



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES
DE COMUNICACIÓN**

**MODELO DE GESTIÓN DE RED FUNCIONAL EN LA RED
LOCAL DE DATOS DEL GOBIERNO AUTÓNOMO
DESCENTRALIZADO DE SAN MIGUEL DE IBARRA
BASADO EN EL ESTÁNDAR ISO**

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTORA: VIVIANA ELIZABETH AYALA YANDÚN

DIRECTOR: ING. CARLOS VÁSQUEZ

Ibarra, Junio 2015

DECLARACIÓN

Yo, Viviana Elizabeth Ayala Yandún con cédula de identidad Nro. 100306856-4, estudiante de la Facultad de Ingeniería en Ciencias Aplicadas – Carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro que el presente trabajo de investigación, es de mi autoría y no ha sido realizado, ni calificado por otro profesional, para efectos académicos y legales será de mi responsabilidad.

A través de la presente declaración cedo el derecho de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, reglamentos y normatividad vigente de la Universidad Técnica del Norte.

Firma:



Nombre: Ayala V. Elizabeth

C.I.: 100306856-4

CERTIFICACIÓN

Certifico que la Señorita Viviana Elizabeth Ayala Yandún estudiante de la Facultad de Ingeniería en Ciencias Aplicadas – Carrera de Ingeniería en Electrónica y Redes de Comunicación, ha desarrollado y terminado en su totalidad el presente proyecto de grado **“MODELO DE GESTIÓN DE RED FUNCIONAL EN LA RED LOCAL DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA BASADO EN EL ESTÁNDAR ISO”**, bajo mi supervisión.



ING. CARLOS VÁSQUEZ
DIRECTOR DE TESIS



UNIVERSIDAD TÉCNICA DEL NORTE
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO
DE INVESTIGACIÓN A FAVOR DE LA UNIVERSIDAD
TÉCNICA DEL NORTE

Yo, VIVIANA ELIZABETH AYALA YANDÚN portadora de la cédula de ciudadanía Nro. 100306856-4, manifiesto que es mi voluntad de ceder a la Universidad Técnica del Norte, los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de grado denominado: **"MODELO DE GESTIÓN DE RED FUNCIONAL EN LA RED LOCAL DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA BASADO EN EL ESTÁNDAR ISO"**, que ha sido desarrollado para obtener el título de **INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN** en la Universidad Técnica del Norte, quedando facultada la Universidad para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento en que realizó la entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

Firma:

Nombre: VIVIANA ELIZABETH AYALA YANDÚN

Cédula: 100306856-4



UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA
AUTORIZACIÓN DE USO Y PUBLICACIÓN A
FAVOR DE LA UNIVERSIDAD TÉCNICA DEL
NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo por sentada mi voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente investigación.

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD	1003068564
APELLIDOS Y NOMBRES	VIVIANA ELIZABETH AYALA YANDÚN
DIRECCIÓN	PANAMÁ 3-62
EMAIL	ayala_yandun@hotmail.com
TELÉFONO FIJO	062956879
TELÉFONO MOVIL	0992054723

DATOS DE LA OBRA	
TÍTULO	“MODELO DE GESTIÓN DE RED FUNCIONAL EN LA RED LOCAL DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA BASADO EN EL ESTÁNDAR ISO”

AUTOR	VIVIANA ELIZABETH AYALA YANDÚN
FECHA	16 DE JUNIO DEL 2015
PROGRAMA	PREGRADO
TÍTULO POR EL QUE SE ASPIRA	INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
DIRECTOR	ING. CARLOS VÁSQUEZ

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, VIVIANA ELIZABETH AYALA YANDÚN, con cédula de ciudadanía Nro. 100306856-4, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 143.

3. CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, Junio del 2015

AGRADECIMIENTOS**AUTORA:**

A mi Divino Niño Jesús y a la Santísima Virgen María por bendecirme e iluminarme cada día de mi vida y permitirme llegar hasta este gran logro.


(Firma): 

Nombre: AYALA YANDÚN VIVIANA ELIZABETH

Cédula: 100306856-4

A los docentes de la carrera de Ingeniería en Electrónica y Redes de Comunicación por guiarme con sus enseñanzas y en especial al Ing. Carlos Vásquez director de asistencia y asesoría en el transcurso de elaboración del proyecto.

ACEPTACIÓN:

(Firma): 

Nombre: Ing. Betty Chávez

Cargo: JEFA DE BIBLIOTECA GENERAL

Facultado por la resolución de Consejo Universitario

Viviana E. Ayala Y.

AGRADECIMIENTOS

A mi Divino Niño Jesús y a la Santísima Virgen María por bendecirme e iluminarme cada día de mi vida y permitirme llegar hasta este gran logro.

A mis padres y hermanos que son el pilar fundamental que me sostiene cada día, con su amor, confianza, apoyo incondicional, me han brindado la oportunidad tan grande y valiosa de tener una profesión.

A los docentes de la carrera de Ingeniería en Electrónica y Redes de Comunicación por guiarme con sus enseñanzas y en especial al Ing. Carlos Vásquez director de tesis por su paciencia y asesoría en el transcurso de elaboración del proyecto.

A la Dirección de Tecnologías de la Información y Comunicación del Municipio de Ibarra por haberme permitido desarrollar este proyecto, brindarme su buena ayuda y colaboración en el lapso del mismo.

A todas aquellas personas que de una u otra manera me tendieron la mano para poder culminar este trabajo.

Viviana E. Ayala Y.

DEDICATORIA

Este proyecto lo dedicó a mis padres Elizabeth y Wilson, quienes me apoyaron incondicionalmente y confiaron en mí, quienes con su esfuerzo diario, consejos, valores, su buen ejemplo y comprensión me han guiado y enseñado a nunca dejarme vencer por ninguna adversidad, para ellos con todo mi amor y cariño.

"Lo que se empieza se termina"

Viviana E. Ayala Y.

ÍNDICE DE CONTENIDO

DECLARACIÓN.....	i
CERTIFICACIÓN.....	ii
AGRADECIMIENTOS.....	vii
DEDICATORIA	viii
ÍNDICE DE TABLAS	xv
ÍNDICE DE FIGURAS.....	xvi
RESUMEN.....	xix
ABSTRACT	xx
PRESENTACIÓN	xxi
CAPÍTULO I.....	1
1. Antecedentes	1
1.1. Problema	1
1.2. Objetivos	2
1.2.1. Objetivos Generales.	2
1.2.2. Objetivos Específicos.....	3
1.3. Alcance.....	4
1.4. Justificación.....	6
CAPÍTULO II	8
2. Modelo de Gestión de Red Funcional Basado en el Estándar ISO	8
2.1. Introducción	8
2.2. Fundamentos de Gestión de Red.....	9
2.2.1. Administración de red.	9
2.2.2. Gestión de red.....	9
2.2.2.1. Objetivos de gestión de red.	10
2.2.3. Necesidad de la gestión de redes.....	11
2.2.4. Elementos de un sistema de gestión de red.	11
2.2.4.1. Dispositivos Gestionados.	12
2.2.4.2. Gestor.	12
2.2.4.3. Agentes.....	12
2.2.4.4. Estación de gestión de red ó Network Management Station (NMS).....	13
2.2.4.5. Protocolo de gestión de red.	13

2.2.4.6.	Base de Información de Gestión (MIB).	13
2.2.5.	Componentes de la gestión de redes.	14
2.2.5.1.	Componente Organizacional.	14
2.2.5.2.	Componente Técnico.	15
2.2.5.3.	Componente Funcional.	15
2.2.6.	Modelo de gestión de red funcional basado en el estándar ISO.	16
2.2.6.1.	Gestión de Configuración.	17
2.2.6.2.	Gestión de Fallos.	19
2.2.6.3.	Gestión de Contabilidad.	22
2.2.6.3.1.	Funciones de la gestión de contabilidad.	22
2.2.6.3.2.	Recursos gestionados.	23
2.2.6.3.3.	Consideraciones.	23
2.2.6.4.	Gestión de Prestaciones.	24
2.2.6.4.1.	Medidas orientadas a servicios.	24
2.2.6.4.2.	Medidas orientadas a eficiencia.	25
2.2.6.4.3.	Funciones de gestión de prestaciones.	25
2.2.6.5.	Gestión de Seguridad.	26
2.2.6.5.1.	Funciones de gestión de seguridad.	26
2.2.6.5.2.	Ataques en la gestión de seguridad.	27
2.3.	Modelo de Gestión Internet o TCP/IP.	27
2.4.	Protocolo Simple de Gestión de Red (SNMP).	28
2.4.1.	Definición.	28
2.4.2.	Componentes de SNMP.	29
2.4.2.1.	Estructura de la información de gestión (SMI).	30
2.4.2.2.	Base de información de gestión (MIB).	31
2.4.2.2.1.	Identificación de objeto (OID).	31
2.4.2.3.	Comunidad SNMP.	32
2.4.3.	Funcionamiento de SNMP.	33
2.4.3.1.	Funcionamiento de SNMP en relación a la pila de protocolos TCP/IP.	34
2.4.4.	Versiones SNMP.	37
2.4.4.1.	SNMP versión 1.	37
2.4.4.2.	SNMP versión 2.	38
2.4.4.3.	SNMP versión 3.	38

2.4.4.4.	Partes de la trama del mensaje SNMP.....	39
2.4.4.4.1.	<i>Mensajes enviados por SNMP</i>	39
2.5.	Monitorización Remota RMON.....	40
2.6.	Virtualización.....	41
2.6.1.	Máquinas virtuales.....	41
2.7.	Software de gestión de redes.....	42
2.8.	Estándar IEEE 830 para elección del software de gestión.....	42
2.8.1.	Especificación de requisitos para el software de gestión.....	42
2.8.1.1.	Introducción.....	42
2.8.1.2.	Propósito.....	43
2.8.1.3.	Descripción general.....	43
2.8.1.3.1.	Valorización de los requerimientos.....	43
2.9.	Red de telefonía celular.....	43
2.9.1.	Estructura de una red de telefonía celular.....	43
2.9.2.	Arquitectura de una red GSM.....	44
2.9.2.1.	Servicios que ofrece GSM.....	45
2.9.2.2.	Servicios de mensajes cortos (SMS).....	46
2.9.2.3.	Soluciones para el envío de alertas empleando SMS.....	47
2.9.2.3.1.	<i>Envío de SMS a través de Internet</i>	47
2.9.2.3.2.	<i>Envío de SMS mediante un celular conectado al servidor</i>	48
2.9.2.3.3.	<i>Envío de SMS a través de un Módem GSM conectado al servidor</i>	49
CAPÍTULO III.....		51
3.	Análisis de la Infraestructura Actual de la Red Local de Datos del GAD-Ibarra.....	51
3.1.	Introducción.....	51
3.2.	Estructura Administrativa.....	52
3.3.	Descripción de las Dependencias Internas.....	53
3.3.1.	Descripción del edificio principal.....	54
3.3.2.	Descripción del edificio antiguo.....	56
3.4.	Descripción de las Dependencias Externas.....	56
3.4.1.	Dirección de Cultura, Proyecto Parque Ciudad Blanca.....	56
3.4.2.	Dirección de Turismo.....	57
3.4.3.	Bodega Municipal.....	57
3.4.4.	Administración de Mercado Amazonas.....	57

3.5.	Situación Actual de la Red Local de Datos	57
3.5.1.	Infraestructura física de la red local de datos.	58
3.5.1.1.	Data Center.....	58
3.5.1.2.	Subsistemas del cableado estructurado.	60
3.5.1.3.	Subsistema del cableado vertical o backbone.	61
3.5.1.4.	Subsistema del cableado horizontal o cableado de distribución.....	61
3.5.1.5.	Áreas de trabajo.....	62
3.5.1.6.	Topología física de la red local de datos.	63
3.5.1.7.	Descripción de Switches (Conmutadores).....	63
3.5.1.8.	Descripción de Servidores Físicos y Virtuales.	66
3.5.1.8.1.	<i>Escenarios de virtualización.</i>	66
3.5.1.9.	Racks Secundarios.....	73
3.5.1.9.1.	<i>Rack del edificio antiguo.</i>	73
3.5.1.9.2.	<i>Rack de los departamentos de la casa de la Ibarreñidad.</i>	74
3.5.1.10.	Elementos de acceso a la red de los usuarios finales.....	74
3.5.1.11.	Situación actual del backbone de fibra óptica.	75
3.5.1.11.1.	<i>Diagrama del backbone de fibra óptica.</i>	76
3.5.1.11.2.	<i>Características del backbone de fibra óptica.</i>	77
3.5.2.	Estructura lógica de la red local de datos.	78
3.5.3.	Análisis de la infraestructura de la red local de datos para identificar las áreas críticas. 79	
3.5.3.1.	Análisis para elección de switches.	79
3.5.3.1.1.	Núcleo	80
3.5.3.1.2.	Distribución.....	81
3.5.3.1.3.	Acceso	82
3.5.3.2.	Análisis para elección de servidores.....	83
3.5.3.2.1.	<i>Distribución del tráfico generado por aplicaciones y protocolos.</i>	84
3.5.3.3.	Análisis para elección de servidores físicos.	93
3.5.3.3.1.	<i>Servidor POSTGRESQL.</i>	94
3.5.3.3.2.	<i>Servidor OLYMPO</i>	94
3.5.3.3.3.	<i>Servidor de antivirus.</i>	94
3.5.3.3.4.	<i>Servidores HP.</i>	94
3.5.3.4.	Análisis para elección de servidores virtuales.....	95

3.5.3.4.1.	<i>Servidor de Correo</i>	95
3.5.3.4.2.	<i>Servidor DNS y DHCP</i>	96
3.5.3.4.3.	<i>Servidor documental Quipux</i>	96
3.5.3.4.4.	<i>Servidor de repositorios</i>	96
3.5.3.4.5.	<i>Servidor de aplicaciones web</i>	96
3.5.3.4.6.	<i>Servidor SRI</i>	97
3.5.3.4.7.	<i>Servidor MAPSERVER</i>	97
3.5.3.4.8.	<i>Servidor WEBSERVICE</i>	97
3.5.3.4.9.	<i>Servidor de Base de datos POSTGIS</i>	97
CAPÍTULO IV.....		99
4.	Gestión de la Red Local de Datos del GAD-Ibarra.....	99
4.1.	Establecimiento de Políticas de Gestión para la Red Local de Datos del GAD-Ibarra.....	99
4.1.1.	Introducción.....	99
4.2.	Implementación de Herramientas de Gestión en la Red Local de Datos del GAD-Ibarra.....	114
4.2.1.	Implementación dentro de la Gestión de Configuración.....	114
4.2.1.1.	Requerimientos para elección del software de gestión.....	114
4.2.1.1.1.	<i>Archivos principales de Nagios</i>	116
4.2.1.1.2.	<i>Directorios principales de Nagios</i>	117
4.2.1.1.3.	<i>Requerimientos hardware para Nagios</i>	117
4.2.1.2.	Diseño utilizado para implementar el modelo de gestión de red funcional. 118	
4.2.1.3.	Configuración del Gestor.....	119
4.2.1.3.1.	<i>Instalación y configuración del software de gestión Nagios</i>	120
4.2.1.3.2.	<i>Instalación de agente SNMP</i>	122
4.2.1.3.3.	<i>Instalación de PNP4Nagios</i>	123
4.2.1.3.4.	<i>Instalación de agente NRPE</i>	123
4.2.1.3.5.	<i>Instalación para el envío de correo electrónico</i>	124
4.2.1.3.6.	<i>Instalación para el envío de SMS</i>	126
4.2.1.4.	Instalación de agente SNMP en switches.....	126
4.2.1.4.1.	<i>Configuración de switches dentro de Nagios</i>	127
4.2.1.5.	Instalación de agente SNMP en enlaces inalámbricos.....	135
4.2.1.6.	Instalación de agente NRPE en servidores Linux.....	136
4.2.1.6.1.	<i>Funcionamiento General</i>	136

4.2.1.6.2.	<i>Instalación de NRPE.</i>	137
4.2.1.6.3.	<i>Configuración de servidores Linux dentro de Nagios.</i>	138
4.2.1.7.	Instalación de agente NSClient++ en servidores Windows.	139
4.2.1.7.1.	<i>Configuración de servidores Windows dentro de Nagios</i>	139
4.2.2.	Implementación dentro de la Gestión de Fallos.	140
4.2.2.1.	Gestión Proactiva.	141
4.2.2.1.1.	<i>Definición de umbrales.</i>	141
4.2.2.2.	Gestión de pruebas preventivas.	144
4.2.2.2.1.	<i>Pruebas de conectividad física.</i>	144
4.2.2.2.2.	<i>Pruebas de conectividad lógica.</i>	144
4.2.2.3.	Gestión Reactiva.	145
4.2.2.3.1.	<i>Detectar.</i>	145
4.2.2.3.2.	<i>Aislar.</i>	149
4.2.2.3.3.	<i>Diagnosticar.</i>	151
4.2.2.3.4.	<i>Corregir.</i>	152
4.2.2.3.5.	<i>Documentar.</i>	153
4.2.3.	Implementación dentro de la Gestión de Contabilidad.	153
4.2.3.1.	Parámetros de monitoreo.	153
4.2.3.2.	Parámetros de estado.	154
4.2.3.1.	Parámetros de chequeo.	155
4.2.4.	Implementación dentro de la Gestión de Prestaciones.	157
4.2.4.1.	Análisis del rendimiento general de la red.	157
4.2.4.1.1.	<i>Distribución de protocolos sin configuración de SNMP.</i>	158
4.2.4.1.2.	<i>Distribución de protocolos con configuración de SNMP.</i>	159
4.2.4.1.1.	<i>Throughput de la red.</i>	160
4.2.4.1.2.	<i>Resultados obtenidos con Wireshark y Ntop</i>	160
4.2.4.2.	Datos estadísticos del rendimiento de los recursos de la red en Nagios....	163
4.2.4.2.1.	<i>Rendimiento por áreas críticas</i>	164
4.2.4.2.2.	<i>Rendimiento en la Capa Núcleo.</i>	165
4.2.4.2.3.	<i>Rendimiento en la Capa Distribución.</i>	168
4.2.4.2.4.	<i>Rendimiento en la Capa Acceso.</i>	169
4.2.4.2.5.	<i>Rendimiento en Enlaces Inalámbricos.</i>	170
4.2.4.2.6.	<i>Rendimiento en servidores Virtuales.</i>	171

4.2.4.2.7. Rendimiento en servidores Físicos.....	172
4.2.4.2.8. Rendimiento en host.....	173
4.2.4.3. Reportes.....	173
4.2.5. Implementación dentro de la Gestión de Seguridad.....	178
4.2.5.1. Acceso y autorización al software de gestión.....	178
4.3. Manuales de Procedimientos.....	180
4.3.1. Introducción.....	180
4.3.2. Manual de procedimientos para la Gestión de Configuración.....	181
4.3.3. Manual de procedimientos para la Gestión de Fallos.....	187
4.3.4. Manual de procedimientos para la Gestión de Contabilidad.....	192
4.3.5. Manual de procedimientos para la Gestión de Prestaciones.....	196
4.3.6. Manual de procedimientos para la Gestión de Seguridad.....	200
CAPÍTULO V.....	203
6. Conclusiones y Recomendaciones.....	203
6.1. Conclusiones.....	203
6.2. Recomendaciones.....	205
Referencias:.....	208
Anexo A: Parámetros respecto al envío de SMS.....	212
Anexo B: Especificaciones Técnicas del Data Center del GAD-Ibarra.....	216
Anexo C: Resultados del monitoreo del tráfico de datos.....	226
Anexo D: Elección del software de gestión en base al estándar IEEE 830.....	228
Anexo E: Manual de Instalación y Configuración del Software de Gestión Nagios.....	246
Anexo F: Base de Datos para la Gestión de Fallos.....	310
Anexo G: Test de rendimiento de la red mediante Ntop y Wireshark.....	320
Anexo H: Simulación del proyecto implementado en la red del GAD-Ibarra con el software GNS3.....	332

ÍNDICE DE TABLAS

Tabla 1. Elementos de una red de telefonía celular.....	44
Tabla 2. Distribución de las Unidades del Edificio Principal.....	54
Tabla 3. Distribución de Unidades del Edificio Antiguo.....	56
Tabla 4. Equipos del Data Center.....	60

Tabla 5. Estándares utilizados en una infraestructura de cableado estructurado.....	62
Tabla 6. Descripción de Switches del GAD-Ibarra.....	65
Tabla 7. Servidores Físicos y Virtuales del GAD-Ibarra.....	71
Tabla 8. Dispositivos de red ubicados en el rack del edificio antiguo	73
Tabla 9. Elementos del rack de la casa de la Ibarreñidad.....	74
Tabla 10. Características del backbone de fibra óptica.....	77
Tabla 11. Distribución de VLAN.....	78
Tabla 12. Servidores Físicos y Virtuales en Funcionamiento del GAD-Ibarra.....	91
Tabla 13. Evaluación de Software de Gestión	115
Tabla 14. Requerimientos Hardware para Nagios.....	118
Tabla 15. Requerimientos del Software Nagios.....	121
Tabla 16. Plugins utilizados para switches.....	132
Tabla 17. Plugins utilizados para enlaces inalámbricos.....	136
Tabla 18. Plugins utilizados para servidores Linux	139
Tabla 19. Plugins utilizados para servidores Windows.....	140
Tabla 20. Umbrales para el Monitoreo.....	142
Tabla 21. Jerarquía de alertas que genera Nagios	150
Tabla 22. Parámetros de Monitoreo	154
Tabla 23. Parámetros de estado para dispositivos.....	155
Tabla 24. Parámetros de estado para servicios.....	155
Tabla 25. Parámetros de chequeo.....	156
Tabla 26. Parámetros de tiempo 24x7	156
Tabla 27. Parámetros de tiempo por horas de trabajo	157

ÍNDICE DE FIGURAS

Figura 1. Elementos de un modelo de gestión de red.....	14
Figura 2. Áreas del Modelo Funcional.....	16
Figura 3. Componentes involucrados en SNMP	29
Figura 4. Árbol de la Infraestructura MIB	32
Figura 5. Elementos que interactúan para el funcionamiento de SNMP.....	33
Figura 6. SNMP y Modelo de Comunicación TCP/IP	35
Figura 7. Formato de Mensaje SNMP.....	39
Figura 8. Mensajes SNMP	40
Figura 9. Estructura de una red GSM y principales interfaces entre sus elementos.....	45
Figura 10. Envío de SMS mediante un dispositivo móvil.....	48
Figura 11. Envío de SMS mediante un Módem GSM	50
Figura 12. Organigrama Estructural del GAD-Ibarra	53
Figura 13. Organigrama de la Dirección TIC.....	55
Figura 14. Topología física de la red de datos	64
Figura 15. Escenario de virtualización servidor HP BL 460 G6.....	67

Figura 16. Escenario de virtualización servidor HP BL 460 G6.....	68
Figura 17. Escenario de virtualización servidor HP BL 460 G8.....	69
Figura 18. Escenario de virtualización servidor HP 160 G5.....	70
Figura 19. Diagrama del backbone de Fibra óptica.....	76
Figura 20. Modelo Jerárquico de la red del GAD-Ibarra.....	80
Figura 21. Volumen de tráfico generado por el protocolo SSL.....	84
Figura 22. Volumen de tráfico generado por el protocolo FTP.....	85
Figura 23. Volumen de tráfico generado por el protocolo HTTP.....	85
Figura 24. Volumen de tráfico generado por la aplicación PostgreSQL.....	86
Figura 25. Volumen de tráfico generado por el protocolo RTP.....	86
Figura 26. Volumen de tráfico generado por el protocolo POP.....	87
Figura 27. Volumen de tráfico generado por el protocolo SIP.....	87
Figura 28. Volumen de tráfico generado por el protocolo IMAP.....	88
Figura 29. Volumen de tráfico generado por el protocolo DNS.....	88
Figura 30. Volumen de tráfico generado por el protocolo SMTP.....	89
Figura 31. Volumen de tráfico general de aplicaciones y protocolos utilizados.....	89
Figura 32. Mapeo de puertos del switch que interconecta los servidores.....	93
Figura 33. Estructura de Archivos Nagios.....	116
Figura 34. Diseño del Sistema de Gestión implementado.....	119
Figura 35. Representación del orden de Instalación.....	120
Figura 36. Agentes en Switches.....	126
Figura 37. Estructura de PNP4 Nagios.....	133
Figura 38. Diseño de Monitoreo de Servidores Linux.....	136
Figura 39. Comunicación entre Nagios y agente NSClient.....	139
Figura 40. Proceso de Gestión Reactiva.....	145
Figura 41. Detección de fallos en el mapa de la interfaz web.....	146
Figura 42. Envío de correo electrónico desde Nagios.....	147
Figura 43. Envío de mensaje de texto desde Nagios.....	148
Figura 44. Envío de correo electrónico desde Nagios.....	148
Figura 45. Envío de correo electrónico desde Nagios.....	149
Figura 46. Datos obtenidos sin configuración de SNMP.....	158
Figura 47. Datos obtenidos con configuración de SNMP.....	159
Figura 48. Tráfico capturado de Ntop.....	161
Figura 49. Tráfico capturado de Ntop.....	161
Figura 50. Tráfico capturado de Wireshak.....	162
Figura 51. Tráfico capturado de Wireshak.....	162
Figura 52. Tráfico capturado de Wireshak.....	163
Figura 53. Rendimiento de Nagios.....	164
Figura 54. Rendimiento de servicios del Switch Core.....	165
Figura 55. Rendimiento de servicios del Switch Core.....	166
Figura 56. Tráfico de interfaz del switch core.....	167
Figura 57. Rendimiento de servicios del switch de distribución.....	168
Figura 58. Tráfico de interfaz del switch de distribución.....	169
Figura 59. Rendimiento de servicios de switch de acceso.....	170

Figura 60. Rendimiento de servicios de los enlaces inalámbricos	171
Figura 61. Rendimiento de servicios de un servidor virtual.....	171
Figura 62. Rendimiento de servicios de un servidor físico	172
Figura 63. Rendimiento de servicios de un host	173
Figura 64. Vínculos para la generación de Reportes	173
Figura 65. Reporte de disponibilidad	174
Figura 66. Reporte de tendencia.....	174
Figura 67. Reporte de alertas.....	175
Figura 68. Resumen de reportes	176
Figura 69. Reporte en forma de histograma	176
Figura 70. Reporte de notificaciones.....	177
Figura 71. Iconos que generan reportes en PNP4Nagios	177
Figura 72. Permiso de acceso de los usuarios a vínculos de Nagios	179

ÍNDICE DE LÍNEAS DE CÓDIGO

Líneas de código 1. Configuración de plantilla a heredar por switches	128
Líneas de código 2. Configuración de plantilla a heredar por switches (1)	129
Líneas de código 3. Definición de sintaxis para switches	129
Líneas de código 4. Definición de grupos de switches	130
Líneas de código 5. Definición de sintaxis para plantilla de servicios.....	131
Líneas de código 6. Definición de sintaxis para comandos	131
Líneas de código 7. Definición de sintaxis para servicios	133
Líneas de código 8. Definición de sintaxis para plantilla de contactos.....	134
Líneas de código 9. Definición de sintaxis para contactos.....	134

RESUMEN

Actualmente el reto de las empresas u organizaciones es que sus servicios estén disponibles los 365 días del año, esto implica que los elementos de red funcionen eficazmente.

Por lo tanto, analizando la realidad del Gobierno Autónomo Descentralizado de San Miguel de Ibarra (GAD-Ibarra), este proyecto propone la implementación de un modelo de gestión de red funcional en áreas críticas de la red local de datos, el cual se basa en el estándar ISO, mediante herramientas de software libre con el objetivo de optimizar los recursos de la red. Permitiendo de esta forma actuar oportunamente ante cualquier evento que pueda suceder.

Mediante la implementación del software de gestión se podrá mantener monitoreados los dispositivos de red, las 24 horas del día, los 7 días de la semana, el cual permitirá tener una base de conocimiento sobre los incidentes que se presenten, facilitando al administrador de la red tomar a tiempo las medidas correctivas en los dispositivos más sensibles a fallas.

Con la presentación de manuales de procedimientos se establece una guía que facilita mantener disponibles los dispositivos de la infraestructura de red del GAD-Ibarra que se consideren prioritarios.

ABSTRACT

Nowadays, the challenge for enterprises or organizations is that their services are available 365 days a year; this implies the network elements function effectively.

Therefore, analyzing the reality of Autonomous Decentralized Government of San Miguel de Ibarra (Ibarra-GAD), this project proposes the implementation a model of management of functional network in critical areas of the local data network which is based on ISO standard, by tools of free software with the objective of optimize network resources, allowing this form perform opportunely in any event may happen.

By implementing management software may keep monitored the network devices, 24 hours a day, 7 days a week, which will allow having a base of knowledge about the incidents that occur, providing the network administrator take to time corrective action in the devices more sensitive to failure.

With the performance of manuals of procedures establishes a guide that facilitates keep available the devices of the network infrastructure of GAD-Ibarra are considered priorities.

PRESENTACIÓN

El proyecto que se presenta a continuación tiene como propósito implementar un Modelo de Gestión de Red Funcional en la Red Local de Datos del Gobierno Autónomo Descentralizado de San Miguel de Ibarra basado en el estándar ISO, con la finalidad de mantener monitoreada constantemente la red y de esta forma poder resolver problemas que se susciten, de una manera eficaz.

En el primer capítulo se presenta los antecedentes que ayudaron a la elección del proyecto.

El segundo capítulo detalla un breve análisis del modelo de gestión de red para fundamentar los lineamientos de implementación, además analiza el protocolo SNMP y el estándar IEEE 830 para elección del software de gestión, el mismo que debe cumplir con los requerimientos de la red.

En el tercer capítulo se realiza el levantamiento de información de la situación actual del estado físico y lógico de la red del GAD-Ibarra, para identificar las áreas críticas y poder conocer los equipos de mayor prioridad que soporten la habilitación del protocolo SNMP.

En el cuarto capítulo se describe el proceso de implementación de las herramientas de gestión en la red, donde como primer punto esta el desarrollo de políticas de gestión que cubran las necesidades de la entidad de acuerdo a sus requerimientos, como segundo punto realiza la implementación del modelo planteado en la red local de datos del GAD-Ibarra mediante herramientas de gestión en software

libre, además realiza la verificación del funcionamiento del modelo de gestión a través de una evaluación de pruebas.

Como último punto de este capítulo se realiza los manuales de procedimientos concatenados con las políticas de gestión, los cuales especifican como detectar posibles problemas que se presenten en el monitoreo de la red para poder aislar y resolver eficazmente los mismos sin pérdida de tiempo.

En el quinto capítulo se puntualizan las conclusiones y recomendaciones obtenidas durante el transcurso de desarrollo de la implementación del proyecto.

CAPÍTULO I

1. Antecedentes

1.1. Problema

El **Gobierno Autónomo Descentralizado de San Miguel de Ibarra** es una entidad pública que ha logrado construir una infraestructura tecnológica adecuada para resguardar los datos e información de los ciudadanos del cantón, la cual es administrada por el **Departamento de Tecnologías de Información y Comunicación (TIC)** que se encarga de ver problemas y cambios en la red, incrementando además nuevos servicios con la finalidad de ofrecer una mejor atención a los usuarios, conjuntamente ha ampliado la red interna de datos para ofrecer mayor conectividad dentro de la institución.

Actualmente el incremento de usuarios necesarios para trabajar en los distintos departamentos del GAD-Ibarra se ha vuelto obligatorio un aumento de equipos en la red como host, servidores, conmutadores y enrutadores, recursos que se ven afectados por cambios de estados que sobrepasan el nivel normal de funcionamiento, ocasionando problemas en el rendimiento y eficiencia de la red al no tener inventarios, notificaciones e historiales, esto provoca que no se pueda prevenir fallas a tiempo evitando molestias y retrasos en el trabajo de las personas que laboran en la entidad y prestan su servicio a la ciudadanía. La administración actual de la red carece de un modelo de gestión de red que sustente toda la información oportunamente para que el administrador pueda solucionar problemas que se presenten.

El **Departamento de Tecnología de la Información y Comunicación (TIC)** del GAD-Ibarra debe estar en constante evolución tecnológica ofreciendo una mejor disponibilidad y funcionalidad de la red, realizando registros e informes en forma sistematizada de los comportamientos que suceden en la red, por lo tanto es fundamental basarse en un modelo de gestión que pueda cubrir dichas necesidades para la monitorización de los equipos con la finalidad de tener conocimiento del estado de los recursos de la red, garantizando la estabilidad de la misma mediante detección, aislamiento y resolución de fallas.

La red de datos interna del GAD-Ibarra resguarda los datos e información de los ciudadanos del cantón, debido al aumento de recursos host, routers, switch y servidores se han presentado algunas eventualidades que salen fuera de los umbrales normales de funcionamiento, los cuales no se han podido resolver con anticipación por los administradores encargados por lo tanto el trabajo de grado busca implementar un sistema que se acople a un modelo de gestión de red funcional para mejorar el rendimiento de la red y por ende prestar mejor servicio a la ciudadanía.

1.2. Objetivos

1.2.1. Objetivos Generales.

Implementar el modelo de gestión de red funcional en áreas críticas de la red local de datos del GAD-Ibarra basado en el estándar ISO, mediante herramientas de software libre para optimizar los recursos de la red.

1.2.2. Objetivos Específicos.

- Analizar el modelo de gestión de red para establecer los criterios que se deben aplicar y adecuar a las necesidades de la red.
- Realizar un análisis de los recursos y estado actual de la red local de datos del GAD-Ibarra para identificar las áreas críticas.
- Determinar las políticas de gestión, de acuerdo al modelo planteado que se acoplen a las necesidades de la entidad, para monitorear los dispositivos de red a gestionar que soporten SNMP.
- Análisis y elección de las herramientas de gestión en software libre, en base al estándar IEEE 830 para su implementación en la red local.
- Establecer una jerarquía de alarmas dependiendo de los equipos de mayor prioridad y la importancia de los departamentos que conforman el GAD-Ibarra, con la finalidad de enviar notificaciones a través de correo electrónico y vía SMS a los administradores.
- Realizar pruebas del comportamiento del sistema de gestión instalado y corregir fallos en caso de existir.
- Realizar manual de procedimientos de cada uno de los parámetros de las áreas funcionales del modelo de gestión realizadas con las aplicaciones instaladas.

1.3. Alcance

El propósito del presente proyecto es implementar el modelo de gestión de red funcional en áreas críticas de la red local de datos del Gobierno Autónomo Descentralizado de San Miguel de Ibarra basado en el estándar ISO.

Para cubrir el modelo de gestión de red funcional, en la red se plantean las siguientes áreas que lo conforman: La gestión de configuración, comprenderá en realizar un análisis de la situación actual de la red de datos del GAD-Ibarra para conocer el estado físico y lógico en el que se encuentra con el objetivo de conocer los equipos de mayor prioridad y el orden de acuerdo a la importancia de los departamentos que conforman la entidad, para determinar los equipos que soporten la habilitación del Protocolo Simple de Administración de Red (SNMP).

Además para elegir el software de gestión se tomará como base el estándar IEEE 830, realizando un previo análisis y comparación de las funcionalidades y mejores características de software libres este debe ser completo, verificable, modificable, consistente, el mismo que debe cumplir con las necesidades de la red, como son monitorear los recursos de sistemas hardware (carga del procesador, espacio en disco, carga de memoria física, carga de memoria virtual, interfaces de red activas) y envío de notificaciones vía email y a través de mensajes cortos (SMS) para posteriormente realizar la configuración del software de gestión que tendrá como finalidad brindar la información requerida al administrador para poder diagnosticar, aislar y resolver oportunamente incidentes anormales de los elementos de la red, presentando inventarios, registro de topología de red de los equipos que se van a monitorear como host de mayor prioridad, switch, routers y servidores.

En la gestión de fallos se realizará el proceso para localizar, diagnosticar y corregir problemas en los componentes hardware de los equipos y evitar comportamientos anormales de funcionamiento determinando una jerarquía de alarmas dependiendo de los equipos de mayor prioridad y la importancia de los departamentos que conforman el GAD-Ibarra, a través del estándar RMON extensión de SNMP, las cuales puedan ser identificadas fácilmente por el administrador de la red a través del servicio de mensajes cortos (SMS) prioritarios y correo electrónico para que pueda intervenir inmediatamente a resolver el incidente evitando retardos en la disponibilidad y funcionamiento de la red, aumentando la confiabilidad y efectividad de la misma obteniendo reportes de los acontecimientos, facilitando la solución a los mismos problemas que se repitan en un futuro.

Para aplicar la gestión de prestaciones en la administración de la red se realizará la medición del rendimiento de los recursos de la red, colección de datos estadísticos, informes, historiales que ayudarán a mantener continuamente monitoreados los equipos de la red como también se presentará la elaboración de manuales de todas las configuraciones en el cual se especifique el funcionamiento de cada uno de los parámetros de las herramientas (hardware o software) utilizadas para la monitorización de los equipos, facilitando de esta manera la disponibilidad de la información la cual el administrador de la red pueda hacer uso en cualquier momento para solucionar los inconvenientes que se presenten detectando, aislando y resolviendo eficientemente los mismos, de igual manera si hubiese un incremento de equipos no tendría ningún problema en configurar y habilitar el protocolo SNMP.

La gestión de contabilidad que plantea el modelo se la realizará mediante el registro sobre la utilización de los recursos de la red.

La gestión de seguridad se encargará de proteger la red y la gestión de los equipos de accesos no deseados mediante el acceso, autorización y confidencialidad exclusiva del administrador de la red al sistema de gestión de los equipos y a la información, de igual forma será al mismo al que se le envíe las notificaciones de cualquier percance en la red.

Finalmente se realizará pruebas de funcionamiento del sistema implementado.

1.4. Justificación

El gobierno actual ha planteado el Código Orgánico de Organización Territorial, Autonomía y Descentralización, que en la sección cuarta, Gobierno y Democracia digital plantea que los gobiernos autónomos descentralizados propiciarán el uso masivo de las tecnologías de la información y la comunicación (TIC) en distintas áreas, incrementando la eficacia y la eficiencia individual y colectiva del quehacer humano, como también realizarán procesos para asegurar progresivamente a la comunidad la prestación de servicios electrónicos acordes con el desarrollo de las tecnologías es por eso el afán del GAD-Ibarra implementar un modelo de gestión de red, porque es un requerimiento fundamental para el mejor funcionamiento y disponibilidad de la red.

Se ha vuelto de mucha importancia la necesidad de conocer el estado de los recursos que conforman la red como son switch, routers, host y servidores, con el objetivo de prevenir fallos y detectar posibles efectos perjudiciales a la hora de prestar

ciertos servicios a los usuarios y anticiparse a ellos, preparándose para buscar soluciones y reaccionar a tiempo en el caso de que se produzcan.

Esto conlleva a implementar un modelo de gestión de red que se complementa con una herramienta de monitoreo OpenSource que se sustenta en el decreto Nro. 1014 que se establece como política del Estado para las entidades de la administración pública la utilización de Software Libre en sus sistemas y equipamientos informáticos. De esta manera se busca conseguir una visión en tiempo real del estado de los recursos de la red para su mejor rendimiento, como también logrando detectar rápidamente eventualidades por medio de notificaciones o alarmas.

Con la implementación del modelo de gestión de red se logrará prestar un mejor servicio en el que se verán beneficiados directamente los encargados de la administración de la red de datos al poder cumplir eficientemente su trabajo y sin problema y por ende la ciudadanía quienes dispondrán de un servicio constante.

CAPÍTULO II

2. Modelo de Gestión de Red Funcional Basado en el Estándar ISO

2.1. Introducción

El desarrollo de las telecomunicaciones está creciendo a un ritmo inmensurable, estar permanentemente conectado es esencial para las organizaciones, de esta forma se han vuelto más ágiles gracias a la adopción de nuevos métodos de trabajo, pero a medida que las operaciones críticas de la empresa se vuelven más dependientes de la red la necesidad de un sistema de gestión eficiente se ha convertido en un aspecto de gran importancia en el mundo de las comunicaciones, punto que los administradores de red quienes están constantemente pendientes del mantenimiento de sus redes deben tomar en cuenta.

Por lo tanto se propone realizar un modelo de gestión de red funcional a través de herramientas basadas en software libre que sean capaces de permitir una visión del estado de los dispositivos de la infraestructura de la red con el fin de maximizar su eficacia, productividad y disponibilidad, lo cual implica una vigilancia activa y pasiva para detectar y solucionar problemas, mejorando de esta forma el rendimiento de la misma.

2.2. Fundamentos de Gestión de Red

Las aplicaciones de gestión y de administración son herramientas que apoyan a una entidad en la gestión de su red. La administración y gestión de red son dos términos muy utilizados dentro de este proyecto por lo que se definirá a continuación:

2.2.1. Administración de red.

Es un proceso de planeación y control de todas aquellas actividades que manejan el funcionamiento de la red de datos de una organización, con la finalidad de obtener el máximo beneficio posible.

Tiene la capacidad de garantizar que el uso de la red se realice de manera eficaz, mejorando la continuidad en la operación de la red mediante mecanismos de monitoreo que ayudan a resolver problemas y tener monitoreados los recursos (Alarcón Ávila, 2007).

2.2.2. Gestión de red.

Según la ISO¹ (International Organization for Standardization) afirma a la gestión de red como: El conjunto de actividades necesarias para el control y supervisión de los recursos que ayudan al intercambio de información que circula por la red de datos, aumentando su funcionalidad y rendimiento (ISO / IEC , 1989).

Por lo tanto la gestión de redes tiene como propósito proveer la integración y coordinación del hardware, software y elementos humanos para monitorizar, probar,

¹ ISO.- Es una federación mundial de organismos nacionales de normalización que promueven el desarrollo de la estandarización

sondear, configurar, planear, organizar, analizar, evaluar y controlar los recursos de la red para garantizar un nivel de servicio, de acuerdo a un determinado coste. Además toma medidas que garanticen las operaciones de sus recursos en conformidad con los objetivos corporativos con el fin de evitar que llegue a funcionar incorrectamente degradando sus prestaciones (Escobar Vallejo, 2012).

Por los conceptos antes mencionados cabe recalcar que la administración es un complemento que forma parte de la construcción e implementación de un sistema de gestión de red.

2.2.2.1. *Objetivos de gestión de red.*

Las tareas de gestión se llevan a cabo por el personal responsable o por procesos automáticos de gestión. Según (Ding, 2010) afirma los siguientes objetivos para la gestión de red:

- Los recursos y servicios del sistema de gestión deben controlar, supervisar, actualizar e informar los estados del sistema.
- Los sistemas de gestión deben tener la capacidad de interpretar la información de gestión en una forma prácticamente manejable.
- El sistema de gestión debe detectar y corregir fallas en la red.
- Hacer un seguimiento de los recursos del sistema y usuarios de la red. Todos los recursos de la red y el uso del servicio deben ser registrados y reportados.
- Planificación y crecimiento del sistema de manera controlada.
- Finalmente el sistema de gestión de red debe garantizar un nivel de servicio en los sistemas de una organización el máximo tiempo posible, minimizando la

perdida que ocasionaría un incorrecto funcionamiento del sistema (Montes & León de Mora, 2002).

2.2.3. Necesidad de la gestión de redes.

Las razones por las que surge la necesidad de contar con un sistema de gestión en una red de telecomunicaciones son las siguientes (Romero, 2014):

- Entornos heterogéneos.
- Gran cantidad de recursos que se hacen indispensables para las organizaciones.
- Complejidad, debida a variedad y número de tecnologías distintas, gran número de fabricantes distintos.
- Aumento de expectativas de los usuarios: la red como entorno seguro, fiable y operacional.
- Prevenir, diagnosticar y resolver problemas de la red.
- Mejorar el servicio.
- Reducir indisponibilidad.

2.2.4. Elementos de un sistema de gestión de red.

Según como se especifica en el RFC² de Internet y otros documentos distribuidos un sistema de gestión comprende los siguientes elementos (Ding, 2010, págs. 45-48):

- Dispositivos Gestionados.
- Gestor.
- Agentes.

² RFC.- Requests for Comments (Petición de Comentario). Conforman la documentación de protocolos y tecnologías de Internet, siendo muchas de ellas estándares.

- Estación de gestión de red ó Network Management Station (NMS).
- Protocolo de Administración de red.
- Base de Información de Gestión (MIB).

2.2.4.1. Dispositivos Gestionados.

Equipamientos que se comunican con la red, con el propósito de ser monitoreados o controlados, se denominan elementos de red o dispositivos gestionados, tales como routers, switches, servidores, computadoras, impresoras, etc. Un elemento de red es un nodo de red que contiene un agente y es controlado por un gestor.

2.2.4.2. Gestor.

El gestor es la consola a través de la cual el administrador de red realiza funciones de gestión de red, genera operaciones de gestión (comandos, peticiones) y recibe (respuestas, notificaciones) de los agentes. Por lo general hay sólo unos pocos gestores en un sistema de gestión.

2.2.4.3. Agentes.

Son módulos software que recopilan y almacenan información local como (memoria, número de paquetes recibidos, enviados, direcciones IP, rutas, etc.) acerca de los dispositivos gestionados en el que reside y luego almacenan esta información en una base de datos de gestión, para finalmente proporcionarla a las entidades de gestión dentro del sistema de gestión de red (NMS) a través de un protocolo de gestión de red.

Un agente puede utilizar el protocolo de gestión de red para informar al sistema de gestión de un evento inesperado, además responde a los comandos del gestor y envía una notificación al administrador. Existen muchos agentes en un sistema de gestión.

2.2.4.4. Estación de gestión de red ó Network Management Station (NMS).

Son dispositivos independientes que sirven como interfaz entre el administrador y la red. Estos dispositivos ejecutan aplicaciones de gestión para el seguimiento y control de los elementos de red. Físicamente, los NMS son generalmente equipos de ingeniería con CPUs rápidas, memoria sustancial y abundante espacio de disco, aquí se encuentra instalados programas que permiten recibir información de administración proveniente de los dispositivos gestionados. Dentro de una red administrada debe haber por lo menos una NMS.

2.2.4.5. Protocolo de gestión de red.

Un protocolo de gestión se utiliza para transmitir información de gestión entre los agentes y las estaciones de gestión de red (NMS).

2.2.4.6. Base de Información de Gestión (MIB).

Una base de información de gestión (MIB) se deriva del modelo de gestión de red OSI/ISO, es un tipo de base de datos utilizada para gestionar los dispositivos en una red de comunicaciones. Se compone de una colección de objetos en una base de datos (virtual).

En la Figura 1 se muestra gráficamente representados los elementos básicos que conforman un sistema de gestión de red:

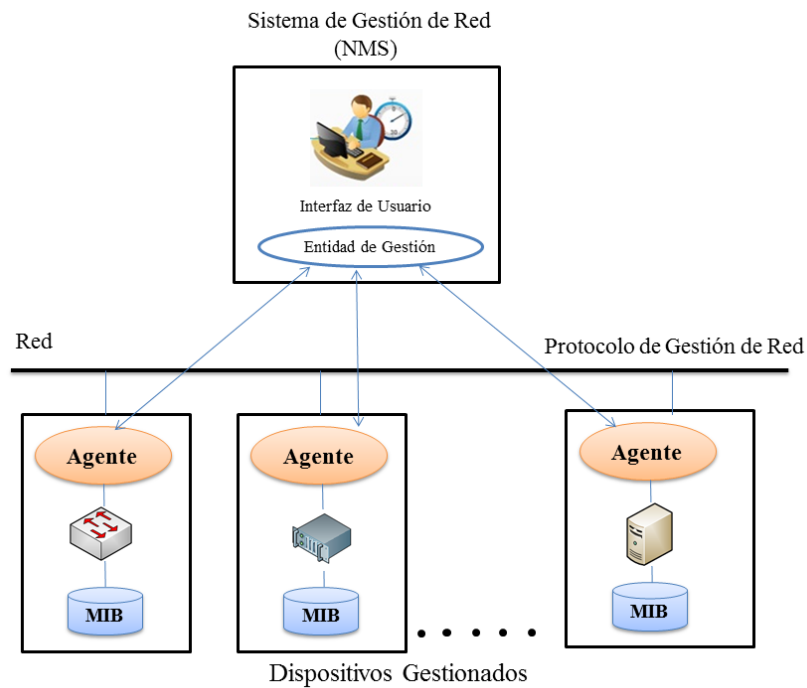


Figura 1. Elementos de un modelo de gestión de red

Fuente: (Ding, 2010)

2.2.5. Componentes de la gestión de redes.

La gestión de red se fundamenta en tres componentes que se nombran a continuación (Orozco, 2010, págs. 5-16):

2.2.5.1. Componente Organizacional.

Define la estructura para el proceso de gestión y la estrategia apropiada para llevarla a cabo de acuerdo con las necesidades de la entidad.

Dentro de este componente se conforma el grupo de gestión, estructurado alrededor de cuatro aspectos que son; control operacional, administración, análisis, planificación.

2.2.5.2. Componente Técnico.

Define las herramientas a utilizar para realizar la función de gestión y su implantación dentro de la infraestructura.

Existen muchas herramientas de gestión las cuales se basan en el paradigma gestor-agente. Para llevar a cabo una multitud de tareas los sistemas de gestión se basan en dos procedimientos que se nombran a continuación:

- ***Monitorización.-*** Busca mantener información del estado de los recursos gestionados. Particularmente pasivo.
- ***Control.-*** Toma información de la monitorización y actúa sobre el comportamiento de los elementos de la red gestionada. Particularmente activo, permite tomar medidas.

2.2.5.3. Componente Funcional.

Define las funciones de gestión que el componente organizacional debe ejecutar utilizando las herramientas de gestión.

Dentro de este componente la ISO propone una agrupación de competencias de la gestión de red en cinco grandes áreas funcionales que se detallan a continuación.

2.2.6. Modelo de gestión de red funcional basado en el estándar ISO.

La (ISO / IEC , 1989) y la UIT-T³ (Comité Consultivo Internacional Telegráfico y Telefónico (CCITT-UIT), 1992) fueron preparadas en estrecha colaboración y son técnicamente idénticas, donde han definido un modelo de gestión de red funcional el cual abarca las cinco áreas funcionales conocidas como FCAPS que es un acrónimo de Fallas (Fault), Configuración (Configuration), Contabilidad (Accounting), Rendimiento (Performance), y Seguridad (Security) como indica la Figura 2, áreas que definen las tareas de gestión de red (Ding, 2010).

En el presente proyecto se utilizará este modelo de gestión, porque sus distintas áreas ayudan al mejoramiento de la red de la entidad.

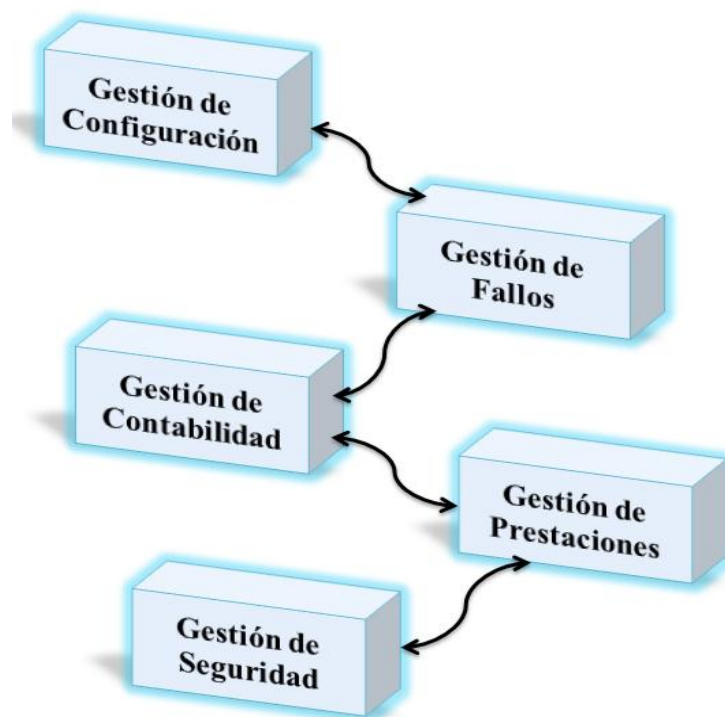


Figura 2. Áreas del Modelo Funcional

Fuente: (Jorquera, 2010)

³ UIT-T.- Organización encargada de la reglamentación y normalización de las telecomunicaciones

2.2.6.1. Gestión de Configuración.

La gestión de configuración se refiere a mantener información relativa al diseño y configuración actual de la red. Esta área es quizás la más importante de la administración de la red porque una configuración incorrecta puede hacer que la red no funcione en absoluto (Ding, 2010).

Además esta área de gestión está asociada con otras de las áreas funcionales FCAPS tales como; la gestión de fallos, es decir, los problemas suscitados en las redes no se pueden diagnosticar correctamente sin un previo conocimiento preciso de la configuración de la red, con la gestión de prestaciones, para recopilar información estadística, con la gestión de seguridad para detectar patrones sospechosos en la utilización de la red que pueden indicar un ataque de denegación de servicio (Clemm, 2007).

Dentro de las tareas básicas de la gestión de configuración se encuentran las siguientes (Ding, 2010):

- Facilitar la creación de controles.
- Supervisar y hacer cumplir las normas básicas de hardware y software específico.
- Conservar los datos de configuración y mantenimiento de un inventario actualizado de todos los componentes de la red.
- Registro e informe de cambios en las configuraciones, incluyendo la identidad del usuario.
- Configuración remota.
- Copia de seguridad de configuración de red y restaurarla en caso de fallos.

Esta área de gestión está relacionada con el funcionamiento detallado de la configuración de hardware y software como se explica a continuación:

- ***Gestión de configuración de hardware***

Es el proceso de crear y mantener un registro actual de todos los componentes de la infraestructura, incluyendo su documentación. Su objetivo es mostrar lo que hace la infraestructura e ilustrar las ubicaciones físicas y vínculos entre cada elemento, que se conocen como elementos de configuración.

- ***Gestión de configuración de software***

Dentro del proceso de gestión de configuración de software de red incluye:

- ✓ Identificación de la configuración

Es el proceso de identificación de los atributos que definen todos los aspectos de un elemento de configuración. Estos atributos se registran en la documentación de configuración.

- ✓ Control de cambios de configuración

Es un conjunto de procesos y la aprobación de etapas necesarias para cambiar los atributos de un elemento de configuración.

- ✓ Determinación del estado de configuración

Es la capacidad de registrar y reportar en cualquier momento las configuraciones asociadas con cada elemento de configuración.

✓ Configuración de autenticación

Se refiere a una auditoría de configuración funcional y física, donde la auditoría de la configuración funcional garantiza que se cumplan los atributos funcionales y de rendimiento de un elemento de configuración, mientras que una auditoría de configuración física asegura que un elemento de configuración está instalado de acuerdo con los requisitos de la documentación de diseño detallado.

2.2.6.2. Gestión de Fallos.

Esta área de gestión tiene como objetivo detectar, aislar y solucionar comportamientos anormales que afectan al funcionamiento y disponibilidad de la red gestionada, además realiza el mantenimiento, el análisis de los registros de fallos, secuencias de pruebas de diagnóstico y presentación de informes de fallos (Ding, 2010).

