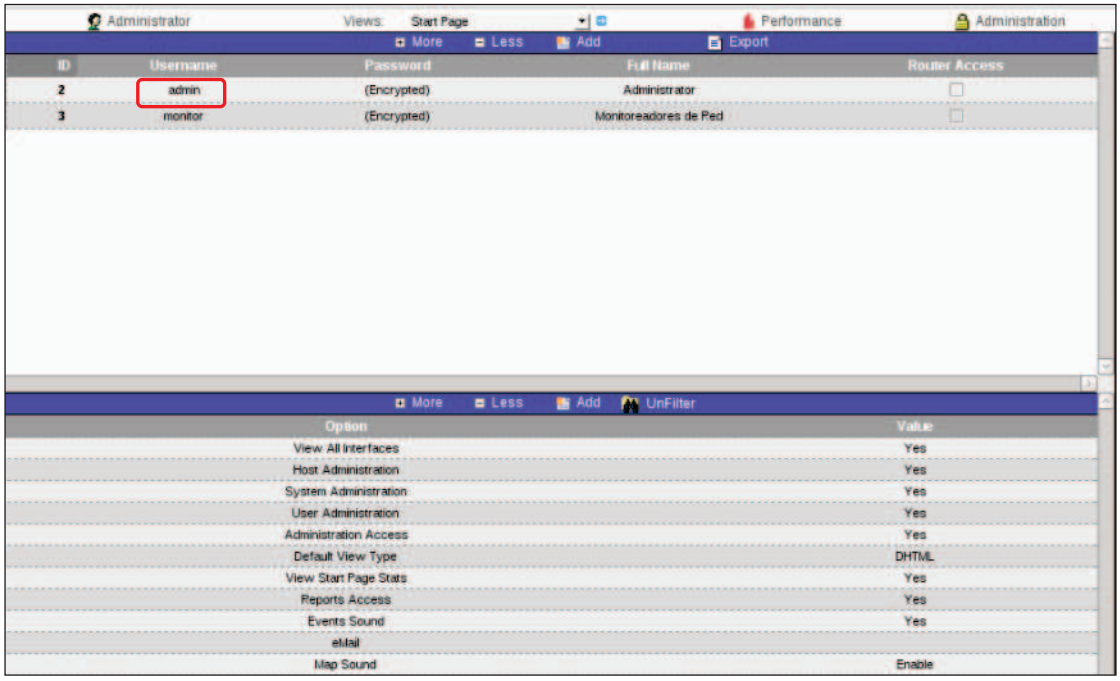


Figura 4-7.- Perfil del usuario Admin.

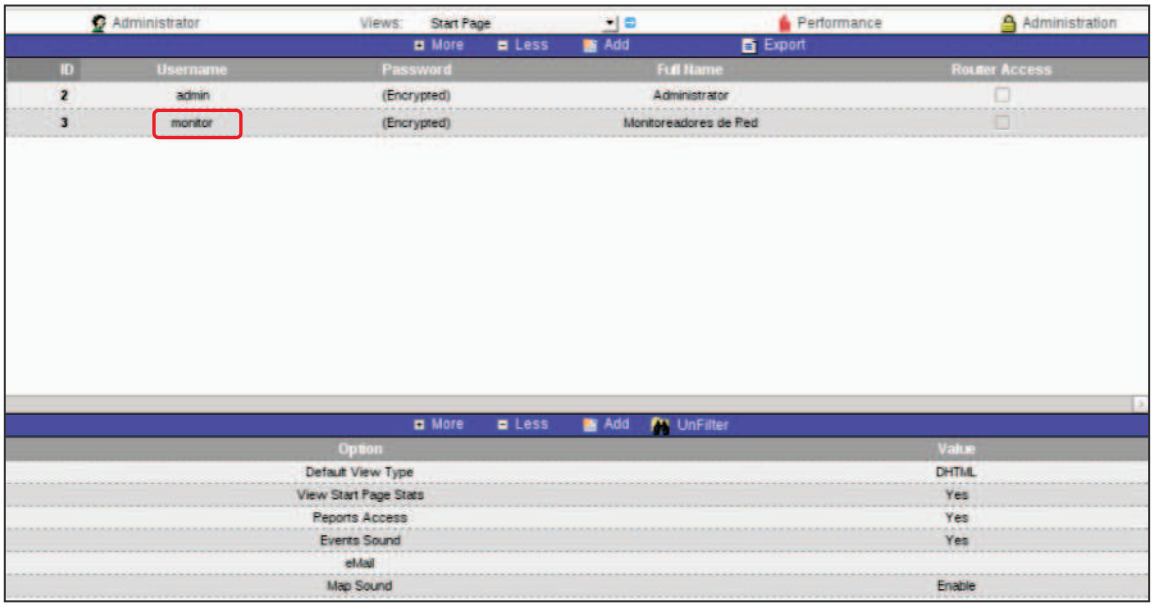


Figura 4-8.- Perfil del usuario Monitor.

4.4.5. ESPECIFICACIÓN DE ZONAS

El programa JFFNMS define zonas como una forma de organización para separar agentes en grupos (en función de los criterios del administrador) y para dar políticas de descubrimiento a cada una de ellas. En la Figura 4-9 se aprecian las opciones existentes para el descubrimiento de dispositivos.

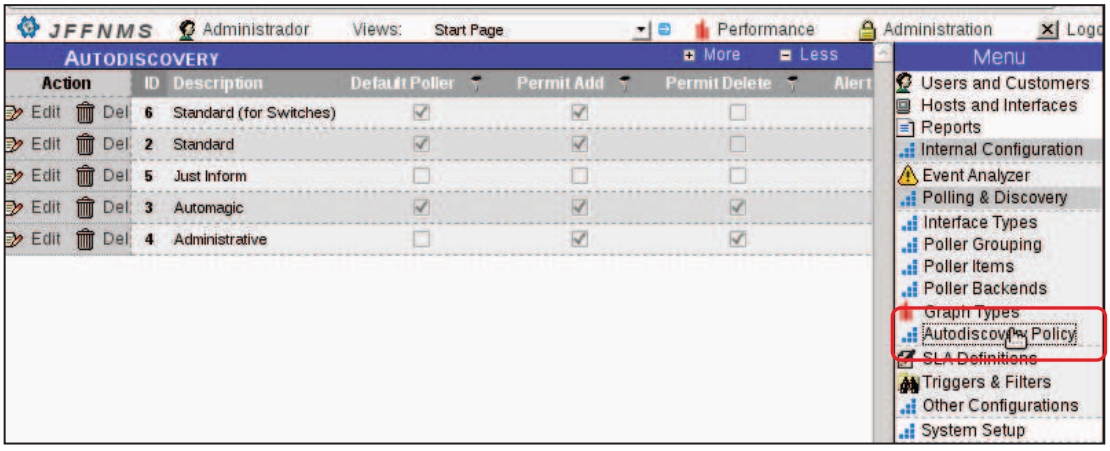


Figura 4-9.- Políticas de Autodescubrimiento de JFFNMS.

Las políticas de descubrimiento previamente configuradas son:

- **Standard (for Switches):** Usado para switches que pueden ser añadidos o borrados pero con la condición que estén en funcionamiento.
- **Standard.-** Las interfaces se añaden si una alarma es detectada.
- **Just inform.-** Solo advierte de los cambios a las listas de las interfaces pero no hace cambios a la base de datos.
- **Automagic.-** Permite a los procesos hacer lo que necesiten.
- **Administrative**: Añaden las interfaces si una alarma es detectada pero no utiliza el poleo por defecto.

Para el monitoreo en la red se crean distintas zonas en base a la ubicación física de los dispositivos (Locación) principalmente, y a la función que desempeñan dentro de la red. Las zonas que fueron definidas se presentan en Tabla 4-4 y se verifica su creación dentro de JFFNMS en la Figura 4-10.

ZONA	DESCRIPCIÓN
Routers	Incluye los equipos de Ruteo de las distintas dependencias de Petroproducción.
Server_tri	Involucra a los servidores del edificio Tribuna.
Server_vill	Involucra a los servidores del edificio Villafuerte.
Switch_tri	Comprende los Switches a ser monitoreados del edificio Tribuna.
Switch_vill	Comprende los Switches a ser monitoreados del edificio Villafuerte.
Distrito_Amazónico	Todo equipo a ser monitoreado del D.A. desde Quito.

Tabla 4-4.- Zonas definidas para su monitoreo

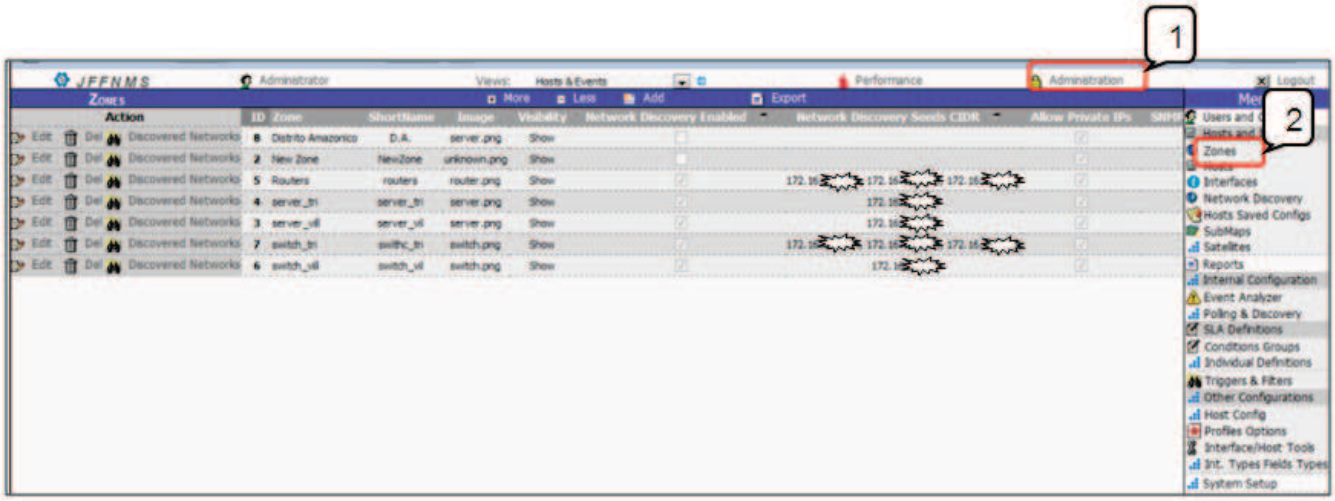


Figura 4-10.- Zonas creadas para Petroproducción en JFFNMS.

4.4.6. ESPECIFICACION DE HOSTS

Los Host son los dispositivos agentes que serán monitoreados por la consola independientemente sean switches, servidores o routers. Estos equipos se encuentran descritos en la Tabla 4-3, a los cuales, para diferenciarlos se procedió a identificarlos mediante una descripción del dispositivo y mediante imágenes subidas a la consola que muestren el tipo de elemento monitoreado y son las que se presentan en la Figura 4-11.

Figura 4-11.- Imágenes Cargadas.

Para el ingreso de un nuevo equipo a ser gestionado se procede:

En la opción hosts, se selecciona **Add** y se colocan los datos necesarios del agente a añadir para su monitoreo, especificando:

- La zona a la que pertenece.
- La política de autodescubrimiento a utilizar.
- Si el elemento será visible o no.
- Las comunidades tanto de lectura como de escritura que se encuentra configurada en el agente.
- El "*customer*" del host, y
- Tiempo de poleo del dispositivo.

La Figura 4-12 muestra como se añade el host Switch de Distribución del edificio Villafuerte.

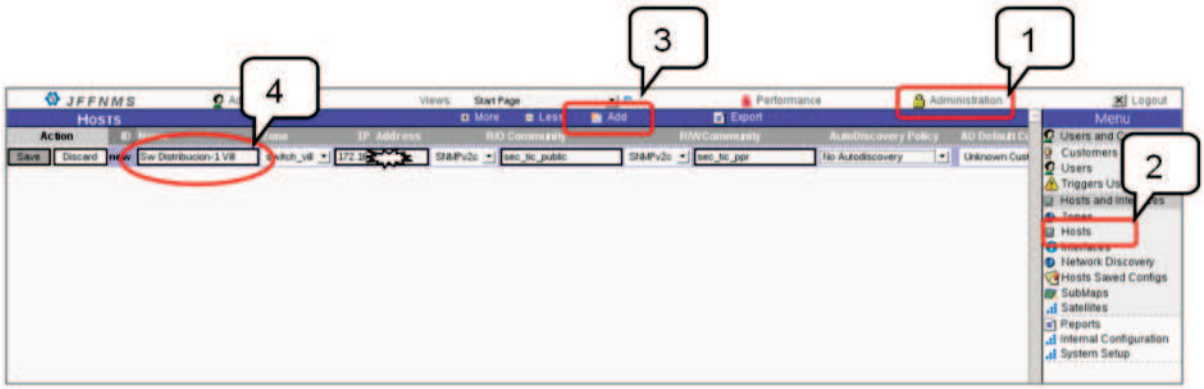


Figura 4-12.- Añadir un host al JFFNMS.

Como las políticas de autodescubrimiento involucran el análisis de interfaces, puertos y procesos de los dispositivos agentes detectados que encuentre en la subred especificada, se procede a realizar un descubrimiento Manual donde se puede seleccionar las interfaces específicas de manera personalizada de cada host según el interés para el administrador. En el proyecto piloto se realiza el **"manual discovery"** como se aprecia en la Figura 4-13, esta presenta la primera parte de las interfaces que se encontraron del switch de acceso del octavo piso del edificio Villafuerte, en el cual se escoge únicamente los parámetros que el administrador esté interesado en monitorear, en este caso la interfaz gigabitEthernet 0/1.

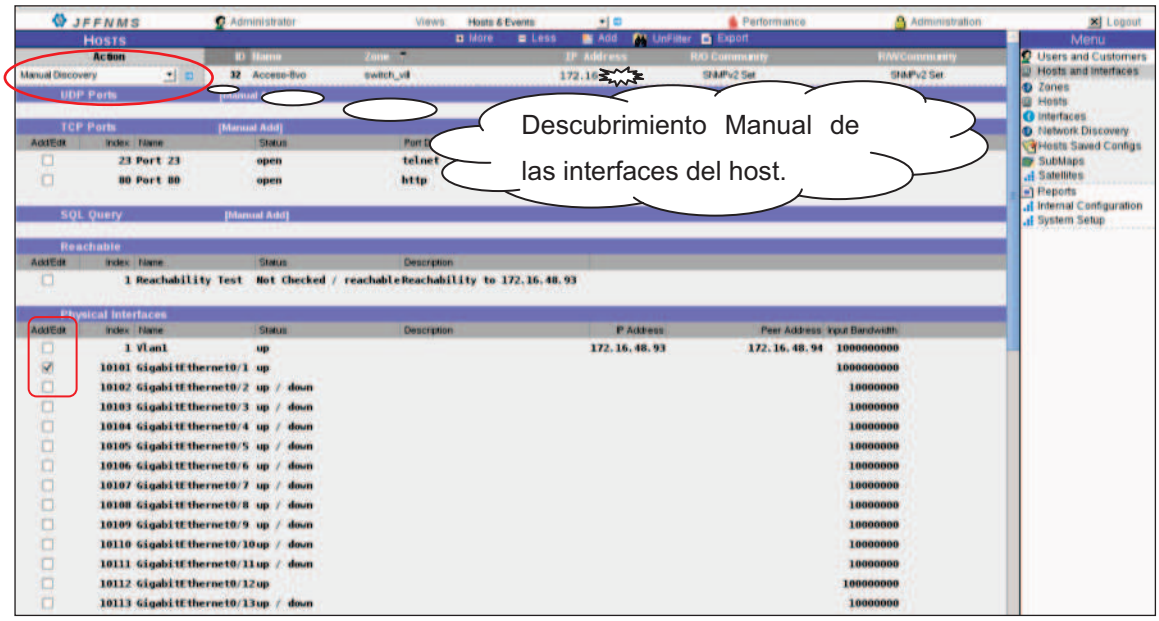


Figura 4-13.-Selección de interfaces de un host.

Ya descubiertas y seleccionadas las interfaces, se puede añadir una descripción para tener mejor referencia a donde se encuentra conectada determinada interfaz.

Dentro de los dispositivos de interconectividad, se establece las interfaces de red a ser monitoreadas de la siguiente manera:

- **Switches**: puertos troncales activos.
- **Routers:** puertos activos en funcionamiento (seriales y Ethernet).
- **Servidores**: las interfaces de red, memoria y Utilización de CPU.

Sus descripciones fueron puestas en base a la documentación obtenida en el análisis de la red explícito en el capítulo 2 y mediante la exploración de los equipos Cisco mediante el uso del protocolo CDP[49] que muestra los equipos de marca Cisco vecinos conectados al dispositivo examinado.
Los demás parámetros monitoreados estarán en función del descubrimiento del dispositivo por parte del servidor. La

[49] CDP: Cisco Discovery Protocol

Figura 4-14 muestra las interfaces seleccionadas del router del edificio Tribuna. Cada una de las interfaces puede ser añadida a un mapa determinado en función de los requerimientos del administrador.

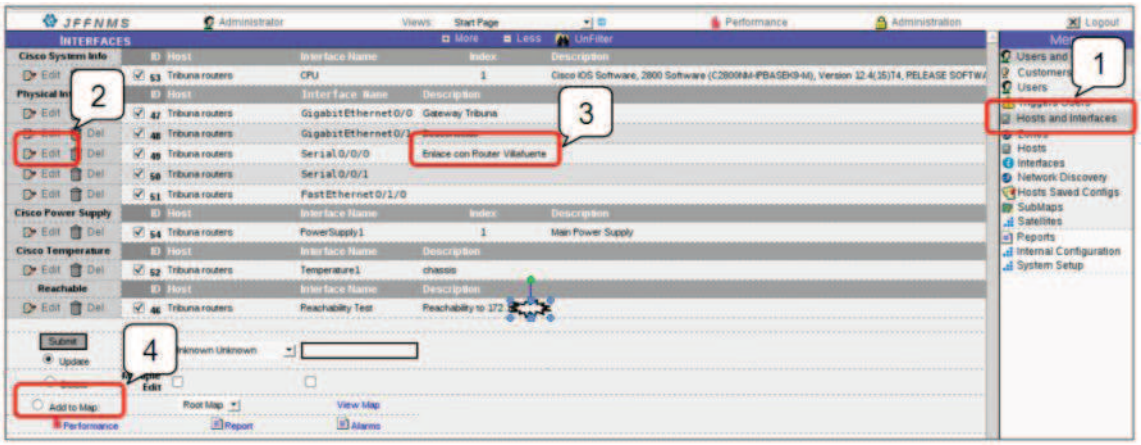


Figura 4-14.- Visor de interfaces seleccionadas para monitoreo.

La Figura 4-15 muestra los host configurados en el servidor todos pertenecientes al *customer* previamente creado y denominado "**petro**".

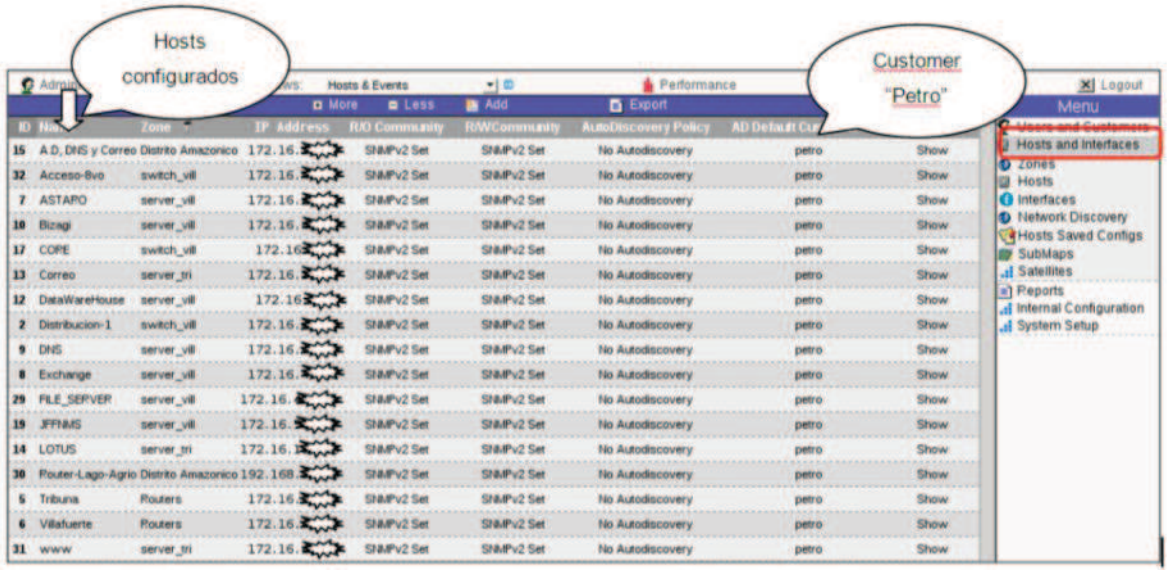


Figura 4-15.- Host a monitorear dentro de PPR QUITO.

4.4.7. ESPECIFICACION DE MAPAS

La creación de mapas simplifica la forma de gestionar en forma grupal las interfaces de los hosts monitoreados. Ésta característica permite un acceso directo a lo que el administrador requiera observar. En el piloto se crearon tres mapas básicos donde se colocaron interfaces de interés que actualmente están siendo monitoreadas, estos mapas son:

MAPA	DESCRIPCIÓN
Enlaces Principales	Están los enlaces importantes de los diferentes dispositivos gestionados, interfaces troncales de switches, interfaces de ruteadores y servidores.
Memoria Servidores	Se encuentran las interfaces de la memoria cache y memoria física únicamente de servidores.
Uso CPU Servidores	Contiene las interfaces que monitorea el uso del procesador de los servidores monitoreados.

Tabla 4-5.- Mapas Implementados

En la Figura 4-16 se aprecia los mapas creados en la consola de administración JFFNMS y en cada uno se indica su número de interfaces y cuantas están alarmadas como es el caso del mapa "*Uso de Memoria Servidores*" donde se tiene dos interfaces con algún aviso dentro de las 10 alarmas en total dentro del mapa, por tal motivo se encuentra de color amarillo.

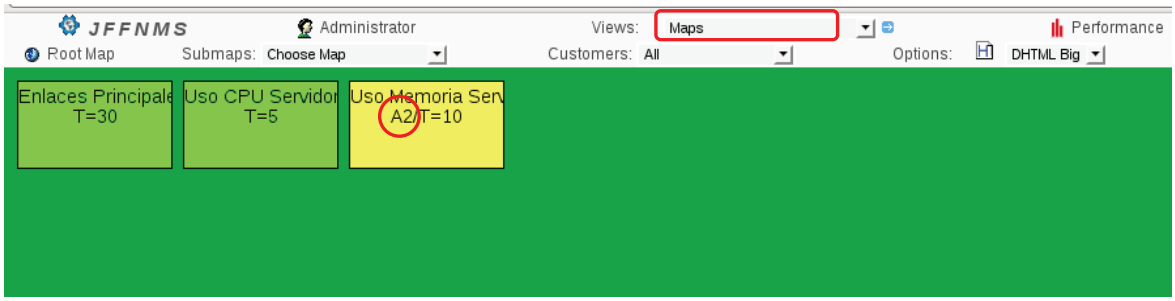


Figura 4-16.- Visualización de mapas.

La Figura 4-17 presenta las interfaces añadidas al mapa "enlaces principales", todos los enlaces están en perfecto estado en el instante que se capturo la imagen, mientras que la Figura 4-18 muestra la misma información pero en formato de vista Graphviz[50].

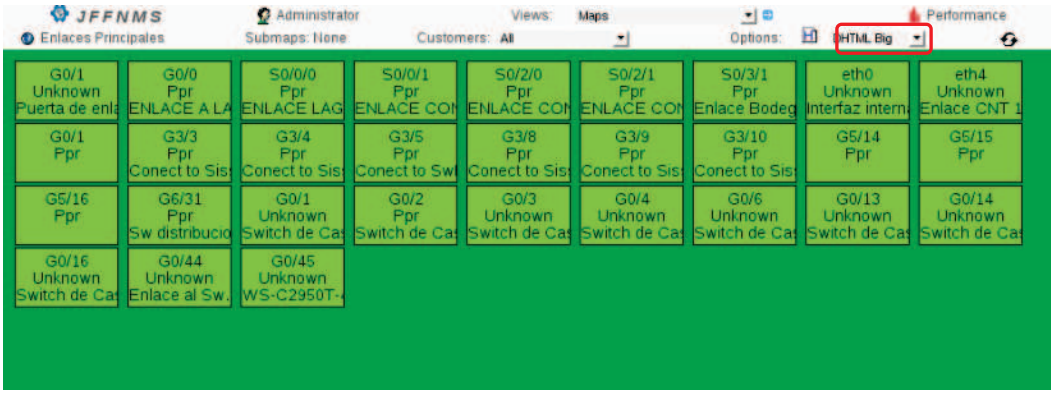


Figura 4-17.- Mapa Enlaces Principales en vista DHTML Big.

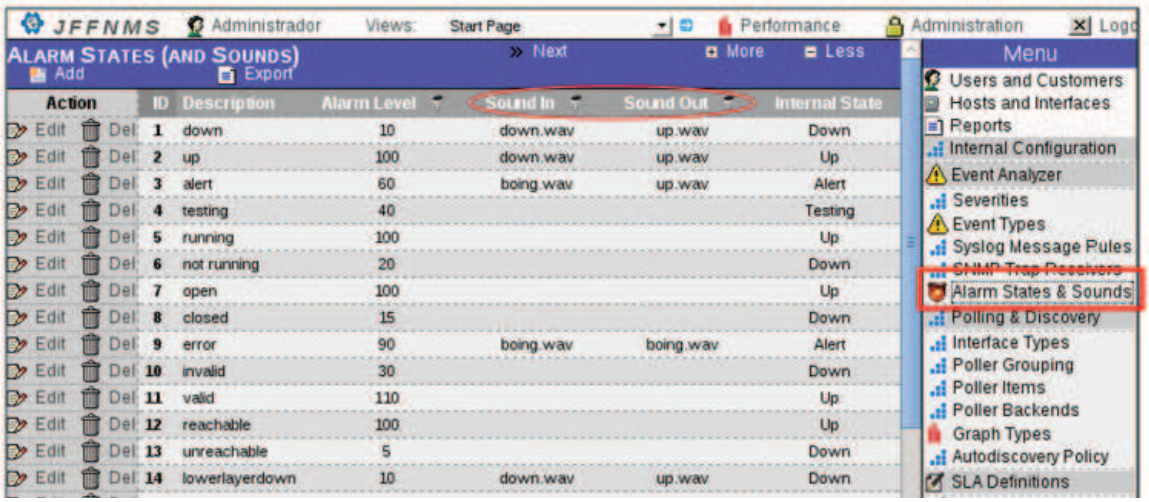
Figura 4-18.- Mapa Enlaces Principales en vista Graphviz.

4.4.8. ESPECIFICACIÓN DE ALARMAS

En el menú de Administración, en la opción *Internal Configuration*, se encuentra el apartado "*Alarm States & Sounds*", donde se presentan las alarmas

[50] Conjunto de herramientas que generan representaciones visuales gráficas.

preestablecidas del sistema JFFNMS, el administrador de la herramienta puede personalizar o añadir nuevas alarmas. Sus características incluyen: sonidos, cambio del nivel de la alerta, el estado cuando sucede un aviso, entre otras. En la siguiente Figura se puede apreciar los sonidos configurados el momento de detección de determinado suceso o evento.



Action	ID	Description	Alarm Level	Sound In	Sound Out	Internal State
Edit Del	1	down	10	down.wav	up.wav	Down
Edit Del	2	up	100	down.wav	up.wav	Up
Edit Del	3	alert	60	boing.wav	up.wav	Alert
Edit Del	4	testing	40			Testing
Edit Del	5	running	100			Up
Edit Del	6	not running	20			Down
Edit Del	7	open	100			Up
Edit Del	8	closed	15			Down
Edit Del	9	error	90	boing.wav	boing.wav	Alert
Edit Del	10	invalid	30			Down
Edit Del	11	valid	110			Up
Edit Del	12	reachable	100			Up
Edit Del	13	unreachable	5			Down
Edit Del	14	lowerlayerdown	10	down.wav	up.wav	Down

Figura 4-19.- Estado de Alarmas y Sonidos de JFFNMS.

Los sonidos se pueden agregar en la carpeta *sounds* del programa JFFNMS, esto se lo debe realizar vía comandos Linux, otorgando los permisos suficientes de escritura en dicha carpeta.

La Figura 4-20 presenta las definiciones de SLA por defecto del sistema, En este punto es donde el administrador define los umbrales para las alarmas definidas en el Capitulo 3, por ejemplo el que una advertencia se produzca cuando el uso de la memoria o la utilización de CPU sobrepase el 75%.

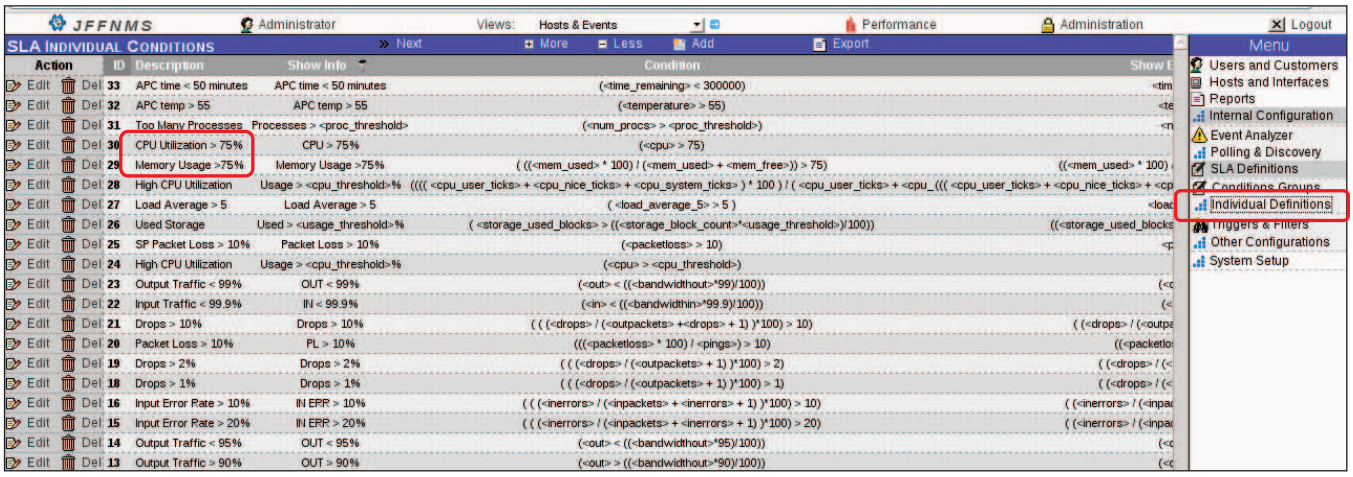


Figura 4-20.- Definiciones de SLA en JFFNMS.

4.5. MONITOREO DE LA RED

El monitoreo de la red se lo puede realizar una vez definidos los parámetros, los elementos de monitoreo y sus interfaces. En la parte superior de la consola de administración se encuentra un cuadro se selección de las vistas generadas por el servidor como se muestra en la siguiente Figura:

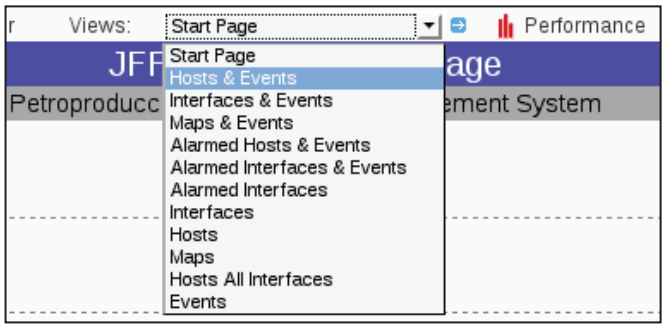


Figura 4-21.- Opciones del Sistema JFFNMS.

- **Start page:** Muestra la página de inicio con información general de la red.
- **Hosts & Events:** Pantalla dividida, en la parte superior se encuentran los hosts y en la parte inferior los eventos sucedidos.
- **Interfaces & Events:** Pantalla dividida, arriba están las interfaces de los hosts que estén configuradas y en la parte inferior los eventos sucedidos.

- **Maps & Events:** Presenta una Pantalla dividida, arriba están los mapas pre-configurados en los que se puede explorar las interfaces pertenecientes a los mapas y en la parte inferior los eventos sucedidos.
- **Alarmed Hosts & Events:** Pantalla dividida, arriba los hosts que tienen alguna alerta o aviso y en la parte inferior los eventos sucedidos.
- **Alarmed Interfaces & Events:** Presenta una Pantalla dividida, arriba las interfaces de los hosts que tienen alguna alerta o aviso y en la parte inferior los eventos sucedidos.
- **Alarmed Interfaces:** Presenta todas las interfaces que presenten algún aviso o alarma.
- **Interfaces:** Muestra las interfaces de todos los hosts configurados en la consola de administración.
- **Hosts:** Muestra todos los Hosts insertados en la gestión. Permite ingresar a cualquier dispositivo para ver su información.
- **Maps:** Presenta los mapas creados en el sistema y se puede explorar las interfaces que pertenezcan a cada sub-mapa.
- **Hosts All Interfaces:** Presenta los host y todas las interfaces monitoreadas del sistema.
- **Events:** Muestra los acontecimientos sucedidos, las alertas y avisos lanzados por el sistema o algún host.

Figura 4-22.- Pantalla de Hosts & Events.

Se puede apreciar en la Pantalla de *Hosts & Events* que hay la presencia de alarma advirtiendo el Uso del disco G que sobrepasa el 80% de su capacidad, cambiando el recuadro del servidor a un color amarillo significativo de la presencia de alguna alerta en una de sus interfaces configuradas.

Otra forma de monitorear la red es ingresando en el icono de PERFORMANCE en la parte superior de la consola de administración. En la parte de la izquierda aparecen las opciones a escoger, se selecciona la opción hosts, y se despliegan todos los dispositivos configurados como se aprecia en la Figura 4-23, se ingresa a dispositivo que se desee y se escoge la interfaz específica a monitorear.

Figura 4-23.- Monitorización con Performance de JFFNMS

En la siguiente figura se aprecia uso de procesador del servidor Astaro desde el lunes 19 de abril hasta las 14 horas del 20 de abril de 2010. Se puede visualizar que la carga aumenta considerablemente alrededor de las 8:00 que es la hora de ingreso de los trabajadores. Las gráficas además dan los valores Máximos, promedio y últimos capturados en el periodo de tiempo especificado.

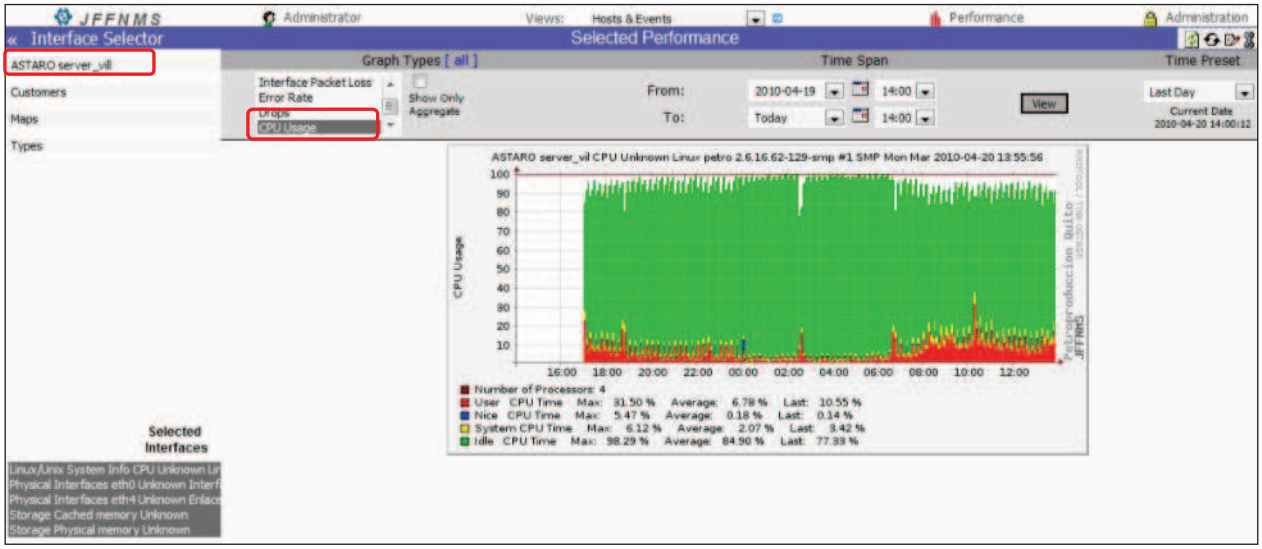


Figura 4-24.- Monitoreo del Uso de CPU en servidor ASTARO.

La utilización de CPU del servidor trabaja en promedio al 9.02 % y su utilización máxima en el periodo de monitoreo fue de 43.09%, lo que significa que en este

punto el servidor está trabajando correctamente sin ningún riesgo, como se aprecia en la Figura 4-24.

Para el proceso de monitoreo y con el afán de ingresar lo menos posible a los elementos de red (servidores en especial, por situaciones de autorización de la Coordinación TIC de la empresa), a más de la configuración de los parámetros SNMP previamente mencionado en el anexo D, la consola JFFNMS convive con comunidades SNMP que estaban previamente configuradas en algunos dispositivos de red.

La siguiente figura muestra una captura de paquetes mediante un sniffer donde se puede apreciar el poleo de la consola a través de una comunidad distinta "sistemasr" a las especificadas en este proyecto.

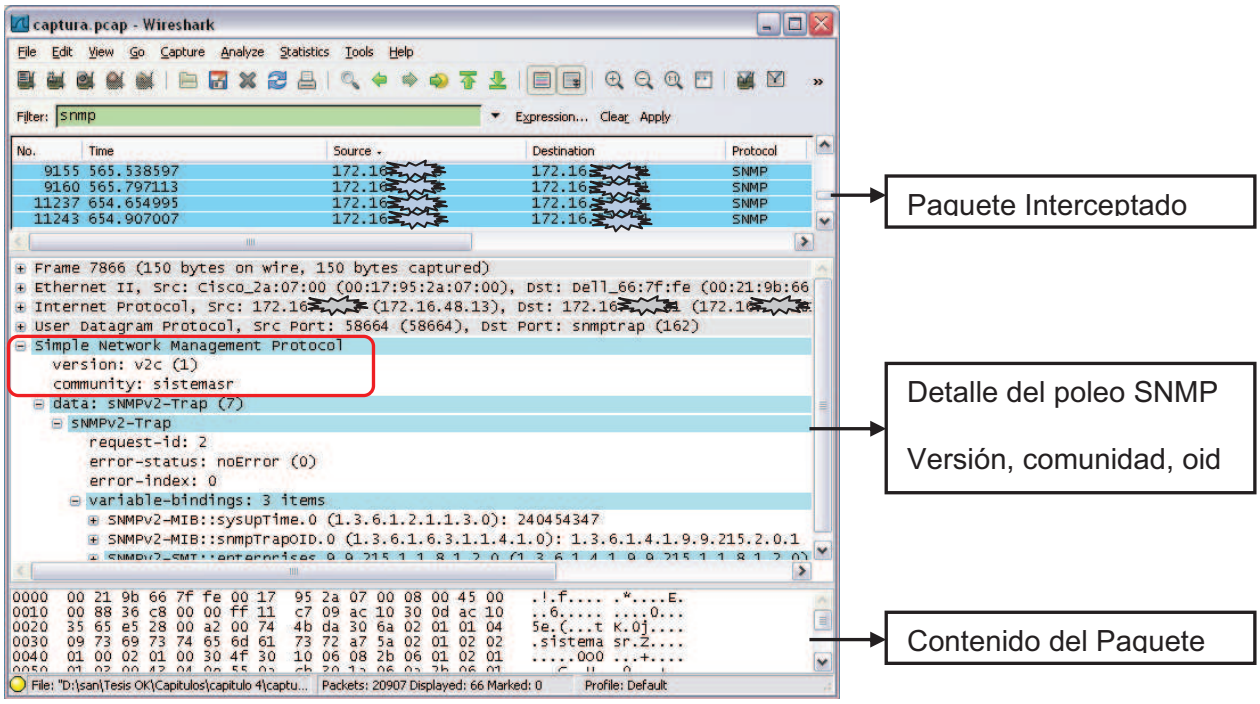


Figura 4-25.- Captura de paquetes con Wireshark.

4.5.1. PRUEBAS DE MONITOREO

Se procedió a la realización de varias pruebas del funcionamiento del sistema de Monitoreo implementado como son:

- Provocar caída de interfaces.
- Verificación de alarma al superar el 75% en utilización de memoria.
- Verificación de alarma al superar del 80% en uso de disco duro.
- Veracidad de los datos recibidos.
- Comparación datos monitoreados con los datos de análisis del capítulo 2.
- Obtención de datos en Monitoreo de routers y switches.

En los siguientes puntos se presentan los resultados obtenidos de las pruebas realizadas.

4.5.1.1. Caída de Interfaces en dispositivos de red

Por medio de una sesión telnet se ingresó al switch de acceso del octavo piso del edificio Villafuerte y se procedió a la ejecución del comando ***Shutdown*** a la interfaz troncal con el switch de distribución. Esta prueba se realizó fuera de horario de oficina debido al impedimento de suspensión del servicio en horas laborables.

En un minuto y medio se lanzó la alarma advirtiendo con un sonido de alerta, al revisar la pantalla de hosts & Events se aprecia que el host del switch del 8vo piso esta en amarillo, y en los eventos aparece la alarma crítica de enlace en down. Seguidamente al tratarse de una interfaz por la cual se monitorea el switch, aparecieron las alarmas de no haber respuesta de las interfaces del host. Con estas alarmas el administrador logro identificar el problema e ir al sitio del dispositivo afectado, resolviendo el problema en 6 minutos aproximadamente colocando la interfaz en Up con la ejecución del comando ***no shutdown***. Dos minutos después se levantaron las alarmas del switch de distribución en la consola. El tiempo Total de la prueba fue de 10 minutos.

En la Figura 4-26 se puede apreciar las alarmas generadas durante la realización de la prueba antes mencionada. El primer evento que se muestra es el enlace en *down* del switch de distribución en el puerto 14 conectado al switch de acceso del octavo piso, esto fue a las 17h35. Un minuto después al no tener

respuesta en el poleo al equipo se genera el aviso de *"interface Protocol Down"* en su enlace troncal.

Una vez levantada la interfaz de switch afectado se notifica *"Interface Protocol UP"*, con lo que finalmente se recibe el último aviso de activación del enlace en el switch de distribución a las 17h45. Dando por terminado la prueba y verificando el estado normal de funcionamiento de los equipos.

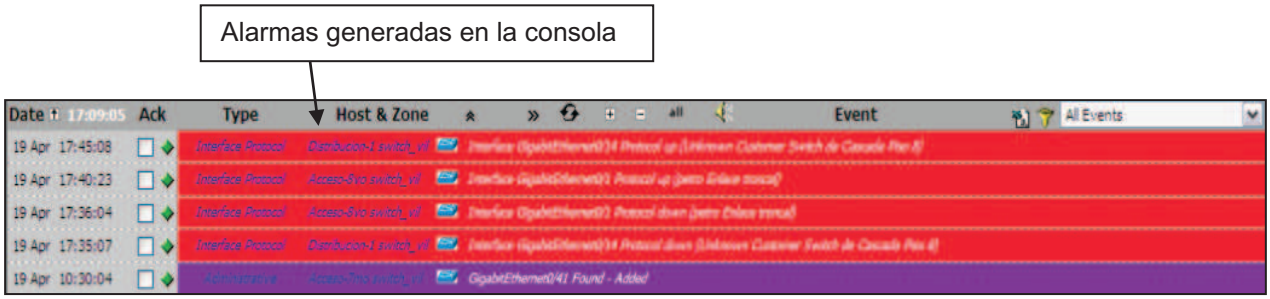
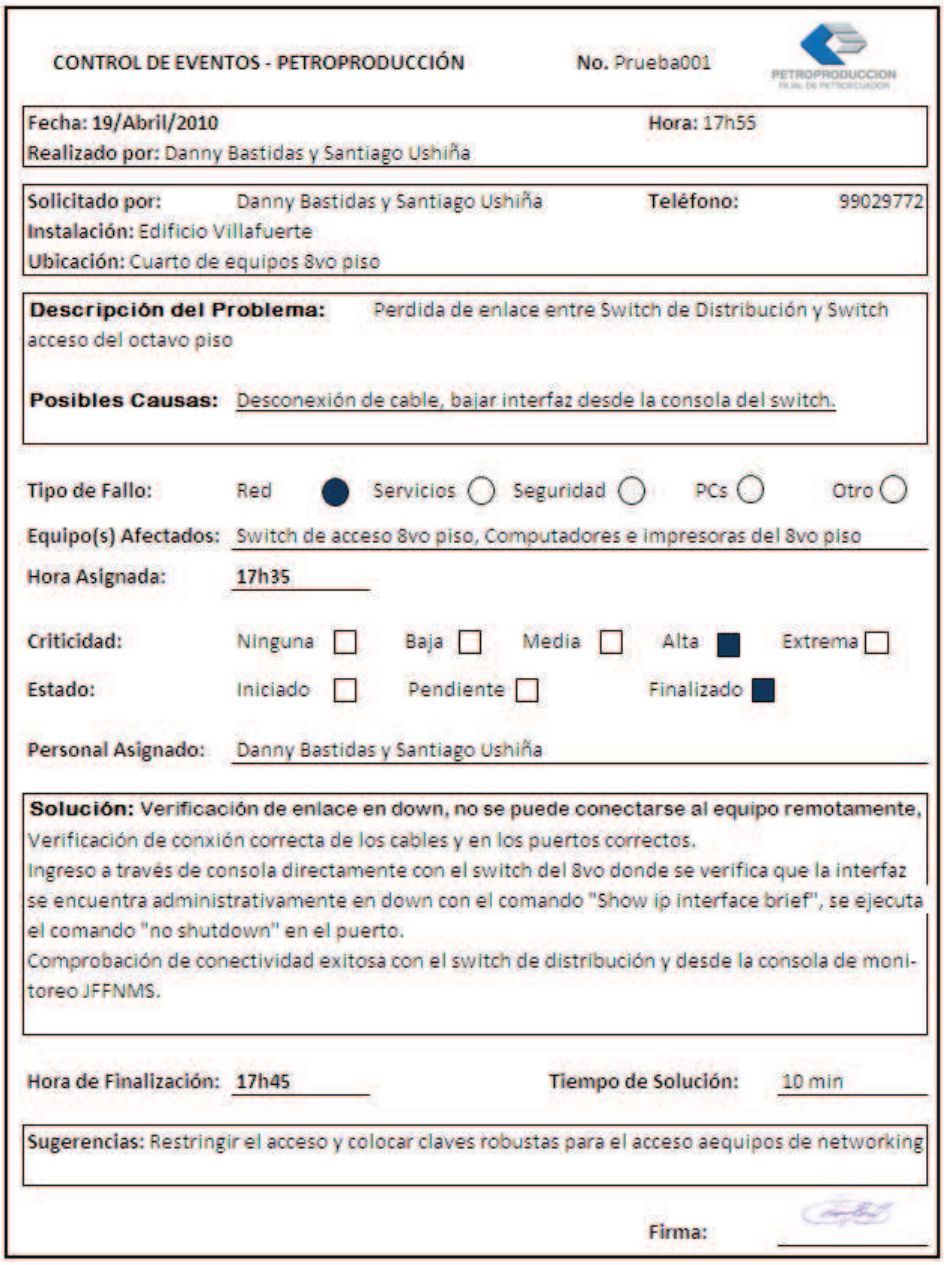


Figura 4-26.- Prueba-Eventos lanzados por detección de alarma

La notificación de las alarmas depende también del intervalo de poleo que se haya configurado a cada host en la administración, mientras menor sea el tiempo de poleo a un dispositivo, sus alarmas se generarán lo más cercanamente posible al tiempo real, JFFNMS tiene un periodo de poleo por default de 5 minutos.

La Figura 4-27 muestra el formato lleno de la prueba realizada, esta información debe ser registrada en una base de datos para que la solución sea consultada en caso de presencia de fallas similares.



CONTROL DE EVENTOS - PETROPRODUCCIÓN No. Prueba001

PETROPRODUCCION

Fecha: 19/Abril/2010 Hora: 17h55
Realizado por: Danny Bastidas y Santiago Ushiña

Solicitado por: Danny Bastidas y Santiago Ushiña Teléfono: 99029772
Instalación: Edificio Villafuerte
Ubicación: Cuarto de equipos 8vo piso

Descripción del Problema: Perdida de enlace entre Switch de Distribución y Switch acceso del octavo piso

Posibles Causas: Desconexión de cable, bajar interfaz desde la consola del switch.

Tipo de Fallo: Red ● Servicios ○ Seguridad ○ PCs ○ Otro ○

Equipo(s) Afectados: Switch de acceso 8vo piso, Computadores e impresoras del 8vo piso

Hora Asignada: 17h35

Criticidad: Ninguna ☐ Baja ☐ Media ☐ Alta ■ Extrema ☐

Estado: Iniciado ☐ Pendiente ☐ Finalizado ■

Personal Asignado: Danny Bastidas y Santiago Ushiña

Solución: Verificación de enlace en down, no se puede conectarse al equipo remotamente, Verificación de conxión correcta de los cables y en los puertos correctos.
Ingreso a través de consola directamente con el switch del 8vo donde se verifica que la interfaz se encuentra administrativamente en down con el comando "Show ip interface brief", se ejecuta el comando "no shutdown" en el puerto.
Comprobación de conectividad exitosa con el switch de distribución y desde la consola de monitoreo JFFNMS.

Hora de Finalización: 17h45 Tiempo de Solución: 10 min

Sugerencias: Restringir el acceso y colocar claves robustas para el acceso aequipos de networking

Firma:

Figura 4-27.- Formato de registro de prueba realizada.

4.5.1.2. Alarmas en utilización de memoria Física.

En la Figura 4-28 se presenta la utilización de la memoria física como de la memoria cache en el servidor ASTARO, en donde se aprecia que trabajan en promedio al 89% y 100% respectivamente.

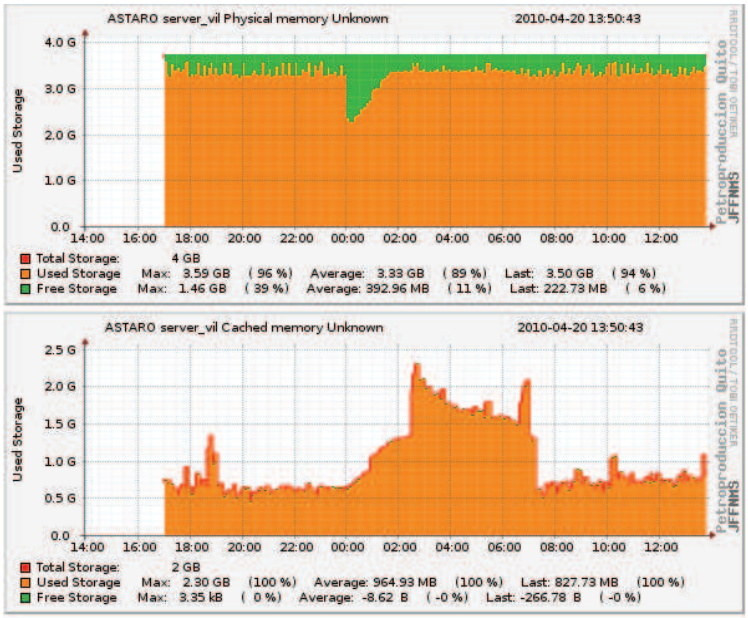


Figura 4-28.- Utilización Memoria del Servidor ASTARO.

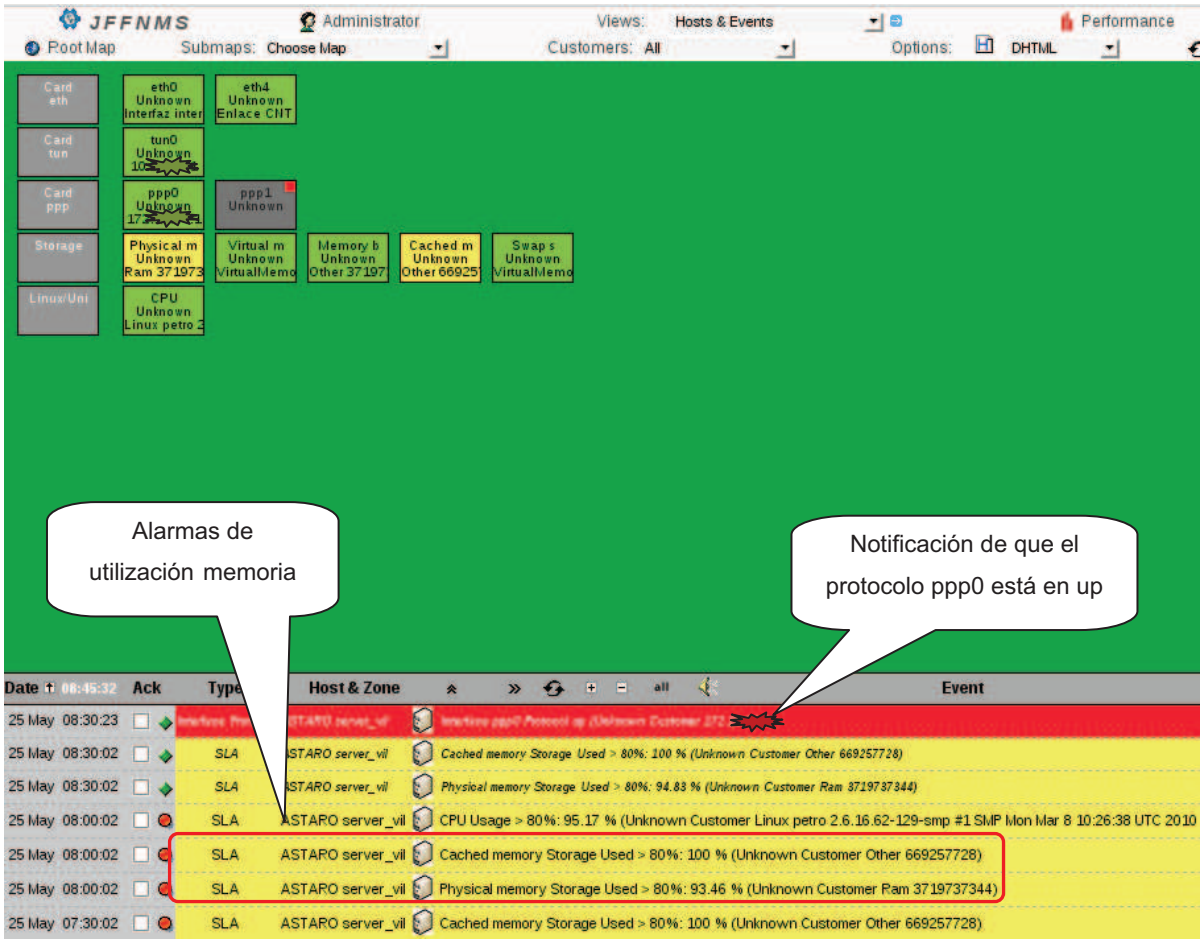


Figura 4-29.- Alarmas en utilización de memoria en servidor Astaro.

Las alarmas se encuentran configuradas cuando se detecte que se sobrepase el 75% de la capacidad de memoria, se tiene avisos continuos en los eventos de la consola hasta que el problema sea corregido como se aprecia en la Figura 4-29. Los avisos tienen configuración por defecto de notificar cada 30 minutos si el problema se sigue presentando.

4.5.1.3. Alarmas en utilización de disco Duro.

Los umbrales predefinidos en el capítulo 3 y ya configurados como se menciona en el punto 4.4.8, se definió que las alarmas de utilización de disco duro se presenten cuando esta sobrepase del 80% de su capacidad total para permitir al administrador tomar acciones antes de que se llene por completo el disco.

La Figura 4-30 presenta las alertas generadas por el servidor de correo del edificio Tribuna puesto que sus discos duros D: y F: se encuentran completamente llenos. Esto es posible debido a que el servidor escribe nuevos archivos en el disco pero va eliminando los archivos más antiguos para lograrlo.

Figura 4-30.- Alarmas en utilización de disco duro de servidor de Correo.

4.5.1.4. Comparación de datos y Veracidad de información capturada.

Para la comparativa de resultados capturados se escoge al dispositivo Astaro Gateway como ejemplo representativo por ser un servidor de gran utilización en la organización y por tener sus capturas del análisis de la red realizado en el capítulo 2.

La Figura 4-31 y la Figura 4-32 presentan el monitoreo del trafico y utilización de las interfaces eht0 (interna) y eth4 (externa) que se encuentran activas en el servidor, se presentan los resultados de Inbound y Outbound. Donde se puede apreciar el aumento considerable del tráfico a partir de las 8h00, hora de ingreso del personal a sus áreas de trabajo e inicio de las actividades empresariales.

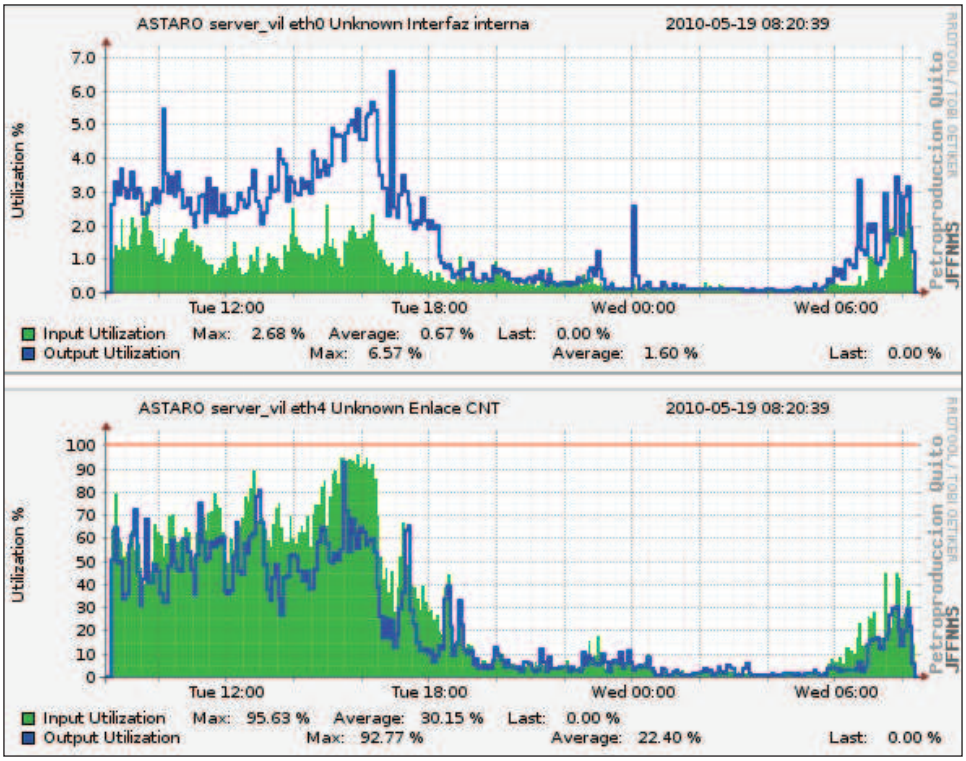


Figura 4-31.- Utilización de las interfaces del Servidor Astaro, diario.

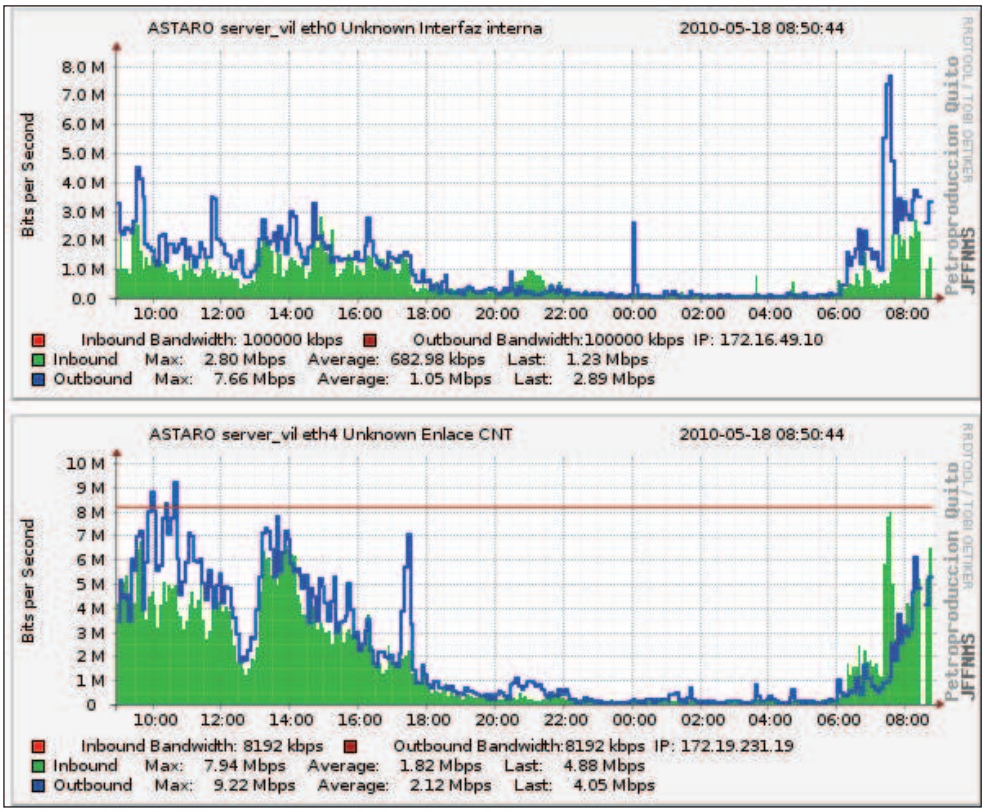


Figura 4-32.- Tráfico en Interfaces Ethernet servidor Astaro tomado del JFFNMS.

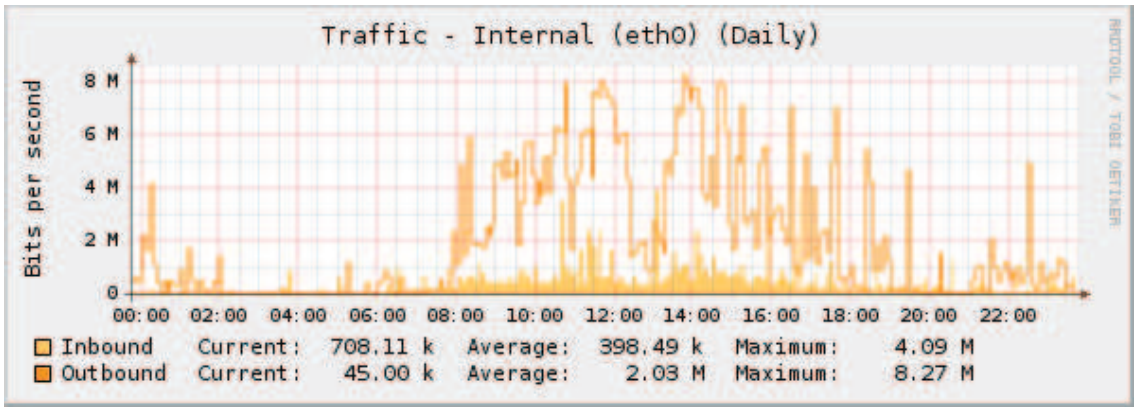


Figura 4-33.- Análisis de tráfico de la interfaz eth0 tomado del servidor Astaro.

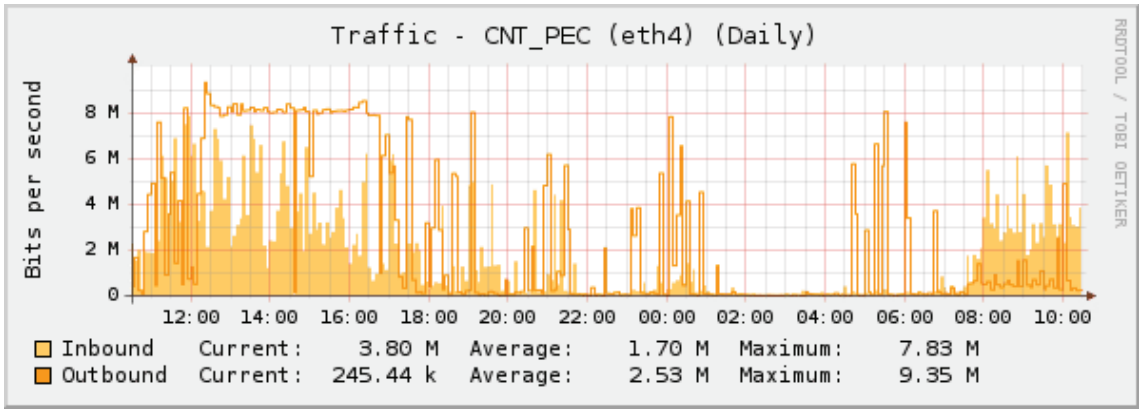


Figura 4-34.- Análisis de tráfico de la interfaz eth4 tomado del servidor Astaro.

La Figura 4-33 y la Figura 4-34 son tomadas del Anexo A para realizar una comparación gráfica con las capturas realizadas por el servidor de monitoreo JFFNMS. En la siguiente tabla de resultados de las gráficas del tráfico se puede apreciar que los datos obtenidos son similares, principalmente en lo referente a valores promedio y máximo de la interfaz eth 4 tanto en Inbound y outbound en la captura diaria, comprobando que la herramienta esta capturando datos reales.

De igual manera en las siguientes figuras se realiza esta comparación en un periodo de monitoreo semanal.

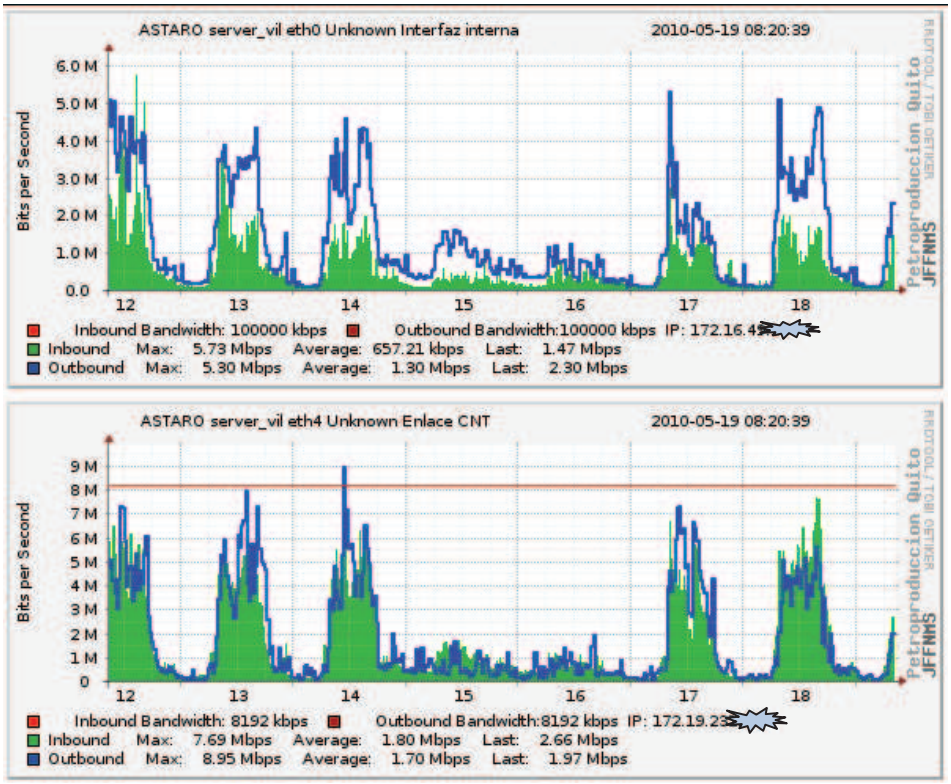


Figura 4-35.- Tráfico servidor Astaro semanal tomado del JFFNMS.

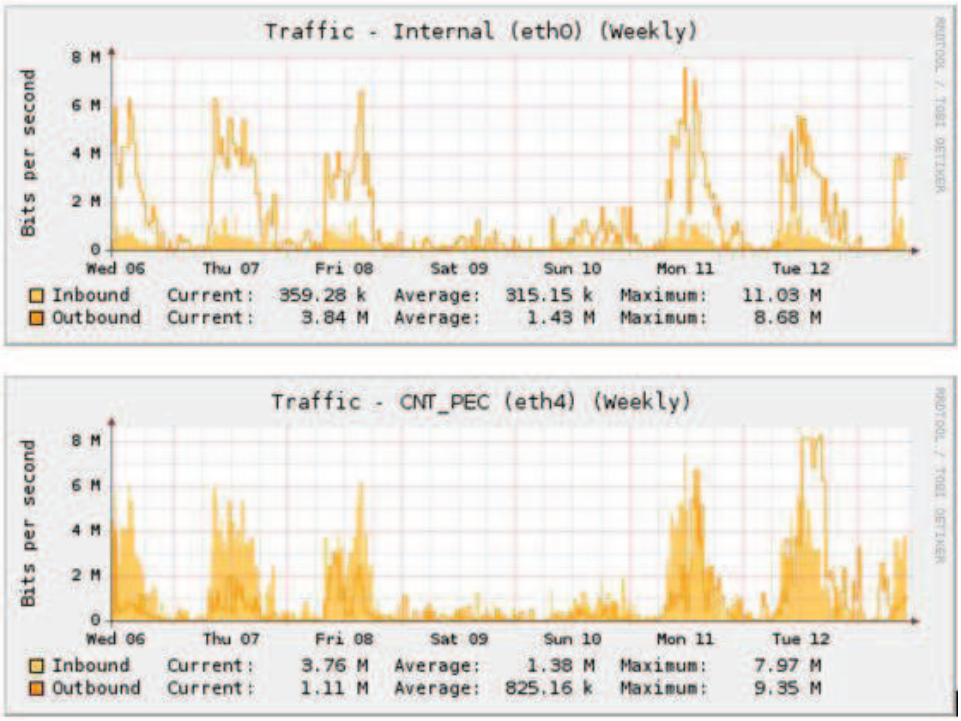


Figura 4-36.- Tráfico servidor Astaro semanal tomado del Astaro.

JFFNMS			ASTARO		
DIARIO			**DIARIO**		
INBOUND ETH 0	Promedio	682.98 kbps	**INBOUND ETH 0**	Promedio	398.49 kbps
	Máximo	2.80 Mbps		Máximo	4.09 Mbps
OUTBOUND ETH 0	Promedio	1.05 Mbps	**OUTBOUND ETH 0**	Promedio	2.03 Mbps
	Máximo	7.66 Mbps		Máximo	8.27 Mbps
INBOUND ETH 4	Promedio	1.82 Mbps	**INBOUND ETH 4**	Promedio	1.7 Mbps
	Máximo	7.84 Mbps		Máximo	7.83 Mbps
OUTBOUND ETH 4	Promedio	2.12 Mbps	**OUTBOUND ETH 4**	Promedio	2.53 Mbps
	Máximo	9.22 Mbps		Máximo	9.35 Mbps
SEMANAL			**SEMANAL**		
INBOUND ETH 0	Promedio	657.21 kbps	**INBOUND ETH 0**	Promedio	315.15 kbps
	Máximo	5.73 Mbps		Máximo	11.03 Mbps
OUTBOUND ETH 0	Promedio	1.30 Mbps	**OUTBOUND ETH 0**	Promedio	1.43 Mbps
	Máximo	5.30 Mbps		Máximo	8.68 Mbps
INBOUND ETH 4	Promedio	1.80 Mbps	**INBOUND ETH 4**	Promedio	1.38 Mbps
	Máximo	7.69 Mbps		Máximo	7.97 Mbps
OUTBOUND ETH 4	Promedio	1.70 Mbps	**OUTBOUND ETH 4**	Promedio	825.2 Kbps
	Máximo	8.95 Mbps		Máximo	9.35 Mbps

Tabla 4-6.- Comparación valores tomados de interfaces de servidor Astaro.

En la comparación de las capturas en el periodo de una semana, en las del servidor Astaro se puede apreciar que los valores de 11.03 Mbps en inbound y de 8.68 Mbps en outbound son picos inusuales como se aprecia en la Figura 4-36, y gráficamente se puede visualizar la similitud de las estadísticas de datos del tráfico en las dos interfaces

A continuación se muestran capturas de monitoreo de las demás interfaces del servidor Astaro.

La Figura 4-37 presenta el promedio de carga del CPU en tres intervalos de tiempo que son en un minuto, 5 minutos y 15 minutos. Dando una visión general para encontrar puntos picos producidos.

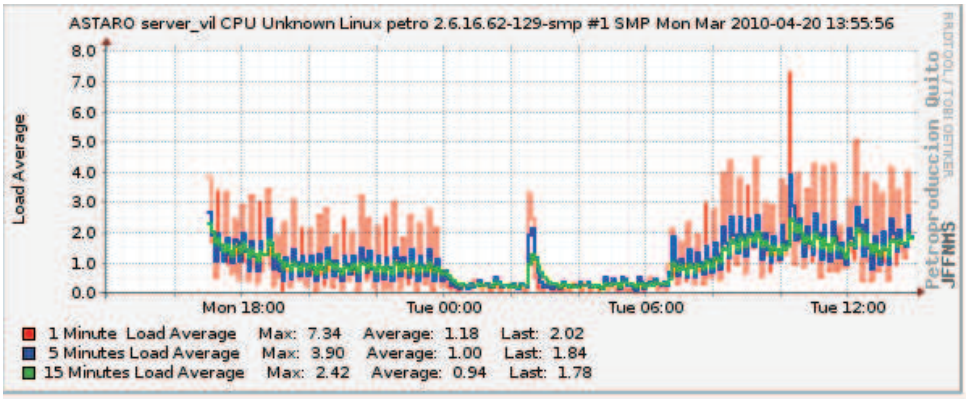


Figura 4-37.- Promedio de Carga de CPU del Servidor ASTARO.

Como se muestra en la Figura 4-38, se puede también presentar los resultados en resumen, en lo referente al tráfico y al uso de la memoria, permitiendo tener una visión global para un análisis inicial en caso de ser necesario.

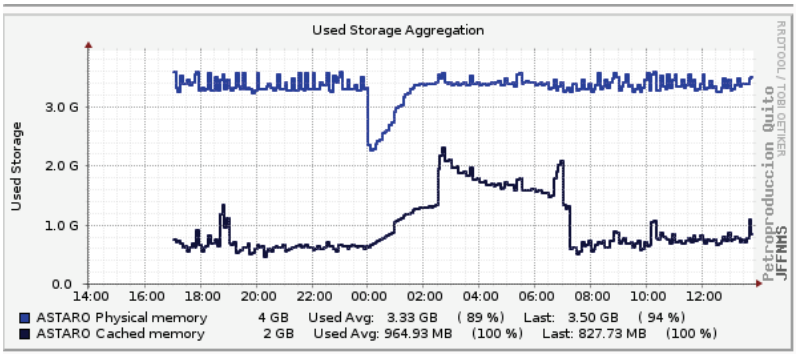


Figura 4-38.- Agregación de Memoria del servidor ASTARO.

Se tiene la posibilidad de visualizar el estado de las conexiones TCP del servidor que se esté monitoreando como lo muestra la Figura 4-39 del servidor Astaro.

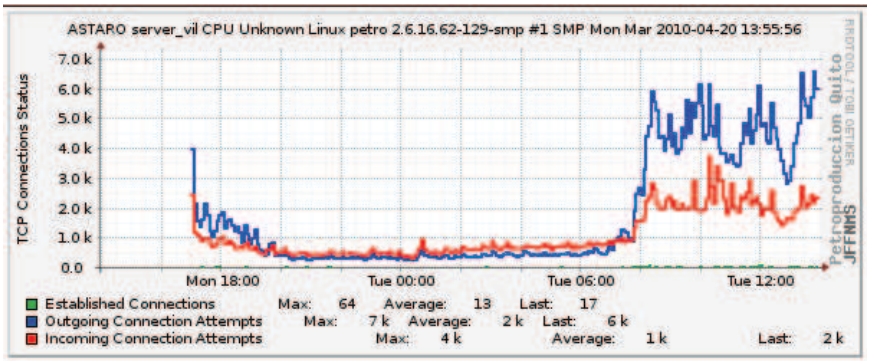


Figura 4-39.- Estado de las Conexiones TCP en el servidor ASTARO

Para casos de análisis y verificación del funcionamiento de las interfaces del servidor se puede visualizar los paquetes perdidos, en la Figura 4-40 se aprecia que en el corto periodo de tiempo monitoreado no se tienen paquetes perdidos en las interfaces eth0 y eth4.

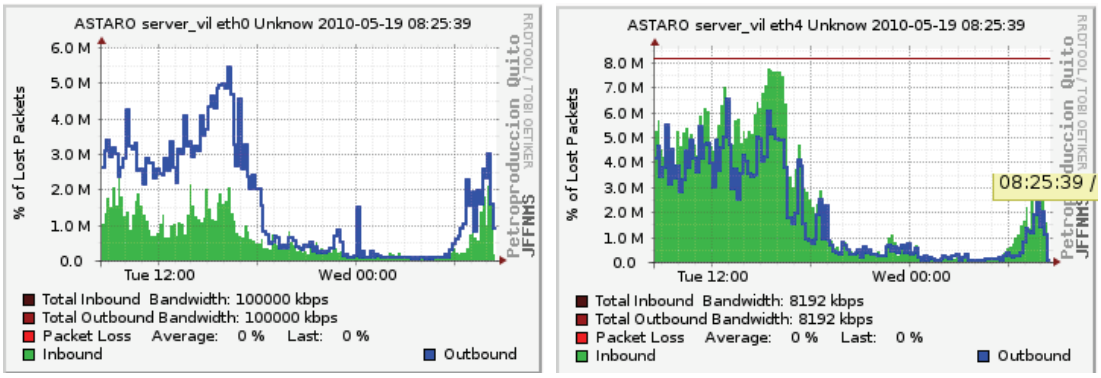


Figura 4-40.- Paquetes Perdidos Servidor ASTARO.

4.5.1.5. Monitoreo de equipos de Networking

Para el análisis de equipos de networking se escoge como dispositivos representativos el router principal del edificio Villafuerte y el switch de core (catalys 4507).

4.5.1.5.1. Router

Las siguientes figuras presentan resultados del monitoreo del router principal del edificio Villafuerte, donde están configuradas interfaces Ethernet y seriales que son enlaces importantes dentro de la conectividad de Petroproducción.

Se puede apreciar imágenes del puerto Ge0/0 que se conecta a la LAN interna del edificio Villafuerte, el tráfico y porcentaje de utilización de los diferentes seriales que son enlaces con el router Tribuna, San Rafael, Bodega de Transito y Lago Agrio. Además otros resultados que son monitoreados por JFFNMS como el RTT(Round to Trip), paquetes perdidos, errores, paquetes descartados, la temperatura, la utilización de procesamiento y memoria del dispositivo.

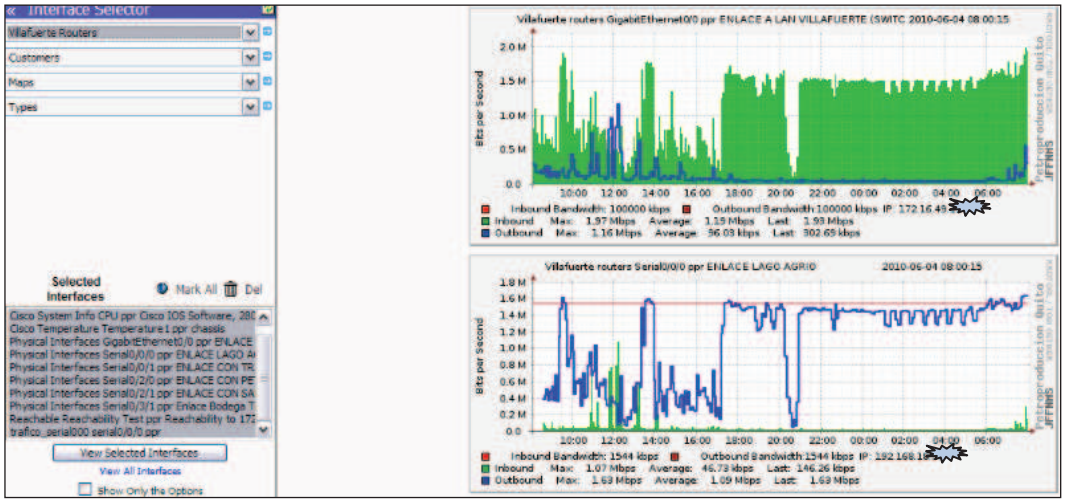


Figura 4-41.- Monitoreo de interfaces del router Villafuerte (Parte I)

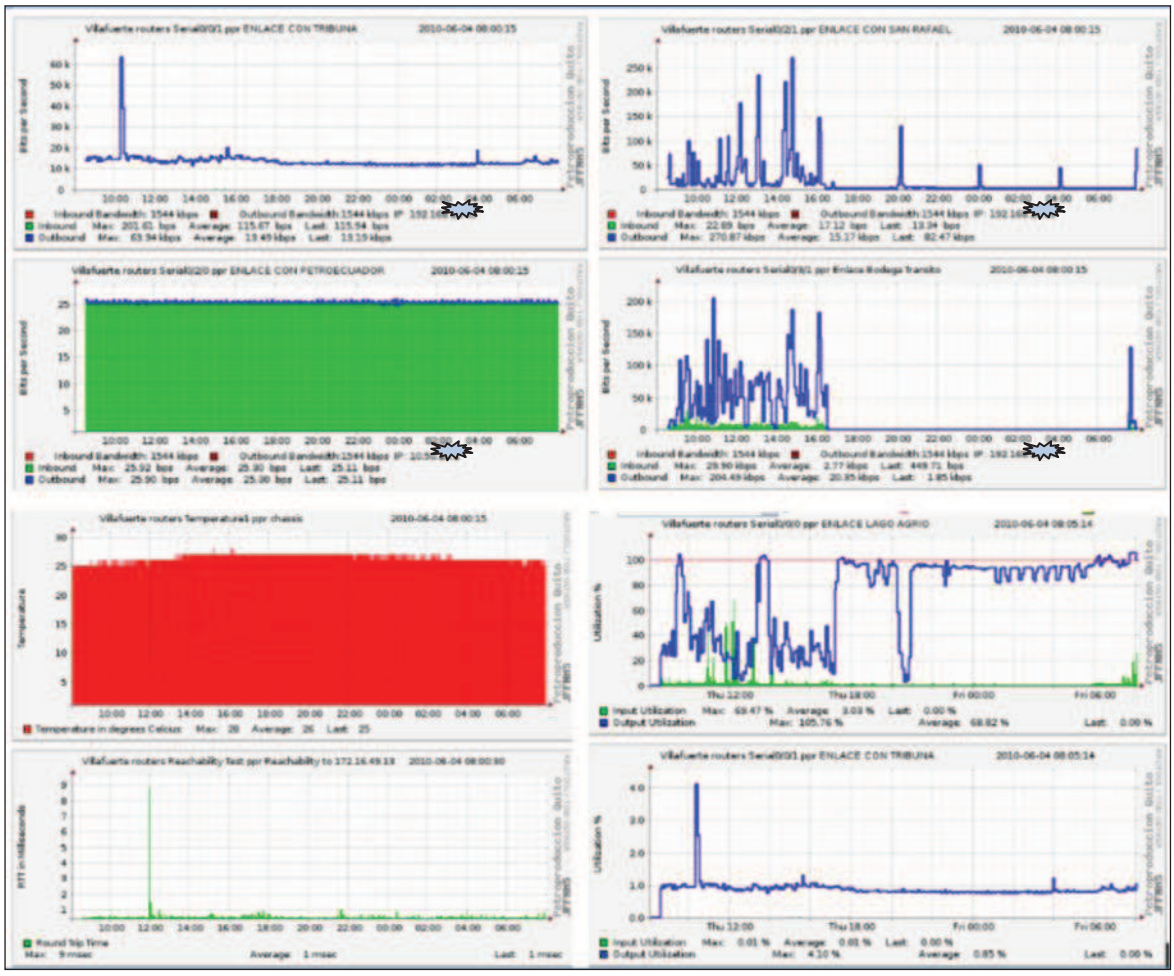


Figura 4-42.- Monitoreo de interfaces del router Villafuerte (Parte II)

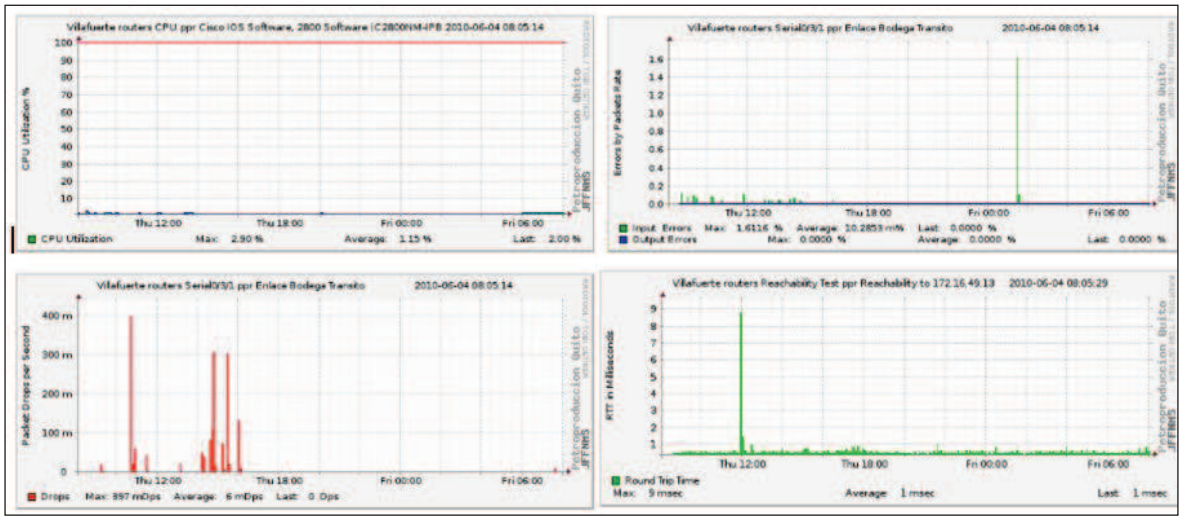


Figura 4-43.- Monitoreo de interfaces del router Villafuerte (Parte III)

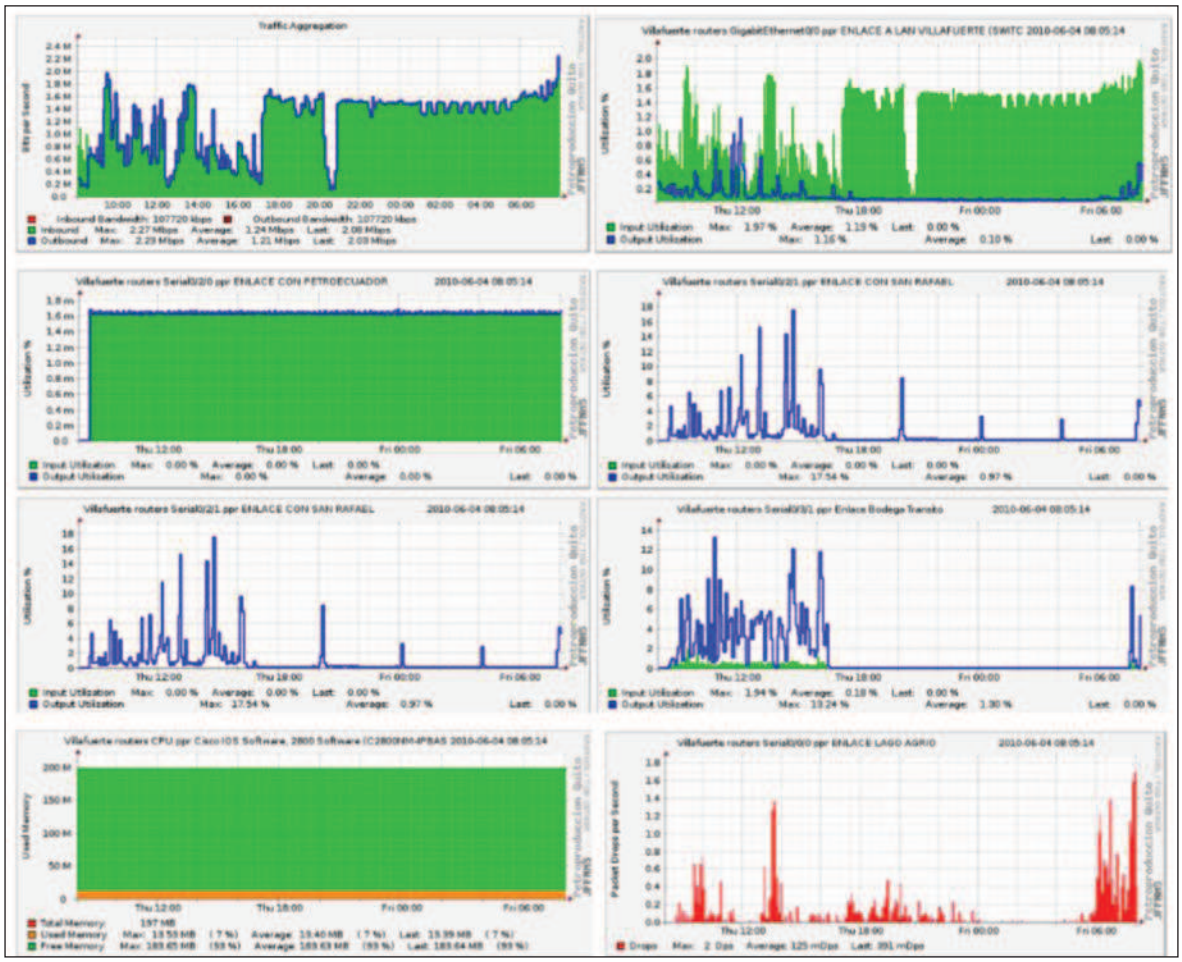


Figura 4-44.- Monitoreo de interfaces del router Villafuerte (Parte IV)

4.5.1.5.2. Switch de Core.

La siguiente figura presentan varios resultados del monitoreo del Switch de core, donde están configuradas interfaces Ethernet que son enlaces importantes dentro de la conectividad de Petroproducción.