Además en esta área de gestión se establece alertas que son invocadas por umbrales establecidos previamente por el administrador es decir cuando se produce un fallo en un elemento gestionado de la red se enviará una notificación al administrador de la red.

La gestión de fallos debe ser capaz de identificar correctamente los sucesos y tomar una acción de forma automática, ya sea el lanzamiento de un programa o el software de notificación que permite al administrador tomar la debida intervención por medio del envío de un correo electrónico o un mensaje de texto SMS a un teléfono móvil.

Existen dos formas principales para llevar a cabo la gestión de fallos:

Gestión de fallos pasiva.- Se realiza mediante la recopilación de alarmas de dispositivos (normalmente a través de SNMP⁴). En este modo, el sistema de gestión de fallos sólo sabe si un dispositivo que está supervisando es lo suficientemente inteligente como para generar un fallo y reportar al software de gestión. Sin embargo, si el dispositivo que se está supervisando falla por completo o se bloquea, no se producirá una alarma y el problema no será detectado.

Gestión de fallos activa.- Consiste en la vigilancia activa de dispositivos gestionados a través de herramientas como PING para determinar si el dispositivo está activo. Si el dispositivo deja de responder, el seguimiento activo generará una alarma que muestra el dispositivo como no disponible y permite la corrección proactiva del problema.

Dentro de las funciones de la gestión de fallos se encuentra las siguientes (Orozco, 2010):

- Evitar el fallo antes de que suceda, aquí se encuentra la gestión proactiva y la gestión de pruebas preventivas, que se detalla a continuación:

- ***Gestión proactiva***

- ✓ Detección de fallos antes de que estos sucedan.

⁴ SNMP.- Protocolo de Gestión de Red que sirve para informar el estado de los dispositivos de red.

- ✓ Determinar umbrales de ciertos parámetros, y además monitorizar estos parámetros o programar notificaciones automáticas cuando estos umbrales sean superados.

- *Gestión de pruebas preventivas*

- ✓ Detectan fallos ocultos que no podrían detectarse normalmente.
- ✓ Suelen ser de efecto intrusivo: necesitan desactivación del servicio entre las pruebas están las siguientes: pruebas de conectividad, pruebas de integridad de datos, pruebas de integridad de protocolos, pruebas de saturación de datos, pruebas de saturación de conexiones, pruebas de tiempo de respuesta.

- Si el fallo ha sucedido, se conoce como gestión reactiva:

- *Detección de fallos*

La detección de fallos determina la causa de una avería, radica en el proceso de capturar indicaciones en forma de alarmas de (usuarios o de herramientas), acerca del desorden en las redes proporcionadas por los dispositivos que funcionan mal. El proceso de localización de averías es de importancia significativa debido a que la velocidad y la precisión del proceso de gestión de fallos dependen en gran medida en ella.

- *Aislamiento de fallos*

Se analiza una serie de indicaciones de fallos observados para encontrar una explicación de las alarmas. Esta etapa incluye la identificación de la causa que conduce a la propagación de un fallo y la determinación de la causa raíz. Una vez detectado,

aislar el componente que falla, reconfigurar la red para minimizar el impacto del fallo, informar del fallo a los usuarios del sistema y reparar el elemento que falla.

- *Diagnos de fallos*

Se refiere al seguimiento del fallo, observación de síntomas, elaboración de hipótesis basadas en la experiencia del administrador y en el registro de fallos anteriores, verificación de hipótesis donde se realiza un conjunto de pruebas que permiten aprobar y/o descartar las diferentes hipótesis.

2.2.6.3. Gestión de Contabilidad.

La Gestión de Contabilidad se basa en el registro del uso de recursos y servicios prestados por la red a los usuarios. Dentro de esta Gestión se menciona lo siguiente (Molero, Villaruel, Aguirre, & Martínez, 2010):

2.2.6.3.1. Funciones de la gestión de contabilidad.

A continuación se enumera las principales tareas y funciones realizadas por la gestión de contabilidad:

- Recolección de datos sobre la utilización de los recursos.
- Mantenimiento del registro de cuentas de usuario.
- Mantenimiento de estadísticas de uso.
- Ayuda a mantener el rendimiento de la red a un nivel aceptable.
- Definición de procedimientos para tarifación.

En la red del GAD-Ibarra no se aplicará el procedimiento de tarificación debido a que es una entidad sin fines de lucro.

2.2.6.3.2. *Recursos gestionados.*

En esta área se nombran algunos de los recursos gestionados (Molero, Villaruel, Aguirre, & Martínez, 2010, págs. 23-25):

- **Recursos de comunicación.-** Estos recursos están referidos a redes LAN, WAN, líneas dedicadas de datos, entre otros.
- **Hardware de computación.-** Están referidos a servidores, estaciones de trabajo.
- **Software.-** Está el software de servidores, aplicaciones de datos, entre otros.
- **Servicios.-** Son todos los servicios de información y servicios de comunicaciones comerciales disponibles.

2.2.6.3.3. *Consideraciones.*

A continuación se presenta algunas consideraciones a tomar en cuenta dentro de esta área de gestión (Guerrero Pantoja, 2011):

- Definir niveles de tráfico entrante y saliente en puntos críticos.
- Definir niveles de conectividad entre dispositivos.
- Comprobar la capacidad que aún posee libre un disco duro.
- Los niveles mostrados sobre el uso del procesador permite identificar la carga procesal a la que está siendo expuesto un dispositivo de red; niveles que permiten evaluar cambios o revisiones del flujo de trabajo y servicios ejecutados.

- La contabilización de alertas mediante los registros que los mismos generan permite evaluar cuáles son los eventos más recurrentes y establecer medidas para solventarlos.

Los puntos mencionados anteriormente se pueden evidenciar mediante reportes y gráficas que permiten al administrador contabilizar adecuadamente las medidas a tomarse según las necesidades.

2.2.6.4. Gestión de Prestaciones.

La gestión de prestaciones se refiere a evaluar el comportamiento y asegurar el correcto funcionamiento de los dispositivos gestionados y la efectividad de determinadas actividades, además, recoge y procesa los datos medidos para generar los informes correspondientes. En esta área de gestión, se determina los siguientes indicadores proporcionados para monitorizar adecuadamente las prestaciones de la red (Molero, Villaruel, Aguirre, & Martínez, 2010).

2.2.6.4.1. Medidas orientadas a servicios.

Se refiere a las medidas que permiten mantener los niveles de determinados servicios para satisfacción de los usuarios. Donde se encuentra los siguientes aspectos:

- **Disponibilidad:** Es el porcentaje de tiempo que una red, un dispositivo o una aplicación se encuentra disponible para el usuario.
- **Tiempo de respuesta:** Tiempo que requieren los datos para entrar en la red, ser procesados por sus recursos y salir de la red es decir cuánto tarda en aparecer la respuesta en el terminal del usuario cuando éste realiza una acción.

- **Fiabilidad:** Porcentaje de tiempo en que un dispositivo de red funcione correctamente bajo ciertas condiciones específicas.

2.2.6.4.2. *Medidas orientadas a eficiencia.*

Se refiere a las medidas que permiten mantener el grado de utilización de recursos y servicios al mínimo costo posible.

- **Prestaciones (throughput):** Es la capacidad teórica máxima de los recursos de una red. Por lo tanto, es útil realizar un seguimiento de medidas en el tiempo, para conseguir una visión aproximada de la diferencia entre las demandas reales de la red y las previstas y detectar puntos probables de problemas de prestaciones.
- **Utilización:** Porcentaje de la capacidad teórica de un recurso que se está utilizando durante un periodo de tiempo y es empleado para ubicar posibles áreas de congestión en la red.

2.2.6.4.3. *Funciones de gestión de prestaciones.*

A continuación se puntualizan las funciones o tareas de esta área de gestión:

- Capturar los datos o variables indicadoras de rendimiento, tales como: tasa de datos efectiva de la red, los tiempos de respuesta a los usuarios, entre otros, recursos (utilización de la CPU, memoria disponible, la utilización de disco, puertos) y comparar esta información con los valores normales y/o deseables para cada uno.
- Analizar los datos para determinar los niveles normales de rendimiento.

- Establecer indicadores de problemas en el rendimiento de la red, en caso de quebrantarse.
- Determinar un sistema de procesamiento periódico de datos de desempeño acerca de los distintos equipos en la red para su estudio permanente.
- Generar informes y estadísticas.

2.2.6.5. Gestión de Seguridad.

La gestión de seguridad se refiere al conjunto de funciones que protege las redes de accesos no autorizados, por lo que se relaciona con la generación, distribución y almacenamiento de claves de cifrado, información de contraseñas. Se encarga también de proteger los equipos de comunicación, servidores y estaciones de trabajo de posibles ataques provenientes de terceros para mantener la integridad del sistema (Ding, 2010).

2.2.6.5.1. Funciones de gestión de seguridad.

Dentro de las funciones y tareas que debe cumplir esta área de gestión se puntualizan algunas de ellas a continuación (Molero, Villaruel, Aguirre, & Martínez, 2010):

- Monitorear la red o el sistema frente ataques.
- Encriptado de la información.
- Establecimiento de procedimientos de autenticación.
- Implementación de medidas de seguridad.
- Mantenimiento de la información de seguridad.
- Control de acceso a los recursos.

- Proteger la información confidencial mediante la configuración de directivas de cifrado.
- Mantener reportes de intentos de intrusiones para su posterior análisis.

2.2.6.5.2. *Ataques en la gestión de seguridad.*

A continuación se nombra algunos ataques que pueden ser ejecutados hacia el hardware o software dentro de esta gestión:

- **Interrupción.-** La interrupción de un recurso de software ó hardware, como puede ser un equipo de comunicaciones o un servidor de archivos. Es decir, por ejemplo: Existen técnicas de Hacking que son utilizadas por usuarios malintencionados para apagar servidores de datos, de forma que sea inaccesible la información que contienen.
- **Intercepción.-** Intercepción de un usuario no autorizado que logra entrar a través de una computadora a la red para violar la integridad de los datos. Por ejemplo existen usuarios que se introducen a las redes por medio de cables de red o suplantando identidades de red, para ejecutar actos destructivos contra el equipamiento y/o el software.
- **Modificación.-** Cuando un usuario no autorizado, luego de tener acceso a los datos de la red los modifica.

2.3. **Modelo de Gestión Internet o TCP/IP**

TCP/IP presenta el monitoreo y control para mejorar la administración de la red donde; el primero se basa en observar el comportamiento de los dispositivos que conforman una red, para detectar problemas y mejorar su funcionamiento, y el segundo

trata de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras esta en operación, para mejorar el funcionamiento y reparar fallos.

En el modelo TCP/IP, SNMP es el protocolo de gestión de red que emplea los servicios ofrecidos por TCP/IP y que ha llegado a convertirse en un estándar de la ISO en el área de comunicación de datos para la administración de redes. (Hernández Escobar, 2006).

2.4. Protocolo Simple de Gestión de Red (SNMP)

2.4.1. Definición.

Es un protocolo de capa aplicación basado en la arquitectura TCP/IP, este hace posible el intercambio de información de gestión entre dispositivos de red. SNMP permite a los administradores de red supervisar la operación de la red, configurar equipos, encontrar y resolver fallos, planificar el crecimiento de la red, analizar prestaciones de los equipos, acceder a la información de productos de diferentes fabricantes de una misma manera, desarrollando una herramienta común de monitoreo (Ding, 2010).

A través de este protocolo se puede administrar de forma remota una red informática mediante el sondeo y el establecimiento de los valores terminales, de esta forma obtener información de los dispositivos de red como memoria libre, uso de CPU, detección de errores, establecimiento de alertas, estado de funcionamiento entre otros.

2.4.2. Componentes de SNMP.

SNMP posee los siguientes componentes principales que se puntualizan a continuación, los cuales interactúan entre sí para establecer su funcionamiento como se observa en la Figura 3:

- Estación de Gestión de red (NMS).
- Agente.
- Protocolo de Gestión de red.
- Una base de información de gestión (MIB).

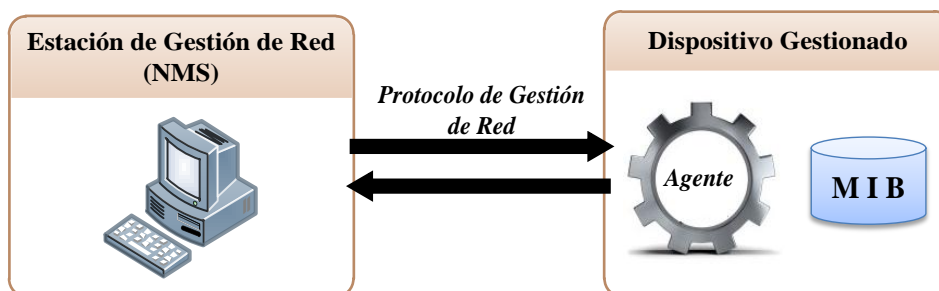


Figura 3. Componentes involucrados en SNMP

Fuente: (Guerrero Pantoja, 2011)

Estos componentes interactúan con los operadores humanos y desencadenan las acciones necesarias para llevar a cabo las tareas por ellos invocadas o programadas (Guerrero Pantoja, 2011).

Los componentes NMS y agente se los definió en el punto 2.2.4 por lo tanto en esta sección se detallará un poco más acerca del protocolo de gestión de red, la MIB y otros componentes que forman parte de SNMP:

2.4.2.1. Estructura de la información de gestión (SMI).

Define el marco general por el que se construyen las MIBs, especifica los tipos de datos que se pueden utilizar en una MIB. Dichas estructuras que construyen las MIBs, están formateadas en ASN.1⁵ (Abstract Syntax Notation One), indicando cómo debe ser el nombre, la sintaxis y el método de codificación de los datos para su transmisión por la red. SMI debe proveer:

- Un mecanismo para definir la estructura de una MIB.
- Una técnica estándar para definir objetos individuales, incluyendo la sintaxis y el valor de cada uno de ellos.
- Un mecanismo para codificar el valor de cada objeto.

SMI se subdivide en tres partes: definiciones del módulo, definiciones de objetos, y definiciones de notificación:

Definiciones del módulo se emplean para describir los módulos de información. Un macro ASN.1, **MÓDULO-IDENTIDAD**, se utiliza para transmitir en forma concisa la semántica de un módulo de información.

Definiciones de objetos describen objetos administrados. Una macro ASN.1, **TIPO DE OBJETO**, se utiliza para transmitir en forma concisa la sintaxis y la semántica de un objeto administrado.

⁵ ASN.1.- Abstract Syntax Notation One (Notación Sintáctica Abstracta 1) es una norma que utiliza SNMP para representar objetos gestionados.

Definiciones de notificación (también conocidos como "trampas") se utilizan al describir transmisiones no solicitadas de información de gestión. Una macro ASN.1, TIPO DE NOTIFICACIÓN, expresa concisamente la sintaxis y la semántica de una notificación.

2.4.2.2. Base de información de gestión (MIB).

Para SNMP, la MIB contiene información sobre todos los dispositivos de la red en forma de instancias de objetos, que se describen utilizando el lenguaje formal ASN.1. Gracias a este lenguaje, se pueden acoger las diferentes incompatibilidades en la representación de información que utilizan diferentes fabricantes. Cada uno de estos objetos se corresponde con un dispositivo gestionado, cuyas características están definidas en sus propiedades o valores.

La base de datos MIB está organizada en forma de jerarquía de objetos. Esta jerarquía está compuesta por una raíz sin nombre de la que sostiene diferentes organizaciones de estandarización, como, por ejemplo, iso, ccitt o joint-iso ccitt. En los niveles más bajos de esta jerarquía se encuentran las organizaciones asociadas y diferentes fabricantes, de forma que pueden definir ramas privadas que incluyan objetos gestionados para sus propios productos. Los sistemas no estandarizados suelen incluirse como objetos situados en ramas experimentales del árbol MIB (Molina, 2010, pág. 604).

2.4.2.2.1. Identificación de objeto (OID).

Un OID de objeto se compone de una serie de números enteros basados en los nodos en el árbol, separados por puntos (.). Aunque hay un formato legible eso es más

amigable que una cadena de números, esta forma no es más que una serie de nombres separados por puntos, cada uno representando un nodo del árbol. Se puede utilizar los números en sí, una secuencia de nombres que representan los números (Douglas & Schmidt, 2005). En la Figura 4 se puede observar un ejemplo:

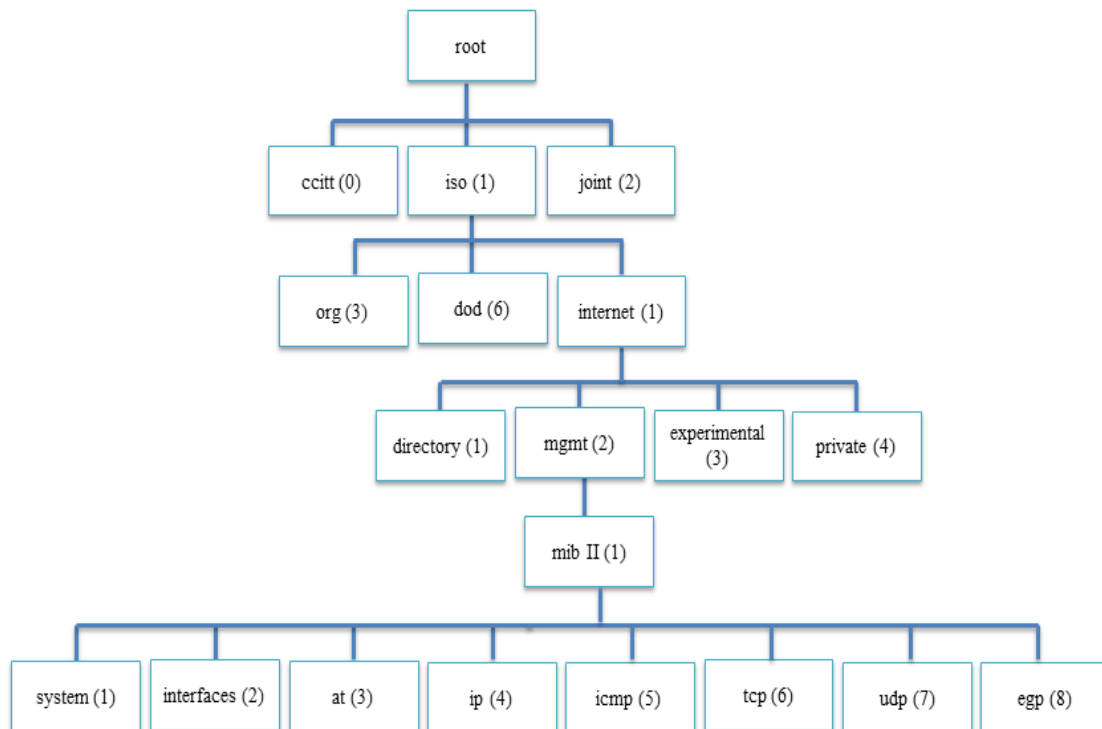


Figura 4. Árbol de la Infraestructura MIB

Fuente: (Solís Álvarez, 2014)

El OID numérico `.1.3.6.1.2.1.1.1` y el mismo OID en modo texto `iso.org.dod.internet.mgmt.mib-2.system.sysDescr` es un OID que está debajo de MIB-II, el cual mantiene información acerca del sistema como su marca, modelo, SO, etc.

2.4.2.3. Comunidad SNMP.

Este concepto de comunidad SNMP se refiere a establecer comunicación entre un conjunto de agentes y gestores. A las comunidades se les asignan nombres, de tal forma

que este nombre junto con cierta información adicional sirva para validar un mensaje SNMP.

2.4.3. Funcionamiento de SNMP.

En la Figura 5 se muestra cómo interactúan los componentes de SNMP:

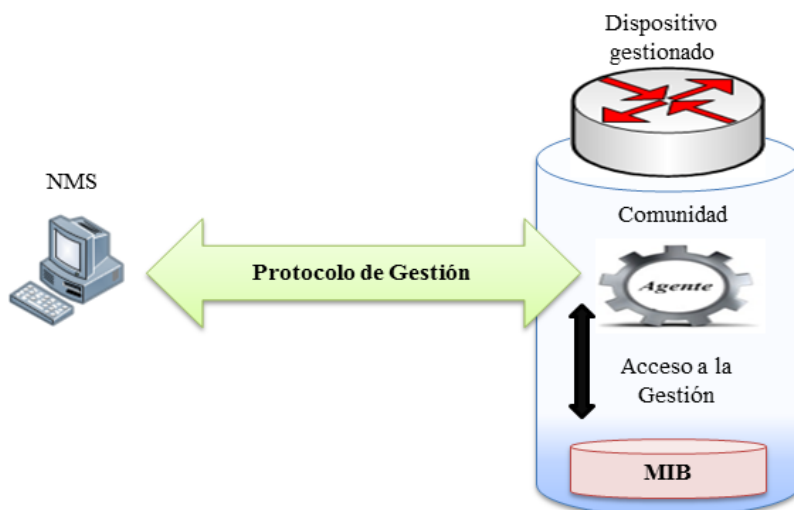


Figura 5. Elementos que interactúan para el funcionamiento de SNMP

Fuente: (Abeck, 2009)

En lugar de definir muchas operaciones, SNMP utiliza el paradigma de obtención y almacenamiento. El cual el administrador envía solicitudes de obtención y almacenamiento de valores en variables.

Toda la información de administración y monitorización de los dispositivos de la red que usan SNMP se almacena en una base de datos conocida como MIB. Esta base de datos está estructurada formando una jerarquía de objetos que poseen unas propiedades o valores como se explicó en el punto 2.4.2.1. El protocolo SNMP define tres operaciones básicas sobre esta base de datos: obtener un valor de un objeto para monitorear un dispositivo (read), almacenar un valor en un objeto para administrar un

dispositivo (write) o informar de un suceso producido en un equipo gestionado sin necesidad de una petición previa (trap). Además para el caso de lectura y escritura, se utilizan comunidades distintas (aunque pueden ser del mismo nombre, se deben definir por separado).

Se fundamenta en el intercambio de mensajes entre la parte NMS, que actúa como servidor el cual es un software SNMP gestor y otra parte cliente de SNMP que consiste en un software SNMP agente que mantiene en cada dispositivo gestionado información acerca de su estado y configuración.

El proceso de intercambio de mensajes puede ser iniciado por la estación de gestión o por el agente (cuando no existe una petición previa por parte de la estación de gestión). Por lo tanto existen dos formas de empezar la comunicación; la primera cuando la NMS pide la información que requiere a un dispositivo gestionado específico, el agente verifica el pedido si es auténtico y responde con la información de gestión que le ha sido solicitada para la comunidad a la que pertenecen; donde una comunidad es un dominio administrativo de agentes y gestores SNMP. La segunda forma es cuando el agente envía información de un evento suscitado en el sin que sea pedido con anterioridad por la NMS (Bastidas F & Ushiña G, 2010)

2.4.3.1. Funcionamiento de SNMP en relación a la pila de protocolos

TCP/IP.

SNMP funciona bajo TCP/IP, lo cual facilita que se pueda gestionar desde un sistema central cualquier dispositivo de una red de datos sea esta LAN, WAN, WLAN o Internet. El modo sin conexión se eligió en parte para simplificar la implementación de

SNMP y porque sin conexión suele ser la forma preferida para aplicaciones de gestión, debido a la necesidad de comunicarse con muchos agentes.

En la Figura 6 se indica la pila de protocolos TCP/IP sobre la cual se realiza la comunicación SNMP. Cuando un NMS o un agente desean realizar una función SNMP (por ejemplo, una petición o trampa), los siguientes eventos ocurren en la pila de protocolos (Douglas & Schmidt, 2005):

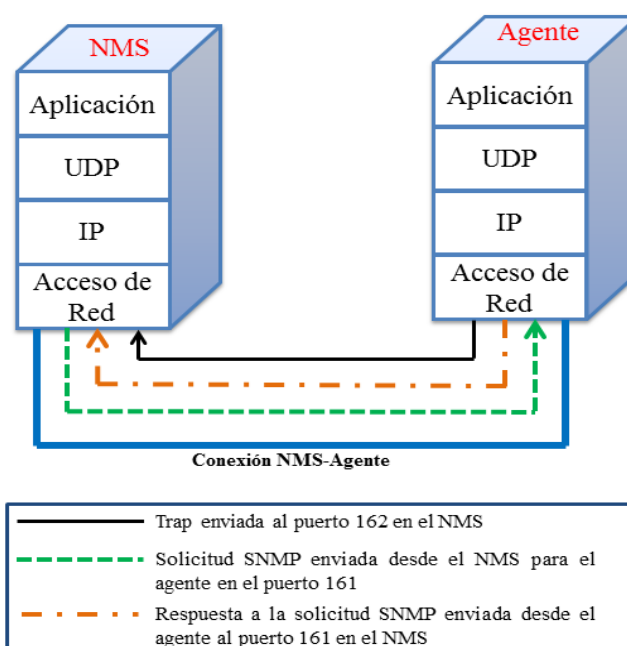


Figura 6. SNMP y Modelo de Comunicación TCP/IP

Fuente: (Douglas & Schmidt, 2005)

Empezando con la capa de aplicación esta ofrece a un usuario final servicios necesarios para llevar a cabo las actividades SNMP. La aplicación SNMP (NMS o agente) decide la actividad que va a realizar. Por ejemplo, puede enviar una solicitud SNMP a un agente, enviar una respuesta a una solicitud SNMP (este sería enviado desde el agente), o enviar una trampa a un NMS, tales como información de estado operador solicitante para un puerto de un switch Ethernet.

Dentro de la siguiente capa SNMP utiliza el protocolo UDP (Protocolo de Datagrama de Usuario- User Datagram Protocol) para el transporte de datos entre gestores y agentes. UDP, fue elegido sobre el Protocolo de Control de Transmisión (TCP), ya que posee características como el ser no orientado a conexión y no confiable, el cual posee la ventaja de requerir pocos gastos generales, sin embargo, gracias a esto, SNMP puede ejercer sus operaciones en tiempo real y con mínimo impacto en el rendimiento de la red. En el caso de que se produzcan pérdidas de paquetes por cualquier motivo, la corrección de errores estará a cargo de la aplicación NMS. Para detectar si existe pérdida de paquetes la aplicación puede basarse en el método de tiempo de espera. El NMS envía una petición de UDP a un agente y espera una respuesta, si el tiempo de espera ha superado el valor umbral, entonces el NMS asume que el paquete fue perdido y retransmite la petición si así lo desea (Castañeda Villarreal, 2011).

La cabecera UDP contiene, entre otras cosas, información del puerto destino del dispositivo al que está enviando la solicitud o trampa. El puerto de destino será o bien 161 (consulta) o 162 (trampa).

La capa IP, es la responsable de entregar el paquete SNMP hacia el host destino identificado por una dirección IP.

La capa MAC (Media Access Control o Control de Acceso al Medio), evento final que debe ocurrir para que un paquete SNMP pueda llegar a su destino, es para que traspase a la red física, donde se puede dirigir a su destino final. La capa MAC se compone de los controladores de hardware y dispositivos reales que ponen sus datos en

una pieza física, tal como una tarjeta Ethernet. La capa MAC es también responsable de recibir paquetes de la red física y el envío de vuelta hasta la pila de protocolos de modo que puedan ser procesados por la capa de aplicación (SNMP, en este caso).

SNMP se ha implementado a través de TCP, para situaciones de casos especiales en los que alguien está desarrollando un agente para una pieza de propiedad de un equipo específico. En una gran gestión red, SNMP sobre TCP es una mala idea. SNMP está diseñado para trabajar con redes que están en problemas.

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:

2.4.4. Versiones SNMP.

Varias versiones de SNMP se han desarrollado. Algunos de ellos se han convertido en estándares de la industria, tales como SNMP versión 1 (SNMPv1), SNMP versión 2 basado en la comunidad (SNMPv2c) y SNMP versión 3 (SNMPv3). Estas versiones tienen un número de características en común que ayudan a la evolución del protocolo, las cuales se describen a continuación (Ding, 2010):

2.4.4.1. *SNMP versión 1.*

La primera versión de SNMP se estandarizó en 1990 la cual se describe en los RFC 1155, 1157, y 1212, fue diseñado como una solución a los problemas de comunicaciones entre diferentes tipos de redes. Existen tres comunidades en SNMPv1:

de sólo lectura, lectura y escritura, y trap. Además cabe recalcar que mientras SNMPv1 es histórico, todavía es la aplicación principal que muchos vendedores apoyan.

Presenta un mecanismo de autenticación trivial entre el agente y el gestor, basado en nombres de comunidad y perfiles de comunidad, los mismos que viajan en texto plano provocando que un usuario no autorizado tenga acceso a información de la red, quedando vulnerable a cambios de configuración y detección de los dispositivos de red vía remota (Hidalgo Crespo & Vergara Cueva, 2013).

2.4.4.2. SNMP versión 2.

La segunda versión de SNMP se estandarizó en 1996 y se describe en los RFC 2578, 2579, 2380, 3416, 3417, y 3418. SNMPv2 es una evolución del SNMPv1 con mejoras notables en lo que se refiere a cantidad de información, interacción entre los diferentes dispositivos de red, monitorización remota; en redes que no están conectadas directamente a la estación de administración y eficiencia de administración de red. Funciona de manera similar a la versión anterior y mantiene el mismo mecanismo de seguridad (Hidalgo Crespo & Vergara Cueva, 2013).

Cuando se habla de SNMPv2, se refiere a la versión actualizada (SNMPv2c). SNMPv2c (la versión basada en la comunidad SNMP 2) es un marco experimental que complementa a SNMPv2.

2.4.4.3. SNMP versión 3.

Es la última versión de SNMP se estandarizó en el año 2002, su principal contribución a la gestión de red es la seguridad. Se añade soporte para la autenticación y

el cifrado de la comunicación entre entidades gestionadas. Se describe en RFC 3412, 3414, y 3417. A pesar del aumento de la seguridad de SNMPv3, SNMP sigue siendo en gran parte un protocolo de monitoreo para obtener información.

2.4.4.4. Partes de la trama del mensaje SNMP.

En la Figura 7 se puede observar la trama que envía el NMS al agente, la cual lleva la información de la versión de SNMP utilizada, la comunidad y el tipo de mensaje (que puede ser un Get Request, Get Next Request, Get Response, Set Response o Trap).

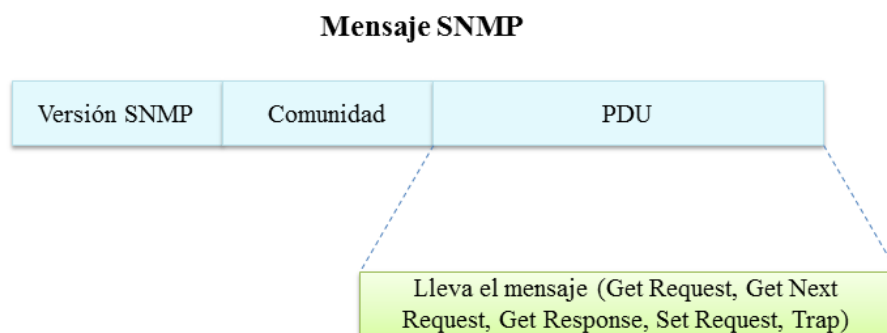


Figura 7. Formato de Mensaje SNMP

Fuente: (Solís Álvarez, 2014)

2.4.4.4.1. Mensajes enviados por SNMP.

En la Figura 8 se explica como el NMS envía un mensaje **Get Request** solicitando al agente para que le envíe valores específicos contenidos en la MIB, el agente devuelve un **Get Response** con los valores solicitados, en seguida el NMS envía un **Get Next Request** solicitando el siguiente valor del objeto contenido en la MIB del agente y este a su vez responde de nuevo con un **Get Response**, luego el NMS envía un **Set Request** al agente para que actualice los atributos de un objeto y este envía un **Get Response**. O puede ser el envío de un **Trap** generado por el agente si previa petición

donde informa de fallos como (como pérdida de la comunicación, caída de un servicio, problemas con la interfaz, etc).

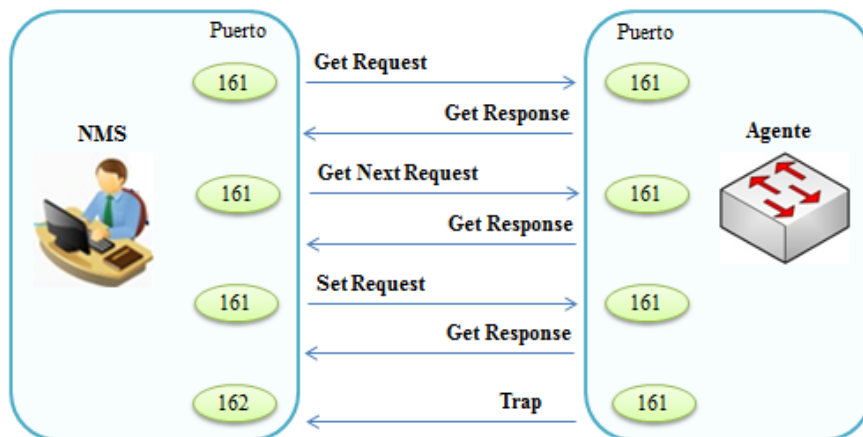


Figura 8. Mensajes SNMP

Fuente: (Castañeda Villarreal, 2011)

Además en SNMP versión 2 emite un mensaje **Get Bulk Request** el cual obtiene una tabla de valores de variables.

2.5. Monitorización Remota RMON

RMON es un estándar abierto administrado por la Internet Engineering Task Force (IETF) y está interrelacionado con SNMP estos son estándares de redes que permiten capturar información en tiempo real a través de toda la red.

Características puntuales de la monitorización remota:

- Accede en forma remota a la información empleando SNMP.
- La información se almacena en un MIB de gestión llamada MIB RMON.
- Permite detección local de fallos e informa al gestor.

2.6. Virtualización

Es una tecnología que permite ejecutar varias máquinas virtuales con diferentes sistemas operativos en una misma máquina física. Actualmente el tipo de virtualización que se está implementado es la creación de máquinas virtuales, estas se comunican con la maquina física a través de la capa de virtualización, cada una de estas máquinas virtuales estará aislada de las otras y se mapeará desde el hardware, la capacidad de procesamiento, memoria, dispositivos de red y discos asociados a cada una de ellas.

La capa de virtualización aísla las máquinas virtuales de los sistemas operativos anfitriones y, por tanto, de las dependencias de estos referidas al hardware. Los recursos asociados a una máquina virtual pueden ser modificados, debido a que por necesidades de computación o conexión, sea necesario asociar más cantidades de procesamiento, memoria, almacenamiento o dispositivos de red de una máquina virtual.

Estas operaciones, dependiendo de la solución utilizada, se podrán realizar con la máquina virtual en funcionamiento o será necesario pararla, añadir más recursos y, después, volver a iniciarla (Raya González, Raya Cabrera, Santos González, & Martinez Ruiz, 2010, págs. 11-12).

2.6.1. Máquinas virtuales.

Una máquina virtual es un software que emula un ordenador, es decir, es como tener un ordenador dentro de otro ordenador, pero funcionando en forma virtual. Las máquinas virtuales no tiene procesador, memoria, conexiones de red, puertos, discos duros, etc., únicamente lo simulan.

2.7. Software de gestión de redes

Un software de gestión es utilizado para conocer los puntos más débiles de la infraestructura de red es decir (servidores con demasiada carga, enlaces que se saturan regularmente, etc.). Determina equipos o servicios donde se produce la mayor cantidad de fallos, saber en el momento si algo está fuera de lo normal (no necesariamente un mal funcionamiento).

2.8. Estándar IEEE 830 para elección del software de gestión

El estándar IEEE Std. 830-1998 es el encargado de proporcionar normas para la creación de la Especificación de Requisitos Software (ERS) que debe estructurarse en base al requerimiento del software a utilizarse.

La ERS es una descripción del comportamiento del sistema que se va a desarrollar es decir presenta características como; correcta, completa, consistente, modificable, utilizable durante las tareas de mantenimiento y uso (Monferrer Agút, 2014).

2.8.1. Especificación de requisitos para el software de gestión.

A continuación se indica los requisitos pertinentes para elegir el software de gestión que se necesita:

2.8.1.1. Introducción.

En esta parte se proporcionará una introducción de todo el documento y consta de las siguientes subsecciones:

2.8.1.2. Propósito.

Se define el propósito del documento ERS y se especifica a quien va dirigido.

2.8.1.3. Descripción general.

Dentro de esta sección se describe todos los factores que afectan al producto y a sus requisitos, además de establecer los lineamientos en las subsecciones de: perspectiva del producto, funciones del producto, restricciones, requisitos específicos, requisitos funcionales y finalmente una valorización.

2.8.1.3.1. Valorización de los requerimientos.

Después de haber determinado los requerimientos para la selección del software, se procede a establecer un puntaje para cada requerimiento y poder encontrar la mejor solución para la implementación de este proyecto.

2.9. Red de telefonía celular

Es importante introducir el término celular, porque es en el cual se basan todos los sistemas de telefonía móvil. Entre las principales características de un sistema celular son las siguientes; gran capacidad de usuarios, utilización eficiente del espectro, amplia cobertura.

2.9.1. Estructura de una red de telefonía celular.

(Huidobro Moya, 2012) Afirma: “La Unión Internacional de Telecomunicaciones (UIT) define en el Reglamento de Radiocomunicaciones el servicio móvil como el servicio de radiocomunicaciones que se presta entre estaciones móviles y terrestres o entre estaciones móviles” (pág. 68).

En la Tabla 1 se describe los elementos de esta estructura (Huidobro Moya, 2012, págs. 68-70):

Tabla 1. Elementos de una red de telefonía celular

Elemento	Descripción
Estaciones Móviles (MS)	Dispositivos que proporciona el servicio a los usuarios. Cada estación móvil puede funcionar en modo emisor, receptor o en ambos modos.
Estaciones Base (BTS)	Los teléfonos móviles utilizan una red de estaciones base que envían y reciben llamadas y otros servicios móviles, las estaciones base deben estar ubicadas cerca de los usuarios de teléfonos móviles para permitir una buena calidad en la recepción. Se encargan de mantener el enlace radioeléctrico entre la estación móvil y la estación de control de servicio durante la comunicación.
Estaciones de Control (BSC)	Realiza las funciones de gestión y mantenimiento del servicio. Una tarea específica consiste en la asignación de estaciones base en un sector, dentro de un área de cobertura, a las estaciones móviles que se desplazan por el sector.
Centros de Conmutación (MSC)	Son elementos de las redes de comunicaciones móviles que tienen como función interconectar usuarios de la red fija con la red móvil, o usuarios de la red móvil entre sí.

Fuente: (Huidobro Moya, 2012)

2.9.2. Arquitectura de una red GSM⁶.

Una red GSM se organiza como un conjunto de células radioeléctricas continuas que proporcionan cobertura completa al área de servicio. Cada una de estas células pertenece a una estación base (BTS), que opera en un conjunto de canales de radio diferentes a los usados en las células adyacentes y que se encuentran distribuidas según un plan celular de frecuencias.

⁶ GSM.- Sus siglas en inglés (Global System for Mobile communications) es decir sistema global para las comunicaciones móviles, es un estándar de comunicación para la telefonía móvil, que utiliza la combinación de satélites y antenas terrestres.

La Figura 9 indica la arquitectura básica de un sistema GSM, en la cual se puede distinguir los principales bloques que lo construyen. Un grupo de estaciones base se encuentra conectado a un controlador de estaciones base (BSC), encargado, de situaciones como traspaso del móvil de una célula a otra. El BSC se ocupa de la gestión de toda la red de radio. Una o varias BSC se conectan a una central de conmutación de móviles (MSC), verdadero núcleo de la red, responsable del inicio, enrutamiento, control y finalización de las llamadas.

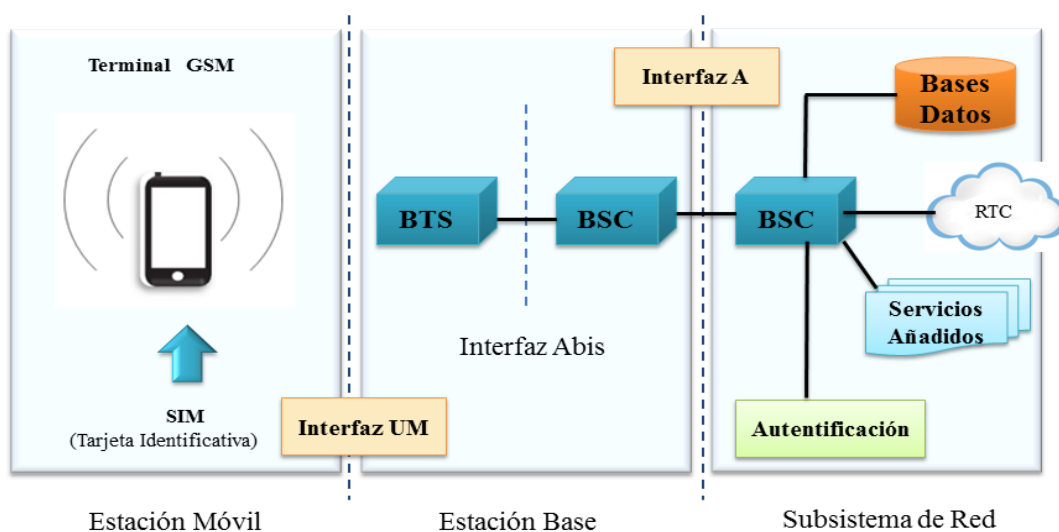


Figura 9. Estructura de una red GSM y principales interfaces entre sus elementos

Fuente: (Huidobro Moya, 2012)

2.9.2.1. Servicios que ofrece GSM.

El estándar de telefonía móvil GSM facilita la existencia de una serie de servicios, sin necesidad de un módem externo a través de una tarjeta para conexión con el puerto serie del ordenador. GSM posibilita la creación de redes privadas virtuales, permite la identificación de un abonado bajo dos números distintos, ofrece un servicio de mensajes alfanuméricos cortos (SMS) de hasta 160 caracteres y toda una completa gama de servicios suplementarios.

2.9.2.2. Servicios de mensajes cortos (SMS).

En un principio, los mensajes (SMS) se definieron en el estándar GSM como un medio para que los operadores de red enviaran información sobre el servicio a los abonados, sin que estos pudieran responder ni enviar mensajes a otros clientes. Sin embargo la empresa Nokia desarrollo un sistema para permitir la comunicación bidireccional por SMS. Los mensajes de texto son procesados por un SMSC (Short Message Service Center) o centro de servicio de mensajes cortos, que se encarga de almacenarlos hasta que son enviados y de conectar con el resto de elementos de la red GSM.

El servicio SMS consiste en el envío de mensajes en modo almacenamiento y reenvío a través de un centro de servicio de mensajes cortos. Se basa en los procedimientos SMS proporcionados por el subnivel de gestión de comunicación (CM). El servicio SMS permite el envío de mensajes alfanuméricos de hasta 140 bytes (160 caracteres de 7 bits) desde una estación móvil hacia una o más estaciones móviles destinatarias. La limitación de longitud no es específica de GSM, sino que se debe a la longitud máxima de mensajes que puede transportar la red.

A diferencia de los demás servicios GSM, el servicio SMS no implica el establecimiento de un trayecto de comunicación directo entre las MS origen y destino, sino que sigue el enfoque tradicional de las redes de conmutación de mensajes, basado en el empleo de nodos de almacenamiento y reenvío. En GSM, estos nodos reciben el nombre de centro de servicio de mensajes cortos (SMSC). Las especificaciones GSM consideran a los SMSC como elementos ajenos a la red, y la comunicación entre ambos se lleva a cabo a través de las pasarelas SMS (SMSG, SMS Gateway). Desde la

perspectiva de GSM, el envío de un mensaje corto se limita al encaminamiento desde la MS hasta el SMSC adecuado, y finaliza cuando este se ha entregado a la SMSG.

2.9.2.3. Soluciones para el envío de alertas empleando SMS.

Actualmente existen diferentes maneras a elegir para el envío de mensajes de texto cortos hacia un dispositivo móvil. A continuación se indica rápidamente el funcionamiento de cada una de las opciones a elegir, para poder definir cuál método se ajusta más al software de gestión.

2.9.2.3.1. Envío de SMS a través de Internet.

La primera opción que se tiene a disposición para el envío de la información vía SMS es a través de internet, actualmente existen varias páginas Web que brindan este servicio para adaptarlo al software de gestión, se lo realiza mediante una suscripción de usuario y posteriormente permiten el envío masivo de mensajes a un determinado costo. Entre las desventajas que presenta esta opción son:

- El costo para contratación de paquetes de mensaje es muy elevado por tratarse de empresas que se encuentran en otros países, comparado con los paquetes de mensajes que actualmente brindan las operadoras móviles de nuestro país en el Anexo A se indica un ejemplo.
- El tiempo que tardaría en enviarse el mensaje hacia el destinatario dependería del congestionamiento de la red.
- No se garantiza que los mensajes de alertas lleguen a su destinatario, debido a que puede existir el caso de que el servicio de internet de la empresa se encuentre inactivo.

2.9.2.3.2. Envío de SMS mediante un celular conectado al servidor.

La segunda opción que se tiene a disposición es el envío de mensajes de texto cortos mediante un dispositivo móvil conectado al servidor. El establecimiento de conexión entre el servidor y el dispositivo móvil puede ser mediante un cable de datos. La funcionalidad que cumple el dispositivo móvil es el actuar como módem con la finalidad de procesar la información que se envíe desde el servidor hacia el celular. En la Figura 10 se muestra la representación del envío de SMS a través de un dispositivo móvil conectado en el servidor.

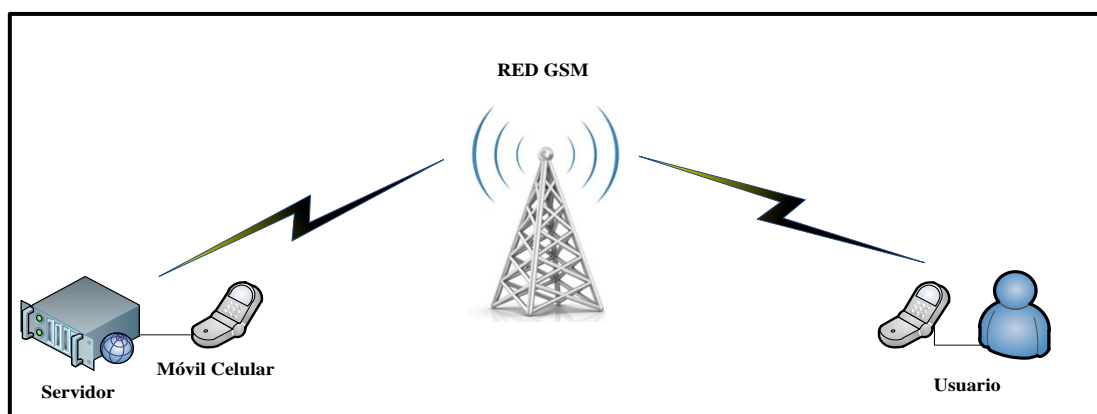


Figura 10. Envío de SMS mediante un dispositivo móvil

Fuente: (Gualotuña Amagua & Cando Cofre, 2010)

El establecimiento de la comunicación entre el servidor y el dispositivo móvil se realiza mediante el uso de comandos AT⁷. Los comandos AT se envían desde el servidor a través de una aplicación que permita tomar control sobre el dispositivo móvil (Gualotuña Amagua & Cando Cofre, 2010).

Las desventajas que se debe tomar en cuenta al elegir esta opción son las siguientes:

⁷ AT.- Sus siglas en inglés ATTENTION, son instrucciones codificadas que conforman un lenguaje de comunicación entre el usuario y un terminal modem.

- El software de aplicación que se utilice para establecer la comunicación entre el servidor y el dispositivo móvil a través de comandos AT, no tenga funcionalidad con algunas marcas y modelos de celulares existentes actualmente.
- El dispositivo móvil que se utilice deberá contar con ciertos parámetros como son: servicio de SMS, soporte para el manejo a través de comandos AT, disponer de un medio para la comunicación con el servidor ya sea por medio de un cable de datos usb o serial, infrarrojos o Bluetooth.

2.9.2.3.3. Envío de SMS a través de un Módem GSM conectado al servidor.

La tercera opción a diferencia de la segunda es que esta utiliza un módem GSM externo. La principal funcionalidad de estos módems es que son más robustos, es decir tienen la capacidad de utilizar la red GSM para aplicaciones de voz, datos, fax, SMS, además de soportar un amplio set de comandos AT.

Actualmente en el mercado existe diferentes tipos de estos módems con diversas características y de igual manera su precio varía considerablemente.

En la Figura 11 se indica la representación del envío de SMS mediante un módem GSM conectado en el servidor.

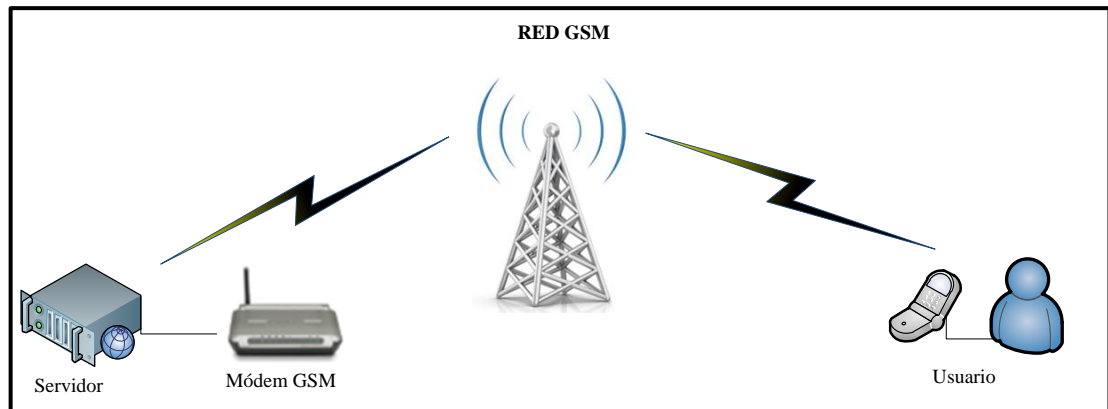


Figura 11. Envío de SMS mediante un Módem GSM

Fuente: (Gualotuña Amagua & Cando Cofre, 2010)

En el Anexo A se describe a detalle los parámetros que influyen en la elección de cada solución para el envío de SMS y además está una breve descripción del porque utilizar la tecnología 3G y no otras tecnologías.

CAPÍTULO III

3. Análisis de la Infraestructura Actual de la Red Local de Datos del GAD-Ibarra

En este capítulo se describe la forma estructural de las dependencias internas y externas del Gobierno Autónomo Descentralizado de San Miguel de Ibarra (GAD-Ibarra). Se realiza el análisis de la situación actual en la que se encuentra la red local de datos de la entidad, donde a partir de esta información se determina los equipos de mayor prioridad que soporten el Protocolo SNMP y posteriormente desarrollar la implementación del modelo de gestión de red funcional.

3.1. Introducción

El Gobierno Autónomo Descentralizado de San Miguel de Ibarra se encuentra ubicado en el cantón Ibarra, provincia de Imbabura. Es una entidad de Derecho Público constituida por una comunidad humana, que administra sus propios recursos económicos, cuya finalidad es el bien común local y, dentro de éste y en forma primordial, la atención de las necesidades de la ciudad, del área metropolitana y de las parroquias rurales de la respectiva localidad (GAD-Ibarra, 2011).

Es una entidad que día a día se compromete con el uso masivo de las Tecnologías de la Información y la Comunicación (TIC⁸), conformando una plataforma integrada con todas sus unidades para brindar conectividad de servicios, a través de herramientas

⁸ Tecnologías de Información y Comunicación (TIC).- Agrupan elementos y técnicas usadas en el tratamiento y la transmisión de la información.

hardware y software para satisfacer los requerimientos y exigencias de los usuarios del cantón. El Portal Web de la entidad presenta la misión y visión:

➤ **Misión de la Entidad**

El municipio de Ibarra planifica, regula, ejecuta y promueve el desarrollo integral sostenible del cantón, a través de servicios de calidad eficientes y transparentes con la participación activa de la ciudadanía socialmente responsable a fin de lograr el buen vivir.

➤ **Visión de la Entidad**

Seremos un municipio líder en gestión con responsabilidad social, que garantice equidad, honestidad, trabajo y eficiencia por qué Ibarra se constituya en un cantón próspero, atractivo e incluyente, capital de los servicios y el conocimiento, referente del buen vivir en la región norte del Ecuador (GAD-Ibarra, 2011).

3.2. Estructura Administrativa

A continuación en la Figura 12 se muestra la Estructura Administrativa del Gobierno Autónomo Descentralizado de San Miguel de Ibarra:

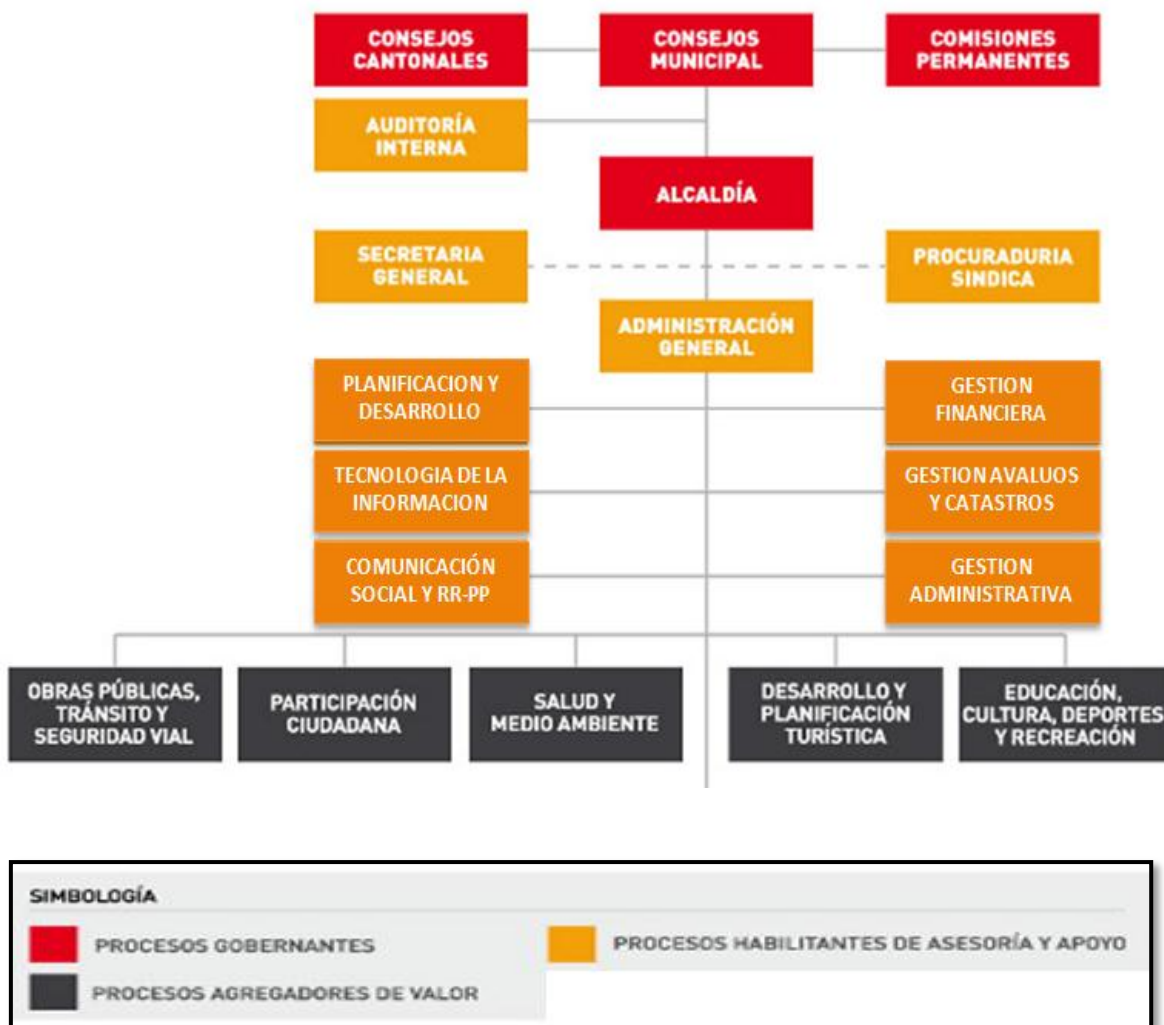


Figura 12. Organigrama Estructural del GAD-Ibarra

Fuente: (GAD-Ibarra, 2013)

3.3. Descripción de las Dependencias Internas

La información expuesta a continuación se realizó basada en inventarios obtenidos de la entidad y un proyecto realizado anteriormente (Culqui Medina, 2013, págs. 88-97).

El GAD-Ibarra está formado por distintos departamentos que se encuentran distribuidos en dos edificios, los cuales se puntualizan a continuación:

3.3.1. Descripción del edificio principal.

El edificio principal se encuentra ubicado en las calles Gabriel García Moreno 6-31 y Simón Bolívar, en el sector centro de la ciudad de Ibarra. Su infraestructura esta dividida en tres plantas como se describe en la Tabla 2 y cuenta aproximadamente con 196 empleados, quienes son encargados de realizar diferentes funciones en cada departamento.

Tabla 2. Distribución de las Unidades del Edificio Principal

Planta	Departamentos	Número de empleados
Planta Baja	▪ Rentas	42
	▪ Atención al cliente	
	▪ Tesorería	
	▪ Coactivas	
	▪ Dirección de Comunicación Social	
	▪ Recursos Humanos y Capacitación	
	▪ Auditorio	
Primera Planta	▪ Alcaldía	49
	▪ Sala de Sesiones	
	▪ Auditoria Interna	
	▪ Procuraduría Municipal	
	▪ Secretaria General	
	▪ Administración General	
	▪ Dirección de Gestión Administrativa	
	▪ Dirección de Gestión Financiera	
	▪ Presupuesto	
	▪ Finanzas	
	▪ Contabilidad	
▪ Copiadora		
Segunda Planta	▪ Dirección de Planificación	97
	▪ Dirección de Avalúos y Catastros Urbano	
	▪ Dirección de Tecnologías de la información y Comunicación (TIC)	
	▪ Dirección de Obras Públicas	
	▪ Archivo Histórico	
Tercera Planta	▪ Gestión de Avalúos y Catastros Rural	8

Fuente: (GAD-Ibarra, 2013)

En la Figura 13 se indica el organigrama de la dirección de Tecnologías de la Información y Comunicación (TIC) que se encuentra ubicada en la segunda planta lugar en el que se enfoca el proyecto, debido a que en este departamento se encuentra el Data Center⁹, donde están los equipos de red que interconectan, comparten, transmiten y reciben información (voz, datos y video) de toda la entidad. A continuación se presenta:

➤ **Misión del departamento TIC del GAD-Ibarra**

Proporcionar tecnología de información de vanguardia para satisfacer los requerimientos y expectativas de nuestros usuarios, a través de una plataforma de conectividad, hardware y software, que permita a las distintas unidades de la Municipalidad operar de manera integrada con información disponible en los diferentes niveles para la toma de decisiones.



Figura 13. Organigrama de la Dirección TIC

Fuente: (GAD-Ibarra, 2011)

En las otras plantas está distribuida la parte de información, administrativa, económica y social.

⁹ Data Center o (Centro de Datos).- Es un lugar diseñado y construido de acuerdo a normas internacionales dentro de un espacio físico en una organización, que cumple la función de interconectar los dispositivos de la red y el procesamiento íntegro de la información de voz, datos y video.

3.3.2. Descripción del edificio antiguo.

El edificio antiguo se encuentra ubicado en la calle Simón Bolívar entre las calles Juan José Flores y Gabriel García Moreno, en el centro de la ciudad de Ibarra, este edificio está distribuido de la siguiente forma, como se observa en la Tabla 3 y cuenta aproximadamente con 78 usuarios:

Tabla 3. Distribución de Unidades del Edificio Antiguo

Planta	Departamentos	Número de empleados
Planta Baja	▪ Comisaria de Construcciones	40
	▪ Comisaria de Higiene	
	▪ Archivo Institucional	
	▪ Recaudación	
	▪ Dirección de Medio Ambiente	
	▪ Plan de Ordenamiento Territorial	
	▪ Biblioteca	
	▪ Unidad de proyectos	
Primera Planta	▪ Central de Operadora Telefónica	38
	▪ Secretaria de Comisiones /Concejales	
	▪ Radio	
	▪ SISMERT	
	▪ Tránsito y Transporte	
	▪ Dirección de Salud y Medio Ambiente	

Fuente: (GAD-Ibarra, 2013)

3.4. Descripción de las Dependencias Externas

El GAD-Ibarra tiene también dependencias externas que cumplen con distintas funciones y se puntualizan a continuación:

3.4.1. Dirección de Cultura, Proyecto Parque Ciudad Blanca.

Esta dependencia se encuentra ubicada en las calles Simón Bolívar y Juan José Flores (esquina) en la casa de la Ibarreñidad, donde en la primera planta se encuentra el

proyecto parque Ciudad Blanca y en la tercera planta el departamento de Cultura, esta dependencia cuenta con 22 usuarios.

3.4.2. Dirección de Turismo.

La dirección de Turismo se encuentra ubicada en las calles Miguel Oviedo y Antonio José de Sucre de la ciudad de Ibarra y cuenta con una cantidad de 15 usuarios.

3.4.3. Bodega Municipal.

La Bodega Municipal se encuentra ubicada en la Avenida Víctor Manuel Guzmán y calle Uruguay junto al Hospital del Seguro Social de la ciudad de Ibarra. Aquí se realiza el almacenamiento de materiales, equipos y maquinaria perteneciente al GAD-Ibarra, además también se encuentra el área de Mecánica, Reciclaje y Desechos Sólidos, la Dirección de Gestión de Seguridad Industrial y Salud Ocupacional. Esta dependencia cuenta con 5 usuarios.

3.4.4. Administración de Mercado Amazonas.

Se encuentra ubicada en la Avenida Pérez Guerrero y cuenta con 4 usuarios.

3.5. Situación Actual de la Red Local de Datos

Para poder determinar los equipos que soportan el protocolo SNMP para el monitoreo es necesario conocer la situación actual de la infraestructura física y lógica de la red local de datos del GAD-Ibarra.

Actualmente la red permite la transmisión y recepción de (voz, datos y video), además de compartir archivos, acceder a internet, posee servicios internos como (correo

interno institucional, sistemas prediales, sistemas administrativos, financieros, consultas, etc.) entre otros servicios que ayudan al desarrollo de las actividades de la entidad. Sin embargo dentro de la infraestructura de la red local de datos de la entidad no cuenta con un modelo de gestión de red.

La red de área local cuenta con un direccionamiento IPv4 Clase B (172.X.X.X) máscara 255.255.248.0 que satisface la capacidad de usuarios que posee la entidad y mediante el número de puertos existentes garantiza la disponibilidad de sus servicios, además permite a la red un gran crecimiento y escalabilidad.

La información obtenida de la situación actual de la red del GAD-Ibarra se realizó a partir de inventarios realizados por la Dirección de Tecnologías de la Información y Comunicación.

3.5.1. Infraestructura física de la red local de datos.

El cuarto principal de telecomunicaciones del GAD-Ibarra se encuentra en la segunda planta dentro de la dirección (TIC) como se mencionó anteriormente. A continuación se detallan los componentes principales que forman parte de la red de local de datos:

3.5.1.1. Data Center.

El centro de procesamiento de datos o Data Center es un espacio físico que se encuentra ubicado en la dirección TIC de la entidad el cual ha sido construido y diseñado bajo normas internacionales de seguridad e infraestructura física y lógica, en donde se interconectan todos los equipos de la red de datos tanto de dependencias

internas como externas, facilitando la administración y acceso a todos los recursos de la red, cumple con ciertas especificaciones de la norma TIA-942¹⁰, el cual provee lineamientos como diseño eléctrico, control ambiental, protección contra riesgos físicos, almacenamiento de archivos, además por seguridad de acuerdo a las normas posee un sistema de acceso restringido, en el Anexo B.1 se detallan las especificaciones técnicas del Data Center. A continuación se presentan algunas características:

- El funcionamiento de la red local de datos se basa en la tecnología Ethernet.
- La entidad en su estructura utiliza una topología tipo estrella.
- Dispone de configuración de VLAN's¹¹ para los equipos y la VoIP¹².
- El cableado vertical y horizontal de la red se encuentra realizado con cable UTP¹³ categoría 6, este se encuentra etiquetado para la identificación de los puntos, pero actualmente no existe una documentación completa, debido al crecimiento de la red y situaciones imprevistas. El cableado estructurado del edificio principal cuenta con un periodo de vida útil de 15 años a partir del año 2010.
- Dispone de puesta a tierra tipo malla que se encuentra en la parte del edificio antiguo, no dispone de un generador eléctrico.

¹⁰ TIA-942.- Es un estándar que especifica lineamientos, guías y recomendaciones para la planificación y diseño de Centro de Datos.

¹¹ VLAN (Red de Área Local Virtual).- Es un método para crear redes lógicamente independientes dentro de una misma red física, de esta forma se simplifica la administración de la red brindando mayor flexibilidad y seguridad.

¹² VoIP (Voz sobre un Protocolo de Internet).- Es un grupo de recursos hardware y software que permite a los usuarios utilizar Internet como medio de transmisión de llamadas telefónicas, enviando datos de voz en paquetes, usando un protocolo IP en lugar de los circuitos de transmisión telefónicos.

¹³ UTP (Unshielded Twister Pair).- Par trenzado no blindado en español, es un tipo de cable que se utiliza en las telecomunicaciones y redes informáticas.

En la Tabla 4 se describe la cantidad de elementos que se encuentran en el interior del Data Center:

Tabla 4. Equipos del Data Center

Cantidad	Elementos	Marca/Modelo
10	Switch Administrables	▪ Cisco, 3COM
4	Switch no Administrables	▪ TP-LINK MC110C
10	Servidores Físicos	▪ HP ProLiant DL, BL, ML
20	Servidores Virtuales	-
1	Check Point Firewall	-
1	Chasis Blade System	▪ HP c3000
16	Patch Panel categoría 6 para voz y datos	-
6	Convertidores de fibra óptica	-
2	Equipos de proveedores de internet	
	▪ Un módem	-
	▪ Un convertor de fibra óptica	
1	Sistema de detección de incendios	▪ Marca: Chemetron ▪ Panel de Control: Micro 1012
2	Sistemas de aire acondicionado	▪ Aire acondicionado marca Lenux ▪ Sistema de aire acondicionado de precisión Marca Liebel
1	Sistema de seguridad del Data Center	▪ Marca: iGuard LM Series
2	Monitores	▪ Un monitor Samsung ▪ Un monitor Acer
4	UPS ¹⁴ (Sistema de Alimentación Ininterrumpida)	▪ UPS Marca PowerWare 9170 Plus de 12KVA ▪ UPS Marca Tripplite de 3KVA ▪ UPS Marca APP de 1.5 KVA
1	Tablero PDU ¹⁵ (Unidad de distribución de energía) para Data Center	-

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

3.5.1.2. Subsistemas del cableado estructurado.

En este ítem se indica una breve explicación de cableado estructurado que conforma la red del GAD-Ibarra:

¹⁴ UPS (Uninterruptible Power Supply).- Energía de seguridad durante un cierto periodo de tiempo que posee una batería que se emplea cuando la energía eléctrica de la línea se interrumpe.

¹⁵ PDU (Power Distribution unit).- Distribución de energía confiable mediante una entrada única con diversos tomacorrientes de salida para centros de datos.

3.5.1.3. Subsistema del cableado vertical o backbone.

El cableado del backbone desempeña la función de interconectar el cableado horizontal de los diferentes pisos del edificio principal a través de medios de transmisión fibra óptica y cableado UTP con los gabinetes de telecomunicaciones que se encuentran en el Data Center.

El backbone de la entidad se interconecta con los gabinetes de telecomunicaciones ubicados en el edificio antiguo, la dirección de Cultura que se encuentra en la casa de la Ibarreñidad y la dirección de Turismo a través de fibra óptica, donde el área de distribución principal (MDF) se encuentra en la segunda planta alta del edificio principal en la dirección TIC y las áreas de distribución secundarias (SDF) están ubicadas en la primera planta del edificio antiguo, en la tercera planta de la dirección de Cultura y en la primera planta de la dirección de Turismo.

La fibra óptica es de tipo multimodo para la conexión entre las dependencias externas del GAD-Ibarra y monomodo entre entidades independientes, las entidades independientes no se analizan en este proyecto. Presenta una certificación ISO 9001 y cumple con las especificaciones ISO/IEC 11801 certificación Tier I¹⁶ en fibra óptica.

3.5.1.4. Subsistema del cableado horizontal o cableado de distribución.

El cableado horizontal interconecta el backbone con las áreas de trabajo. En la entidad este cableado está realizado con cable UTP categoría 6, conectores dobles RJ-45

¹⁶ Tier I.- Especificaciones que determinan que un Data Center es confiable en base a cumplimiento de recomendaciones

que se conectan a cajetines sobrepuestos para tomas simples y dobles, con tapas de protección para las salidas RJ-45 para tomas dobles de voz y datos.

Para la conexión del cableado horizontal del edificio principal y el edificio antiguo al backbone, utiliza bandejas metálicas sobre el cielo falso y para la conexión de los puntos de red de las áreas de trabajo mediante canaletas plásticas.

3.5.1.5. Áreas de trabajo.

La conexión de las distintas unidades de la entidad a los dispositivos terminales (computadoras, impresoras, teléfonos) se realiza mediante patch cord UTP categoría 6/Clase E, con conectores RJ-45 a los dos lados cumpliendo con las normas del cableado estructurado EIA (Electronics Industries Association) / TIA (Telecommunications Industries Association), a continuación en la Tabla 5 se indica las normas aplicadas:

Tabla 5. Estándares utilizados en una infraestructura de cableado estructurado

NORMA	DESCRIPCIÓN
TIA/EIA-569-A	Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales
TIA/EIA-568-B y sus addendums	Estándares de cableado de Telecomunicaciones en Edificios Comerciales
TIA/EIA-606-A	Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.

Fuente: (Unitel, 2014)

3.5.1.6. Topología física de la red local de datos.

En el diagrama que se muestra en la Figura 14 se detalla la estructura de la topología física de la red local de datos del GAD-Ibarra, donde se observa las conexiones de los enlaces LAN que se dirigen hacia los edificios de las dependencias internas y externas, como se explicó en los subsistemas de cableado estructurado en el punto 3.5.1.2.

Además se puede observar la conexión del switch core mediante fibra óptica con el enlace de Telconet, el cual entrega un ancho de banda de 10 Mbps a la red de la entidad, se observa también la conexión de los servidores físicos ubicados en el Data Center y los enlaces inalámbricos que se dirigen hacia el parque ciudad blanca donde se encuentra el área de participación ciudadana y hacia la bodega municipal.

3.5.1.7. Descripción de Switches (Conmutadores).

Los switches son dispositivos que dividen una gran LAN en varios segmentos. A continuación en la Tabla 6 se detalla las características más relevantes de los conmutadores que interconectan la red de área local de datos del GAD-Ibarra. En el Anexo B. 2 se detalla las especificaciones técnicas de cada uno de estos switches.

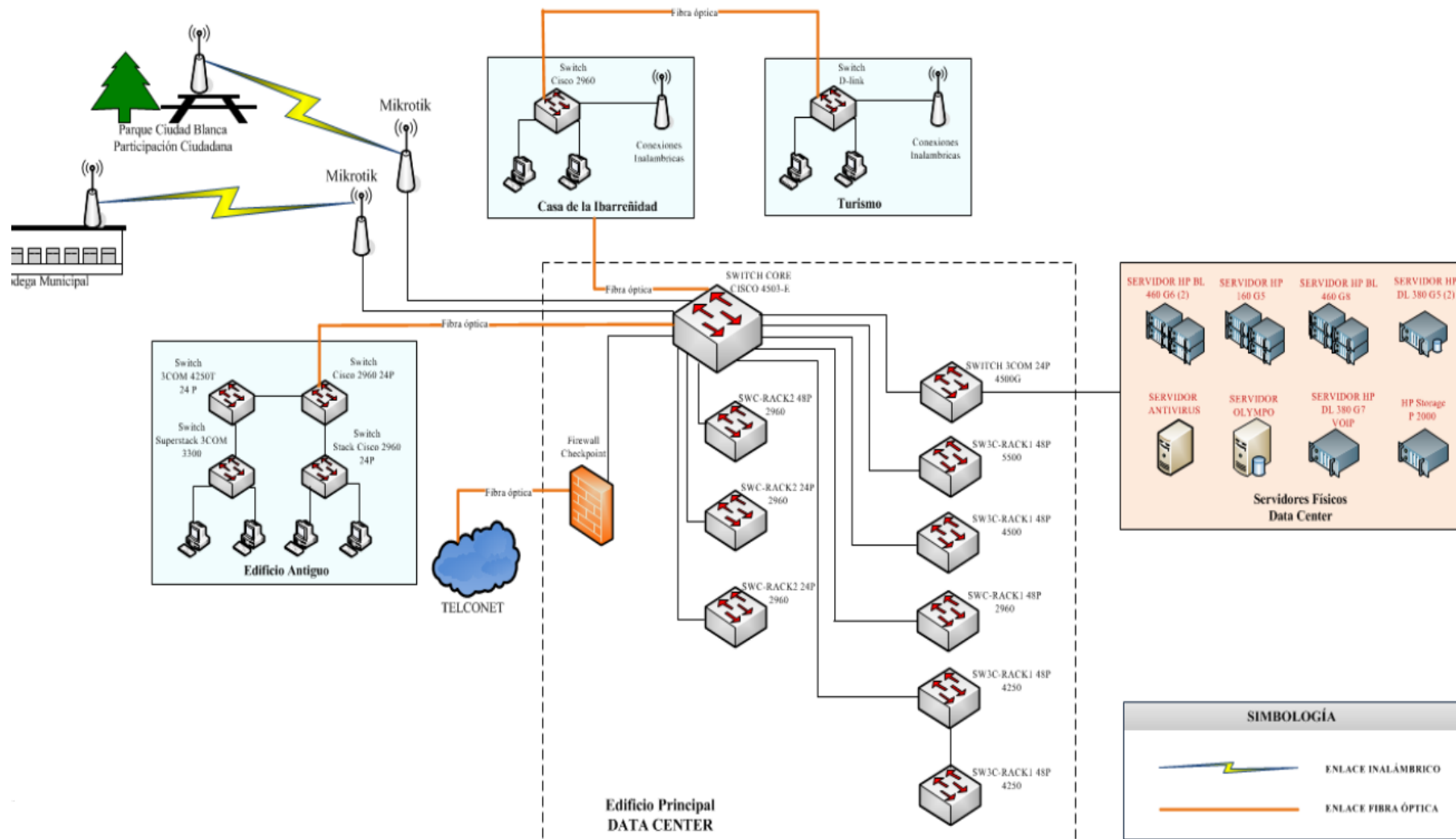


Figura 14. Topología física de la red de datos

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

Tabla 6. Descripción de Switches del GAD-Ibarra

Switch	Características Generales	Memoria	Procesador	Soporte SNMP	Función
Cisco Catalyst 4503- E	48 GigaEthernet 10/100/1000 Mbps 8 puertos SPF 1000 BASE-T Conmutador: Capas 2, 3 y 4	RAM: 256MB FLASH: 32MB	CPU:266 MHz	Versión 1, 2 y 3	Switch core que permite la conexión entre dependencias externas e internas mediante fibra óptica y utp.
3COM 4500 G	24 GigaEthernet 10/100/1000 Mbps 4 puertos de uso dual 10/100/1000 Conmutador: Capas 2, 3	FLASH: 28MB	CPU: 264MHz	Versión 1, 2 y 3	Utilizado para interconectar los servidores del Data Center
3COM 5500 SI	48 Fast Ethernet - 10/100 Mbps 4 Giga Ethernet - 1000 Mbps Conmutador: Capas 2, 3	-	-	Versión 1, 2 y 3	Utilizado para interconectar los segmentos de red del edificio principal
3COM 4500	48 Fast Ethernet - 10/100 Mbps 2 Giga Ethernet – 1000 Mbps Conmutador: Capas 2, 3	SDRAM: 64 MB FLASH: 8 MB	-	Versión 1, 2 y 3	Utilizado para interconectar los segmentos de red del edificio principal
3Com 4250T (2)	48 Fast Ethernet -10/100 Mbps 2 Giga Ethernet - 10/100/1000 Mbps Conmutador: Capa 2	-	-	Versión 1	Utilizado para interconectar los segmentos de red del edificio principal.
Cisco Catalyst 2960 (4)	24/48 FastEthernet 10/100 Mbps 2 Giga Ethernet:10/100/1000 Mbps Conmutador: Capa 2	RAM: 64 MB, FLASH: 32MB	Single: core	Versión 1, 2 y 3	Utilizados para interconectar los segmentos de red del edificio principal

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

3.5.1.8. Descripción de Servidores Físicos y Virtuales.

Los servidores se encuentran ubicados en el gabinete uno y dos del Data Center, en el Anexo B.1.1.1 se indica el diseño de distribución. Actualmente los servidores se encuentran en un entorno de virtualización los cuales se detallan a continuación:

3.5.1.8.1. Escenarios de virtualización.

La red del GAD-Ibarra cuenta con un Chasis Blade System HP c3000 que soporta hasta ocho servidores, donde se encuentran ubicados los servidores físicos HP Blade en los cuales están instalados los escenarios de virtualización mostrados en las Figuras 15, 16, 17, 18, donde se indica una descripción técnica de cada uno de ellos. Están desarrollados con la herramienta de virtualización KVM¹⁷ sobre el sistema operativo Debian, además en algunos servidores se ha creado Raid¹⁸ 1 y Raid 5 debido a las aplicaciones y servidores a ser virtualizados, aquellos tienen una característica importante al poseer un buen nivel de tolerancia a fallos. La información que se presenta a continuación se ha obtenido de los inventarios de la dirección de Tecnologías de la Información y Comunicación del GAD-Ibarra y un proyecto anteriormente realizado (Rosero Vinuesa, 2012).

¹⁷ **KVM.-** Kernel Virtual Machine base (Máquina virtual basada en el Kernel). Es una solución de virtualización para Linux

¹⁸ **Raid.-** Sus siglas en inglés Redundant Array of Independent Disks, es decir, conjunto redundante de discos independientes que se utilizan para proteger información que se considera crítica.

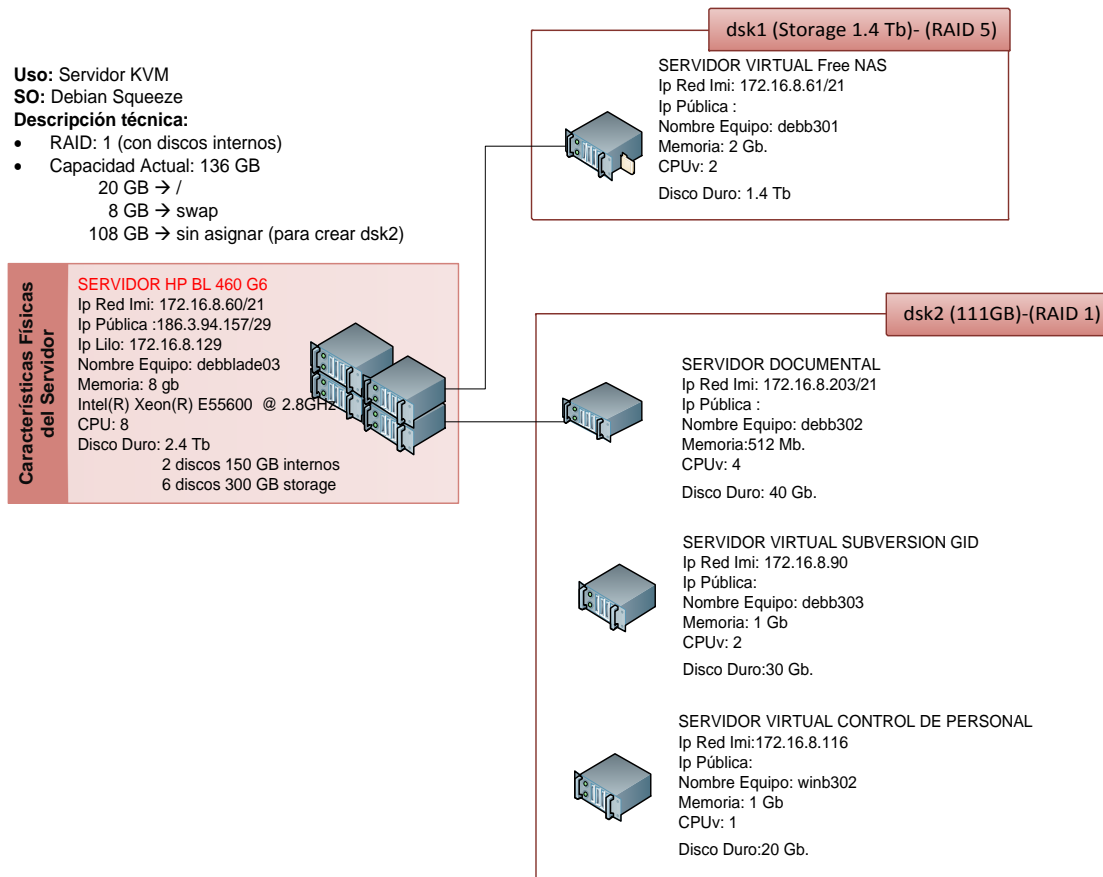


Figura 15. Escenario de virtualización servidor HP BL 460 G6

Fuente: (Rosero Vinueza, 2012)

Uso: Servidor KVM

SO: Debian Squeeze

Descripción técnica:

- RAID: 1 (con discos internos)
- Capacidad Actual: 136 GB
 - 20 GB → /
 - 16 GB → swap
 - 103 GB → sin asignar (para crear dsk2)

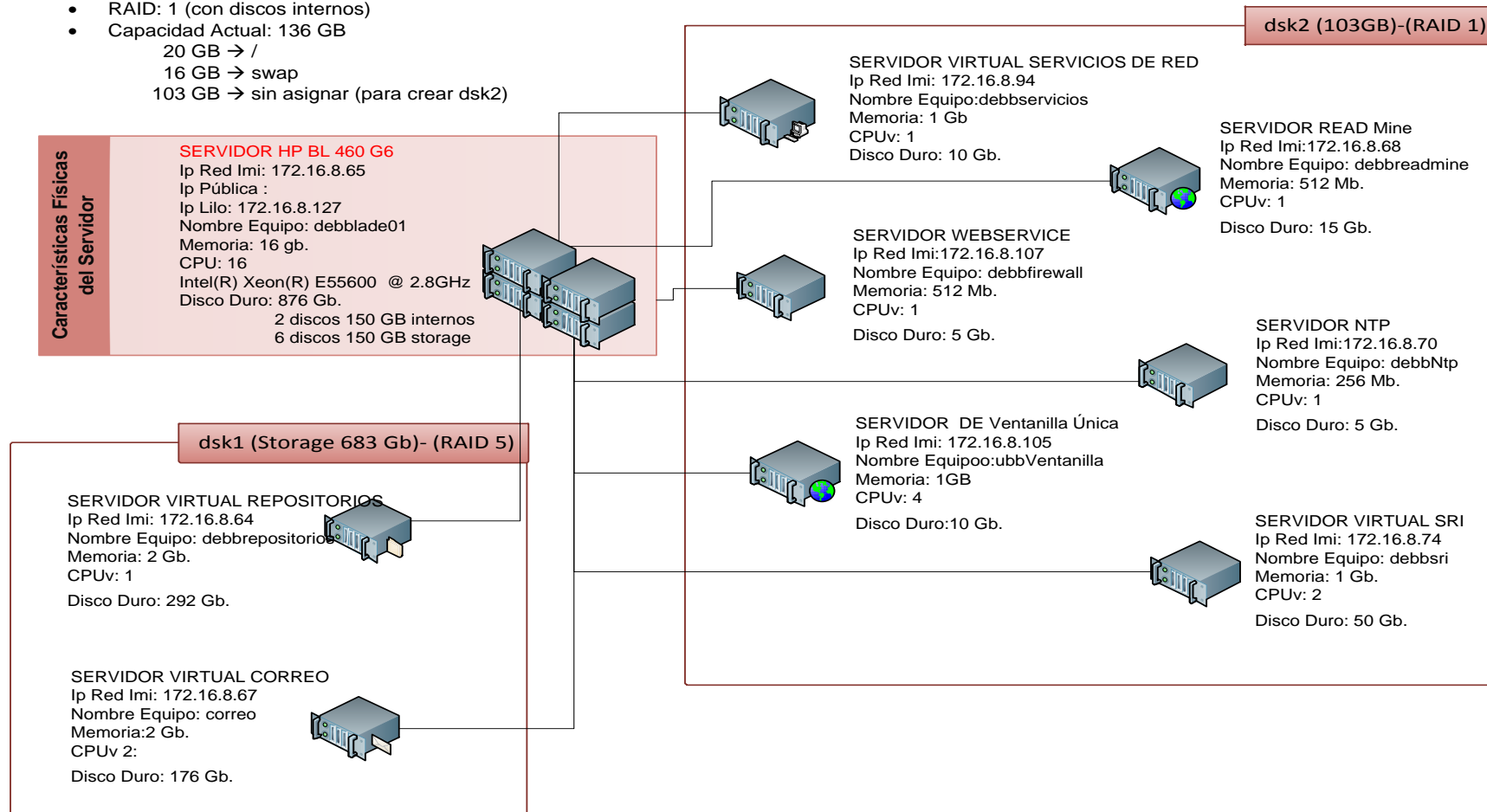


Figura 16. Escenario de virtualización servidor HP BL 460 G6

Fuente: (Rosero Vinueza, 2012)

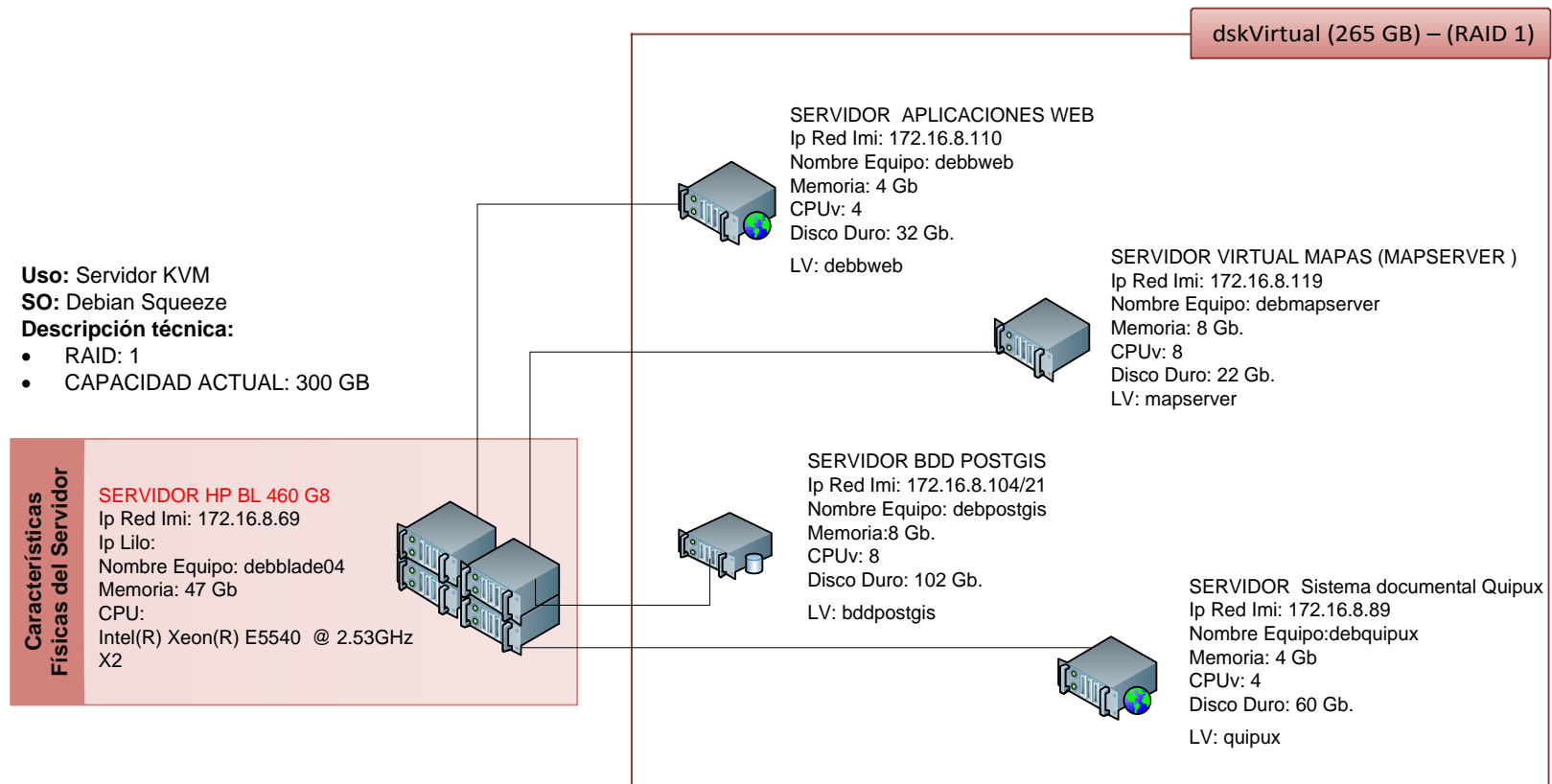


Figura 17. Escenario de virtualización servidor HP BL 460 G8

Fuente: (Rosero Vinueza, 2012)

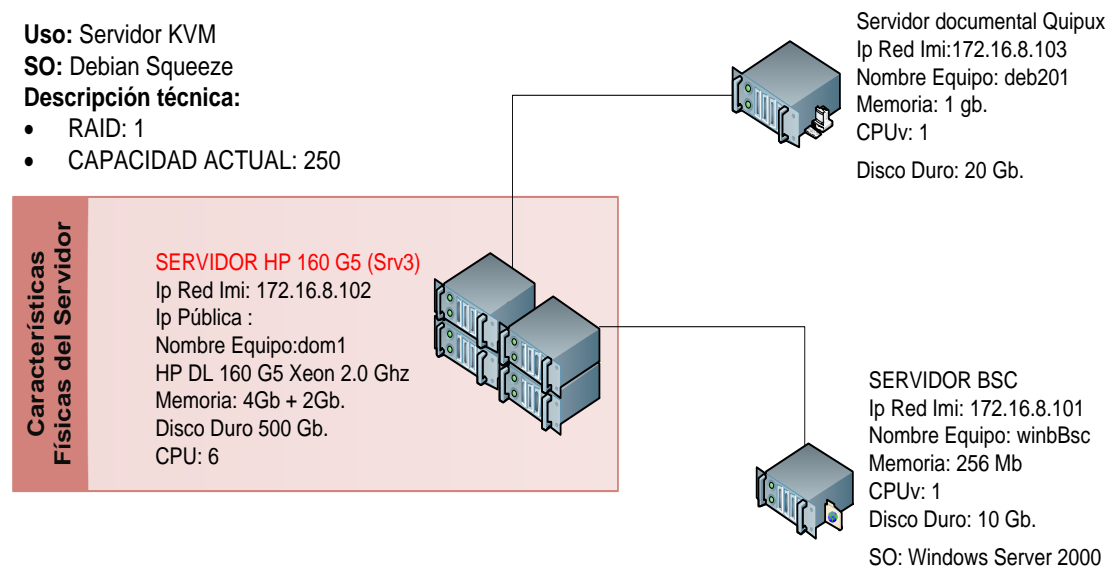


Figura 18. Escenario de virtualización servidor HP 160 G5

Fuente: (Rosero Vinueza, 2012)

En la Tabla 7 se describe el tipo de servidor físico o virtual, sistema operativo que utiliza, memoria RAM y capacidad de disco duro, procesador y funcionalidad de cada uno de ellos.

Tabla 7. Servidores Físicos y Virtuales del GAD-Ibarra

Servidor	Tipo	Sistema operativo	Memoria RAM y Capacidad	Procesador	Función
SERVIDOR HP BL 460 G6	Físico	Debian 6.0.1	Memoria: 8 GB Disco Duro: 1.4 TB	Intel(R) Xeon(R) E55600 @ 2.8GHz	Master de virtualización para gestión de servidores
FREE NAS	Virtual	FreeNAS	Memoria: 1 GB Disco Duro: 1.4 TB	2	Permite simplificar el mantenimiento de los datos
SERVIDOR DOCUMENTAL	Virtual	Debian 7.0.1	Memoria:1 GB Disco Duro: 40 GB	2	Almacena documentos electrónicos
SERVIDOR SUBVERSIÓN GID	Virtual	Debian 7.0.1	Memoria:1 GB Disco Duro: 30 GB	2	Modificación de versiones antiguas-actuales
SERVIDOR CONTROL DE PERSONAL	Virtual	Windows Server 2003	Memoria:1 GB Disco Duro: 20 GB	2	Control de Personal de la entidad
SERVIDOR HP BL 460 G6	Físico	Debian 6.0.1	Memoria: 16 GB Disco Duro: 683 GB	Intel(R) Xeon(R) E55600 @ 2.8GHz	Master de virtualización para gestión de servidores
SERVIDOR REPOSITARIOS	Virtual	Debian 6.0.1	Memoria:2 GB Disco Duro: 292 GB	1	Evita descargar paquetes nuevamente
SERVIDOR DE CORREO	Virtual	Ubuntu 12.04	Memoria:2 GB Disco Duro: 176 GB	2	Correo institucional con la herramienta zimbra
SERVIDOR DE SERVICIOS DE RED	Virtual	Debian 6.0.1	Memoria: 1 GB Disco Duro: 10 GB	2	Funciones de DNS (Servidor de Dominio de Nombres) y DHCP (Direccionamiento IP dinámico)
SERVIDOR DE REDMINE	Virtual	Debian 6.0.1	Memoria: 512 MB Disco Duro: 15 GB	1	Para el seguimiento de errores y gestión de proyectos (aplicaciones web)
SERVIDOR NTP	Virtual	Debian 6.0.1	Memoria: 256 MB Disco Duro: 5 GB	1	Para la sincronización de relojes de sistemas computacionales a través de red
SERVIDOR DE VENTANILLA ÚNICA	Virtual	Ubuntu 10.0.4	Memoria:1 GB Disco Duro: 10 GB	4	Aplicación web en Java para cobros y registros, en ventanilla
SERVIDOR SRI	Virtual	Windows Server 2003	Memoria:1 GB Disco Duro: 50 GB	2	Transacciones SRI
SERVIDOR WEBSERVICE	Virtual	Debian 6.0.1	Memoria:512 MB Disco Duro: 5 GB	1	Comunicación de servicios web con instituciones financieras
SERVIDOR HP 160 G5 (Srv3)	Físico	Debian 5.0.1	Memoria:4 GB Disco Duro: 250 GB	Procesador Intel	Master de Virtualización para

				Xeon 2.0 GHz	Gestión de servidores. Permite emular hardware para cada servidor.
SISTEMA DOCUMENTAL QUIPUX	Virtual	Debian 5.0.1	Memoria:1 GB Disco Duro: 50 GB	2	Para sistema documental interno.
SERVIDOR DE BALANCE SCORD CARD	Virtual	Windows Server 2000	Memoria: 256 MB Disco Duro: 10 GB	2	Administrador de gestión de proyectos
SERVIDOR PROMOX HP DL 380 G5 (Srv5)	Físico	PROMOX	Memoria:8 GB Disco Duro: 100 GB	Intel(R) Xeon(TM) CPU 3.60GHz	Servidor Master de virtualización para gestión de servidores.
SERVIDOR DE BASE DE DATOS POSTGRES Pruebas (deb101)	Virtual	Debian 5.0.1	Memoria:2 GB Disco Duro: 80 GB	4	Base de Datos de prueba
SERVIDOR MOODLE	Virtual	Debian 5.0.1	Memoria:512 MB Disco Duro: 20 GB	1	Sistema de gestión de aprendizaje
SERVIDOR HP BL 460 G8	Físico	Debian 7.0.1	Memoria:47 GB Disco Duro: 300 GB	Xeon(R) CPU E5-2650 0 @ 2.00GHz	
SERVIDOR APLICACIONES WEB	Virtual	Debian 7.0.1	Memoria:4 GB Disco Duro: 32 GB	4	Proporciona servicios de aplicación a los usuarios
SERVIDOR VIRTUAL MAPAS (MAPSERVER)	Virtual	Debian 7.0.1	Memoria:8 GB Disco Duro: 22 GB	8	Servidor de mapas. Aplicaciones web.
SERVIDOR BDD POSTGIS	Virtual	Debian 7.0.1	Memoria:8 GB Disco Duro: 102 GB	8	Servidor de base de datos basado en Postgres para aplicaciones Geoespacial.
SERVIDOR SISTEMA DOCUMENTAL QUIPUX (MIGRAR)	Virtual	Debian 7.0.1	Memoria: 4 GB Disco Duro: 60 GB	4	Servidor documental
SERVIDOR DE BDD POSTGRESQL	Físico	Debian 5.0.1	Memoria: 8 GB Disco Duro: 440 GB	Intel(R) Xeon(TM) CPU 3.60GHz	Usado para aplicaciones internas municipales Sistema de Base de Datos
SERVIDOR DE APLICACIONES TERCEROS OLYMPO	Físico	Windows Server 2003	Memoria: 3 GB Disco Duro: 101 GB	Intel(R) Xeon(TM) CPU 3.20GHz	Aplicaciones de escritorio para Windows de terceros
SERVIDOR DE ANTIVIRUS	Físico	Windows Server 2003	Memoria:1 GB Disco Duro: 80 GB	Intel Pentium 4	Antivirus de la entidad

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

3.5.1.9. Racks Secundarios.

Los rack secundarios permiten ubicar distintos dispositivos de red para obtener una mejor distribución, disponibilidad y administración de la red de toda la entidad. A continuación se puntualiza los racks secundarios:

3.5.1.9.1. Rack del edificio antiguo.

Se encuentra ubicado en la primera planta del edificio antiguo en la unidad de la central telefónica, es un rack de 19' que provee la comunicación con todos los departamentos de este edificio y el Data Center del edificio principal a través de un backbone de fibra óptica interno.

En la Tabla 8 se indica los dispositivos de red que se encuentran en este rack:

Tabla 8. Dispositivos de red ubicados en el rack del edificio antiguo

Nro.	Dispositivo	Modelo	Descripción General
4	Switch Administrables	Superstack 3COM, Serie 3C16471	Puertos Fast Ethernet: 24 (10 /100) Conexión: brinda conectividad a una parte del edificio antiguo.
		3COM 4250T, Serie 3C17302	Puertos Fast Ethernet: 48 (10 /100) Conexión: brinda conectividad a una parte del edificio antiguo.
		Cisco Catalyst 2960	Puertos Fast Ethernet: 24 (10 /100) Conexión: permite la conectividad con el Data Center a través de fibra óptica.
		Cisco Catalyst 2960	Puertos Fast Ethernet: 24 (10 /100) Conexión: está en stack con el switch Cisco 2960 anterior.
4	Patch Panel		Un patch panel de 24 puertos y dos patch panel de 48 puertos Marca: HUBBEL Para cableado UTP Categoría 6
1	Patch Panel de Fibra óptica		Conexión: Permite establecer un enlace de fibra óptica con el Data Center. Utiliza un hilo de fibra monomodo
6	Organizadores de cable UTP		Permiten distribuir de mejor manera el cableado de la red.

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

3.5.1.9.2. Rack de los departamentos de la casa de la Ibarreñidad.

Está ubicado en la segunda planta en el departamento de Cultura, es un rack cerrado de 19" de 25U, este permite conectividad entre los departamentos de Cultura y proyecto parque ciudad Blanca con el Data Center del edificio principal. En la Tabla 9 se muestra los elementos que se encuentran en el rack:

Tabla 9. Elementos del rack de la casa de la Ibarreñidad

Nro.	DISPOSITIVO	DESCRIPCIÓN
1	Switch Administrable	Modelo: CISCO 2960 Puertos Fast Ethernet: 24 Puertos Gigabit Ethernet: 2 Conexión: Permite la conectividad mediante fibra óptica con el Data Center. Además interconecta los segmentos de red de la unidad de cultura, y proyecto parque ciudad blanca
1	Patch Panel	Patch Panel de 24 puertos para cableado UTP Categoría 6
1	Patch Panel de Fibra óptica	Permite la conectividad con el Data Center
1	Organizadores de cable UTP	Permiten distribuir de mejor manera el cableado de la red.

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

3.5.1.10. Elementos de acceso a la red de los usuarios finales.

Los elementos que se utilizan para el acceso a la red son portátiles y computadores de escritorio. Aproximadamente existen 20 portátiles correspondientes cada una a cada director de los distintos departamentos de la entidad, y alrededor de 380 computadores de escritorio, tomando en cuenta las dependencias internas y externas.

3.5.1.11. Situación actual del backbone de fibra óptica.

La información que se presenta a continuación se ha tomado de inventarios del GAD-Ibarra y un proyecto anteriormente realizado (Culqui Medina, 2013, págs. 131-134).

El GAD-Ibarra constantemente desarrolla proyectos innovadores y para eso necesita crear una infraestructura integrada y robusta para mejorar la calidad de los servicios que ofrece a los usuarios de la ciudadanía, además de compartir infraestructuras tecnológicas con empresas privadas y gubernamentales; por lo que se realiza convenios entre distintas entidades como son el Patronato Municipal de San Miguel de Ibarra, EMAPA, Bomberos y EMELNORTE para implementar una misma red de fibra óptica.

La entidad dispone de una red de fibra óptica entre algunas dependencias y el edificio principal para establecer una transmisión de datos confiable, con alta disponibilidad y eficiente con las unidades del edificio antiguo y las unidades de la casa de la Ibarreñidad. El backbone de fibra óptica es un medio de transmisión que permite altas velocidades de transmisión el cual ayuda a enviar gran cantidad de información sin interferencias.

3.5.1.11.1. Diagrama del backbone de fibra óptica.

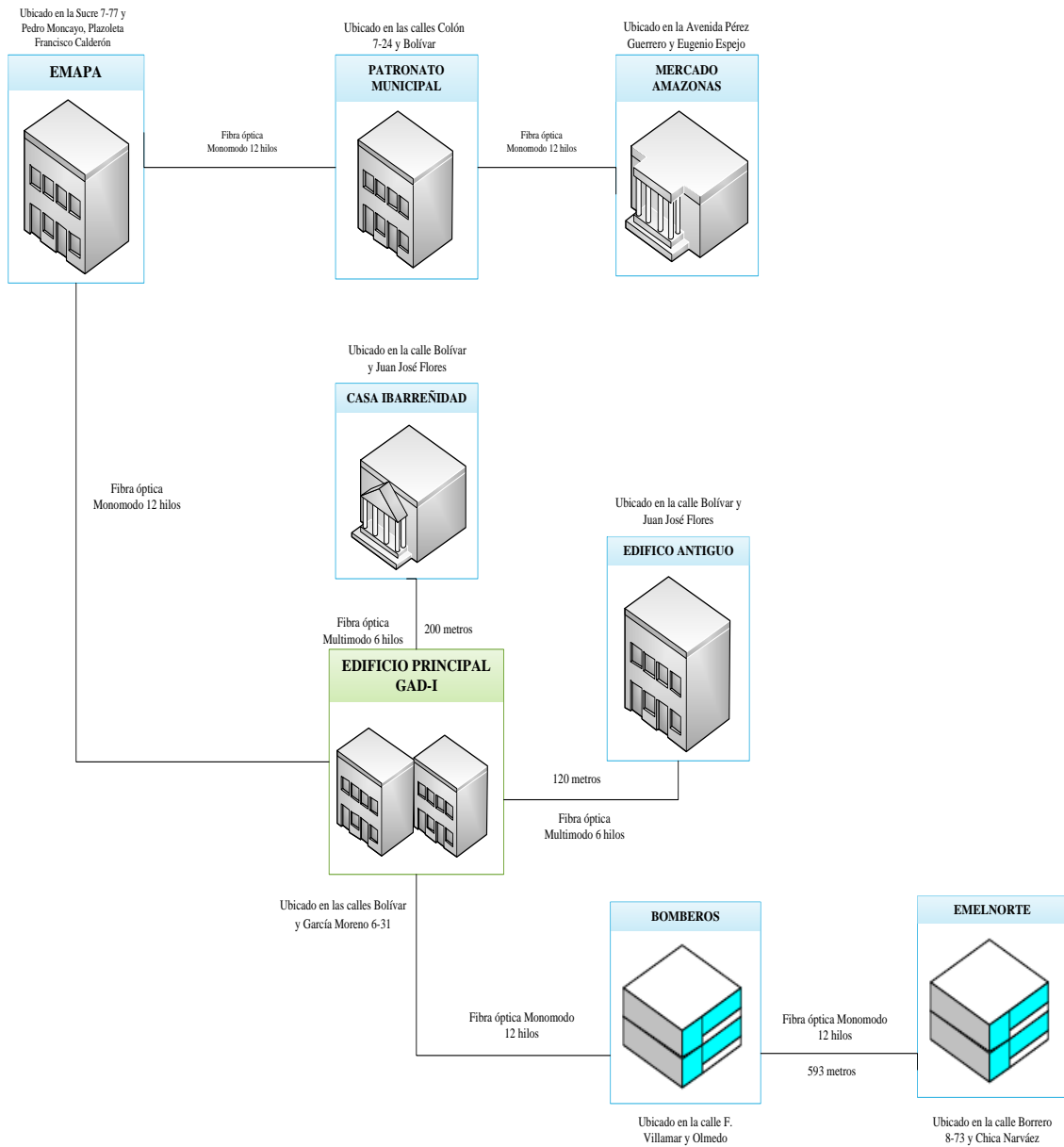


Figura 19. Diagrama del backbone de Fibra óptica

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

Cabe recalcar que para la implementación del proyecto solo se toma en consideración los enlaces hacia la casa de la Ibarreñidad y hacia el edificio antiguo.

3.5.1.11.2. Características del backbone de fibra óptica.

En la Tabla 10 se presenta las características del backbone de fibra óptica. Aproximadamente existe un total de 2155 metros de fibra óptica que sigue una trayectoria subterránea desde el GAD-Ibarra, EMAPA y Patronato Municipal.

En cada nodo se ubica un switch de perímetro con los equipos correspondientes que permiten la conectividad con las cámaras de vigilancia y con los cuartos de comunicación de cada entidad independiente al GAD-Ibarra, creando una sola infraestructura de datos.

Tabla 10. Características del backbone de fibra óptica

Origen	Destino	Tipo de conexión	Caraterísticas Generales
Edificio Principal del GAD-I	Edificio Antiguo	Tipo: Fibra óptica Hilos de fibra: 6	Velocidad de Transferencia de datos: 1 Gbps AB: 10/100/1000Mbps Distancia: 120 metros
Edificio Principal del GAD-I	Casa Ibarreñidad	Tipo: Fibra óptica Hilos de fibra: 6	Velocidad de Transferencia de datos: 1 Gbps AB: 10/100/1000Mbps Distancia: 200 metros
Edificio Principal del GAD-I	Bomberos	Tipo: Fibra óptica Monomodo Hilos: 12	Velocidad de Transferencia de datos: 1 Gbps AB: 10/100/1000Mbps Distancia: 400 metros
Bomberos	EMELNORTE	Tipo: Fibra óptica Monomodo Hilos: 12	Velocidad de Transferencia de datos: 1 Gbps AB: 10/100/1000Mbps Distancia: 593 metros
Edificio Principal del GAD-I	EMAPA	Tipo: Fibra óptica Monomodo Hilos: 12	Velocidad de Transferencia de datos: 1 Gbps AB: 10/100/1000Mbps Distancia: 342 metros
EMAPA	Patronato Municipal	Tipo: Fibra óptica Monomodo Hilos: 12	Velocidad de Transferencia de datos: 1 Gbps AB: 10/100/1000Mbps Distancia: 200 metros

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

3.5.2. Estructura lógica de la red local de datos.

En la Tabla 11 se detalla la estructura lógica que posee la entidad en sus distintas dependencias internas y externas. Se puede observar que la entidad cuenta con una distribución de vlan's que ayudan a reducir los tamaños de broadcast y mejorar la administración de la red.

Tabla 11. Distribución de VLAN

Distribución	Nro. de VLAN	Descripción	Enlaces	Interfaces
EDIFICIO PRINCIPAL				
SW-4500-CORE	VLAN 1	172.x.x.x		
	VLAN 2	172.x.x.x		
	VLAN 3	172.x.x.x /VoIP		
	VLAN 7	172.x.x.x		
			Enlace troncal	Gigabit Ethernet 1/1-3-11-12-15-17-18-19-20 Gigabit Ethernet 2/47
			Servidor VoIP	Gigabit Ethernet 2/48
SW-2960-RACK2-01	VLAN 1	DHCP		
	VLAN 2	172.x.x.x		
	VLAN 7	Tecnología		Fast Ethernet 0/13-24
SW-2960POE-RACK2-01	VLAN 2	172.x.x.x		
	VLAN 3	VoIP		Fast Ethernet 0/1-48
	VLAN 7	Tecnología		Fast Ethernet 0/1-2
			Enlace troncal	Gigabit Ethernet 0/3
SW-2960-RACK2-02	VLAN 1	172.x.x.x		
	VLAN 2	172.x.x.x		
			Enlace troncal	Gigabit Ethernet 0/1
SW-2960POE-RACK1-02	VLAN 2	172.x.x.x		
	VLAN 7-VLAN 3	Tecnología /VoIP		Fast Ethernet 0/1-3
	VLAN 3	VoIP		Fast Ethernet 0/4-48
			Enlace troncal	GigabitEthernet0/3
EDIFICIO ANTIGUO				
SW-2960POE-RACKS1-03	VLAN 3	VoIP		Fast Ethernet0/1-24
	VLAN 2	172.x.x.x		
			Enlace troncal	Gigabit Ethernet0/1
swea2960p101	VLAN 1	172.x.x.x		
CASA DE LA IBARREÑIDAD				
SW-2960POE-CULT-S1	VLAN 3	VoIP		Fast Ethernet 0/1-24
	VLAN 2	172.x.x.x		
			Enlace troncal	Gigabit Ethernet 0/1

Fuente: (GAD-Ibarra, 2013)

3.5.3. Análisis de la infraestructura de la red local de datos para identificar las áreas críticas.

Después de haber obtenido los datos de la infraestructura física y lógica de la red local de datos del GAD-Ibarra se procede a realizar un análisis conjuntamente con el administrador de la red, en el cual se determina las áreas críticas y los equipos mayor prioridad los cuales van hacer objeto para la posterior implementación.