Se puede apreciar la utilización del procesamiento del switch, el uso de memoria, temperatura, un ejemplo de visualización de paquetes perdidos el cual es mínimo que no se puede mirar a simple vista y la gráfica muestra un promedio de 0%, y por último el porcentaje de utilización en las interfaces Ge6/31 y Ge 5/16 que son enlaces de cascada hacia Switches de distribución y acceso.

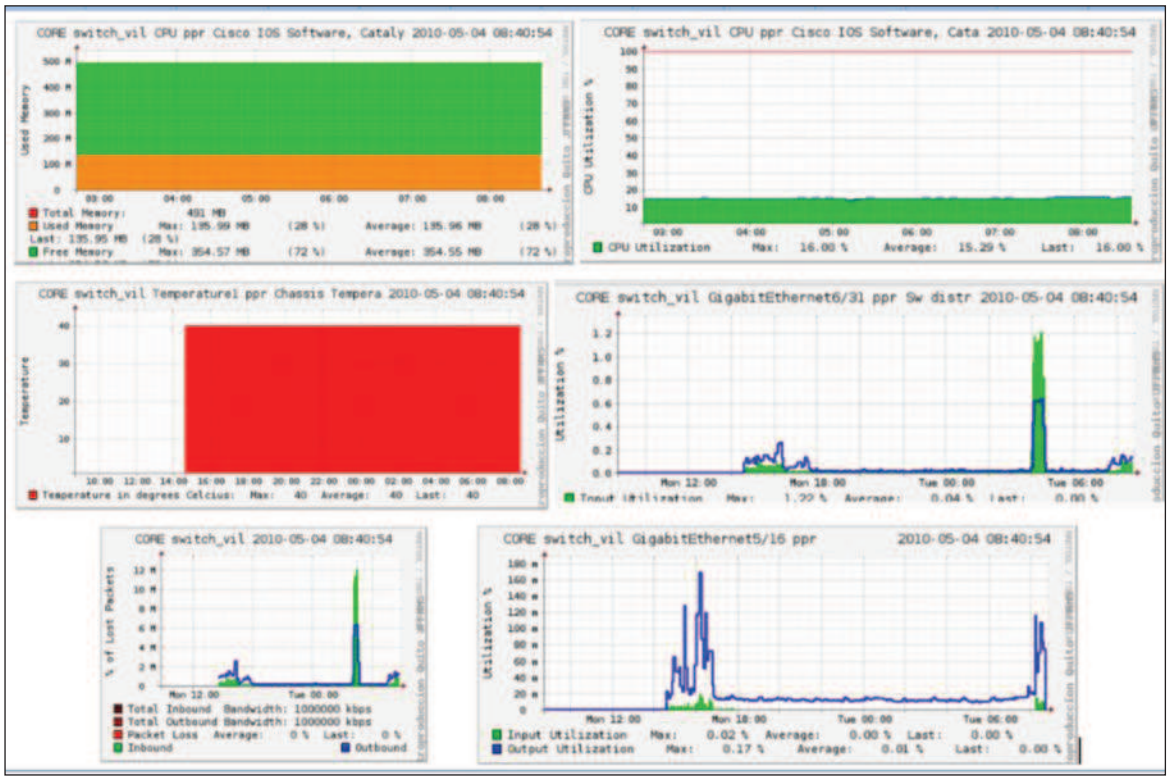


Figura 4-45.- Imágenes de Monitoreo de Switch de Core Catalyst 4507

4.6. RESULTADOS DEL MONITOREO

La utilización de la herramienta de monitoreo JFFNMS permite tener una visión global de los dispositivos configurados, su comportamiento y cuáles son los problemas que presentan, siendo esta la principal utilidad en Petroproducción ya que permite a los administradores verificar puntos a resolver dentro de la red y permitir mayor eficiencia en rendimiento. El monitoreo con una herramienta como el JFFNMS es el primer paso en el proceso troubleshooting de manera proactiva por parte de los administradores.

Mediante un proceso de análisis de datos, se tabulan los resultados en las siguientes tablas:

La Tabla 4-7 presenta las eventos generados, las interfaces monitoreadas de los Servidores de la red mencionados en el punto 4.3, la zona a la que

pertenecen, porcentaje de utilización promedio de la interfaz tomado en el periodo de monitoreo que fue desde el martes 20 de abril hasta el 4 de Junio de 2010.

EQUIPO	ZONA	INTERFAZ	UTILIZACION PROMEDIO	EVENTOS
A.D, DNS Y CORREO	Distrito Amazónico	Conectividad	OK	Perdida de comunicación momentáneas en abril.
ASTARO	Server_vill	Memoria Caché	98%	En memoria Caché y memoria Física se presenta alerta permanentes por trabajar sobre el 75% definido como Umbral límite. . Las interfaces de Protocolos PPP0 y PPP1 varian de up/down porque son interfaces de administración..
		Memoria Física	88%	
		Memoria Swap	10%	
		Memoria Virtual	68%	
		Uso CPU	25%	
		Protocolo PPP0	20%	
		Protocolo PPP1	5%	
		Eth 0 (Interfaz interna)	4.74%	
		Eth 4 (Enlace CNT)	70%	
		Estados Conexiones TCP	IN: 4K	
			OUT: 2K	
CORREO	Server_Tri	Memoria Física	63%	
		Memoria Virtual	44%	
		Uso CPU	10.30%	
		Utilización DISCO F:	100%	Alarma permanente por que el porcentaje de utilización está sobre 80%.
		Utilización DISCO D:	100%	Alarma permanente por que el porcentaje de utilización está sobre 80%.
		Utilización DISCO C:	17%	
		Utilización DISCO E:	49%	
		Utilización DISCO K:	58%	
		TCP Conection status	IN: 645	
			OUT: 99	
		IIS - bytes recived	10k	
FILE SERVER	Server_vill	Memoria Física	37%	
		Uso CPU	10.26%	
		Utilización DISCO G:	98.00%	Alarma permanente por que el porcentaje de utilización está sobre 80%.
		Utilización DISCO C:	49%	OK
		Utilización DISCO D:	65%	
		Utilización DISCO F:	48%	
		Conectividad	ok	

Continúa en la página 203.

EQUIPO	ZONA	INTERFAZ	UTILIZACION PROMEDIO	EVENTOS
JFFNMS	Server_vill	Memoria Física	96%	Alarma Permanente por que la memoria del servidor pasa ocupada sobre el 75% de su totalidad.
		Uso CPU	20%	
		Espacio utilizado en /	5%	
		Memoria Virtual	25%	
		Tarjeta Eth0	0.25%	
LOTUS	Server_Vill	Memoria Física	60%	OK
		Memoria Virtual	30%	
		Uso CPU	3.26%	
		Utilización DISCO C:	15%	
		Utilización DISCO E:	7%	
		Conectividad	ok	
LOTUS	Server_Tri	Memoria Física	58%	OK
		Memoria Virtual	36%	
		Uso CPU	3.26%	
		Utilización DISCO C:	8%	
		Utilización DISCO E:	3%	
		Conectividad	ok	
AS 400 - PAMLAGO	Distrito Amazónico	Uso CPU	13%	
		Utilización DISCO (system ASP)	68%	
		RAM1	95%	En memoria se presenta alertas permanentes por trabajar sobre el 75% definido como Umbral límite.
		RAM2	96%	
		RAM3	97%	
		RAM4	97%	
		Ethernet card.	0.3%	
		Conectividad	ok	
AS 400 - PPRO2	Distrito Amazónico	Uso CPU	9%	
		Utilización DISCO (system ASP)	78%	La Utilización del disco está al borde de sobrepasar el umbral límite.
		RAM1	97%	En memoria se presenta alerta permanentes por trabajar sobre el 75% definido como Umbral límite.
		RAM2	97%	
		RAM3	97%	
		RAM4	97%	
		Ethernet card.	0.20%	
		Conectividad	ok	
AS 400 - PPRQ1A	Server_vill	Uso CPU	8%	
		Utilización DISCO (system ASP)	53%	
		RAM1	99%	En memoria se presenta alerta permanentes por trabajar sobre el 75% definido como Umbral límite.
		RAM2	99%	
		RAM3	99%	

Continúa en la página 204.

EQUIPO	ZONA	INTERFAZ	UTILIZACION PROMEDIO	EVENTOS
		RAM4	99%	
		Ethernet card.	0.04%	
		Conectividad	ok	
AS 400 -PPRQ3A	Server_vill	Uso CPU	13%	
		Utilización DISCO (system ASP)	0.85	Alarma permanente por que el porcentaje de utilización está sobre 80%.
		RAM1	98%	En memoria se presenta alerta permanentes por trabajar sobre el 75% definido como Umbral límite.
		RAM2	98%	
		RAM3	98%	
		RAM4	98%	
		Ethernet card.	0.60%	
		Conectividad	ok	

Tabla 4-7.- Resumen monitoreo de servidores

La Tabla 4-8 muestra las interfaces monitoreadas en el Switch de Core y de Distribución que se encuentran en el edificio Villafuerte. Presentando como resultado que estos se encuentran con su capacidad operativa en buen nivel, ya que no presentan ningún problema y los rangos promedios de CPU y Memoria principalmente están bajo los umbrales establecidos.

EQUIPO	ZONA	INTERFAZ (Conectado a)	UTILIZACION PROMEDIO
CORE (CATALYST 4507)	Switch_vill	Uso CPU	15.55%
		Memoria	28%
		GigaEth3/3 (Sissw20)	40%
		GigaEth3/4 (Sissw19)	10%
		GigaEth3/5 (SwMoscu)	20%
		GigaEth3/8 (Sissw25)	5.00%
		GigaEth3/9 (Sissw08)	12%
		GigaEth6/31 (Sw Distribución)	11%
		GigaEth3/10 (Sissw14)	4.00%
		GigaEth5/14	10%
		GigaEth5/15	5.00%
		GigaEth5/16	0.10%
		Temperatura Chasis	36ºC
DISTRIBUCIÓN-1	Switch_vill	Uso CPU	6.21%
		Memoria Cisco	19%
		GigaEth 0/1 (Cascada Piso 5)	0.38%
		GigaEth 0/2 (Cascada Piso 1)	0.92%

Continúa en la página 205.

EQUIPO	ZONA	INTERFAZ (Conectado a)	UTILIZACION PROMEDIO
		GigaEth 0/3 (Cascada Piso 4)	0.20%
		GigaEth 0/4 (Cascada Piso 3)	0.50%
		GigaEth 0/6 (Cascada Piso 2)	1.60%
		GigaEth 0/11 (Cascada MZ)	1.90%
		GigaEth 0/13 (Cascada Piso 6)	3.10%
		GigaEth 0/16 (Cascada Piso 7)	1.55%
		GigaEth 0/44 (Enlace Sw Core)	12.10%
		GigaEth 0/45 (C2950T Sistemas)	32.30%

Tabla 4-8.- Resumen Switches críticos

La Tabla 4-9 muestra el resumen de utilización de los dispositivos de acceso del 8vo piso y del mezanine del Edificio Villafuerte. La única alarma que se tiene en el periodo del monitoreo es la realizada en la prueba donde se bajó la interfaz del Switch del 8vo piso como se explicó en el punto 4.5.1.1.

EQUIPO	ZONA	INTERFAZ	UTILIZACION PROMEDIO
Acceso-8vo (Cisco 2960)	Switch_vill	Uso CPU	5.40%
		Memoria Cisco	18%
		GigaEth 0/1 (Troncal)	1.40%
Mezanine2	Switch_vill	Uso CPU	20.54%
		FastEth 0/1	0.60%
		FastEth 0/47	33.10%
		FastEth 0/48	6%
		Conectividad	OK

Tabla 4-9.- Interfaces Switches Acceso (Villafuerte)

La Tabla 4-10 presenta las interfaces monitoreadas de los Routers del edificio Villafuerte y del edificio Tribuna con sus porcentajes de utilización, además muestra la conectividad con el Router de Lago Agrio. Su capacidad de Procesamiento y Memoria están dentro del Umbral óptimo, los enlaces tienen momentos picos pero no por periodos largos de tiempo por lo que no requieren de una acción contra fallo.

EQUIPO	ZONA	INTERFAZ	UTILIZACION PROMEDIO
VILLAFUERTE	ROUTERS	Uso CPU	2%
		Memoria	7%
		GigaEth 0/0 (Enlace a LAN Villafuerte)	2%
		serial 0/3/1 (Bodega Transito)	6%
		Serial 0/0/0 (Enlace Lago Agrio)	40%
		Serial 0/0/1 (Enlace Tribuna)	1%
		Serial 0/2/0 (Enlace Petroecuador)	0.01
		Serial 0/2/1 (Enlace san Rafael)	4%
		Temperatura	27ºC
TRIBUNA	ROUTERS	Uso CPU	4.60%
		Memoria Cisco	7%
		FasthEth0/1/0	30%
		GigaEth 0/0 (Gw Tribuna)	2%
		GigaEth 0/1 (Puerta enlace 18.13)	3%
		Serial 0/0/0 (Router Villafuerte)	0.01%
		Conectividad	100%
		Temperatura	26ºC
LAGO AGRIO	ROUTERS	Conectividad	OK

Tabla 4-10.- Resumen Routers Petroproducción.

4.7. APLICACIÓN DE SOLUCIONES

4.7.1. MONITOREO

Una vez analizadas las diferentes interfaces de los servidores monitoreados y verificando los resultados de los eventos o alarmas lanzadas en la consola se presentan las siguientes propuestas para solucionar los problemas presentes en PPR, se recalca la importancia de seguir el proceso de Troubleshooting descrito en capitulo 3 para atacar las fallas en los dispositivos de PPR.

La Tabla 4-11 presenta las alarmas que se mantienen y las soluciones a considerar.

DISPOSITIVO	ALARMA	SOLUCIÓN PROPUESTA
Astaro, JFFNMS, Web, AS-400(2 UIO y 2 D.A)	Utilización Memoria Física > 75 %	Estudio de los procesos que corren en el servidor, cuales son realmente necesarios y cuales consumen recursos y pueden ser detenidos para minimizar la carga de utilización de memoria.
		Ampliación de Memoria RAM en el servidor.
		Redimensionamiento de la capacidad de memoria.
Servidor Correo(Tribuna), File Server (Vill), Exchange(Vill)	Utilización disco Duro > 80%	Añadir un disco duro de gran capacidad y re-direccionar los archivos al nuevo disco.
		Sacar Backups periódicos de la información de los discos duros.
		Eliminar archivos antiguos y se encuentran respaldados en caso de necesitarlos.
		Eliminación de archivos temporales.
Router Lago Agrio	Perdida paquetes de Ping (Conectividad)	Verificación del enlace este correcto.
		Comprobar que las conexiones finales del enlace estén correctas.
		Seguimiento del camino del enlace y tiempos de respuesta con el comando “tracert” o “traceroute”.
		Controlar el acceso en Lago Agrio al cuarto de Equipos y mantener un cableado correcto para evitar problemas.
		Verificación de no existencia de cambios de direccionamiento IP.
Dispositivo en General	No monitorea o no recibe datos de interfaces configuradas.	Verificación de que el agente SNMP del dispositivo se encuentre activo y correctamente configurado.
		Comprobación de configuración en la consola de administración especialmente la dirección IP del dispositivo y la comunidad SNMP.
		En Switches y Routers comprobación de vistas configuradas en SNMP que permita la obtención de datos de interfaces (Seriales o Ethernet).

Tabla 4-11.- Propuesta de Soluciones

En las soluciones presentadas que ameritan la desconexión momentánea de los servidores, los administradores encargados de resolver el problema deberán sujetarse al procedimiento de resolución de fallos planteado en el capítulo 3, que consiste en aislar el problema para evitar afectación al resto de la red, verificar que el tiempo para quitar el servicio sea fuera de horarios de oficina, se recomienda hacerla en horas nocturnas y que la solución sea transparente para los usuarios. Como último paso documentar y detallar todo el proceso realizado en la plantilla presentada en el punto 3.3.4.3 del plan de

contingencia ante fallos. Se puede hacer referencia a la tabla 3-11 de solución de fallos en discos.

La tabla 3-12 presenta el procedimiento ante fallos de enlaces de comunicaciones y recomienda que los enlaces sean monitoreados constantemente, además para evitar estos problemas es importante dar mantenimiento a los equipos de networking, en caso de que un enlace falle implica perdida de comunicación entre los diferentes departamentos de la organización.
En base a la metodología buttom-up en cuestión de enlaces se debe revisar que los cables estén correctamente conectados, los conectores bien ponchados, realizar un tester del cable, esto debido a que los errores suelen estar en la capa física comúnmente. Posterior a estas verificaciones se deben realizar pruebas hasta determinar cuál es el motivo de la falla presentada.

Es importante tener en cuenta en cumplimiento de los tiempos máximos a resolver los fallos según su severidad como se determina en el punto 3.3.4.1.5, siendo factor importante para mantener un buen rendimiento en la red.

En la gestión de monitoreo tener presente que las interfaces analizadas no lleguen a sobrepasar los umbrales límites establecidos, cuando los valores capturados lleguen al nivel de prevención, los administradores del NOC ya deberán verificar cuales son los motivos principales que generan el aumento inesperado de la utilización de la interfaz y buscar soluciones que controlen el problema antes de que llegue afectar a la red.

Cuando un host o interfaz se aprecia como down en la consola de monitoreo, la primera prueba es comprobar que en efecto está caída la interfaz realizando pruebas con el comando ping, traceroute, ó un get manual del agente snmp. Puede tratarse de una falsa alarma por un retraso por parte del dispositivo en la respuesta al sondeo del JFFNMS generando que el “timeout” se active. Este es un problema no común pero que puede existir. Si todo esta correcto y no se restablece el estado a “up” se recomienda sondear nuevamente el equipo para

que lo detecte en el estado real que se encuentre. El reinicio del equipo agente será la última alternativa a aplicarse.

4.7.2. SEGURIDAD

- El comité de seguridad será el encargado de delegar el manejo de claves en servidores y equipos de networking para que su acceso sea restrictivo y junto con el personal del área de redes mantener un registro de ingreso a los diferentes cuartos de equipos y las actividades realizadas, para que mensualmente se tenga reportes con documentación del trabajo sobre los dispositivos.

- La creación de listas de acceso en ruteadores y Switches es recomendable que maneje el comité bajo políticas de seguridad previamente establecidas, advirtiendo el trafico que puede circular o denegar a través del dispositivo, así como el acceso a solo ciertos usuarios o direcciones IP para la administración de equipos.

- Habilitar el protocolo ssh y deshabilitar el uso de telnet en los equipos para incrementar la seguridad la seguridad en acceso remoto.

- Establecer un modelo de autenticación más sofisticado para acceso a equipos con privilegios administrativos en conjunto con un servidor de seguridad (TACACS+ o RADIUS).

- Es importante asegurar todas las configuraciones de equipos mediante copias y respaldos de archivos de configuración obtenidos cuando se realiza un cambio en el dispositivo.

- Eliminar las configuraciones snmp anteriores al proyecto y que están en desuso para manejar lo normado en el diseño del NOC.

Capítulo 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- El empleo del modelo FCAPS permitió analizar y gestionar los recursos a través de la creación de Áreas dentro del NOC, que conjuntamente con JFFNMS, ayuda en la detección de problemas y degradaciones en el desempeño de servidores críticos como Astaro Gateway y AS/400, equipo activo como routers de los edificios Tribuna y Villafuerte, además del switch de núcleo Cisco 4507. Esto permitirá elaborar estrategias que optimicen la infraestructura existente y mejoren el rendimiento de las comunicaciones, aplicaciones y servicios.

- El NOC se constituye en un ente gestionador de las Tecnologías de la Información para Petroproducción a lo largo del país, ayuda a mejorar índices de calidad en los servicios de comunicaciones generando alarmas al pasar umbrales de 75% en utilización de memoria, o el 80% de uso de un disco, lo que permite a los administradores ser proactivos ante fallos, y como consecuencia colaborando en el cumplimiento de la visión empresarial.

- La principal ventaja de implementar un NOC es tener un control centralizado de la red, permitiendo que la información se concentre en un solo punto al cual pueden acceder todos los operadores, atacando problemas y analizando estadísticas, igualmente posibilita el análisis de dispositivos y la toma de decisiones proactivas, en base al funcionamiento de los mismos y a la detección de anomalías en cualquier red empresarial.

- Los altos costos de licencias de software con similar servicio bordean los $5000 en promedio por año, a lo que se añade costos de soporte, dando

origen a la búsqueda de soluciones alternas económicas que cumplan con los requisitos de la empresa. Se desarrolló el presente proyecto aprovechando las ventajas del software libre mediante la herramienta de monitoreo JFFNMS que cubre las necesidades para monitoreo de un NOC, con una mínima inversión al emplear licencia GPL y con soporte libre en internet.

- La distribución Linux Debian 5.0.4 se presenta como una plataforma estable y de altas características en el manejo de servidores según estudio en base al estándar IEEE830, donde obtiene una puntuación de 79/80, siendo óptima para albergar cualesquier tipo de servidor y a la consola JFFNMS, reduciendo gastos a la empresa en uso de licencias.

- La generación de un lineamiento base permite tener una visión global de los puntos necesarios a enfatizar en el diseño del NOC, permitió determinar las horas pico de tráfico, servidores, equipos de conectividad con mayor carga operativa y el tipo de tráfico con más peso en la empresa definiendo al tráfico web (HTTP) con aproximadamente el 70% de datos y correo electrónico SMTP con un 20% del total del tráfico que circulan por la red.

- El sistema de monitoreo en producción mostró la importancia del seguimiento continuo a los equipos de comunicación y de servicios en la red, ya que los administradores se pudieron percatar que discos duros tenían su capacidad utilizada el 100%, o que otros servidores trabajan en su memoria física sobre el 90% del total como el caso del servidor proxy-firewall Astaro, dando la posibilidad de aplicar un mantenimiento preventivo para evitar complicaciones a futuro y cumpliendo con las expectativas del actual departamento de TIC.

- La creación de un Comité de Seguridad se presenta como un primer paso para la elaboración de un sistema de seguridad de la información que guíe a la empresa en actividades y genere políticas claras para preservar la

integridad del equipamiento físico, servicios, aplicaciones, recurso humano y en toda información circulante en la red.

- Una gestión de contabilidad complementa la gestión de monitoreo, determinando el uso actual de los recursos de la red mediante el análisis de estadísticas, tasas de errores, tiempos de respuesta, utilización de enlaces, recursos, entre otros. Esta gestión se pone en evidencia al tabular los datos obtenidos en el proyecto piloto planteado, en el cual se verifica que los routers están trabajando actualmente bajo el 10% de su capacidad, la razón es porque se tiene nuevo enlace de fibra y estos funcionan como backup.

- El Manual de Procedimientos ante Fallos se constituye en una ayuda importante para los administradores de red y para el personal de soporte técnico de Petroproducción, además brinda soluciones a problemáticas y sirve para encontrar correcciones a errores en equipo activo actualmente con tasas de error menor al 0,5% en el procesamiento de datos de dispositivos críticos, o enlaces sobrecargados por encima del 75% que podrían fallar.

- El establecimiento de umbrales se constituyó en la referencia para el lanzamiento de alarmas por parte de la consola JFFNMS, si bien se establecieron éstos a un valor del 75% de la capacidad operativa del elemento, dicho porcentaje varía y es ajustable en función de la criticidad e importancia que el NOC dé al elemento.

- La asignación de responsabilidades ayuda a Petroproducción a determinar quiénes son los encargados de atender los diferentes requerimientos de la empresa y mejorar el tiempo de respuesta ante un fallo al establecer un tiempo de solución entre 30 minutos hasta 15 días. En el proyecto se trata de cubrir los puntos no estimados en la actual organización y que son determinantes como seguridad, seguimiento a fallos, procedimientos de solución, monitoreo, entre otros, para mantener el rendimiento de la red.

- El sistema JFFNMS es una herramienta útil para Petroproducción que requiere un trabajo en conjunto con dispositivos adicionales existentes actualmente como la solución de seguridad Astaro, Manejador de Ancho de Banda Allot Enforcer y la herramienta de soporte a usuarios Resolve it, con la finalidad de obtener un control adecuado de toda la infraestructura.

- Para verificar el funcionamiento de la consola de monitoreo, en el proyecto piloto se realizaron pruebas y comparación de datos obtenidos de la herramienta JFFNMS, con los recogidos durante el análisis de la red actual del capítulo 2, con lo que se concluyó que los datos son correctos y que se dispone de una herramienta confiable para esta función.

- JFFNMS utiliza configuraciones básicas preestablecidas, que permiten un monitoreo global de cualquier red IP, sin embargo puede ser extensible y programable para monitorear nuevos parámetros. Esto implica un conocimiento en programación PHP a un bajo nivel, representando la principal desventaja del software, sin embargo, se posee documentación y una comunidad de apoyo en soluciones en el internet.

- De los resultados obtenidos del piloto se concluye que los problemas a tener consideración son el uso en exceso de discos duros y memoria física presentes en 8 de los servidores monitoreados, así Petroproducción pudo conocer falencias que eran transparentes e iniciar acciones preventivas sobre las fallas en los dispositivos alarmados teniendo control sobre sus equipos de comunicaciones.

5.2. RECOMENDACIONES

- Las plantillas propuestas para el seguimiento y control de fallos pueden ser ingresadas a una base de datos, otorgando al personal técnico un ahorro de tiempo tanto en la búsqueda de información de registros a problemas anteriores como ahorro en el tiempo de solución. Se recomienda tener esta base de datos como un servicio de red a disposición y alcance del personal del NOC, por ejemplo mediante la creación de una página web o su ingreso a través del portal electrónico actual de la empresa.

- Una vez identificado y puesto en marcha el plan de resolución a un problema, se recomienda que éste no sea cambiado en el transcurso de su ejecución, puesto que a la larga puede ser el causal de otro problema.

- Se recomienda hacer uso de la versión 2c de SNMP en el proceso de monitoreo a fin de no sobrecargar los recursos del servidor actual. A futuro se podrá plantear la utilización de la versión 3 con la autorización de las autoridades pertinentes para el acceso a los equipos.

- Se recomienda mantener el poleo manual de los dispositivos y la creación de nuevas alarmas para un mejor control, y seguir expandiendo la herramienta de monitoreo según las necesidades de la empresa.

- Una evaluación de las herramientas de monitoreo licenciadas existentes en el mercado es recomendable para realizar una comparación con sistemas Open Source, de tal manera que se pueda elegir la más adecuada a las necesidades de la empresa para una futura implementación a nivel de todo el territorio ecuatoriano.

- Cuando se instala software que es nuevo para los administradores se recomienda primero leer los archivos de configuración e instalación, analizar los requisitos de la herramienta para que esta pueda ser aprovechada al máximo. En este caso leer el manual de instalación de la NMS y datasheets

de cómo habilitar la ejecución del protocolo SNMP en los agentes a ser monitoreados.

- La documentación de los errores se recomienda que sea lo más detallada y explicativamente posible para tener un mejor efecto en la implementación del NOC y de las soluciones de posibles fallas reiteradas sobre los dispositivos de la red.

- Se recomienda poner énfasis en la creación de políticas de seguridad y normas que permitan llevar un control sobre la infraestructura física como: el acceso a cuartos de equipos, así como en la infraestructura lógica definiendo por ejemplo el cambio de claves periódicamente de los usuarios de la red.

- El manual de procedimientos ante fallos debe ser constantemente actualizado, modificando o añadiendo soluciones a los diferentes problemas que se vayan suscitando en la red a través del tiempo.

- En toda implementación es recomendable seguir con estándares que garantizan una correcta operatividad. Este proyecto hace mención a las normas ANSI/TIA/EIA-568B, ANSI/TIA/EIA-606, ISO 27002, entre otras.

- Al tener un sistema centralizado en el monitoreo se recomienda sacar respaldos periódicos de la herramienta. En caso de tener algún fallo de funcionamiento esta puede ser restaurada sin pérdida de datos de importancia para el análisis de resultados.

- De los resultados obtenidos del piloto se recomienda que pequeñas y medianas empresas posean herramientas como la presentada en este proyecto, pueden ser licenciadas si se requiere cosas más especificas o considerar el software libre como una buena opción que genera resultados y ayuda a la organización a tener control sobre sus dispositivos de comunicaciones.

GLOSARIO

- **AS/400** Equipo de IBM de gama media y alta, con un sistema multiusuario, interfaz controlada mediante menús y comandos CL (Control Language) y un sistema operativo basado en objetos y bibliotecas, OS/400.
- **Astaro** Simplifiying Network, Mail & Web Security
- **Bottom-Up** Estrategias de procesamiento de información características de las ciencias de la información.
- **CLI** Command line interface - Línea de comandos
- **CMIP** Common Management Information Protocol - Protocolo de Administración de Información Común
- **CMIP** Common Management Information Protocol - Common Management Information Services
- **CMISE** Common Management Information Service Element - Elemento de Servicio Común de Información de Gestión
- **CMOT** Common Management Information Protocol over TCP/IP
- **CNT** Corporación Nacional de Telecomunicaciones
- **COBIT** Control Objectives for Information and related Technology -
- **D.A.** Distrito Amazónico (instalaciones de Petroproducción en el oriente ecuatoriano)
- **DMZ** Demilitarized Zone - Zona Desmilitarizada
- **DNS** Domain Name System - Sistema de Nombre de Dominio
- **FCAPS** Fauls, Configuration, Accounting, Performance, Security
- **FTP** File Transfer Protocol -Protocolo de Transferencia de Archivos
- **GNU.** Proyecto que ha desarrollado un sistema completo de software libre llamado “GNU” (GNU No es Unix) que es compatible con Unix.

- **GNU-GPL** GNU General Public License - Licencia Pública General de GNU.
- **HTTP.** HyperText Transfer Protocol - Protocolo de Transferencia de Hipertexto.
- **HTTPS** Hypertext Transfer Protocol Secure - Protocolo de Transferencia de Hipertexto Seguro.
- **IEEE** Instituto de Ingenieros Electricistas y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización.
- **IETF** Internet Engineering Task Force.
- **IOS.** Sistema de Entrada y Salida (Input Output System). Es el sistema operativo de switches y ruteadores.
- **ISO** International Organization for Standardization - Organización Internacional para la Estandarización.
- **ISP** Internet Service Provider - Proveedor de servicios de Internet.
- **ITIL** Information Technology Infrastructure Library - Biblioteca de Infraestructura de Tecnologías de Información.
- **JFFNMS** Just For Fun Network Management System.
- **Log** Notificaciones que envía un agente a un gestor, sin que este le haya solicitado información.
- **LOSCCA** Ley Orgánica de Servicio Civil y Carrera Administrativa y de Unificación y Homologación de las Remuneraciones del Sector Público.
- **Lotus** Sistema cliente/servidor de colaboración y correo electrónico, desarrollado por Lotus Software, filial de IBM
- **MIB** Management Information Base - Base de Información de Gestión
- **NMS** Network Monitoring System - Sistema de Monitoreo de Red
- **NOC** Network Operation Center
- **ODF** Distribuidor de fibra óptica**.** Elemento usado como punto de interconexión entre cable de fibra

- **OID** Object identifier – identificador de objeto.
- **OSI** Open Systems Interconnection - Interconexión de Sistemas Abiertos.
- **P2P** Point to Point.- transferencia de archivos entre usuarios de una red.
- **PDU** Protocol Data Units - Unidades de Datos de Protocolo.
- **PDU** Protocol Data Units - Unidades de Datos de Protocolo.
- **PHP** Hypertext Preprocessor - lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas.
- **PPR** Acrónimo identificativo de la red de Petroproducción, nombre del dominio de la red.
- **Proxy.** Dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.
- **RADIUS** Remote Authentication Dial-In User Server - protocolo de autenticación y autorización para aplicaciones de acceso a la red.
- **RFC** Request For Comments - "Petición De Comentarios", serie de notas sobre Internet
- **RRDTool** Round Robin Database tool - herramienta que trabaja con una base de datos que maneja planificación según Round-Robin.
- **SLA** Service Level Agreement - Acuerdo de nivel de se
- **SMFA** Systems Management Functional Areas
- **SMTP** Simple Mail Transfer Protocol - Protocolo Simple de Transferencia
- **SNMP** Simple Network Management Protocol - Protocolo de Gestión de Red Simple
- **STP** Spanning Tree Protocol - protocolo de red de nivel 2 de la capa OSI.

- **SysLog** Estándar de facto para el envío de mensajes de registro en una red informática IP
- **TACACS** Terminal Access Controller Access Control System - Sistema de Control de Acceso mediante Control del Acceso desde Terminales
- **TCP/IP** Transmission-Control-Protocol/ Internet Protocol - Protocolo de Control de Transmisión/ Protocolo de Internet
- **Throughput.** Tasa de transferencia, rendimiento o throughput, se refiere a la tasa efectiva de bits.
- **TIC** Tecnologías de la Información y Comunicaciones
- **TMN** Telecommunication Management Network - Red de Gestión de las Telecomunicaciones
- **TOM** Telecommunication Operation Map - Mapa de Operaciones de Telecomunicaciones
- **Trap** Una trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración
- **Troubleshooting** Es la forma sistemática de buscar el origen de un problema para que éste pueda ser resuelto
- **UDP** User Datagram Protocol - Protocolo de Datagrama de Usuario
- **UIT-T** International Telecommunications Union – Telecommunications
- **USM** User-Based Security Model

REFERENCIAS BIBLIOGRÁFICAS

- ANDRÉS PARRA CARABALLO y SHARON MENDIETA BUENO, **Protocolo SNMP "Simple Network Management Protocol"**, Universidad Tecnológica de Bolívar, Facultad de Ingeniería Eléctrica y Electrónica Cartagena De Indias D.T., 2005 http://biblioteca.unitecnologica.edu.co/notas/2005-12-12/0032134.pdf

- RAMÓN JESÚS MILLÁN TEJEDOR, **"SNMPV3 (Simple Network Management Protocol Version 3)"**, Publicado en BIT Nº 139, COIT & AEIT, 2003. http://www.ramonmillan.com/tutorialeshtml/snmpv3.htm

- ALICIA CAMINERO CAMINERO, **"Sistema de Gestión para Redes Inalámbricas"**, Universidad de Alcalá, Escuela Técnica Superior de Ingeniería Informática, Trabajo Fin de Carrera, 2006. https://portal.uah.es/portal/page/portal/epd2_profesores/prof127418/enlaces/PFC-Alicia%20Caminero.pdf

- STALLINGS William, **"Comunicaciones y Redes de Computadores"**, Séptima Edición, Ed. Prentice Hall, 2004.

- JIMÉNEZ PUMISACHO GLADYS MAGALY, PAZMIÑO SANTIN CARLOS ALBERTO, **"Análisis, implementación y evaluación de un prototipo ruteador dual IPv4/IPv6 con soporte de QoS e IPsec sobre Linux, usando AHP para la selección del hardware e IEEE 830 para la selección del Software"**, Proyecto de Titulación de Ingeniería, Escuela Politécnica Nacional, Quito. Escuela de Ingeniería, Agosto 2009.

- IBM Corporation, **OS/400 Simple Network Management Protocol (SNMP) Support V4R1**, First Edition (August 1997) https://publib.boulder.ibm.com/infocenter/iseries/v6r1m0/topic/books_web/sc415412.pdf

- CARLOS VICENTE ALTAMIRANO, **"Un Modelo funcional para la Administración de Redes"**, Centro de operación de RedUNAM (NOC-UNAM), Julio de 2003

- NORMA TÉCNICA PERUANA 2007 NTP-ISO/IEC 17799, "**EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información"**. (EQV. ISO/IEC 17799:2005 Information technology. Code of practice for information security management), 2ª Edición, Lima, Perú, Enero 2007.

REFERENCIAS DE INTERNET

Consola de Monitoreo JJFNMS "Just for Fun Network Management System"
http://www.jffnms.org

Redes de Computadoras II, Administración de Redes
http://www.ciudadranelagh.com.ar/unlz/unocursada/Redes%20de%20Computadoras/ClaseAdmRedes_unlz.pdf

Descripción del rendimiento de Exchange
http://technet.microsoft.com/es-es/library/bb124583%28EXCHG.65%29.aspx

Documentación JFFNMS
http://www.scribd.com/doc/18110697/Jffnms-Manual

http://www.jffnms.org/docs/jffnms.html

Configuraciones JFFNMS

http://wiki.canaima.softwarelibre.gob.ve/wiki/index.php/Servidor_Jffnms#.Creaci.C3.B3n_de_Zonas_para_Discovery_autom.C3.A1tico

SNMP Object Navigator

http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Clasificación de Costos

http://www.infoeconomicas.com.ar/idx.php/0/021/article/Clasificacin-de-Costos.html

ANEXOS

ANEXO A

ANÁLISIS DE LA RED DE PETROPRODUCCIÓN

ANÁLISIS DE LA RED DE PETROPRODUCCIÓN

TOMA DE DATOS PARA EL ANALISIS DE TRÁFICO DE PETROPRODUCCIÓN

La toma de datos para el análisis de tráfico circulante en la red de Petroproducción se realizó de las conexiones simultáneas que se tiene, así como del tráfico interno entrante y saliente, y el enlace con la CNT. Además se analizan gráficas de ataques que tiene la empresa en los mismos periodos de tiempo que se realizó las capturas.

CONEXIONES SIMULTÁNEAS A LA RED

Las siguientes graficas de las conexiones simultáneas de la Red de Petroproducción son proporcionadas por el servidor ASTARO que posee la empresa como Firewall y presenta estas facilidades de captura para control del tráfico en la misma.

Las variables que intervienen en las siguientes gráficas de conexiones simultáneas son: en el eje "X" (Abscisas) que representa el tiempo, mientras que en el eje "Y" (Ordenadas) representa en número de conexiones en cada instante de tiempo.

La gráfica además nos da los valores promedio, actual y máximo del número de conexiones simultáneas en el periodo de tiempo capturado.

TOMA DE DATOS MENSUAL

Se realizó solo una toma mensual en durante el mes de diciembre y enero.

Lunes 14 de diciembre de 2009 – miércoles 13 de enero de 2010.

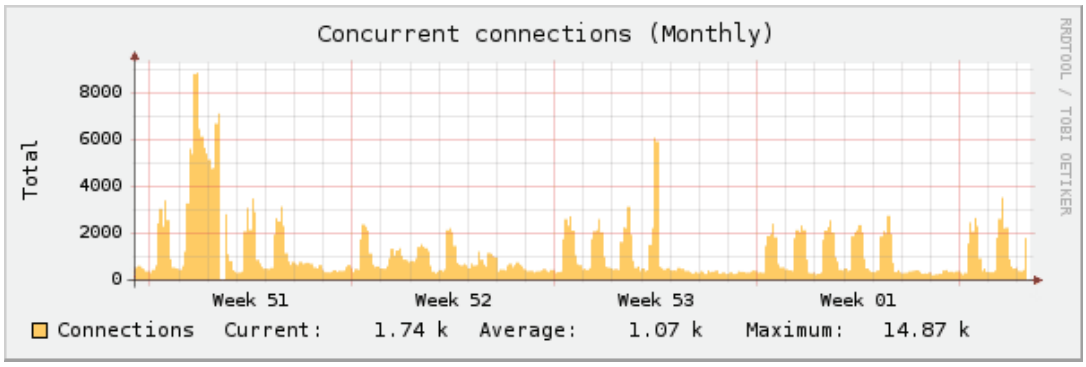


Figura A-1.- Conexiones simultáneas Mensualmente

TOMA DE DATOS SEMANAL

Se realizó solo una toma semanal desde el 6 al 13 de enero.

Miércoles 6 – Miércoles 13 de Enero de 2010

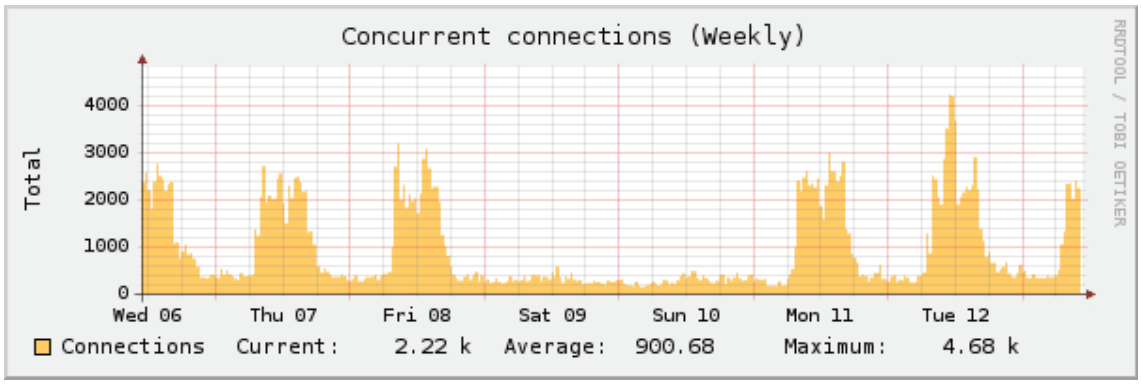


Figura A-2.-Conexiones simultaneas semanalmente.

TOMA DE DATOS DIARIO

Se realizó tres tomas diarias en las fechas 8, 11 y 12 de enero.

MEDICIÓN 1: viernes 8 de enero de 2010

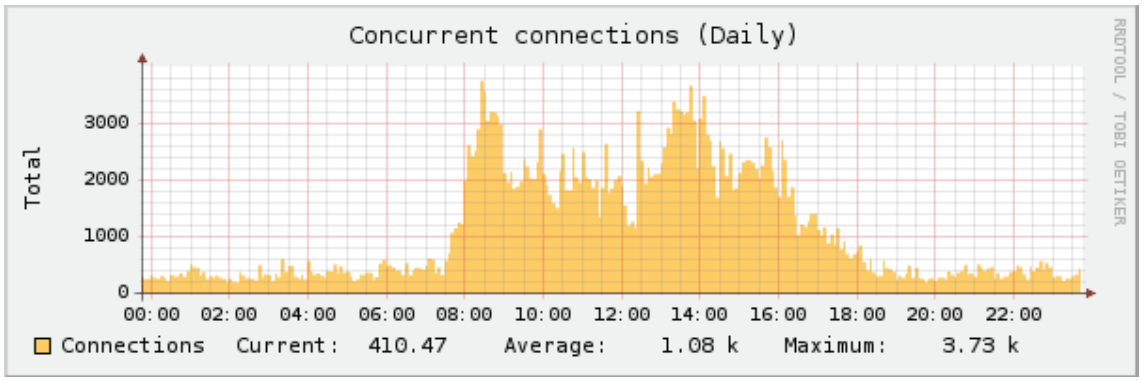


Figura A-3.- Conexiones simultaneas diariamente MEDICION 1.

MEDICIÓN 2: lunes 11 de enero de 2010.

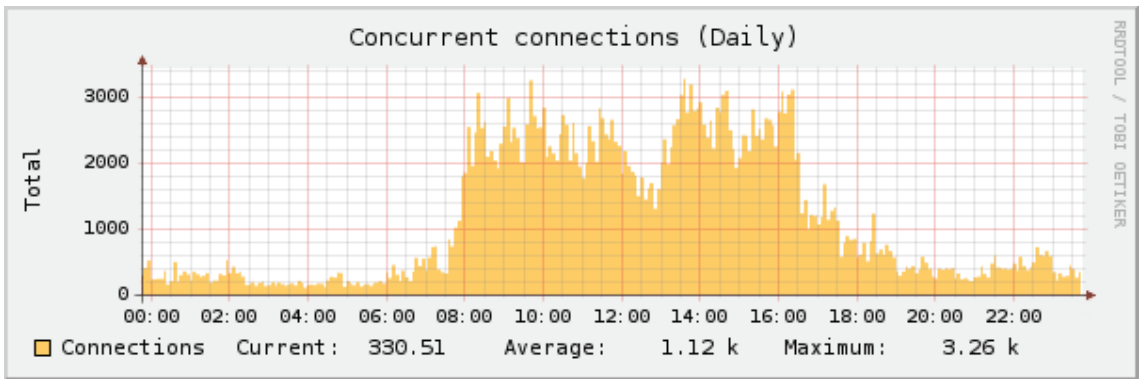


Figura A-4.- Conexiones simultaneas diariamente MEDICION 2.

MEDICIÓN 3: martes 12 de enero de 2010.

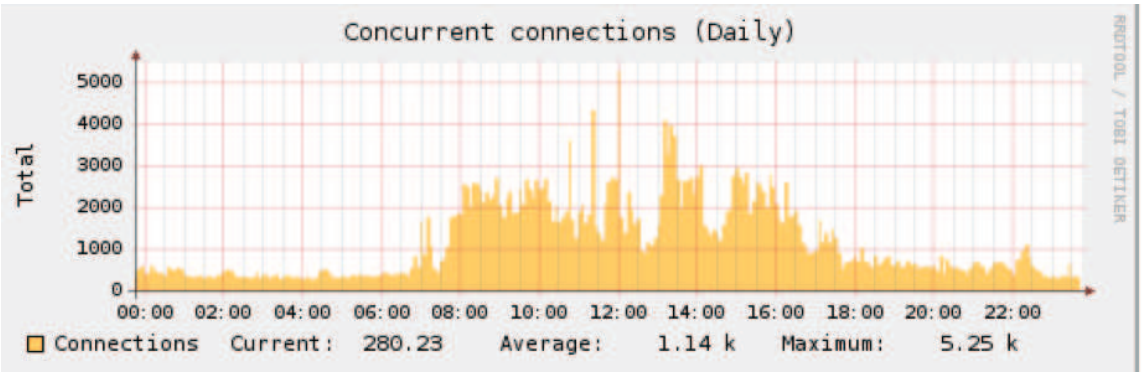


Figura A-5. Conexiones simultaneas diariamente MEDICION 3.