3.5.3.1. Análisis para elección de switches.

Luego de establecer un diálogo con los administradores encargados de la red se determina que la principal área crítica de la red es el Data Center, tomando en consideración que su indisponibilidad provocaría la caída de toda la red de la entidad, por tal motivo es de primordial importancia implementar un modelo de gestión que pueda ayudar a evitar con anterioridad que lleguen a fallar los elementos activos de la red.

Se determina los dispositivos de red de mayor prioridad de acuerdo al establecimiento de un modelo jerárquico en capas, con su respectivo diagrama unifilar de puertos, como se observa en la Figura 20. Se estructuró en tres capas que son: núcleo, distribución y acceso los cuales cumple funciones específicas que se detallan a continuación:

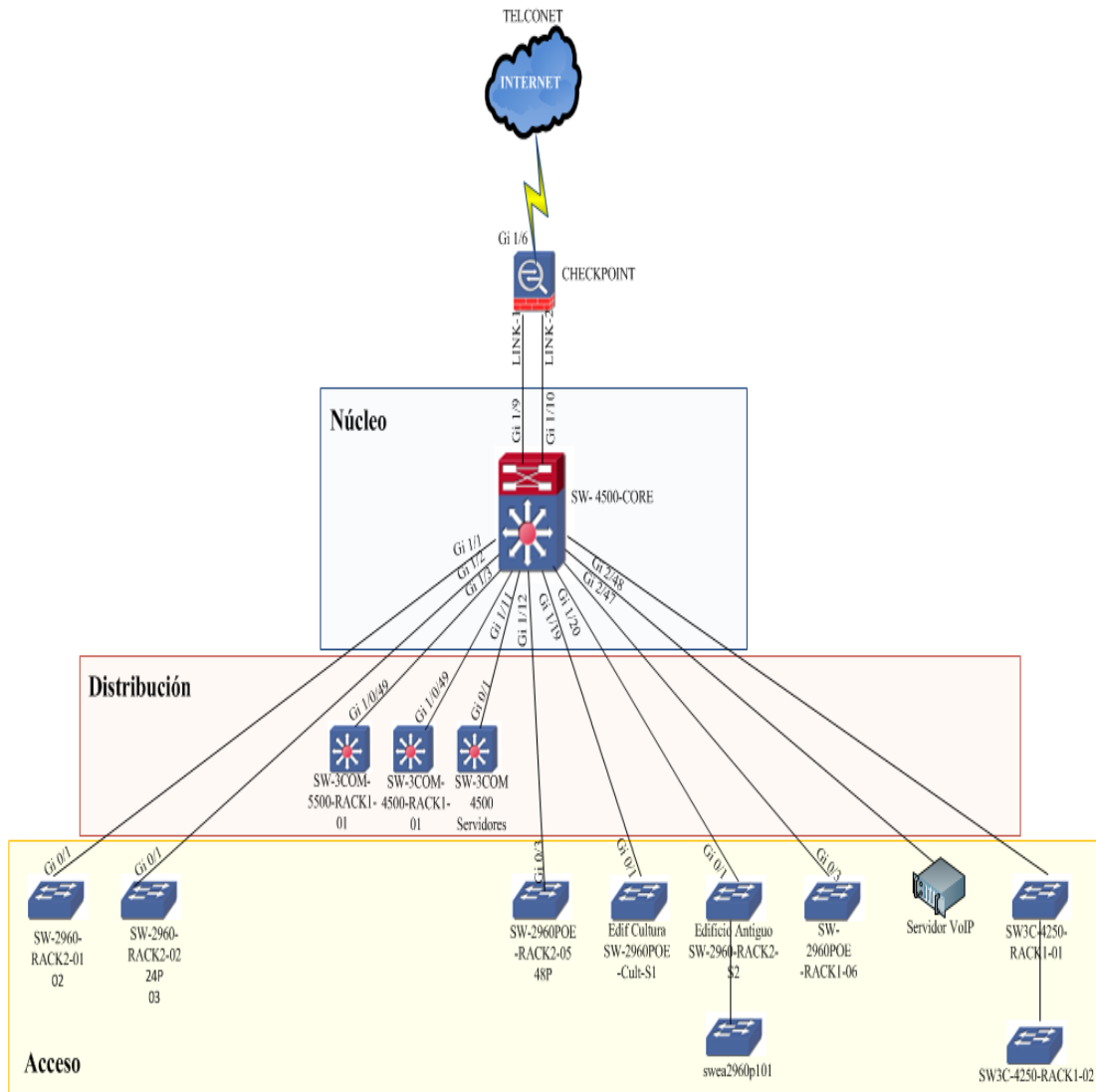


Figura 20. Modelo Jerárquico de la red del GAD-Ibarra

Fuente: (GAD-Ibarra, 2013)

3.5.3.1.1. Núcleo

Esta capa está constituida por un switch Cisco Catalyst 4503-E de alto rendimiento que es el Núcleo o Core; posee dos módulos de 48 puertos Gigabit Ethernet, ocho puertos SFP, los cuales son encargados de brindar conectividad a toda la entidad tanto a dependencias internas como externas de la misma, mediante enlaces de fibra óptica y administración de vlans.

Este equipo se interconecta a través de la controladora uno hacia la capa de distribución, capa de acceso y conjuntamente con el equipo Firewall Check Point, el mismo que se conecta a su vez con la red Internet de Telconet. Y a través de la controladora dos se conecta con un switch de la capa de acceso y el servidor de VoIP.

Por lo tanto por las funciones que posee dentro de la red de la entidad en esta capa se ha identificado el único switch 4503-E como prioritario y crítico, además cumple con las especificaciones técnicas para llevar a cabo la implementación del modelo de gestión.

3.5.3.1.2. Distribución

Dentro de esta capa se encuentran tres switches 3Com donde; el switch 3Com 4500G por ser el encargado del funcionamiento de los servidores físicos y virtuales es de carácter prioritario y crítico, porque de este dispositivo depende asegurar la entrega de los servicios a los usuarios de la entidad las 24 horas del día. Y los otros dos switch son encargados de interconectar a los segmentos de la red del edificio principal por lo tanto son considerados como críticos.

Estos equipos de red de acuerdo a sus características soportan la habilitación del protocolo SNMP pero a través de un software adicional propietario llamado 3Com Network Director ó 3Com Enterprise Management el cual carga automáticamente las MIB correctas y los archivos necesarios, por consiguiente en estos equipos se realizarán posteriores pruebas en la implementación para verificar su funcionamiento.

3.5.3.1.3. Acceso

Esta capa se encarga de establecer conectividad con los usuarios finales de la entidad integrando equipos de red como; impresoras de red, computadores, teléfonos IP, Access Point, entre otros. Los switches que conforman esta capa poseen un manejo de VLAN's que permiten segmentar los dominios de broadcast, y brindar mayor seguridad a los dispositivos del nodo final de la red, de tal manera que se ha establecido como área crítica.

Otra área crítica que se encuentra dentro de esta capa son los switch que están en las dependencias externas es decir; se consideró gestionar el switch que se ubica en el departamento de Cultura ya que este switch mantiene conectividad para el envío de información al edificio principal, es fundamental porque aquí se realizan actividades sociales y proyectos que deben ser supervisados por las autoridades de mayor orden.

Además dos switch que se encuentran en el edificio antiguo los cuales brindan conectividad a la planta baja y primera planta del mismo. Conjuntamente los switch escogidos para la gestión en esta área crítica son administrables y soportan la habilitación del protocolo SNMP.

Por lo antes mencionado se ha comprobado que los equipos poseen todas las características necesarias para implementar el modelo de gestión es decir, todos los equipos cuentan con (memoria, carga de procesador, interfaces de red y soportan la habilitación del protocolo SNMP) con la observación, de que los switches de marca 3Com se puede administrar eficazmente con un software propietario.

Además otro aspecto importante a tomar en cuenta es el monitoreo de interfaces de red críticas de los equipos, como se observa en la Figura 20 las interfaces de mayor prioridad son las del switch core porque del tráfico que genere cada una de ellas dependerá el correcto funcionamiento de toda la red esta particularidad se analizará posteriormente en la gestión de rendimiento.

3.5.3.2. *Análisis para elección de servidores.*

Para establecer este análisis se realizó la medición del tráfico en tiempo real para obtener la información acerca de los protocolos y aplicaciones más utilizadas por la red de la entidad, y determinar los servidores que están actualmente en funcionamiento, para eso se hizo uso del software de monitoreo llamado Ntop el cual se encuentra disponible para ejecutarse en Windows como en Linux y se basa en la librería de captura de paquetes libpcap. Ntop posee variadas características entre ellas:

- Utiliza una interfaz sencilla y mediante via web además es un proyecto de software libre.
- Permite la visualización de informes: globales de rendimiento de red, tráfico entre elementos, de sesiones activas de cada elemento, entre otros.
- Detecta posibles paquetes perniciosos.
- Analiza protocolos TCP/UDP/ICMP y dentro de TCP/UDP es capaz de agruparlos por tipo de servicio que se este utilizando como FTP, HTTP, SSH, DNS, Telnet, SMTP/POP/IMAP, SNMP.

La captura del tráfico se realizó mediante la configuración de un puerto espejo (SPAN, Switched Port Analyzer) en el switch núcleo Cisco Catalyst 4503-E que duplica en un solo puerto el tráfico que genera todo el switch y lo replica hacia el host en el que se encuentra instalado el software de monitoreo Ntop.

En seguida se indica los resultados obtenidos del tráfico generado por la red de la entidad, durante un periodo de tiempo de siete días consecutivos.

3.5.3.2.1. Distribución del tráfico generado por aplicaciones y protocolos.

Se procede a describir brevemente los protocolos y aplicaciones con mayor recurrencia ocupados dentro de la red de la entidad. En las gráficas presentadas a continuación se observa altos y bajos que se crean por mayor y menor grado de utilización de la red. En la Figura 21 se visualiza el tráfico generado por SSL¹⁹, el cual alcanza un volumen de datos de 1,1 MBytes/s y un promedio de 244,9 Kbytes/s este protocolo se posiciona en primer lugar al ser el más utilizado por la red.

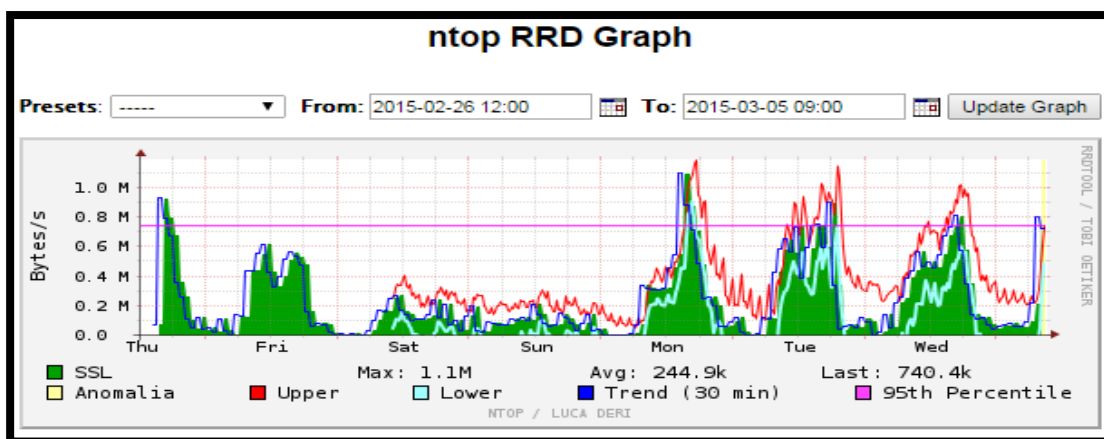


Figura 21. Volumen de tráfico generado por el protocolo SSL

Fuente: Resultados obtenidos del software de monitoreo Ntop

¹⁹ SSL.- Sus siglas en inglés Secure Socket Layer, en español Capa de Conexión Segura, protocolo criptográfico para establecer conexión segura entre un cliente y un servidor.

El segundo protocolo con mayor consumo en la red es el FTP²⁰ como se aprecia en la Figura 22 presenta un máximo consumo de 978,0 Kbytes/s y un promedio de 154,6 Kbytes/s.

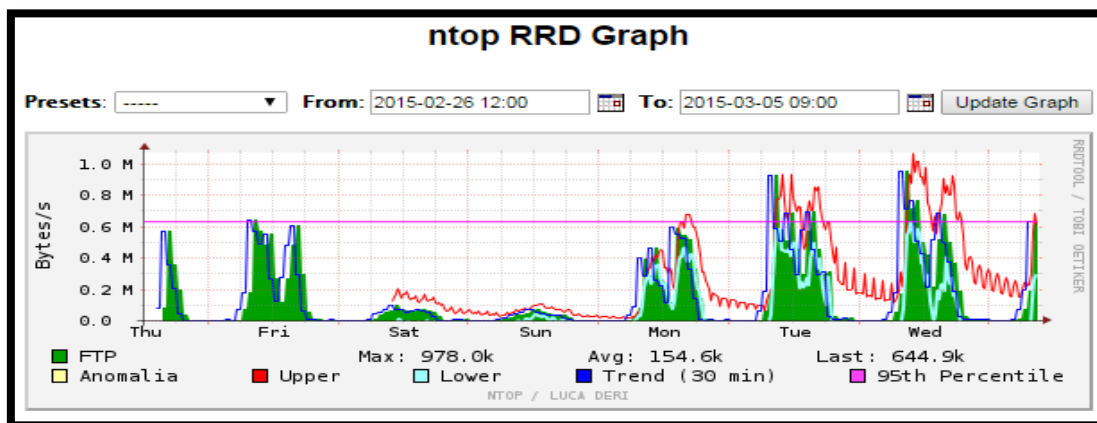


Figura 22. Volumen de tráfico generado por el protocolo FTP

Fuente: Resultados obtenidos del software de monitoreo Ntop

Como se observa en la Figura 23 el tercer lugar ocupa el protocolo HTTP que presenta un máximo consumo de volumen de datos de 660,9 Kbytes y un promedio de 109,6 Kbytes.

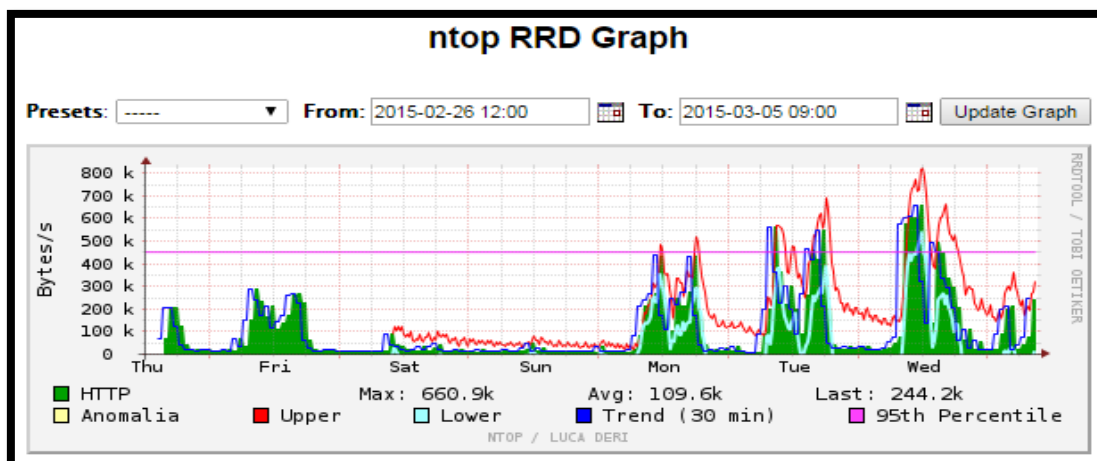


Figura 23. Volumen de tráfico generado por el protocolo HTTP

Fuente: Resultados obtenidos del software de monitoreo Ntop

²⁰ FTP.- Protocolo que permite a los usuarios transferir archivos entre ordenadores en una red TCP/IP.

En cuarto lugar se encuentra la aplicación para base de datos PostgreSQL²¹ que alcanza un valor máximo de 380,6 Kbytes/s y un valor promedio de 21,4 Kbytes/s como se observa en la Figura 24.

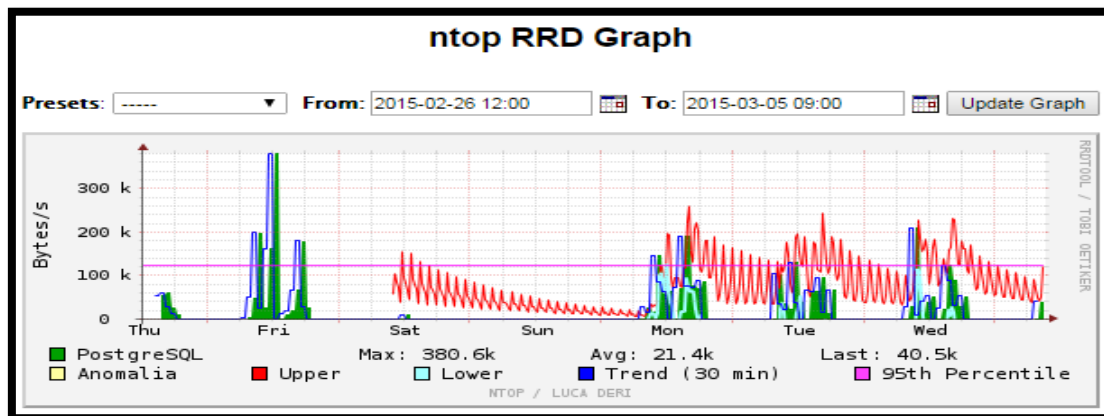


Figura 24. Volumen de tráfico generado por la aplicación PostgreSQL

Fuente: Resultados obtenidos del software de monitoreo Ntop

El volumen de tráfico máximo que presenta el protocolo RTP²² es de 91,2 Kbytes/s y un promedio de 14,9 Kbytes/s lo que hace que ocupe el quinto lugar como se puede observar en la Figura 25.

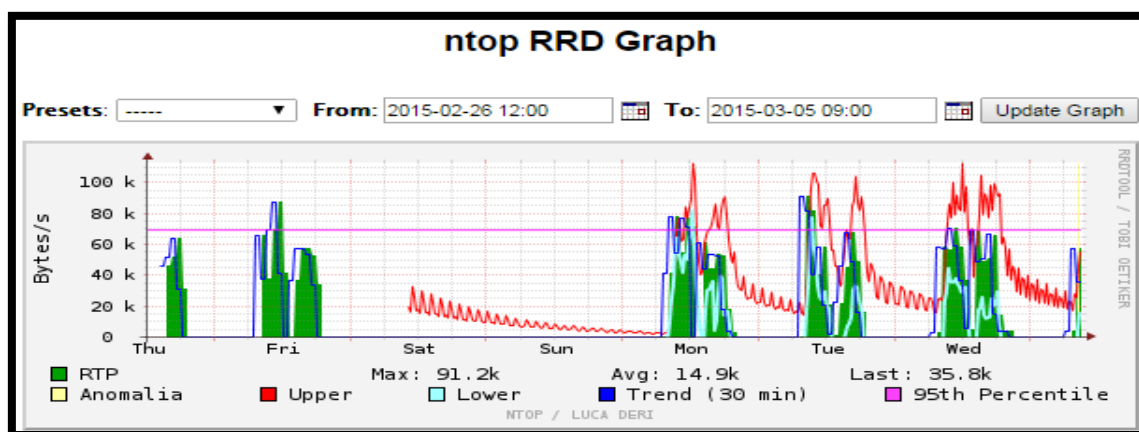


Figura 25. Volumen de tráfico generado por el protocolo RTP

Fuente: Resultados obtenidos del software de monitoreo Ntop

²¹ PostgreSQL.- Sistema de gestión de base de datos orientada a objetos y de código abierto.

²² RTP.- Protocolo de transporte en tiempo real utilizado para la transmisión confiable de voz sobre IP.

En la Figura 26 se describe un volumen de tráfico máximo generado por el protocolo POP, de 48,4 Kbytes/s y un promedio de 4,8 Kbytes/s por lo que ocupa el sexto lugar.

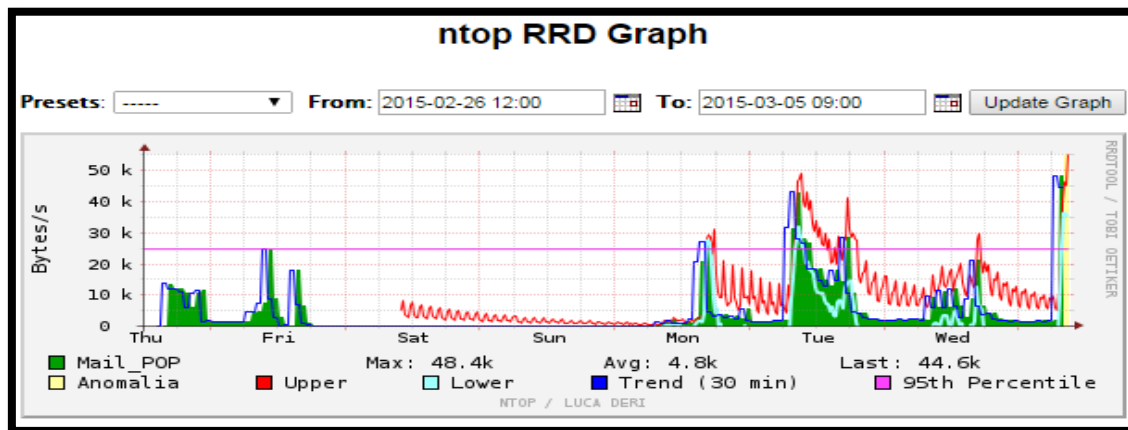


Figura 26. Volumen de tráfico generado por el protocolo POP²³

Fuente: Resultados obtenidos del software de monitoreo Ntop

En la Figura 27 se puede observar que el protocolo SIP²⁴ ocupa el séptimo lugar por el volumen de tráfico máximo consumido de 8,4 Kbytes/s y promedio de 6,4 Kbytes/s.

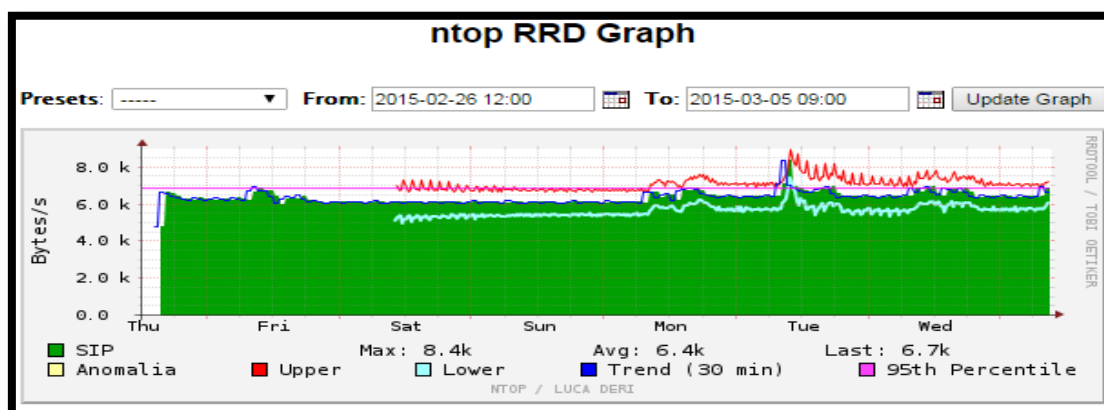


Figura 27. Volumen de tráfico generado por el protocolo SIP

Fuente: Resultados obtenidos del software de monitoreo Ntop

²³ POP.- Protocolo utilizado para recibir e-mails

²⁴ SIP.- Protocolo de inicio de sesiones utilizado en la configuración de llamadas de voz o video.

En la Figura 28 se observa el protocolo IMAP²⁵ con un volumen de consumo de datos máximo de 1,3 Kbytes/s y un promedio de 507,0 Bytes/s ocupa el octavo lugar.

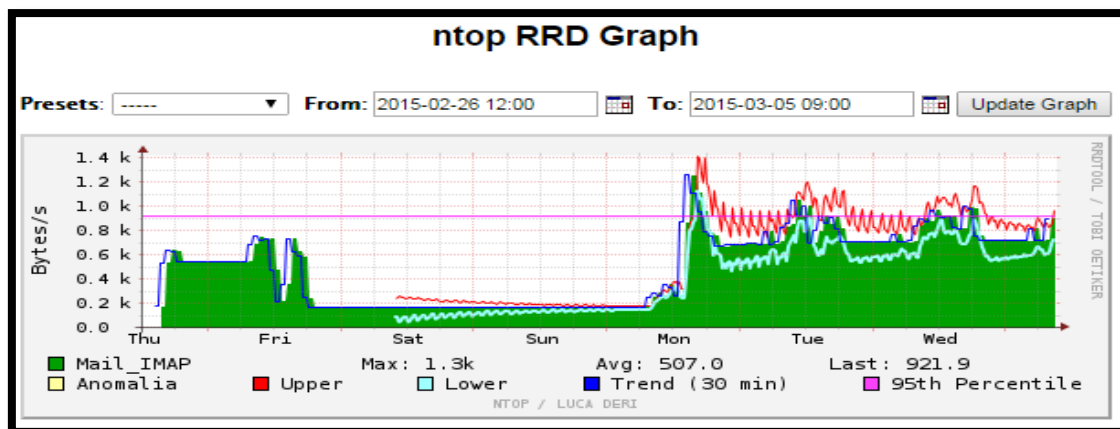


Figura 28. Volumen de tráfico generado por el protocolo IMAP

Fuente: Resultados obtenidos del software de monitoreo Ntop

En la Figura 29 se observa el servicio de nombres de dominio DNS²⁶ con un volumen de consumo de datos máximo de 618,0 Bytes/s y un promedio de 119,7 Bytes/s ocupa el noveno lugar.

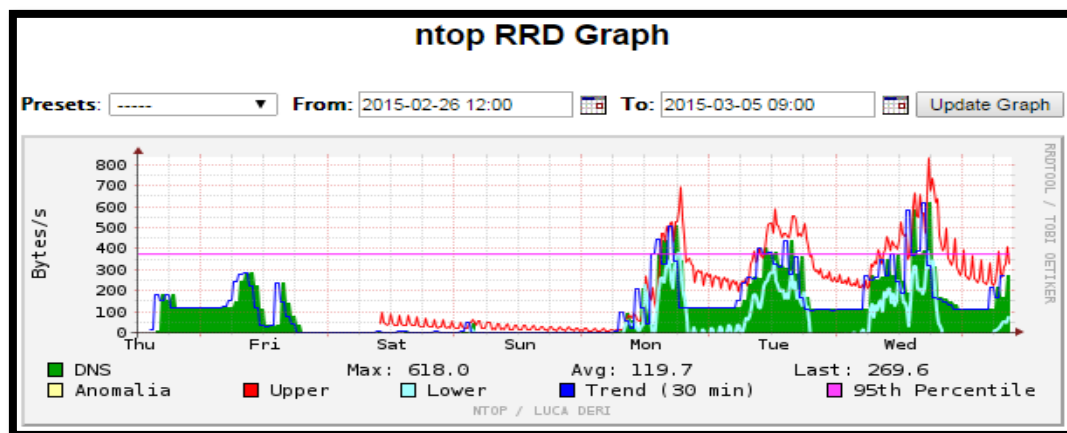


Figura 29. Volumen de tráfico generado por el protocolo DNS

Fuente: Resultados obtenidos del software de monitoreo Ntop

El protocolo SMTP²⁷ ocupa el décimo lugar con un volumen de tráfico máximo de 26,8 Bytes y promedio de 3,0 Bytes como se muestra en la Figura 30.

²⁵ IMAP.- Protocolo que permite el acceso a e-mails almacenados en un servidor de internet.

²⁶ DNS.- Es una base de datos distribuida y jerárquica, que sirve para resolver nombres en la redes IP

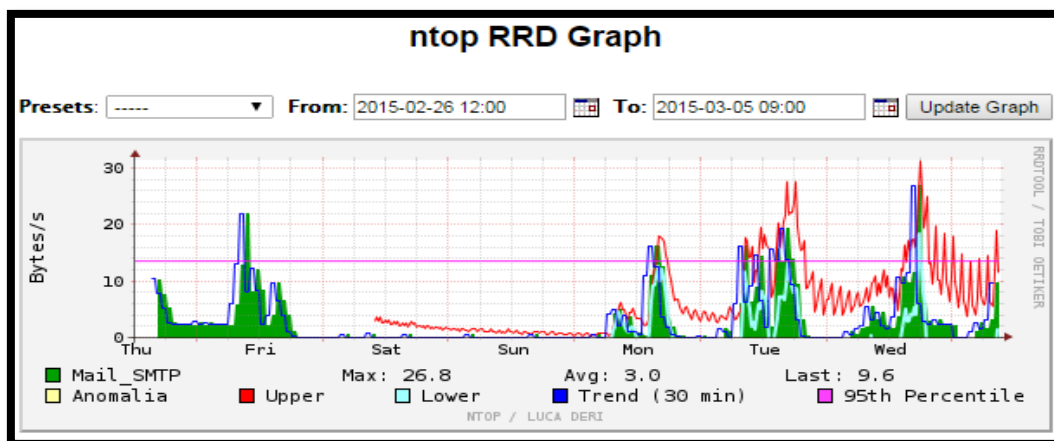


Figura 30. Volumen de tráfico generado por el protocolo SMTP

Fuente: Resultados obtenidos del software de monitoreo Ntop

A continuación la Figura 31 muestra en resumen otras aplicaciones y protocolos de menos recurrencia utilizados en la red de la entidad y capturados por Ntop.

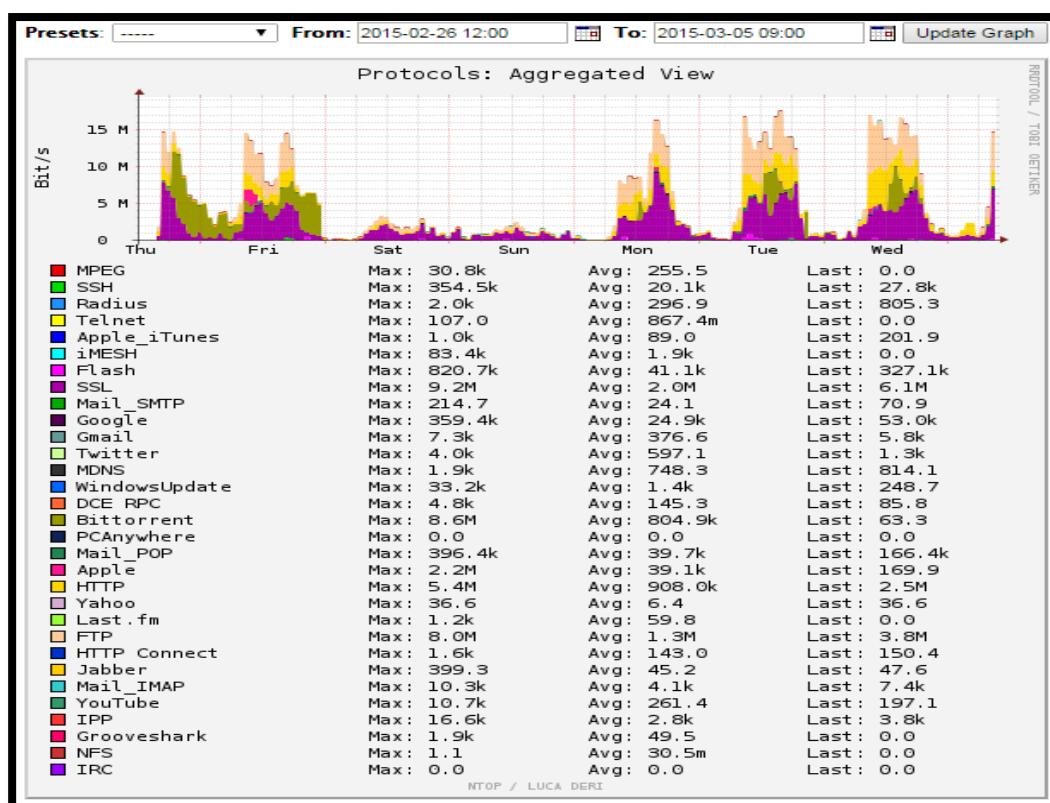


Figura 31. Volumen de tráfico general de aplicaciones y protocolos utilizados

Fuente: Resultados obtenidos del software de monitoreo Ntop

²⁷ SMTP.- Protocolo de red utilizado para el intercambio de mensajes de correo electrónico.

De acuerdo al análisis realizado con Ntop, durante siete días consecutivos, los servidores que están actualmente activos y en funcionamiento son los siguientes; como se puede observar en la Tabla 12 donde se expone el nombre del servidor, el sistema operativo utilizado, los datos enviados y recibidos, los protocolos que más consumen y el número de puerto que cada uno de ellos utiliza. En el Anexo C se presenta una descripción de como se obtuvo estos datos.

Tabla 12. Servidores Físicos y Virtuales en Funcionamiento del GAD-Ibarra

SERVIDOR	TIPO	SISTEMA OPERATIVO	Total Datos Enviados	Total Datos Recibidos	Protocolos más utilizados	Nro. de Puertos	Soporta SNMP
SERVIDOR HP BL 460 G6	Físico	Debian 6.0.1	--	--	--	--	SI
FREE NAS	Virtual	FreeNAS	192.7 MBytes	1,7GBytes	TCP, FTP	ntp (12) - netbios-ns (137) netbios-ssn (139) snmp (161) microsoft-ds - 445	NO
SERVIDOR DOCUMENTAL	Virtual	Debian 7.0.1	--	--	--	--	SI
SERVIDOR CONTROL DE PERSONAL	Virtual	Windows Server 2003	20,6 KBytes	13,3 KBytes	TCP, UDP, FTP	netbios-ns (137) – netbios-dgm (138) – netbios-ssn (139) – snmp (161) – microsoft-ds (445)	SI
SERVIDOR HP BL 460 G6	Físico	Debian 6.0.1	--	--	--	--	SI
SERVIDOR REPOSITARIOS	Virtual	Debian 6.0.1	66,2 MBytes	29,8 MBytes	TCP, MAIL_POP, HTTP	http (80) - netbios-ns (137) - snmp (161) - pop3s (995)	SI
SERVIDOR DE CORREO	Virtual	Ubuntu 12.04	4,0 GBytes	1,5 GBytes	TCP, MAIL_POP, SSL, HTTP	ssh (22) - smtp (25) – http(80) kerberos (88) – pop3 (110) - ntp (123) - netbios-ns (137) - imap2 (143) - https (443) - ssmtp (465) - domain (53) - login (513) - submission (587) - imaps (993)	SI
SERVIDOR DE SERVICIOS DE RED	Virtual	Debian 6.0.1	3,7 GBytes	1,7 GBytes	UDP, TCP, DNS	ftp-data (20) – ftp (21) – smtp (25) – domain (53) – http (80) – nntp (119) – kerberos (88) – ssh (22) –telnet (23)	SI
SERVIDOR DE REDMINE	Virtual	Debian 6.0.1	5,4 KBytes	2,8 KBytes	TCP, HTTP, SSH	ssh (22) - http (80)	SI
SERVIDOR NTP	Virtual	Debian 6.0.1	270 Bytes	604 Bytes	UDP, ICMP, ARP NTP	ntp (123)	SI
SERVIDOR SRI	Virtual	Windows Server 2003	2,3 MBytes	530,7 KBytes	TCP, FTP	netbios-ns (137) - netbios-ssn (139)	SI

SERVIDOR WEBSERVICE	Virtual	Debian 6.0.1	2,7 Kbytes	2,0 KBytes	TCP, ARP, SSH	ssh (22)	SI
SERVIDOR HP 160 G5 (Srv3)	Físico	Debian 5.0.1	--	--	--	--	SI
SISTEMA DOCUMENTAL QUIPUX	Virtual	Debian 5.0.1	84,6 MBytes	17,9 MBytes	TCP, HTTP, SSH	ssh (22) - http (80)	NO
SERVIDOR DE BALANCE SCORD CARD	Virtual	Windows Server 2000	478,1 KBytes	345,3 KBytes	TCP, UDP, ARP FTP, TeamViewer	netbios-ns (137) - netbios-ssn (139) - snmp (161) - microsoft-ds (445)	NO
SERVIDOR PROMOX HP DL 380 G5 (Srv5)	Físico	PROMOX	180 Bytes	46 Bytes	UDP, NTP	ntp (123)	NO
SERVIDOR MOODLE	Virtual	Debian 5.0.1	103.1 KBytes	93,0KBytes	TCP, UDP, ARP NTP, SSH	ssh (22), domain (53) - ntp (123)	SI
SERVIDOR HP BL 460 G8	Físico	Debian 7.0.1	0	196 Bytes	ICMP	--	SI
SERVIDOR APLICACIONES WEB	Virtual	Debian 7.0.1	45,5 MBytes	6,0 MBytes	TCP, HTTP, SSH MAIL_POP	ssh (22), domain (53), http (80)	SI
SERVIDOR VIRTUAL MAPAS (MAPSERVER)	Virtual	Debian 7.0.1	63,7 KBytes	10,5 KBytes	TCP, HTTP	http (80)	SI
SERVIDOR BDD POSTGIS	Virtual	Debian 7.0.1	0	396 Bytes	TCP, FTP	--	SI
SERVIDOR DE BDD POSTGREST	Físico	Debian 5.0.1	41,1 GBytes	7,6 GBytes	TCP, PostgreSQL	FTP, ftp (21) - domain (53) - http (80) ntp (123) - netbios-ns (137) - netbios-dgm (138) - netbios-ssn (139) - snmp (161) - microsoft-ds (445)	SI
SERVIDOR DE APLICACIONES TERCEROS OLYMPO	Físico	Windows Server 2003	11,4 GBytes	922,8 MBytes	FTP	domain (53) - http (80) - ntp (123) - netbios-ns (137) - netbios-dgm (138) - netbios-ssn (139) - microsoft-ds (445) - snmp (161)	SI
SERVIDOR DE ANTIVIRUS	Físico	Windows Server 2003	628,7 MBytes	187,2 MBytes	TCP, HTTP	http (80) - netbios-ns (137) - netbios-dgm (138) - netbios-ssn (139) - snmp (161)	SI

Fuente: (Unidad de Hardware y Comunicaciones, 2013)

3.5.3.3. Análisis para elección de servidores físicos.

Como se ha planteado anteriormente la principal área crítica de la red es el Data Center, por consiguiente los servidores implican una gran relevancia para la entidad, de forma tal que la interrupción de sus prestaciones implicaría un alto valor de pérdidas es por eso que su correcto funcionamiento es fundamental.

Con el análisis de la distribución del tráfico generado por aplicaciones y protocolos se puede concluir que el protocolo SSL es el más utilizado por la red, seguido por los protocolos FTP, HTTP, PostgreSQL, RTP, POP, SIP, IMAP, DNS, SMTP. Además el protocolo más utilizado por los servidores actualmente activos es TCP.

Por lo que para determinar los servidores de mayor prioridad y criticidad de la red se realizó el análisis tomando en cuenta la disponibilidad de funcionamiento y los datos obtenidos en la Tabla 12. Cabe recalcar que los servidores críticos que se van a monitorear son los que ocupan más volumen de datos enviados y recibidos. En la Figura 32 se identifica los puertos a los que se encuentran conectados los servidores en el Switch 3Com 4500G, aquellos serán tratados mediante el control de tráfico.

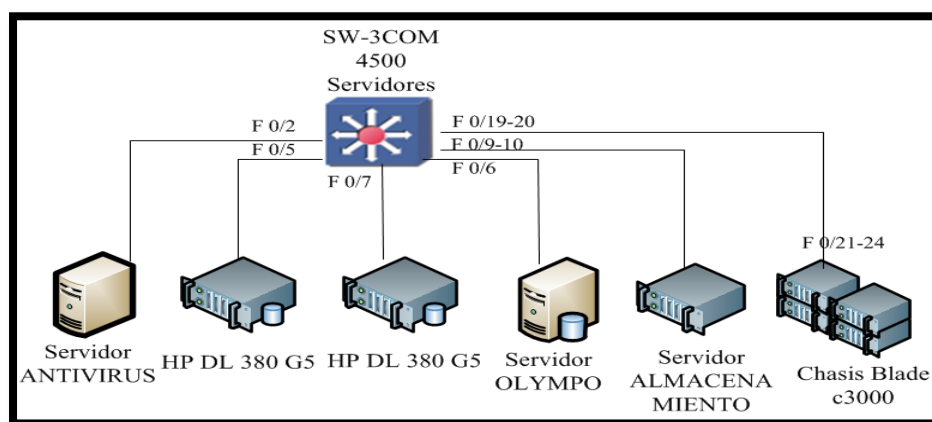


Figura 32. Mapeo de puertos del switch que interconecta los servidores

Fuente: (GAD-Ibarra, 2013)

3.5.3.3.1. *Servidor POSTGRESQL.*

Este servidor maneja un total de datos enviados de 41,1 GBytes y recibidos 7,6 GBytes por lo que se ubica en el primer lugar de mayor criticidad al ser un servidor de base de datos maneja un sistema integrado único que tiene procesos de impuestos, consultas, información de toda la ciudadanía si este llegaría a fallar no se podría realizar ningún trámite de los usuarios.

3.5.3.3.2. *Servidor OLYMPO*

Este servidor maneja un total de datos enviados de 11,4 GBytes y recibidos 922,8 MBytes por lo que se ubica en segundo lugar de mayor criticidad, es muy importante que su funcionamiento sea correcto ya que este es un sistema contable financiero cuando este llegaría a fallar se paralizaría los balances, pagos, elaboración de cheques, etc.

3.5.3.3.3. *Servidor de antivirus.*

Este servidor maneja un total de datos enviados de 628,7 MBytes y recibidos 187,2 MBytes por lo que ocupa el tercer lugar de mayor criticidad, si este dejaría de funcionar se puede propagar virus, gusanos, troyanos, etc., que afectaría el funcionamiento de la red.

3.5.3.3.4. *Servidores HP.*

Los servidores HP; BL 460 G6, 160 G5, DL 380 G5, no presentan un total de datos enviados y recibidos por lo que no presentan criticidad pero se implementará el monitoreo de conectividad, porque de estos dependen el funcionamiento de los servidores virtuales, tomando en cuenta que el chasis donde se conectan posee dos

puertos SAN los cuales tienen redundancia en una controladora de almacenamiento de tal manera que si un puerto llegaría a fallar quedaría funcionando el otro y de esa forma mantiene la conectividad de los servidores.

3.5.3.4. Análisis para elección de servidores virtuales.

El análisis para la elección de los servidores virtuales se realizó tomando en cuenta la disponibilidad de funcionamiento de los servicios que brinda cada uno de ellos dentro de la entidad, y de los datos obtenidos en la Tabla 12, a continuación se puntualiza cada servidor elegido para el monitoreo:

3.5.3.4.1. Servidor de Correo.

El servidor de correo presenta un total de datos enviados de 4,0 GBytes y recibidos de 1,5 GBytes, es el primero de los servidores prioritarios y críticos, debe estar funcionando correctamente porque la entidad trabaja solamente con cuentas de correo institucionales debido a que la información que se envía o recibe es de uso exclusivo y confidencial de la entidad, las cuentas de correo personales no está permitido usar para enviar información y como se observa en las gráficas generadas por Ntop anteriormente los protocolos que utiliza la red son Mail_IMAP, Mail_POP, Mail_SMTP. Por este motivo es de suma importancia que este servidor este constantemente monitoreado su espacio de disco, carga de cpu y memoria, caso contrario afectaría los procesos de funcionamiento al no poder enviar ni recibir información.

3.5.3.4.2. *Servidor DNS y DHCP.*

Este servidor presenta un total de datos enviados de 3,7 GBytes y recibidos de 1,7 GBytes, es el segundo prioritario y crítico porque dejaría de realizar sus funciones, los equipos perderían conectividad dentro de la red.

3.5.3.4.3. *Servidor documental Quipux.*

Este servidor presenta un total de datos enviados de 84,6 MBytes y recibidos de 17,9 MBytes, es el tercer servidor considerado como prioritario y crítico porque al dejar de funcionar hace que se paralice la gestión de trámites para envío y recepción lo cual retrasaría los procesos de atención hacia los usuarios.

3.5.3.4.4. *Servidor de repositorios.*

Este servidor presenta un total de datos enviados de 66,2 MBytes y recibidos de 29,8 MBytes, es el cuarto servidor prioritario y crítico, porque es indispensable el correcto funcionamiento para evitar una sobrecarga de paquetes en la red.

3.5.3.4.5. *Servidor de aplicaciones web.*

Este servidor presenta un total de datos enviados de 45,5 MBytes y recibidos de 6,0 MBytes, es el quinto servidor considerado como prioritario y crítico porque además es uno de los servidores que más consumen el protocolo HTTP, aquí se alojan las aplicaciones web para el intercambio de datos. Este servidor mantiene las páginas de alarmas, turismo, sismert, consulta de documentos, consulta de impuestos.

3.5.3.4.6. *Servidor SRI.*

Este servidor presenta un total de datos enviados de 2,3 MBytes y recibidos de 530,7 KBytes, es el sexto servidor considerado como prioritario y crítico porque aquí se encuentran los servicios destinados a contribuir con las necesidades de la ciudadanía, tales como: servicios de rentas y recaudaciones, proceso de cobros y transacciones que realizan directamente con los usuarios.

3.5.3.4.7. *Servidor MAPSERVER.*

Este servidor presenta un total de datos enviados de 63,7 KBytes y recibidos de 10,5 KBytes, es el séptimo servidor considerado como prioritario y crítico, es fundamental su correcto funcionamiento porque se utiliza para localizar ubicaciones de terrenos, casas, para los trámites de impuestos de la ciudadanía.

3.5.3.4.8. *Servidor WEBSERVICE.*

Este servidor presenta un total de datos enviados de 2,7 KBytes y recibidos de 2,0 KBytes, es el octavo servidor considerado como prioritario y crítico porque sirve para la comunicación con servicios web de instituciones financieras.

3.5.3.4.9. *Servidor de Base de datos POSTGIS.*

Los servidores de base de datos son primordiales que estén en funcionamiento las 24 horas del día porque ahí se encuentra alojada toda la información de años atrás de toda la ciudadanía, al fallar este servidor se paralizaría cualquier tipo de trámite porque no se podría acceder a la información requerida.

Los servidores virtuales restantes que no se toman en cuenta es porque no soportan la habilitación del protocolo SNMP y además si estos en algún momento dejarían de funcionar no afectaría el funcionamiento de la red, no son de carácter prioritario. Debido a los cambios de actualización algunos servidores no están disponibles.

CAPÍTULO IV

4. Gestión de la Red Local de Datos del GAD-Ibarra

En este capítulo se detalla inicialmente el establecimiento de políticas de gestión para posteriormente realizar el procedimiento de implementación de cada una de las herramientas de gestión utilizadas y finalmente se especifica los manuales de procedimientos.

4.1. Establecimiento de Políticas de Gestión para la Red Local de Datos del GAD-Ibarra

En este punto se establece las políticas de gestión, fundamentadas en las áreas del modelo de gestión de red funcional basadas en el estándar ISO y están dirigidas hacia los administradores de la red quienes tienen el compromiso de cumplirlas para mantener eficazmente la disponibilidad de funcionamiento de los dispositivos de red críticos.

Previamente se definen algunos términos que se utilizan para desarrollo de las políticas de gestión.

4.1.1. Introducción.

Las políticas de gestión que se presentan a continuación se establecen después de haber realizado el análisis de las áreas críticas de la red local de datos del GAD-Ibarra y el estudio de las áreas funcionales del modelo de gestión basadas en el estándar ISO, cubriendo las necesidades de la red de datos de la entidad de acuerdo a sus requerimientos.

La principal funcionalidad de realizar las políticas de gestión es para generar reglas que gobiernen el buen funcionamiento del modelo de gestión, las mismas que están orientadas a las personas encargadas de la administración de la red para que puedan actuar de forma inmediata y ordenada frente a cualquier inconveniente que se presente en el entorno de los dispositivos de red gestionados de la entidad y evitar que los servicios ofrecidos a la ciudadanía queden suspendidos.

Las políticas de gestión expuestas en este documento se interrelacionan conjuntamente con la implementación del punto 4.2 y el manual de procedimientos que se desarrolla más adelante en el punto 4.3 de este mismo capítulo.

**GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN
MIGUEL DE IBARRA**

POLÍTICAS DE GESTIÓN PARA LA RED DE ÁREA LOCAL DE DATOS



Versión:	1.0.0
Elaborado por:	<ul style="list-style-type: none"> ▪ Viviana Ayala
Revisado por:	<ul style="list-style-type: none"> ▪ Lcdo. Miguel Tobar Reina / Jefe del Área de Hardware y Comunicaciones. ▪ Ing. Gabriel Bucheli / Administrador de la red.
Aprobado por:	<ul style="list-style-type: none"> ▪ Ing. Carlos Gudiño / Director TIC

I. PROPÓSITO

El presente documento tiene como propósito dar a conocer las políticas de gestión que deberán cumplir los responsables de la administración de la red, con el fin de mantener la disponibilidad y rendimiento de la red.

II. CONCEPTOS PREVIOS

❖ Gestión de red

La gestión de redes tiene la finalidad de proveer organización, supervisión e integración de hardware, software y elementos humanos para monitorizar, probar, configurar, analizar y evaluar los recursos de la red de una forma eficaz y así garantizar un nivel óptimo de servicio a sus usuarios, a un determinado coste.

❖ Políticas de gestión

Actualmente no existe un determinado estándar que indique un proceso a seguir para establecer las políticas de gestión de red por lo tanto se tomará una política de gestión como directrices que representan el buen funcionamiento de los recursos gestionados de la red.

III. GENERALIDADES

- a) La redacción del presente escrito se ha realizado para que sea interpretado de una forma entendible por el personal conformado por el departamento TIC.
- b) Las políticas de gestión presentadas en este escrito se utilizan de referencia, por lo que está totalmente expuesta a cambios, siempre y cuando las nuevas reglas estén complementadas dentro del modelo de gestión de red.
- c) Toda persona que haga uso de las políticas sin importar el nivel organizacional en el que se encuentre dentro del departamento TIC deberá tratar de cumplir con un orden, dependiendo de los requerimientos suscitados en la red.

IV. NIVELES ORGANIZACIONALES

- a) **Director.-** Autoridad de nivel superior. Bajo su administración está la aceptación de las políticas de gestión, en concordancia con el encargado de la Unidad de Hardware y Comunicaciones y la Unidad de Informática.
- b) **Encargado de la Unidad de Hardware y Comunicaciones.-** Persona encargada del análisis previo del estado de la red de la entidad mediante evaluaciones de disponibilidad, mantenimiento y rendimiento. Mantiene informes de los procedimientos realizados conjuntamente en coordinación con la Unidad Informática.

- c) **Unidad Informática.-** Departamento dentro de la entidad, que se encarga del funcionamiento del Data Center para la efectividad del procesamiento de datos e información con todo lo relacionado a la instalación de redes LAN y WLAN, utilización, mantenimiento y actualización de equipos informáticos.

V. VIGENCIA

La documentación presentada con sus respectivas políticas de gestión entrará en vigencia desde el momento en que sea aprobado como documento técnico de gestión de red por las autoridades correspondientes del departamento TIC del GAD-Ibarra. Este conjunto de reglas deberá ser revisado y actualizado conforme a las exigencias de este departamento o en su defecto modificado en el momento en que haya la necesidad de realizar cambios fundamentales en la infraestructura tecnológica de la red de la entidad.

VI. REFERENCIA

El presente documento es realizado tomando como referencia el formato que la institución ya tiene de un proyecto anterior (Cevallos Michilena, 2013, págs. 55-82).

Actualmente no existe un estándar específico que ayude a la formulación de las políticas de gestión por tal razón se las realiza tomando como guía las áreas funcionales del modelo de gestión basado en el estándar ISO:

1. Políticas de Gestión de la red de área local de datos.

1.1 Objetivo de la Política de Gestión.

1.2 Compromiso de las Autoridades.

2. Gestión de Configuración.

2.1 Ingreso de dispositivos de red al software de gestión.

2.2 Configuración de dispositivos de red.

3. Gestión de Fallos.

3.1 Manejo de fallos.

3.2 Manejo de umbrales.

4. Gestión de Contabilidad.

4.1 Parámetros de monitoreo.

5. Gestión de Prestación.

5.1 Colección de datos estadísticos del rendimiento de la red.

5.2 Reportes.

6. Gestión de Seguridad.


6.1 Acceso al Software de Gestión.


6.2 Acceso a los dispositivos de red gestionados.


VII. TÉRMINOS Y DEFINICIONES	
GAD-Ibarra	Gobierno Autónomo Descentralizado de San Miguel de Ibarra, entidad encargada de brindar servicios eficientes en beneficio de la ciudadanía del cantón Ibarra.
Dirección de TIC	Departamento de tecnologías de la información y comunicación perteneciente al GAD-Ibarra, encargado de velar por todo lo relacionado a la utilización de los recursos informáticos, procesamiento de datos e información.
Red de Área Local	Son redes que se utilizan para conectar dispositivos de red que se encuentran dentro de en un solo edificio o en un campus de pocos kilómetros de longitud, para compartir recursos e intercambiar información.
Hardware	Componentes físicos tangibles que funcionan dentro de un sistema informático.
Software	Componentes lógicos intangibles necesarios que hacen posible la realización de tareas informáticas.
Dispositivos de red	Componentes hardware que permiten la interconexión y comunicación entre distintas dependencias.
Disponibilidad	Los servicios ofrecidos por la entidad a la ciudadanía siempre deben estar activos y en buen funcionamiento.
ISO (International Standarization Organization)	En español (Organización Internacional de Estándares). Entidad internacional encargada tanto de la evaluación como la gestión y puesta en práctica de procedimientos, normas de fabricación, comercio y comunicación, aceptadas y legalmente reconocidas.


SNMP(Simple Network Management Protocol)	Protocolo simple de administración de redes, opera en el nivel de aplicación, utilizando el protocolo de transporte TCP/IP, permitiendo supervisar, analizar y comunicar información de estado entre una gran variedad de equipos de red.
Historiales	Información que se muestra en determinados periodos de tiempo acerca del estado de los recursos locales de los dispositivos gestionados.
Estadísticas porcentuales	Datos que se indican en forma porcentual del estado de los recursos locales de los dispositivos gestionados como también gráficos que recolectan información del tráfico ocurrido en las interfaces de los dispositivos.
Reporte	Informe que puede ser obtenido en forma impresa o digital acerca del estado de los dispositivos gestionados.
Notificación	Es un aviso mediante correo electrónico o SMS de algún dispositivo gestionado que este fallando.

VIII. DESARROLLO DE POLÍTICAS DE GESTIÓN

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	1. Políticas de Gestión de la red de área local	DESTINATARIO	Administrador y usuarios
	CONTROL	1.1 Objetivos de las Políticas de Gestión		
<p>Art. 1. Dar a conocer la información necesaria del funcionamiento del sistema de gestión a las personas encargadas de la administración de la red, con sus respectivos lineamientos que deben cumplir y utilizar para evitar posibles problemas de falta de disponibilidad en los recursos locales hardware de los dispositivos gestionados.</p>				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	1. Política de Gestión de la red de área local	DESTINATARIO	Administradores de la red
	CONTROL	1.2. Compromiso de las Autoridades		
<p>Art. 2. La Dirección de TIC y el encargado de la unidad de Hardware y Comunicaciones, como responsables de la elaboración de las Políticas de Gestión para la red de área local el GAD-Ibarra, toman el compromiso de revisión constante y socialización de los lineamientos descritos en este documento.</p>				


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	2. Gestión de Configuración	DESTINATARIO	Administradores de la red
	CONTROL	2.1. Ingreso de dispositivos de red al software de gestión		
<p>Art. 3. Antes de ingresar un dispositivo al software de gestión el administrador deberá analizar el estado actual en el que se encuentra la red y posteriormente a eso deberá ingresar la información básica y técnica de los equipos que se integren al monitoreo, usando un formato de base de datos (Excel), mediante la cual pueda localizar el dispositivo sin pérdida de tiempo.</p> <p>Art. 4. Para el ingreso de equipos en la base de datos se usará la nomenclatura establecida por la Unidad de Hardware y Comunicaciones de GAD-Ibarra.</p>				


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	2. Gestión de Configuración	DESTINATARIO	Administradores de la red
	CONTROL	2.2. Configuración de dispositivos de red		
<p>Art. 5. Los equipos que se integran al sistema de gestión deberán tener una configuración básica que permita al administrador ubicarlos dentro de la red con facilidad y asignarles los servicios respectivos.</p> <p>Art. 6. Para que el administrador de la red pueda proceder a la configuración de los equipos estos deben soportar SNMP, el cual deberá ser configurado con su respectiva sintaxis para poder ser gestionado.</p> <p>Art. 7. Si se realiza cambios en los equipos de la red o en sus configuraciones, estos cambios deberán ser actualizados en la base de datos, para tener un orden y un buen</p>				


funcionamiento de los mismos.

Art. 8. Las personas encargadas de la administración de la red deberán tener un respaldo de las configuraciones de los equipos como también la documentación actualizada del mapa topológico de la red con sus respectivos enlaces tanto de fibra óptica como del cableado estructurado y sus relativas velocidades de transmisión para evitar que se originen cuellos de botella en los enlaces.


Para la realización de los artículos antes mencionados de la política número dos se presentan los formatos para el registro de equipos y configuraciones de los mismos, en el manual de gestión de configuraciones ubicado en el ítem 4.3.2


 GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
DOMINIO	3. Gestión de Fallos	DESTINATARIO	Administradores de la red
CONTROL	3.1. Manejo de Fallos		
<p>Art. 9. El administrador de la red deberá detectar un fallo de un dispositivo de red crítico a través de la visualización del monitoreo que presenta la interfaz web del software de gestión o mediante la notificación de correo electrónico o SMS para poder posteriormente aislarlo, diagnosticarlo y corregirlo.</p> <p>Art. 10. Las personas encargadas de la administración de la red deberán dar las soluciones respectivas en el menor tiempo posible, evitando la falta de disponibilidad de los servicios que ofrece la entidad a la ciudadanía.</p>			

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	3. Gestión de Fallos	DESTINATARIO	Administradores de la red
	CONTROL	3.2. Manejo de umbrales		
<p>Art. 11. El administrador de la red deberá revisar los niveles de umbrales que se establecen en el software de gestión para generar las alertas de los estados como; advertencia, desconocido, crítico y recuperado de los dispositivos de red gestionados para previamente ser notificado.</p> <p>Para el desempeño de los artículos antes mencionados de la política número tres se tomará el procedimiento detallado en el manual de gestión de fallos ubicado en el ítem 4.3.3.</p>				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	4. Gestión de Contabilidad	DESTINATARIO	Administradores de la red
	CONTROL	4.1. Parámetros de monitoreo.		
<p>Art. 12. El administrador de la red deberá revisar que los dispositivos que ingresen al software de gestión cumplan con los parámetros fundamentales de monitoreo los cuales sirven para evitar que se susciten fallos inesperados en la red de la entidad tanto en las dependencias internas como externas.</p> <p>Art. 13. Con la finalidad de exponer en la interfaz web del software de gestión el correcto funcionamiento de los dispositivos de red críticos el administrador deberá conocer los parámetros de monitoreo, estado, chequeo y tiempo de cada uno de ellos.</p> <p>Art. 14. El GAD-Ibarra es una entidad sin fines de lucro, por lo que la facturación no se toma en cuenta en la realización de este modelo de gestión.</p>				


Para la realización de los artículos antes mencionados se presentan los parámetros de monitoreo en el manual de gestión de contabilidad, ubicado en el ítem 4.3.4.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	5. Gestión de Prestaciones	de	DESTINATARIO
CONTROL	5.1. Colección de datos estadísticos del rendimiento de la red			
<p>Art. 15. La dirección TIC podrá observar el rendimiento de los recursos locales de los dispositivos de red en forma porcentual en la interfaz web del software de gestión.</p> <p>Art. 16. Los administradores de la red podrán visualizar el consumo de ancho de banda que generan las interfaces de red mediante gráficos que miden el rendimiento de cada uno de los enlaces críticos.</p>				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	5. Gestión de Prestaciones	de	DESTINATARIO
CONTROL	5.2. Reportes			
<p>Art. 17. La dirección de TIC, podrá tener en forma impresa todos los informes e historiales de la información que necesiten acerca de los recursos monitoreados por el software de gestión.</p> <p>Art. 18. La dirección de TIC, podrá tomar los reportes del software de gestión en forma, diaria, mensual y anual, para estar al tanto del proceso de funcionamiento de los recursos activos de la red.</p> <p>Art. 19. Al término de cada mes el administrador deberá sacar un reporte para poder tener constancia de la disponibilidad de funcionamiento de los recursos locales</p>				


monitoreados por el software de gestión.

Para la realización de los artículos antes mencionados de la política número cinco se presentan el rendimiento de los recursos en el manual de gestión de prestaciones ubicado en el ítem 4.3.5.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	6. Gestión de Seguridad	DESTINATARIO	Administradores de la red
	CONTROL	6.1. Acceso al software de gestión		

Art. 20. Solamente las personas encargadas de la administración de la red podrán ingresar al sistema de gestión mediante el acceso único, autorización y confidencialidad que se debe tener con la información de la entidad.

Art. 21. Las notificaciones de cualquier percance que se suscite en los dispositivos gestionados se enviarán solamente a los administradores de la red a través de SMS o correo electrónico.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA			
	DOMINIO	6. Gestión de Seguridad	DESTINATARIO	Administradores de la red
	CONTROL	6.2 Acceso a los dispositivos de red gestionados		

Art. 22. El sistema de gestión está sujeto a cambios de configuraciones, nuevas actualizaciones o ingreso de nuevos equipos de red a ser gestionados por lo tanto estas modificaciones las realizarán exclusivamente las personas encargadas de la administración de la red.

Art. 23. El acceso a los dispositivos gestionados solo debe ser posible bajo una

contraseña de seguridad asignada por el administrador de la red, que posibilite los permisos necesarios para el acceso y administración remota del dispositivo.

Para la realización de los artículos antes mencionados de la política número seis se presenta el acceso al software de gestión en el manual de gestión de seguridad, ubicado en el ítem 4.3.6.

4.2. Implementación de Herramientas de Gestión en la Red Local de Datos del GAD-Ibarra

La presente sección del capítulo describe el desarrollo que se realizó para llevar a cabo la implementación del proyecto enfocado en las áreas críticas de la red local de datos, tomando en cuenta las cinco áreas funcionales del modelo de gestión de red y su interacción en el proceso.

4.2.1. Implementación dentro de la Gestión de Configuración.

Esta área de gestión comprende en realizar el análisis de la situación actual de la red de datos del GAD-Ibarra para conocer el estado físico y lógico en el que se encuentra, análisis que se realizó en el Capítulo III y donde se determinó las áreas críticas de la red, estableciendo de esta manera un orden entendible del proceso generado para la implementación del proyecto.

4.2.1.1. Requerimientos para elección del software de gestión.

Para iniciar el proceso de implementación dentro de esta área de gestión es necesario realizar un previo análisis comparativo de las funcionalidades y mejores características de software de gestión libres, como se puede ver a detalle en el Anexo D.1, se ha seleccionado Pandora FMS, Zabbix, Cacti y Nagios. El software de gestión fue elegido en base al estándar IEEE Std. 830-1998, el cual es el encargado de proporcionar normas para la creación de Especificación de Requisitos de Software (ERS) que están estructuradas tomando como referencia el cumplimiento del modelo de gestión FCAPS y las necesidades de la entidad. A continuación en la Tabla 13 se

presenta la valoración obtenida de la evaluación realizada que se presenta a detalle en el Anexo D.2:

Tabla 13. Evaluación de Software de Gestión

Requerimientos	PANDORA FMS	ZABBIX	CACTI	NAGIOS
REQ#1	1	1	1	1
REQ#2	0	0	1	1
REQ#3	1	1	0	1
REQ#4	1	1	1	1
REQ#5	2	2	2	2
REQ#6	1	1	1	1
REQ#7	1	1	1	1
REQ#8	1	1	1	1
REQ#9	1	1	1	2
REQ#10	1	1	1	1
REQ#11	1	1	1	1
REQ#12	1	1	2	1
REQ#13	0	0	0	1
REQ#14	1	1	1	1
Total	13	13	14	<u>16</u>

Fuente: Extraída de análisis realizado Anexo D.2.

Al realizar la calificación de cada requerimiento planteado se puede considerar que la puntuación entre ellos es relativa es decir todos los software de gestión planteados cumplen un sin número de características y funcionalidades que se acercan a los requerimientos planteados en el proyecto, sin embargo Nagios es un software de gestión líder en el mercado en cuanto a reconocimiento y cantidad bibliográfica disponible.

Nagios ha sido elegido porque cumple con los aspectos requeridos por el modelo de gestión FCAPS, aspectos como; presentar una interfaz de gestión centralizada, soportar el monitoreo remoto de varios sistemas operativos, establecimiento de umbrales que generan alertas cuando llegan a su límite máximo de funcionamiento y envían notificaciones de correo electrónico o SMS al administrador de la red, proporciona distintas opciones para la generación de informes, datos estadísticos,

basándose en la información recolectada y además soporta su instalación en un entorno virtualizado característica fundamental para el desarrollo de la implementación. A continuación se describe brevemente los archivos y directorios principales de Nagios.

4.2.1.1.1. Archivos principales de Nagios.

Para iniciar el monitoreo con Nagios es necesario crear y modificar varios archivos de su estructura como se muestran en la Figura 33 (Nagios Enterprises, 2014):

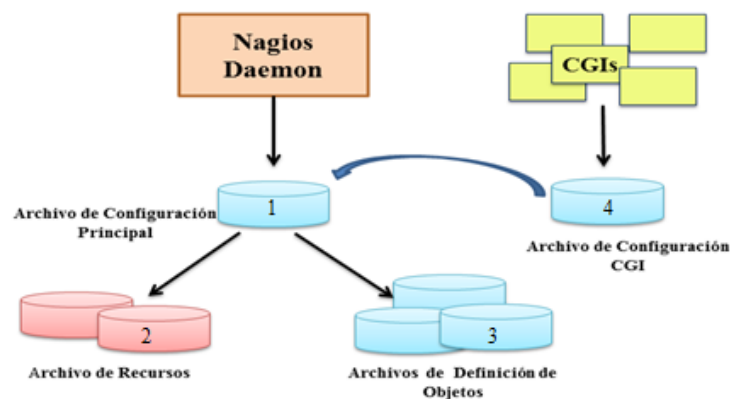


Figura 33. Estructura de Archivos Nagios

Fuente: (Nagios Enterprises, 2014)

1. Archivo de configuración principal.
2. Archivos de recursos.
 - Host
 - Grupos de Host (host groups)
 - Comandos (commands)
 - Servicios (services)
 - Grupo de Servicios (service groups)
3. Archivos de definición de objetos.

- Contactos (contacts)
 - Grupos de Contactos (contactsgroups)
 - Periodos de tiempo (timeperiods)
 - Plantillas (templates)
4. Archivos de configuración CGI.

4.2.1.1.2. Directorios principales de Nagios.

Nagios almacena su configuración, funcionamiento y ejecución en un directorio independiente ubicado en `/usr/local/nagios` que a su vez tiene subdirectorios, nombrados a continuación, que sirven de enlace para la puesta en marcha del software:

- `/usr/local/nagios/bin`
- `/usr/local/nagios/etc`
- `/usr/local/nagios/libexec`
- `/usr/local/nagios/sbin`
- `/usr/local/nagios/share`
- `/usr/local/nagios/var`

En el Anexo E ítem E.1.1.1 se puede observar detalladamente la descripción de archivos y directorios que posee Nagios para su configuración.

4.2.1.1.3. Requerimientos hardware para Nagios.

En la Tabla 14 se indica los requerimientos mínimos necesarios para el funcionamiento de Nagios de los cuales se ha establecido conveniente asignar los requerimientos virtuales basado en el estudio del estándar IEEE 830 donde se explica

que para aproximadamente 50 equipos y 250 servicios son necesarios los valores que se observan a continuación:

Tabla 14. Requerimientos Hardware para Nagios

Recursos	Requerimientos Mínimos	Requerimientos Virtuales Utilizados
Memoria RAM	1 GB	4 GB
Disco Duro	40 GB	80 GB
Procesador	Intel (R) Core (TM) 1.8 GHz	Intel (R) Xeon (R) E55600 @ 2.8 GHz Asignado CPU virtual: CPUv4

Fuente: Análisis Anexo D.1.4

4.2.1.2. Diseño utilizado para implementar el modelo de gestión de red funcional.

Una vez determinado el software de gestión a utilizar y los requerimientos hardware que necesita para su funcionamiento se procedió a realizar el diseño del sistema de gestión como se indica en la Figura 34. Donde se explica que el servidor de administración Nagios se encuentra instalado en un servidor físico HP BL 460 G6 mediante un entorno virtualizado, el mismo que está conectado al switch 3Com 4500 G y a la vez este está conectado con el switch Core 4503-E, donde se encuentra conectada toda la red local de datos de la entidad. Nagios fue instalado en el sistema operativo Debian 6.0.1 debido a que los servidores actualmente se encuentran dentro de un entorno de virtualización y utilizando esta versión de software libre, porque para los administradores de la red esta versión de Linux es la que más utilizan por su fácil adaptación.

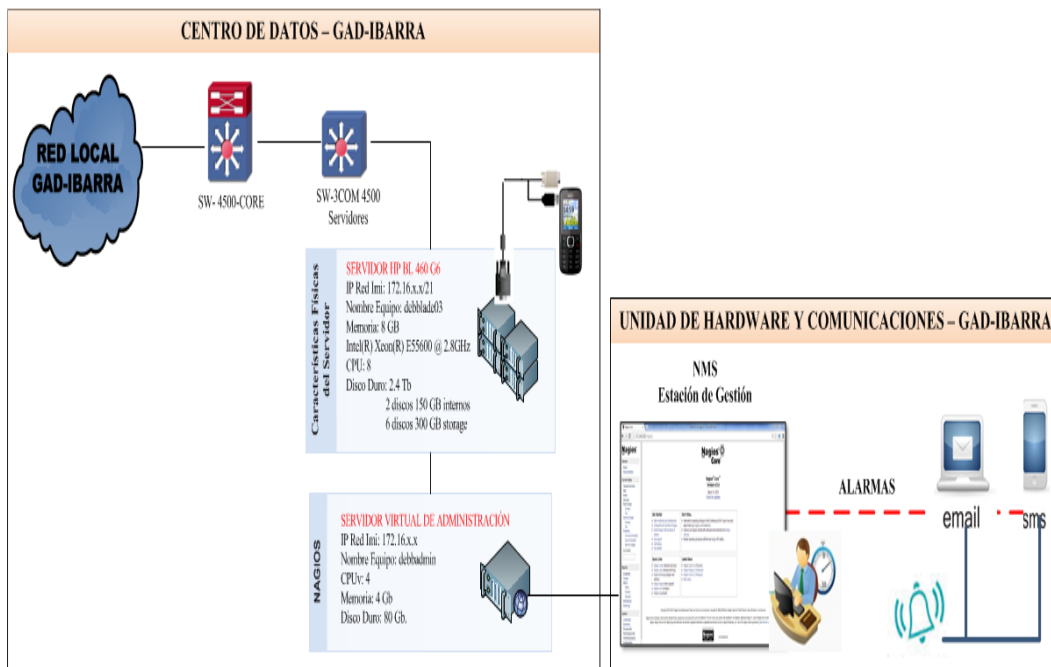


Figura 34. Diseño del Sistema de Gestión implementado

Fuente: Basada en inventario de TIC del GAD-Ibarra

4.2.1.3. Configuración del Gestor.

Dentro de este complemento de la gestión de configuración se incluye la secuencia de pasos de instalación que necesita el software de gestión Nagios para entrar en funcionamiento y en la Figura 35 se ilustra la misma:

- Instalación y configuración del software de gestión Nagios.
- Configuración de SNMP para establecer comunicación con los agentes.
- Configuración de PNP4Nagios para generar gráficos de los enlaces críticos.
- Configuración de NRPE complemento de Nagios para establecer comunicación con servidores físicos y virtuales que funcionen dentro de software libre.
- Configuración de un servidor de correo el cual sirve de transporte para el envío de correo electrónico al administrador acerca de los estados críticos de los dispositivos gestionados.

- Configuración de una aplicación para el envío de mensajes de texto cortos (SMS).

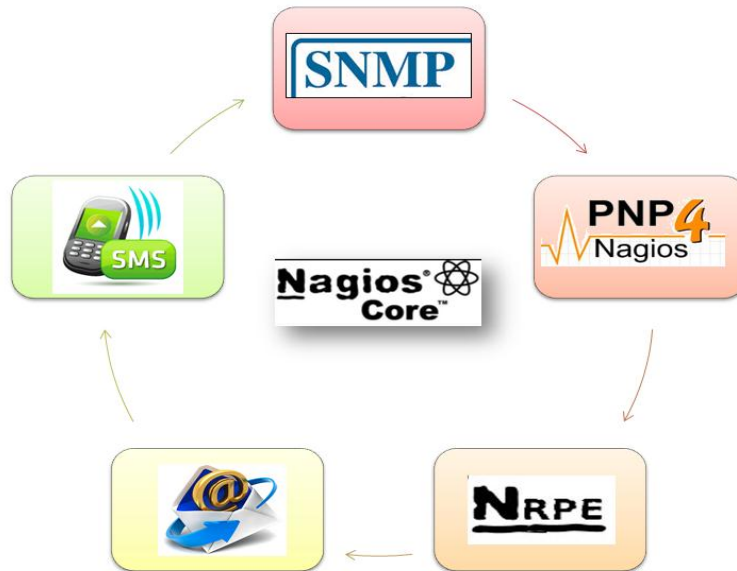


Figura 35. Representación del orden de Instalación

Fuente: Basada en software de gestión Nagios

4.2.1.3.1. Instalación y configuración del software de gestión Nagios.

Previamente a la configuración de Nagios se debe instalar ciertos requerimientos de software que se puntualizan a continuación:

- Servidor web Apache.
- PHP: intérprete de lenguaje de script PHP, para algunos plugins que lo requieran.
- Perl: intérprete de lenguaje de script Perl, para algunos plugins que lo requieran.
- GCC: librerías de desarrollo y compilación.
- Net:: paquete SNMP para comunicarse con los dispositivos a través del protocolo SNMP.

- Se necesita la biblioteca de gráficos GD para la visualización de la interfaz web de Nagios para crear un mapa de ubicación y tendencias de las imágenes. También se necesita instalar bibliotecas para JPEG, imágenes PNG para que GD puede crear imágenes en estos formatos.

Como se puede observar en la Tabla 15 se ha utilizado los paquetes en sus versiones estables y actuales:

Tabla 15. Requerimientos del Software Nagios

Software	Versión
Debian	6.0.1
Apache	2.2.x
PHP	5.3.x
LibGD	2.1.0
Nagios Core	4.0.4
Plugins Nagios	2.0.0
NRPE	2.15
PNP4Nagios	0.6.21
Net-SNMP	5.7.2.1

Fuente: Basada en Anexo E.1.2

1. Instalación de Nagios

- a) Se crea la cuenta del usuario Nagios y la asignación de contraseña.
- b) Crear los grupos de Nagios.
- c) Asignar los usuarios a sus respectivos grupos.
- d) Descargar el paquete de nagios-4.0.4.tar.gz.
- e) Descomprimir, ingresar e instalar el paquete nagios-4.0.4.tar.gz.
- f) Crear un usuario (**nagiosadmin**) http para el acceso vía web a Nagios.
- g) Reiniciar el servicio Apache para que actualice el último cambio.
- h) Crear enlace para que Nagios arranque el inicio automáticamente.

- i) Comprobar configuración y reinicio de Nagios.

2. *Instalación de Plugins*²⁸

- a) Descargar el paquete de Plugins *nagios-plugins-2.0.tar.gz*.
- b) Descomprimir e ingresar el paquete *nagios-plugins-2.0.tar.gz*.
- c) Compilar e instalar los Plugins.

El procedimiento de configuración de Nagios y sus Plugins se presenta a detalle en el Anexo E ítem E.1.2 con todos sus requerimientos para su eficaz funcionamiento.

4.2.1.3.2. *Instalación de agente SNMP.*

Se realiza la configuración de SNMP en el software de gestión para que pueda comunicarse con los dispositivos gestionados en los cuales también se instala este agente y pueda obtener información del estado de sus recursos.

Los servidores Linux utilizan el demonio `snmpd` para petitionar información de administración desde el gestor hacia los agentes. Para la configuración de este agente se presenta a detalle en el Anexo E ítem E.1.2.1.

- Instalar el demonio `snmp` y `snmpd`
- Modificar los archivos de configuración `snmp.conf` y `snmpd.conf`
- Iniciar el servicio SNMP

²⁸Plugins.- Es un complemento de un software que añade una funcionalidad adicional.

4.2.1.3.3. *Instalación de PNP4Nagios.*

PNP4Nagios es un complemento que posee Nagios para analizar los datos obtenidos de rendimiento y realizar gráficas del estado de las interfaces de red activas, en las últimas horas, días, semanas y meses las cuales son almacenadas automáticamente en la base de datos Round Robin (RRD²⁹). El proceso de instalación y configuración a seguir se indica a continuación y en el Anexo E ítem E.1.2.2 se lo detalla:

- Instalar librerías previas para la visualización de las gráficas.
- Descargar el paquete de pnp4nagios-0.6.21.tar.gz.
- Ingresar, compilar e instalar el paquete pnp4nagios-0.6.21.tar.gz.
- Necesita el módulo de reescritura activa en apache.
- Configurar los archivos nagios.cfg, commands.cfg, templates.cfg
- Reiniciar apache y acceder a la interfaz de pnp4Nagios.
- Iniciar el servicio pnp4nagios.

4.2.1.3.4. *Instalación de agente NRPE³⁰.*

Nagios necesita la configuración del agente NRPE para comunicarse con dispositivos que utilicen software libre y obtener los valores de rendimiento de sus recursos locales a través del plugin check_nrpe que crea el agente. Los pasos a seguir se puntualizan en seguida y en el Anexo E ítem E.1.2.3 se explica a detalle:

²⁹ RRD.- Roud Robin Database: es un estándar OpenSource que permite almacenar el rendimiento y graficar los datos en intervalos de tiempo. Se puede integrar fácilmente en los scripts de shell, Perl, Python, Ruby.

³⁰ NRPE.- Sus siglas en inglés Nagios Remote Plugin Executor que viene a ser ejecutor de plugin remoto de Nagios.

1. Xinetd
 - a. Instalar dependencias del paquete xinetd.
2. NRPE daemon
 - a. Descargar NRPE.
 - b. Descomprimir el paquete.
 - c. Compilar e instalar el paquete NRPE.
 - d. Instalar nrpe como un servicio de xinetd.
 - e. Editar el archivo de configuración de xinetd.
 - f. Editar el archivo de configuración de servicios.
 - g. Reiniciar el demonio xinetd.
 - h. Probar el funcionamiento de NRPE localmente y remotamente.

4.2.1.3.5. *Instalación para el envío de correo electrónico.*

Para proceder a la configuración de correo se ha considerado describir rápidamente algunos MTA³¹ que funcionan bajo el ambiente de GNU/Linux:

➤ **Sendmail.-** Es uno de los más populares agentes de transporte de correo (MTA).

Es utilizado en sistemas Unix y Linux. A continuación se puntualizan algunas características principales:

- Utiliza el puerto 25 para las conexiones con los clientes.
- Soporta dominios virtuales.
- Presenta problemas en la seguridad.
- Software libre y de código abierto.

³¹ MTA (Mail Transfer Agent).- En español Agente de Transporte de Correo que actúa como intermediario para comunicarse con otros servidores de correo.

Postfix.- Es un agente de transporte de correo (MTA) de código abierto, creado con la principal funcionalidad de ser rápido, fácil de administrar y seguro que Sendmail. A continuación se puntualizan algunas características principales de postfix:

- Control de correo basura.
- Soporte de bases de datos.
- Soporte para cifrado y autenticación.
- Amplia información disponible.
- Gran rendimiento.

Para la configuración del correo electrónico se ha elegido la opción de postfix por sus características que presenta, donde es necesario seguir los pasos que se muestran a continuación y en el Anexo E ítem E 1.2.4 se explican detalladamente:

1. Crear enlace para el comando mail.
2. Instalar postfix como medio de transporte para el envío de correo.
3. Copiar la configuración original del postfix.
4. Crear la configuración para Gmail.
5. Generar el fichero con la autenticación.
6. Asignar permisos adecuados.
7. Transformar el fichero passwd a un fichero indexado hash.
8. Añadir la autoridad certificadora.
9. Reiniciar postfix.
10. Probar el funcionamiento del envío de correo.

4.2.1.3.6. Instalación para el envío de SMS.

Para la configuración de SMS se realizan los pasos que se muestran a continuación y en el Anexo E ítem E 1.2.5 se lo detalla:

1. Para instalar SMS se utiliza el siguiente paquete:
 - a) Descargar el paquete smstools-3.3.1.15.tar.gz.
 - b) Ingresar y compilar el paquete.
 - c) Ingresar al directorio /etc/sms.conf.
 - d) Iniciar el servicio sms3.
 - e) Probar el funcionamiento del envío de SMS.
 - f) Interconectar al usuario Nagios con SMS Server.
 - g) Configurar el archivo commands.cfg que se encuentra en el directorio:

```
#nano /usr/local/nagios/etc/objects.
```

4.2.1.4. Instalación de agente SNMP en switches.

Como se observa en la Figura 36 se realiza la configuración del agente SNMP en switches Cisco y 3Com para que el software de gestión Nagios a través de plugins pueda obtener información del estado de sus recursos locales.

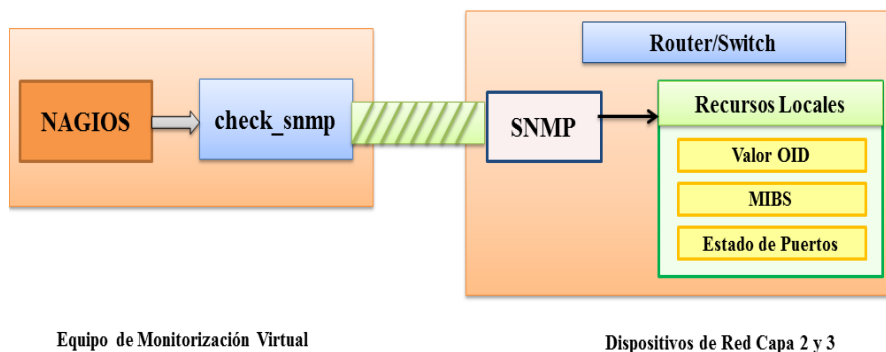


Figura 36. Agentes en Switches

Fuente: Software de gestión Nagios

Para la activación de SNMP se ejecutaron los comandos en modo de configuración global como están detallados en el Anexo E ítem E 1.3.1 para switches Cisco e ítem E.1.3.2 para switches 3Com.

- Configuración de comunidad.
- Destino del envío de notificaciones SNMP.

4.2.1.4.1. Configuración de switches dentro de Nagios.

Para iniciar la configuración de switches de la capa core, distribución y acceso de la red local de datos del GAD-Ibarra en Nagios se procede a realizar la siguiente secuencia de pasos basándose en el formato y sintaxis explicada detalladamente en el Anexo E ítem E.2.1:

1. Se ingresa en Debian a un terminal en modo root.
2. Se crea el nuevo archivo, por ejemplo **sw-cisco-core-4503E.cfg** tanto en el directorio:

```
#nano /usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

como en el archivo de configuración principal:

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

```
cfg_file=/usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

3. Configuración de plantillas para switches.

Nagios permite configurar “plantillas heredadas” es decir plantillas que se enlazan consecutivamente con otras para luego ser llamadas en la definición de dispositivos y

servicios. Se define la plantilla que será utilizada por este dispositivo, dentro del archivo:

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

```
define host{                                [Inicia proceso de definición]
    name                                    [Define nombre asignando a la plantilla]
    notifications_enabled                  [Define notificaciones: 1-Activa, 0-Desactiva]
    event_handler_enabled                  [Define control de eventos del sistema: 1-Activa, 0-Desactiva]
    flap_detection_enabled                 [Define detección de flapeo: 1-Activa, 0-Desactiva]
    process_perf_data                     [Define proceso de rendimiento: 1-Activa, 0-Desactiva]
    retain_status_information              [Conservar la información de estado en los reinicios del programa: 1-Activa, 0-Desactiva]
    retain_nonstatus_information           [Retiene la información sin estado en los reinicios del programa 1-Activa, 0-Desactiva]
    notification_period                    [Define periodo de tiempo que enviará notificaciones]
    register                               [Solo define una plantilla no un verdadero dispositivo]
}
```

Líneas de código 1. Configuración de plantilla a heredar por switches

La plantilla que se muestra a continuación es la que se utilizó para los switches, la cual hereda los valores de la plantilla anterior de la siguiente manera:

```
define host{                                [Inicio de proceso de definición]
    name                                    [Define nombre asignando a la plantilla]
    use                                    [Define nombre de la plantilla a heredar ]
    check_period                           [Define período de chequeo]
    check_interval                         [Define intervalo de tiempo en minutos entre cada chequeo]
    retry_interval                         [Define reintentos de chequeo de estado en intervalos de minutos]
```

max_check_attempts	[Número de veces que chequea el comando, comprueba el estado Up/Down del dispositivo y después notifica]
check_command	[Nombre del comando que comprueba el estado del dispositivo]
notification_perio	[Nombre de la plantilla que especifica el periodo de notificación]
notification_interval	[Define periodo de tiempo entre cada notificación enviada]
notification_options	[Tipo de notificación a enviar d:down, r:recovery, u:unreacheable]
register	[Solo define una plantilla no un verdadero dispositivo]
}	[Finaliza proceso de definición]

Líneas de código 2. Configuración de plantilla a heredar por switches (1)

4. Definición de switches.

Para agregar un switch en Nagios se define los siguientes parámetros ingresando en los archivos creados en el directorio */usr/local/nagios/etc/objects/Switches/* y cambiar los valores solamente en las líneas que están con negrita:

```
#nano /usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

define host{	[Inicia proceso de definición]
use	[Define nombre de la plantilla a utilizar]
host_name	[Define nombre del dispositivo]
alias	[Define nombre descriptivo del dispositivo que aparece en
.	la interfaz web]
address	[Define dirección IP del dispositivo]
hostgroups	[Define en nombre del grupo al que pertenece el dispositivo]
parent	[Define nombre del dispositivo al cual se encuentra conectado]
icon_image	[Define la imagen utilizada como icono en la interfaz web]
statusmap_image	[Define la imagen utiliza en el mapa de red de la interfaz]
}	[Finaliza proceso de definición]

Líneas de código 3. Definición de sintaxis para switches

5. Creación de grupos de switches.

Se define el nombre del grupo de switches al que pertenecerá el nuevo switch que se integre al software de gestión es decir sea este Cisco o 3Com, en el siguiente directorio:

```
#nano /usr/local/nagios/etc/objects/Switches/hostgroup-switches.cfg
```

```
define hostgroup{           [Inicia proceso de definición]
    hostgroup_name        [Define nombre del grupo]
    alias                  [Define nombre descriptivo que aparece en la interfaz
                           . web]
    }                      [Finaliza proceso de definición]
```

Líneas de código 4. Definición de grupos de switches

6. Configuración de plantillas para servicios de switches.

Para proceder a configurar servicios utilizados por switches que serán monitoreados por Nagios se debe definir en primera instancia una plantilla que será utilizada por dichos servicios como se indica a continuación:

```
define service{           [Inicia proceso de definición]
    name                   [Definición de nombre de plantilla para servicios]
    active_checks_enabled [Define chequeo de servicio activos. 1: Activa, 0:
                           Desactiva]
    passive_checks_enable [Define chequeo de servicio pasivos. 1: Activa,
                           0:Desactiva]
    check_freshness        [Por default desactiva los chequeos pasivos de frescura]
    notifications_enabled  [Notificaciones para los servicios. 1: Activa, 0:
                           Desactiva]
    event_handler_enabled  [Controlador de eventos para servicios. 1: Activa, 0:
                           Desactiva]
    flap_detection_enabled [Define la habilitación de flapeo. 1: Activa, 0: Desactiva]
    process_perf_data      [Define procesamiento del rendimiento de los datos. 1:
```

	Activa, 0: Desactiva]
retain_status_information	[Almacena información sobre el estado de los servicios antes de un reinicio. 1: Activa, 0: Desactiva]
is_volatile	[Define este servicio como no volátil]
check_period	[Define el nombre de la plantilla con el período de tiempo para el chequeo]
max_check_attempts	[Define máxima cantidad de chequeos]
normal_check_interval	[Define intervalo de tiempo a programar los chequeos en (min)]
retry_check_interval	[Define intervalo de tiempo para un re-chequeo en (min)]
contacts	[Define nombre de contacto]
notification_options	[Define cuando enviar notificaciones de w: warning, c: critical]
notification_interval	[Define intervalo de envío de notificación]
notification_period	[Define nombre de plantilla con el período para notificaciones]
register	[Solo define una plantilla no un verdadero servicio]
}	[Finaliza proceso de definición]

Líneas de código 5. Definición de sintaxis para plantilla de servicios

7. Configuración de comandos

Previamente a la definición de servicios que se van a monitorear en los switches se debe probar los plugins necesarios que serán configurados en las líneas de comando del directorio que se indica a continuación, para luego ser enlazados en la definición de servicios:

```
#nano /usr/local/nagios/etc/objects/commands.cfg
```

define command{	[Inicia definición]
command_name	[Define nombre de comando]
command_line	[Define sintaxis de ejecución del comando con su respectivo plugin]
}	[Finaliza proceso de definición]

Líneas de código 6. Definición de sintaxis para comandos

➤ **Descripción de Plugins utilizados en Nagios para switches**

En la Tabla 16 se describen los plugins que utiliza Nagios para recibir datos de los recursos locales de cada uno de los switches del GAD-Ibarra los cuales son; el plugin para realizar un ping (se toma solo este servicio debido a que es importante saber que exista conectividad, no se toman otros servicios de aplicaciones porque no corresponde al tema del proyecto), como también se define recursos locales memoria flash, memoria ram, ventiladores, carga del CPU, fuente de alimentación, uso de ancho de banda de las interfaces de los enlaces críticos. Se encuentran ubicados dentro del siguiente directorio, desde donde se prueba el funcionamiento de cada uno:

```
#cd /usr/local/nagios/libexec
```

Tabla 16. Plugins utilizados para switches

Plugin	Descripción
check_ping	Verifica el estado del equipo a través de paquetes ICMP
check_catalyst_mem.pl	Verifica el uso de memoria RAM
check_catalyst_flash.pl	Verifica el uso de memoria Flash
check_catalyst_load.pl	Verifica el uso de CPU
check_catalyst_fans.pl	Verifica el estado de los ventiladores
check-cisco.pl	Verifica el estado de la Fuente de alimentación
check_snmp	Verifica el estado de temperatura
check_iftraffic43.pl	Verifica el tráfico que cursa por interfaces físicas y virtuales

Fuente: Software de gestión Nagios

Además la Figura 37 indica como Nagios a través del plugin check_iftraffic43.pl recibe información de consumo de ancho de banda de cada una de las interfaces del switch y a través de PNP4Nagios permite visualizar una gráfica del rendimiento de las mismas.

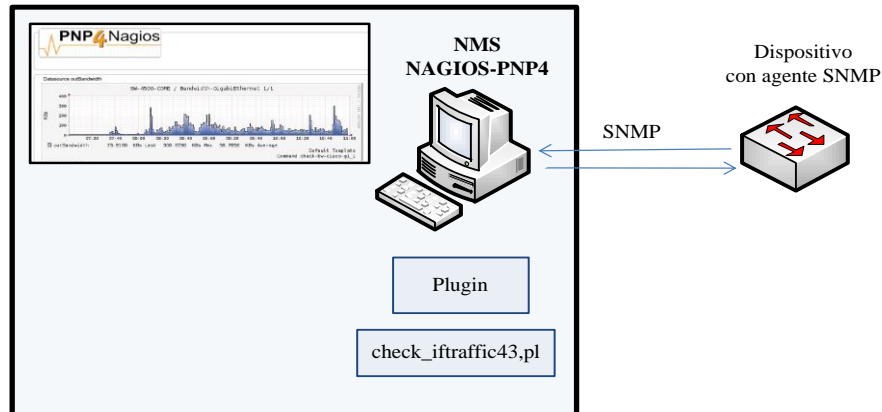


Figura 37. Estructura de PNP4 Nagios

Fuente: Software de gestión Nagios

8. Definición de servicios

Con la información descrita en el paso 7 se continúa con la definición de servicios que verificará el nuevo switch ingresado a Nagios dentro del directorio:

```
#nano /usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

```
define service{                                [Inicia definición]
    use                                         [Define el nombre de plantilla a heredar]
    host_name                                  [Define nombre del dispositivo]
    service_description                        [Define nombre del servicio a verificar]
    check_command                              [Define el comando que realiza la ejecucion del servicio]
}
```

Líneas de código 7. Definición de sintaxis para servicios

9. Configuración de plantilla para contactos

Los switches necesitan enviar notificaciones al administrador de la red cuando sobrepasen su límite de funcionamiento normal y para eso se configura otra plantilla para contactos en el mismo directorio:

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

```

define contact{                                [Inicia proceso de definición]

    name                                       [Nombre asignado a la plantilla de contacto ]
    service_notification_period               [Período de tiempo de notificaciones de servicios]
    host_notification_period                 [Período de tiempo de notificaciones para
                                          dispositivos]
    service_notification_options             [Opciones de notificaciones por servicio]
    host_notification_options               [Opciones de notificaciones por dispositivo]
    service_notification_commands           [Comando de notificaciones a utilizar por servicio]
    host_notification_commands              [Comando de notificaciones a utilizar por
                                          dispositivo]

}                                             [Finaliza proceso de definición]

```

Líneas de código 8. Definición de sintaxis para plantilla de contactos

10. Definición de contacto

La plantilla creada en el paso 9 será enlazada dentro del archivo de configuración del directorio `#nano /usr/local/nagios/etc/objects/contacts.cfg`, donde se define el número de teléfono celular y cuenta de correo electrónico del administrador a quien se le envía las notificaciones:

```

define contact{                                [Inicia proceso de definición]

    contact_name                             [Define nombre de contacto]
    use                                       [Define nombre de plantilla de contacto a utilizar]
    alias                                    [Define nombre descriptivo]
    pager                                    [Define el número de teléfono móvildel contacto]
    email                                    [Define la cuenta de correo electrónico del contacto]

}

```

Líneas de código 9. Definición de sintaxis para contactos

4.2.1.5. Instalación de agente SNMP en enlaces inalámbricos.

Para la instalación de agente SNMP en enlaces inalámbricos Mikrotik se encuentra una detallada explicación en el Anexo E ítem E.1.3.3, al igual que la configuración de los archivos dentro de Nagios está descrita en el Anexo E ítem E.2.2:

1. Crear el nuevo archivo .cfg en los directorios::

```
#nano /usr/local/nagios/etc/objects/Enlaces-Inalambricos/mikrotik.cfg
```

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

```
cfg_file=/usr/local/nagios/etc/objects/Enlaces-Inalambricos/mikrotik.cfg
```

2. Configuración de plantillas para enlaces inalámbricos.
3. Definición de enlaces inalámbricos.
4. Creación de grupos de enlaces inalámbricos.
5. Configuración de plantillas para servicios.
6. Configuración de comandos.
7. Definición de servicios.

➤ **Descripción de Plugins utilizados en Nagios para enlaces inalámbricos**

En esta parte solamente se describe la funcionalidad de los plugins utilizados por Nagios para la configuración de servicios a ser monitoreados como se puede observar en la Tabla 17.

Además cabe recalcar que estos plugins se utilizan para los nuevos enlaces que ingresen al software de gestión y se encuentran en el directorio:

```
#cd /usr/local/nagios/libexec
```

Tabla 17. Plugins utilizados para enlaces inalámbricos

Plugin	Descripción
check_ping	Verifica el estado del equipo a través de paquetes ICMP
check_snmp	Verifica el uso de memoria principal y disco
check_mikrotik_users	Verifica cuántos enlaces están conectados
check_mikrotik_signal	Verifica el nivel de señal en dBm

Fuente: Software de gestión Nagios

4.2.1.6. Instalación de agente NRPE en servidores Linux.

Para la monitorización de servidores Linux, Nagios utiliza el plugin `check_nrpe`, que interactúa con el demonio NRPE que es un agente SNMP que está instalado en los servidores remotos Linux, este permite ejecutar plugins de Nagios y devuelve información a quien se lo solicite. Este agente es útil para controlar los recursos locales como el uso de disco, carga de cpu, consumo de memoria.

4.2.1.6.1. Funcionamiento General.

El funcionamiento de este agente se basa en que un equipo de monitorización (gestor) ejecuta `check_nrpe` y este a su vez hace una petición NRPE al equipo remoto, este último ejecuta un determinado algoritmo que tiene guardado y devuelve el resultado al servidor como se muestra en la Figura 38.

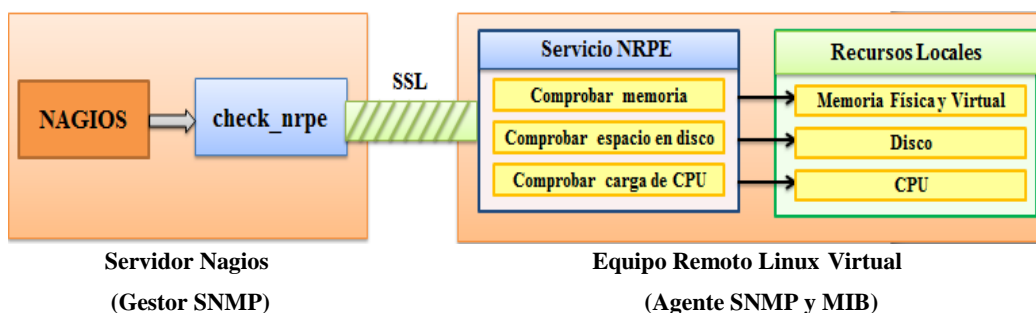


Figura 38. Diseño de Monitoreo de Servidores Linux

Fuente: Software de gestión Nagios

4.2.1.6.2. *Instalación de NRPE.*

Para la configuración de NRPE es necesario considerar los siguientes puntos que se indican a continuación y el procedimiento detallado de cada uno de estos pasos se muestra en el Anexo E ítem E 1.3.4.

1. Crear una cuenta de usuario para Nagios
2. Plugins de Nagios
 - a. Descargar los Plugins de Nagios
 - b. Descomprimir el paquete de Plugins
 - c. Compilar los Plugins
 - d. Instalar los Plugins
3. Xinetd
 - a. Instalar dependencias del paquete xinetd
4. NRPE daemon
 - a. Descargar NRPE
 - b. Descomprimir el paquete
 - c. Compilar e instalar el paquete nrpe
 - d. Instalar nrpe como un servicio de xinetd
 - e. Editar el archivo de configuración de xinetd
 - f. Editar el archivo de configuración de servicios
 - g. Reiniciar el demonio xinetd
 - h. Probar el funcionamiento de nrpe localmente y remotamente.

4.2.1.6.3. Configuración de servidores Linux dentro de Nagios

La configuración es igual para servidores con sistema operativo Linux tanto en servidores físicos como virtuales y en el Anexo E ítem E.2.3 se detalla los pasos indicados a continuación:

1. Crear el nuevo archivo .cfg en los directorios::

```
#nano
```

```
/usr/local/nagios/etc/objects/Servidores_Virtuales/serv01_debbservicios.cfg
```

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

```
cfg_file=/usr/local/nagios/etc/objects/Servidores_Virtuales/serv01_debbservicio  
s.cfg
```

2. Configuración de plantillas para servidores linux
3. Definición de servidores linux
4. Creación de grupos de servidores linux
5. Configuración de plantillas para servicios.
6. Configuración de comandos.
7. Definición de servicios.

➤ **Descripción de Plugins utilizados en Nagios para servidores Linux**

En esta parte solamente se describe la funcionalidad de los plugins utilizados por Nagios para la configuración de servidores Linux físicos o virtuales a ser monitoreados. En la Tabla 18 se puede observar los plugins definidos para los servidores con software de licencia libre que fueron ingresados al software de gestión y se encuentran en el directorio:

```
#cd /usr/local/nagios/libexec
```

Tabla 18. Plugins utilizados para servidores Linux

Plugin	Descripción
check_ping	Verifica el estado del equipo a través de paquetes ICMP
check_nrpe	Recopila información en el agente nrpe
check_mem	Verifica el uso de memoria RAM
check_swap	Verifica el uso de memoria Swap
check_load	Verifica el uso de CPU
check_disk	Verifica el espacio de disco

Fuente: Software de gestión Nagios

4.2.1.7. Instalación de agente NSClient++ en servidores Windows.

Para que Nagios pueda obtener datos de los recursos locales de servidores físicos y virtuales con sistema operativo Windows Server 2003, 2008 es necesario instalar en cada uno un agente llamado **NSClient++** como se observa en la Figura 39, el cual se comunica a través del puerto 1248 con el plugin **check_nt** ubicado en el directorio **/usr/local/nagios/libexec** de Nagios. Este agente se utiliza también para los equipos de la entidad que manejen el sistema operativo Windows XP, 7, 8. La configuración del agente se encuentra detallada en el Anexo E ítem E 1.3.5.

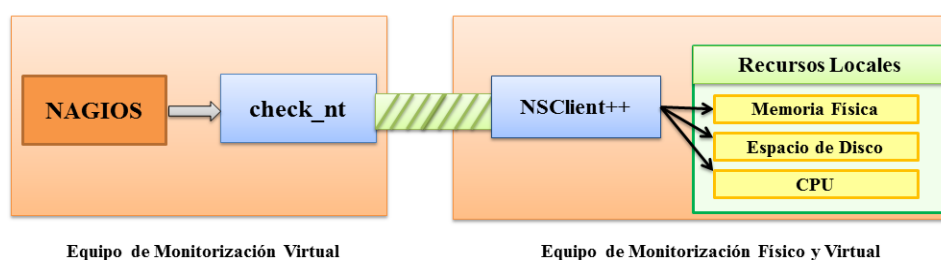


Figura 39. Comunicación entre Nagios y agente NSClient

Fuente: Basada en agente NSClient

4.2.1.7.1. Configuración de servidores Windows dentro de Nagios

La configuración es igual para servidores y host con sistema operativo Windows y en el Anexo E ítem E 2.4 se indica la configuración detallada:

1. Crear el nuevo archivo .cfg en los directorios::

```
#nano /usr/local/nagios/etc/objects/Servidores_Fisicos/serv07_Olympo.cfg
#nano /usr/local/nagios/etc/nagios.cfg
cfg_file=/usr/local/nagios/etc/objects/Servidores_Fisicos/serv07_Olympo.cfg
```

2. Configuración de plantillas para servidores Windows.
3. Definición de servidores Windows.
4. Creación de grupos de servidores Windows.
5. Configuración de plantillas para servicios.
6. Configuración de comandos.
7. Definición de servicios.

➤ **Descripción de Plugins utilizados en Nagios para switches**

En la Tabla 19 se describe los plugins que son utilizados por todos los servidores con sistema operativo Windows del GAD-Ibarra, de igual forma para los nuevos dispositivos que ingresen a Nagios y se encuentran ubicados dentro del directorio:

```
# cd /usr/local/nagios/libexec
```

Tabla 19. Plugins utilizados para servidores Windows

Plugin	Descripción
check_ping	Verifica el estado del equipo a través de paquetes ICMP
check_nt!CPULOAD	Verifica el uso de CPU
check_nt!MEMUSE	Verifica el uso de memoria RAM
check_nt!USEDISKSPACE	Verifica el espacio de disco

Fuente: Software de gestión Nagios

4.2.2. Implementación dentro de la Gestión de Fallos.

La implementación de la gestión de fallos comprende en realizar el proceso de localizar, diagnosticar y corregir problemas antes de que sucedan y una vez que han

sucedido en los componentes hardware de los dispositivos de red gestionados. Esta gestión está interrelacionada con las otras gestiones del modelo. El objetivo principal de la gestión de fallos, es encontrar la mejor solución frente a cualquier incidente que ocurra, en el menor tiempo posible.

Los fallos son detectados de acuerdo a alertas que genera el software de gestión, Nagios, estas pueden ser visuales, mediante correos electrónicos o SMS que el administrador de la red genera para el seguimiento de un problema dentro de los dispositivos gestionados. Dentro de esta gestión de fallos se presentan dos situaciones a considerar:

- Evitar el fallo antes de que suceda se encarga la gestión proactiva y la gestión de pruebas preventivas.
- Si el fallo ha sucedido se encarga la gestión reactiva.

4.2.2.1. Gestión Proactiva.

Esta gestión determina un fallo antes de que este suceda, es decir determinando umbrales en el software Nagios para que el administrador pueda visualizar los fallos y de acuerdo a los colores que presenta pueda tomar medidas de solución.

4.2.2.1.1. Definición de umbrales.

Los umbrales que se establecen a continuación en la Tabla 20 se encuentran en función de las características propias del dispositivo gestionado, por tal razón se establece un margen o porcentaje referencial.

Tabla 20. Umbrales para el Monitoreo

Dispositivos Gestionados	Métrica	Umbrales de Advertencia (WARNING)	Umbrales de Criticidad (CRITICAL)
Switches	Carga de CPU	70 %	80 %
	Memoria (RAM y Flash)	30 %	20 %
	Consumo de ancho de banda de interfaces	40 %	50 %
Servidores	Carga de CPU	60 %	75 %
	Memoria (RAM y Swap)	30 %	20 %
	Disco	25 %	15 %
Margen de funcionamiento recomendable		< 60%	

Fuente: Basada en umbrales de monitoreo

Se establece los umbrales de advertencia para que el administrador pueda dar una solución rápida antes que el dispositivo gestionado llegue a un estado crítico y de esta forma optimizar sus recursos.

Debido a que no existe un estándar que defina estos parámetros, se considera el criterio de (Microsoft, 2005) el cual afirma:

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 continuada, el rendimiento del procesador se considera un cuello de botella.

Tomando en cuenta la recomendación anterior se ha determinado que la carga del procesador de los servidores no debe sobrepasar el 75 por ciento dentro de su funcionalidad normal de rendimiento caso contrario se debe tomar las respectivas acciones correctivas.

Para el caso de la memoria si esta se encuentra utilizada en su totalidad, no aceptará aplicaciones que consuman memoria y además se demorará más tiempo en ejecutar las que ya estén solicitadas por esta razón el umbral de memoria no debe sobrepasar del 70 por ciento de ser utilizada (Microsoft, 2011).

Barrios (2014) afirma:

El espacio de memoria de intercambio o Swap, se conoce como memoria virtual, esta utiliza espacio en el disco duro en lugar de un módulo de memoria. Cuando la memoria real se agota, el sistema copia parte del contenido de esta directamente en este espacio de memoria virtual para poder realizar otras tareas. (p. 124)

Debido a un alto consumo de memoria swap implica el consumo de espacio en el disco duro afectando de esta forma también a este recurso. En general es más lento, pero siempre es necesario tener una memoria de intercambio porque si al servidor se le agota la memoria (RAM, o intercambio), puede caerse.

Para el caso del disco se recomienda tener un umbral del 25 por ciento libre (Microsoft, 2011).

Para la definición de umbrales en switches se ha considerado la experiencia del administrador de la red del GAD-Ibarra con respecto a porcentaje de utilización de consumo de CPU que no ha llegado a sobrepasar el 25%, y por lo tanto si este valor llegaría a un 70% se considera una advertencia y un 80% se considera como crítico, donde el administrador debe revisar los procesos que están consumiendo el rendimiento de la CPU, al igual que la memoria RAM, Flash deben mantener un porcentaje libre de

30% para un estado de advertencia y un porcentaje de 20% para un estado crítico y además el consumo de ancho de banda de interfaces no deben sobrepasar de un 40% de estado de advertencia y de un 50% de un estado crítico para evitar que exista una saturación en los enlaces.

4.2.2.2. Gestión de pruebas preventivas.

Esta gestión se encarga de evitar el fallo antes de que suceda a través de pruebas que se explican a continuación:

4.2.2.2.1. Pruebas de conectividad física.

Pruebas que se realizan para verificar que los medios de transmisión se encuentran en funcionamiento, es decir; tarjetas de red, cables de red, cables de fuentes de poder, ups, reguladores de voltaje.