TOMA DE DATOS ANUAL

Además el servidor ASTARO está programado para capturar esta información anualmente, en este caso captura desde el mes de junio de 2009 teniendo el siguiente resultado hasta el 13 de enero de 2010.

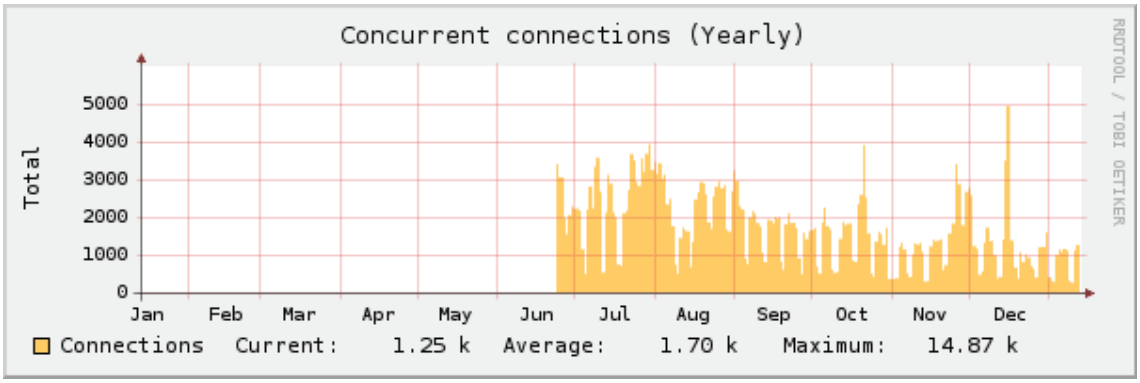


Figura A-6.- Conexiones simultaneas anualmente

Se pueden apreciar los siguientes resultados:

Conexiones Simultáneas (Anual)		
Actual	**Promedio**	**Máximo**
1284	1740.8	15196

Tabla A-1.- Conexiones simultáneas anualmente.

TRÁFICO INTERNO DE LA RED

Las siguientes graficas del tráfico interno circulante de la Red de Petroproducción son proporcionadas por el servidor ASTARO que posee la empresa como Firewall y presenta estas facilidades de captura para control del tráfico en la misma.

Las variables que intervienen en las siguientes gráficas de tráfico interno son: en el eje “X” (Abscisas) que representa el tiempo, mientras que en el eje “Y” (Ordenadas) representa en bits por segundo el tráfico entrante y saliente en cada instante de tiempo.

La gráfica además nos da los valores promedio, actual y máximo del de tráfico entrante y saliente en el periodo de tiempo capturado a través de la interfaz Ethernet 0 del servidor Astaro.

TOMA DE DATOS MENSUAL

Se realizó solo una toma mensual en durante el mes de diciembre y enero.
Lunes 14 de diciembre de 2009 – miércoles 13 de enero de 2010

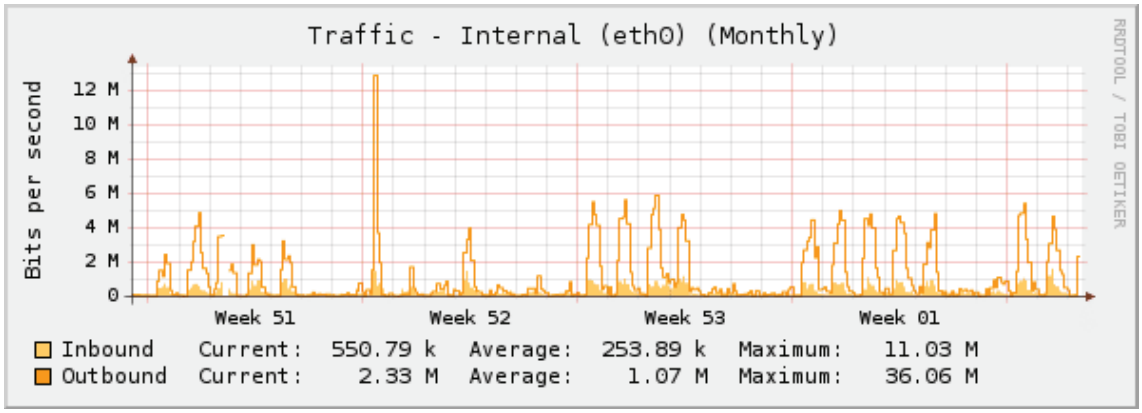


Figura A-7.- Tráfico interno mensual de Petroproducción

TOMA DE DATOS SEMANAL

Se realizó solo una toma semanal desde el 6 al 13 de enero.
Miércoles 6 – Miércoles 13 de Enero de 2010

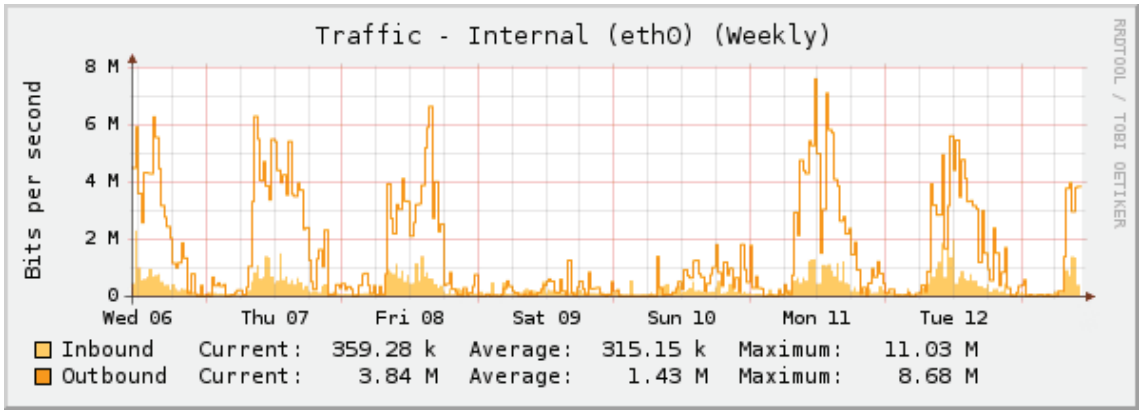


Figura A-8 .-Tráfico interno semanal de Petroproducción

TOMA DE DATOS DIARIO

Se realizó tres tomas diarias en las fechas 8, 11 y 12 de enero.

MEDICIÓN 1: viernes 8 de enero de 2010.

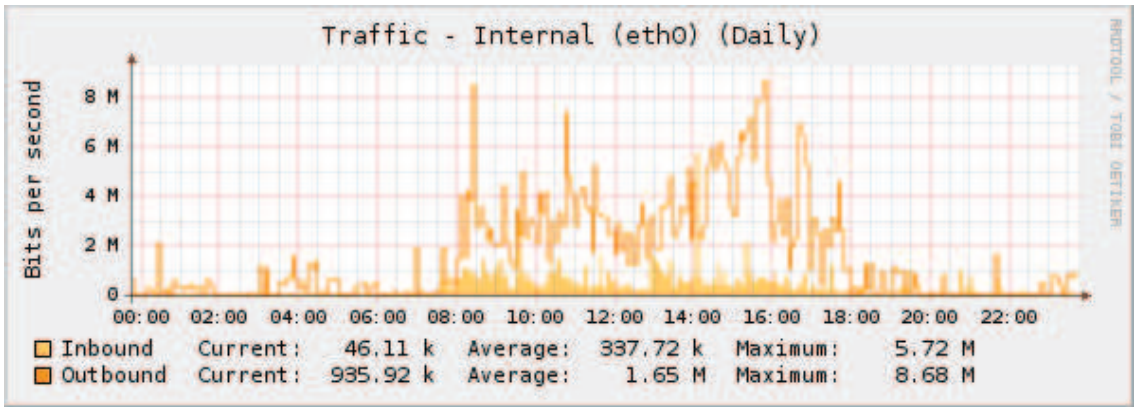


Figura A-9.- Tráfico interno diario de Petroproducción, MEDICIÓN 1

MEDICIÓN 2: lunes 11 de enero de 2010.

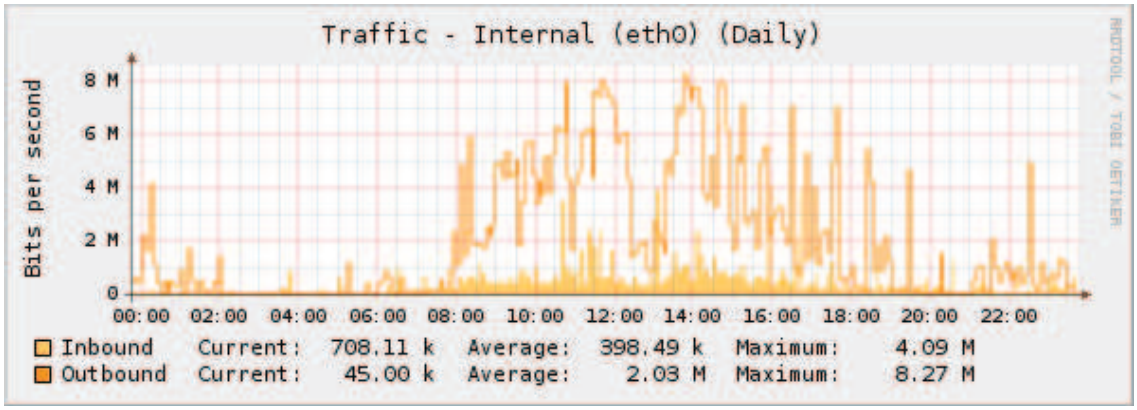


Figura A-10.- Tráfico interno diario de Petroproducción, MEDICIÓN 2.

MEDICIÓN 3: martes 12 de enero de 2010.

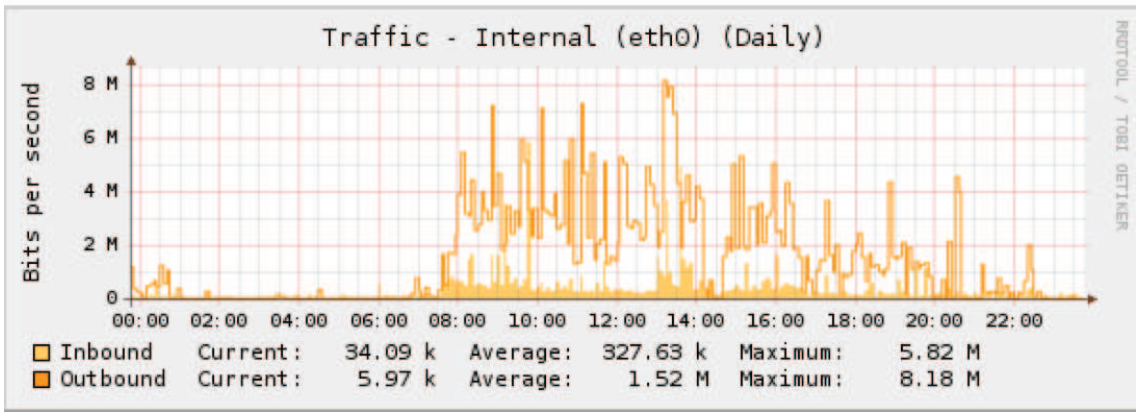


Figura A-11.- Tráfico interno diario de Petroproducción, MEDICIÓN 3.

TOMA DE DATOS ANUAL

El servidor ASTARO está programado para capturar información anualmente, en este caso desde el mes de junio de 2009 teniendo el siguiente resultado hasta el 13 de enero de 2010.

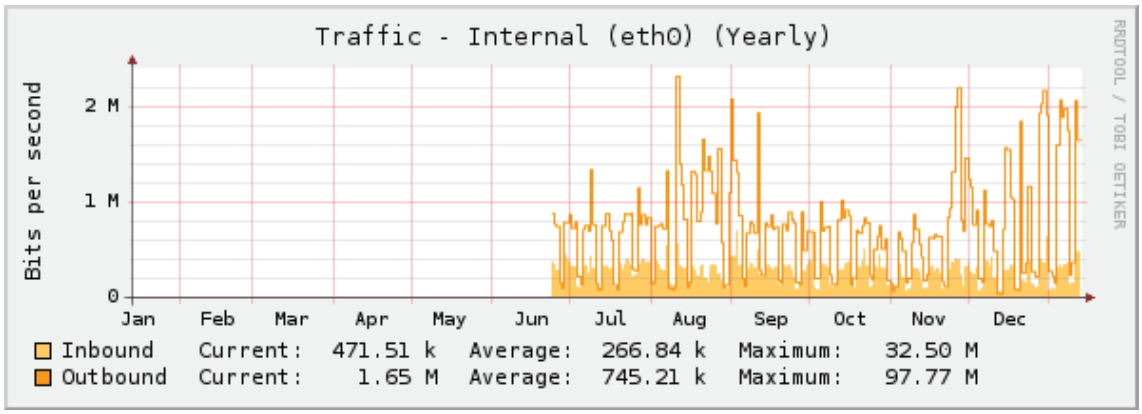


Figura A-12.-Tráfico interno anual de Petroproducción

TRÁFICO ENTRE CNT Y PETROPRODUCCIÓN

Las siguientes graficas del tráfico circulante entre CNT y Petroproducción son proporcionadas por el servidor y presenta estas facilidades de captura para control del tráfico.

Las variables que intervienen en las siguientes gráficas de tráfico interno son: en el eje "X" (Abscisas) que representa el tiempo, mientras que en el eje "Y" (Ordenadas) representa en bits por segundo el tráfico entrante y saliente en cada instante de tiempo.

La gráfica además nos da los valores promedio, actual y máximo del de tráfico entrante y saliente en el periodo de tiempo capturado a través de la interfaz Ethernet 4 del servidor.

TOMA DE DATOS MENSUAL

Se realizó solo una toma mensual en durante el mes de diciembre y enero.
Lunes 14 de diciembre de 2009 – miércoles 13 de enero de 2010

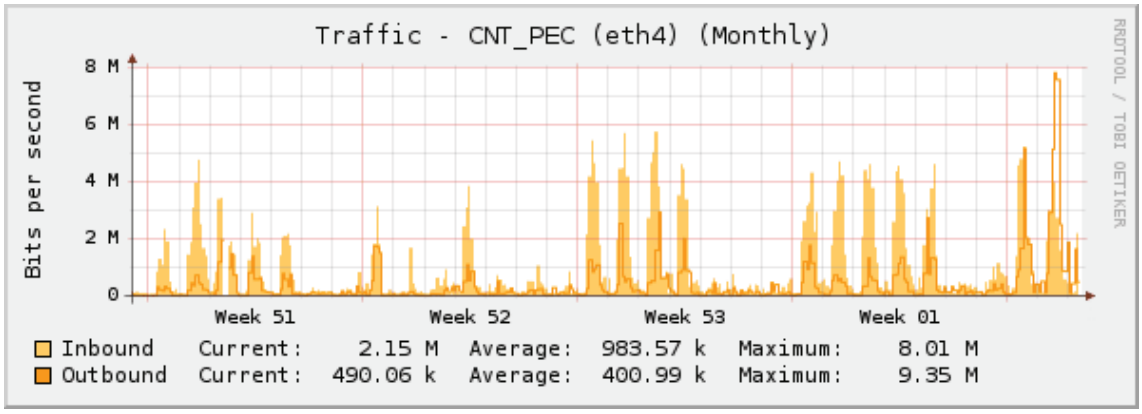


Figura A-13.- Tráfico mensual de Petroproducción con CNT

TOMA DE DATOS SEMANAL

Se realizó solo una toma semanal desde el 6 al 13 de enero.

Miércoles 6 – Miércoles 13 de Enero de 2010

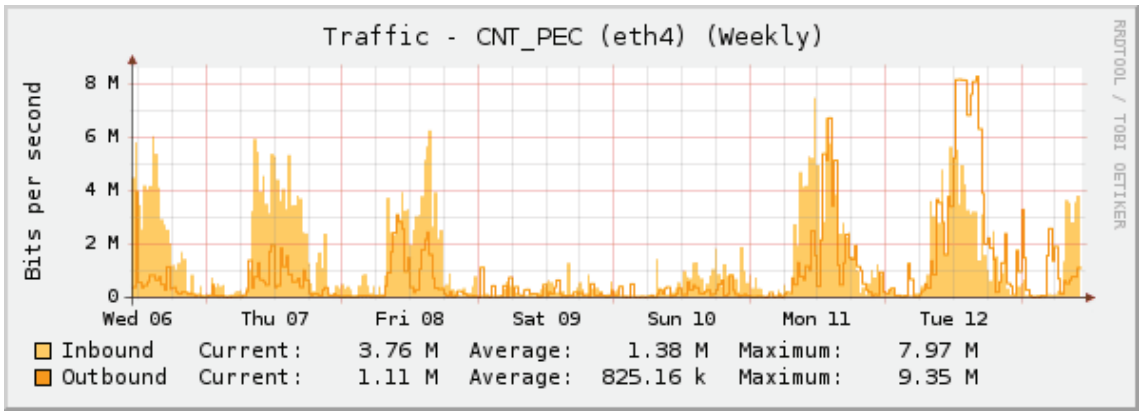


Figura A-14.- Tráfico semanal de Petroproducción con CNT

TOMA DE DATOS DIARIO

Se realizó tres tomas diarias en las fechas, 12 de enero, 18 y 19 de enero.

MEDICIÓN 1: viernes 8 de enero de 2010.

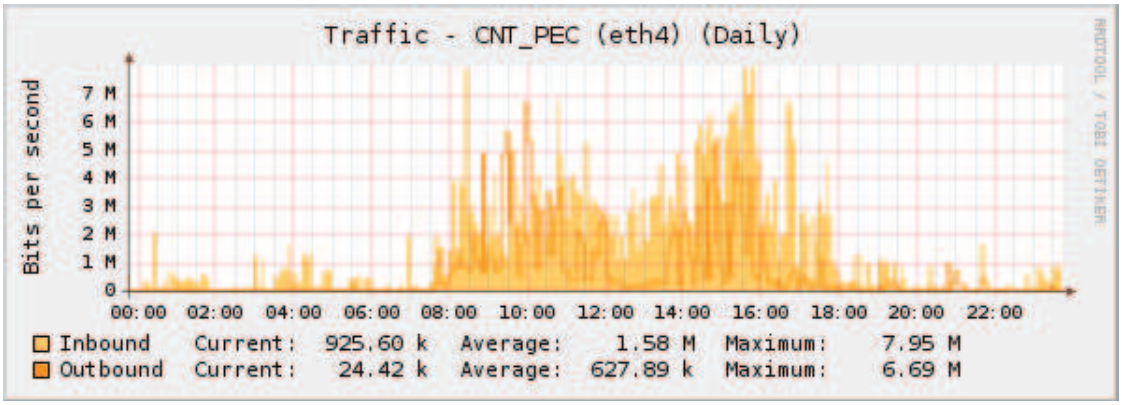


Figura A-15.- Tráfico diario de Petroproducción con CNT, MEDICIÓN 1

MEDICIÓN 2: lunes 11 de enero de 2010.

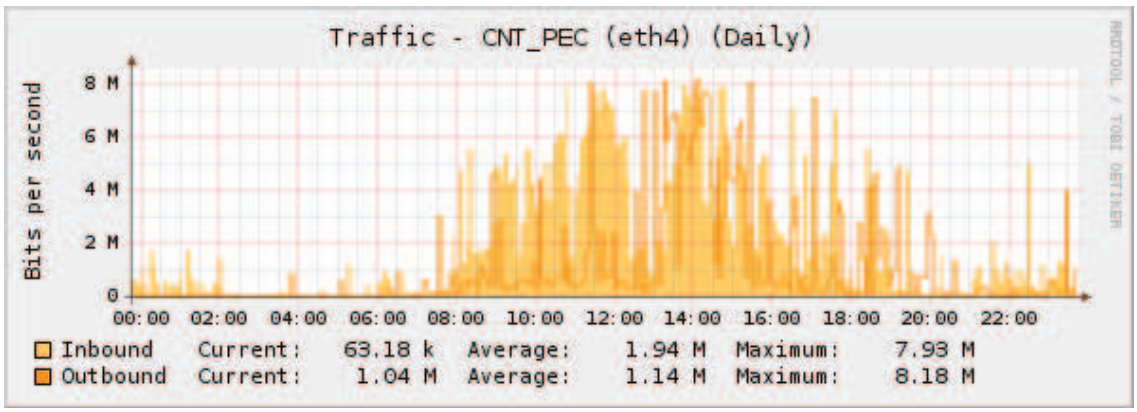


Figura A-16.- Tráfico diario de Petroproducción con CNT, MEDICIÓN 2.

MEDICIÓN 3: martes 12 de enero de 2010.

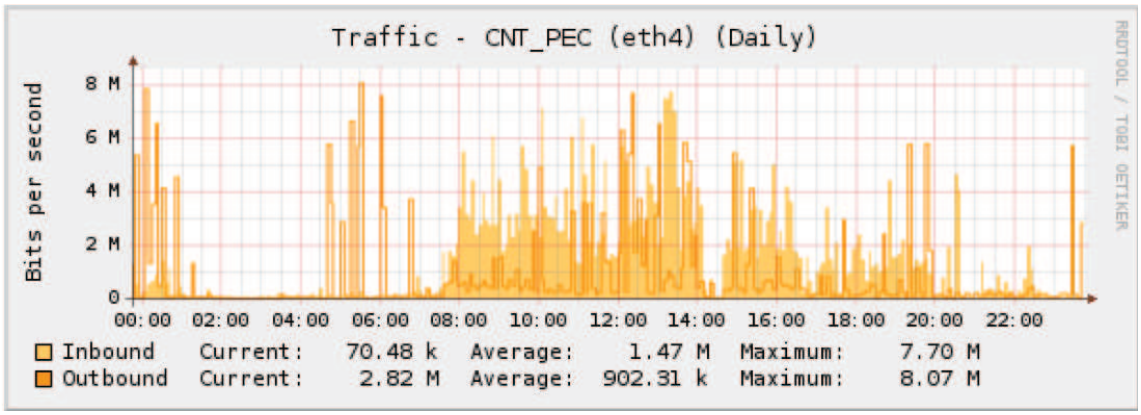


Figura A-17.- Tráfico diario de Petroproducción con CNT, MEDICIÓN 3

TOMA DE DATOS ANUAL

La información anual en este caso va desde el mes de Noviembre de 2009 teniendo el siguiente resultado hasta el 13 de enero de 2010.

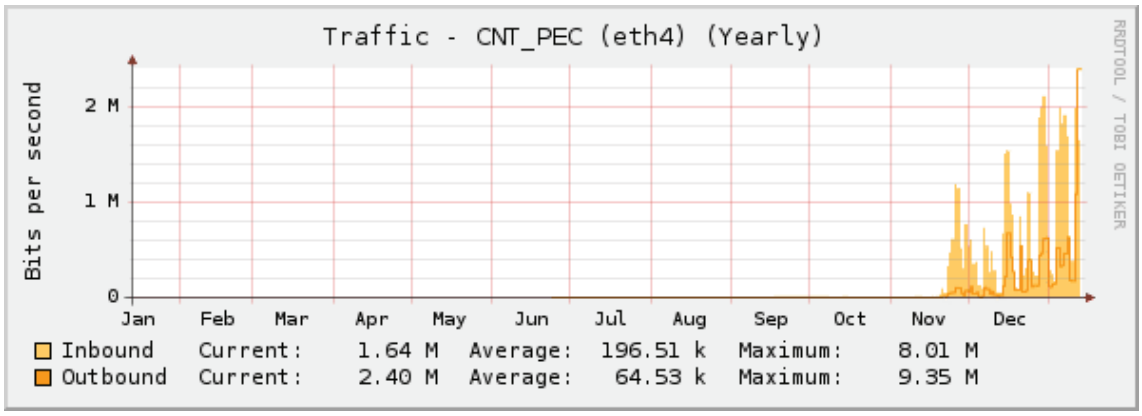


Figura A-18.-Tráfico anual de Petroproducción con CNT

Se tienen los siguientes resultados:

Tráfico CNT-PEC (Diario)					
ENTRANTE (Mbps)			SALIENTE (Mbps)		
Actual	Promedio	Máximo	Actual	Promedio	Máximo
1.64	0.192	8.01	2.40	0.063	9.35

Tabla A-2.- Trafico anual entre CNT y Petroproducción

ANALISIS DE UTILIZACIÓN DE EQUIPO DE NETWORKING PRINCIPAL DE PETROPRODUCCIÓN

Se analizó los principales routers y Switches que se tiene en Petroproducción para tener un conocimiento de línea base sobre su funcionamiento.

Se implemento la recolección de los datos a través de la utilización de las interfaces gráficas vía web de los dispositivos. Para el caso de ruteadores se muestran gráficas obtenidas mediante la herramienta SDM (Security Device Manager) de Cisco, mientras que para switches se usó la página de administración web de cada uno.

Así se muestran los datos obtenidos para cada dispositivo:

ROUTER VILLAFUERTE

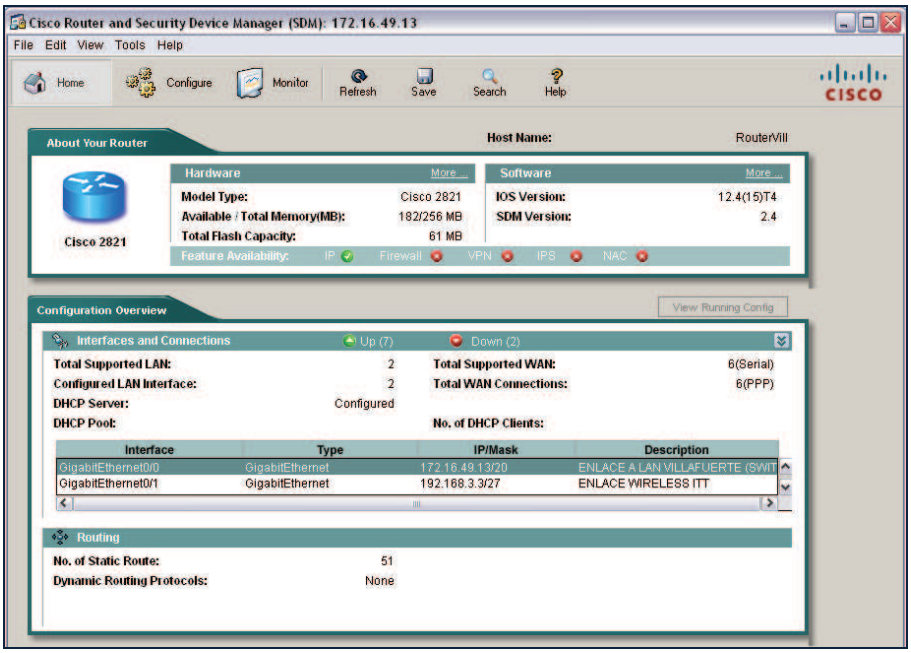


Figura A-19.- Router Villafuerte

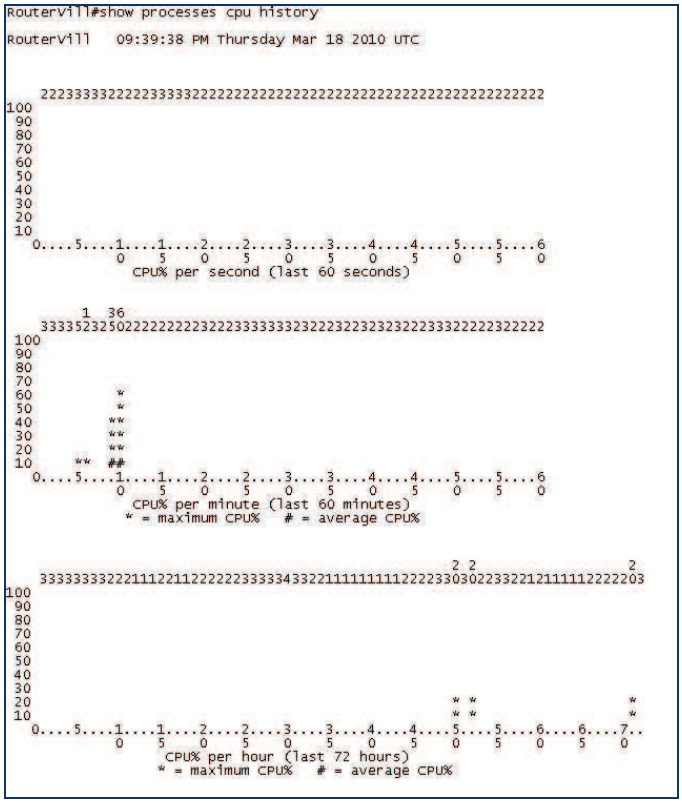


Figura A-20.- Uso del Procesador del Router Villafuerte

```
RouterVill#show ip traffic
IP statistics:
  Rcvd:  2163363076 total, 28903743 local destination
         0 format errors, 0 checksum errors, 1638865 bad hop count
         0 unknown protocol, 91 not a gateway
         0 security failures, 0 bad options, 180 with options
  Opts:  0 end, 171 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 171 record route
         0 stream ID, 0 strict source route, 9 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 26465041 received, 30 sent
  Mcast: 0 received, 0 sent
  Sent:  19984300 generated, 3159171057 forwarded
  Drop:  9682640 encapsulation failed, 205 unresolved, 0 no adjacency
         1243615 no route, 0 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address
         19049 physical broadcast

ICMP statistics:
  Rcvd: 10 format errors, 0 checksum errors, 0 redirects, 13 unreachable
  2386078 echo, 340 echo reply, 0 mask requests, 0 mask replies, 0 quench
  0 parameter, 0 timestamp, 0 timestamp replies, 0 info request, 0 other
  0 irdp solicitations, 0 irdp advertisements
  Sent: 4955799 redirects, 11075106 unreachable, 340 echo, 2386078 echo reply
  0 mask requests, 0 mask replies, 0 quench, 0 timestamp, 0 timestamp replies
        0 info reply, 1638581 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements

TCP statistics:
  Rcvd: 32146 total, 0 checksum errors, 2 no port
  Sent: 29998 total

UDP statistics:
  Rcvd: 26485129 total, 13 checksum errors, 26302205 no port
  Sent: 150 total, 0 forwarded broadcasts
```

Figura A-21.- Estadísticas de Tráfico del Router Villafuerte

```
RouterVill#show processes memory
Processor Pool Total:  197055616 Used:   13499572 Free:  183556044
      I/O Pool Total:   12582912 Used:    4101760 Free:    8481152

  PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
    0   0   34001928   13620856   14151996          0          0 *Init*
    0   0      77640   63373936      77640          0          0 *Sched*
    0   0   98559568  102988304      64560     194448     194448 *Dead*
    1   0     117376          0     124580          0          0 Chunk Manager
    2   0        252        252       4204          0          0 Load Meter
    4   0       3352        252      10364          0          0 Check heaps
    5   0   55243164   56709428     182284   30482368   30782408 Pool Manager
    6   0        252        252       7204          0          0 Timers
    7 514      15988      15736      13320          0          0 Virtual Exec
    8   0          0          0      13204          0          0 OIR Handler
    9   0          0          0      25204          0          0 Crash writer
   10   0        252        252       7204          0          0 Environmental mo
   11   0   44860120   44800800      41264          0          0 ARP Input
   12   0  250094600  251010460       7548          0          0 ARP Background
   13   0        252        252       7204          0          0 ATM Idle Timer
   14   0        252        252       7204          0          0 AAA high-capacit
   15   0          0          0       7204          0          0 AAA_SERVER_DEADT
```

Figura A-22.- Uso de Memoria del Router Villafuerte

INTERFAZ LAN

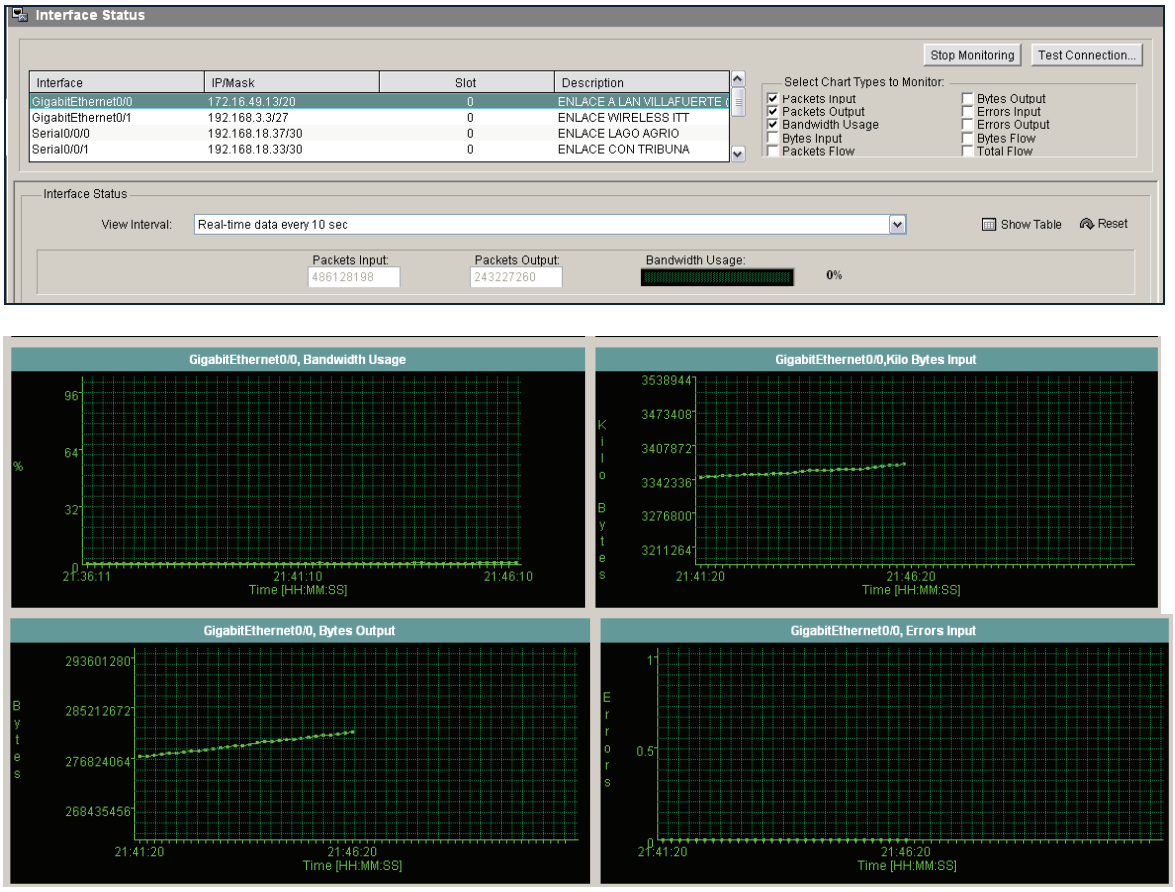


Figura A-23.- Gráficos Interfaz LAN de router Villafuerte

ENLACE CON TRIBUNA

Figura A-24.- Gráficas enlace Villafuerte - Tribuna

ENLACE VILLAFUERTE - LAGO AGRIO

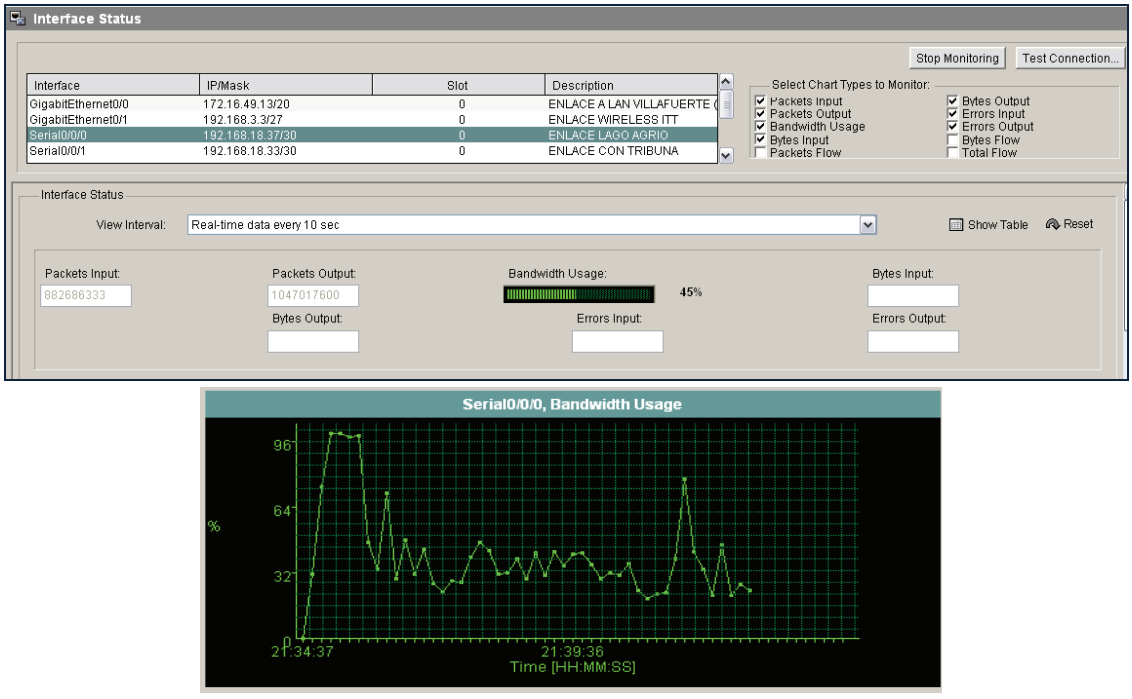


Figura A-25.- Gráficas enlace Villafuerte – Lago Agrio

ENLACE SAN RAFAEL

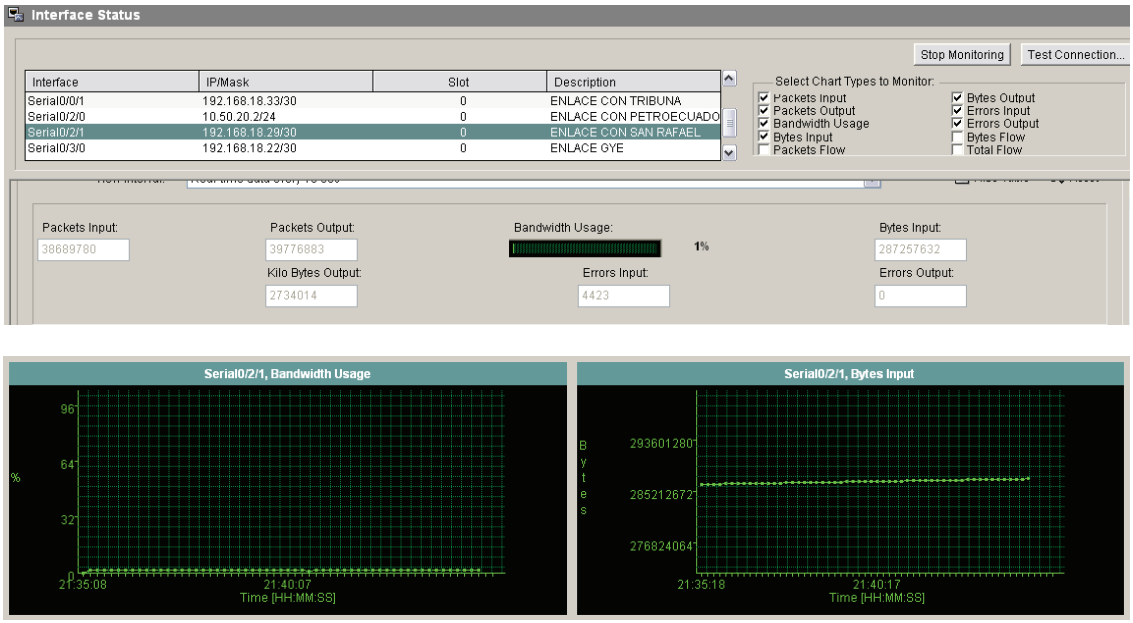


Figura A-26.- Gráficas enlace Villafuerte – San Rafael

ROUTER TRIBUNA

Las siguientes figuras nos dan una visión general de utilización del Router principal del edificio Tribuna. Las tomas se realizaron mediante la herramienta Security Device Manager de Cisco.

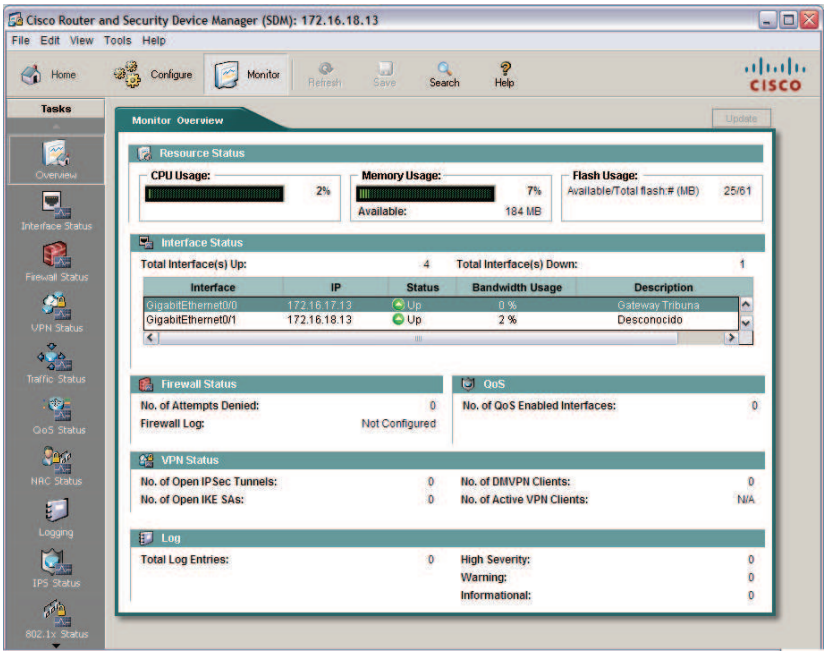


Figura A-27.- Vista general del Router Tribuna

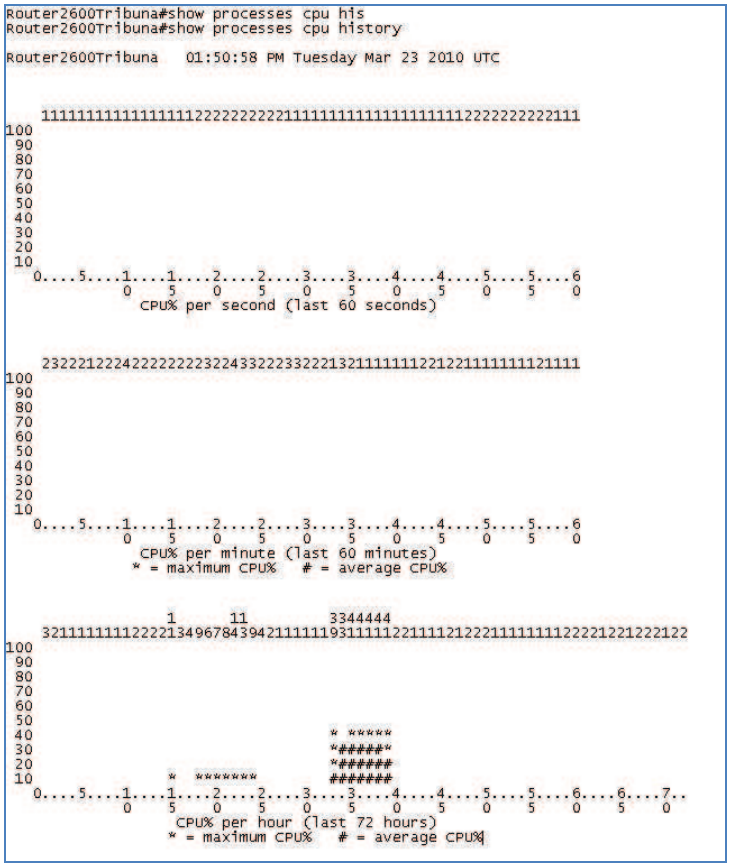


Figura A-28.- Vista general del Router Tribuna

```
Router2600Tribuna#show processes memory
Processor Pool Total:  197082512 Used:   12923668 Free:  184158844
      I/O Pool Total:   12582912 Used:    3621920 Free:    8960992

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0   29119664   13514784   13274672          0          0 *Init*
   0   0      12052   26077784      12052          0          0 *Sched*
   0   0   54215696   55066620     129048     177720     177720 *Dead*
   1   0     146972      40208     113968          0          0 Chunk Manager
   2   0        252        252       4204          0          0 Load Meter
   4   0       3352        252      10364          0          0 Check heaps
   5   0    9254620    9450696      64556    7185492    7234080 Pool Manager
   6   0        252        252       7204          0          0 Timers
   7 514     127064     126756      13376          0          0 Virtual Exec
   8   0          0          0      13204          0          0 OIR Handler
   9   0          0          0      25204          0          0 Crash writer
  10   0        252        252       7204          0          0 Environmental mo
  11   0    9756792    9736740      27256          0          0 ARP Input
  12   0  256369960  256651656       7204          0          0 ARP Background
  13   0        252        252       7204          0          0 ATM Idle Timer
  14   0        252        252       7204          0          0 AAA high-capacit
  15   0          0          0       7204          0          0 AAA_SERVER_DEADT
```

Figura A-29.- Uso de Memoria del Router Tribuna

ENLACE TRIBUNA – VILLAFUERTE

```
Router2600Tribuna#show ip traffic
IP statistics:
  Rcvd:  3370414466 total, 17943604 local destination
         0 format errors, 145 checksum errors, 42978 bad hop count
         0 unknown protocol, 18 not a gateway
         0 security failures, 0 bad options, 340 with options
  Opts:  0 end, 340 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 340 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 12187359 received, 12 sent
  Mcast: 0 received, 0 sent
  Sent:  2954222 generated, 3815487171 forwarded
  Drop:  5481511 encapsulation failed, 0 unresolved, 0 no adjacency
         568 no route, 0 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address
         10951370 physical broadcast

ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 5 unreachable
        19617 echo, 69 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
  Sent: 0 redirects, 9233 unreachable, 70 echo, 19617 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp, 0 timestamp replies
        0 info reply, 42634 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements

TCP statistics:
  Rcvd: 5725472 total, 0 checksum errors, 2849590 no port
  Sent: 2882691 total

UDP statistics:
  Rcvd: 12198375 total, 2 checksum errors, 9443380 no port
  Sent: 12 total, 0 forwarded broadcasts

ARP statistics:
  Rcvd: 4735851 requests, 8713 replies, 54 reverse, 0 other
  Sent: 3978828 requests, 584178 replies (176767 proxy), 0 reverse
  Drop due to input queue full: 0
```

Figura A-30.- Estadísticas de Tráfico Router Tribuna

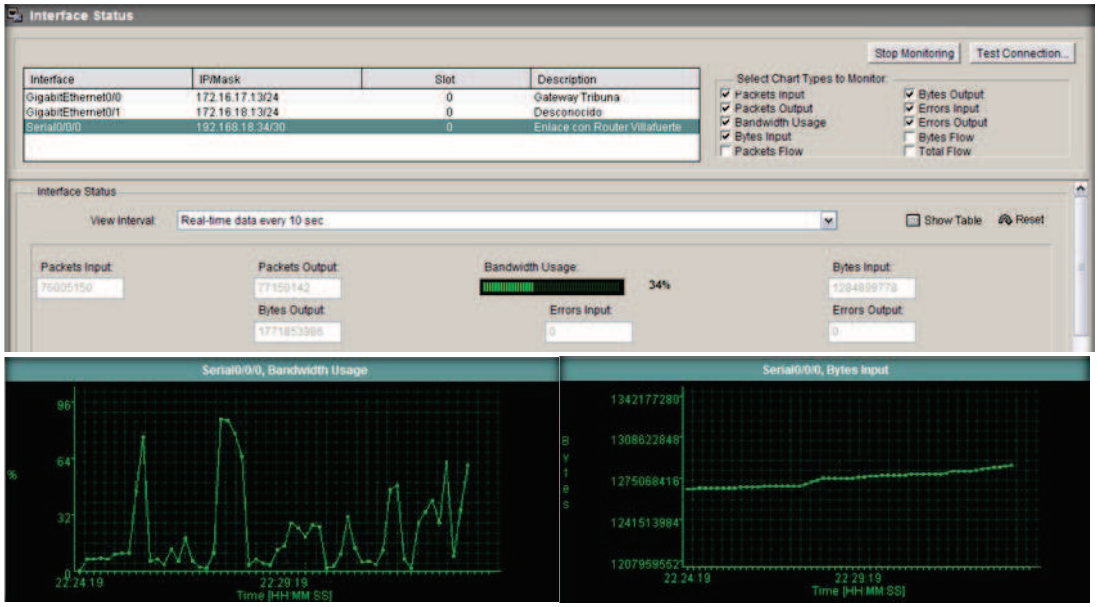


Figura A-31.- Gráficas enlace Tribuna - Villafuerte

SWITCH DE CORE: CISCO CATALYST 4500

Al no disponer de una interfaz gráfica vía web adecuada que muestre los datos y estadísticas del switch de núcleo, se procedió a su recopilación mediante una conexión Telnet al switch y la ejecución de comandos de monitoreo. Los resultados se almacenaron en archivos de texto.

Los comandos utilizados fueron:

- **Show processes cpu history**.- como una muestra del uso del cpu de hasta 72 horas atrás
- **Show ip traffic**.- resumen del tráfico procesado por el dispositivo
- **Show processes cpu sorted 5min**.- utilización de la memoria del dispositivo en los últimos cinco minutos

A continuación se muestra un extracto de toda la información recogida del switch Catalyst de núcleo Cisco 4500.

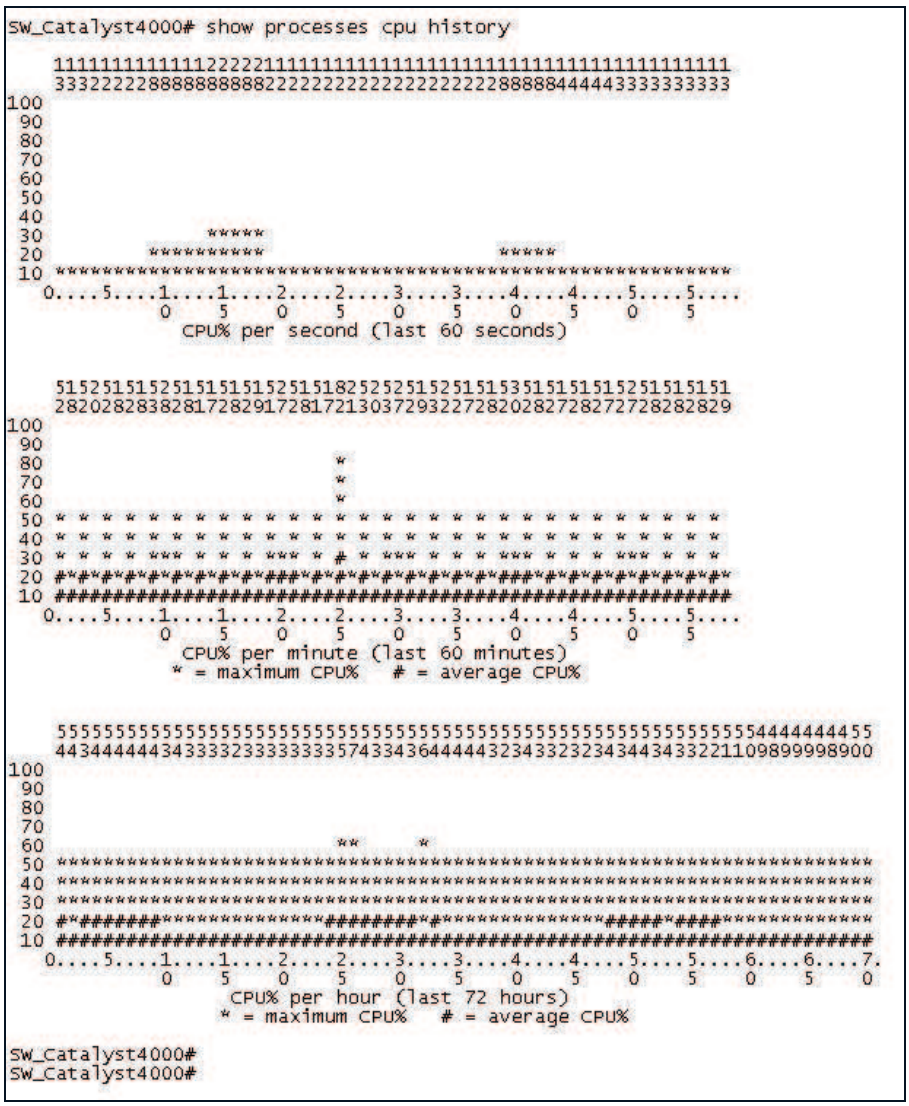


Figura A-32.- Uso del Procesador de Switch de Núcleo

```
SW_Catalyst4000#show ip traffic
IP statistics:
Rcvd:  22034069 total, 21747527 local destination
0 format errors, 0 checksum errors, 102991 bad hop count
0 unknown protocol, 0 not a gateway
0 security failures, 0 bad options, 79188 with options
Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
0 timestamp, 0 extended security, 0 record route
0 stream ID, 0 strict source route, 79188 alert, 0 cipso, 0 ump
0 other
Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
0 fragmented, 0 couldn't fragment
Bcast: 21523442 received, 3 sent
Mcast: 0 received, 0 sent
Sent:  153907 generated, 0 forwarded
Drop:  83455 encapsulation failed, 0 unresolved, 0 no adjacency
385 no route, 0 unicast RPF, 0 forced drop
0 options denied, 0 source IP address zero

ICMP statistics:
Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
55523 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
0 parameter, 0 timestamp, 0 info request, 0 other
0 irdp solicitations, 0 irdp advertisements
Sent: 0 redirects, 88652 unreachable, 0 echo, 55523 echo reply
0 mask requests, 0 mask replies, 0 quench, 0 timestamp
0 info reply, 0 time exceeded, 0 parameter problem
0 irdp solicitations, 0 irdp advertisements

TCP statistics:
Rcvd: 7695 total, 0 checksum errors, 2 no port
Sent: 9760 total

Probe statistics:
Rcvd: 0 address requests, 0 address replies
0 proxy name requests, 0 where-is requests, 0 other
Sent: 0 address requests, 0 address replies (0 proxy)
0 proxy name replies, 0 where-is replies

UDP statistics:
Rcvd: 21684312 total, 13 checksum errors, 21449060 no port
Sent: 3 total, 0 forwarded broadcasts

SW_Catalyst4000#
SW_Catalyst4000#
```

Figura A-33.- Estadísticas de Tráfico Switch de Núcleo

```
SW_Catalyst4000# show processes memory
Processor Pool Total:  490507888 Used:  136013344 Free:  354494544

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0  117256900    2563012  100283692          0          0 *Init*
   0   0      14436    2888732      14436          0          0 *Sched*
   0   0   40711200   20290560   26790104     489968      12756 *Dead*
   1   0     309604 1305310436      42392          0          0 Chunk Manager
   2   0        180        180      29924          0          0 Load Meter
   3   0      28212      28724      34924          0          0 crypto sw pk pro
   4   0          0          0      32924          0          0 Deferred Events
   5   0          0          0      32924          0          0 Retransmission o
   6   0      11656      10480      34100          0          0 IPC ISSU Receive
   7   0          0          0      32924          0          0 Check heaps
   8   0      15564   24888276      32924      12756   11599296 Pool Manager
   9   0        180        180      32924          0          0 Timers
  10   0        180        180      32924          0          0 Serial Backgroun
  11   0          0          0      50924          0          0 Crash writer
  12   0      65344        816      38316      25512          0 ifIndex Receive
  13   0     169956    6971204     186016          0          0 ARP Input
  14   0          0          0      32924          0          0 AAA_SERVER_DEADT
  15   0        180        180      32924          0          0 AAA high-capacit
```

Figura A-34.- Consumo de Memoria del Switch de Núcleo

SWITCH DE DISTRIBUCIÓN

Se empleó el mismo proceso de ejecución de comandos mediante una sesión telnet, para este caso el dispositivo cuenta con una interfaz gráfica, sin embargo esta muestra estadísticas no con el mayor detalle que vía comandos.

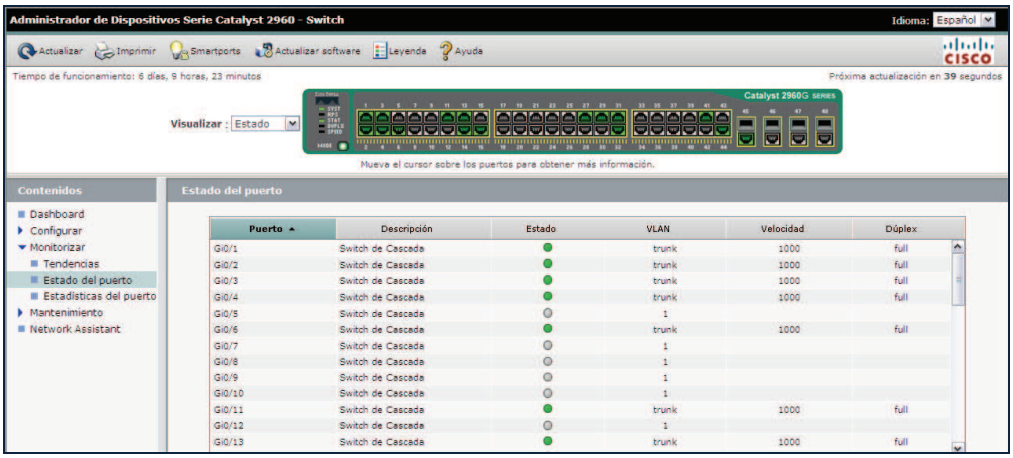


Figura A-35.- Interfaz web de Switch de Distribución

La gráfica nos muestra que los puertos activos del dispositivo se encuentran con una configuración de puertos troncales, destinados sólo a la conexión con otros switches.

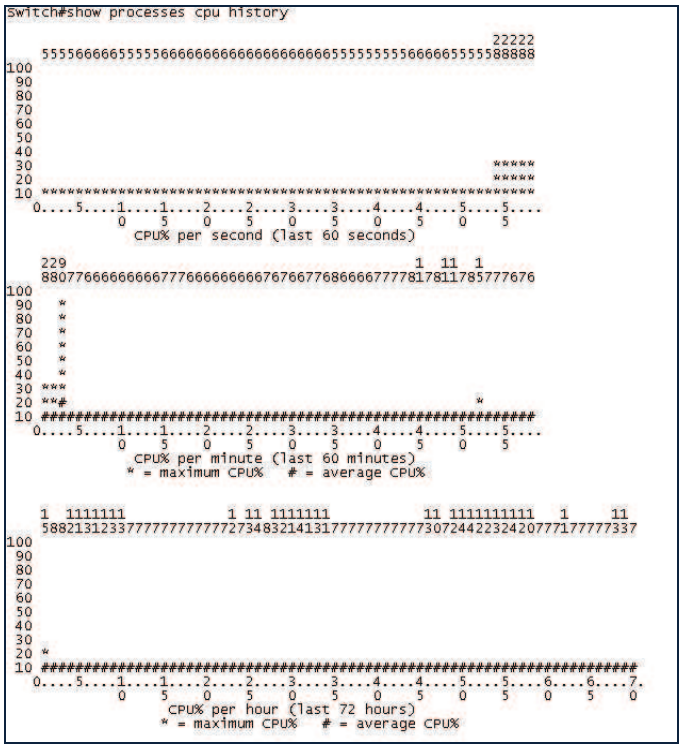


Figura A-36.- Uso del Procesador de Switch de Distribución

```
Switch#show ip traffic
IP statistics:
  Rcvd:  1454318 total, 1441906 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 12412 not a gateway
         0 security failures, 0 bad options, 148 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 148 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 1440831 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  1606 generated, 0 forwarded
  Drop:  2 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
         0 options denied, 0 source IP address zero

ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
        1 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
  Sent: 0 redirects, 0 unreachable, 0 echo, 1 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 0 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements

TCP statistics:
  Rcvd: 1077 total, 0 checksum errors, 0 no port
  Sent: 1607 total

UDP statistics:
  Rcvd: 1440835 total, 0 checksum errors, 1433785 no port
  Sent: 0 total, 0 forwarded broadcasts

ARP statistics:
  Rcvd: 2803487 requests, 4045 replies, 1 reverse, 0 other
  Sent: 4 requests, 7 replies (0 proxy), 0 reverse
  Drop due to input queue full: 0
```

Figura A-37.-Tráfico de Switch de Distribución

```
Switch#  show processes memory
Processor Pool Total:   41031056 Used:    7481852 Free:   33549204
      I/O Pool Total:    4186112 Used:    1650360 Free:    2535752
Driver te Pool Total:    1048576 Used:         40 Free:    1048536

  PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
    0   0   14002392    6026576    6348448          0          0 *Init*
    0   0      13136    2017732      13136          0          0 *Sched*
    0   0   38119324   37722800     333240    3515584    1991772 *Dead*
    1   0       5172       1544      12080          0          0 Chunk Manager
    2   0        180        180       3908          0          0 Load Meter
    3   0     741688     498848       7316          0          0 SpanTree Helper
    4   0          0          0       6908          0          0 Check heaps
    5   0          0    3025472       6908          0    1126592 Pool Manager
    6   0        180        180       6908          0          0 Timers
    7   0          0          0       6908          0          0 HRPC asic-stats
    8   0          0          0      24908          0          0 Crash writer
    9   0        396        580       7072          0          0 ARP Input
   10   0          0          0       6908          0          0 AAA_SERVER_DEADT
   11   0        204        204       6908          0          0 AAA high-capacit
   12   0          0          0      12908          0          0 Policy Manager
   13   0     146252     260844      91432          0      58440 Entity MIB API
   14   0          0          0       6908          0          0 IFS Agent Manage
   15   0          0          0       6908          0          0 HC Counter Timer
```

Figura A-38.- Uso de Memoria de Switch de Distribución

REPORTES DE MEDICIONES ASTARO GATEWAY V7

Device	petro
Date	Wed Jan 13 12:11:38 2010
Query	Top Services by Server
Timeframe	Start: 2010-01-8 Stop: 2010-01-8
Filter	Destination IP = "172.16.49.35"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	DOMAIN	TCP	174.0 kB	78.99	2.1 MB	95.18	2.3 MB	2.3 MB	253	34.66	5 643	81.17	53
2	DOMAIN	UDP	31.4 kB	14.27	75.9 kB	3.32	107.3 kB	107.3 kB	418	57.26	999	14.37	53
3	LDAPS	TCP	5.4 kB	2.45	24.6 kB	1.08	30.0 kB	30.0 kB	4	0.55	102	1.47	636
4	NETBIOS-NS	UDP	7.7 kB	3.46	7.7 kB	0.34	15.4 kB	15.4 kB	50	6.85	180	2.59	137
5	KERBEROS	TCP	1.4 kB	0.62	1.3 kB	0.06	2.7 kB	2.7 kB	3	0.41	24	0.35	88
6	NETBIOS-DGM	UDP	0.3 kB	0.12	0.3 kB	0.01	0.6 kB	0.6 kB	1	0.14	2	0.03	138
7	LDAP	UDP	0.1 kB	0.07	0.2 kB	0.01	0.3 kB	0.3 kB	1	0.14	2	0.03	389
Totals	-	-	220.3 kB	-	2.2 MB	-	2.4 MB	2.4 MB	730	-	6 952	-	-

Device	petro
Date	Wed Jan 13 12:13:20 2010
Query	Top Services by Server
Timeframe	Start: 2010-01-11 Stop: 2010-01-11
Filter	Destination IP = "172.16.49.35"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	DOMAIN	TCP	170.2 kB	58.84	2.1 MB	91.39	2.2 MB	2.2 MB	240	29.13	5 467	62.22	53
2	NETBIOS-NS	UDP	84.1 kB	29.08	88.9 kB	3.81	173.1 kB	173.1 kB	62	7.52	2 174	24.74	137
3	DOMAIN	UDP	34.9 kB	12.07	111.8 kB	4.79	146.7 kB	146.7 kB	522	63.35	1 146	13.04	53
Totals	-	-	289.3 kB	-	2.3 MB	-	2.6 MB	2.6 MB	824	-	8 787	-	-

Device	petro
Date	Wed Jan 13 12:14:32 2010
Query	Top Services by Server
Timeframe	Start: 2010-01-12 Stop: 2010-01-12
Filter	Destination IP = "172.16.49.35"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	DOMAIN	TCP	182.8 kB	91.21	2.4 MB	98.43	2.5 MB	2.5 MB	257	51.40	5 993	90.49	53
2	DOMAIN	UDP	16.3 kB	8.14	37.0 kB	1.51	53.3 kB	53.3 kB	235	47.00	600	9.06	53
3	NETBIOS-NS	UDP	1.3 kB	0.65	1.3 kB	0.05	2.6 kB	2.6 kB	8	1.60	30	0.45	137
Totals	-	-	200.4 kB	-	2.4 MB	-	2.6 MB	2.6 MB	500	-	6 623	-	-

Figura A-39 .- Tráfico DNS Diario

Device	petro
Date	Mon Jan 18 10:13:23 2010
Query	Top Services by Server
Timeframe	Start: 2010-01-06 Stop: 2010-01-12
Filter	Destination IP = "172.16.49.35"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	DOMAIN	TCP	1.1 MB	72.20	13.8 MB	94.79	14.9 MB	14.9 MB	1 678	36.52	37 096	75.01	53
2	DOMAIN	UDP	182.6 kB	11.43	490.6 kB	3.29	673.2 kB	673.2 kB	2 651	57.69	6 119	12.37	53
3	NETBIOS-NS	UDP	231.6 kB	14.50	242.0 kB	1.62	473.6 kB	473.6 kB	229	4.98	5 923	11.98	137
4	LDAPS	TCP	5.4 kB	0.34	24.6 kB	0.17	30.0 kB	30.0 kB	4	0.09	102	0.21	636
5	KERBEROS	UDP	8.1 kB	0.51	9.0 kB	0.06	17.1 kB	17.1 kB	7	0.15	14	0.03	88
6	MICROSOFT-DS	TCP	7.2 kB	0.45	2.9 kB	0.02	10.1 kB	10.1 kB	2	0.04	48	0.10	445
7	KERBEROS	TCP	3.2 kB	0.20	2.3 kB	0.02	5.6 kB	5.6 kB	7	0.15	56	0.11	88
8	BLACKJACK	TCP	2.9 kB	0.18	2.3 kB	0.02	5.2 kB	5.2 kB	3	0.07	45	0.09	1025
9	EPMAP	TCP	1.2 kB	0.08	1.0 kB	0.01	2.3 kB	2.3 kB	2	0.04	28	0.06	135
10	LDAP	UDP	1.2 kB	0.07	1.1 kB	0.01	2.3 kB	2.3 kB	6	0.13	12	0.02	389
11	NETBIOS-DGM	UDP	0.3 kB	0.02	0.3 kB	0.00	0.6 kB	0.6 kB	1	0.02	2	0.00	138
12	0	ICMP	0.2 kB	0.01	0.2 kB	0.00	0.5 kB	0.5 kB	4	0.09	8	0.02	0
13	NTP	UDP	<0.1 kB	0.01	<0.1 kB	0.00	0.2 kB	0.2 kB	1	0.02	2	0.00	123
Totals	-	-	1.6 MB	-	14.6 MB	-	16.1 MB	16.1 MB	4 595	-	49 455	-	-

Figura A-40.- Tráfico DNS Semanal

Device	petro
Date	Wed Jan 13 12:04:29 2010
Query	Top Services by Server
Timeframe	Last 30 days
Filter	Destination IP = "172.16.49.35"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	DOMAIN	TCP	5.3 MB	52.70	61.5 MB	74.73	66.8 MB	66.8 MB	7 074	27.41	158 900	52.95	53
2	MS-WBT-SERVER	TCP	2.0 MB	19.96	15.8 MB	19.19	17.8 MB	17.8 MB	8	0.03	81 544	27.17	3389
3	DOMAIN	UDP	1.2 MB	12.22	2.3 MB	2.83	3.6 MB	3.6 MB	17 576	68.10	39 845	13.28	53
4	MSFT-GC	TCP	383.4 kB	3.74	1.2 MB	1.51	1.6 MB	1.6 MB	167	0.65	3 421	1.14	3268
5	MICROSOFT-DS	TCP	478.2 kB	4.67	355.4 kB	0.42	833.6 kB	833.6 kB	56	0.22	4 954	1.65	445
6	LDAP	TCP	195.4 kB	1.91	482.9 kB	0.57	678.3 kB	678.3 kB	62	0.24	1 360	0.45	389
7	NETBIOS-NS	UDP	307.3 kB	3.00	320.4 kB	0.38	627.7 kB	627.7 kB	486	1.88	7 772	2.59	137
8	LDAPS	TCP	36.1 kB	0.35	162.7 kB	0.19	198.8 kB	198.8 kB	29	0.11	693	0.23	636
9	KERBEROS	UDP	47.4 kB	0.46	51.5 kB	0.06	98.9 kB	98.9 kB	38	0.15	80	0.03	88
10	BLACKJACK	TCP	26.2 kB	0.26	21.0 kB	0.02	47.2 kB	47.2 kB	26	0.10	423	0.14	1025
11	LDAP	UDP	20.8 kB	0.20	19.5 kB	0.02	40.2 kB	40.2 kB	109	0.42	217	0.07	389
12	CAP	TCP	18.6 kB	0.18	12.4 kB	0.01	30.9 kB	30.9 kB	11	0.04	185	0.06	1026
13	EPMAP	TCP	16.5 kB	0.16	13.1 kB	0.02	29.6 kB	29.6 kB	28	0.11	365	0.12	135
14	0	ICMP	12.1 kB	0.12	12.1 kB	0.01	24.3 kB	24.3 kB	110	0.43	220	0.07	0
15	HTTP	TCP	1.7 kB	0.02	5.3 kB	0.01	7.0 kB	7.0 kB	2	0.01	26	0.01	80
16	KERBEROS	TCP	3.2 kB	0.03	2.3 kB	0.00	5.6 kB	5.6 kB	7	0.03	56	0.02	88
17	NETBIOS-DGM	UDP	1.1 kB	0.01	1.2 kB	0.00	2.3 kB	2.3 kB	3	0.01	8	0.00	138
18	NTP	UDP	0.9 kB	0.01	0.9 kB	0.00	1.9 kB	1.9 kB	10	0.04	20	0.01	123
19	NETBIOS-SSN	TCP	0.5 kB	0.01	0.3 kB	0.00	0.8 kB	0.8 kB	6	0.02	18	0.01	139
Totals	-	-	10.0 MB	-	82.3 MB	-	92.3 MB	92.3 MB	25 808	-	300 107	-	-

Figura A-41.- Tráfico DNS Mensual

Device	petro
Date	Mon Jan 18 10:55:33 2010
Query	Top Services
Timeframe	Start: 2009-12-06 Stop: 2010-01-12
Filter	-
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	%	Conns	%	Packets	%	Port
1	HTTP	TCP	24.2 GB	10.71	288.4 GB	48.02	312.6 GB	37.82	9 348 800	19.12	462 208 218	36.67	80
2	HTTP-ALT	TCP	25.5 GB	11.27	277.7 GB	46.23	303.1 GB	36.68	4 686 098	9.59	422 301 668	33.50	8080
3	SMTP	TCP	164.9 GB	73.02	5.8 GB	0.96	170.6 GB	20.65	2 387 689	4.88	238 602 071	18.93	25
4	HTTPS	TCP	3.1 GB	1.36	17.2 GB	2.86	20.3 GB	2.45	916 735	1.88	37 852 534	3.00	443
5	DOMAIN	UDP	1.7 GB	0.75	4.5 GB	0.75	6.2 GB	0.75	24 887 191	50.91	48 675 555	3.86	53
6	TINCAN	TCP	49.5 MB	0.02	2.4 GB	0.41	2.5 GB	0.30	368	0.00	3 058 672	0.24	1935
7	MS-WBT-SERVER	TCP	152.9 MB	0.07	1.9 GB	0.31	2.0 GB	0.24	742	0.00	7 373 002	0.58	3389
8	0	GRE	1.4 GB	0.61	333.4 MB	0.05	1.7 GB	0.21	396	0.00	8 918 026	0.71	0
9	MS-SQL-S	TCP	832.3 MB	0.36	779.5 MB	0.13	1.6 GB	0.19	238 147	0.49	9 101 787	0.72	1433
10	WEBADMIN	TCP	33.3 MB	0.01	257.3 MB	0.04	290.6 MB	0.03	11 345	0.02	483 286	0.04	4444
11	MICROSOFT-DS	TCP	230.0 MB	0.10	39.6 MB	0.01	269.6 MB	0.03	2 223 052	4.55	4 731 264	0.38	445
12	0	ICMP	180.4 MB	0.08	49.1 MB	0.01	229.5 MB	0.03	3 304 997	6.76	5 298 002	0.42	0
13	8500	TCP	18.2 MB	0.01	164.5 MB	0.03	182.8 MB	0.02	16 270	0.03	353 870	0.03	8500
14	6616	TCP	3.4 MB	0.00	157.0 MB	0.03	160.4 MB	0.02	13	0.00	216 134	0.02	6616
15	13000	TCP	15.5 MB	0.01	125.1 MB	0.02	140.6 MB	0.02	22 131	0.05	310 761	0.02	13000
16	42307	TCP	130.4 MB	0.06	2.3 MB	0.00	132.7 MB	0.02	1	0.00	136 716	0.01	42307
17	53407	TCP	129.6 MB	0.06	2.2 MB	0.00	131.9 MB	0.02	1	0.00	135 901	0.01	53407
18	43895	TCP	126.7 MB	0.05	2.2 MB	0.00	128.9 MB	0.02	2	0.00	132 779	0.01	43895
19	46034	TCP	123.2 MB	0.05	2.1 MB	0.00	125.3 MB	0.01	2	0.00	129 105	0.01	46034
20	48155	TCP	122.0 MB	0.05	2.1 MB	0.00	124.1 MB	0.01	4	0.00	127 882	0.01	48155

Figura A-42.- Servicios por Mes

Device	petro
Date	Wed Jan 13 12:36:17 2010
Query	Top Services
Timeframe	Last 7 days
Filter	-
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	%	Conns	%	Packets	%	Port
1	HTTP	TCP	5.4 GB	7.94	78.6 GB	47.98	84.0 GB	36.16	1 632 980	24.53	115 145 735	35.89	80
2	HTTP-ALT	TCP	4.5 GB	6.61	77.7 GB	47.44	82.3 GB	35.39	864 598	12.99	109 857 495	34.24	8080
3	SMTP	TCP	56.6 GB	82.45	1.6 GB	0.99	58.2 GB	25.04	469 389	7.05	74 296 216	23.16	25
4	HTTPS	TCP	757.1 MB	1.08	4.1 GB	2.49	4.8 GB	2.07	195 479	2.94	8 447 237	2.63	443
5	DOMAIN	UDP	198.4 MB	0.28	566.7 MB	0.34	765.1 MB	0.32	2 818 679	42.33	5 538 128	1.73	53
6	0	GRE	456.8 MB	0.65	82.1 MB	0.05	538.9 MB	0.23	111	0.00	2 456 802	0.77	0
7	MS-WBT-SERVER	TCP	39.0 MB	0.06	330.8 MB	0.20	369.9 MB	0.16	348	0.01	1 683 636	0.52	3389
8	TINCAN	TCP	4.5 MB	0.01	238.2 MB	0.14	242.7 MB	0.10	42	0.00	280 255	0.09	1935
9	DYNAMID	TCP	2.2 MB	0.00	140.4 MB	0.08	142.6 MB	0.06	51	0.00	158 257	0.05	9002
10	WEBADMIN	TCP	8.2 MB	0.01	131.3 MB	0.08	139.5 MB	0.06	3 840	0.06	198 291	0.06	4444
11	8020	TCP	2.7 MB	0.00	113.8 MB	0.07	116.5 MB	0.05	6	0.00	173 201	0.05	8020
12	57875	TCP	85.5 MB	0.12	1.5 MB	0.00	87.0 MB	0.04	1	0.00	89 622	0.03	57875
13	54394	TCP	83.4 MB	0.12	1.4 MB	0.00	84.8 MB	0.04	1	0.00	87 414	0.03	54394
14	38875	TCP	80.8 MB	0.12	1.4 MB	0.00	82.2 MB	0.03	1	0.00	84 720	0.03	38875
15	41791	TCP	80.0 MB	0.11	1.4 MB	0.00	81.4 MB	0.03	1	0.00	83 867	0.03	41791
16	10303	TCP	78.1 MB	0.11	1.4 MB	0.00	79.4 MB	0.03	1	0.00	81 818	0.03	10303
17	42414	TCP	1.4 MB	0.00	73.7 MB	0.04	75.1 MB	0.03	1	0.00	89 952	0.03	42414
18	16827	TCP	48.4 MB	0.07	858.5 kB	0.00	49.2 MB	0.02	2	0.00	50 709	0.02	16827
19	25590	TCP	46.3 MB	0.07	821.5 kB	0.00	47.1 MB	0.02	1	0.00	48 517	0.02	25590
20	40551	TCP	726.7 kB	0.00	37.6 MB	0.02	38.3 MB	0.02	1	0.00	45 780	0.01	40551

Figura A-43.- Servicios por Semana

Device	petro
Date	Mon Jan 18 10:32:00 2010
Query	Top Services
Timeframe	Start: 2010-01-8 Stop: 2010-01-8
Filter	-
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	%	Conns	%	Packets	%	Port
1	HTTP-ALT	TCP	1.2 GB	12.34	15.2 GB	48.90	16.5 GB	40.00	227 530	19.86	22 365 816	38.39	8080
2	HTTP	TCP	1.1 GB	10.79	14.7 GB	47.31	15.8 GB	38.42	312 821	27.30	21 759 535	37.35	80
3	SMTP	TCP	7.4 GB	73.57	236.2 MB	0.74	7.6 GB	18.47	84 607	7.38	10 157 337	17.43	25
4	HTTPS	TCP	123.6 MB	1.21	646.6 MB	2.03	770.2 MB	1.83	38 043	3.32	1 405 217	2.41	443
5	TINCAN	TCP	2.5 MB	0.02	135.6 MB	0.43	138.1 MB	0.33	8	0.00	158 524	0.27	1935
6	DOMAIN	UDP	25.8 MB	0.25	79.8 MB	0.25	105.6 MB	0.25	376 526	32.86	747 706	1.28	53
7	0	GRE	75.6 MB	0.74	18.4 MB	0.06	94.0 MB	0.22	7	0.00	741 194	1.27	0
8	54394	TCP	83.4 MB	0.81	1.4 MB	0.00	84.8 MB	0.20	1	0.00	87 414	0.15	54394
9	MS-WBT-SERVER	TCP	8.4 MB	0.08	55.3 MB	0.17	63.7 MB	0.15	13	0.00	520 582	0.89	3389
10	WEBADMIN	TCP	802.5 kB	0.01	4.6 MB	0.01	5.4 MB	0.01	912	0.08	15 584	0.03	4444
11	HYDAP	UDP	5.2 MB	0.05	0	0.00	5.2 MB	0.01	264	0.02	14 424	0.02	15000
12	8500	TCP	739.6 kB	0.01	4.2 MB	0.01	5.0 MB	0.01	549	0.05	10 922	0.02	8500
13	11764	UDP	2.4 MB	0.02	1.5 MB	0.00	3.9 MB	0.01	56	0.00	29 256	0.05	11764
14	0	ICMP	3.7 MB	0.04	103.8 kB	0.00	3.8 MB	0.01	96 050	8.38	109 372	0.19	0
15	44603	TCP	99.8 kB	0.00	2.8 MB	0.01	2.9 MB	0.01	1	0.00	4 709	0.01	44603
16	44182	TCP	78.0 kB	0.00	2.7 MB	0.01	2.8 MB	0.01	1	0.00	3 860	0.01	44182
17	DOMAIN	TCP	364.7 kB	0.00	2.3 MB	0.01	2.7 MB	0.01	1 025	0.09	12 697	0.02	53
18	41220	TCP	81.3 kB	0.00	2.4 MB	0.01	2.5 MB	0.01	1	0.00	3 794	0.01	41220
19	43003	TCP	67.3 kB	0.00	2.4 MB	0.01	2.5 MB	0.01	1	0.00	3 420	0.01	43003
20	44786	TCP	52.7 kB	0.00	2.4 MB	0.01	2.4 MB	0.01	1	0.00	2 897	0.00	44786

Figura A-44.- Servicios 8 de Enero

Device	petro
Date	Mon Jan 18 10:32:00 2010
Query	Top Services
Timeframe	Start: 2010-01-8 Stop: 2010-01-8
Filter	-
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	%	Conns	%	Packets	%	Port
1	HTTP-ALT	TCP	1.2 GB	12.34	15.2 GB	48.90	16.5 GB	40.00	227 530	19.86	22 365 816	38.39	8080
2	HTTP	TCP	1.1 GB	10.79	14.7 GB	47.31	15.8 GB	38.42	312 821	27.30	21 759 535	37.35	80
3	SMTP	TCP	7.4 GB	73.57	236.2 MB	0.74	7.6 GB	18.47	84 607	7.38	10 157 337	17.43	25
4	HTTPS	TCP	123.6 MB	1.21	646.6 MB	2.03	770.2 MB	1.83	38 043	3.32	1 405 217	2.41	443
5	TINCAN	TCP	2.5 MB	0.02	135.6 MB	0.43	138.1 MB	0.33	8	0.00	158 524	0.27	1935
6	DOMAIN	UDP	25.8 MB	0.25	79.8 MB	0.25	105.6 MB	0.25	376 526	32.86	747 706	1.28	53
7	0	GRE	75.6 MB	0.74	18.4 MB	0.06	94.0 MB	0.22	7	0.00	741 194	1.27	0
8	54394	TCP	83.4 MB	0.81	1.4 MB	0.00	84.8 MB	0.20	1	0.00	87 414	0.15	54394
9	MS-WBT-SERVER	TCP	8.4 MB	0.08	55.3 MB	0.17	63.7 MB	0.15	13	0.00	520 582	0.89	3389
10	WEBADMIN	TCP	802.5 kB	0.01	4.6 MB	0.01	5.4 MB	0.01	912	0.08	15 584	0.03	4444
11	HYDAP	UDP	5.2 MB	0.05	0	0.00	5.2 MB	0.01	264	0.02	14 424	0.02	15000
12	8500	TCP	739.6 kB	0.01	4.2 MB	0.01	5.0 MB	0.01	549	0.05	10 922	0.02	8500
13	11764	UDP	2.4 MB	0.02	1.5 MB	0.00	3.9 MB	0.01	56	0.00	29 256	0.05	11764
14	0	ICMP	3.7 MB	0.04	103.8 kB	0.00	3.8 MB	0.01	96 050	8.38	109 372	0.19	0
15	44603	TCP	99.8 kB	0.00	2.8 MB	0.01	2.9 MB	0.01	1	0.00	4 709	0.01	44603
16	44182	TCP	78.0 kB	0.00	2.7 MB	0.01	2.8 MB	0.01	1	0.00	3 860	0.01	44182
17	DOMAIN	TCP	364.7 kB	0.00	2.3 MB	0.01	2.7 MB	0.01	1 025	0.09	12 697	0.02	53
18	41220	TCP	81.3 kB	0.00	2.4 MB	0.01	2.5 MB	0.01	1	0.00	3 794	0.01	41220
19	43003	TCP	67.3 kB	0.00	2.4 MB	0.01	2.5 MB	0.01	1	0.00	3 420	0.01	43003
20	44786	TCP	52.7 kB	0.00	2.4 MB	0.01	2.4 MB	0.01	1	0.00	2 897	0.00	44786

Figura A-45.- Servicios 11 de Enero

Device	petro
Date	Mon Jan 18 10:25:49 2010
Query	Top Services
Timeframe	Start: 2010-01-12 Stop: 2010-01-12
Filter	-
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	%	Conns	%	Packets	%	Port
1	SMTP	TCP	24.9 GB	92.19	619.9 MB	2.01	25.6 GB	44.72	62 340	4.01	30 226 797	39.80	25
2	HTTP	TCP	988.7 MB	3.57	14.6 GB	48.59	15.6 GB	27.27	340 492	21.88	21 735 229	28.62	80
3	HTTP-ALT	TCP	825.8 MB	2.98	13.6 GB	45.27	14.4 GB	25.24	185 186	11.90	19 893 289	26.19	8080
4	HTTPS	TCP	149.9 MB	0.54	902.3 MB	2.93	1.0 GB	1.80	40 872	2.63	1 785 040	2.35	443
5	DOMAIN	UDP	57.2 MB	0.21	143.1 MB	0.46	200.4 MB	0.34	772 931	49.66	1 487 692	1.96	53
6	WEBADMIN	TCP	3.7 MB	0.01	108.0 MB	0.35	111.7 MB	0.19	1 818	0.12	142 554	0.19	4444
7	8020	TCP	2.3 MB	0.01	96.6 MB	0.31	98.9 MB	0.17	4	0.00	145 692	0.19	8020
8	57875	TCP	85.5 MB	0.31	1.5 MB	0.00	87.0 MB	0.15	1	0.00	89 622	0.12	57875
9	0	GRE	23.2 MB	0.08	2.7 MB	0.01	25.9 MB	0.04	10	0.00	73 026	0.10	0
10	8500	TCP	1.6 MB	0.01	9.5 MB	0.03	11.1 MB	0.02	1 126	0.07	23 323	0.03	8500
11	0	ICMP	5.6 MB	0.02	357.1 kB	0.00	6.0 MB	0.01	134 230	8.62	151 832	0.20	0
12	HYDAP	UDP	5.4 MB	0.02	0	0.00	5.4 MB	0.01	309	0.02	15 072	0.02	15000
13	MS-WBT-SERVER	TCP	791.0 kB	0.00	2.8 MB	0.01	3.5 MB	0.01	10	0.00	19 602	0.03	3389
14	DOMAIN	TCP	380.1 kB	0.00	2.6 MB	0.01	2.9 MB	0.01	1 045	0.07	13 233	0.02	53
15	SNS-PROTOCOL	UDP	1.1 MB	0.00	921.1 kB	0.00	2.0 MB	0.00	2 931	0.19	22 081	0.03	2409
16	TINCAN	TCP	60.5 kB	0.00	963.3 kB	0.00	1023.8 kB	0.00	10	0.00	1 414	0.00	1935
17	12643	UDP	466.3 kB	0.00	385.3 kB	0.00	851.6 kB	0.00	1	0.00	6 222	0.01	12643
18	X11	UDP	631.3 kB	0.00	0	0.00	631.3 kB	0.00	2 257	0.15	17 956	0.02	6004
19	NETVIEW-AIX-11	TCP	447.0 kB	0.00	0	0.00	447.0 kB	0.00	1	0.00	384	0.00	1671
20	NETBIOS-NS	UDP	392.4 kB	0.00	10.4 kB	0.00	402.8 kB	0.00	314	0.02	5 040	0.01	137

Figura A-46.- Servicios 12 de Enero

Device	petro
Date	Wed Jan 13 12:03:11 2010
Query	Top Services by Server
Timeframe	Last 30 days
Filter	Destination IP = "172.16.49.31"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	SMTP	TCP	35.1 GB	99.99	1.4 GB	99.72	36.4 GB	36.4 GB	665 886	95.12	54 267 457	99.83	25
2	MS-WBT-SERVER	TCP	1.6 MB	0.00	2.3 MB	0.17	4.0 MB	4.0 MB	127	0.02	42 606	0.08	3389
3	HTTPS	TCP	1.6 MB	0.00	0	0.00	1.6 MB	1.6 MB	28 286	4.04	28 418	0.05	443
4	HTTP	TCP	250.4 kB	0.00	719.7 kB	0.05	970.1 kB	970.1 kB	313	0.04	3 582	0.01	80
5	EPMAP	TCP	402.5 kB	0.00	54.8 kB	0.00	457.3 kB	457.3 kB	160	0.02	1 845	0.00	135
6	0	ICMP	187.2 kB	0.00	186.3 kB	0.01	373.4 kB	373.4 kB	2 425	0.35	4 861	0.01	0
7	NETBIOS-NS	UDP	90.9 kB	0.00	257.3 kB	0.02	348.1 kB	348.1 kB	787	0.11	2 385	0.00	137
8	1196	TCP	76.0 kB	0.00	224.9 kB	0.02	300.9 kB	300.9 kB	5	0.00	1 021	0.00	1196
9	SYMBIOS-RAID	TCP	106.0 kB	0.00	153.3 kB	0.01	259.3 kB	259.3 kB	125	0.02	4 355	0.01	2463
10	MS-SQL-M	UDP	45.0 kB	0.00	0	0.00	45.0 kB	45.0 kB	114	0.02	114	0.00	1434

Figura A-47.- Servidor Exchange por Mes

Device	petro
Date	Wed Jan 13 11:59:42 2010
Query	Top Services by Server
Timeframe	Last 7 days
Filter	Destination IP = "172.16.49.31"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	SMTP	TCP	6.5 GB	99.98	279.3 MB	99.89	6.8 GB	6.8 GB	152 066	92.64	10 559 655	99.86	25
2	HTTPS	TCP	627.3 kB	0.01	0	0.00	627.3 kB	627.3 kB	10 772	6.56	10 773	0.10	443
3	EPMAP	TCP	287.3 kB	0.00	39.4 kB	0.01	326.7 kB	326.7 kB	111	0.07	1 332	0.01	135
4	HTTP	TCP	97.0 kB	0.00	182.4 kB	0.06	279.5 kB	279.5 kB	81	0.05	937	0.01	80
5	NETBIOS-NS	UDP	24.0 kB	0.00	68.0 kB	0.02	92.0 kB	92.0 kB	222	0.14	630	0.01	137
6	0	ICMP	19.6 kB	0.00	19.6 kB	0.01	39.1 kB	39.1 kB	314	0.19	628	0.01	0
7	MS-SQL-M	UDP	13.4 kB	0.00	0	0.00	13.4 kB	13.4 kB	34	0.02	34	0.00	1434
8	4899	TCP	4.6 kB	0.00	0	0.00	4.6 kB	4.6 kB	96	0.06	96	0.00	4899
9	ISAKMP	UDP	3.9 kB	0.00	0	0.00	3.9 kB	3.9 kB	4	0.00	14	0.00	500
10	5900	TCP	3.8 kB	0.00	0	0.00	3.8 kB	3.8 kB	78	0.05	78	0.00	5900
11	SIP	UDP	3.0 kB	0.00	0	0.00	3.0 kB	3.0 kB	3	0.00	3	0.00	5060