4.2.2.2.2. Pruebas de conectividad lógica.

Este tipo de pruebas se realizan desde Nagios ingresando mediante el programa PuTTY a través del puerto 22 correspondiente a SSH para comprobar conectividad punto a punto mediante el comando “ping” y mediante “traceroute” comprobar conectividad salto por salto hacia los servidores y a través del puerto 23 correspondiente a Telnet para comprobar conectividad punto a punto hacia los switches mediante el comando “ping” y mediante “traceroute” comprobar conectividad salto por salto

Ademas se puede comprobar el establecimiento de comunicación SNMP entre gestor y agentes mediante el comando snmpwalk que sirve para recorrer un arbol MIB

del agente y poder obtener determinada información de la MIB a través del nombre de la rama o mediante número OID.

4.2.2.3. *Gestión Reactiva.*

Este tipo de gestión se ejecuta cuando el fallo ha sucedido y se realiza el proceso de detectar, aislar, diagnosticar, corregir y documentar como se observa en la secuencia de la Figura 40:

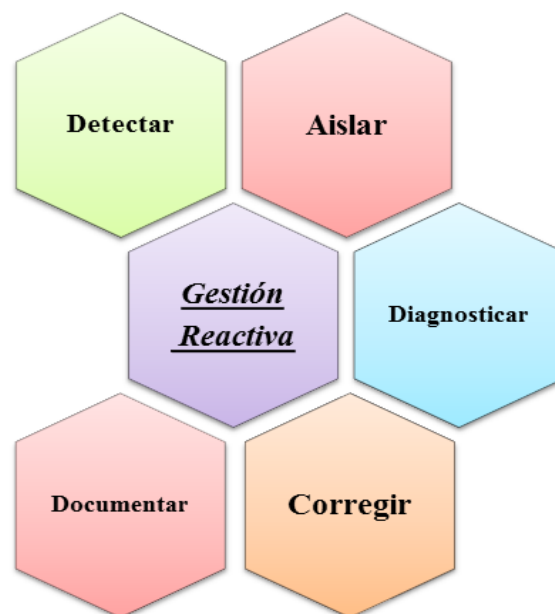


Figura 40. Proceso de Gestión Reactiva

Fuente: Basada en la Gestión Reactiva

4.2.2.3.1. *Detectar.*

Nagios permite detectar en la primera señal que emita el fallo mediante la visualización de cambio de colores en el mapa de la interfaz web de acuerdo a los (parents) es decir que dispositivo es el que está afectado, un switch de la capa de acceso que esta conectado al switch core o un servidor que esta conectado en un switch de la

capa de distribución. En la Figura 41 se observa como Nagios permite al administrador que detecte facilmente un fallo.

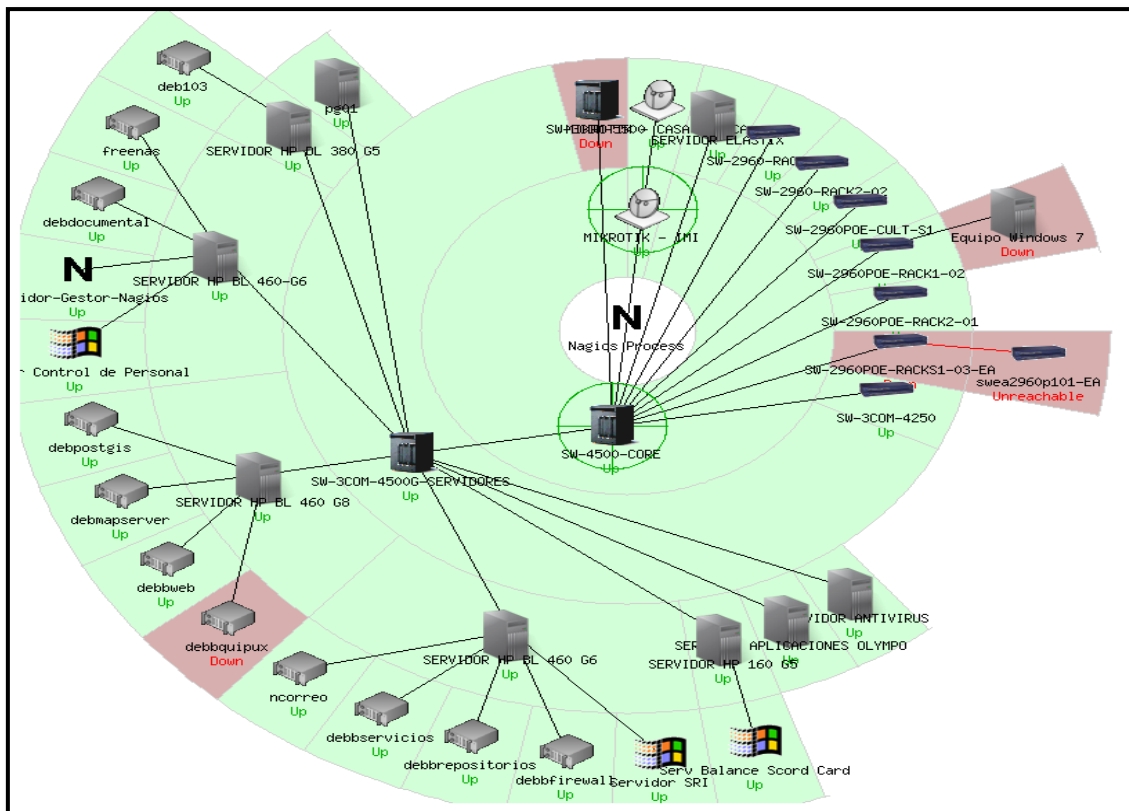


Figura 41. Detección de fallos en el mapa de la interfaz web

Fuente: Extraída del gestor Nagios

➤ *Envío de notificaciones vía correo electrónico y SMS*

Ademas el administrador de la red puede detectar un fallo cuando Nagios realiza la notificación de la existencia de una falla y del lugar donde se ha generado a través de un mensaje de texto o un correo electrónico de las siguientes instancias:

- Cuando ocurre un cambio de estado en el equipo de red gestionados o en los servicios.
- Cuando un host o servicio permanece en un estado diferente de OK y el tiempo especificado en la opción *notification_interval* en la definición de host o servicio ha pasado desde la última notificación que fue enviada.

- Cuando Nagios envía una notificación este notificará solamente al contacto que ha sido configurado.

En las Figuras 42 y 43 se indica una notificación enviada desde Nagios a la cuenta de correo electrónico Gmail donde informa que existe un problema, el servicio número 17 donde se encuentra configurada la interfaz GigabitEthernet 1/20 Enlace de Fibra Óptica que se conecta con el Edificio Antiguo del Switch_CORE con la dirección IP 172.x.x.x presenta un estado crítico porque la interfaz esta down (abajo).

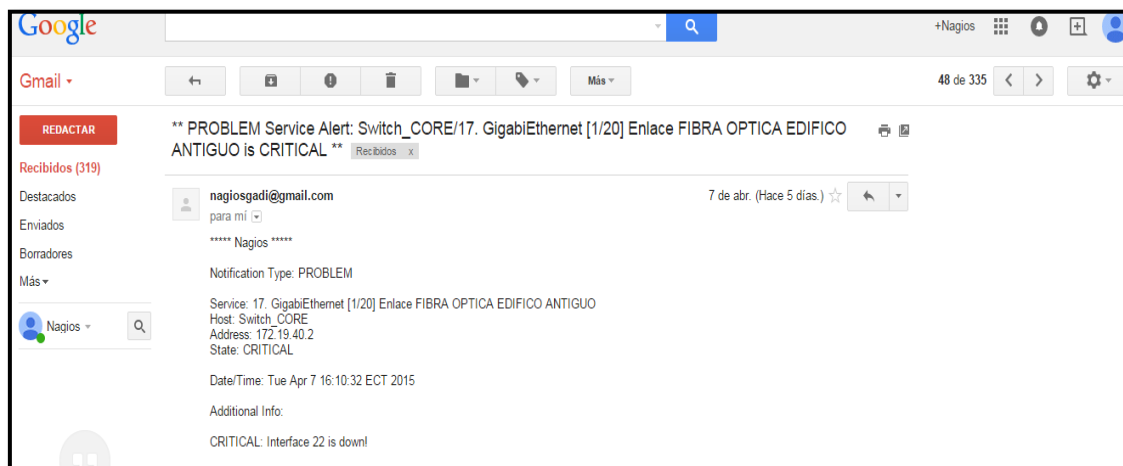


Figura 42. Envío de correo electrónico desde Nagios

Fuente: Extraída de cuenta de correo Gmail, creada específicamente para la entidad

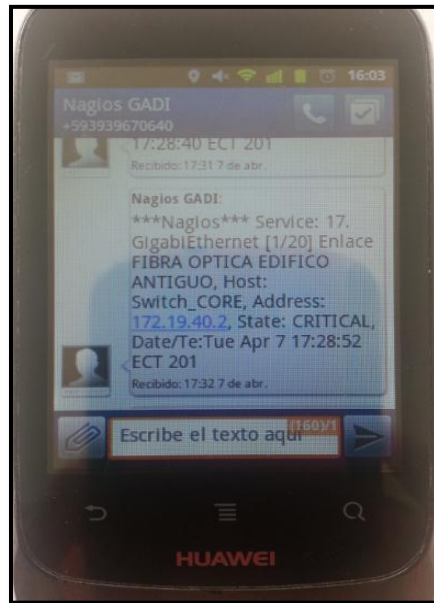


Figura 43. Envío de mensaje de texto desde Nagios

Fuente: Extraída desde teléfono móvil del administrador de la red

En las Figuras 44 y 45 se indica otra notificación enviada desde Nagios a la cuenta de correo electrónico Gmail donde informa que existe un problema, el servicio número 03 donde se encuentra configurado la verificación de Espacio de la unidad de Disco C:\ del servidor 07 con la dirección IP 172.x.x.x presenta un estado crítico porque el porcentaje de espacio libre esta en 9% del total.

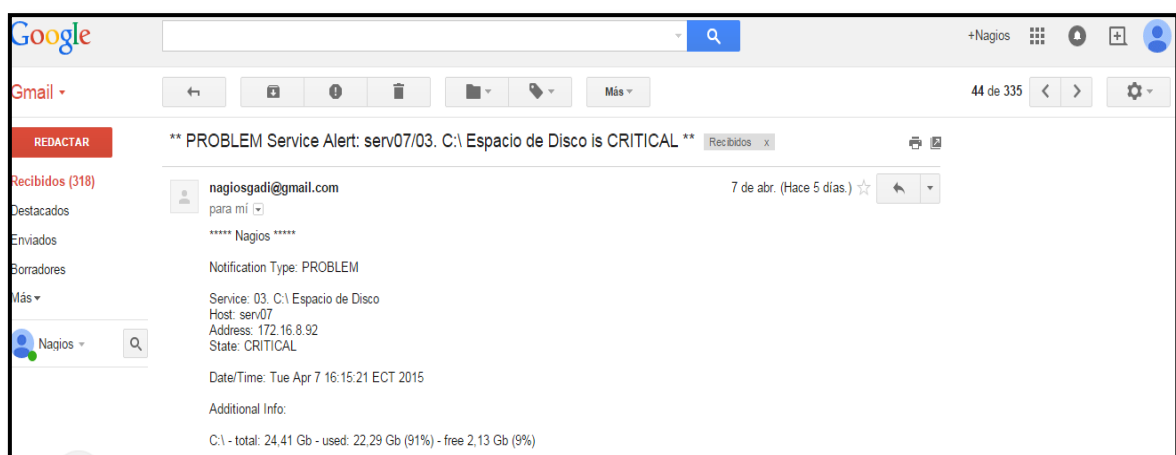


Figura 44. Envío de correo electrónico desde Nagios

Fuente: Extraída de cuenta de correo Gmail, creada específicamente para la entidad



Figura 45. Envío de correo electrónico desde Nagios

Fuente: Extraída desde teléfono móvil del administrador de la red

4.2.2.3.2. *Aislar.*

Nagios permite aislar un fallo mediante la jerarquía de dispositivos de red denominados parents (padres) donde se puede aislar fácilmente que dispositivo de red gestionado está afectado y no por falta de ese equipo se vea afectada toda la red, además permite aislar un fallo mediante una jerarquía de alertas de acuerdo a los estados de funcionamiento que genere cada dispositivo como se muestra a continuación:






➤ *Jerarquía de alertas*

Dentro de la implementación del proyecto se menciona que se determinará una jerarquía de alertas dependiendo de la importancia de los departamentos que conforman el GAD-Ibarra, a través del estándar RMON extensión de SNMP, pero no se realizó por las razones que se presentan a continuación:

Después de haber mantenido diálogos con el administrador de la red se ha concluido que no se determinará la jerarquía de alertas de acuerdo a la importancia de los departamentos porque no son equipos que presenten mayores dificultades dentro de la entidad. Sino solamente en los equipos de mayor prioridad para la entidad como se determinó en la situación actual.

Además dentro de la implementación no se utilizó el estándar RMON extensión de SNMP porque el software de gestión Nagios facilita establecer una jerarquía de alertas configuradas previamente por el administrador a través de umbrales. En la Tabla 21 se indica como se puede aislar un fallo dependiendo del color que generan los dispositivos gestionados de acuerdo a la jerarquía de alertas, mediante cinco tipos de estados, tratando así de que otros equipos no se vean afectados a causa del mismo problema y poder encontrar la mejor solución asegurando que el resto de los elementos de la red pueden seguir funcionando.

Tabla 21. Jerarquía de alertas que genera Nagios

Estado	Representaciones	Descripción
Recovery/Recuperado		Cuando un host está en UP y/o un servicio está en OK en la última comprobación del estado.
Warning/Advertencia		Cuando se ha detectado problemas en la última comprobación en un host o servicio, antes de volverse crítico.
Down/Abajo		Cuando en la última comprobación de estado ha ocurrido un fallo, un host está en Down / Abajo o Unreachable/Inalcanzable. Cuando un servicio esta en estado Critical/Crítico porque presentan problemas que sobrepasan de los umbrales normales de funcionamiento.
Unreachable/Inalcanzable		
Critical/Crítico		
Unknow/Desconocido		Cuando un servicio no esta bien definido presenta este estado Desconocido.
Pending/Pendiente		Cuando esta reconociendo una nueva configuración.

Fuente: Datos obtenidos del software de gestión Nagios

Cuando la estación de gestión genera una alerta esta debe ser detectada aproximadamente en el mismo instante de haber sido emitida, para que el administrador de la red pueda actuar de forma inmediata.

4.2.2.3.3. *Diagnosticar.*

Este elemento de la gestión de fallos es fundamental una vez que se ha detectado y aislado el origen del fallo sea en equipos o servicios que se vieron afectados. Se procede a establecer un diagnóstico mediante Nagios de las posibles causas que han provocado un fallo:

- El dispositivo gestionado perdió conectividad lógica, no existe tiempos de respuesta en ambos sentidos de la comunicación.
- El dispositivo gestionado perdió conectividad física, cables de red rotos, tarjetas de red dañadas.
- Nagios permite diagnosticar un fallo a través de chequeos que ha realizado.
- Los dispositivos gestionados no responden a peticiones de SNMP.
- Los dispositivos gestionados no establecen conexión de gestión vía telnet de manera local y remota.
- Después de haber aislado mediante parents (padres) Nagios permite diagnosticar los nodos, por ejemplo el parent de un pc conectado a un switch sería el switch y además evita que Nagios envíe alertas si un parent ya no responde.
- Tan solo con dar click en el dispositivo que se ha detectado y aislado Nagios diagnostica un fallo crítico cuando existe un elevado consumo de niveles de umbrales normales de funcionamiento.

- Fallos que se relacionan con el tráfico de la red y con la falta de disponibilidad de los servicios.

4.2.2.3.4. *Corregir.*

Siguiendo el proceso de la gestión reactiva en esta parte se tiene que tomar las acciones suficientes para reparar el daño. Entre los mecanismos más recurrentes y más utilizados se encuentran los siguientes:

- Reemplazo de recursos dañados, hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente. En la infraestructura de la red local de datos del GAD-Ibarra los equipos más susceptibles a fallos y con más criticidad en la red se encuentran los switch Cisco Catalyst de la serie 2960 los cuales forman parte de la capa de acceso.
- Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento. En este punto, el diseño de la red de la entidad cuenta con la existencia un enlace redundante activo para el chasis de servidores, garantizando de esta manera el funcionamiento normal de los servicios utilizados por los diferentes equipos de la capa de distribución y la capa core.
- Los dispositivos de red recuperan conectividad y se estabilizan si son reiniciados.
- Instalación de software, sea una nueva versión de sistema operativo, una actualización o un parche que solucione un fallo específico.
- Verificación de configuración también es algo muy usual cambiar algún parámetro en la configuración del dispositivo de la red.

- Los dispositivos deben soportar gestión a través de un puerto de consola y vía telnet de manera local y remota.

4.2.2.3.5. Documentar.

La documentación será registrada en una base de datos para su respectivo manejo y seguimiento como se indica en el Anexo F con el procedimiento realizado para solucionar los fallos más relevantes que se susciten nuevamente en un futuro. Además cabe recalcar que esta área de gestión es de competencia solamente de la entidad.

4.2.3. Implementación dentro de la Gestión de Contabilidad.

Dentro de la gestión de contabilidad se considera los siguientes parámetros elegidos de acuerdo a las necesidades de la red local de datos del GAD-Ibarra:

4.2.3.1. Parámetros de monitoreo.

La principal funcionalidad de esta área de gestión es registrar la utilización de los recursos de la red, en la Tabla 22 se muestra los dispositivos de red gestionados por Nagios, como son; switches Cisco, 3Com, enlaces inalámbricos, servidores físicos y virtuales, host. Cabe recalcar que por restricciones de fabricantes algunos equipos no permiten monitorear todos los parámetros necesarios es decir no se puede obtener los valores de OID.

Tabla 22. Parámetros de Monitoreo

Dispositivos de red	Parámetros de Monitoreo	Funcionalidad	Alertas
Switches Cisco	Estado	Si el dispositivo esta encendido y/o apagado	Envian vía SMS Envian vía correo electrónico
	Procesador	Uso de CPU	
	Memoria RAM	Cantidad de memoria RAM utilizada	
	Memoria Flash	Cantidad de memoria Flash utilizada	
	Interfaces de red críticas	Ancho de banda que cursa por cada interfaz	
	Fuente de alimentación	Verificar funcionamiento	
	Ventiladores	Verificar funcionamiento	
	Temperatura	Verificar sensor de temperatura	
Swithes 3Com	Estado	Si el dispositivo esta encendido y/o apagado	Envian vía SMS Envian vía correo electrónico
	Interfaces de red críticas	Ancho de banda que cursa por cada interfaz	
	Fuente de alimentación	Verificar funcionamiento	
	Ventiladores	Verificar funcionamiento	
Enlaces Inalámbricos Mikrotik	Estado	Si el dispositivo esta encendido y/o apagado	Envian via correo electrónico
	Nivel de señal	Verifica el nivel de señal en dBm	
	Dispositivos conectados	Número de dispositivos conectados al enlace	
	Memoria principal	Verifica estado de memoria	
	Disco	Verifica estado de disco	
Servidores Fisicos y Virtuales	Estado	Si el dispositivo esta encendido y/o apagado	Envian vía correo electrónico
	Procesador	Uso de CPU	
	Memoria Física	Cantidad de memoria RAM utilizada	
	Memoria Virtual	Cantidad de memoria Swap utilizada	
	Espacio de disco duro	Capacidad utilizada de disco duro	
Host	Estado	Si el dispositivo esta encendido y/o apagado	
	Procesador	Uso de CPU	
	Memoria RAM	Cantidad de memoria RAM utilizada	
	Espacio de disco duro	Capacidad utilizada de disco duro	

Fuente: Basada en inventarios de TIC del GAD-Ibarra

4.2.3.2. Parámetros de estado.

Nagios permite definir ciertos parámetros de alertas de acuerdo a las necesidades de la red mediante la opción “*notification_options*”, en la Tabla 23 se indica la

descripción para el estado de dispositivos gestionados y en la Tabla 24 se indica la descripción para el estado de los servicios.

Tabla 23. Parámetros de estado para dispositivos

Letra	Significado	Descripción
d	Down	Cuando el dispositivo esta abajo
u	Unreachable	Cuando el dispositivo no es visible o es inalcanzable
r	Recovery	Cuando el dispositivo se recuperó presenta un estado (OK)
f	Flapping	Cuando el dispositivo se inicia o detiene, o el estado es indeterminado
n	None	No enviar notificaciones

Fuente: Software de gestión Nagios

Tabla 24. Parámetros de estado para servicios

Letra	Significado	Descripción
w	Warning	Cuando el servicio indica esta sobre el umbral de Advertencia
c	Critical	Cuando el servicio sobrepasa umbrales normales de funcionamiento
r	Recovery	Cuando el servicio se recuperó presenta un estado (OK)
f	Flapping	Cuando el servicio se inicia o detiene, o el estado es indeterminado
n	None	No enviar notificaciones

Fuente: Software de gestión Nagios

4.2.3.1. Parámetros de chequeo.

Nagios permite realizar periódicamente chequeos de cada servicio y dispositivo gestionado como se muestra en la Tabla 25, determina si se ha generado algún cambio de estado. El intervalo de generación de chequeos se encuentra en el archivo **templates.cfg** ubicado en el directorio `#cd /usr/local/nagios/etc/objects/`.

Tabla 25. Parámetros de chequeo

Opción	Valor	Descripción
max_check_attempts	3	Número máximo de chequeos, comprueba hasta 10 veces el estado del servicio o dispositivo
normal_check_interval	1	Intervalo de chequeo normal, comprueba el dispositivo o servicio cada 10 minutos en condiciones normales
check_interval	1	Intervalo de chequeo en minutos de dispositivo o servicio
retry_interval	1	Intervalo de re-chequeo, reintentos de verificación de dispositivo o servicio en intervalos de 1 minuto
notification_interval	5	Intervalo de notificaciones enviadas cada 5 min
check_period	24x7	Período de chequeo las 24 horas del día, los 7 días de la semana

Fuente: Software de gestión Nagios

Otra de las opciones que presenta el software de gestión es la programación de periodos de tiempo que controlan los chequeos y notificaciones de los dispositivos y servicios, es posible configurar que un dispositivo este monitoreándose las 24 horas del día los 7 días de la semana como se observa en la Tabla 26 o solamente en horas de trabajo como se observa en la Tabla 27:

Tabla 26. Parámetros de tiempo 24x7

Opción	Horario	Descripción
timeperiod_name	24x7	Nombre del período de tiempo
alias	24 Horas del Día, 7 Días de la Semana	Nombre descriptivo del período de tiempo definido
sunday	00:00-24:00	Horario definido para el día Domingo
monday	00:00-24:00	Horario definido para el día Lunes
tuesday	00:00-24:00	Horario definido para el día Martes
wednesday	00:00-24:00	Horario definido para el día Miércoles
thursday	00:00-24:00	Horario definido para el día Jueves
friday	00:00-24:00	Horario definido para el día Viernes
saturday	00:00-24:00	Horario definido para el día Sábado

Fuente: Software de gestión Nagios

Tabla 27. Parámetros de tiempo por horas de trabajo

Opción	Horario	Descripción
timeperiod_name	workhours	Nombre del período de tiempo
alias	Horario Normal de Trabajo	Nombre descriptivo del período de tiempo definido
monday	07:00-18:00	Horario definido para el día Lunes
tuesday	07:00-18:00	Horario definido para el día Martes
wednesday	07:00-18:00	Horario definido para el día Miércoles
thursday	07:00-18:00	Horario definido para el día Jueves
friday	07:00-18:00	Horario definido para el día Viernes

Fuente: Software de gestión Nagios

4.2.4. Implementación dentro de la Gestión de Prestaciones.

La red del GAD-Ibarra crece constantemente para brindar mayor conectividad, en los últimos años se han agregado nuevos enlaces y equipos, hasta el punto en que es muy difícil para los administradores conocer el estado de los mismos. Por consiguiente esta área de gestión consiste en mantener monitoreado constantemente el estado de los dispositivos gestionados y salvaguardar su rendimiento para determinar su comportamiento sea este en un en un intervalo de tiempo o en tiempo real.

4.2.4.1. Análisis del rendimiento general de la red.

Este análisis se realizó con la finalidad de demostrar que el rendimiento de la red del GAD-Ibarra no afecta al implementar el modelo de gestión para lograr este objetivo se ha configurado un puerto espejo en la interfaz Gigabit Ethernet 1/4 del switch core 4503-E en donde se duplicará todo el tráfico que circula por la red de la entidad y será enviado al host donde se encuentra instalado Ntop y Wireshark, esta recopilación de información se la ha realizado durante seis días consecutivos y se muestra a detalle en el Anexo G.

4.2.4.1.1. Distribución de protocolos sin configuración de SNMP.

Los resultados que se observan en la Figura 46 son capturados por Ntop antes de la configuración de SNMP en la red, y señalan que el 96.4% del total de datos corresponden al protocolo de internet IP, donde el 83.3% corresponde al protocolo TCP, el 19.8% corresponde al protocolo UDP y el 0.1% se distribuye en los protocolos ICMP, ICMPv6, IGMP y otros no identificados por el software, el 0.2% ocupa el protocolo ARP y el 3,1% ocupa el protocolo IPv6.

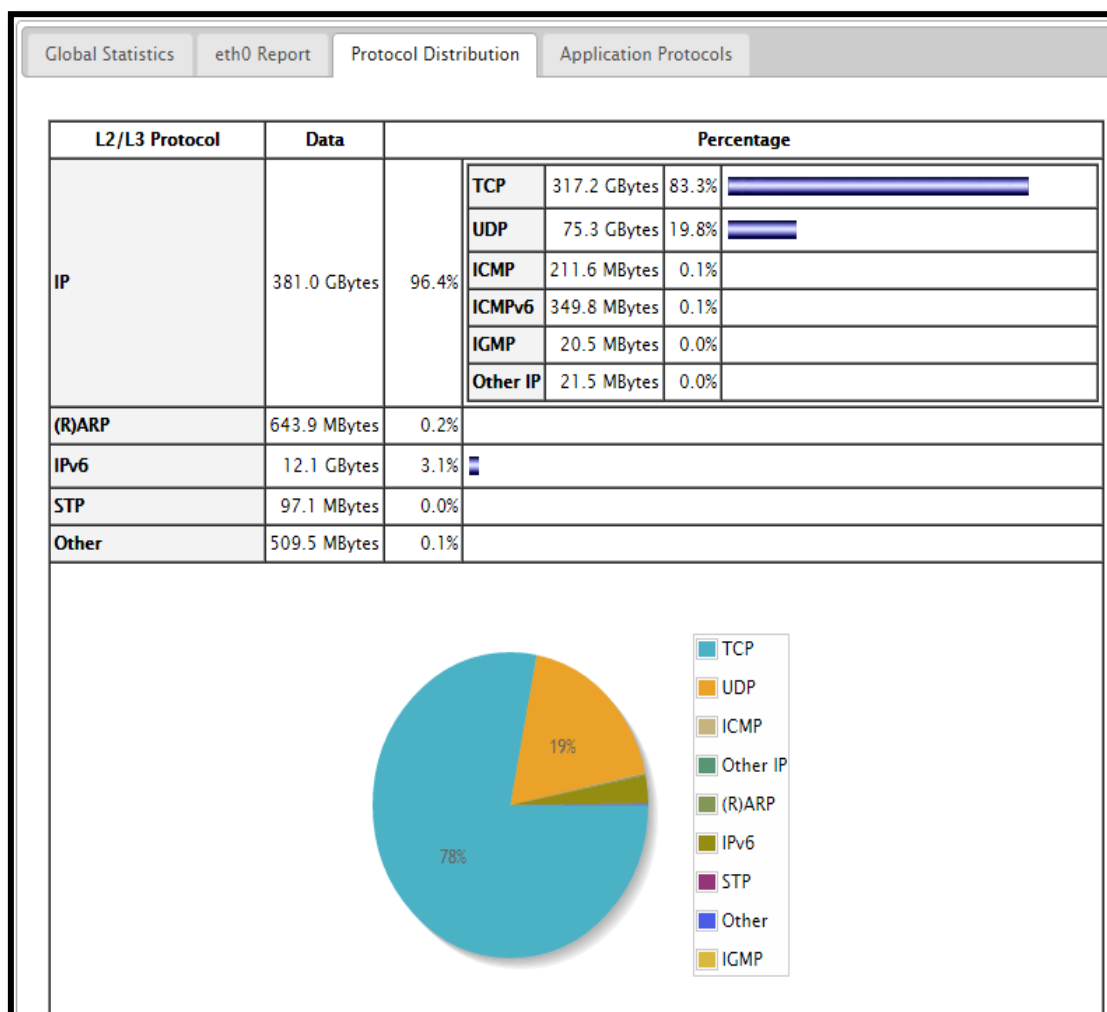


Figura 46. Datos obtenidos sin configuración de SNMP

Fuente: Captura propia extraída de software Ntop

4.2.4.1.2. Distribución de protocolos con configuración de SNMP.

Los resultados que se observan en la Figura 47 son capturados por Ntop después de la configuración de SNMP en la red y señalan que el 97.0% del total de datos corresponden al protocolo de internet IP, donde el 87.5% corresponde al protocolo TCP, el 15.0% corresponde al protocolo UDP y el 0.1% se distribuye en los protocolos ICMP, ICMPv6, IGMP y otros no identificados por el software, el 0.2% ocupa el protocolo ARP y el 2.5% ocupa el protocolo IPv6.

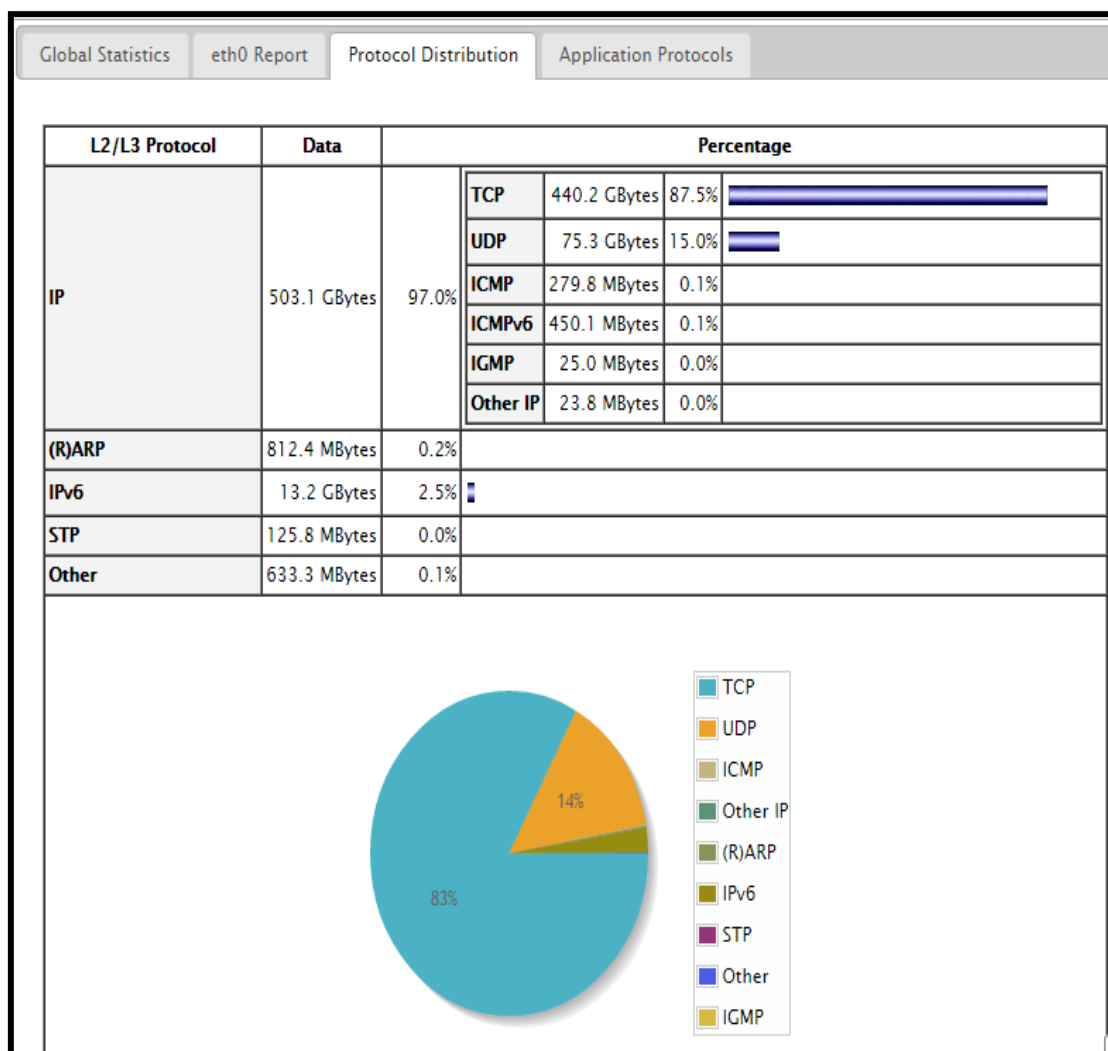


Figura 47. Datos obtenidos con configuración de SNMP

Fuente: Captura propia extraída de software Ntop

De los resultados obtenidos por Ntop se puede identificar claramente que el protocolo SNMP se encuentra dentro de la familia de protocolos UDP y en la gráfica de la Figura 46 de distribución de protocolos sin configuración de SNMP presenta, un porcentaje de 19,8% y en la gráfica de la Figura 47 de distribución de protocolos con configuración de SNMP, presenta un porcentaje de 15,0%, porcentaje relativo mínimo de consumo de SNMP que no afecta el funcionamiento y disponibilidad de la red con la implementación del modelo de gestión.

4.2.4.1.1. Throughput de la red.

Es la medida del desempeño de un sistema que hace referencia al número de bits que pueden ser enviados a través de un enlace durante un intervalo de tiempo determinado. En el Anexo G.3 se muestra detalladamente mediante valores y gráficos capturados por el software Ntop el throughput que generó la red sin configuración de SNMP en los días 27 de Febrero hasta el 05 de Marzo del 2015 y con configuración de SNMP en los días desde el 06 de Marzo hasta el 12 de Marzo del 2015.

4.2.4.1.2. Resultados obtenidos con Wireshark y Ntop

En la Figura 48 que se indica a continuación se puede observar el porcentaje de tráfico Unicast, Broadcast, Multicast, obtenido mediante el software de monitoreo Ntop durante cinco días consecutivos sin configuración de SNMP y cinco días consecutivos con configuración de SNMP como se observa en la Figura 49, en el Anexo G.2 se puede observar a detalle los porcentajes obtenidos. Con el presente resultado se puede concluir que al implementar la configuración del protocolo SNMP en la red, no se produce un porcentaje elevado de tráfico broadcast por lo que no ocasiona ningún conflicto en el envío y recepción de datos entre dispositivos de red de la entidad.

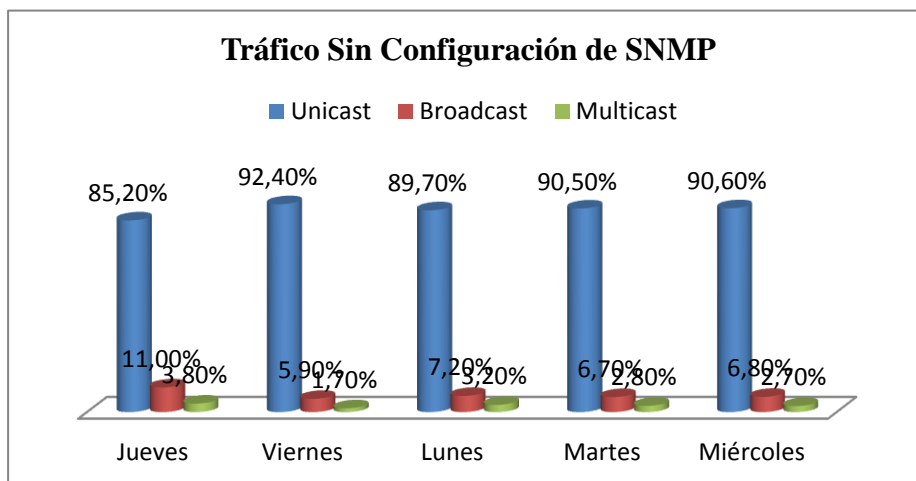


Figura 48. Tráfico capturado de Ntop

Fuente: Datos extraídos de Anexo G Tabla G 1

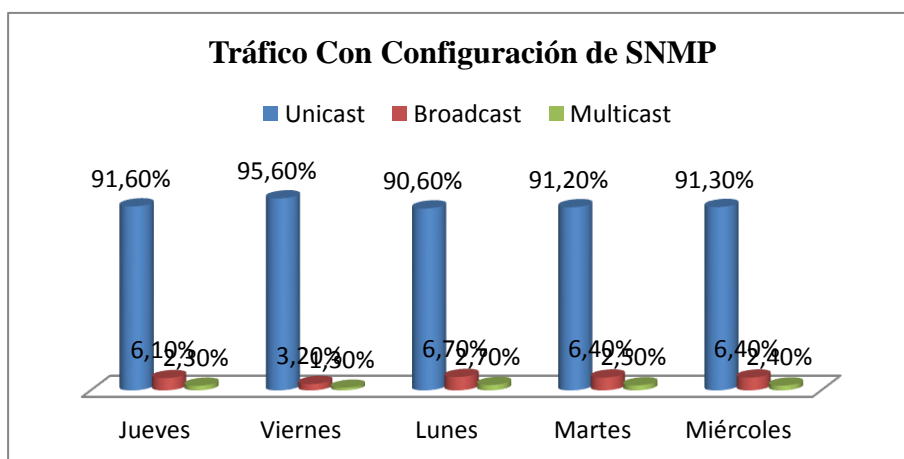


Figura 49. Tráfico capturado de Ntop

Fuente: Datos extraídos de Anexo G Tabla G 2

En la Figura 50 que se indica a continuación se puede observar el porcentaje de tráfico TCP, UDP y otros, obtenido mediante el software de monitoreo Wireshark durante cinco días consecutivos sin configuración de SNMP y cinco días consecutivos con configuración de SNMP como se observa en la Figura 51, en el Anexo G.2 se puede observar a detalle los porcentajes obtenidos. Con el presente resultado medido en tiempo real por lapsos de tiempo aleatorios de 15 minutos se puede concluir que al

implementar la configuración del protocolo SNMP en la red, no aumenta el porcentaje de tráfico UDP por lo que no ocasiona ningún conflicto en el envío y recepción de datos entre dispositivos de red de la entidad.

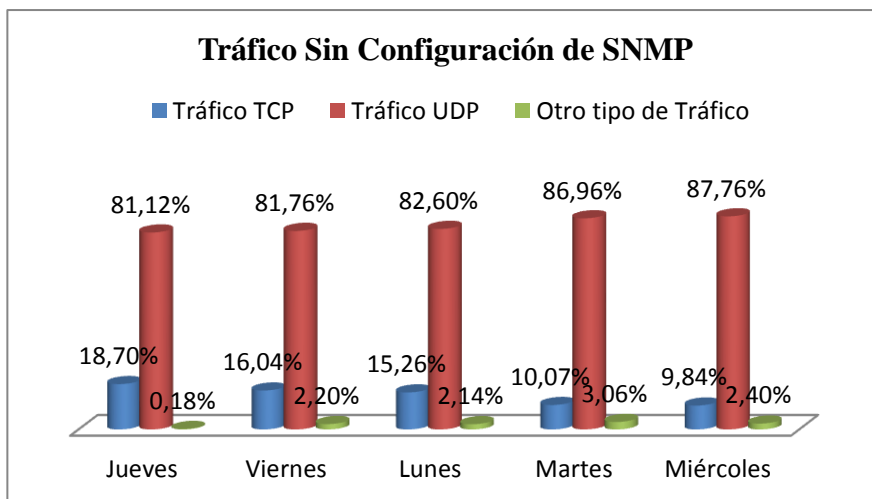


Figura 50. Tráfico capturado de Wireshak

Fuente: Datos extraídos de Anexo G Tabla G 3

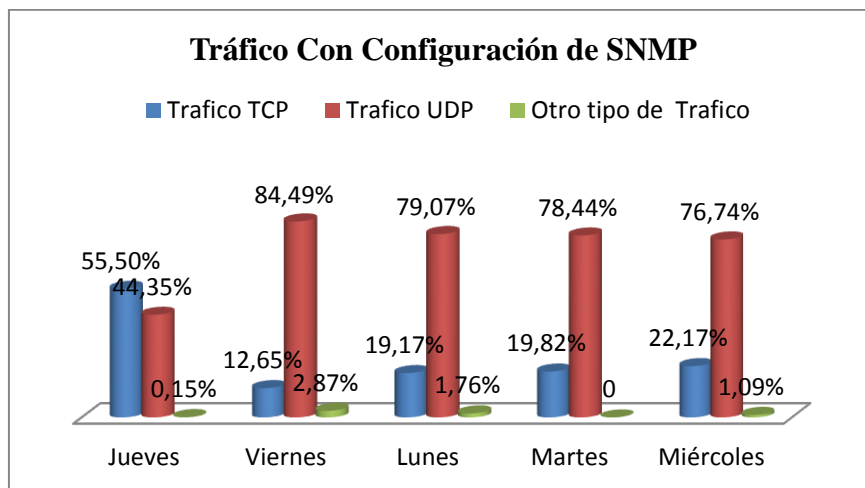


Figura 51. Tráfico capturado de Wireshak

Fuente: Datos extraídos de Anexo G Tabla G 4

En la Figura 52 se puede observar una captura generada por Wireshark, donde presenta una gráfica de consumo del protocolo SNMP baja con respecto a los protocolos TCP y UDP.

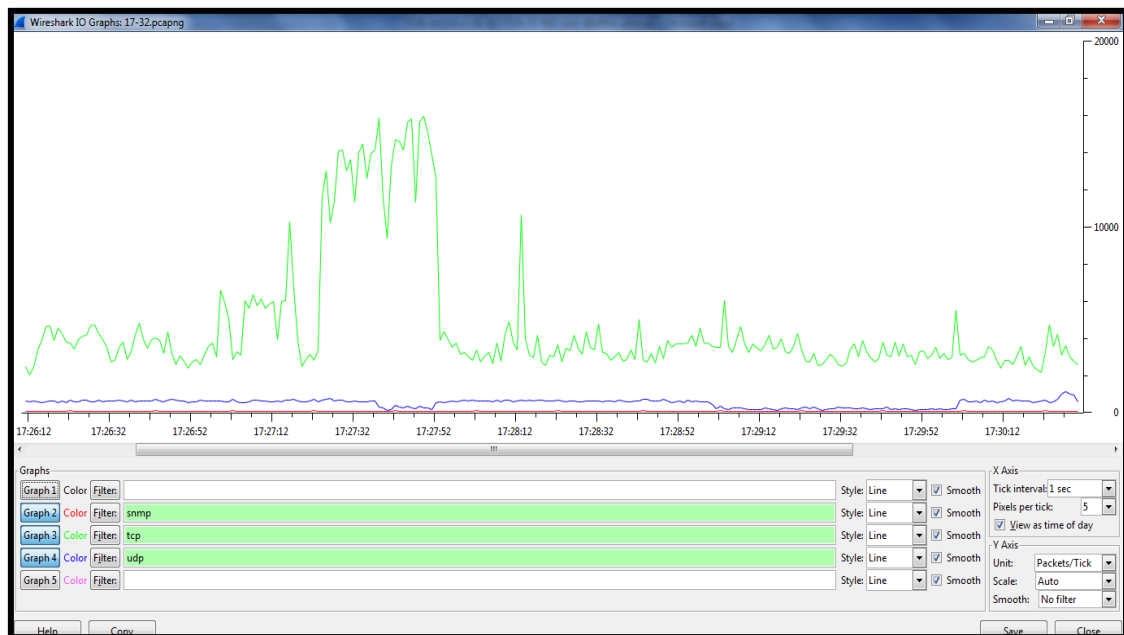


Figura 52. Tráfico capturado de Wireshak

Fuente: Datos extraídos de software Wireshark

4.2.4.2. Datos estadísticos del rendimiento de los recursos de la red en Nagios.

Dentro de la medición del rendimiento de la red se debe tener en cuenta los siguientes aspectos:

- La disponibilidad de funcionamiento de la red local de datos es una labor primordial dentro del Departamento TIC del GAD-Ibarra. Mediante esta actividad lo que se prioriza es aquellos servidores, servicios y elementos de red que permiten la conectividad con toda la entidad.
- Verificar constantemente que los límites de umbrales que se determinó se cumplan correctamente dentro de los parámetros establecidos para su medición.

4.2.4.2.1. Rendimiento por áreas críticas

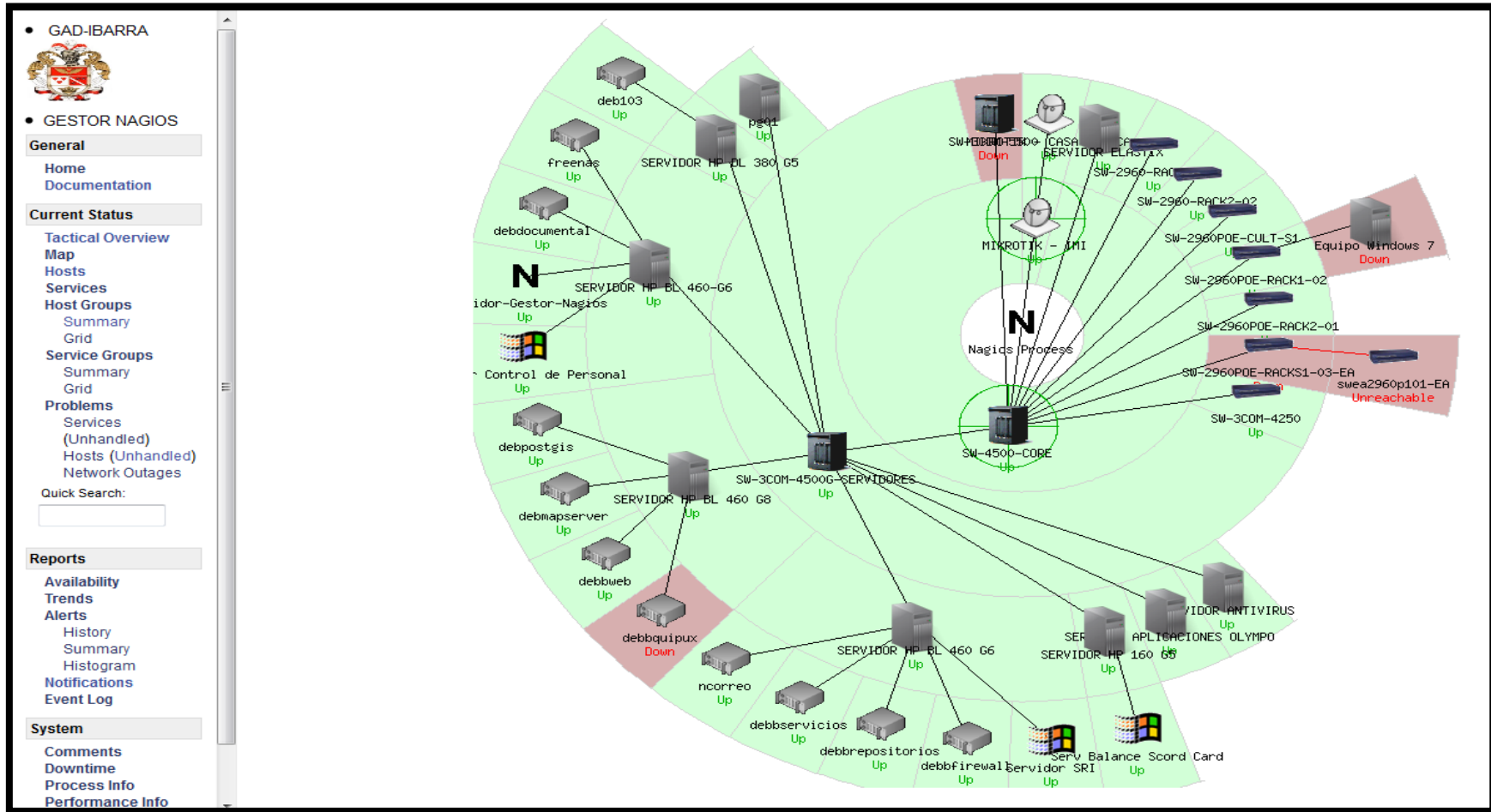


Figura 53. Rendimiento de Nagios

Fuente: Captura propia obtenida del software de gestión Nagios

A partir de la Figura 53 se muestra los datos estadísticos que indican el rendimiento que genera cada uno de los dispositivos gestionados de la red local de datos con solo dar un click en el que se desea conocer sus resultados monitoreados. A continuación se indica el rendimiento por áreas críticas.

4.2.4.2.2. Rendimiento en la Capa Núcleo.

Nagios permite al administrador visualizar en su interfaz web el nombre del dispositivo gestionado, servicio que esta monitoreando, estado, tiempo de chequeo, duración y la información del servicio en tiempo real. En seguida se describe los parámetros que indica la interfaz web en la Figura 54.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
SWI-4500-CORE	01. PING	OK	04-01-2015 14:51:34	15d 4h 42m 59s	1/3	PING OK - Packet loss = 0%, RTA = 1.26 ms
	02. Memoria RAM	OK	04-01-2015 14:54:04	15d 4h 43m 26s	1/3	OK: Processor: valid, Used: 127147260B Free: 89769480B (41%)
	03. Sensor de Temperatura Chasis	OK	04-01-2015 14:53:49	0d 2h 34m 34s	1/3	SNMP OK - "Chassis Temperature Sensor"
	04. Carga de CPU	OK	04-01-2015 14:54:05	15d 4h 43m 38s	1/3	OK: CPU1000: 17% 20% 21% !
	05. Ventilador	CRITICAL	04-01-2015 14:53:51	15d 4h 43m 18s	3/3	CRITICAL: Power Supply 1 Fan: normal Chassis Fan Tray 1: normal Power Supply 2 Fan: notPresent!
	06. Fuente de Alimentación	CRITICAL	04-01-2015 14:54:05	15d 4h 42m 58s	3/3	PS: Crit - 2 PS are running , Power Supply 2 -> notPresent have an error

Figura 54. Rendimiento de servicios del Switch Core

Fuente: Captura propia extraída de software de gestión Nagios

01. Ping.- Indica el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
02. Memoria RAM.- Indica la cantidad de memoria utilizada y el porcentaje libre de su totalidad.
03. Sensor de Temperatura Chasis.- Indica estado de sensor de temperatura de chasis.

04. Carga de CPU.- Indica el porcentaje de uso que consume la CPU.
05. Ventiladores.- Indica el número de ventiladores presentes y estado de funcionamiento de cada uno.
06. Fuente de alimentación.- Indica el número de fuentes de alimentación presentes y estado de funcionamiento de cada una.

El procesamiento del switch core no supera el 25% pico de utilización durante el periodo de diez meses de monitoreo por lo que se deduce que el dimensionamiento de los equipos de la red se ajustan a las necesidades actuales.

En la Figura 55 se muestra el rendimiento capturado por Nagios en su interfaz web de cada una de las interfaces Gigabit Ethernet y VLAN configuradas del switch core y que se conectan a los diferentes switches de distribución y acceso de la entidad.

07. GigabitEthernet [1/1] Hacia SW-2960-RACK2-01		OK	03-22-2015 11:35:56	4d 23h 44m 43s	1/3	OK - Average IN: 184.29Kbps 0.18% Average OUT: 222.33Kbps 0.22%
08. GigabitEthernet [1/2] Hacia SW-2960-RACK2-02		OK	03-22-2015 11:36:06	2d 0h 43m 45s	1/3	OK - Average IN: 42.98Kbps 0.04% Average OUT: 185.08Kbps 0.19%
09. GigabitEthernet [1/3] Hacia SW-3COM-5500-RACK1-01		OK	03-22-2015 11:36:31	2d 2h 46m 44s	1/3	OK - Average IN: 12.34Kbps 0.01% Average OUT: 44.00Kbps 0.04%
10. GigabitEthernet [1/7]		OK	03-22-2015 11:36:46	2d 2h 46m 42s	1/3	OK - Average IN: 1.24Kbps 0.00% Average OUT: 18.52Kbps 0.02%
11. GigabitEthernet [1/9] Hacia LINK-1-CHECKPOINT		OK	03-22-2015 11:36:21	2d 2h 46m 43s	1/3	OK - Average IN: 4.31Mbps 4.31% Average OUT: 157.50Kbps 0.16%
12. GigabitEthernet [1/10] Hacia LINK-2-CHECKPOINT		CRITICAL	03-22-2015 11:36:16	5d 1h 27m 29s	3/3	CRITICAL: Interface 12 is down!
13. GigabitEthernet [1/11] Hacia SW-3COM-SERVIDORES		OK	03-22-2015 11:36:15	2d 0h 15m 43s	1/3	OK for 13 - Average IN: 77.48Kbps 0.01% Average OUT: 455.74Kbps 0.05%
14. GigabitEthernet [1/12] Hacia SW-2960POE-RACK2-05		OK	03-22-2015 11:35:51	2d 2h 46m 6s	1/3	OK - Average IN: 406.27Kbps 0.41% Average OUT: 2.50Mbps 2.50%
15. GigabitEthernet [1/18] Hacia CUARTEL		CRITICAL	03-22-2015 11:36:11	4d 23h 36m 14s	3/3	CRITICAL: Interface 20 is down!
16. GigabitEthernet [1/19] Enlace FIBRA OPTICA CULTURA		OK	03-22-2015 11:36:31	2d 2h 46m 6s	1/3	OK - Average IN: 11.84Kbps 0.01% Average OUT: 36.42Kbps 0.04%
17. GigabitEthernet [1/20] Enlace FIBRA OPTICA EDIFICIO ANTIGUO		CRITICAL	03-22-2015 11:35:56	4d 23h 36m 13s	3/3	CRITICAL: Interface 22 is down!
18. GigabitEthernet [2/47] Hacia SW-2960POE-RACK1-06		OK	03-22-2015 11:35:56	2d 2h 46m 6s	1/3	OK - Average IN: 11.19Kbps 0.01% Average OUT: 27.46Kbps 0.03%
19. GigabitEthernet [2/48] Hacia Servidor VoIP		OK	03-22-2015 11:36:45	2d 2h 46m 11s	1/3	OK - Average IN: 16.58Kbps 0.02% Average OUT: 26.79Kbps 0.03%
20. VLAN 1		OK	03-22-2015 11:36:29	2d 2h 46m 41s	1/3	OK - Average IN: 134.13Kbps 0.13% Average OUT: 4.55Mbps 4.55%
21. VLAN 2		OK	03-22-2015 11:36:11	2d 2h 46m 6s	1/3	OK - Average IN: 1.70Kbps 0.00% Average OUT: 967.73bps 0.00%
22. VLAN 3 VoIP		CRITICAL	03-22-2015 11:35:51	1d 18h 29m 13s	3/3	CRITICAL Traffic IN for 80 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 80
23. VLAN 7		OK	03-22-2015 11:36:11	4d 23h 36m 50s	1/3	OK - Average IN: 166.55Kbps 0.17% Average OUT: 224.33Kbps 0.22%

Figura 55. Rendimiento de servicios del Switch Core

Fuente: Captura propia extraída de software de gestión Nagios

Además Nagios permite visualizar mediante una gráfica el rendimiento de cada interfaz de los enlaces críticos de la red local de datos del GAD-Ibarra, mediante la aplicación PNP4Nagios haciendo click en el icono que se encuentra en el lado derecho junto al nombre de cada interfaz. En la Figura 56 se puede observar el ancho de banda de entrada y salida consumido por una interfaz de red.