Figura A-48.- Servidor Exchange por Semana

Device	petro
Date	Wed Jan 13 12:16:25 2010
Query	Top Services by Server
Timeframe	Start: 2010-01-8 Stop: 2010-01-8
Filter	Destination IP = "172.16.49.31"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	SMTP	TCP	1.1 GB	99.98	46.2 MB	99.86	1.2 GB	1.2 GB	23 782	92.66	1 771 197	99.85	25
2	EPMAP	TCP	132.8 kB	0.01	19.2 kB	0.04	152.1 kB	152.1 kB	52	0.20	623	0.04	135
3	HTTPS	TCP	94.9 kB	0.01	0	0.00	94.9 kB	94.9 kB	1 626	6.34	1 626	0.09	443
4	HTTP	TCP	7.3 kB	0.00	34.4 kB	0.07	41.7 kB	41.7 kB	14	0.05	161	0.01	80
5	NETBIOS-NS	UDP	3.5 kB	0.00	9.9 kB	0.02	13.4 kB	13.4 kB	29	0.11	92	0.01	137
6	0	ICMP	3.0 kB	0.00	3.0 kB	0.01	6.0 kB	6.0 kB	48	0.19	96	0.01	0
7	ISAKMP	UDP	2.0 kB	0.00	0	0.00	2.0 kB	2.0 kB	1	0.00	7	0.00	500
8	MS-SQL-M	UDP	1.6 kB	0.00	0	0.00	1.6 kB	1.6 kB	4	0.02	4	0.00	1434
9	4899	TCP	0.9 kB	0.00	0	0.00	0.9 kB	0.9 kB	18	0.07	18	0.00	4899
10	NDL-AAS	TCP	0.5 kB	0.00	0	0.00	0.5 kB	0.5 kB	11	0.04	11	0.00	3128
11	HTTP-ALT	TCP	0.5 kB	0.00	0	0.00	0.5 kB	0.5 kB	10	0.04	10	0.00	8080

Device	petro
Date	Wed Jan 13 12:15:55 2010
Query	Top Services by Server
Timeframe	Start: 2010-01-11 Stop: 2010-01-11
Filter	Destination IP = "172.16.49.31"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	SMTP	TCP	1.3 GB	99.99	45.1 MB	99.89	1.3 GB	1.3 GB	21 622	91.61	1 858 603	99.88	25
2	HTTPS	TCP	102.5 kB	0.01	0	0.00	102.5 kB	102.5 kB	1 783	7.55	1 783	0.10	443
3	HTTP	TCP	11.6 kB	0.00	38.6 kB	0.08	50.1 kB	50.1 kB	17	0.07	187	0.01	80
4	NETBIOS-NS	UDP	3.6 kB	0.00	10.1 kB	0.02	13.7 kB	13.7 kB	33	0.14	94	0.01	137
5	0	ICMP	3.8 kB	0.00	3.8 kB	0.01	7.7 kB	7.7 kB	62	0.26	124	0.01	0
6	EPMAP	TCP	3.4 kB	0.00	0.4 kB	0.00	3.7 kB	3.7 kB	1	0.00	12	0.00	135
7	ISAKMP	UDP	1.9 kB	0.00	0	0.00	1.9 kB	1.9 kB	3	0.01	7	0.00	500
8	4899	TCP	1.4 kB	0.00	0	0.00	1.4 kB	1.4 kB	28	0.12	28	0.00	4899
9	MS-SQL-M	UDP	1.2 kB	0.00	0	0.00	1.2 kB	1.2 kB	3	0.01	3	0.00	1434
10	NDL-AAS	TCP	0.4 kB	0.00	0	0.00	0.4 kB	0.4 kB	8	0.03	8	0.00	3128

Device	petro
Date	Wed Jan 13 12:15:16 2010
Query	Top Services by Server
Timeframe	Start: 2010-01-12 Stop: 2010-01-12
Filter	Destination IP = "172.16.49.31"
Ordered by	Traffic (descending)

Top	Service	Protocol	In	%	Out	%	Traffic	Traffic	Conns	%	Packets	%	Port
1	SMTP	TCP	1.2 GB	99.99	45.8 MB	99.92	1.3 GB	1.3 GB	22 905	91.73	1 841 997	99.87	25
2	HTTPS	TCP	109.1 kB	0.01	0	0.00	109.1 kB	109.1 kB	1 874	7.51	1 874	0.10	443
3	HTTP	TCP	6.8 kB	0.00	21.9 kB	0.05	28.6 kB	28.6 kB	9	0.04	115	0.01	80
4	NETBIOS-NS	UDP	3.0 kB	0.00	8.4 kB	0.02	11.4 kB	11.4 kB	32	0.13	78	0.00	137
5	EPMAP	TCP	9.9 kB	0.00	0.9 kB	0.00	10.8 kB	10.8 kB	3	0.01	33	0.00	135
6	0	ICMP	5.2 kB	0.00	5.2 kB	0.01	10.5 kB	10.5 kB	83	0.33	166	0.01	0
7	MS-SQL-M	UDP	2.8 kB	0.00	0	0.00	2.8 kB	2.8 kB	7	0.03	7	0.00	1434
8	SIP	UDP	1.0 kB	0.00	0	0.00	1.0 kB	1.0 kB	1	0.00	1	0.00	5060
9	4899	TCP	0.6 kB	0.00	0	0.00	0.6 kB	0.6 kB	12	0.05	12	0.00	4899
10	SMTPS	TCP	0.4 kB	0.00	0	0.00	0.4 kB	0.4 kB	9	0.04	9	0.00	465

Figura A-49.- Servidor Exchange por Día

ANEXO B

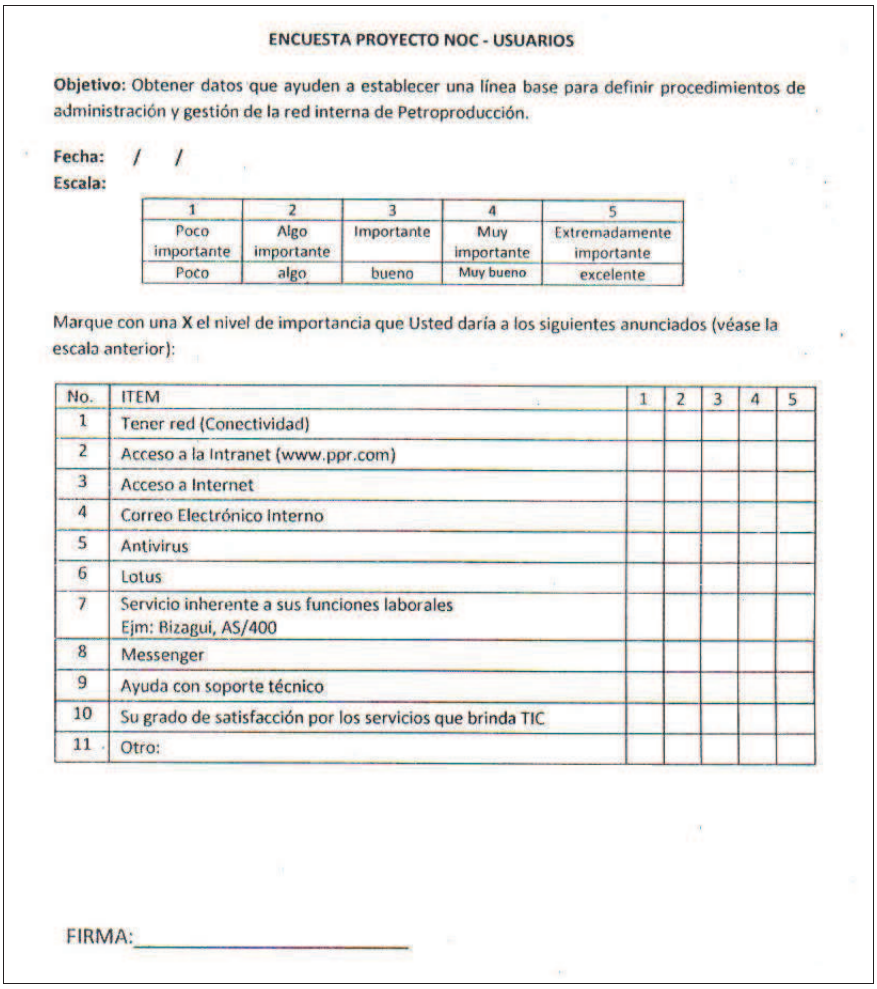
ANÁLISIS DE ENCUESTAS.

ANÁLISIS DE ENCUESTAS

La recolección de información se realizó en base a los métodos de Visualización, Encuestas y estadísticas.

ENCUESTA A USUARIOS

La figura B.1 muestra la encuesta realizada a usuarios comunes de la red de Petroproducción[1].



ENCUESTA PROYECTO NOC - USUARIOS

Objetivo: Obtener datos que ayuden a establecer una línea base para definir procedimientos de administración y gestión de la red interna de Petroproducción.

Fecha: / /

Escala:

1	2	3	4	5
Poco importante	Algo importante	Importante	Muy importante	Extremadamente importante
Poco	algo	bueno	Muy bueno	excelente

Marque con una **X** el nivel de importancia que Usted daría a los siguientes anunciados (véase la escala anterior):

No.	ITEM	1	2	3	4	5
1	Tener red (Conectividad)					
2	Acceso a la Intranet (www.ppr.com)					
3	Acceso a Internet					
4	Correo Electrónico Interno					
5	Antivirus					
6	Lotus					
7	Servicio inherente a sus funciones laborales Ejm: Bizagui, AS/400					
8	Messenger					
9	Ayuda con soporte técnico					
10	Su grado de satisfacción por los servicios que brinda TIC					
11	Otro:					

FIRMA:_____

Figura B-1.- Encuesta para Usuarios Comunes

ENCUESTA A PERSONAL DEL TIC

La figura B.2 y la figura B.3 muestra la encuesta realizada al personal del TIC de Petroproducción Quito para obtener información acerca de gestión de fallos, opinión del sistema operativo Linux y de administración de red.

[1] Un usuario común es todo usuario que no sea de gerencia y no sea parte del personal de TIC.

ENCUESTA PROYECTO NOC (Network Operation Center)

Objetivo: Obtener datos que ayuden a establecer una línea base para definir procedimientos de administración y gestión de la red interna de Petroproducción.

Datos del Encuestado: **Fecha:** / /

Función dentro del departamento de TIC: _____

Tiempo trabajando en Petroproducción:

Menos de un año	Entre 1 y 3 años	Entre 3 y 5 años	Más de 5 años.

Escala:

1	2	3	4	5
Poco importante	Algo importante	Importante	Muy importante	Extremadamente importante

Tema 1: Sistema Operativo Linux y Administración de Redes

Marque con una **X** el nivel de importancia que Usted daría a los siguientes anunciados:

N.	Enunciado	1	2	3	4	5
	Linux					
1	¿Conoce acerca del sistema Linux?	SI:		NO:		
2	¿Considera importante la utilización de aplicaciones de Linux en redes empresariales?					
3	¿Cuál considera la distribución Linux más solvente para un servidor?	Ubuntu	RedHat	Centos	Suse	Fedora
	Administración					
4	Monitoreo de equipos activos de una red.					
5	Monitoreo de Enlaces (LAN, WAN, Microonda)					
6	Administración de Red					
7	Seguridad de la Red (Políticas, Mecanismos y Procedimientos)					

Tema 2: Respuesta a Fallos

En la siguiente escala cuán crítico considera los siguientes problemas/fallos para la operación y correcto funcionamiento de la red interna.

N.	FALLA	1	2	3	4	5
8	Caída de un enlace WAN interno de la Red (Dentro de Quito).					
9	Caída de un enlace WAN de la Red (Fuera de Quito).					
10	Caída del enlace a Internet					
11	Caída de un servidor de área operativa. Ejm: Bizagi, Geographics,					
12	Caída del servidor Active Directory					
13	Caída de un servidor de uso general Ejm: Mail, Antivirus, Lotus, Web					
14	Problemas en la red de transporte.					
15	Fuera de servicio de Hardware o Software del backbone.					
16	Problemas con un Switch de acceso.					
17	Problemas con un Switch de distribución.					
18	Problemas con un Switch de Core.					
19	Problemas con un Router					
20	Problemas con puntos de red y cableado estructurado					
21	Problemas software o hardware en equipos de usuarios normales.					
22	No se pueden leer las MIBs de un equipo.					
23	Equipo no responde a SNMP pero si a Ping.					
24	No existe conectividad alguna sobre el dispositivo					
25	El dispositivo a sufrido un problema eléctrico y deja de funcionar					

Figura B-2.- Encuesta para personal del TIC Quito PARTE 1.

Tema 3. Tiempos de Respuesta

Suponga que los fallos descritos anteriormente suceden, ¿En qué tiempo máximo considera Usted se debería solucionar dichos problemas?

N.	FALLA	5-15 min	15-30 min	30-60 min	1-2 horas	> 2 horas
26	Caída de un enlace WAN interno de la Red (Dentro de Quito).					
27	Caída de un enlace WAN de la Red (Fuera de Quito).					
28	Caída del enlace a Internet					
29	Caída de un servidor de área operativa. Ejm: Bizagi, Geographics,					
30	Caída del servidor Active Directory					
31	Caída de un servidor de uso general Ejm: Mail, Antivirus, Lotus, Web					
32	Problemas en la red de transporte.					
33	Fuera de servicio de Hardware o Software del backbone.					
34	Problemas con un Switch de acceso.					
35	Problemas con un Switch de distribución.					
36	Problemas con un Switch de Core.					
37	Problemas con un Router					
38	Problemas con puntos de red y cableado estructurado					
39	Problemas software o hardware en equipos de usuarios normales.					
40	No se pueden leer las MIBs de un equipo. (información de un equipo)					
41	Equipo no responde a SNMP pero si a Ping.					
42	No existe conectividad alguna sobre el dispositivo					
43	El dispositivo a sufrido un problema eléctrico y deja de funcionar					

FIRMA: _____

Figura B-3.- Encuesta para personal del TIC Quito PARTE 2.

RESULTADOS DE LAS ENCUESTAS AL PERSONAL DE TIC

Para el análisis de las encuestas primeramente se ponderó un factor multiplicativo para dar mayor énfasis a criterios del Personal del TIC con mayor tiempo y experiencia dentro de la empresa, los valores se muestran en la Tabla B-1.

Tiempo	Factor	Cantidad
Menor a 1 año	1	2
Entre 1 y 3 años	2	1
Entre 3 y 5 años	3	0
Más de 5 años	4	6
	TOTAL:	9

Tabla B-1.- Factor multiplicativo según experiencia en PPR.

DISTRIBUCIÓN LINUX SOLVENTE

La Tabla B-2 muestra como resultado que el personal de TIC considera a Redhat como la distribución de Linux más solvente de las presentadas.

Distribución LINUX	Ubuntu	RedHat	Centos	Suse	Fedora
Menor a 1 año		1	2		
Entre 1 y 3 años		1			
Entre 3 y 5 años					
Más de 5 años		5			
Cantidad:	0	7	2	0	0
RESULTADO	0	23	2	0	0

Tabla B-2.- Consideración de distribución Linux solvente.

IMPORTANCIA LINUX

Según la escala presentada en las encuestas realizadas, se tiene como valor de "1" a la equivalencia "Poco importante" subiendo paulatinamente hasta el valor de "5" que es "Extremadamente importante"

La Tabla B-3 y la Figura B-4.- Consideración de Importancia del S.O. Linux a nivel empresarial.Figura B-4 muestran que el personal de TIC considera que es extremadamente el Sistema Operativo Linux a nivel empresarial por todos los beneficios que este puede dar.

NIVEL	1	2	3	4	5
Menor a 1 año		1			1
Entre 1 y 3 años		1			
Entre 3 y 5 años					
Más de 5 años			2	1	2
Cantidad:	0	2	2	1	3
RESULTADO	0	3	8	4	9

Tabla B-3.- Importancia del S.O. Linux a nivel empresarial.

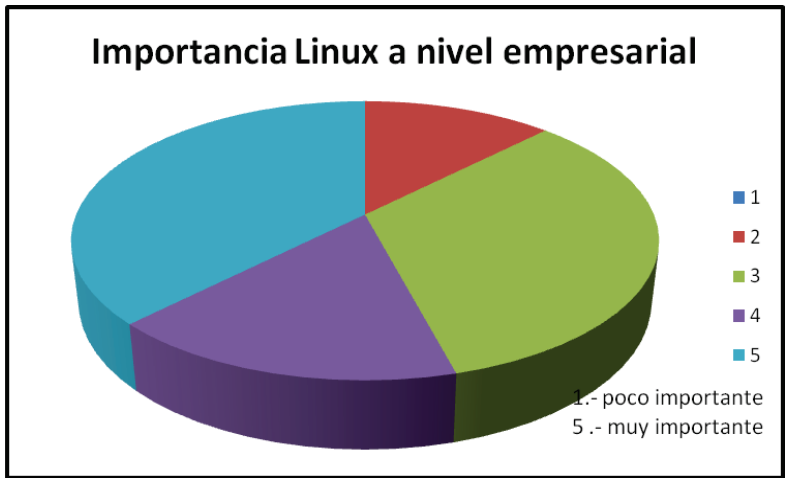


Figura B-4.- Consideración de Importancia del S.O. Linux a nivel empresarial.

ADMINISTRACIÓN Y GESTIÓN DE RED

Las siguientes tablas y la **¡Error! No se encuentra el origen de la referencia.** presentan los resultados sobre las preguntas referentes a la administración y gestión de una red.

Monitoreo Equipos activos	1	2	3	4	5
Menor a 1 año			1	1	
Entre 1 y 3 años		1			
Entre 3 y 5 años					
Más de 5 años		2		3	1
RESULTADO	0	10	1	13	4
Cantidad:	0	3	1	4	1

Tabla B-4.- Importancia del monitoreo de equipos activos de una red.

Administración de Red	1	2	3	4	5
Menor a 1 año				2	
Entre 1 y 3 años					1
Entre 3 y 5 años					
Más de 5 años		2	1	1	2
RESULTADO	0	8	4	6	10
Cantidad:	0	2	1	3	3

Tabla B-5.- Importancia de la Administración de una red.

Monitoreo Enlaces	1	2	3	4	5
Menor a 1 año				2	
Entre 1 y 3 años		1			
Entre 3 y 5 años					
Más de 5 años		2		2	2
RESULTADO	0	10	0	10	8
Cantidad:	0	3	0	4	2

Tabla B-6.- Importancia del monitoreo de enlaces.

Seguridad de Red	1	2	3	4	5
Menor a 1 año		1		1	
Entre 1 y 3 años					1
Entre 3 y 5 años					
Más de 5 años		2		2	2
RESULTADO	0	9	0	9	10
Cantidad:	0	3	0	3	3

Tabla B-7.- Importancia de la Seguridad de Red.

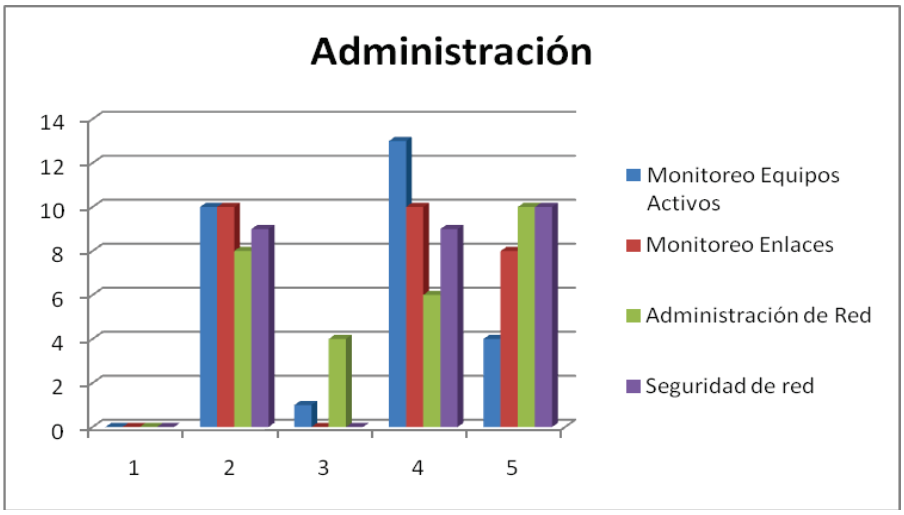


Figura B-5.- Importancia de Administración y Gestión de Red

Se puede concluir que el personal de TIC de PPR considera que tanto la Administración como la Seguridad de Red son extremadamente importantes, mientras que el monitoreo de equipos y enlaces son un muy importantes, basando en la escala planteada en la encuesta.

FALLOS

Finalmente la Tabla B-8 presenta las consideraciones de el nivel de criticidad de algunos de los posibles fallos que se pueden presentar en la red, siendo "1" el valor que representa a lo menos crítico y el "5" a extremadamente Crítico; Mientras que la Tabla B-9 muestra lo que el personal de TIC considera el tiempo máximo en el cual deben ser corregidos dichos problemas para generar el menor impacto en el rendimiento de la red.

		TOTAL Criticidad				
		NIVEL				
	FALLA	1	2	3	4	5
1	Caída enlace WAN interno (Quito)				X	
2	Caída enlace WAN externo (Fuera de Quito)					X
3	Caída enlace internet					X
4	Caída Servidor de área Operativa					X
5	Caída servidor Active Directory					X
6	Caída servidor de uso general					X
7	Problemas en la red de transporte			X		
8	Fuera de servicio de Hw. o Sw de Backbone					X
9	Problemas Switch acceso			X		
10	Problemas Switch distribución				X	
11	Problemas Switch core					X
12	Problemas con un Router					X
13	Problemas con cableado estructurado			X		
14	Problemas Hw. o Sw de usuario normal.			X		

15	No se pueden leer las MIBs de un equipo			X	X	
16	Equipo no responde a SNMP pero si a ping.			X		
17	No existe conectividad en un dispositivo común			X		
18	Dispositivo fuera de servicio por problema eléctrico.			X		

Tabla B-8.- Consideración de Criticidad de Fallos.

		TOTAL Tiempos de Respuesta				
		Tiempo				
	FALLA	5-15 min	15-30 min	30-60 min	1-2 horas	> 2 horas
1	Caída enlace WAN interno (Quito)		X			
2	Caída enlace WAN externo (Fuera de Quito)	X				
3	Caída enlace internet			X		
4	Caída Servidor de área Operativa	X				
5	Caída servidor Active Directory	X				
6	Caída servidor de uso general	X				
7	Problemas en la red de transporte		X			
8	Fuera de servicio de Hw. o Sw de Backbone	X				
9	Problemas Switch acceso		X			
10	Problemas Switch distribución		X			
11	Problemas Switch core	X				
12	Problemas con un Router	X				
13	Problemas con cableado estructurado		X			
14	Problemas Hw. o Sw de usuario normal.			X		
15	No se pueden leer las MIBs de un equipo		X			
16	Equipo no responde a SNMP pero si a ping.			X		
17	No existe conectividad en un dispositivo común			X		
18	Dispositivo fuera de servicio por problema eléctrico.			X		

Tabla B-9.- Consideración de Tiempos máximos de Respuesta a Fallos.

ANEXO C

PERSONAL PETROPRODUCCIÓN.

PERSONAL DE PETROPRODUCCIÓN.

CARGOS DE PERSONAL DEL TIC

El área de Tecnologías de información y Comunicaciones de Petroproducción tiene su personal con los siguientes cargos:

- Coordinador TIC.
- Supervisor de Aplicaciones.
- Analista de Aplicaciones.
- Asistente de Aplicaciones.
- Supervisor de Datos.
- Analista de Datos.
- Supervisor de Infraestructura de Comunicaciones.
- Analista de Infraestructura de Comunicaciones.
- Asistente de Infraestructura de Comunicaciones.
- Supervisor de Seguridad Tecnológica.
- Analista de seguridad Tecnológica.
- Supervisor de soporte a Usuario.
- Asistente de soporte a Usuario.

Este personal tiene diferentes responsabilidades según su cargo como se detallan en las siguientes tablas.

COORDINADOR DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

CARGO	
COORDINADOR DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	
MISIÓN	
COORDINAR Y ADMINISTRAR LAS FUNCIONES DE TODAS LAS SECCIONES PERTENECIENTES A LA COORDINACIÓN EN FUNCIÓN DE LAS NECESIDADES TECNOLÓGICAS DE PETROPRODUCCIÓN.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	COORDINAR Y SUPERVISAR LAS ACTIVIDADES DE LAS DIFERENTES SECCIONES Y PERSONAL DE LA COORDINACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN SU ÁMBITO DE GESTIÓN.
2	DIFUNDIR Y PROPICIAR EL USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LA EMPRESA EN SU ÁMBITO DE GESTIÓN.
3	CUMPLIR Y HACER CUMPLIR LAS NORMAS EMITIDAS POR LOS ORGANISMOS DE CONTROL.
4	DAR SEGUIMIENTO Y EJECUTAR RECOMENDACIONES DE AUDITORIAS REALIZADAS POR ORGANISMOS DE CONTROL EXTERNOS E INTERNOS.
5	PLANIFICAR Y SOMETER A LA APROBACIÓN DE LA COORDINACIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES LAS POLÍTICAS PARA EL DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN, SISTEMAS DE COMUNICACIONES Y LA ADQUISICIÓN E IMPLEMENTACIÓN DE SOFTWARE, ASÍ COMO DEL FORTALECIMIENTO DE LA INFRAESTRUCTURA COMPUTACIONAL Y DE COMUNICACIONES DE LA EMPRESA.
6	ESTABLECER Y MANTENER ACTUALIZADOS POLÍTICAS, NORMAS Y ESTÁNDARES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES PARA PETROPRODUCCIÓN.

7	SUPERVISAR EL CUMPLIMIENTO DE ESTÁNDARES, NORMAS Y PROCEDIMIENTOS ESTABLECIDOS Y VIGENTES EN LA EMPRESA PARA LA UTILIZACIÓN DE LOS RECURSOS DE TECNOLOGÍA.
8	INVESTIGAR, ASESORAR Y RECOMENDAR A LOS NIVELES DE DECISIÓN SOBRE ASUNTOS RELACIONADOS CON LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.
9	PLANIFICAR, DIRIGIR Y DAR SEGUIMIENTO A LA EJECUCIÓN DE PROYECTOS DE TECNOLOGÍA DE LA EMPRESA.
10	GESTIONAR RECURSOS PARA LAS DIFERENTES SECCIONES DE LA COORDINACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN SU ÁMBITO.
11	ADMINISTRAR CONTRATOS ESTABLECIDOS CON PROVEEDORES Y CONTRATISTAS DE LOS SISTEMAS DE INFORMACIÓN Y DE COMUNICACIONES.
12	ESTUDIAR EL MERCADO INFORMÁTICO Y DE COMUNICACIONES EN REFERENCIA A NUEVOS PRODUCTOS, TENDENCIAS Y SERVICIOS TECNOLÓGICOS QUE PUEDAN SER IMPLEMENTADOS EN PETROPRODUCCIÓN.
13	PLANIFICAR Y COORDINAR EL EQUIPO TÉCNICO DE LAS DIFERENTES SECCIONES, QUE PARTICIPARÁN EN LOS PROYECTOS QUE INVOLUCREN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.
14	PRIORIZAR Y ATENDER LOS REQUERIMIENTOS DE LAS ÁREAS USUARIAS.
15	GESTIONAR LA CAPACITACIÓN INTEGRAL DEL PERSONAL DE LA COORDINACIÓN A SU CARGO.
16	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE; PARTICIPAR EN REUNIONES DE DIRECTIVOS DE LA EMPRESA, REUNIONES DE STAFF, DE PROYECTOS, DE PRESUPUESTOS, ENTRE OTRAS.

Tabla C-1.- Actividades del Coordinador de Tecnologías de Información y Comunicaciones.

SUPERVISOR DE APLICACIONES

CARGO	
SUPERVISOR DE APLICACIONES	
MISIÓN	
COORDINAR LAS ACTIVIDADES DE LA SECCIÓN, IDENTIFICAR NECESIDADES INFORMÁTICAS DE LOS USUARIOS FINALES, COORDINAR LA EJECUCIÓN DE PROYECTOS QUE SATISFAGAN LAS NECESIDADES TECNOLÓGICAS DE LA EMPRESA.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	DEFINIR Y VELAR POR EL CUMPLIMIENTO DE LOS ÍNDICES DE GESTIÓN PARA LA SECCIÓN.
2	ANALIZAR LAS NECESIDADES DE APLICACIONES INFORMÁTICAS DE LOS DIFERENTES DEPARTAMENTOS DE LA EMPRESA Y PROPONER SOLUCIONES PARA MEJORAR LA SITUACIÓN EVIDENCIADA.
3	ELABORAR, ACORDAR E INFORMAR A LA COORDINACIÓN AVANCES EN EL PLAN DE LA SECCIÓN DE APLICACIONES (INVERSIONES, CRONOGRAMAS, PROYECTOS, PRESUPUESTOS, ETC).
4	REDACTAR, CUMPLIR Y HACER CUMPLIR PROTOCOLOS, NORMATIVAS Y PROCEDIMIENTOS DE LA SECCIÓN.
5	PLANIFICAR, GESTIONAR Y CONTROLAR PROYECTOS DE LA SECCIÓN EN COORDINACIÓN CON LAS OTRAS SECCIONES.
6	DESIGNAR Y SUPERVISAR LA ELABORACIÓN DE ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE APLICACIONES, Y LA ELABORACIÓN DE INFORMES DE JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.
7	IMPLANTAR LOS PLANES DE SEGURIDAD EN APLICACIONES.
8	ESTUDIAR, ESTABLECER Y EVALUAR LAS PRUEBAS A REALIZARSE PARA DETECTAR POSIBLES PROBLEMAS DE FUNCIONAMIENTO EN APLICACIONES.

9	ESTUDIAR EL MERCADO INFORMÁTICO EN REFERENCIA A NUEVAS APLICACIONES QUE PUEDAN SER IMPLANTADAS EN PETROPRODUCCIÓN
10	APROBAR INFORMES DE ANÁLISIS DE REQUISITOS DE APLICACIONES INFORMÁTICAS DE LA EMPRESA EN FUNCIÓN DE LOS REQUERIMIENTOS DEL USUARIO.
11	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-2.- Actividades del Supervisor de Aplicaciones.

ANALISTA DE APLICACIONES

CARGO	
ANALISTA DE APLICACIONES	
MISIÓN	
DISEÑAR, PROGRAMAR E IMPLANTAR APLICACIONES INFORMÁTICAS PARA PETROPRODUCCIÓN	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	PREPARAR ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE APLICACIONES, ELABORAR INFORMES DE JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.
2	IMPLEMENTAR TÉCNICAS Y PROCEDIMIENTOS INFORMÁTICOS EN SU ÁMBITO DE ACCIÓN.
3	BRINDAR SOPORTE DE NIVEL 2 A LAS APLICACIONES DE PETROPRODUCCIÓN
4	ANALIZAR Y ESPECIFICAR EL ALCANCE Y FACTIBILIDAD DE DESARROLLO E IMPLEMENTACIÓN DE NUEVAS APLICACIONES UTILIZANDO LAS TÉCNICAS, HERRAMIENTAS Y MÉTODOS ADECUADOS.
5	DESARROLLAR, PERSONALIZAR E IMPLANTAR APLICACIONES INFORMÁTICAS ACORDES A LAS NECESIDADES DE LA EMPRESA. ELABORAR LA DOCUMENTACIÓN INHERENTE.
6	EJECUTAR PLANES DE SEGURIDAD DE LA INFORMACIÓN DE LAS APLICACIONES.
7	ANALIZAR Y EJECUTAR PRUEBAS PARA DETECTAR LAS PROBLEMAS DE FUNCIONAMIENTO DE LAS APLICACIONES
8	ADMINISTRAR Y OPTIMIZAR LAS APLICACIONES INFORMÁTICAS
9	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-3.- Actividades del Analista de Aplicaciones.

ASISTENTE DE APLICACIONES

CARGO
ASISTENTE DE APLICACIONES
MISIÓN
ATENDER SOLICITUDES DE TERCER NIVEL DE SOPORTE DE APLICACIONES. IMPLANTAR Y CAPACITAR AL USUARIO FINAL EN LAS NUEVAS APLICACIONES DESARROLLADAS O IMPLANTADAS POR LA SECCIÓN.
ACTIVIDADES

NÚMERO	ACTIVIDADES
1	CAPACITAR A FUNCIONARIOS DE PETROPRODUCCIÓN ACERCA DEL USO DE APLICACIONES INHERENTES A SUS CARGOS.
2	REALIZAR LA INSTALACIÓN E IMPLANTACIÓN DE APLICACIONES.
3	REALIZAR INFORMES EN REFERENCIA A RESULTADOS OBTENIDOS CON LA IMPLANTACIÓN DE APLICACIONES.
4	LLEVAR EL CONTROL DE LAS INCIDENCIAS DE LAS DIFERENTES APLICACIONES Y NOTIFICARLAS A SU SUPERIOR.
5	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE.

Tabla C-4.- Actividades del Asistente de Aplicaciones.

SUPERVISOR DE DATOS

CARGO	
SUPERVISOR DE DATOS	
MISIÓN	
COORDINAR LAS ACTIVIDADES DE LA SECCIÓN, IMPLEMENTAR Y EJECUTAR POLÍTICAS DE SEGURIDAD Y RESPALDOS DE INFORMACIÓN CONTENIDA EN LAS BASES DE DATOS, PLANIFICAR PROYECTOS DE EXPANSIÓN DE BASES DE DATOS.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	DEFINIR Y VELAR POR EL CUMPLIMIENTO DE LOS ÍNDICES DE GESTIÓN PARA LA SECCIÓN.
2	ELABORAR, ACORDAR E INFORMAR A LA COORDINACIÓN AVANCES EN EL PLAN DE LA SECCIÓN DE DATOS (INVERSIONES, CRONOGRAMAS, PROYECTOS, PRESUPUESTOS, ETC).
3	REDACTAR, CUMPLIR Y HACER CUMPLIR PROTOCOLOS, NORMATIVAS Y PROCEDIMIENTOS DE LA SECCIÓN.
4	PLANIFICAR, GESTIONAR Y CONTROLAR PROYECTOS DE LA SECCIÓN EN COORDINACIÓN CON LAS OTRAS SECCIONES.
5	DESIGNAR Y SUPERVISAR LA ELABORACIÓN DE ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE HERRAMIENTAS PARA EL ALMACENAMIENTO Y ADMINISTRACIÓN DE DATOS, Y LA ELABORACIÓN DE INFORMES DE JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.
6	IMPLANTAR PLANES DE SEGURIDAD PARA DATOS.
7	ESTUDIAR, ESTABLECER Y EVALUAR LAS PRUEBAS A REALIZARSE PARA DETECTAR POSIBLES INCONSISTENCIAS EN LOS DATOS.
8	ESTUDIAR EL MERCADO INFORMÁTICO EN REFERENCIA A NUEVAS HERRAMIENTAS DE ALMACENAMIENTO Y ADMINISTRACIÓN DE DATOS QUE PUEDAN SER IMPLANTADAS EN PETROPRODUCCIÓN.
9	APROBAR INFORMES DE ANÁLISIS DE REQUISITOS DE ALMACENAMIENTO DE DATOS DE LA EMPRESA EN FUNCIÓN DE LOS REQUERIMIENTOS DE LAS APLICACIONES.
10	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-5.- Actividades del Supervisor de Datos.

ANALISTA DE DATOS

CARGO	
ANALISTA DE DATOS	
MISIÓN	
CREAR, ADMINISTRAR Y DAR MANTENIMIENTO A LAS BASES DE DATOS DE PETROPRODUCCIÓN. APLICAR LAS POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN CONTENIDA EN LAS BASES. MONITOREAR EVENTOS DE SEGURIDAD EN LAS BASES DE DATOS.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	PREPARAR ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE HERRAMIENTAS DE ALMACENAMIENTO Y ADMINISTRACIÓN DE DATOS, ELABORAR INFORMES DE JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.
2	IMPLEMENTAR TÉCNICAS Y PROCEDIMIENTOS INFORMÁTICOS EN SU ÁMBITO DE ACCIÓN.
3	ANALIZAR Y ESPECIFICAR EL ALCANCE, FACTIBILIDAD E IMPLANTACIÓN DE NUEVAS HERRAMIENTAS PARA EL ALMACENAMIENTO Y ADMINISTRACIÓN DE DATOS.
4	EJECUTAR PLANES DE SEGURIDAD DE LA ADMINISTRACIÓN DE LOS DATOS.
5	ANALIZAR Y EJECUTAR PRUEBAS PARA DETECTAR LOS PROBLEMAS DE INTEGRIDAD Y CONSISTENCIA DE LOS DATOS.
6	ADMINISTRAR Y OPTIMIZAR LAS BASES DE DATOS.
7	REALIZAR PERIÓDICAMENTE RESPALDOS DE LOS DATOS Y REALIZAR PRUEBAS DE RESTAURACIÓN.
8	CAPACITAR, ASESORAR Y ASISTIR A LAS DIFERENTES SECCIONES EN LA ORGANIZACIÓN DE LOS DATOS
9	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-6.- Actividades del Analista de Datos.

SUPERVISOR DE INFRAESTRUCTURA DE COMUNICACIONES

CARGO	
SUPERVISOR DE INFRAESTRUCTURA DE COMUNICACIONES	
MISIÓN	
COORDINAR LAS ACTIVIDADES DE LA SECCIÓN, IDENTIFICAR Y DAR SOLUCIÓN A LAS NECESIDADES DE COMUNICACIÓN E INFORMACIÓN QUE PETROPRODUCCIÓN PRESENTE. ASEGURANDO LA DISPONIBILIDAD, Y CONFIABILIDAD DEL SERVICIO.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	DEFINIR Y VELAR POR EL CUMPLIMIENTO DE LOS ÍNDICES DE GESTIÓN PARA LA SECCIÓN.
2	ESTUDIAR EL MERCADO DE INFRAESTRUCTURA EN NUEVAS TECNOLOGÍAS QUE PUEDAN SER IMPLANTADAS EN PETROPRODUCCIÓN.
3	ANALIZAR LAS NECESIDADES DE INFRAESTRUCTURA DE LOS DIFERENTES DEPARTAMENTOS DE LA EMPRESA Y PROPONER SOLUCIONES PARA MEJORAR LA SITUACIÓN EVIDENCIADA.
4	REDACTAR, CUMPLIR Y HACER CUMPLIR PROTOCOLOS, NORMATIVAS Y PROCEDIMIENTOS DE LA SECCIÓN.
5	ESTABLECER, EVALUAR Y EJECUTAR LAS PRUEBAS A REALIZARSE PARA DETECTAR POSIBLES PROBLEMAS DE FUNCIONAMIENTO EN INFRAESTRUCTURA
6	CUMPLIR Y HACER CUMPLIR LAS POLÍTICAS DE BUEN USO DE LA INFRAESTRUCTURA

7	DESIGNAR Y SUPERVISAR LA ELABORACIÓN DE ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE INFRAESTRUCTURA Y LA ELABORACIÓN DE INFORMES DE JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.
8	PLANIFICAR, GESTIONAR Y CONTROLAR PROYECTOS DE LA SECCIÓN EN COORDINACIÓN CON LAS OTRAS SECCIONES.
9	IMPLANTAR LOS PLANES DE SEGURIDAD Y CONTINGENCIA EN INFRAESTRUCTURA.
10	COORDINAR CON LAS DEMÁS SECCIONES LA DISPONIBILIDAD DE INFRAESTRUCTURA.
11	MANTENER ACTUALIZADO EL INVENTARIO DE EQUIPOS DE INFRAESTRUCTURA.
12	ELABORAR PLANES DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LA INFRAESTRUCTURA.
13	ELABORAR, ACORDAR E INFORMAR A LA COORDINACIÓN AVANCES EN EL PLAN DE LA SECCIÓN DE INFRAESTRUCTURA (INVERSIONES, CRONOGRAMAS, PROYECTOS, PRESUPUESTOS, ETC).
14	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-7.- Actividades del Supervisor de Infraestructura de Comunicaciones.

ANALISTA DE INFRAESTRUCTURA DE COMUNICACIONES

CARGO	
ANALISTA DE INFRAESTRUCTURA DE COMUNICACIONES	
MISIÓN	
DISEÑAR E IMPLEMENTAR REDES DE INFORMACIÓN Y COMUNICACIONES, BASÁNDOSE EN LAS NECESIDADES OPERATIVAS DE PETROPRODUCCIÓN.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	PREPARAR ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE INFRAESTRUCTURA, ELABORAR INFORMES DE JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.
2	IMPLEMENTAR MEJORES PRÁCTICAS EN INFRAESTRUCTURA COMO ITIL, COBIT.
3	BRINDAR SOPORTE DE NIVEL 2 A LA INFRAESTRUCTURA.
4	ANALIZAR Y ESPECIFICAR EL ALCANCE Y FACTIBILIDAD DE DESARROLLO E IMPLEMENTACIÓN DE NUEVA INFRAESTRUCTURA UTILIZANDO LAS TÉCNICAS, HERRAMIENTAS Y MÉTODOS ADECUADOS.
5	IMPLANTAR Y DOCUMENTAR SOLUCIONES DE INFRAESTRUCTURA.
6	EJECUTAR PLANES DE SEGURIDAD Y CONTINGENCIA EN LA INFRAESTRUCTURA.
7	DISEÑAR Y EJECUTAR SISTEMAS DE PRUEBAS PARA DETECTAR LOS PROBLEMAS DE FUNCIONAMIENTO DE LA INFRAESTRUCTURA Y ANALIZAR RESULTADOS.
8	ADMINISTRAR Y OPTIMIZAR LA INFRAESTRUCTURA.
9	EJECUTAR PLANES DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LA INFRAESTRUCTURA.
10	GARANTIZAR LA DISPONIBILIDAD Y CONFIABILIDAD DE LOS SERVICIOS DE INFRAESTRUCTURA.
11	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-8.- Actividades del Analista de Infraestructura de Comunicaciones.

ASISTENTE DE INFRAESTRUCTURA DE COMUNICACIONES

CARGO	
ASISTENTE DE INFRAESTRUCTURA DE COMUNICACIONES	
MISIÓN	
REALIZAR LA EJECUCIÓN OPERATIVA (INSTALACIÓN Y MANTENIMIENTO) Y PUESTA A PUNTO DE LAS REDES DE INFORMACIÓN Y COMUNICACIONES DE PETROPRODUCCIÓN.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	EJECUTAR PLANES DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LA INFRAESTRUCTURA
2	DAR SOPORTE TÉCNICO DE TERCER NIVEL A USUARIOS FINALES EN LO REFERENTE A INFRAESTRUCTURA.
3	IMPLANTAR LAS DIFERENTES SOLUCIONES DE INFRAESTRUCTURA.
4	LLEVAR EL CONTROL DE LAS INCIDENCIAS (MONITOREAR) LOS DIFERENTES EQUIPOS Y REPORTAR A SU SUPERIOR.
5	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE.

Tabla C-9.- Actividades del Asistente de Infraestructura de Comunicaciones.

SUPERVISOR DE SEGURIDAD TECNOLÓGICA

CARGO	
SUPERVISOR DE SEGURIDAD TECNOLÓGICA	
MISIÓN	
COORDINAR LAS ACTIVIDADES DE LA SECCIÓN, DISEÑAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN Y APLICACIONES Y PLANES DE CONTINGENCIA PARA EL ÁREA INFORMÁTICA.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	DEFINIR Y VELAR POR EL CUMPLIMIENTO DE LOS ÍNDICES DE GESTIÓN PARA LA SECCIÓN
2	ELABORAR, ACORDAR E INFORMAR A LA COORDINACIÓN AVANCES EN EL PLAN DE SEGURIDAD DE TECNOLOGÍA (INVERSIONES, CRONOGRAMAS, PROYECTOS, PRESUPUESTOS, ETC).
3	REDACTAR, CUMPLIR Y HACER CUMPLIR PROTOCOLOS, NORMATIVAS Y PROCEDIMIENTOS DE LA SECCIÓN.
4	DESIGNAR Y SUPERVISAR LA ELABORACIÓN DE ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE HERRAMIENTAS PARA SEGURIDAD TECNOLÓGICA Y LA ELABORACIÓN DE INFORMES DE JUSTIFICACIÓN TÉCNICA Y ECONÓMICA.
5	ESTUDIAR Y ESTABLECER LAS PRUEBAS A REALIZARSE PARA DETECTAR POSIBLES FALLAS DE SEGURIDAD TECNOLÓGICA; PROPONER ACCIONES PARA CORREGIRLAS EN COORDINACIÓN CON LAS ÁREAS INVOLUCRADAS.
6	ESTUDIAR EL MERCADO INFORMÁTICO EN REFERENCIA A NUEVAS HERRAMIENTAS DE SEGURIDAD QUE PUEDAN SER IMPLANTADAS EN PETROPRODUCCIÓN
7	APROBAR INFORMES DE ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD TECNOLÓGICA.
8	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-10.- Actividades del Supervisor de Seguridad Tecnológica.

ANALISTA DE SEGURIDAD TECNOLÓGICA

CARGO	
ANALISTA DE SEGURIDAD TECNOLÓGICA	
MISIÓN	
IMPLANTAR Y EJECUTAR LAS POLÍTICAS Y SISTEMAS DE SEGURIDAD DE INFORMACIÓN Y APLICACIONES.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	IMPLEMENTAR TÉCNICAS Y PROCEDIMIENTOS INFORMÁTICOS EN SU ÁMBITO DE ACCIÓN.
2	BRINDAR SOPORTE EN ASPECTOS DE SEGURIDAD TECNOLÓGICA A LAS DIFERENTES ÁREAS DE PETROPRODUCCIÓN.
3	ELABORAR ESPECIFICACIONES TÉCNICAS, PRESUPUESTOS PARA EL MANTENIMIENTO O ADQUISICIÓN DE HERRAMIENTAS PARA SEGURIDAD TECNOLÓGICA.
4	REALIZAR PRUEBAS PARA DETECTAR POSIBLES FALLAS DE SEGURIDAD TECNOLÓGICA, EVALUAR LOS INCIDENTES REPORTADOS, PREPARAR INFORME DE RESULTADOS.
5	ANALIZAR LOS REQUERIMIENTOS DE SEGURIDAD TECNOLÓGICA Y PREPARAR EL INFORME DE RESULTADOS RESPECTIVO.
6	IMPLANTAR Y ADMINISTRAR LAS HERRAMIENTAS PARA SEGURIDAD TECNOLÓGICA EN SU ÁMBITO DE ACCIÓN (FIREWALLS, SISTEMAS DE DETECCIÓN DE INTRUSOS, ETC). ELABORAR LA DOCUMENTACIÓN INHERENTE.
7	COORDINAR LA EJECUCIÓN DE LOS PLANES DE CONTINGENCIA TECNOLÓGICOS CON LAS DIFERENTES SECCIONES.
8	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE, PARTICIPAR EN REUNIONES, ETC.

Tabla C-11.- Actividades del Analista de Seguridad Tecnológica.

SUPERVISOR DE SOPORTE AL USUARIO

CARGO	
SUPERVISOR DE SOPORTE AL USUARIO	
MISIÓN	
COORDINAR LAS ACTIVIDADES DE LA SECCIÓN Y REQUERIMIENTOS DE ATENCIÓN CON LAS DEMÁS SECCIONES DE TIC, SUPERVISAR LA ACTUALIZACIÓN DE LA BASE DEL CONOCIMIENTO GENERADA POR LOS REPORTES DE INCIDENTES DE SOPORTE A USUARIOS.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	DEFINIR Y VELAR POR EL CUMPLIMIENTO DE LOS ÍNDICES DE GESTIÓN PARA LA SECCIÓN.
2	REDACTAR, CUMPLIR Y HACER CUMPLIR PROTOCOLOS, NORMATIVAS Y PROCEDIMIENTOS DE LA SECCIÓN.
3	IMPLANTAR LOS PLANES DE SEGURIDAD Y CONTINGENCIA DE LA SECCIÓN.
4	DEFINIR NIVELES DE ACUERDO DE SERVICIO (SLA) PARA LOS DIFERENTES REPORTES DE INCIDENTES.
5	SUPERVISAR LA ACTUALIZACIÓN DE LA BASE DEL CONOCIMIENTO GENERADA POR LOS REPORTES DE INCIDENTES.
6	COORDINAR CON LAS DEMÁS SECCIONES LOS REQUERIMIENTOS DE ATENCIÓN.
7	INFORMAR A LA SECCIÓN DE INFRAESTRUCTURA LAS NOVEDADES EVIDENCIADAS (TRASLADO DE EQUIPOS, EQUIPOS SIN INVENTARIAR, ETC).
8	ELABORAR, ACORDAR E INFORMAR A LA COORDINACIÓN EL DESEMPEÑO DE LA SECCIÓN.
9	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE: ATENDER TRÁMITES Y COMUNICACIONES DE DIFERENTE ÍNDOLE; PARTICIPAR EN REUNIONES.

Tabla C-12.- Actividades del Supervisor de Soporte al Usuario.

ASISTENTE DE SOPORTE AL USUARIO

CARGO	
ASISTENTE DE SOPORTE AL USUARIO	
MISIÓN	
ATENDER LOS INCIDENTES REPORTADOS POR LOS USUARIOS DE PETROPRODUCCIÓN SEGÚN ACUERDO DE NIVEL DE SERVICIO ESTABLECIDO. REGISTRAR LOS INCIDENTES REPORTADOS Y SUS SOLUCIONES PARA CREACIÓN DE LA BASE DE CONOCIMIENTO.	
ACTIVIDADES	
NÚMERO	ACTIVIDADES
1	CUMPLIR CON LOS ÍNDICES DE GESTIÓN Y NORMAS DE SEGURIDAD PARA LA SECCIÓN
2	ATENDER LOS INCIDENTES REPORTADOS POR LOS USUARIOS
3	MONITOREAR EL ESTADO OPERATIVO DE EQUIPOS TECNOLÓGICOS DE OFICINA.
4	REGISTRAR LOS INCIDENTES REPORTADOS Y SUS SOLUCIONES PARA LA CREACIÓN DE LA BASE DE CONOCIMIENTO.
5	INSTALAR, CONFIGURAR Y ACTUALIZAR LAS APLICACIONES DE OFIMÁTICA Y COMPUTADORES PERSONALES.
6	INSTALAR, CONFIGURAR Y DAR SOPORTE DE PERIFÉRICOS Y DISPOSITIVOS TECNOLÓGICOS BÁSICOS (PROYECTORES, IMPRESORAS, RADIOS MÓVILES, TELÉFONOS, ETC)
7	CUMPLIR CON OTRAS FUNCIONES Y RESPONSABILIDADES COMPATIBLES CON SU ACTIVIDAD, QUE LE SEAN ASIGNADAS POR LA AUTORIDAD COMPETENTE.

Tabla C-13.- Actividades del Asistente de Soporte Al Usuario.

ANEXO D

GESTIÓN DE CONFIGURACIÓN

GESTIÓN DE CONFIGURACIÓN

CONFIGURACION DEL AGENTE SNMP

Para el correcto funcionamiento de SNMP v2 primero se debe definir ciertos parámetros para lo cual se especificaron los siguientes:

- COMUNIDAD que permite Lectura y Escritura: **sec_tic_ppr**.
- COMUNIDAD que permite solo Lectura: **sec_tic_public**.
- GRUPO para Lectura y Escritura: **nocrw**.
- GRUPO para solo lectura: **nocro.**
- MIBs permitidas para ser Vistas: **MIB-2, cisco, snmp v2**.

CONFIGURACION DEL AGENTE SNMP WINDOWS 2003 SERVER.

En Windows XP para poder configurar SNMP primeramente se debe instalar el servicio, para lo cual se realiza el siguiente procedimiento:

1. Hacer clic en Inicio, seleccionar Panel de control, Herramientas administrativas y, a continuación clic en Agregar y Quitar programas.

Figura D-1 .- Agregar servicio SNMP en Windows Server 2003 paso 1.

2. Una vez dentro del asistente de configuración se da clic en la pestaña Agregar o quitar componentes de Windows, luego se busca y se selecciona la opción herramientas de administración y supervisión, luego clic en la pestaña detalles.

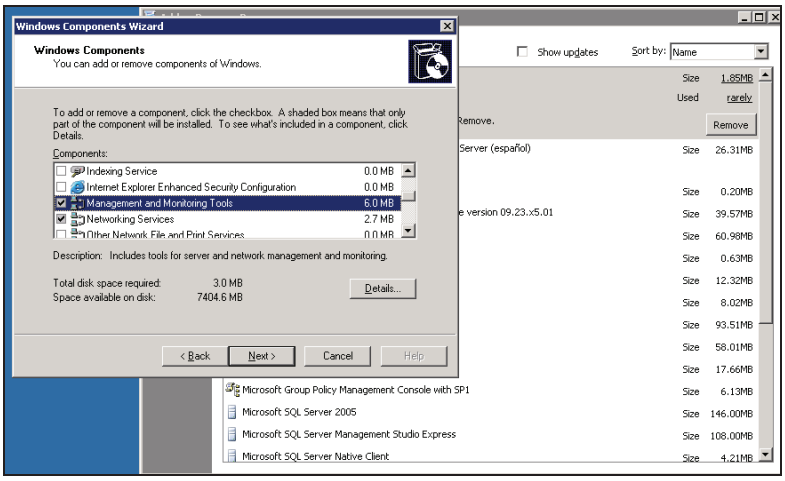


Figura D-2.- Agregar servicio SNMP en Windows 2003 Server paso 2.

3. Aparecen dentro del asistente varias herramientas de administración y supervisión. Se debe seleccionar el protocolo simple de administración de redes (SNMP) y por ultimo dar clic en aceptar.

   Nota: el sistema pedirá un Cd de instalación para poder copiar en el disco duro los paquetes necesarios para que el protocolo SNMP funcione.

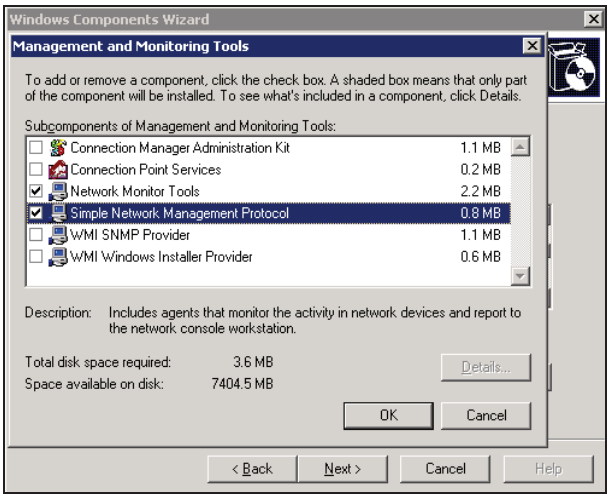


Figura D-3.- Agregar servicio SNMP en Windows 2003 Server paso 3.

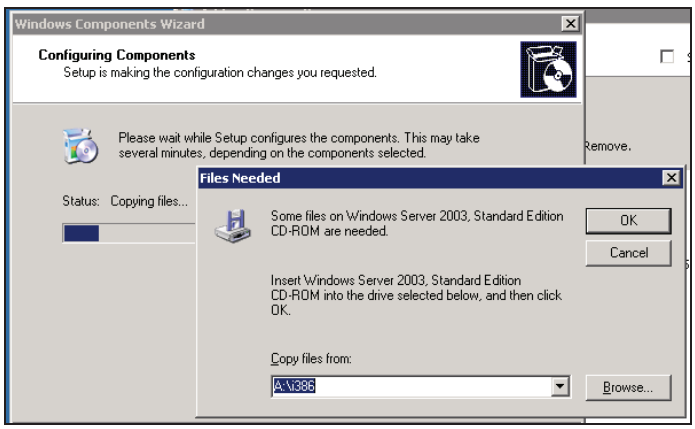


Figura D-4.- Agregar servicio SNMP en Windows 2003 Server paso 3 continuación.

4. Se finaliza la instalación y ya se puede configurar el agente, para lo cual se ingresa en Herramientas Administrativas en el panel de control, y se entra en servicios.

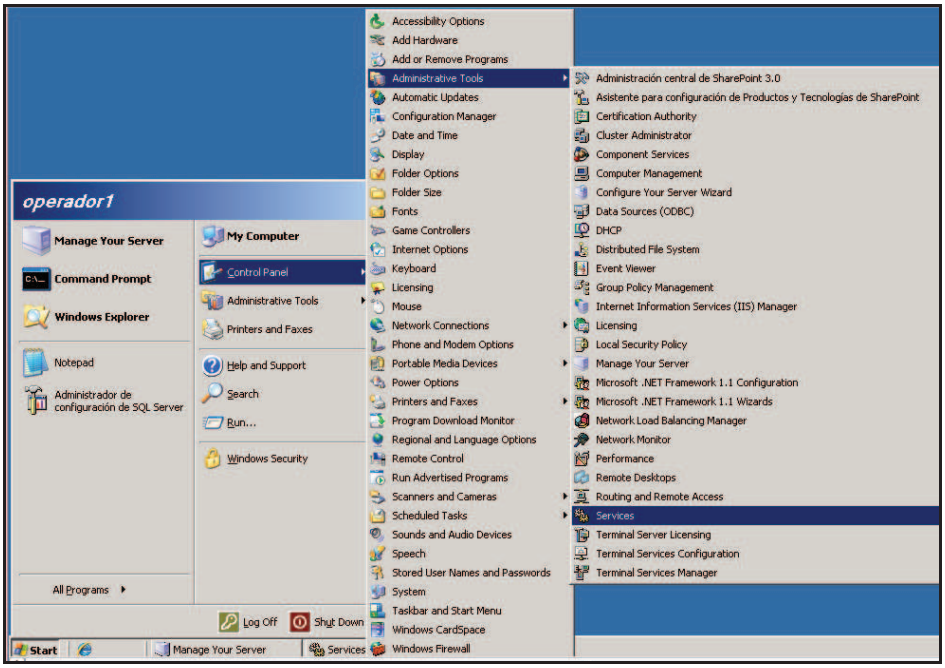


Figura D-5.-Ingreso a configurar servicio SNMP en Windows 2003 Server paso 1.

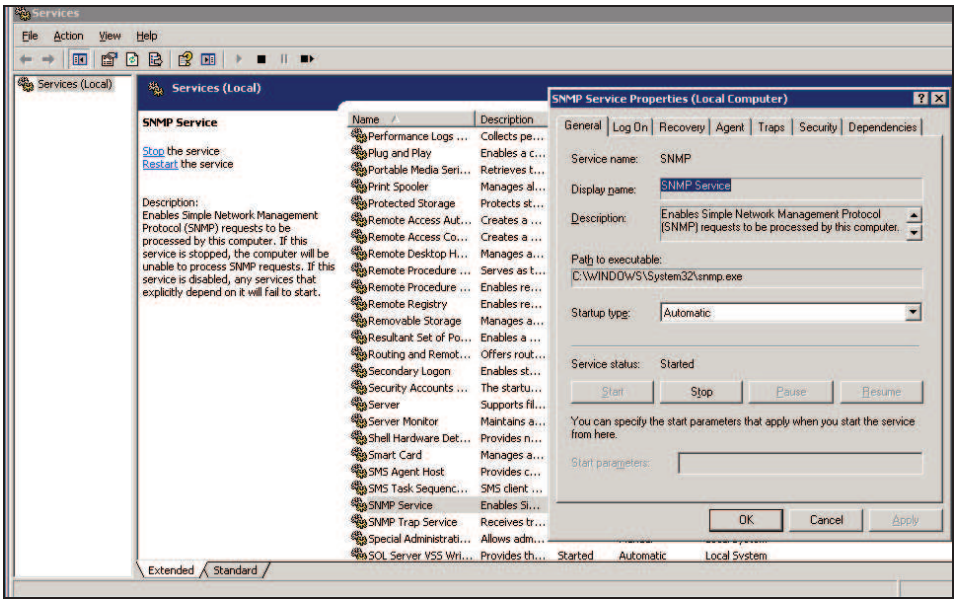


Figura D-6.- Ingreso a configurar servicio SNMP en Windows 2003 Server paso 2.

5. Se selecciona con doble clic en Servicio SNMP en el panel de la derecha. En la pantalla propiedades de SNMP, seleccionar la pestaña capturas y agregamos el Nombre de la comunidad "**sec_tic_public**" y el destino de la captura que será la IP del servidor "172.16.X.X"

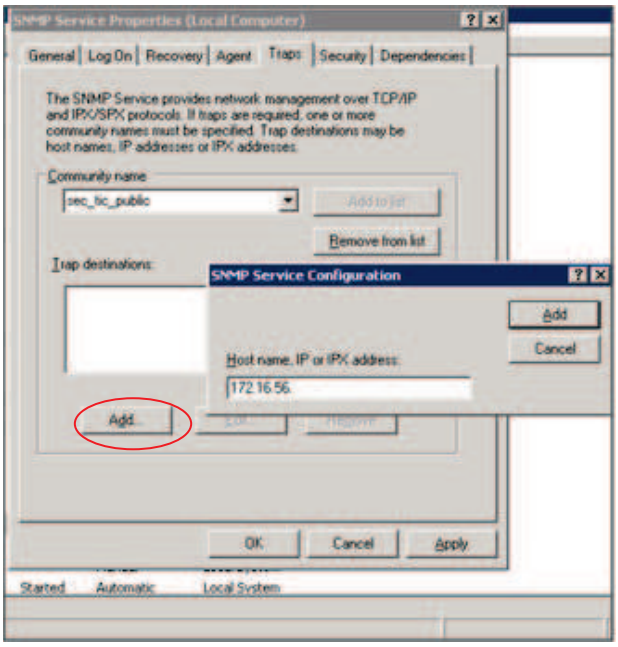


Figura D-7.- Configuración de nombre de comunidad y destino de capturas.

6. En la pestaña Agente se escribe el nombre del usuario o administrador del equipo en el cuadro Contacto y después se escribe la ubicación física del equipo o contacto en el cuadro Ubicación (Estos comentarios se tratan como texto y son opcionales).
7. En la pestaña Servicio, hacer clic para activar las casillas de verificación situadas junto a los servicios proporcionados por el equipo. Las opciones de servicio son las siguientes:

    - Físico: especifica si el equipo administra dispositivos físicos como una partición de disco duro.
    - Aplicaciones: especifica si el equipo utiliza programas que envían datos a través de TCP/IP.
    - Vínculo de datos y subred: especifica si este equipo administra una subred o un vínculo de datos TCP/IP, como un puente.
    - Internet: especifica si este equipo actúa como una puerta de enlace IP (enrutador).
    - De un extremo a otro: especifica si este equipo actúa como un host IP.

8. Aceptar.

En la pestaña seguridad están las siguientes opciones:

- **Enviar captura de autenticación:** Cuando el agente recibe una solicitud que no contiene un nombre de comunidad válido o bien el host emisor del mensaje no está en la lista de los permitidos, el agente puede enviar un mensaje de captura (alarma) a las NMS con el mensaje del fallo de la autenticación.

- **Nombres de comunidad aceptados:** Es necesario configurar al menos un nombre de comunidad predeterminado. Generalmente se usa el nombre public, en caso de PPR se

utilizará ***sec_tic_public y sec_tic_ppr,*** se puede cambiar y añadir otros. Se recomienda el cambio de public a otro nombre pues éste no es seguro. Únicamente se procesarán los mensajes provenientes de una comunidad válida.

- **Derechos de comunidad:** Se pueden configurar con que permisos se procesan las solicitudes de los miembros de determinadas comunidades.

- **Aceptar paquetes SNMP de cualquier host:** Cuando esta opción está habilitada nunca se descartan paquetes SNMP en base a la dirección o nombre del host fuente

- **Aceptar paquetes SNMP de estos host:** Cuando esta opción está habilitada sólo se aceptan paquetes de los host de la lista de los permitidos. Esto añade un nivel de seguridad más alto que el nombre de la comunidad.

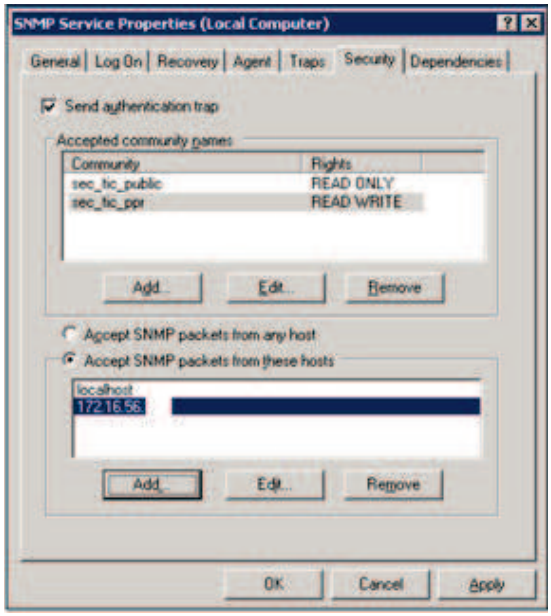


Figura D-8.- Configuración de la comunidad de SNMP en Windows 2003 Server.

Finalmente se reinicia el servicio para que los cambios surtan efecto, para lo cual se da clic derecho en "servicio SNMP" y se selecciona **reiniciar**. Para los sistemas operativos Windows Vista y Windows 7 se tiene el mismo procedimiento que en Windows XP o server.

CONFIGURACION DEL AGENTE EN LINUX.

Snmpd es el demonio del servicio de snmp para que corra en sistema operativo Linux; Primeramente para configurar el servidor snmp se debe descargar los repositorios necesarios para lo cual se ejecuta lo siguiente:

#apt-get install snmpd. *Ó* **#apt-get install net-snmp**

Dependiendo la distribucion se debera utlizar el comando respectivo para gestión de repositorios.

Creación de la comunidad:

Para agregar una comunidad se debe editar el archivo **/etc/snmp/snmpd.conf** y buscar la línea **sec.name source**, a línea siguiente se debe añadir la siguiente sintaxis:
Com2sec group network community

Para PPR se tiene:

com2sec nocro 172.16.52.X sec_tic_public

Donde **nocro** es el nombre del grupo para lectura, **172.16.56.X** es el identificador del host que puede monitorear, en este caso del JFFNMS, se puede poner el identificador de la red que va a ser monitoreada, y **sec_tic_public** es el nombre de la comunidad, este nombre será cambiado por personal de Petroproducción para brindar mayor seguridad.

Para las demás redes de PPR se añade las siguientes sintaxis:

com2sec nocrw localhost sec_tic_ppr
com2sec nocro 172.16.52.X sec_tic_public

El siguiente paso es buscar la línea comentada con contiene "**sec.model sec.name",** documentar lo que este ahí y agregar:

group MyROGroup v1 nocro
group MyROGroup v2c nocro
group MyROGroup usm nocro

group MyRWGroup v1 nocrw
group MyRWGroup v2c nocrw
group MyRWGroup usm nocrw

Creación de las vistas para tener acceso a la información del agente, permite obtener la información del agente.

incl/excl subtree mask
view all included .1 80
view system included .iso.org.dod.internet.mgmt.mib-2.system
view snmpV2 included .iso.org.dod.internet.snmpV2

En el mismo archive se añade la información del syslocation y syscontact del agente; Se guardan los cambios del archivo. El siguiente paso es la configuración del archivo **/etc/default/snmpd**, se debe buscar la línea que dice **SNMPDOPTS** y se borra la dirección de loopback (172.0.0.1) para que pueda monitorear el resto de redes como se muestra en la Figura **D-9**, y setear en YES el TRAPDRUN para inicializar el demonio de snmptrap, Finalmente se guarda los cambios.

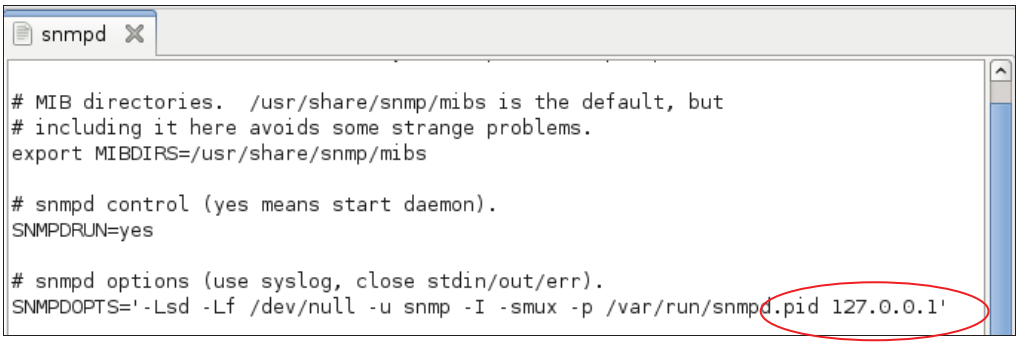


Figura D-9.- Configuracion archivo /etc/default/snmpd.

Debe quedar de la siguiente manera:

```
# snmpd options (use syslog, close stdin/out/err).
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid'
```

Con esto queda configurado el servicio, entonces se procede a iniciar o reiniciar el mismo para que los cambios surtan efecto con los siguientes comandos:

/etc/init.d/snmpd/ start ó /etc/init.d/snmpd/ restart

CONFIGURACIÓN DE SNMP EN UN ROUTER y SWITCH CISCO.

Para habilitar SNMP en un Router o Switch Cisco, se debe ingresar en modo de configuración global.

```
Router> enable
Router# configure terminal
Router(config)#
```

Posteriormente se ejecuta los siguientes comandos habilitando y configurando la generación de traps SNMP sobre una base global. Y se configuran las comunidades.

```
Router(config)# snmp-server enable traps
```

Para definir una comunidad se utiliza la siguiente sintaxis:

```
Router(config)# snmp-server community nombre_comunidad [view nombre_vista]
[ro|rw] [número_de_acl]
```

Por defecto, si no se especifican los parámetros opcionales, se facilita acceso de sólo lectura a toda la MIB (vista por defecto *everything*) y a todos los hosts. El número de acl es cuando se configuran listas de acceso para tener un mayor control en la administración del equipo.

```
Router(config)# snmp-server community sec_tic_ppr rw
Router(config)# snmp-server community sec_tic_public ro
```

Los comandos anteriores agregan la comunidad (sec_tic_ppr) con permisos de lectura y escritura (read write), y la comunidad “sec_tic_public” con permisos de solo lectura (read only).

Con el comando: **`Router# show running-config | include snmp`** se puede apreciar la configuración que tiene el dispositivo filtrando la parte de SNMP.

CREAR UN REGISTRO DE VISTA SNMP

Para su creación los comandos a utilizar requieren como argumento una *vista*. Éstas se emplean para delimitar los objetos de la MIB accesibles para un gestor SNMP. Se puede usar una vista predefinida, o bien, crear nuevas vistas.

Las vistas predefinidas son dos:

everything, que abarca toda la MIB y, **restricted**, que incluye sólo los grupos system, snmpStats y snmpParties.

Para crear o modificar un registro de vista SNMP se ejecuta:

```
Router(config)# snmp-server view nombre_vista arbol_OID {included |
excluded}
```

Se puede introducir este comando varias veces para el mismo registro de vista. Lo que se hace es añadir o eliminar elementos, dependiendo la especificación *included o excluded*. Si un identificador de objeto se incluye en dos o más comandos, es el más reciente es el que tiene efecto. El parámetro "**arbol_OID**" es el identificador de objeto del nodo raíz dentro del árbol de nombres al que va a afectar el comando.

Las vistas a configurarse en Routers y Switches de Petroproducción son:

```
Router(config)# snmp-server view vista_Mib mib-2 included

Router(config)# snmp-server view vista_Cisco cisco included

Router(config)# snmp-server view vista_snmp snmp included
```

NOTIFICACIONES SNMP

Para configurar el envío de interrupciones o informes a un host o a un servidor de logs. Cabe señalar que para emitir notificaciones en forma de informes, el dispositivo debe contar con un gestor proxy SNMP. Este gestor no está disponible en todas las imágenes de IOS, sino sólo en las versiones PLUS.

En primer lugar, hay que especificar a quién irán dirigidas las notificaciones para lo cual se utiliza la siguiente sintaxis:

```
Router(config)# snmp-server host id-host [traps|informs] [version {1 | 2c |
3 [auth | noauth | priv]} ] nombre_comunidad [udp-port numero_puerto]
[tipo_notificación]
```

Configuración para PPR:

```
Router(config)# snmp-server host 172.16.X.X  traps version  2c sec_tic_ppr

Router(config)# snmp-server host 172.16.X.X  traps version  2c
sec_tic_public
```

```
Router(config)# Logging on
Router(config)# Logging 172.16.56.XXX
```

Así, se especifica el host por su dirección IP, y de forma opcional, si se le van a enviar informes o traps, la versión del protocolo a emplear, para PPR se empleará la versión 2c (en el caso de querer configurar la versión 3, hay que indicar el nivel de seguridad), el número de puerto al que se dirigirán las notificaciones (162 de UDP), y el tipo de notificación (todas).
Existen diversos tipos de notificaciones. Se puede especificar más de un tipo a la vez. También es posible introducir varios comandos snmp-server host para dirigir distintos tipos de notificación a varios hosts.

También se pueden cambiar el interfaz por defecto por donde se enviarán las notificaciones o traps, para lo cual se utiliza la siguiente sentencia:

```
Router(config)# snmp-server trap-source interface
```

Información de contacto y situación del agente SNMP.

Con los siguientes comandos, se pueden establecer la información de contacto, y situación del agente SNMP, de manera que puedan ser accedidos a través del fichero de Configuración:

```
Router(config)# snmp-server contact descripción

Router(config)# snmp-server contact adminjffnms

Router(config)# snmp-server location descripción
```

Ejemplo de configuración del Router principal del edificio Villafuerte.

```
Router(config)# snmp-server location "El Router está en la PB de edificio
Villafuerte"
```

Con todo esto el Router o Switch queda configurado, operativo y listo para ser monitoreado por la consola de Administración.

CONFIGURACIÓN SNMP EN EL SISTEMA OS/400

Los siguientes comandos inician y detienen el agente SNMP. El subagente OS/400 empieza y detiene paralelamente con el agente.

STRTCPSVR (*SNMP) – Inicia el agente TCP/IP SNMP
ENDTCPSVR (*SNMP) – Termina el agente TCP/IP SNMP

Los siguientes comandos cambian la configuración SNMP:

Añadir la comunidad para SNMP - **ADDCOMSNMP**
Configurar TCP/IP para SNMP - **CFGTCPSNMP**
Cambio de comunidad para SNMP - **CHGCOMSNMP**
Cambio de atributos SNMP - **CHGSNMPA**
Eliminar la comunidad para SNMP - **RMVCOMSNMP**

CONFIGURACIÓN SERVIDORES ISERIES (OS/400)

Se la realiza mediante el ingreso de comandos propios de estos servidores:
Cambio de configuración del servicio SNMP: **CFGTCPSNMP**

Comando	Descripción	Opciones
COM	Nombre de Comunidad	Valor carácter
ASCIICOM	Determina que el nombre de comunidad sea traducido a ASCII antes de ser comparado con la petición SNMP del administrador.	*YES, *NO
INTNETADR	Dirección IP de la estación NMS	Single values: *ANY Otros valores (mayors a 300 repeticiones): valor character
OBJACC	Object Access	*SNMPATR, *READ, *WRITE, *NONE
LOGSET	Log set requests	*SNMPATR, *YES, *NO
LOGGET	Log get requests	*SNMPATR, *YES, *NO
SYSLOC	Ubicación del sistema	Valores del tipo carácter
SYSCONTACT	Administrador del sistema	Valores del tipo carácter

Tabla D-1.- Parámetros configuración sistemas AS/400

La siguiente figura es un ejemplo de pantalla al momento de cambiar las configuraciones del agente SNMP.

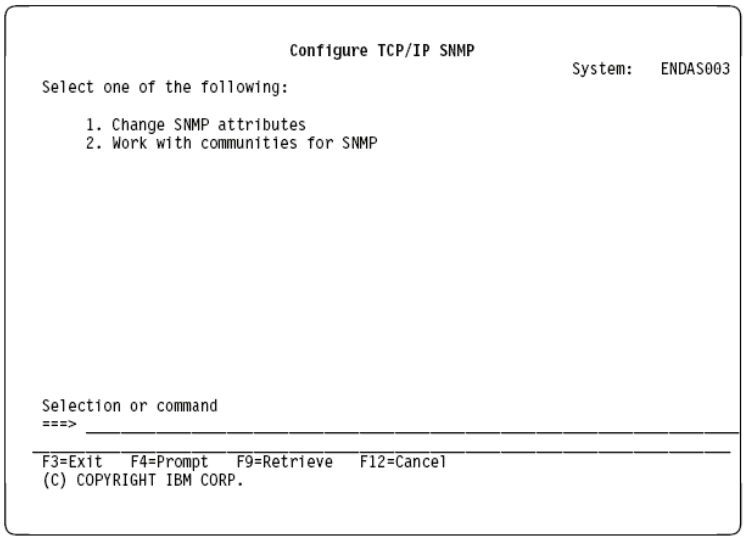


Figura D-10.- Pantalla para cambiar configuraciones en AS/400

PARÁMETROS CONFIGURADOS

community name sec_tic_public
ASCIICOM *YES
INTNETADR 172.16.56.197
OBJACC *READ
LOGSET *NO
LOGGET *NO

Atributos

system contact Administrador
system location Edificio Villafuerte
send authentication traps *YES
autostart *YES
object access *READ
log set requests *NO
log get requests *NO
log traps *NO
trap managers *NONE

CONFIGURACION DE LA CONSOLA DE ADMINISTRACION

Instalación JFFNMS 0.8.3 en Debian 5.0.4

Instalación de dependencias necesarias de la herramienta, para lo cual primeramente se deben colocar los repositorios o fuentes a utilizarse en el archivo /etc/apt/sources.list, Ser recomienda que antes de editar el archivo original respaldarlo con el comando:

cp /etc/apt/sources.list /etc/apt/sources.list.backup

Los repositorios se colocan añadiendo las siguientes líneas en el archivo:
deb http://mirrors.kernel.org/debian stable main
deb http://security.debian.org/ stable/updates main

Las dependencias que requiere ser instaladas son:
Apache2, apache2-common, apache2-utils, mysql-client, mysql-server, rrdtool, php5, php5-gd, php5-snmp, php5-mysql, php5-cli, php5-cgi, php5-odbc, libapache2-mod-php5, snmp, snmpd, tftpd, ttf-bitstream-vera, fontconfig, x-ttcidfont-conf, nmap, fping, tmpreaper, smokeping, dbconfig-common, smsclient, debconf, graphviz, ntp, adduser y cron.

Se realiza con la sentencia **#aptitude install *dependencia*.**
Se actualizan las dependencias con **#aptitude update**

Una vez instalado todas las dependencias se ejecuta el comando **#aptitude install jffnms** para que se instale la herramienta de monitoreo.

Se Crea la carpeta opt para descargar la herramienta mkdir /opt
Descarar el archivo tar.gz desde la siguiente direccion:
http://sourceforge.net/projects/jffnms/files/jffnms%20RC/jffnms-0.8.5rc1.tgz/download
dentro de la carpeta /opt.

Se descomprime el paquete con los siguientes comandos:

cd /opt
Tar xzvf jffnms-0.8.5rc1.gz
mv jffnms-0.8.5rc1.gz /opt/jffnms

Se setean los permisos ejecutando los siguientes comandos:

chown -R jffnms:jffnms /opt/jffnms
chmod 770 /opt/jffnms
chmod -R ug+rw /opt/jffnms

Se añade el grupo y usuario de la aplicación con los siguientes comandos:

groupadd jffnms
useradd -g jffnms -d /opt/jffnms -s /bin/false -c 'jffnms' jffnms
usermod -G jffnms www-data

Con todo instalado se ejecuta el comando **#aptitude update** para actualizar todo lo instalado.

Configuración de JFFNMS y sus dependencias antes de ejecución del programa.

Sección Analizadores de Red.

1.- Configurar **Nmap**: Esto es para explorar los puertos de los agentes a ser monitoreados.
Se debe ejecutar las siguientes sentencias para dar permisos a la carpeta donde está el servicio nmap.

#chmod +s /usr/bin/nmap
#chmod a+x /usr/bin/nmap
 # ls -l /usr/bin/nmap

Se obtendrá lo siguiente: -rwsr-sr-x 1 root root 506564 2006-08-01 11:08 /usr/bin/nmap, para verificar los permisos correctos.

2.- Configurar **Fping**: Permite descubrir los hosts activos en la red, se dan los permisos necesarios con:

#chmod +s /usr/bin/fping
#chmod a+x /usr/bin/fping

Se Verifica con el comando: *# ls -l /usr/bin/fping* obteniendo el siguiente resultado:
-rwsr-sr-x 1 root root 22508 2006-06-23 07:00 /usr/bin/fping

3.- Configuracion **MYSQL.**
Se setea el password en mysql con el comando para ingresar a la configuración de mysql:
mysql -u root -p
Enter password: ***rootpassword***
Se ejecutan las siguientes sentencias donde jffnms sera el password seteado
mysql> SET PASSWORD FOR root@localhost=PASSWORD('jffnms');
Query OK, 0 rows affected (0.00 sec)

Se procede a crear la base de datos "jffnms" y se asigna los privilegios necesarios dentro de la configuración de mysql.

mysql> mysql -u root -p
mysql> CREATE DATABASE jffnms;
mysql> GRANT ALL PRIVILEGES ON jffnms. TO jffnms@localhost IDENTIFIED BY 'jffnms';*
mysql> FLUSH PRIVILEGES;
mysql> quit

mysql -u jffnms -p jffnms < /opt/jffnms/docs/install/jffnms-0.8.5rc1.mysql

4.- Configuración para **PHP**
Se crea un respaldo del archivo con el comando:
 # cp /etc/php5/apache2/php.ini /etc/php5/apache2/php.ini.backup

Sobre esta ruta: */etc/php5/apache2/php.ini* setear los siguientes parametros

register_globals = On
register_argc_argv = On
error_reporting = E_ALL & ~E_NOTICE
allow_url_fopen = On
include_path = .:/usr/share/pear
short_open_tag = On

memory_limit = 128M

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
extension=mysql.so
extension=snmp.so
extension=gd.so
extension=odbc.so

Se modifica el php.ini de la ruta ***etc/php5/cgi/php.ini***

extension=mysql.so
extension=snmp.so
extension=odbc.so

Se modifica el php.ini de la ruta ***etc/php5/cli/php.ini***

extension=mysql.so
extension=gd.so
extension=odbc.so
extension=snmp.so

Setear el serverName en la ruta **/etc/apache2/apache2.conf**

ServerName 127.0.0.1

Configuración de SNMP.

Los archivos de configuración se encuentran en el directorio /etc/snmp los cuales deben ser respaldados con los comandos:

#cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.backup
#cp /etc/snmp/snmptrapd.conf /etc/snmp/snmptrapd.conf.backup

Snmpd/conf es el archivo de configuraciòn para el Agente SNMP y snmptrapd.conf es el archivo de configuraciòn para el demonio SNMP trap.

Se edita el archivo **/etc/snmp/snmpd.conf** y se cambia la configuración quedando la siguiente:

com2sec nocrw 172.16.56.XXX sec_tic_ppr
com2sec nocro 172.16.56.xxx sec_tic_public

Donde por ejemplo en la primera sentencia: **nocrw** es el nombre del grupo para lectura y escritura, **172.16.56.xxx** es el identificador de la red que va a ser monitoreada y **sec_tic_ppr** es el nombre de la comunidad, este nombre será cambiado por personal de Petroproducción para brindar mayor seguridad.

group MyROGroup v1 nocro
group MyROGroup v2c nocro
group MyROGroup usm nocro

group MyRWGroup v1 nocrw
group MyRWGroup v2c nocrw
group MyRWGroup usm nocrw

Creación de las vistas para tener acceso a la información del agente.

 # incl/excl subtree mask
view all included .1 80
view system included .iso.org.dod.internet.mgmt.mib-2.system

Permitir a los dos grupos de acceso los permisos de escritura a la vista creada.

 # context sec.model sec.level match read write notif
access MyROSystem "" any noauth exact system none none
access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all all none

Setear los parametros de snmp:

syslocation data-center Villafuerte
syscontact Root <jjfnms@localhost> (configure /etc/snmp/snmpd.local.conf)

En el archivo ***/etc/snmp/snmptrapd.conf*** incluir la sentencia:
traphandle default /opt/jffnms/engine/trap_receiver.sh para pasar los trap recibidos al demonio. En el archivo ***/etc/default/snmpd*** y setear en YES el TRAPDRUN para inicializar el demonio de snmptrap.

Se debe setear el crontab para los trabajos de backend del JFFNMS, se ejecutan lo siguiente:

#crontab -u jffnms /opt/jffnms/docs/unix/crontab
#crontab –u jffnms –e
#/etc/init.d/cron reload
#echo jffnms >> /etc/cron.allow

En el archivo ***/etc/apache2/sites-enabled/000-default*** se configura el apache2 colocando:

*NameVirtualHost **
*<VirtualHost *:80>*
*ServerAdmin **webmaster@localhost***
#DocumentRoot /var/www/
DocumentRoot /opt/jffnms/htdocs
ServerName 127.0.0.1
LimitRequestLine 20000
*</VirtualHost *>*

Finalmente se crea un Link simbólico para el servidor web. Se ejecuta:

ln -s /opt/jffnms/htdocs /var/www

Finalmente se reinician todos los servicios para poder correr la aplicación via web y proceder a configurar todo lo necesario para monitorear.

/etc/init.d/apache2 restart
/etc/init.d/snmpd restart
/etc/init.d/mysql restart

Con el comando ***#tail -f /var/log/syslog*** para revisar que todo este correcto.

CONFIGURACION VIA WEB

Para la configuración se ingresa el sistema colocando localhost en el browser o en forma remota con la dirección IP del servidor de administración y se desprende una página inicial donde se certificará en la pantalla del setup si todo cumple con lo especificado en la instalación previa con mensajes de OK a un costado de cada configuración, o con mensajes de error si falta alguna dependencia. En smsclient hay error pero es solo de escritura, este se soluciona cambiando el nombre por sms_client. Y hay error en Posgresql porque no se utilizara ya que está configurado con Mysql. (Ver Figura 4.2).

Se guarda la configuración una vez que todo este correcto, se reinicia el navegador y se vuelve a ingresar con el nombre del servidor o localhost en el browser. Aparece mensaje de bienvenida para ingresar al sistema.

Username: admin
Password: admin

Se ingresa al sistema listo para ser utilizado. Los agentes a ser monitoreados ya deben estar previamente configurado con todos sus parámetros del protocolo SNMP y este estar corriendo.

ANEXO E

SISTEMA OPERATIVO A UTILIZAR

SISTEMA OPERATIVO A UTILIZAR

Para el presente proyecto se decidió el uso de un sistema operativo de libre distribución, es así que se ha encaminado y promovido el uso de la plataforma Linux para su uso en un ambiente Servidor. Sin embargo en la actualidad existen varias opciones y distribuciones del sistema que se podrían implementar.

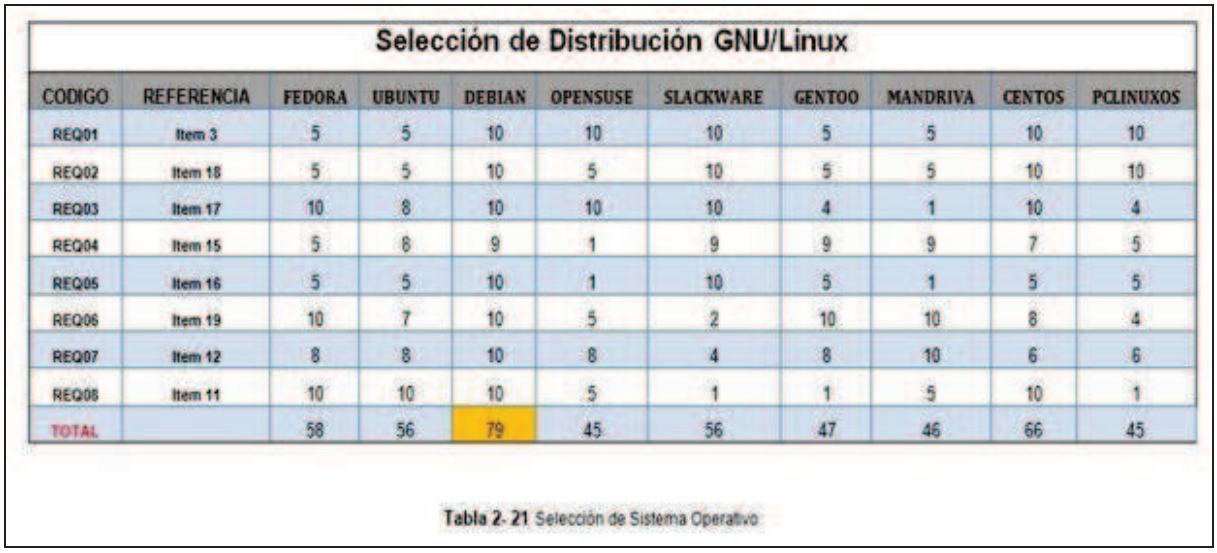
Para la selección del adecuado sistema para la consola de monitoreo que se desea implementar en Petroproducción se necesita una comparativa entre las principales distribuciones Linux. Con tal objetivo hacemos referencia a la Tesis realizada por Gladys Jiménez Y Carlos Pazmiño con tema: ***"Análisis, implementación y evaluación de un prototipo ruteador dual Ipv4/Ipv6 con soporte de QoS e IPsec sobre Linux, usando AHP para la selección del hardware e IEEE 830 para la selección del software".***

Donde se caracterizan y analizan diversas plataformas Linux en base a requerimientos de hardware, funcionalidad, entre otras dadas por sus autores y apreciadas en la siguiente tabla:

No	Ítem	Descripción
1	Software Libre	El sistema operativo deberá tener licencia GPL o una licencia similar sin costo.
2	Poseer una versión estable	El software no debe ser una versión de prueba ni versiones en desarrollo, es decir debe contar con versiones estables distribuidas públicamente.
3	Seguridad	Poseer un nivel de seguridad, que garantice un acceso restringido al núcleo de memoria, protección, detección y reordenamiento de desbordamiento de memoria.
4	Eficiencia	La velocidad del sistema de arranque debe ser lo más rápido posible, para obtener un tiempo de convergencia muy pequeño con el objetivo de mantener una red de comunicaciones eficiente.
5	Velocidad de Respuesta del Sistema	El sistema operativo debe tener una respuesta rápida a la transferencia de información y reenvío de paquetes.
6	Documentación y Ayuda	Tener una amplia y disponible documentación, de parte de los desarrolladores del sistema operativo como de la comunidad de Internet, para facilitar el aprendizaje y conocimiento.
7	Amplio número de paquetes	Disponer de los paquetes necesarios para la implementación de protocolos de enrutamiento, calidad de servicio e IPsec o sus dependencias, que estén incluidos en sus repositorios oficiales y tengan licencia GNU GPL.
Requisitos de interfaces externos		
	Interfaces de usuario	
8	Configurabilidad	El sistema operativo contará con facilidades para que los administradores puedan configurar todas las funcionalidades y funciones por medio de herramientas basadas en consola de texto.