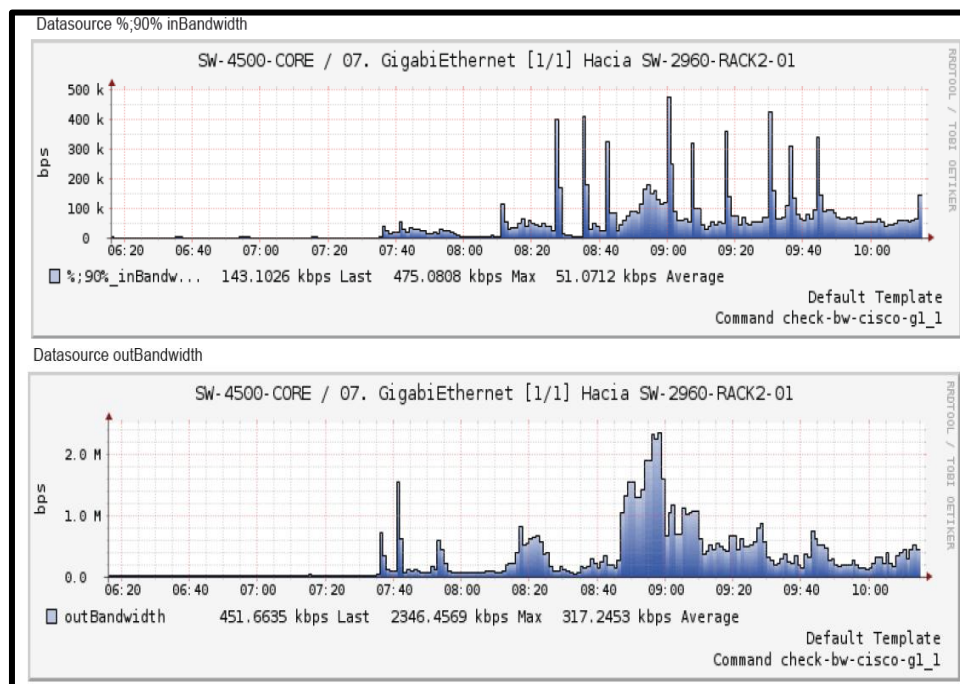


Figura 56. Tráfico de interfaz del switch core

Fuente: Captura propia extraída de software de gestión Nagios

La velocidad de transmisión que manejan los enlaces de la red de la entidad son de tipo GigabitEthernet (1000 Mbps) para la capa core por esta razón no es de mayor preocupación que el ancho de banda que ocupe la red provoque una saturación de enlaces o cuellos de botella, sin embargo en Nagios están configurados umbrales que llegan a notificar en caso de que sobrepasen el consumo de ancho de banda normal.

4.2.4.2.3. Rendimiento en la Capa Distribución.

En la gráfica de la Figura 57 se puede observar el rendimiento del switch 3Com 4500G de la capa de distribución en el cual están conectados los servidores de la entidad y donde se han monitoreado los siguientes parámetros:

SW-3COM-4500G-SERVIDORES	ID	Estado	Fecha y Hora	Uptime	Severidad	Detalle
	01. PING	OK	04-02-2015 09:41:37	16d 0h 15m 54s	1/3	PING OK - Packet loss = 0%, RTA = 1.94 ms
	02. Fuente de Alimentacion	OK	04-02-2015 09:44:15	1d 2h 41m 43s	1/3	SNMP OK - "PowerSupply"
	02. Ventilador	OK	04-02-2015 09:44:31	1d 2h 41m 25s	1/3	SNMP OK - "FAN UNIT"
	03. GigabitEthernet [1/0/1]	OK	04-02-2015 09:44:30	0d 0h 18m 7s	1/3	OK - Average IN: 1.52Mbps 1.52% Average OUT: 2.83Mbps 2.83%
	04. GigabitEthernet [1/0/2] Hacia Servidor Antivirus	OK	04-02-2015 09:43:35	0d 0h 18m 2s	1/3	OK - Average IN: 32.27Kbps 0.03% Average OUT: 85.13Kbps 0.09%
	05. GigabitEthernet [1/0/3]	OK	04-02-2015 09:44:23	0d 0h 0m 14s	1/3	OK - Average IN: 190.53bps 0.00% Average OUT: 66.50Kbps 0.07%
	06. GigabitEthernet [1/0/4]	CRITICAL	04-02-2015 09:42:52	0d 0h 1m 45s	1/3	CRITICAL Average Traffic IN: 8.53bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 4
	07. GigabitEthernet [1/0/5] Hacia HP DL 380 G5	CRITICAL	04-02-2015 09:44:14	1d 2h 41m 24s	3/3	CRITICAL Average Traffic IN: 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 5
	08. GigabitEthernet [1/0/6] Hacia Servidor OLYMPO	OK	04-02-2015 09:43:43	0d 0h 17m 53s	1/3	OK - Average IN: 59.72Kbps 0.06% Average OUT: 64.10Kbps 0.06%
	09. GigabitEthernet [1/0/7]	OK	04-02-2015 09:43:38	0d 0h 17m 59s	1/3	OK - Average IN: 5.88Kbps 0.01% Average OUT: 65.16Kbps 0.07%
	10. GigabitEthernet [1/0/8]	OK	04-02-2015 09:43:42	0d 0h 17m 55s	1/3	OK - Average IN: 1.39Mbps 1.39% Average OUT: 441.50Kbps 0.44%
	11. GigabitEthernet [1/0/9] Hacia Servidor Almacenamiento	OK	04-02-2015 09:44:21	0d 0h 17m 16s	1/3	OK - Average IN: 44.27bps 0.00% Average OUT: 74.11Kbps 0.07%
	12. GigabitEthernet [1/0/10] Hacia Servidor Almacenamiento	OK	04-02-2015 09:43:40	0d 0h 17m 57s	1/3	OK - Average IN: 51.93bps 0.00% Average OUT: 58.98Kbps 0.06%
	13. GigabitEthernet [1/0/15]	OK	04-02-2015 09:43:35	0d 0h 18m 1s	1/3	OK - Average IN: 349.60bps 0.00% Average OUT: 60.57Kbps 0.06%
	14. GigabitEthernet [1/0/19] Hacia Chasis Blade	CRITICAL	04-02-2015 09:44:28	0d 0h 2m 9s	2/3	CRITICAL Average Traffic IN: 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 19
	15. GigabitEthernet [1/0/20] Hacia Chasis Blade	OK	04-02-2015 09:43:40	0d 0h 17m 57s	1/3	OK - Average IN: 1.05Mbps 1.05% Average OUT: 1.67Mbps 1.67%
	VLAN 1	CRITICAL	04-02-2015 09:43:55	8d 5h 40m 18s	3/3	CRITICAL Average Traffic IN: 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 30

Figura 57. Rendimiento de servicios del switch de distribución

Fuente: Captura propia extraída de software de gestión Nagios

01. Ping.- Indica el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
02. Ventilador.- Indica el estado de ventilador.
03. Fuente de alimentación.- Indica el estado de la fuente de alimentación.

En la Figura 58 se observa una gráfica a través de PNP4Nagios, acerca del rendimiento de ancho de banda consumido de entrada y salida por las interfaces de red activas.

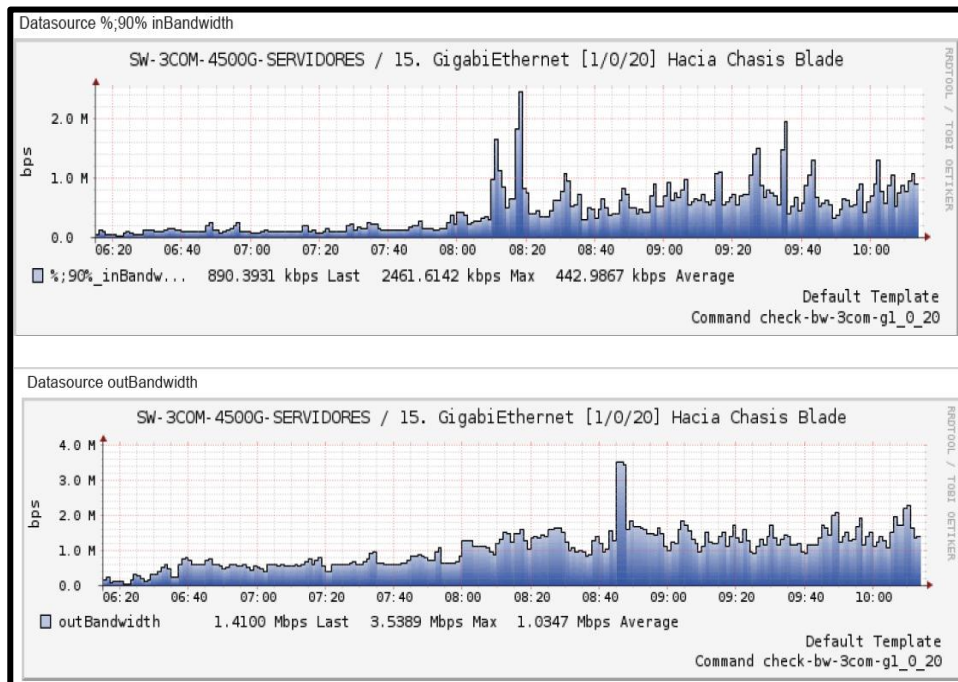


Figura 58. Tráfico de interfaz del switch de distribución

Fuente: Captura propia extraída de software de gestión Nagios

La velocidad de transmisión que manejan los enlaces de la red de la entidad son de tipo GigabitEthernet (1000 Mbps) para la capa de distribución por esta razón no es de mayor preocupación que el ancho de banda que ocupe la red provoque una saturación de enlaces o cuellos de botella, sin embargo en Nagios están configurados umbrales que lleguen a notificar en caso de que sobrepasen el consumo de ancho de banda normal.

4.2.4.2.4. Rendimiento en la Capa Acceso.

En la Figura 59 se puede observar el rendimiento del switch Cisco Catalyst 2960 ubicado en la casa de la ibarreñidad en el departamento de Cultura, dentro de esta capa se monitorearon los siguientes servicios:

SW-2960POE-CULT-S1	01. PING	OK	04-01-2015 10:04:39	0d 18h 20m 29s	1/3	PING OK - Packet loss = 0%, RTA = 1.00 ms
	02. Memoria RAM	OK	04-01-2015 10:04:01	12d 22h 35m 43s	1/3	OK: Driver text: valid, Used: 40B Free: 1048536B (99%) / IO: valid, Used: 1641672B Free: 2544440B (60%) / Processor: valid, Used: 9004856B Free: 26147884B (74%)
	03. Memoria Flash	OK	04-01-2015 10:04:14	12d 22h 35m 57s	1/3	OK: Onboard system FLASH: Size: 27998208 Free: 17231360 (61%) Status: available VPP: installed!
	04. Carga de CPU	OK	04-01-2015 10:04:10	12d 22h 35m 42s	1/3	OK: CPU0: 6% 6% 6% !
	05. Ventilador	OK	04-01-2015 10:04:18	12d 22h 36m 13s	1/3	OK: Switch#1, Fan#1: normal!
	06. Fuente de Alimentacion	OK	04-01-2015 10:03:51	13d 18h 34m 16s	1/3	PS: OK - 1 PS are running all good

Figura 59. Rendimiento de servicios de switch de acceso

Fuente: Captura propia extraída de software de gestión Nagios

01. Ping.- Indica el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
02. Memoria RAM.- Indica la cantidad de memoria utilizada y el porcentaje libre de su totalidad.
03. Memoria Flash.- Indica la cantidad de memoria utilizada y el porcentaje libre de su totalidad.
04. Carga de CPU.- Indica el porcentaje de uso que consume la CPU.
05. Ventilador.- Indica el número de ventiladores presentes y estado de funcionamiento de cada uno.
06. Fuente de alimentación.- Indica el número de fuentes de alimentación presentes y estado de funcionamiento de cada una.

4.2.4.2.5. Rendimiento en Enlaces Inalámbricos.

En la Figura 60 se observa el rendimiento de enlaces inalámbricos Mikrotik ubicados, uno en la entidad y el otro enlace en la casa blanca, aquí se han monitoreado los siguientes servicios:

MIKROTIK - CASA BLANCA	01. PING	OK	04-01-2015 11:43:26	0d 20h 27m 1s	1/3	PING OK - Packet loss = 0%, RTA = 0.47 ms
	02. Mikrotik dBm	OK	04-01-2015 11:43:09	6d 19h 17m 1s	1/3	SNMP OK - Average clients signal level is -37dBm
	03. Dispositivos Conectados	OK	04-01-2015 11:42:48	0d 1h 14m 1s	1/3	SNMP OK - Clients connected 1
	04. Memoria Principal	OK	04-01-2015 11:43:12	0d 0h 0m 33s	1/3	SNMP OK - "main memory"
	05. Disco	OK	04-01-2015 11:43:34	0d 0h 0m 11s	1/3	SNMP OK - "disk: system"
MIKROTIK - IMI	01. PING	OK	04-01-2015 11:43:21	0d 20h 27m 22s	1/3	PING OK - Packet loss = 0%, RTA = 1.03 ms
	02. Mikrotik dBm	OK	04-01-2015 11:42:53	0d 20h 27m 37s	1/3	SNMP OK - Average clients signal level is -34dBm
	03. Dispositivos Conectados	OK	04-01-2015 11:43:04	0d 1h 13m 39s	1/3	SNMP OK - Clients connected 1
	04. Memoria Principal	OK	04-01-2015 11:42:42	0d 0h 2m 3s	1/3	SNMP OK - "main memory"
	05. Disco	OK	04-01-2015 11:43:09	0d 0h 2m 36s	1/3	SNMP OK - "disk: system"

Figura 60. Rendimiento de servicios de los enlaces inalámbricos

Fuente: Captura propia extraída de software de gestión Nagios

01. Ping.- Indica el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
02. Mikrotik dBm.- Indica el nivel de la señal con los enlaces conectados.
03. Dispositivos conectados.- Indica el número de enlaces conectados.
04. Memoria Principal.- Indica el estado de memoria principal.
05. Disco.- Indica el estado del disco.

4.2.4.2.6. Rendimiento en servidores Virtuales.

En el rendimiento de los servidores virtuales los servicios que más se ven afectados son el espacio de memoria swap y el espacio de disco. Dentro de este grupo se han configurado los siguientes servicios como muestra la Figura 61:

debbsservicios	01. PING	OK	04-01-2015 10:01:14	12d 1h 10m 16s	1/4	PING OK - Packet loss = 0%, RTA = 0.70 ms
	02. Memoria RAM	OK	04-01-2015 10:06:12	12d 1h 10m 3s	1/3	Ram : 34%, Swap : 0% :: OK
	03. Memoria Swap	OK	04-01-2015 10:05:52	12d 1h 9m 51s	1/3	SWAP OK - 100% free (1905 MB out of 1905 MB)
	04. Espacio de Disco	OK	04-01-2015 10:05:56	12d 1h 10m 30s	1/3	DISK OK - free space: / 6586 MB (84% in use=89%):
	05. Carga de CPU	OK	04-01-2015 10:05:17	12d 1h 10m 15s	1/3	OK - load average: 0.00, 0.00, 0.00

Figura 61. Rendimiento de servicios de un servidor virtual

Fuente: Captura propia extraída de software de gestión Nagios

01. Ping.- Indica el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
02. Memoria RAM.- Indica el porcentaje utilizado de memoria RAM.
03. Memoria Swap.- Indica el porcentaje libre de memoria Swap.
04. Espacio de Disco.- Indica el porcentaje de espacio libre de disco.
05. Carga de CPU.- Indica el consumo de carga de CPU.

4.2.4.2.7. Rendimiento en servidores Físicos.

En el rendimiento de servidores físicos los servicios que más se ven afectados es el espacio de disco. Dentro de este grupo se han configurado los siguientes servicios como indica la Figura 62:

SERVIDOR OLYMPO	01. PING	OK	04-01-2015 10:29:56	12d 23h 13m 54s	1/4	PING OK - Packet loss = 0%, RTA = 0.37 ms
	02. Memoria RAM	OK	04-01-2015 10:30:16	6d 19h 27m 46s	1/3	Memory usage: total:4452,21 Mb - used: 994,87 Mb (22%) - free: 3457,34 Mb (78%)
	03. C:\ Espacio de Disco	CRITICAL	04-01-2015 10:30:18	7d 0h 14m 55s	3/3	C: - total: 24,41 Gb - used: 22,29 Gb (91%) - free 2,12 Gb (9%)
	04. D:\ Espacio de Disco	OK	04-01-2015 10:29:42	6d 19h 23m 8s	1/3	D: - total: 77,32 Gb - used: 42,43 Gb (55%) - free 34,88 Gb (45%)
	05. Carga de CPU	OK	04-01-2015 10:29:48	0d 13h 48m 7s	1/3	CPU Load 2% (5 min average) 2% (10 min average)

Figura 62. Rendimiento de servicios de un servidor físico

Fuente: Captura propia extraída de software de gestión Nagios

01. Ping.- Indica el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
02. Memoria RAM.- Indica el porcentaje utilizado de memoria RAM y el porcentaje libre
03. Espacio de Disco.- Indica el porcentaje de espacio libre de disco.
04. Carga de CPU.- Indica el consumo de carga de CPU.

4.2.4.2.8. Rendimiento en host.

En la Figura 63 se puede observar el rendimiento de los servicios de ping, memoria RAM, espacio de disco C:\ y D:\, carga de CPU de un host que utiliza el sistema operativo Windows 7.

Equipo Windows 7	01. PING	CRITICAL	04-01-2015 11:39:33	6d 19h 0m 55s	4/4	PING CRITICAL - Packet loss = 100%
	02. Memoria RAM	OK	04-01-2015 11:43:14	0d 3h 29m 29s	1/3	Memory usage: total:7938,32 Mb - used: 1612,78 Mb (20%) - free: 6325,54 Mb (80%)
	03. C:\ Espacio de Disco	OK	04-01-2015 11:43:16	0d 3h 29m 28s	1/3	C: - total: 97,56 Gb - used: 31,39 Gb (32%) - free 66,17 Gb (68%)
	04. D:\ Espacio de Disco	OK	04-01-2015 11:43:14	0d 3h 29m 28s	1/3	D: - total: 368,10 Gb - used: 74,73 Gb (20%) - free 293,37 Gb (80%)
	05. Carga de CPU	OK	04-01-2015 11:43:30	0d 3h 29m 54s	1/3	CPU Load 0% (5 min average) 0% (10 min average)

Figura 63. Rendimiento de servicios de un host

Fuente: Captura propia extraida de software de gestión Nagios

4.2.4.3. Reportes.

El software de gestión Nagios permite disponer de un histórico del comportamiento de los dispositivos de red gestionados, en la Figura 64 se observa el vínculo donde se encuentra los reportes que almacenan los servicios y dispositivos configurados:

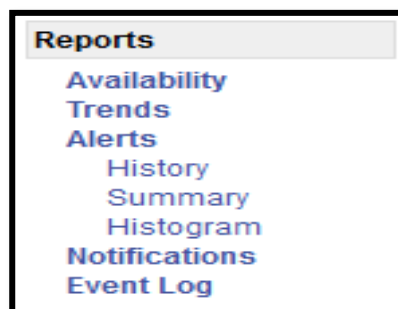


Figura 64. Vínculos para la generación de Reportes

Fuente: Captura extraida de software de gestión Nagios

1. **Availability/Disponibilidad:** Permite obtener estadísticas de disponibilidad es decir muestra las averías que presenta cada estado y cada servicio como se indica en la Figura 65.

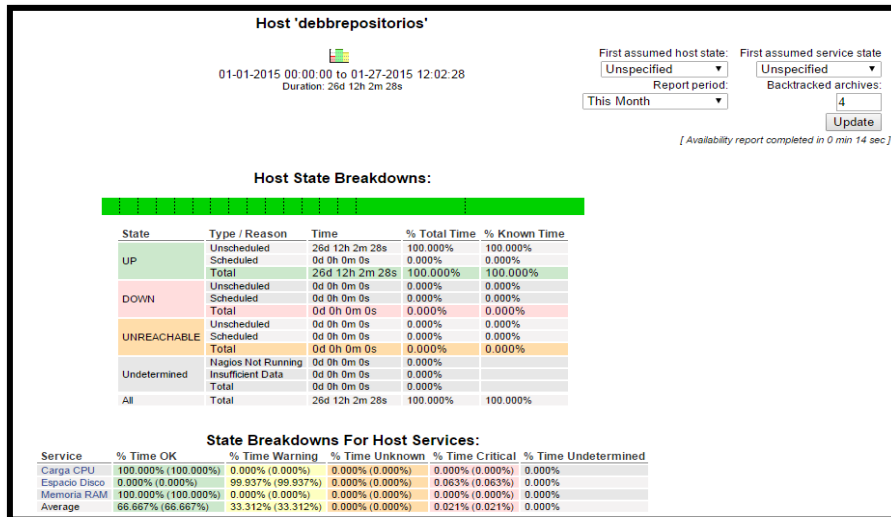


Figura 65. Reporte de disponibilidad

Fuente: Captura propia extraída de software de gestión Nagios

2. **Trends/Tendencia:** Muestra un gráfico que indica el estado un dispositivo de red o un servicio a través del tiempo cuando el estado ha cambiado, y un desglose del porcentaje de los estados.

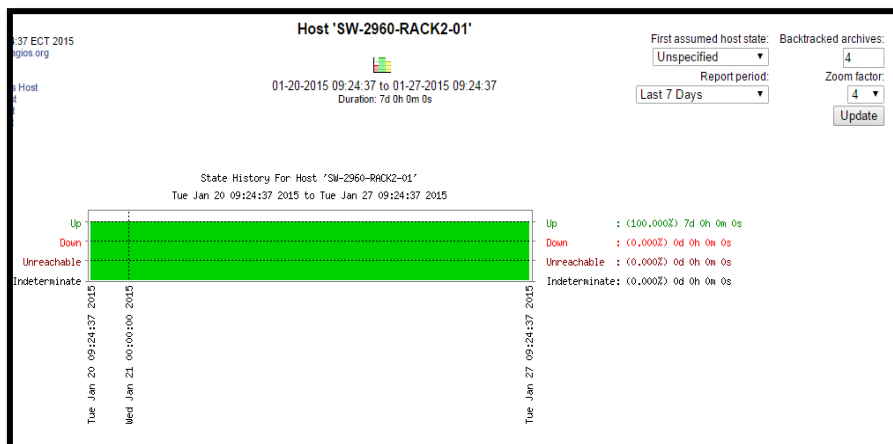


Figura 66. Reporte de tendencia

Fuente: Captura propia extraída de software de gestión Nagios

3. **Alerts/Alertas:** Generadas por una respuesta a un evento cuando un dispositivo o servicio cambia de estado. Dentro de este enlace se encuentran los siguientes subenlaces:

- ✓ *History/Historial.*- Muestra una lista de todas las alertas generadas por dispositivos y servicios indicando iconos de exclamación rojos para estados críticos o abajo, iconos verdes para estados OK y otros. Además la lista se divide en intervalos de horas como se indica en la Figura 67.

The screenshot shows the Nagios Alert History interface. At the top, it displays 'Alert History' with the last update time 'Tue Jan 27 09:24:50 ECT 2015' and the user 'Logged in as nagiosadmin'. Below this, there are links for 'View Status Detail For All Hosts' and 'View Notifications For All Hosts'. The main section is titled 'All Hosts and Services' and shows a 'Log File Navigation' section with a 'Latest Archive' button and a 'Log File Navigation' section showing the current date and time 'Tue Jan 27 09:00:00 ECT 2015' and the file path 'File: /usr/local/nagios/var/nagios.log'. On the right side, there are 'State type options' and 'History detail level for all hosts' sections. The main content area displays a list of alerts for 'January 27, 2015 09:00'. The alerts are listed in a table format with columns for time, severity, and description. The alerts include various system metrics and hardware status reports, such as 'SERVICE ALERT: Servidor-Nagios.Current Load:CRITICAL:HARD:4:CRITICAL - load average: 1.09, 8.53, 18.44' and 'SERVICE ALERT: SW-4500-CORE.Bandwidth-GigabitEthernet 1/12:CRITICAL:HARD:3:(No output on stdout) stErr:'. The alerts are sorted by time, with the most recent at the top.

Figura 67. Reporte de alertas

Fuente: Captura propia extraída de software de gestión Nagios

- ✓ *Summary/Resumen.*- Presenta resultados en forma de tabla de acuerdo con la criterios indicados en el formulario como se observa en la Figura 68.

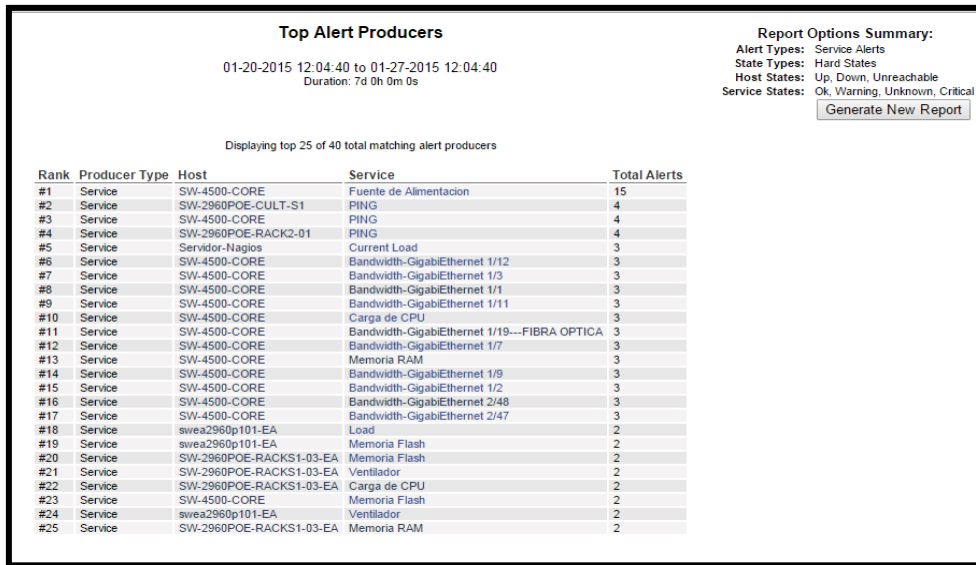


Figura 68. Resumen de reportes

Fuente: Captura propia extraída de software de gestión Nagios

✓ *Histogram/Histograma.*- Muestra un gráfico que indica un desglose de alertas generadas por los dispositivos o servicios designados durante un período de tiempo a elegir en el formulario. En la Figura 69 se indica un histograma de Nagios.

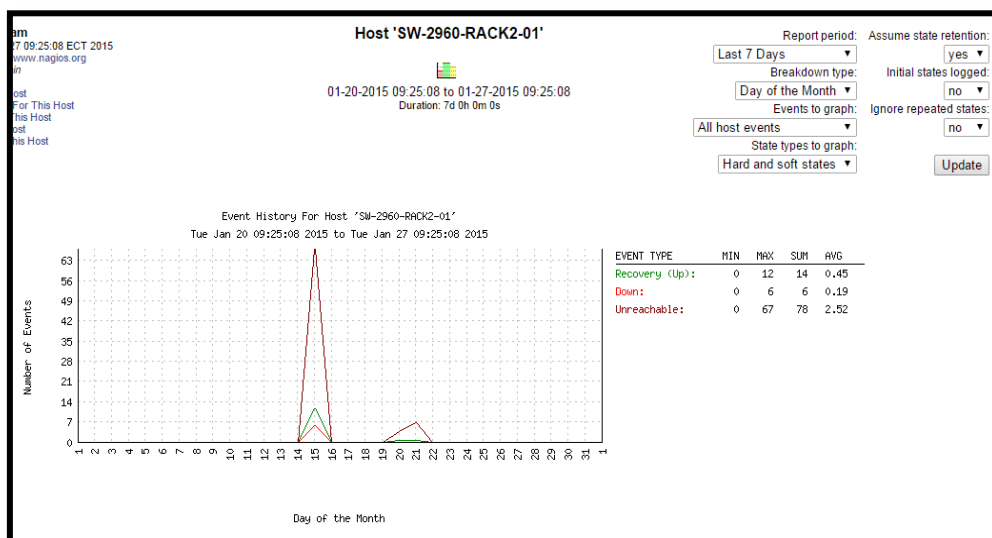


Figura 69. Reporte en forma de histograma

Fuente: Captura propia extraída de software de gestión Nagios

4. **Notifications/Notificaciones:** Muestra el día que se envió la notificación, el tipo de notificación que se envió via SMS o correo electrónico y la información que fue enviada como se puede observar en la Figura 70.

SW-4500-CORE	Fuente de Alimentacion	OK	01-27-2015 09:17:41	nagiosadmin	notify-service-by-email	PS: OK - 0 PS are running all good
SW-4500-CORE	Memoria Flash	OK	01-27-2015 09:17:21	nagiosadmin	notify-service-by-email	(Service check timed out after 519855.50 seconds)
SW-4500-CORE	Bandwidth-GigabitEthernet 1/10	OK	01-27-2015 09:17:21	nagiosadmin	notify-service-by-email	(Service check timed out after 519855.65 seconds)
SW-4500-CORE	Fuente de Alimentacion	CRITICAL	01-21-2015 08:52:08	nagiosadmin	notify-service-by-email	PS: Crit - 2 PS are running , Power Supply 2 -> notPresent have an error
debmapserver	Espacio Disco	CRITICAL	01-21-2015 08:49:05	nagiosadmin	notify-service-by-email	DISK CRITICAL - free space / 174 MB (0% inode=95%):
SW-2960POE-RACK2-01	Memoria Flash	OK	01-21-2015 08:48:11	nagiosadmin	notify-service-by-email	OK: Onboard system FLASH: Size: 27998208 Free: 16079360 (57%) Status: available VPP: installed!
SW-2960POE-RACK2-01	Ventilador	OK	01-21-2015 08:48:09	nagiosadmin	notify-service-by-email	OK: Switch#1, Fan#1: normal
SW-2960POE-CULT-S1	Ventilador	OK	01-21-2015 08:48:05	nagiosadmin	notify-service-by-email	OK: Switch#1, Fan#1: normal
SW-2960POE-CULT-S1	Load	OK	01-21-2015 08:48:05	nagiosadmin	notify-service-by-email	OK: CPU0: 6% 6% 6% !
SW-2960POE-CULT-S1	Memoria Flash	OK	01-21-2015 08:48:05	nagiosadmin	notify-service-by-email	OK: Onboard system FLASH: Size: 27998208 Free: 17231360 (61%) Status: available VPP: installed!
SW-2960-RACK2-01	Memoria Flash	OK	01-21-2015 08:48:05	nagiosadmin	notify-service-by-email	OK: Onboard system FLASH: Size: 27998208 Free: 16784896 (59%) Status: available VPP: installed!
SW-4500-CORE	Carga de CPU	OK	01-21-2015 08:48:05	nagiosadmin	notify-service-by-email	OK: CPU1000: 26% 21% 21% !
SW-2960POE-RACK2-01	Load	OK	01-21-2015 08:48:05	nagiosadmin	notify-service-by-email	OK: CPU0: 23% 24% 23% !
SW-2960POE-RACKS1-03-EA	N/A	HOST DOWN	01-21-2015 08:47:45	nagiosadmin	notify-host-by-email	(Host check timed out after 30.01 seconds)

Figura 70. Reporte de notificaciones

Fuente: Captura propia extraída de software de gestión Nagios

5. **Event Log/Registro de eventos:** Representa de forma más amplia la actividad general de funcionamiento de Nagios.

De igual manera PNP4Nagios permite obtener un reporte al dar un click en el icono que se observa en la Figura 71, donde se abre una página web que permite visualizar y guardar la información almacenada en distintos formatos como; archivo PDF, archivo XML, por 4 horas, 24 horas, una semana, un mes, un año. En el Anexo E.3 se describe a detalle la visualización de reportes.

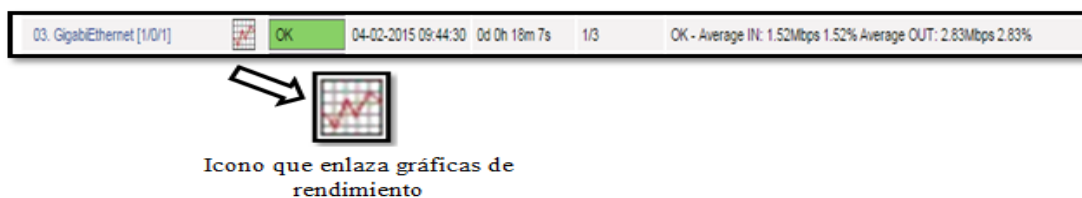


Figura 71. Iconos que generan reportes en PNP4Nagios

Fuente: Captura propia extraída de software de gestión Nagios

4.2.5. Implementación dentro de la Gestión de Seguridad.

Dentro de esta área de gestión es necesario que solo el administrador de la red pueda realizar cambios de configuración al software de gestión por lo que se describe los siguientes parámetros:

4.2.5.1. Acceso y autorización al software de gestión.

El acceso al software de gestión se lo realizará mediante dos permisos de autorización de usuarios los cuales tengan en cuenta la confidencialidad que conlleva acceder a la información de los equipos:

- **Usuario – Administrador**

El usuario nagiosadmin es el usuario administrador del software de gestión el cual tiene todos los privilegios necesarios para realizar cualquier modificación de (agregación, cambio, eliminación, configuración) de equipos y servicios. Además Nagios envía notificaciones de correo electrónico y mensajes de texto al celular a un único contacto informándole de las fallas que se presentan en los dispositivos críticos.

Nagios permite encriptar las claves asignadas a los administradores evitando que un atacante intente ingresar a los archivos de configuración.

- **Usuario – Asistente de Tecnologías**

El usuario asistente de tecnologías tiene permisos de solo lectura es decir solo podrá observar el estado de los equipos y servicios en la interfaz web, no podrá visualizar las pestañas; Process info, Performance info y Scheduling queue, al intentar

ver la configuración le aparecerá el mensaje que se observa en la pantalla de la Figura

72. Donde describe que:

It appears as though you do not have permission to view the configuration information you requested

“El usuario no tiene permiso para ver la información de configuración que solicitó”

If you believe this is an error, check the http server authentication requirements for accessing this CGI and check the authorization options in your CGI configuration file

“Compruebe los requisitos de autenticación del servidor http para acceder a esta CGI y comprobar las opciones de autorización en el archivo de configuración CGI”

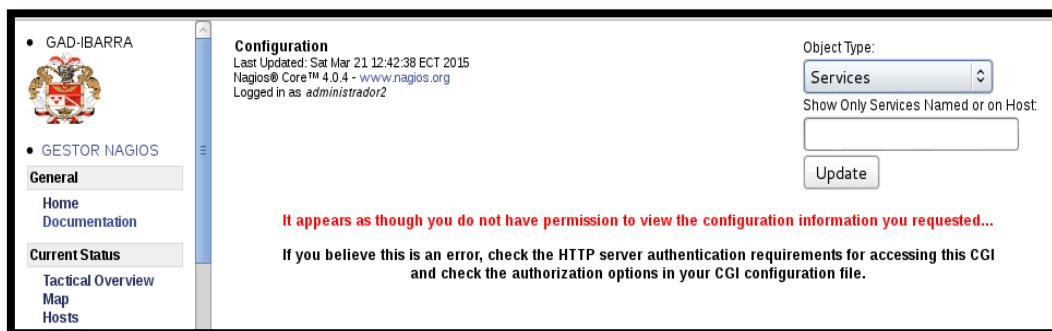


Figura 72. Permiso de acceso de los usuarios a vínculos de Nagios

Fuente: Captura propia de software de gestión Nagios

4.3. Manuales de Procedimientos

Dentro de esta sección se presenta el establecimiento de los manuales de procedimientos estructurados por cada área de gestión de red funcional basadas en el estándar ISO.


4.3.1. Introducción.

El departamento de TIC del GAD-Ibarra tiene la obligación de mantener operativas las tareas informáticas que se realizan dentro de sus diferentes dependencias, para brindar un servicio de calidad a la ciudadanía, por esta razón los equipos deben mantener altos niveles de funcionamiento y disponibilidad.

Por consiguiente se realiza la estructuración de estos manuales con sus respectivas directrices que ayuden a los encargados de la red a diagnosticar y corregir problemas en la red local de datos en el menor tiempo posible, mediante las cinco áreas de gestión las cuales se relacionan entre sí para obtener un mayor rendimiento de sus recursos gestionados. Se presenta el proceso de ingreso y configuración de equipos, localización de fallos, corrección de fallos, visualización de reportes e informes, envío de notificaciones entre otras.

El formato presentado para la elaboración de los manuales de procedimientos que se describen a continuación se rige al estándar que utiliza la entidad de acuerdo a la Norma ISO 9001:2008 elaborado por (Rea Lozada, 2012).

4.3.2. Manual de procedimientos para la Gestión de Configuración.


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.1
	PROCEDIMIENTO:	MANUAL DE GESTIÓN DE CONFIGURACIÓN	VERSIÓN:	1.0

1. **Objetivo.-** Indicar a los administradores de la red el proceso de configuración de nuevos dispositivos a gestionar.


2. **Alcance.-** Aplica este manual al ingreso de dispositivos al software de gestión, los cuales cumplan con los requerimientos de red, su nomenclatura y especificaciones técnicas, además se presenta el procedimiento para switches y servidores.

3. **Abreviaturas**

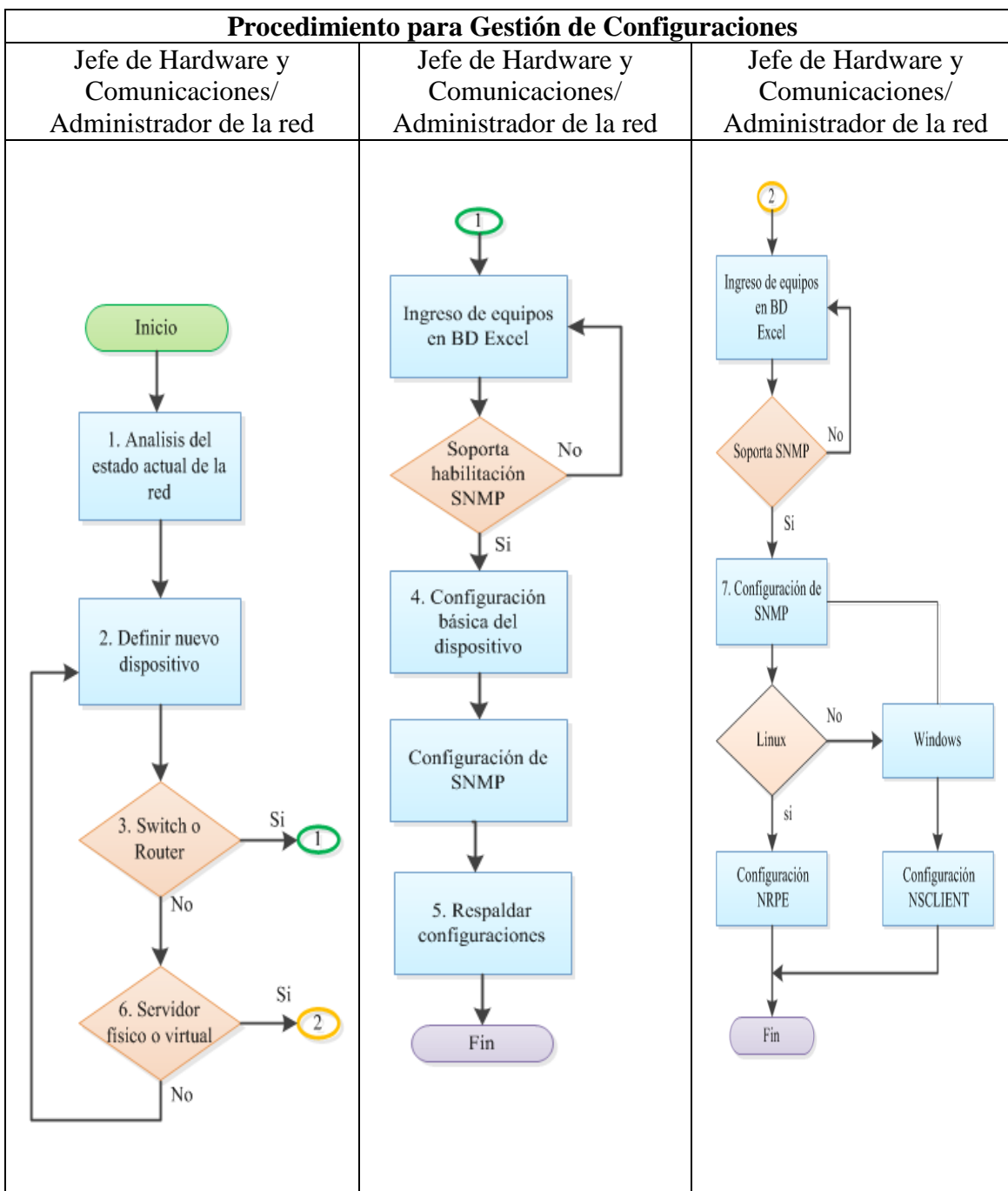
ABREVIATURAS		
Nº	Término	Definición
1	TIC	Tecnología de la Información y Comunicación
2	GAD-Ibarra	Gobierno Autónomo Descentralizado San Miguel de Ibarra
3	SNMP	Protocolo simple de administración de red
4	B.D.	Base de datos donde se almacenan los dispositivos gestionados

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.1
	PROCEDIMIENTO:	MANUAL DE GESTIÓN DE CONFIGURACIÓN	VERSIÓN:	1.0

DEFINICIONES		
Nº	Término	Definición
1	Configuración	Conjunto de pasos y programas que forman parte del funcionamiento de un software.
2	Diagrama de Flujo	Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso.
3	Dispositivo Gestionado	Equipo de red monitoreado en el software de gestión.
4	Software de Gestión	Software que mantiene constantemente monitoreados los equipos de red y permite visualizar en una interfaz web centralizada.
5	Nomeclatura para dispositivos de red	Se define para el formato y sintaxis que deben mantener los equipos de red del GAD-Ibarra al ingresar al modelo de gestión para ser identificados rápidamente.
6	Respaldos	El administrador de la red guarda las configuraciones de cambios de comandos o versiones en una base de datos.
7	Anexo	Documento utilizado para indicar tablas, gráficos, etc, que están relacionados con otro documento que les da origen.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.1
	PROCEDIMIENTO:	GESTIÓN DE CONFIGURACIÓN	VERSIÓN:	1.0


4. Diagrama de flujo:




	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.1
	PROCEDIMIENTO:	GESTIÓN DE CONFIGURACIÓN	VERSIÓN:	1.0

5. Desarrollo de actividades

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Análisis del estado actual de la red	<p>Verificar inventario de dispositivos de red que posee la entidad y las características que tiene cada uno.</p> <p>Mantener información actualizada de direccionamiento de los equipos, ubicación física.</p>	<p>Jefe de área de Hardware y Comunicaciones.</p> <p>Administrador de la red.</p> <p>Asistente de tecnologías.</p>
2	Definir nuevo dispositivo a gestionar	Si es switch ir a Actividad 3 y si es servidor ir a Actividad 6 .	<p>Jefe de área de Hardware y Comunicaciones.</p> <p>Administrador de la red.</p>
3	Dispositivo es un switch	<p>Ingresar el dispositivo en la base de datos Excel de acuerdo a la siguiente nomenclatura establecida por la dirección TIC:</p> <p>- Dirección IP:</p> <p>- Nombre de switch:</p> <p>- Fecha de instalación:</p> <p>- Características Técnicas: Memoria RAM, Procesador, Número de puertos</p> <p>- Funcionalidad:</p> <p>Verificar si soporta la habilitación del protocolo SNMP entonces ir a Actividad 4 caso contrario regresar a la Actividad 2.</p>	<p>Jefe de área de Hardware y Comunicaciones.</p> <p>Administrador de la red.</p>

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.1
	PROCEDIMIENTO:	GESTIÓN DE CONFIGURACIÓN	VERSIÓN:	1.0

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
4	Configuración básica del dispositivo	Asignar un nombre al nuevo dispositivo gestionado, una dirección IP que se encuentre dentro de la red y configurar SNMP v2.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.
5	Respaldar configuraciones	De cada uno de los dispositivos de red gestionados. Controlar que los respaldos se realicen correctamente cuando exista un dispositivo nuevo que ingrese al monitoreo.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.
6	Dispositivo es un servidor	<p>Ingresar el dispositivo en base de datos Excel de acuerdo a la siguiente nomenclatura establecida por la dirección TIC:</p> <ul style="list-style-type: none"> - Dirección IP: - Nombre de Servidor: - Fecha de instalación: - Características <p><i>Técnicas: Memoria RAM, Capacidad Disco Duro, Procesador</i></p> <ul style="list-style-type: none"> - Sistema Operativo: - Versión: - Funcionalidad: <p>Verificar si soporta la habilitación de SNMP, entonces ir a Actividad 7 caso contrario regresar a la Actividad 6.</p>	Jefe de área de Hardware y Comunicaciones. Administrador de la red.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.1
	PROCEDIMIENTO:	GESTIÓN DE CONFIGURACIÓN	VERSIÓN:	1.0

Nro.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
7	Configuración del protocolo SNMP	Configuración del protocolo SNMP v2. Si el servidor se encuentra instalado en un versión de Linux se configurará el agente NRPE caso contrario si el servidor está en un versión de Windows se configurará el agente NSCLIENT++. Las configuraciones se muestra en el Anexo E.2.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.
8	Registro de inventarios	Actualizar las bases de datos en caso de cambios de dispositivos o en caso de cambio de configuraciones y software instalado.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.

4.3.3. Manual de procedimientos para la Gestión de Fallos.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.2
	PROCEDIMIENTO:	GESTIÓN DE FALLOS	VERSIÓN:	1.0

1. **Objetivo.-** Encontrar la mejor solución frente a un problema que se presente en la red local de datos, antes de que sea percibido por los usuarios.

2. **Alcance.-** Aplica el establecimiento de umbrales para los recursos que se van a gestionar, logrando tener mayor disponibilidad de funcionamiento en la red local de datos. Restaurar el servicio tan pronto sea posible e identificar y analizar la causa de los incidentes con el fin de evitar su recurrencia.

El detectar fallas que se basan en su prioridad y urgencia en la red de manera oportuna, permite dar un seguimiento a cualquier eventualidad ocurrida en los dispositivos de gestionados de la red, este punto es de vital importancia cuando se trata del desempeño de una red gubernamental como la del GAD-Ibarra.

3. Abreviaturas

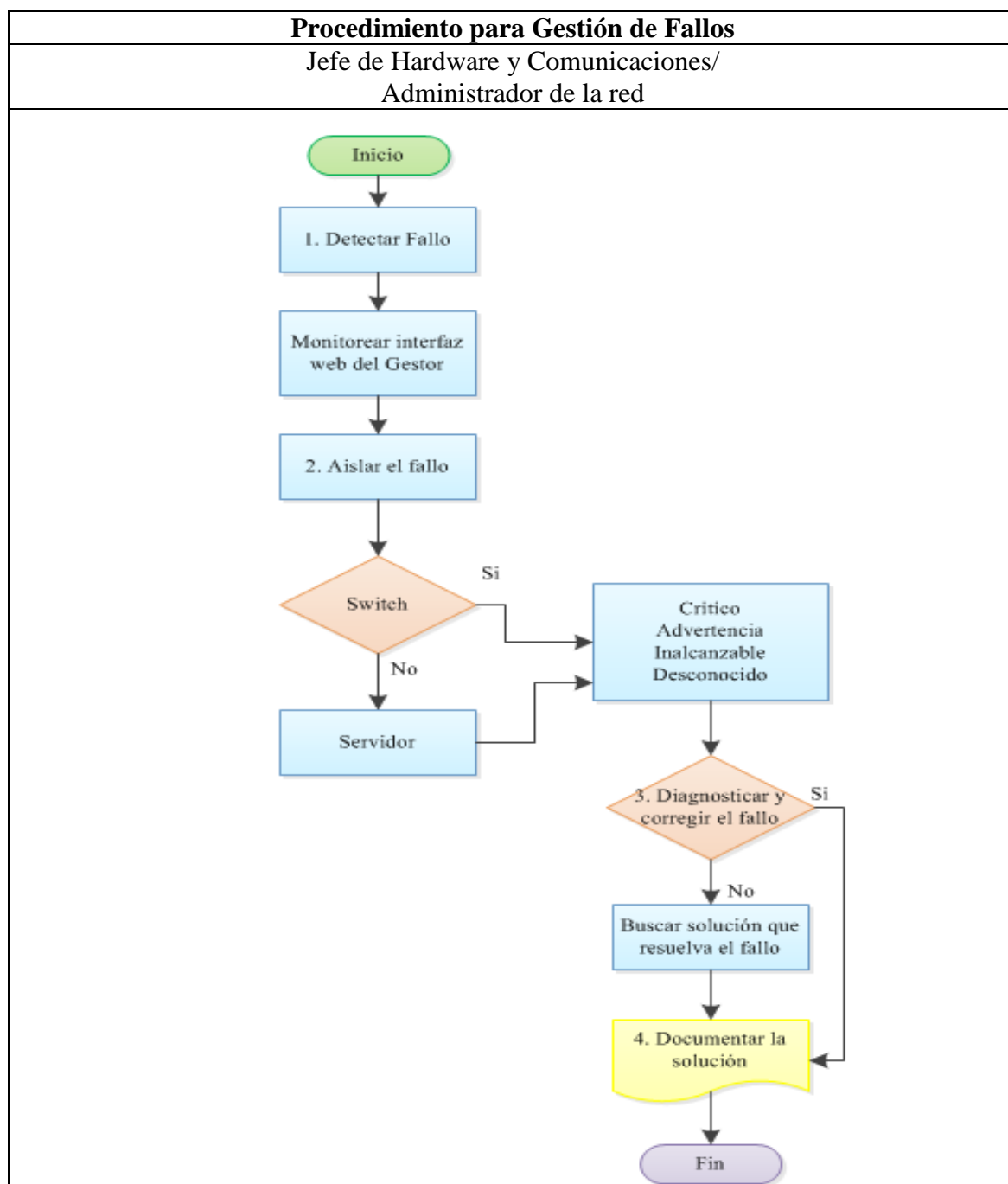
ABREVIATURAS		
Nº	Término	Definición
1	TIC	Tecnología de la Información y Comunicación
2	GAD-Ibarra	Gobierno Autónomo Descentralizado San Miguel de Ibarra
3	SNMP	Protocolo simple de administración de red
4	B.D.	Base de datos donde se almacenan los dispositivos gestionados


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.2
	PROCEDIMIENTO:	GESTIÓN DE FALLOS	VERSIÓN:	1.0

DEFINICIONES		
Nº	Término	Definición
1	Definición de umbrales	Porcentaje referencial de funcionamiento normal de un dispositivo de red.
2	Diagrama de Flujo	Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso.
3	Dispositivo Gestionado	Equipo de red monitoreado en el software de gestión.
4	Software de Gestión	Software que mantiene constantemente monitoreados los equipos de red y permite visualizar en una interfaz web centralizada.
5	Nomeclatura para dispositivos de red	Se define para el formato y sintaxis que deben mantener los equipos de red del GAD-Ibarra al ingresar al modelo de gestión para ser identificados rápidamente.
7	Anexo	Documento utilizado para indicar tablas, gráficos, etc, que están relacionados con otro documento que les da origen.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.2
	PROCEDIMIENTO:	GESTIÓN DE FALLOS	VERSIÓN:	1.0

4. Diagrama de flujo



	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.2
	PROCEDIMIENTO:	GESTIÓN DE FALLOS	VERSIÓN:	1.0


5. Desarrollo de actividades

Nro.	Actividad	Descripción	Responsable
1	Detectar un fallo	<p>Monitorear alertas en la interfaz Web del Gestor e indicar el estado de la red.</p> <p>Detectar mediante un correo electrónico o un SMS.</p>	<p>Jefe de área de Hardware y Comunicaciones.</p> <p>Administrador de la red.</p> <p>Asistente de tecnologías</p>
2	Aislar el fallo	<p>De acuerdo a los parents que se configura en Nagios se determina el equipo que está fallando.</p> <p>Determinar la ubicación exacta de cuellos de botella y problemas en la red, si el dispositivo gestionado ha sobrepasado los niveles de umbrales normales de funcionamiento.</p> <p>Nagios genera mediante colores, cinco estados para localizar el fallo que son:</p> <p>Verde: Host UP y Servicio Ok</p> <p>Rojo: Host Down y Servicio Critico</p> <p>Amarillo: Servicios en advertencia</p> <p>Naranja: Host y Servicios inestables</p> <p>Gris: Host y Servicios desconocido</p>	<p>Jefe de área de Hardware y Comunicaciones.</p> <p>Administrador de la red</p>

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.2
	PROCEDIMIENTO:	GESTIÓN DE FALLOS	VERSIÓN:	1.0

Nro.	Actividad	Descripción	Responsable
		Entre los fallos que se presentan en la red se puede tomar en cuenta el aislamiento del recurso hardware, medio de transmisión o causa externa que provoca la falla.	
		Realizar un seguimiento y control del problema desde su detección hasta su resolución.	
3	Diagnosticar y corregir el fallo	<p>Determinación de posibles soluciones para el problema que se ha suscitado y realizar previas pruebas de la posible solución,</p> <p>Establecer un previo respaldo de las configuraciones para mantener la integridad de la topología de red, antes de proceder a corregir un fallo.</p> <p>Ver más a detalle en la base de datos del Anexo F, la corrección de fallos específicos que se presentan en la red.</p>	Jefe de área de Hardware y Comunicaciones. Administrador de la red.
4	Documentar solución	Si es una falla que no está registrada en la base de datos encontrar la solución y documentar su proceso.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.

4.3.4. Manual de procedimientos para la Gestión de Contabilidad.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.3
	PROCEDIMIENTO:	GESTIÓN DE CONTABILIDAD	VERSIÓN:	1.0

1. **Objetivo.-** Indicar los parámetros que se utilizarán para el monitoreo y configuración de los dispositivos de red que se van a gestionar en la red local de datos.

2. **Alcance.-** Se presenta el procedimiento para agregar dispositivos de red y servicios al software de gestión Nagios los mismos que deben cumplir con las características establecidas para que puedan ser monitoreados y se obtenga la información pertinente de la utilización de cada recurso.