Tabla E-1.- Requerimientos de plataforma Linux

Como resultado del Análisis se obtuvo que la Distribución **DEBIAN** el mejor puntaje entre nueve plataformas analizadas, los resultados se pueden observar en la siguiente figura:



Selección de Distribución GNU/Linux

CODIGO	REFERENCIA	FEDORA	UBUNTU	DEBIAN	OPENSUSE	SLACKWARE	GENTOO	MANDRIVA	CENTOS	PCLINUXOS
REQ01	Item 3	5	5	10	10	10	5	5	10	10
REQ02	Item 18	5	5	10	5	10	5	5	10	10
REQ03	Item 17	10	8	10	10	10	4	1	10	4
REQ04	Item 15	5	8	9	1	9	9	9	7	5
REQ05	Item 16	5	5	10	1	10	5	1	5	5
REQ06	Item 19	10	7	10	5	2	10	10	8	4
REQ07	Item 12	8	8	10	8	4	8	10	6	6
REQ08	Item 11	10	10	10	5	1	1	5	10	1
TOTAL		58	56	79	45	56	47	46	66	45

Tabla 2- 21 Selección de Sistema Operativo

Figura E-1 .- Selección de Distribución Linux[2]

HERRAMIENTA DE ADMINISTRACIÓN

INTRODUCCION

Son aplicaciones que corren sobre los diferentes sistemas operativos dando facilidades de control, monitoreo y gestión de los principales componentes de una red. Muchas de estas herramientas tienen licencia, y otras herramientas con las mismas funcionalidades son implementadas bajo GNU/LINUX con licencia GPL (General Public License).

La herramienta seleccionada depende de los administradores de la Red y de las características que posea según las necesidades de la empresa.

Una vez realizado el análisis de red (Capítulo 2) y teniendo en cuenta las necesidades de la red de Petroproducción descritas en el presente proyecto, se realizará el análisis de varias herramientas de administración y gestión de red Open Source.

Mediante la implementación de la NMS los administradores de red podrán:

- Detectar problemas de forma proactiva.
- Solucionar fallas eficazmente.
- Maximizar el aprovechamiento de los recursos.
- Mejorar el servicio de la Red.

[2] Análisis, implementación y evaluación de un prototipo ruteador dual Ipv4/Ipv6 con soporte de QoS e IPsec sobre Linux, usando AHP para la selección del hardware e IEEE 830 para la selección del software.

- Optimizar inversiones y reducción de costos.
- Garantizar la disponibilidad de los servicios de red.
- Detectar el funcionamiento de los diferentes enlaces y dispositivos.

ANÁLISIS DE HERRAMIENTAS DE ADMINISTRACION

Una vez realizado un sondeo de los productos existentes en el mercado actualmente y teniendo en cuenta los requerimientos de la empresa, así como el trafico que se va a monitorear, las facilidades del análisis de los resultados, que permitan la utilización del protocolo de administración SNMPv2, entre otros. Se seleccionaron las siguientes aplicaciones Open Source para ser comparadas:

- Nagios
- Zenoss
- Zabbix
- OpenNMS
- Pandora FMS
- JFFNMS

1. NAGIOS

Es un sistema Open Source de monitorización y gestión de redes que supervisa tanto hardware como software previamente configurados, es muy flexible porque permite definir distintos tipos de alertas en función de la disponibilidad de los objetos gestionados alertando cuando el comportamiento de los mismos no sea el deseado. Originalmente fue diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix. Por lo que está licenciado bajo la GNU General Public License Version 2 publicada por la Free Software Fundation. Proporciona una gran versatilidad para consultar parámetros de interés de un sistema, generando alertas, que son analizadas por los administradores cuando los parámetros exceden de los márgenes previamente definidos. La Tabla E-2 presenta las principales características de Nagios.

NAGIOS		
ITEM	**CARACTERÍSTICA**	**DESCRIPCIÓN**
1	GRÁFICAS	Posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados y visualización del estado de notificaciones enviadas, historial de problemas, archivos de registros, entre otros.
2	ESTADÍSTICAS	Obtención de información mediante estadísticas.
3	AUTODESCUBRIMIENTO	NO posee autodescubrimiento de la red.
4	SNMP	Permite el protocolo SNMP utilizando plugins.
5	SYSLOG	Permite análisis de Logs del sistema.
6	SCRIPTS EXTERNOS	Permite creación de scripts y acoplarlos a la herramienta.

NAGIOS		
ITEM	**CARACTERÍSTICA**	**DESCRIPCIÓN**
7	ALERTAS	Permite configuración de alertas según necesidades del usuario.
8	INTERFAZ WEB	Visualización del estado de la red en tiempo real a través de interfaz web. Solo Visualización.
9	BASE DE DATOS	Gestor de base de datos SQL.
10	EVENTOS[3]	Notificaciones de cuando ocurren problemas en servicios o dispositivos, así como cuando son resueltos. Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento.
11	LICENCIA	GPL (General Public License).
12	COMPLEMENTOS	Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades.
13	SEGURIDAD	DESCONOCIDO.
14	OTRAS CARACTERÍSTICAS	- Monitorización remota, con SSH (Secure Shell). - Monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP). - Posibilidad de definir la jerarquía de la red permitiendo distinguir entre dispositivos caídos e inaccesibles. - Se puede integrar con otras herramientas.

Tabla E-2.- Características herramienta NAGIOS.

Gráficos Herramienta Nagios.

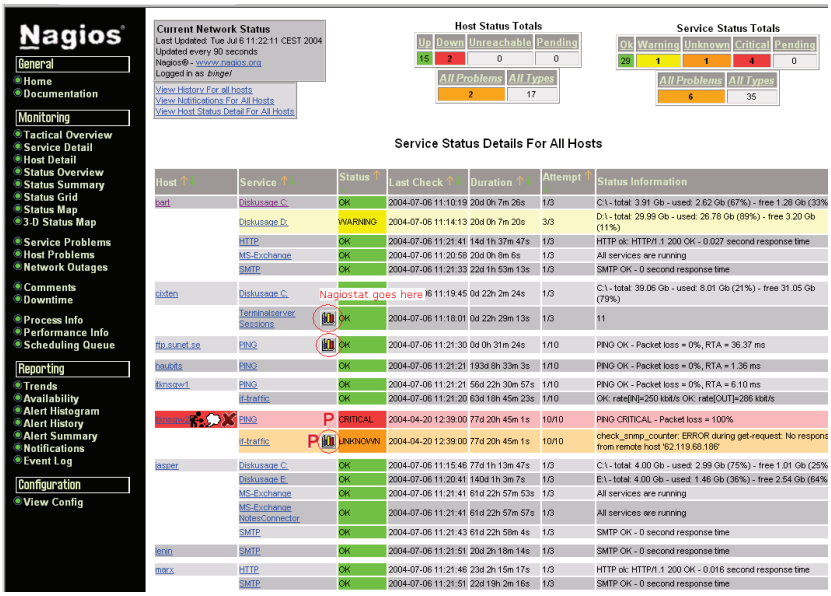


Figura E-2.- Ejemplo monitoreo de dispositivos con Nagios[4]

[3] Los eventos son la capacidad de notificar y guardar acciones.
[4] FUENTE: http://nagiostat.sourceforge.net/screenshots/in-nagios.png

2. ZENOSS

Es una aplicación que se encarga de monitorear toda la infraestructura tecnológica en una organización. Es una alternativa libre que permite una implementación sencilla del sistema, y aporta a la reducción de los costos empresariales, para estas tareas de monitoreo. Posee características que están **preparadas para funcionar bajo un entorno de software libre**, pero también trabaja en plataformas Unix, sistemas **Mac y aunque no fue diseñado para Windows es compatible con él con herramientas adicionales como VMplayer por ejemplo**. Está bajo licencia GLP desde Febrero de 2006, desarrollado y escrita en Python dentro de un entorno Zope, MySQL, RRDtool, CRicket, PySNMP, Net-SNMP, entre otros

Zenoss se ofrece en tres tipos de producto; la primera es la versión Core que es elaborada por la comunidad, la siguiente la versión Profesional y por último la versión Enterprise. Las dos últimas son versiones comerciales que poseen características. La Tabla E-3 presenta las principales características de Zenoss.

ZENOSS		
ITEM	**CARACTERÍSTICA**	**DESCRIPCIÓN**
1	GRÁFICAS	Posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados.
2	ESTADÍSTICAS	Obtención de información mediante estadísticas.
3	AUTODESCUBRIMIENTO	Tiene el "Dashboard Configuration" que permite identificar a cada uno de los equipos, recursos y dispositivos tecnológicos de la organización.
4	SNMP	Posee auto-detección SNMP.
5	SYSLOG	Permite análisis de Logs del sistema.
6	SCRIPTS EXTERNOS	Permite la creación de scripts externos.
7	ALERTAS	Permite gestión de alarmas.
8	INTERFAZ WEB	SI, Complejidad en el manejo de interfaz. Permite Control Total.
9	BDD (ALMACENAJE)	RRDTool y MySQL.
10	EVENTOS	Gestión de la ocurrencia de eventos y alarmas.
11	LICENCIA	GPL (General Public License) desde Febrero 2006.
12	COMPLEMENTOS	Posibilidad de programar plugins específicos que permite a los administradores tener un control completo sobre la infraestructura de red, Incluso con plugins de Nagios.
13	SEGURIDAD	Posee mecanismos de seguridad.
14	OTRAS CARACTERÍSTICAS	- Trabaja con módulos. - Permite realizar evaluaciones de acuerdo a las asignaciones de las IP de los equipos. - Con la herramienta de localización o Dashboard; Zenoss permite integración con Google Maps. - Monitorización remota mediante túneles SSL cifrados ó SSH. - Permite exportar e importar datos.

Tabla E-3.- Características herramienta Zenoss.

Gráficos Herramienta Zenoss.

Figura E-3.- Mapa de la Red en Zenoss / Fuente Web Oficial

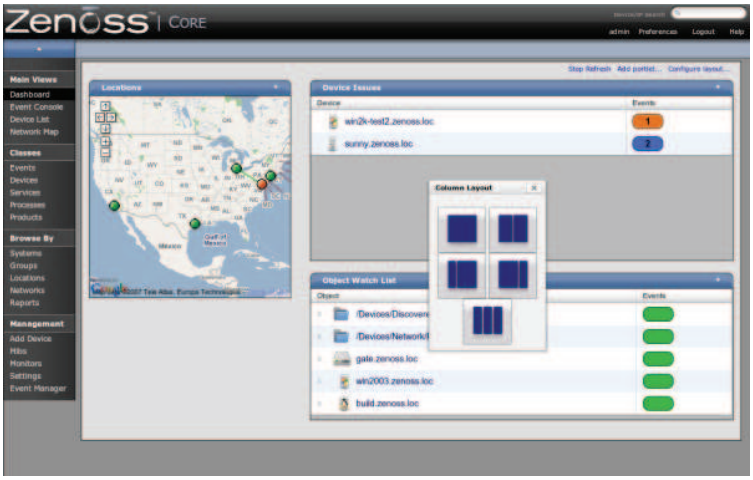


Figura E-4.- Herramienta Dashboard o de localización / Fuente Web Oficial

3. ZABBIX

Es un sistema de monitorización de código abierto que permite el seguimiento de las aplicaciones que corren dentro de una red, servidores, equipos, entre otros. Soporta las técnicas de petición y captura (polling and capture) para recoger datos de los dispositivos controlados, además tiene un mecanismo de notificación flexible que le permite configurar fácil y rápidamente los diferentes tipos de notificaciones de eventos predefinidos. La Tabla E-4 presenta las principales características Zabbix.

ZABBIX		
ITEM	**CARACTERÍSTICA**	**DESCRIPCIÓN**
1	GRÁFICAS	Posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados.

2	ESTADÍSTICAS	Obtención de información mediante estadísticas.
3	AUTODESCUBRIMIENTO	Autodescubrimiento de dispositivos.
4	SNMP	Soporta el protocolo SNMP.
5	SYSLOG	Supervisión de logs con eventlog.
6	SCRIPTS EXTERNOS	Permite la creación de scripts externos.
7	ALERTAS	Sistema de alertas (email, SMS, Jabber[5]).
8	INTERFAZ WEB	Administración vía web completamente. Permite Control Total.
9	BDD (ALMACENAJE)	Base de datos (Oracle, SQL, MySQL).
10	EVENTOS	Gestión de la ocurrencia de eventos.
11	LICENCIA	GPL (General Public License).
12	COMPLEMENTOS	Posibilidad de programar plugins fácilmente que permite a los administradores tener un control sobre la infraestructura de red.
13	SEGURIDAD	Posee mecanismos de seguridad.
14	OTRAS CARACTERÍSTICAS	- Escalabilidad. hasta 10.000 dispositivos. - Posibilidad de monitorizar redes internas y externas. - Tiene capacidades de Dashboard. - Monitorización segura con SSH. - Iconos de notificación de estado, Correcto y error. - Posee un parámetro-T en zabbix_sender que permite poner la fecha en cada valor. - Permite seguimiento distribuido. - Es Flexible y escalable.

Tabla E-4.- Características de la herramienta ZABBIX.

Gráficos de la herramienta Zabbix

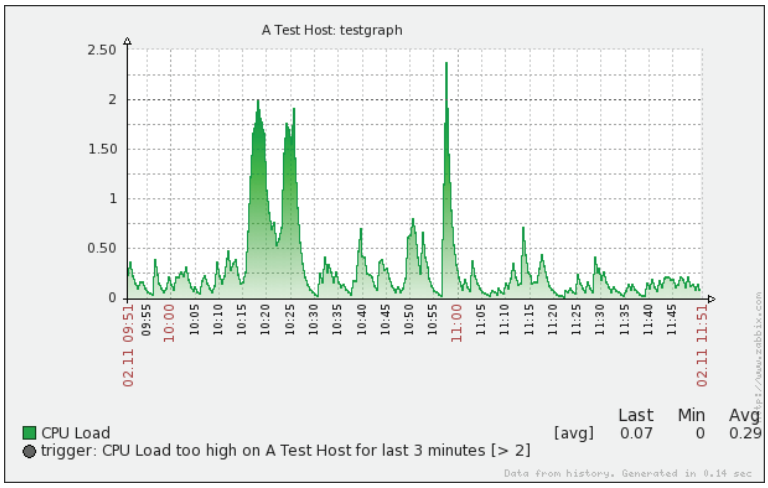


Figura E-5 .-Visualización de Monitoreo con Zabbix[6]

[5] JABBER es un protocolo libre para mensajería instantánea, basado en el estándar XML y gestionado por XMPP Standards Foundation.

[6] FUENTE: http://www.zabbix.com/wiki/_detail/news/updates/graph_gradient.png?id=start

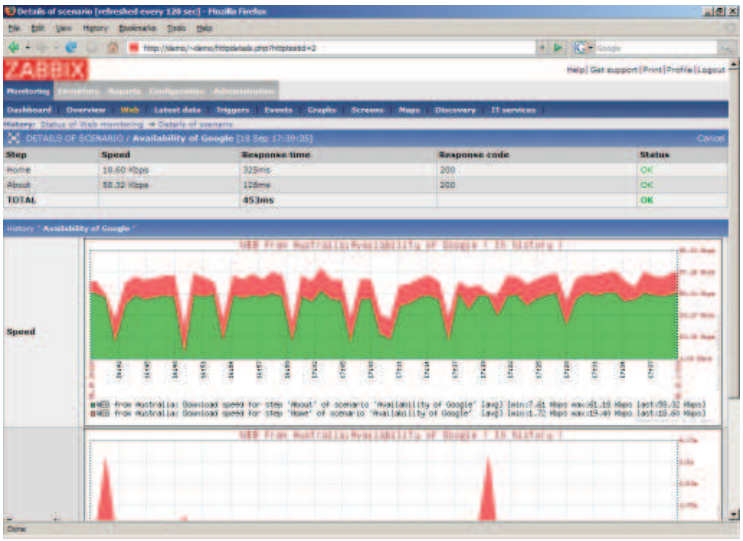


Figura E-6.- Gráficas del Tráfico con Zabbix

4. PANDORA FMS

Es un software Open Source para monitorizar cualquier tipo de servicio TCP/IP y medir todo tipo de elementos dentro de una red. Monitoriza sistemas, aplicaciones o dispositivos, permite saber el estado de cada elemento de un sistema a lo largo del tiempo, además puede detectar cuando se caen las interfaces de red. Permite flexibilidad ya que puede recoger información de cualquier sistema operativo, con agentes, específicos para cada plataforma, que recolectan datos y los envían al servidor. Hay agentes específicos para GNU/Linux, AIX, SUN Solaris, HP-UX, BSD/IPSO y Windows 2000, XP y 2003. Además soporta WMI para comunicarse directamente con sistemas Windows de forma remota y SNMP para recolectar datos o recibir traps. La Tabla E-5 presenta las principales características de Pandora FMS.

PANDORA FMS		
ITEM	**CARACTERÍSTICA**	**DESCRIPCIÓN**
1	GRÁFICAS	Posibilidad de generar informes y gráficas de comportamiento de los dispositivos monitorizados.
2	ESTADÍSTICAS	Recolección de datos de forma automatizada
3	AUTODESCUBRIMIENTO	Autodescubrimiento de dispositivos de la red.
4	SNMP	Soporta consola SNMP.
5	SYSLOG	Realiza recolección de Logs.
6	SCRIPTS EXTERNOS	Permite la creación de scripts externos.
7	ALERTAS	Posee sistema de alarmas
8	INTERFAZ WEB	SI, Permite Control Total.
9	BDD (ALMACENAJE)	Gestor de Base de datos MySQL.
10	EVENTOS	Gestión de la ocurrencia de eventos.
11	LICENCIA	Tiene licencia GPL2 GNU (General Public License v2)
12	COMPLEMENTOS	Posibilidad de programar plugins fácilmente que permite a los administradores tener un control sobre la infraestructura de red.
13	SEGURIDAD	Control de acceso granular, dar permisos de lectura o

		escritura a usuarios.
14	OTRAS CARACTERÍSTICAS	- Soporta múltiples usuarios con diferentes permisos. - Visualización del mapa de la red. - Monitoriza todo servicio TCP/IP. - Monitoreo de servicios, aplicaciones y Dispositivos. - Alta disponibilidad. - Flexible, se adapta a cualquier sistema. - Monitorización local y remota.

Tabla E-5.- Características de la herramienta PANDORA FMS.

GRÁFICOS PANDORA FMS.

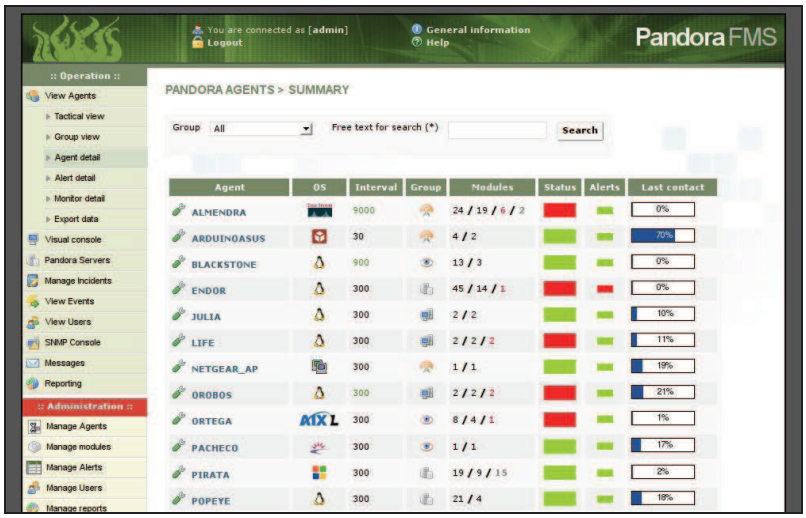


Figura E-7.- Presentación de información.[7]

5. OPENNMS

Es una plataforma de gestión y administración de redes empresariales gratuita y de código abierto que permite el monitoreo de servicios y dispositivos de una red, obteniendo información estadísticamente e informando de los errores. Puede correr en forma distribuida en gran número de dispositivos a ser gestionados, además posee autodescubrimiento de equipos y hosts pertenecientes a la red. La Tabla E-6 presenta las principales Características de OpenNMS.

OPENNMS		
ITEM	CARACTERÍSTICA	DESCRIPCIÓN
1	GRÁFICAS	Análisis de resultados con gráficas.
2	ESTADÍSTICAS	Provee de información estadística.
3	AUTODESCUBRIMIENTO	Autodescubrimiento de dispositivos de red.

[7] FUENTE: http://pandorafms.org/images/screenshots/1.3.1/pandora0.jpg

4	SNMP	Colección de datos con SNMP.
5	SYSLOG	Realiza recolección de Logs.
6	SCRIPTS EXTERNOS	Permite la creación de scripts externos.
7	ALERTAS	Capacidad de manipular alarmas vía comandos de la base de datos.
8	INTERFAZ WEB	Control total vía interfaz Web.
9	BDD (ALMACENAJE)	Utiliza RRDTool para guardar la información.
10	EVENTOS	Permite creación y evaluación de eventos.
11	LICENCIA	GPL (General Public License).
12	COMPLEMENTOS	Posibilidad de programar plugins permitiendo a los administradores tener un control sobre la infraestructura de red.
13	SEGURIDAD	Visualización pantallas con dashboard.
14	OTRAS CARACTERÍSTICAS	- Permite administración distribuida. - Monitorea servicios como: HTTP, IMAP, BDD, SMTP, entre otros. - Posee capacidades de Dashboard. - Permite Notificaciones vía email, XMPP[8] y otros. - Visualización de mapas con pantallas dinámicas. - Escalable en los aspectos del FCAPS.

Tabla E-6.- Características de la herramienta OPENNMS.

GRÁFICOS DE LA HERRAMIENTA OPENNMS.

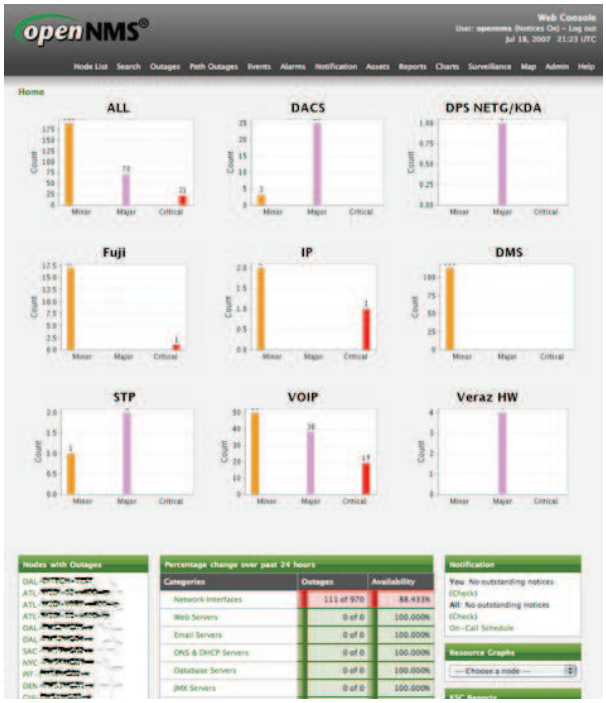


Figura E-8 .-Visualización por Protocolo con OPENNMS[9]

[8] XMPP: Protocolo extensible de mensajería y comunicación de presencia, anteriormente llamado Jabber, es un protocolo abierto y extensible basado en XML, originalmente ideado para mensajería instantánea.

6. JFFNMS

JFFNMS (*Just for Fun Network Monitoring System*) es un "sistema de monitoreo de redes" escrito en PHP de origen Argentino, usado en cientos de proveedores de Internet y redes privadas para monitorear routeadores Cisco, switches, servidores, y cualquier dispositivo que soporte SNMP. Trabaja tanto en ambientes Linux, FreeBSD y Windows 2000 y XP. Es un proyecto desarrollado por Javier Szyszlican, su versión más reciente es la 0.8.3 encuentrandose en constante desarrollo.

Es un sistema diseñado para monitorear redes IP siendo utilizado para supervisar todo dispositivo que soporte el protocolo SNMP como servidores, routers, switches, puertos, entre muchos más. Provee también características enfocadas a dispositivos Cisco.

OPENNMS		
ITEM	**CARACTERÍSTICA**	**DESCRIPCIÓN**
1	GRÁFICAS	Análisis de resultados con gráficas con el uso de herramientas RRDTOOL.
2	ESTADÍSTICAS	Provee de información estadística.
3	AUTODESCUBRIMIENTO	Distintas maneras de descubrimiento: manual, Auto o descubrimientos personalizados en función de la plataforma del dispositivo.
4	SNMP	Colección de datos con SNMP v1, v2c y v3.
5	SYSLOG	Recolección de Logs.
6	SCRIPTS EXTERNOS	Modular y extensible
7	ALERTAS	Capacidad de manipular, gestionar y personalizar alarmas.
8	INTERFAZ WEB	Administración completa vía interfaz Web.
9	BASE DE DATOS	Utiliza MySQL o PostgreSQL
10	EVENTOS	Muestra todos los tipos de eventos en orden de tiempo ocurrido en una misma pantalla
11	LICENCIA	GPL (General Public License).
12	COMPLEMENTOS	Uso de tecnologías: Apache, Cron, MySQL, PHP, RDDTool y SNMP.
13	SEGURIDAD	Creación de usuarios y uso de Tacacs+ para control de acceso.
14	OTRAS CARACTERÍSTICAS	- Soporte de Mapas y submapas - Monitorea servicios como: HTTP, IMAP, BDD, SMTP, entre otros. - Trabaja con SSL y HTTPS - Integración con Smokeping y otras herramientas linux - Sonidos de Alertas en el browser - Soporte de MIBs SNMP

Tabla E-7.- Características de la herramienta JFFNMS.

[9] FUENTE: http://blogs.opennms.org/images/opennms-netcool.png

GRÁFICAS DE JFFNMS

Figura E-9.- Hosts y Eventos Monitoreados

Figura E-10.- Gráfica del Performance de una interfaz monitoreada[10]

CUADRO COMPARATIVO

Una vez analizadas características importantes de varias herramientas de administración Open Source y considerando que tengan varias facilidades para administración así como que permita

[10]FUENTE: http://www.jffnms.com/screenshots/thumb/shot_4t.jpg

la gestión de una red empresarial como es la de Petroproducción, la Tabla E-8 presenta una comparativa entre todas las herramientas consideradas.

CARACTERISITICAS	NAGIOS	ZENOSS	JFFNMS	PANDORA FMS	OPENNMS	ZABBIX
GRÁFICAS	SI	SI	SI	SI	SI	SI
ESTADÍSTICAS	SI	SI	SI	SI	SI	SI
AUTODESCUBRI-MIENTO	NO	SI	SI	SI	SI	SI
SNMP	SI, con plugins	SI	SI	SI	SI	SI
SYSLOG	SI	SI	SI	SI	SI	SI
SCRIPTS EXTERNOS	SI	SI	SI	SI	SI	SI
ALERTAS	SI	SI	SI	SI	Algunas	SI
INTERFAZ WEB	Sólo Visualiza-ción	Control Total	Administra-ción Total	Control Total	Control Total	Control Total
BDD (ALMACENAJE)	SQL	RRDTool y MySQL	RRDTool, MySQL y PostgreSQL	SQL	RRDTool	SQL
EVENTOS	SI	SI	SI	SI	SI	SI
LICENCIA	GPL	GPL	GPL	GPL2	GPL	GPL
COMPLEMENTOS	SI	SI	SI	SI	SI	SI
SEGURIDAD	NO	SI	SI	SI	Pantallas con Dashboard	SI

Tabla E-8.- Cuadro Comparativo de Herramientas de Monitoreo.

Una vez definido las posibles herramientas para la implementación de una consola de monitoreo, fueron cada una de estas instaladas y probadas verificando las ventajas que las mismas presentan, dificultades y aplicaciones que en algunas herramientas sólo se encontraban el su versión comercial empresarial.

Con la premisa que la nms sea una interfaz agradable y amigable ante los usuarios que la administrarán y con el afán de poseer un software con todos sus aplicativos de forma libre, se decidió utilizar la herramienta **JFFNMS** para ser aplicada en el Centro de Operaciones de Red.

Las premisas para su selección fueron:

a. Puede ser instalada en servidores de plataforma Linux y Windows de forma totalmente libre.
b. Posee características enfocadas a la gestión de dispositivos Cisco (solución empleada en Petroproducción en su gran mayoría).
c. Se integra con herramientas Linux como fping, nmap, smokeping, entre otras.

d. Posee una administración sencilla al usuario
e. Permite la visualización de gráficas de acuerdo a parámetros de fecha de inicio y fin.
f. Permite la personalización de eventos y alarmas.
g. Posee un tiempo de respuesta adecuado y mínimo a problemas surgidos en una red

A continuación se presentan a detalle las características de la herramienta elegida:

Parámetro	Características
Sistema	Escrito en PHP, trabaja actualmente con PHP5 Completamente comprobado sobre Linux, FreeBSD y Windows 2000 Trabaja con cualquier sistema que tenga soporte PHP Base de Datos MySQL o PostgreSQL Tipos de eventos configurables y Niveles de severidad Licencia GPL Autodescubrimiento de red, hosts e interfaces
Integración	Autenticación y Accounting Tacacs+ Linux IP Tables NMAP, Smokeping, Syslog, TFTP, NTP
Interfaz WEB	Consola de eventos, syslog, alarmas y tacacs en una misma pantalla Soporte de mapas y submapas Gráficas de tráfico, paquetes perdidos y más Sonidos de Alertas SSL y HTTPS Completa administración web
Monitoreo	Interfaces, Hosts, Dispositivos Storage y aplicaciones en ejecución CISCO MAC, IP, CSS, AGENT SA Ambiente CISCO, CISCO NAT, CISCO PIX Conexiones TCP Estado de sesiones BGP Características de sistemas Windows Sensores MIB
Reportes	Tráfico de Bytes Porcentaje de uso del procesador y memoria Paquetes por segundo, errados, tasa de error y errores por segundo Número de procesos y de usuarios Conexiones TCP entrantes, salientes, establecidas y rechazadas Temperatura
Otros	Monitoreo de Puertos Poleo Distribuido Orientado a Objetos Uso y configurable con SLA

Tabla E-9 .- Caraterísitcas de Herramienta seleccionada

ANEXO F

COTIZACIÓN DE IMPLANTACIÓN DEL PROYECTO

COTIZACIÓN DE IMPLANTACIÓN DEL PROYECTO

OFERTA ECONÓMICA - EQUIPOS - CAPACITACION

Cliente: Petroproducción **Fecha:** Mayo de 2010
Atención:

SERVIDORES

SERVIDOR DE MONITOREO

Característica	Descripción	Cantidad	P. Unitario	P. total
HP DL180 G6 E5520 3x2GB 8LFF Svr		2	$ 2,381.91	$ 4,763.83
487503-001	HP DL180 G6 E5520 3x2GB 8LFF Svr			
458928-B21	HP 500GB 3G SATA 7.2K 3.5in MDL HDD			
Processor(s)	Intel® Xeon® Processor E5520 (2.26 GHz)			
Cache Memory	8MB shared L3 cache			
Memory	6GB (3 x 2GB) PC3-10600E (UDIMM)			
Network Controller	HP NC362i Integrated Dual Port Gigabit Server Adapter			
Storage Controller	HP Smart Array P410 /256MB Controller (RAID 0/1/1+0/5/5+0)			
Internal Storage	Maximum 8TB (8 x 1TB) SATA			
Optical Drive	None ship standard			
Power Supply	460W common slot, high efficiency power supply			
Form Factor	Rack (2U)			
Warranty	3 años en piezas			
	Subtotal			$ 4,763.83

SERVIDOR DE LOG´S

Característica	Descripción	Cantidad	P. Unitario	P. total
HP ML110G5 X3110 500GB NHP Promo Svr (AT040A)		2	$ 796.81	$ 1,593.62
Processor(s)	(1) Intel® Xeon® processor E3110 (3.00 GHz)			
Cache Memory	6MB Level 2 cache			
Memory	1GB (1 x 1 GB) PC2-6400			
Network Controller	Embedded NC105i PCIe Gigabit			
Storage Controller	Embedded SATA RAID (0/1) 4 ports for HDD			
Hard Drive	(1) 500GB SATA 7.2K 3.5"			
Internal Storage	Maximum 3TB (4 x 750GB) SATA			
Optical Drive	DVD-ROM Drive			
Form Factor	Micro ATX Tower (4U)			
Warranty	3 años en piezas, mano de obra, on site			
	Subtotal			$ 1,593.62

SWITCH CAPA2

ITEM	Descripción	Cantidad	P. Unitario	P. total
WS-C2960-24TT-L	Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image	1	$ 870.00	$ 870.00
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1	$0.00	$0.00
	Subtotal			$ 870.00

Figura F-1.- Cotización (PARTE I)

CABLEADO ESTRUCTURADO

Característica	Descripción	Cantidad	P. Unitario	P. total
PUR6X04BUY	CABLE UTP CAT 6A AZUL	1	$ 150,00	$ 150,00
UTP6X10Y	Patch Cord UTP Cat. 6 a de 10 pies color blanco	8	$ 17,01	$ 136,10
CFPE1IWY	Face Plate Ejecutivo de 1 salidas	8	$ 1,67	$ 13,33
DEX-P-1000	Cajas Sobrepuestas	8	$ 1,79	$ 14,36
CJ6X88TGWH	JACK CAT 6A BLANCO	8	$ 14,62	$ 116,92
S/N	Canaletas y accesorios de instalacion	1	$ 200,00	$ 200,00
S/N	Instalacion de los puntos de datos cat 6A	8	$ 30,00	$ 240,00
S/N	Certificacion de los puntos de datos cat 6A	8	$ 5,00	$ 40,00
			Subtotal	$ 910,72

CONFIGURACIÓN

Característica	Descripción	Cantidad	P. Unitario	P. total
S/N	Configuración de equipos	1	$ 5.000,00	$ 5.000,00
S/N	Pruebas de funcionamiento	1	$ 1.000,00	$ 1.000,00
			Subtotal	$ 6.000,00

CAPACITACIÓN

Característica	Descripción	Cantidad	P. Unitario	P. total
CAP-REDES1	Curso administración de Redes, 10 horas incluidas, 5 personas	1	$ 1.200,00	$ 1.200,00
CAP-CISCO-CONFIG	Capacitación en configuración switches y routers CISCO, 10horas, 5personas	1	$ 1.500,00	$ 1.500,00
			Subtotal	$ 2.700,00

TOTAL SIN IVA	$ 16.838,16

Atentamente.

ANDEAN TRADE S.A.
RUC 1791738845001

ANDEANTRADE

Figura F-2.- Cotización (PARTE II)

COSTO MONITOR PARA LA CONSOLA NMS

Se considera un monitor de considerable tamaño a fin de contar con la facilidad de visualización de equipos, alarmas y eventos en la consola de monitoreo, sus características avanzadas podrán servir para nuevas aplicaciones a futuro en la empresa.

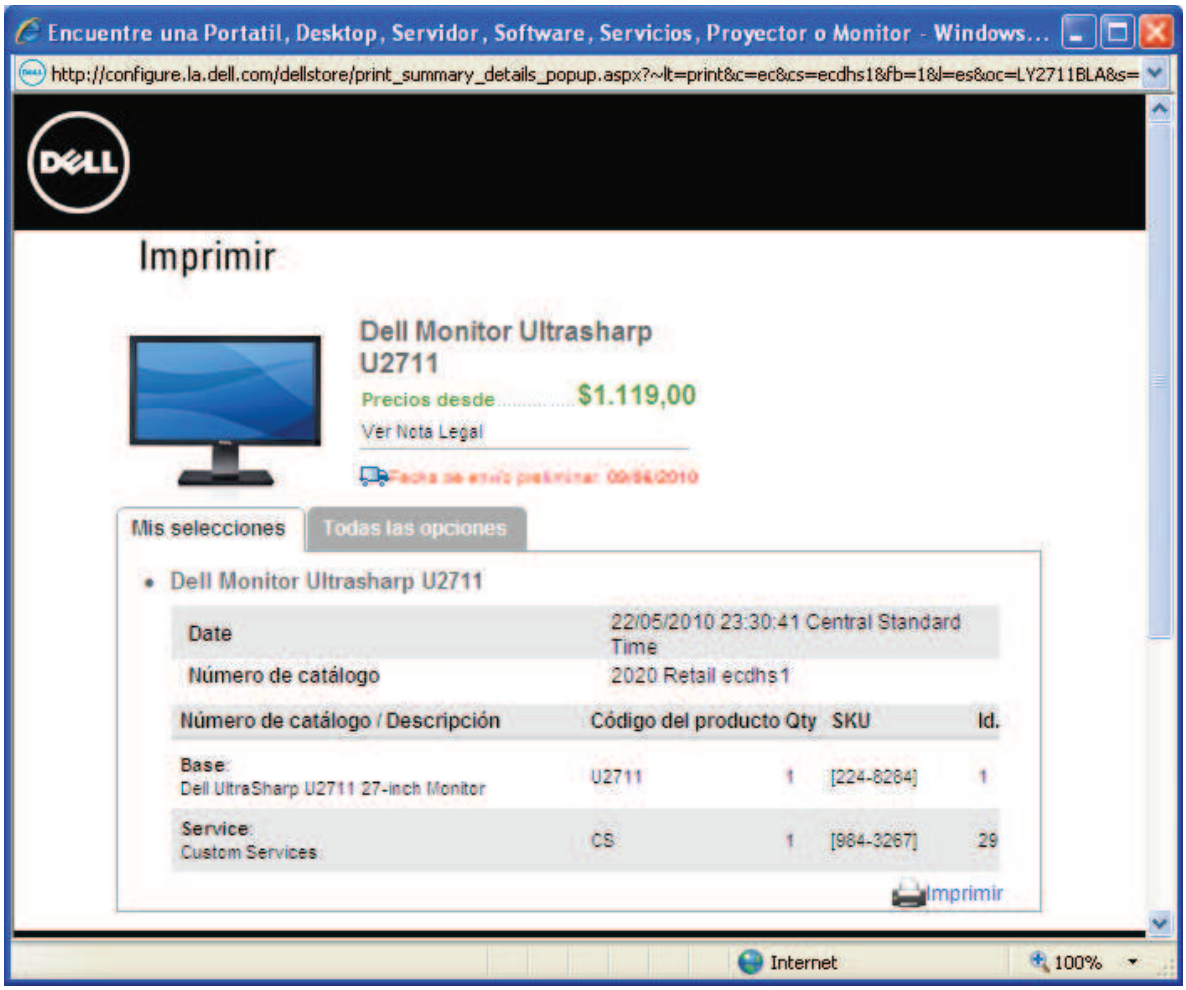


Figura F-3.- Monitor DELL[11]

[11] Fuente: tienda en línea DELL para Ecuador

LINK: http://configure.la.dell.com/dellstore/config.aspx?c=ec&cs=ecdhs1&l=es&oc=LY2711BLA&s=dhs

COSTO SALARIAL DEL PERSONAL ADICIONAL NECESARIO PARA EL NOC

Con la creación del Departamento de Redes, el ingreso de nuevos integrantes al área tecnológica de la empresa, implica un gasto adicional a Petroproducción producto del costo mensual que conlleva la contratación de nuevo personal.

Los datos anexados han sido proporcionados por el Departamento de Recursos Humanos. La fijación de sueldos para nuevas contrataciones se basa en los cuadros remunerativos impuestos por la LOSCCA[12] para empleados del sector público. El costo para la empresa debido al ingreso de un nuevo servidor implica un costo equivalente a la sumatoria de:

- Remuneración mensual unificada
- Décimo tercer y cuarto sueldo
- Aporte patronal al IESS
- Vacaciones
- Fondos de reserva
- Horas extras realizadas.

En el cálculo se emplea una base referencial de veinte horas extraordinarias y cuarenta horas suplementarias[13] .

Para personal técnico profesional con título de tercer nivel se lo ubica dentro de los grado de servidor público 7 hasta el grado 14. Por encima de este rango se encuentran directivos y por debajo personal de apoyo y servicio. De esta manera según el personal adicional propuesto para este proyecto se establece como referencia:

Administrador NMS:

- Con título de Ingeniería y experiencia en el campo: Servidor Público 1

Soporte de Networking:

- Con título de tecnología y experiencia en el campo: Servidor Público 5

El siguiente cuadro muestra en detalle el cuadro empleado para la fijación salarial utilizado actualmente para la contratación de personal en Petroecuador y todas sus filiales.

[12] LOSCCA:

[13] Las horas extraordinarias implican el trabajo realizado en días feriados, fines de semana y días por ley no laborables. Horas suplementarias hacen referencia a horas adicionales después de la jornada laboral normal.

PETROPRODUCCION

CUADRO REMUNERATIVO MENSUAL Y COSTO ANUAL DE LA LOSCCA 2010

						# HORAS 100%	20	#HORAS 50%	40					
						VALOR DECIMO CUARTO		240						
#	GRUPO OCUPACIONAL	GRADO	RMU	DECIMO CUARTO	VACACIONES	VALOR HORA EXTRAORDINARIA	VALOR MES HORAS EXTRAS	VALOR HORA SUPLEMENTARIAS	VALOR MES HORAS SUPLEMENTARIAS	APORTE PATRONAL IESS 11,15	DECIMO TERCERO	FONDOS DE RESERVA	COSTO EMPRESA MENSUAL	VALOR ANUAL
1	SERVIDOR PUBLICO DE SERVICIOS 1	1	500.00	20.00	41.67	4.00	80.00	3.00	120.00	55.75	61.81	61.81	941.03	11,292.33
2	SERVIDOR PUBLICO DE SERVICIOS 2	2	525.00	20.00	43.75	4.20	84.00	3.15	126.00	58.54	64.90	64.90	987.08	11,844.95
3	SERVIDOR PUBLICO DE APOYO 1	3	555.00	20.00	46.25	4.44	88.80	3.33	133.20	61.88	68.60	68.60	1,024.34	12,508.09
4	SERVIDOR PUBLICO DE APOYO 2	4	590.00	20.00	49.17	4.72	94.40	3.54	141.60	65.79	72.93	72.93	1,106.81	13,281.75
5	SERVIDOR PUBLICO DE APOYO 3	5	640.00	20.00	53.33	5.12	102.40	3.84	153.60	71.36	79.11	79.11	1,198.92	14,386.99
6	SERVIDOR PUBLICO DE APOYO 4	6	695.00	20.00	57.92	5.56	111.20	4.17	166.80	77.49	85.91	85.91	1,300.23	15,602.74
7	SERVIDOR PUBLICO 1	7	775.00	20.00	64.58	6.20	124.00	4.65	186.00	86.41	95.80	95.80	1,447.59	17,371.12
8	SERVIDOR PUBLICO 2	8	855.00	20.00	71.25	6.84	136.80	5.13	205.20	95.33	105.69	105.69	1,594.96	19,139.49
9	SERVIDOR PUBLICO 3	9	935.00	20.00	77.92	7.48	149.60	5.61	224.40	104.25	115.58	115.58	1,742.32	20,907.86
10	SERVIDOR PUBLICO 4	10	1,030.00	20.00	85.83	8.24	164.80	6.18	247.20	114.85	127.32	127.32	1,917.32	23,007.81
11	SERVIDOR PUBLICO 5	11	1,150.00	20.00	95.83	9.20	184.00	6.90	276.00	128.23	142.15	142.15	2,138.36	25,660.37
12	SERVIDOR PUBLICO 6	12	1,340.00	20.00	111.67	10.72	214.40	8.04	321.60	149.41	165.64	165.64	2,488.35	29,860.25
13	SERVIDOR PUBLICO 7	13	1,590.00	20.00	132.50	12.72	254.40	9.54	381.60	177.29	196.54	196.54	2,948.87	35,386.42
14	SERVIDOR PUBLICO 8	14	1,670.00	20.00	139.17	13.36	267.20	10.02	400.80	186.21	206.43	206.43	3,096.23	37,154.79
15	SERVIDOR PUBLICO 9	15	1,930.00	20.00	160.83	15.44	308.80	11.58	463.20	215.20	238.57	238.57	3,575.17	42,902.01
16	SERVIDOR PUBLICO 10	16	2,190.00	20.00	182.50	17.52	350.40	13.14	525.60	244.19	270.71	270.71	4,054.10	48,649.22
17	SERVIDOR PUBLICO 11	17	2,345.00	20.00	195.42	18.76	375.20	14.07	562.80	261.47	289.87	289.87	4,339.62	52,075.44
18	SERVIDOR PUBLICO 12	18	2,505.00	20.00	208.75	20.04	400.80	15.03	601.20	279.31	309.65	309.65	4,634.35	55,612.19
19	SERVIDOR PUBLICO 13	19	2,815.00	20.00	234.58	22.52	450.40	16.89	675.60	313.87	347.97	347.97	5,205.39	62,464.64
20	SERVIDOR PUBLICO 14	20	3,360.00	20.00	280.00	26.88	537.60	20.16	806.40	374.64	415.33	415.33	6,209.31	74,511.68

ELABORADO POR RRHH:CEMD/91086

20/05/2010 09:31

Figura F-4.- Cuadro de Remuneraciones de LOSCCA