3. Abreviaturas

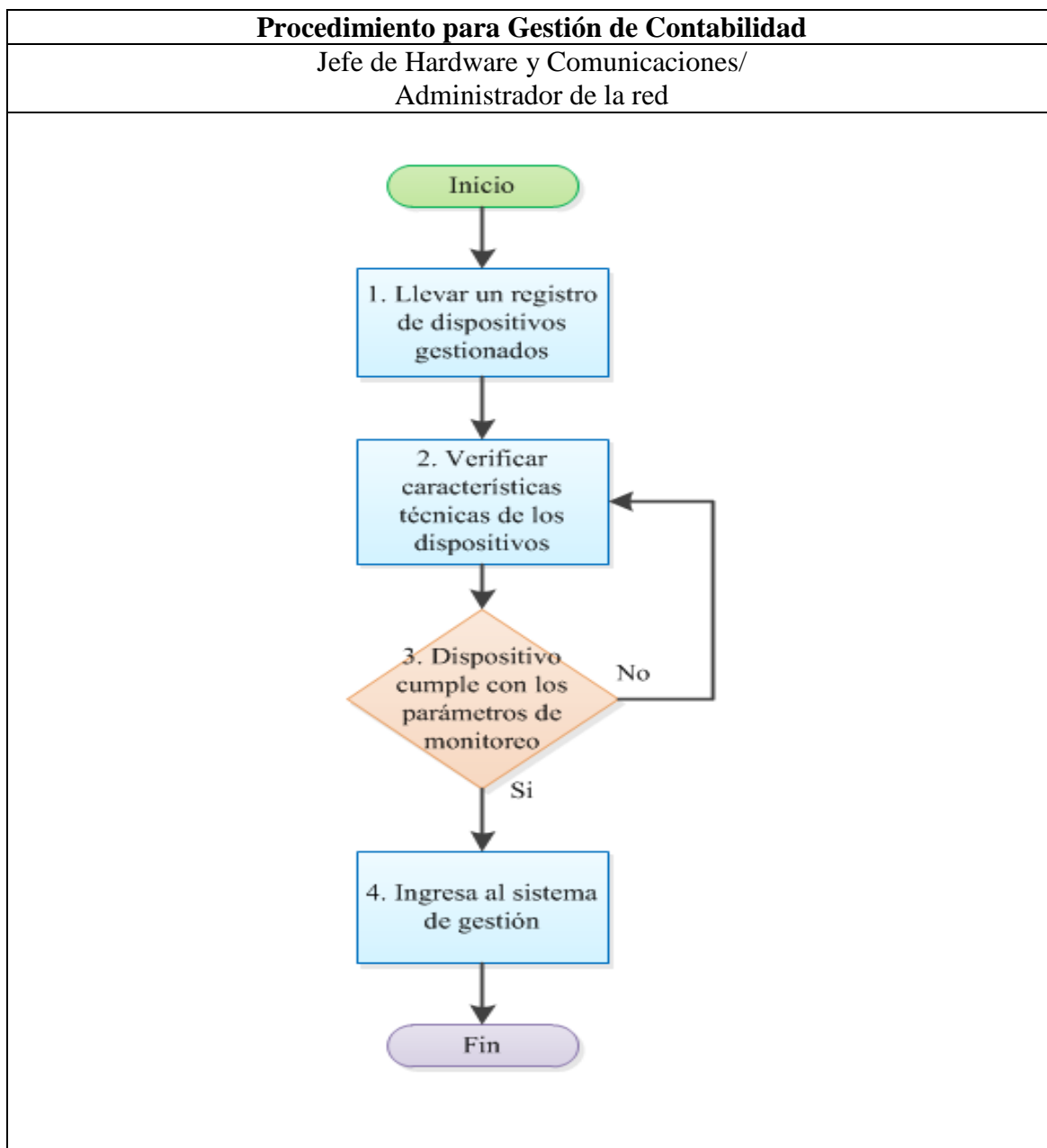
ABREVIATURAS		
Nº	Término	Definición
1	TIC	Tecnología de la Información y Comunicación
2	GAD-Ibarra	Gobierno Autónomo Descentralizado San Miguel de Ibarra
3	SNMP	Protocolo simple de administración de red
4	B.D.	Base de datos donde se almacenan los dispositivos gestionados

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.3
	PROCEDIMIENTO:	GESTIÓN DE CONTABILIDAD	VERSIÓN:	1.0

DEFINICIONES		
Nº	Término	Definición
1	Parámetros de monitoreo	Características técnicas a monitorear en cada dispositivo gestionado es decir; consumo memoria, espacio de disco , carga de CPU.
2	Diagrama de Flujo	Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso.
3	Dispositivo Gestionado	Equipo de red monitoreado en el software de gestión.
4	Software de Gestión	Software que mantiene constantemente monitoreados los equipos de red y permite visualizar en una interfaz web centralizada.
5	Nomeclatura para dispositivos de red	Se define para el formato y sintaxis que deben mantener los equipos de red del GAD-Ibarra al ingresar al modelo de gestión para ser identificados rápidamente.
7	Anexo	Documento utilizado para indicar tablas, gráficos, etc, que están relacionados con otro documento que les da origen.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.3
	PROCEDIMIENTO:	GESTIÓN DE CONTABILIDAD	VERSIÓN:	1.0

4. Diagrama de flujo




	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.3
	PROCEDIMIENTO:	GESTIÓN DE CONTABILIDAD	VERSIÓN:	1.0

5. Desarrollo de Actividades

Nro.	Actividad	Descripción	Responsable
1	Llevar un registro de dispositivos gestionados	Tener un registro de los dispositivos que van a ser gestionados. Tener un registro del tipo de alertas y chequeos que genera Nagios.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.
2	Verificar características técnicas de los dispositivos	Para que los dispositivos de red puedan ingresar al software de gestión deben cumplir con las características técnicas.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.
3	Dispositivo cumple con los parámetros de monitoreo	El dispositivo a ser gestionado debe cumplir con los siguientes parámetros mínimos: soportar la habilitación del protocolo SNMP, consumo de memoria RAM, espacio en disco, consumo de CPU, interfaces de red.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.
4	Ingresa al sistema gestión	El dispositivo está registrado y listo para ser monitoreado por el software de gestión.	Jefe de área de Hardware y Comunicaciones. Administrador de la red.

4.3.5. Manual de procedimientos para la Gestión de Prestaciones.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.4
	PROCEDIMIENTO:	GESTIÓN DE PRESTACIONES	VERSIÓN:	1.0

1. **Objetivo.-** Recopilar y analizar información acerca del rendimiento de los recursos de los dispositivos gestionados.

2. **Alcance.-** Esta gestión se relaciona conjuntamente con la gestión de fallos, por lo tanto aquí se determina el comportamiento en diversos aspectos, ya sea en un intervalo de tiempo en particular o en tiempo real. Esto permitirá tomar las decisiones respectivas de acuerdo a los resultados que generen el comportamiento de los dispositivos gestionados. Además verificar constantemente que los límites de umbrales que se determinó se cumplan correctamente dentro de los parámetros establecidos para su medición.

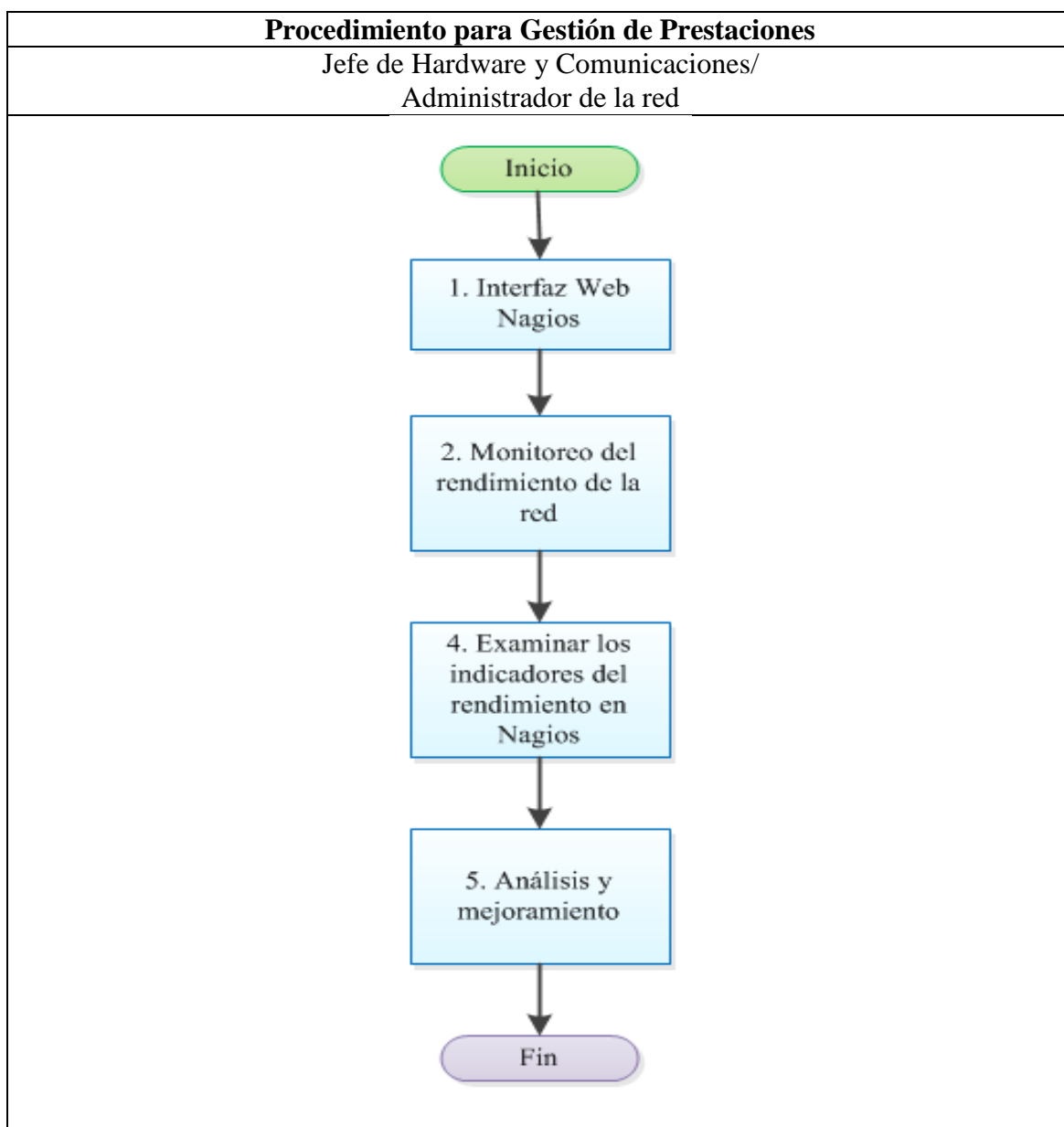
3. **Definiciones**

DEFINICIONES		
Nº	Término	Definición
2	Diagrama de Flujo	Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso.
3	Dispositivo Gestionado	Equipo de red monitoreado en el software de gestión.
4	Software de Gestión	Software que mantiene constantemente monitoreados los equipos de red y permite visualizar en una interfaz web centralizada.
5	Reportes	Son representaciones de informes acerca del rendimiento de cada uno de los recursos de los dispositivos de red monitoreados

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.4
	PROCEDIMIENTO:	GESTIÓN DE PRESTACIONES	VERSIÓN:	1.0


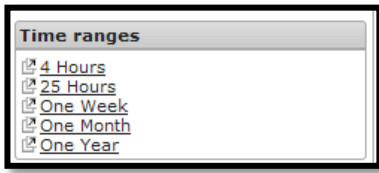
Desarrollo

4. Diagrama de Flujo

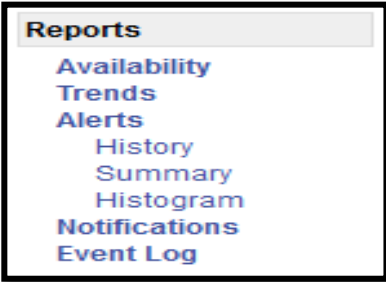


	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.4
	PROCEDIMIENTO:	GESTIÓN DE PRESTACIONES	VERSIÓN:	1.0

5. Desarrollo de Actividades

Nro.	Actividad	Descripción	Responsable
1	Interfaz Web Nagios	Recopila, almacena los datos en forma ordenada para comprensión del administrador.	Jefe de área de Hardware y Comunicaciones Administrador de la red
2	Monitoreo del rendimiento de la red	Visualización del rendimiento de enlaces con PNP4 Nagios en el siguiente icono.  Se podrá observar en la interfaz Web de Nagios de forma porcentual el rendimiento de los recursos.	Jefe de área de Hardware y Comunicaciones Administrador de la red
3	Imprimir informes e historiales	En forma diaria, mensual o anual.  Como respaldo el administrador debe sacar reportes cada mes.	Jefe de área de Hardware y Comunicaciones. Administrador de la red
4	Examinar los indicadores del desempeño en Nagios	Los cuales son los siguientes: Verificar estado de los dispositivos gestionados en las siguientes pestañas del software de gestión Nagios: (Disponibilidad) , reportes, alertas, historiales, resúmenes, histogramas notificaciones.	Jefe de área de Hardware y Comunicaciones. Administrador de la red

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.4
	PROCEDIMIENTO:	GESTIÓN DE PRESTACIONES	VERSIÓN:	1.0

Nro.	Actividad	Descripción	Responsable
			
5	Análisis y mejoramiento	<p>Analizar datos relevantes de la información almacenada para detectar el consumo de los recursos.</p> <p>Usar simulaciones para determinar como la red puede alcanzar máximo rendimiento y poder tomar medidas.</p>	<p>Jefe de área de Hardware y Comunicaciones. Administrador de la red</p>

4.3.6. Manual de procedimientos para la Gestión de Seguridad.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.5
	PROCEDIMIENTO:	GESTIÓN DE SEGURIDAD	VERSIÓN:	1.0

1. **Objetivo.-** Brindar seguridad al sistema de gestión el cual requiere la habilidad para autenticar usuarios y aplicaciones de gestión, con el fin de garantizar la confidencialidad e integridad de intercambios de operaciones de gestión y prevenir accesos no autorizados.

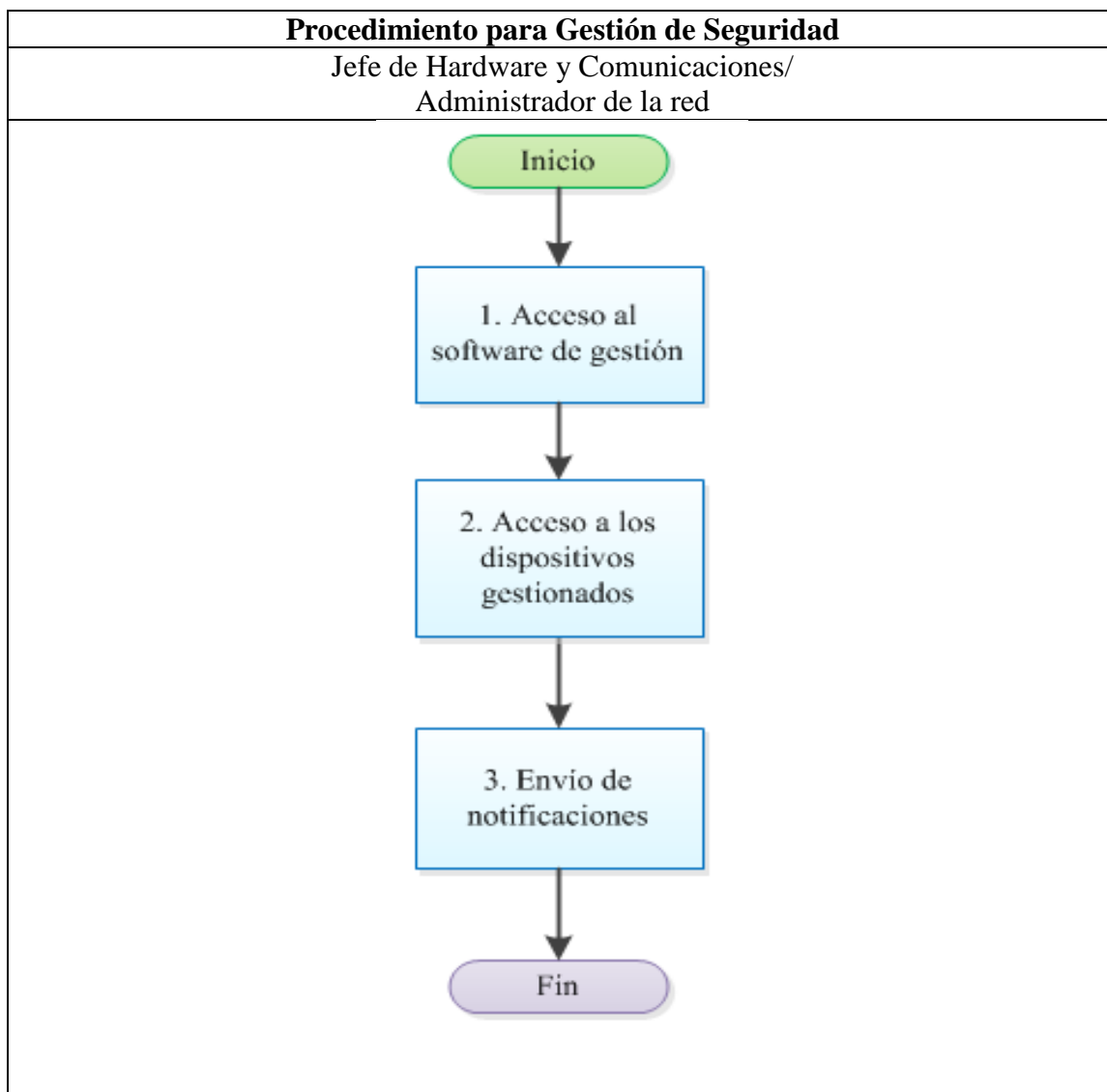
2. **Alcance.-** La información del GAD-Ibarra posee un valor muy importante porque vincula el sistema financiero y el servicio a los usuarios de la ciudadanía por ese motivo es fundamental mantener protegidos los recursos que hacen posible la conectividad y comunicación con entidades externas.

3. Definiciones

DEFINICIONES		
Nº	Término	Definición
2	Diagrama de Flujo	Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso.
3	Dispositivo Gestionado	Equipo de red monitoreado en el software de gestión.
4	Software de Gestión	Software que mantiene constantemente monitoreados los equipos de red y permite visualizar en una interfaz web centralizada.
5	Notificaciones	Son representaciones de informes acerca del rendimiento de cada uno de los recursos de los dispositivos de red monitoreados
6	Autorización	Se refiere a los permisos que posee el administrador de la red para ingresar al software de gestión.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.5
	PROCEDIMIENTO:	GESTIÓN DE SEGURIDAD	VERSIÓN:	1.0

4. Diagrama de Flujo



	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA		PROCEDIMIENTO CONTROL DE DOCUMENTOS TIC	
	SUB PROCESO:	HARDWARE Y COMUNICACIONES	CÓDIGO:	PRO-1.0.5
	PROCEDIMIENTO:	GESTIÓN DE SEGURIDAD	VERSIÓN:	1.0

5. Desarrollo de Actividades

Nro.	Actividad	Descripción	Responsable
1	Acceso al software de gestión	Al servidor pueden ingresar con el mismo usuario y contraseña los responsables que se puntualizan los cuales tienen los permisos necesarios para poder realizar cualquier cambio o modificación al software de gestión.	Jefe de área de Hardware y Comunicaciones Administrador de la red
		Los usuarios que no tengan acceso al software de gestión solamente podrán observar la interfaz web de Nagios.	
2	Acceso a los dispositivos gestionados	Solamente pueden acceder los administradores de la red con previa autorización de usuario y contraseña mediante acceso remoto o local.	Jefe de área de Hardware y Comunicaciones Administrador de la red
3	Envío de notificaciones	Nagios únicamente enviará notificaciones de alertas críticas a los administradores de la red los mismos que estarán previamente configurados. Las notificaciones se realizaran por medio de email o SMS.	Jefe de área de Hardware y Comunicaciones Administrador de la red

CAPÍTULO V

6. Conclusiones y Recomendaciones

6.1. Conclusiones

La implementación de un modelo de gestión basado en el estándar ISO, es fundamental y necesario en una red local de datos gubernamental como la del GAD-Ibarra, debido a la alta disponibilidad de equipos de red que maneja para proveer mayor conectividad tanto a las dependencias internas como externas y el deber que tiene la entidad de brindar un servicio de calidad a la ciudadanía.

Mediante el estudio del modelo de gestión de red funcional se logró establecer la interacción de las cinco áreas de gestión como son; configuración, fallos, contabilidad, rendimiento y seguridad, con las necesidades que tiene la entidad donde se determinó los criterios de implementación.

Con la realización del análisis del estado actual de la red de la entidad se logró identificar las áreas críticas, a través de un modelo jerárquico determinado por capas; core, distribución y acceso además se logró determinar los dispositivos de red críticos que soportan la habilitación del protocolo SNMP a través de inventarios, mapa topológico, características técnicas, medición del consumo de datos enviados y recibidos, mediante el software de monitoreo Ntop para comprobar los servicios que cursan por la red a través de los servidores físicos y virtuales activos.

Mediante la descripción de políticas de gestión de las cinco áreas funcionales del modelo de gestión, se determinó los lineamientos que ayudan a mejorar el

funcionamiento y disponibilidad de los dispositivos que forman parte de la red de la entidad.

A través de la guía que ofrece el estándar IEEE 830 se determinó como mejor opción de software de gestión a Nagios, herramienta que proporciona soluciones en cuanto al manejo óptimo de los recursos de la red, permitiendo al administrador visualizar información en tiempo real en una interfaz web centralizada y de fácil adaptación.

Las incidencias en los dispositivos de la red pueden ser perjudiciales para la entidad por lo que Nagios permite al administrador identificar un fallo mediante la jerarquía de alertas fáciles de reconocer, además los dispositivos de mayor criticidad poseen una identificación de fallos extra, como son el envío de notificaciones de un correo electrónico o un mensaje de texto al teléfono móvil, durante las 24 horas del día los 7 días de la semana, sobre cualquier eventualidad programada y pueda responder inmediatamente a solucionar el problema reduciendo el impacto de indisponibilidad de la red.

El comportamiento de Nagios dentro de la red local de datos de la entidad no afecta el rendimiento de envío y recepción de la información, como se consiguió demostrar a través de los datos obtenidos con el software de monitoreo Ntop donde se verificó que Nagios no genera tormentas de tráfico broadcast y mediante el software Wireshark se verificó que el tráfico UDP generado por el protocolo SNMP no supera el porcentaje normal consumido antes y después de la implementación del modelo de gestión.

A través de la implementación del software de gestión Nagios se logró elaborar los manuales de procedimientos en base a las áreas funcionales del modelo de gestión, que sirven como guía para que los administradores de la red puedan utilizar estos procesos en futuros dispositivos gestionados y de esta forma la red de la entidad este constantemente actualizada y monitoreada garantizando la disponibilidad de funcionamiento de sus recursos.

6.2. Recomendaciones

En la actualidad los departamentos de TIC de entidades gubernamentales buscan mantener una red eficaz y rápida, independientemente de su tamaño, por lo que se recomienda la implementación de un software de gestión que interactúe conjuntamente con un modelo de gestión de red funcional, para que el administrador pueda obtener información del rendimiento de los recursos de la red, logrando los resultados deseados, y lo más fundamental e importante reducir pérdidas económicas.

En el análisis realizado del estado actual de la red se recomienda, que para mantener la disponibilidad de los dispositivos de la red se debe considerar la adquisición de un switch adicional, para tener un respaldo de toda la información que circula por los mismos y mantener activa la red del GAD-Ibarra.

Es recomendable que los cambios de configuración se guarden automáticamente en una base de datos mas sofisticada a la actualmente utilizada. Además mantener una documentación necesaria de la topología en forma organizada de todos los dispositivos de red, que sirva de referencia para evitar que se produzcan cuellos de botella en las interfaces de switches con una nueva instalación de los mismos.

Se recomienda a las personas que intervienen en la administración de la red, manejar las respectivas políticas y manuales de procedimientos que integran el modelo de gestión, el que fue adaptado para mejorar al rendimiento de los recursos de la red.

Para cambiar la definición de valores de plantillas, contactos de grupos, tiempo, es recomendable tomar en cuenta el correcto funcionamiento que debe mantener Nagios para evitar sobrecargar el servidor y la red, con envío de notificaciones innecesarias de correo electrónico y SMS. El software de gestión actualmente se encuentra en la versión 4.0.4, pero está expuesto a actualizaciones de cambio de versión por lo que es recomendable que el administrador tome las medidas necesarias de pruebas previas antes de cambiar a una nueva versión.

Dentro de la implementación se utilizó un teléfono móvil adaptado a Nagios para comprobar el envío de notificaciones de mensajes de texto, es recomendable cambiarlo por un módem GSM que cumpla las mismas funcionalidades de envío, además el administrador deberá ingresar un plan de mensajes al número asignado, aproximadamente cada tres meses caso contrario Nagios no podrá notificar mediante mensajes de texto.

Para evitar el envío masivo de SMS es recomendable configurar correctamente el intervalo de notificaciones, al software de gestión Nagios, actualmente se encuentra configurado para que envíe tres notificaciones cuando se presenten fallos en el horario 24 horas del día, los siete días de la semana.

Debido a un problema suscitado en la red, en el transcurso de implementación del proyecto, recomiendo que la Universidad Técnica del Norte, plantee de alguna manera un respaldo de apoyo al estudiante; como permitir que realice un sondeo del problema presentado en la entidad, para poder ayudar a resolver el inconveniente y continuar con el desarrollo y culminación del proyecto.

Referencias:

- Abeck, S. B. (2009). *Network Management - Know It All*. Estados Unidos: Elsevier.
- Acuña García, E. S., & Caicedo Urresta, V. M. (2005). *GESTIÓN DE REDES DE UN CENTRO DE COMPUTO UTILIZANDO PROTOCOLO SNMP/RMON*. Ambato: Universidad Técnica De Ambato.
- Alarcón Ávila, R. (2007). *Gestión y Administración de Redes como Eje Temático de Investigación*. Bogotá: Universida Libre.
- Artica Soluciones Tecnológicas. (2012). *The monitoring wiki Pandora FMS*. Retrieved from http://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Instalacion
- Aymara Quinga, M. R., & Chancúsig Chicaiza, J. C. (2013). *Análisis E Implementación De Herramientas De Software Libre Para La Seguridad Y Monitoreo De La Red De La Universidad Técnica De Cotopaxi, Ubicada En El Barrio El Ejido, Cantón Latacunga En El Año 2012*. Latacunga: Universidad Técnica de Cotopaxi.
- Barba Martí, A. (1999). *Gestión de Red*. Barcelona: UPC.
- Barrios, J. (2014). *Configuración De Servidores Con GNU/Linux*. Mexico.
- Bastidas F, D. A., & Ushiña G, D. S. (2010). *Estudio para la Implementación de un Centro NOC (Network Operations Center), en la Intranet de PETROPRODUCCIÓN Y REALIZACION DE UN PROYECTO PILOTO PARA LA MATRIZ QUITO*. Quito: Escuela Politécnica Nacional.
- Castañeda Villarreal, F. V. (2011). *Diseño E Implementación De Un Sistema Multiplataforma De Monitorización Y Administración De Red, Con Interfaz Web Para El Usuario Y Utilizando El Portocolo SNMPv3*. Quito: Escuela Politécnica Nacional.
- Cevallos Michilena, M. A. (2013). *Metodología de seguridad informática con base en la norma iso 27002 y en herramientas de prevención de intrusos para la red administrativa del Gobierno Autónomo Descentralizado de San Miguel de Ibarra*. Ibarra: Univesidad Técnica del Norte.
- Chandra Verma, D. (2009). *Principles of Computer Systems and Network Management*. New York: Springer.
- Clemm, A. P. (2007). *Network Management Fundamentals*. Indianapolis, USA: Cisco Press.
- Comité Consultivo Internacional Telegráfico y Telefónico (CCITT-UIT). (1992, 09 10). *ITU-T Recommendations*. Retrieved from ITU-T Recommendations: <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=3051>
- Culqui Medina, A. N. (2013). *Diseño De Un Sistema De Telefonía Ip Basado En Software Libre E Integración Con La Red De Datos; Como Alternativa De Comunicación De Voz Sobre El Protocolo Ip Entre Dependencias Del Gobierno Autónomo Descentralizado Municipal De San Miguel De Ibarra*. Ibarra: Univerisdad Técnica del Norte.

- Ding, J. (2010). *Advances in Network Management*. United States of America: Auerbach Publications Taylor & Francis Group.
- Douglas, M., & Schmidt, K. (2005). *Essential SNMP*. EEUU: O'Reilly.
- Escobar Vallejo, C. V. (2012). Riobamba: Escuela Superior Politécnica de Chimborazo.
- GAD-Ibarra. (21 de Marzo de 2011). *alcaldia Ibarra*. Obtenido de <http://www.ibarra.gob.ec/>
- GAD-Ibarra. (2013). *Inventario de dependencias*. Ibarra: Gobierno Autónomo Descentralizado de San Miguel de Ibarra.
- GAD-Ibarra. (21 de Marzo de 2014). *alcaldia Ibarra*. Obtenido de <http://www.ibarra.gob.ec/>
- Gualotuña Amagua, J. C., & Cando Cofre, E. J. (2010). *Desarrollo e Implementación De Un Prototipo En GNU/Linux, Para Enviar Automáticamente Información Y Notificar Al Administrador A Través De Correo Electrónico Y Sms El Estado Crítico De Los Servicios De Red, Ups Y Logs De La Empresa Acería Del Ecuador C.A.* Quito: Escuela Politécnica Nacional.
- Guerrero Pantoja, C. D. (2011). *Evaluación de Sistemas de Gestión de Redes Bajo Software Libre de la Administración Zonal Norte "EUGENIO ESPEJO"*. Quito: Universidad Politécnica Salesiana.
- Hernández Escobar, J. (2006). *Administración de redes bajo el entorno de Windows XP*. México: Universidad Autónoma del Estado de Hidalgo.
- Hidalgo Crespo, J. C., & Vergara Cueva, A. (2013). *Diseño e Implementación De Un Software De Gestión De Red Con Interfaz Gráfica, Aplicado A La Intranet Del Municipio De Quito "Zona Eloy Alfaro"*. Quito: Escuela Politécnica Nacional.
- Huidobro Moya, J. M. (2012). *COMUNICACIONES MÓVILES. SISTEMAS GSM, UMTS Y LTE*. Mexico: RA-MA.
- ISO / IEC . (1989, 11 15). *ISO / IEC 7498-4:1989*. Retrieved from ISO / IEC 7498-4:1989: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=14258
- Jorquera, D. M. (2010). *Difusión Masiva de Información en los Modelos de Gestión de Redes*. Alicante: Universidad de Alicante.
- Kocjan, W. (2008). *Learning NAGIOS 3.0*. Birmingham: Packt Publishing.
- Microsoft. (2005, Octubre 25). *Microsoft TechNet*. Retrieved from [http://technet.microsoft.com/es-es/library/bb124583\(v=exchg.65\).aspx](http://technet.microsoft.com/es-es/library/bb124583(v=exchg.65).aspx)
- Microsoft. (2011, Mayo 12). *Microsoft TechNet*. Retrieved from [http://technet.microsoft.com/es-es/library/cc850692\(v=office.14\).aspx](http://technet.microsoft.com/es-es/library/cc850692(v=office.14).aspx)
- Mikalsen, A. &. (2002). *Local Area Network Management, Desing and Security*. England: Wiley.

- Molero, L., Villaruel, M., Aguirre, E., & Martínez, A. (2010). *Planificación y Gestión de Red*. Maracibo: Universidad “Dr. Rafael Bellosó Chacín”.
- Molina, F. J. (2010). *Planificación y Administración de Redes*. España: RA-MA.
- Monferrer Agút, R. (2014, 09 09). *Especificación de Requisitos según el estándar de IEEE 830*. Retrieved from Especificación de Requisitos según el estándar de IEEE 830: <https://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf>
- Montes, A. M., & León de Mora, C. (2002). *GESTIÓN DE REDES*. Sevilla.
- Morris, S. B. (2003). *Network Management, MIBs and MPLS*. Canada: Prentice Hall PTR.
- Nagios Enterprises. (2014, Marzo 05). *Nagios Core Documentación*. Retrieved from <http://www.nagios.org/>
- Olups, R. (2010). *Zabbix 1.8 Network Monitoring*. BIRMINGHAM: Packt Publishing.
- Orozco, P. (2010). *Gestión de Red del boli al SNMP*. CASTELLDEFELS: UPCnet.
- Pandora FMS. (2014, Mayo 13). *Recursos - Informacion General*. Retrieved from Recursos - Informacion General: <http://pandorafms.com/Soporte/resources/es>
- Pandora FMS Enterprise. (2014, Mayo 30). *Análisis de Funcionalidades Pandora FMS v 5.1*. Retrieved from PANDORA FMS Enterprise: http://pandorafms.com/downloads/funcionalidades_DEF_ES.pdf
- Raya González, L., Raya Cabrera, J. L., Santos González, M., & Martinez Ruiz, M. Á. (2010). *Guía de Campo Máquinas Virtuales*. Mexico D.F.: Alfaomega-RaMa.
- Rea Lozada, R. A. (2012). *“NORMAS DE CONTROL INTERNO EMITIDAS POR LA CONTRALORÍA GENERAL DEL ESTADO, APLICADAS A LA DIRECCIÓN DE TECNOLOGÍAS*. Ibarra: Universidad Técnica del Norte.
- Romero, M. C. (2014, Octubre 17). *Sistemas Avanzados de Comunicaciones - Gestión de Redes*. Retrieved from Sistemas Avanzados de Comunicaciones - Gestión de Redes: <http://www.dte.us.es/personal/mcromero/docs/sac/sac-gestionderedes.pdf>
- Rosero Vinuesa, V. A. (2012). *Estudio de tecnologías informáticas para asegurar la continuidad de servicios de sistemas computacionales mediante virtualización*. Ibarra: Universidad Técnica del Norte.
- Solís Álvarez, C. J. (2014). *Implementación de NOC para el monitoreo de Servicios e Infraestructura de Redes para el Banco de Loja, Basado en Software Libre*. Loja: Univerisdad Técnica Particular de Loja.
- Tanenbaum, A. S. (2003). *Redes de computadoras*. México: Prentice Hall.
- Tom, R. (2013). *Nagios Core Administration*. BIRMINGHAM : Packt Publishing.
- Unidad de Hardware y Comunicaciones. (2013). *Inventario de TIC*. Ibarra: Gobierno Autónomo Descentralizado de San Miguel de Ibarra.

- Unitel. (24 de Marzo de 2014). *Unitel, Telecomunicaciones*. Obtenido de Normas sobre Cableado Estructurado: <http://www.unitel-tc.com/normas-sobre-cableado-estructurado>
- Urban, T. (2011). *Cacti 0.8 Learn Cacti and desing a robust Network Operations Center* . BIRMINGHAM: Packt Publishing.
- Velasquez Hernandez, J. E. (2009). *Administracion De Redes Utilizando Protocolo Snmp (SIMPLE NETWORK MANAGEMENT PROTOCOL)*. Medellin: Universidad Nacional De Colombia.
- Zabbix. (2014, Junio 20). *Descripción del Producto*. Retrieved from <http://www.zabbix.com/>
- Zabbix SIA. (2008, 11 04). *Zabbix Manual v1.6*. Retrieved from Zabbix Manual v1.6: <http://www.zabbix.com/downloads/ZABBIX%20Manual%20v1.6.pdf>

Anexo A: Parámetros respecto al envío de SMS

A1. Parámetros del envío de SMS a través de internet

Como se mencionó en la solución de envío de SMS a través de internet existen varias páginas Web que brindan el servicio de envío de SMS, dentro de las que existen cabe recalcar la página DescomSMS de España, es una de las páginas que se adaptan directamente con Nagios. En la Tabla A.1 se muestra el costo por créditos de mensajes:

Tabla A.1. Costo de Créditos

Créditos	euros/crédito
Hasta 500	0,115
De 501 a 1.500	0,095
De 1.501 a 5.000	0,080
De 5.001 a 10.000	0,075
Más de 10.000	0,070

Fuente: Datos extraídos de la empresa DescomSMS

A continuación en la Figura A.1 se presenta la solicitud de contratación del servicio de mensajes escritos donde el costo mínimo por 150 créditos es de 20,87 euros transformados a dólares son 22,53 aproximadamente, agregando el costo adicional de 45 dólares por envío de la transacción desde Ecuador a España, el costo es bastante elevado siendo una desventaja para ser utilizado en la implementación.

Otra de las desventajas de este servicio es que no garantiza que los mensajes lleguen al destinatario, el retardo de ayuda es considerable tomando en cuenta que la comunidad de soporte técnico de la página web es de otro país.

DescomSMS

Ref. de compra:
Ref. 72396:
72396

- Usuario: **vivianaeli**
- Saldo: **150 créditos**
- Importe total: **20.87€**

De acuerdo con tu solicitud, te indicamos a continuación los datos para completar la compra de saldo por transferencia:

Importe total: **20.87€**

Núm. de cuenta: ES03 0182 4453 0602 0153 3499 **BBVA**
ES74 0049 4514 1525 9000 9104 **Banco Santander**
ES71 2100 4453 8802 0012 6516 **Caixabank**

Titular: **Desarrollos de Sistemas de Comunicaciones SL**
CIF: B80438088
c/ Guadalest 21 - 03530 La Nucia, Alicante

Concepto: **Ref. 72396**
IMPORTANTE, recuerda indicar este concepto al realizar el pago.

Al recibir la notificación de pago, la recarga de saldo quedará completada.

Un cordial saludo,

El equipo de Descom SMS
descomsms@descom.es
www.descomsms.com

Descom .es
www.descom.es
Tel.: 965.861.024
[Facebook](#)

Descom SMS - Acceso a web para enviar mensajes a móviles - Comenzar sesión

Figura A.1. Solicitud de contratación de mensajes escritos

Fuente: Captura propia extraída de solicitud

A2. Parámetros del envío de SMS mediante un celular conectado al servidor

Uno de los parámetros a tomar en cuenta en esta solución es que el celular debe ser de preferencia Nokia de las marcas que se muestra a continuación; Nokia N95, Nokia N96, Nokia N73, Nokia E63, Nokia 6131, Nokia 6300, Nokia 5630, Nokia 5200, Nokia C1-01, entre otras.

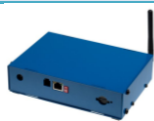

Porque cuentan con una aplicación llamada *Nokia PC Suite* que permite una conexión como uso de módem GSM, parámetro fundamental para establecer la conexión con el servidor.



Una de las desventajas de esta solución es que el celular tiene un tiempo de vida útil menor que un módem GSM que es utilizado precisamente para trabajar en entornos de infraestructura de redes de datos. Sin embargo es una buena opción para la implementación porque es de bajo costo y se puede demostrar que funciona para los fines deseados conjuntamente con el servidor.

A3. Parámetros del envío de SMS a través de un módem GSM conectado al servidor.

La desventaja más relevante de esta solución es el costo del equipo porque el precio rodea desde los 200 dólares hasta los 1000 dólares, presupuesto que una entidad de carácter público no puede solventar. En la Tabla A.2 se describen los precios:

Tabla A.2. Características de Módem GSM

Dispositivo/Módem	Características	Precio
 HWg-SMS-GW	<ul style="list-style-type: none"> - Plugins de Nagios - Interface RJ45 (10BASE-T) – 10 Mbps o 10/100 Mbps - Soporte de protocolos como UDP/IP (SNMP), IP, ARP, HTTP - Interface Quad-Band 850/900/1800/1900 MHz - Dimensiones – 182 x 44 x 125 [mm]/500g 	900,39 \$
 SMSEagle	<ul style="list-style-type: none"> - Plugins para Nagios, Icinga, PRTG, Zabbix, Zenoss. - Tipo de Procesador: ARM9 de 32 bits RISC 200MIPS - Sistema operativo: Linux 2.6 - Interfaz de red: Ethernet 10/100 TX - Dimensiones: (Ancho x Profundidad x Altura) 35 x 120 x 101 mm, Peso: 350 g - Módem GSM / GPRS: - Waveband: GSM / GPRS / EGPRS 900/1800/1900 MHz - Velocidad de transmisión entrante: hasta 30 SMS / min - Velocidad de transmisión de salida: hasta 20 SMS / min - API enviar SMS solicitudes: 30 SMS / min (mensajes se ponen en cola para enviar en una base de datos) - Integrado servidor Web Apache2 construido en el 	820 \$

servidor de base de datos PostgreSQL		
 iTegno W3800U	<ul style="list-style-type: none"> - El 38XX módem GPRS iTegno está diseñado para uso corporativo e industrial. Apoyo a redes GSM / GPRS - iTegno 38XX ofrece conectividad de datos inalámbricos para los profesionales móviles y se puede implementar en diversas aplicaciones de máquina a máquina (M2M). - El 38XX módem iTegno es compatible con Windows 98 SE / ME / 2000 / XP y Vista. Drivers para Linux y Macintosh OS (OS 10.2,10.3 y 10.4) también están disponibles para fines de desarrollo. - Tamaño pequeño: 94.2 x 66.0 x 14.5 mm Peso: 58 gramos - Quad-banda (GSM850 / EGSM900 / DCS1800 / PCS1900) 	300 \$
 Cinterion MC55iT	<ul style="list-style-type: none"> - Cinterion MC55iT es un módem GSM cuatribanda (850/900/1800/1900 MHz) con soporte GPRS clase 10., desarrollado sobre el potente y estable modulo MC55i. - Se añade potencia de su stack TCP-IP. - Disponen de todos los elementos para su inmediata integración: Interface PortaSIM, puerto RS232, rango extendido alimentación y conector antena tipo FME. Listo para usar en aplicaciones M2M usando red GSM en telemetría, control y mantenimiento remoto, seguridad, sistemas de tráfico, transporte, y un largo etcetera. - Dispone de drivers para Windows7, XP y Vista. - Quad-Band GSM 850/900/1800/1900 MHz (MC55iT) 	200 \$

Fuente: Elaboración propia basada en características técnicas de cada equipo GSM

A4. Porque se implementa el proyecto sobre 3G y no sobre 4G LTE

Para la implementación del proyecto se utiliza la tecnología 3G porque solo necesita el servicio de mensajes cortos debido a que el servidor solo envía texto cuando sucede una alerta por lo que es suficiente la velocidad de transmisión con la que envía, además no es necesario la tecnología 4G (HSPA, WiMAX y LTE) porque estas se utilizan para otro servicios adicionales como descarga de juegos, videostreaming, entre otros y por ende son considerablemente más rápidas, parámetro no requerido por Nagios.

Anexo B: Especificaciones Técnicas del Data Center del GAD-Ibarra

B.1. Especificaciones técnicas:

De acuerdo a los pliegos establecidos en compras públicas, la adquisición del Data Center consta de los siguientes puntos:

B.1.1 Descripción General

El contratista suministrará todos los materiales y equipos que se requieren en el Data Center (Centro de datos) para hacerlo operativo, de conformidad con el diseño previamente aprobado y demás documentos contractuales. Se implementará lo siguiente:

❖ Piso falso

- Debe cumplir con las normas OSHA y NFPA 75, 75-6.
- Malla con norma TIA/EIA 942.
- Instalacion de malla bajo el piso elevado, incluir barras colectoras de tierra, conexión a la línea de tierra del edificio.
- El cableado eléctrico y cableado de red en el Data Center debe quedar por debajo del piso falso, a través de escalerillas por separado.
- Periodo de garantía 3 años.

❖ Equipo de aire acondicionado de precisión

- La unidad ofertada, es un aire acondicionado de precisión de tipo split, con capacidad para enfriar, calentar, humidificar y deshumidificar respectivamente.
- La unidad esta diseñada para descarga y retorno de aire frontal.
- La unidad operará con refrigerante ecológico R407 C, para cumplir con las normativas internacionales ecológicas.
- Capacidad total del enfriamiento: 32100 Btu/h
- Capacidad sensible de enfriamiento: 27000 Btu/h

- Capacidad movimiento de aire 1320 CFM, con cambio manual de velocidad desde el display de control.
- La unidad opera con un tipo de compresor tipo scroll, hermético, con protección interna de sobre temperatura, montaje sobre soportes para aislamiento de vibración. switch de alta y calentador tubular para carter. Control de capacidad por medio hot gas Bypass.
- Sistema de humidificación tipo Canister.

❖ **Control de Acceso**

- El sistema de control permite el auto drenaje o renovación de agua automatico, para una correcta eficiencia del sistema.
- Diseño del sistema con tecnología de punta.
- El sistema de control cuenta con un display, separado de la unidad que permite visualizar el status de operación y alarmas.
- El display digital, permite el registro y configuración de parámetros de operación de temperatura y humedad.
- Los parámetros de operación son configurados por el usuario de acuerdo al requerimiento de control ambiental.
- Configuración de parámetros de operación y sensibilidad para temperatura, humedad y alarmas de operación.
- El display permite la visualización de todas las alarmas activas de operación.

❖ **Puertas de Seguridad**

- El recubrimiento contra fuego, deberá al menos constar de 2 planchas de material termo-aislante de 8mm. Pegadas a las planchas de acero en el interior de la puerta; además lana de vidrio de 25mm resistente a 1000 grados F.
- El plegado de batiente deberá estar diseñado para evitar el paso del humo y llamas, entre la hoja y el cerco, utilizar un empaque de Polipropileno cuya composición química ha sido diseñada para efectos de temperatura y humo.
- Conectividad al sistema de control de acceso.
- Cierre hermético al contacto con la puerta.
- Barra antipánico.

❖ Monitoreo de Alarmas

- Sistema de monitoreo modular que incluya vigilancia de parámetros ambientales, contactos secos, entradas universales.
- Alarma de puerta abierta del data center.
- Alerta visual mediante luces estroboscópica de presencia de alarma.
- Almacenamiento de datos.
- Comunicaciones IP/SNMP, en red.
- El dispositivo de control debe enviar mensajes via correo electrónico.
- Capacidad de envío de mensajes a celular (GSM).

❖ Cielo Falso

- El trabajo debe comprender cambio total de los paneles del techo falso tipo amstrong con retardante de fuego.

❖ Red eléctrica de Distribucion de Energia

- Tablero eléctrico de distribución, incluye: breaker principal, breakers para equipos ups. Carga estimada máxima de acuerdo al aire acondicionado ofertados, y a 18 KVA de los UPS.
- Se debe incluir todos los módulos, protector de transientes y componentes adicionales requeridos para el correcto funcionamiento eléctrico del centro de datos.
- Se debe construir el circuito controlado por breakers para el sistema de iluminación. Control de acceso, sistema de control de incendios, UPS y aire acondicionado.

❖ Sistema de energía de respaldo (existente)

- Se instalará y configurará módulos de batería cien por ciento compatible con UPS Powerware Eaton 9170 + UPS especificaciones para 3 KVA de energías adicionales.
- Modulo de baterías.
- Modelo: ASY – 0529
- Characteristics: para 6kva de soporte.

❖ Sistema de control y extinción automática de incendios

- El sistema debe proveer la detección y extinción automática de incendios.
- Elementos de detección y alarma: consola de control, monitoreo y detección de alarma, con baterías, sirena y luz estroboscopia de alarma,

estación de aborto, estación de disparo de detectores de ionización y fotoeléctricos para configuración cruzadas.

- Tipo agente gas ecológico FM-200 o similar.
- Señalización con rótulos visibles.
- Cumplimiento de las dos certificaciones FM y UL cumplir las normas NFPA.

B.1.1.1 Diseño de Distribución del Data Center.

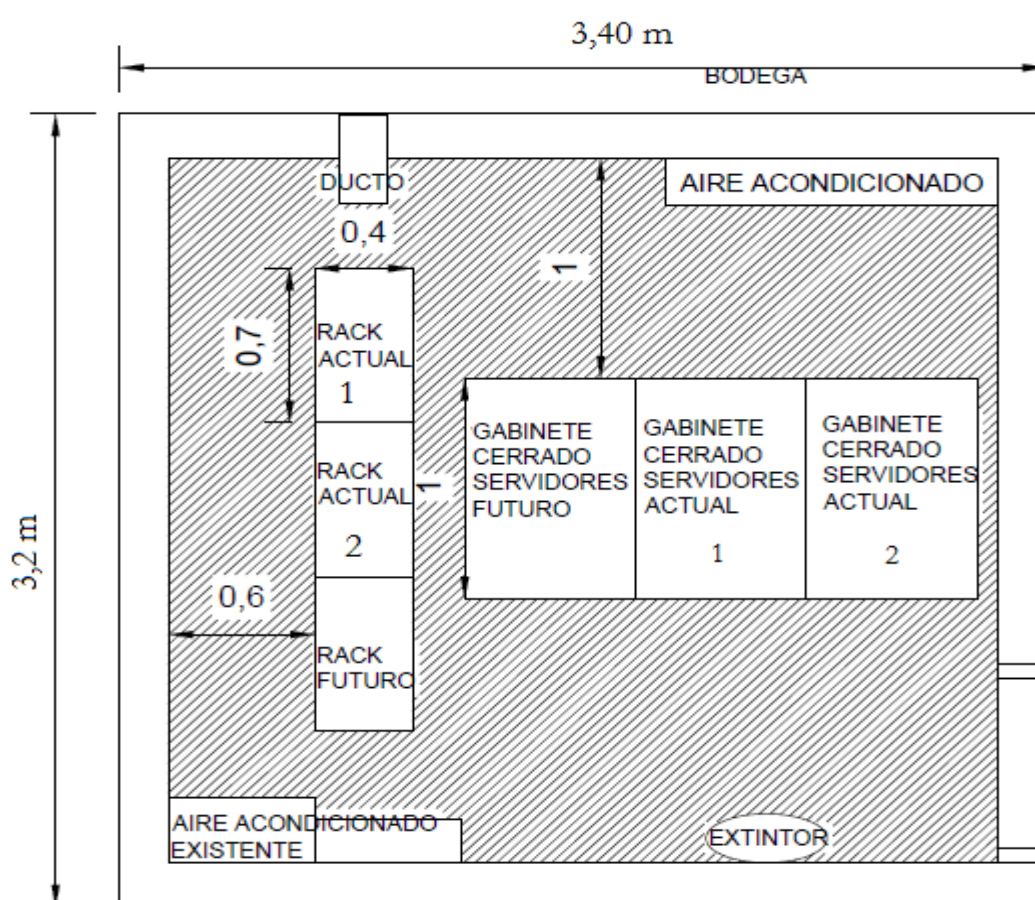


Figura B 1. Diseño de distribución del Data Center

Referencia: CÓDIGO DEL PROCESO: SIE –IMI -31 -2010, Objeto de Contratación: PROVISIÓN E IMPLEMENTACIÓN DEL DATACENTER DEL ILUSTRE MUNICIPIO DE IBARRA.

B.2. Especificaciones técnicas de switches del Data Center:

En esta sección están descritas las características técnicas de los switches instalados en el Data Center.

❖ Switch CISCO CATALYST 4503-E

En la Tabla B 1 se puntualiza brevemente las características técnicas del dispositivo de red que se indica en la Figura B 2:



Figura B 2. Switch Catalyst serie 4503-E

Fuente: Recuperado de <http://www.cisco.com/>

Tabla B 1: Características técnicas Switch Catalyst serie 4503-E

CARACTERÍSTICAS	
Conexión GAD-I	Switch núcleo que permite la conexión entre dependencias externas e internas mediante fibra óptica y utp.
Tipo de dispositivo	- Conmutador Capas 2, 3 y 4
Dimensiones y las unidades de rack (RU)	- Alto 12.25 x 17.31 x ancho 12.50 in (31.12 x 43.97 x 31.70 cm) fondo - 7 RU
Chasis	Tres ranuras horizontales. Las ranuras están numeradas del 1 (superior) a 3 (abajo).
Módulos	Soporta hasta dos módulos de la serie Catalyst 4500.
Backplane	48 Gbps full duplex por ranura (96 Gbps)
Bandeja de ventilador	- El chasis soporta una bandeja de ventilador intercambiable en caliente. - La bandeja de ventilación contiene seis ventiladores individuales. - Los ventiladores individuales no son sustituibles en el campo; debe reemplazar la bandeja del ventilador en caso de un fallo del ventilador.
Fuente de alimentación	Soporta una o dos fuentes de alimentación
Memoria	- RAM: 256MB - FLASH: 32MB
Procesador	- CPU: 266 MHz
Puertos	- 48 Gigabit Ethernet 10/100/1000 Mbps - 8 puertos SPF 1000BASE-T
Descripción de capas	- Encapsulación IEEE 802.1Q VLAN, 802.1s, 802.1w, 802.3ad, 802.1x, entre otros.

- 2.048 VLANs activas y 4.096 IDs de VLAN por switch
- (CoS) para tráfico, direccionamiento IP estático
- Protocolo de información de enrutamiento (RIP) y RIP2
- Soporta Ipv6, ICMP, QoS, ACL, SNMP 1, SNMP 2, SNMP 3.

Fuente: Adaptado de datasheets de los equipos

❖ Switch 3COM 4500 G

En la Tabla B 2 se puntualiza brevemente las características técnicas del dispositivo de red que se indica en la Figura B 3:



Figura B 3. Switch 3COM 4500G

Fuente: Recuperado de

http://www.scts.co.th/catalog/product_info.php?products_id=1707&language=en

Tabla B 2: Características técnicas Switch 3COM 4500G

CARACTERÍSTICAS	
Conexión GAD-I	Utilizado para interconectar los servidores del Data Center.
Tipo de dispositivo	- Conmutador Capas 2, 3
Dimensiones	- Alto: 43,6 mm; ancho: 440 mm, fondo: 450 mm
Fuente de alimentación	Soporta múltiples modos de alimentación: sólo AC, AC y DC, y sólo DC
Memoria	- FLASH: 128MB
Procesador	- CPU : 264MHz
Puertos	- 24 Gigabit Ethernet 10BASE-T/100BASE-TX/1000BASE-T - 4 puertos de uso dual 10/100/1000 ó SPF
Descripción de capas	- Capa 2: IEEE 802.Q VLANs, 802.3ad, control de flujo 802.3x full-duplex, STP 802.1D, RSTP 802.1w, multicast IGMP v1/v2. - Capa 3: Routing basado en hardware, ECMP, ARP, interfaces virtuales, routing estático/dinámico, RIPv1/v2, OSPF, Soporta QoS.
Administración	- Se realiza a través de 3Com Network Supervisor, 3Com Network Director ó 3Com Enterprise Management Suite. - Otro tipo de administración: CLI mediante consola o Telnet, administración SNMP 1, SNMP 2, SNMP 3, RMON-1 (estadísticas, histórico, alarmas, eventos).

Fuente: Adaptado de datasheets de los equipos

❖ Switch 3COM 5500 SI

En la Tabla B 3 se puntualiza brevemente las características técnicas del dispositivo de red que se indica en la Figura B 4:



Figura B 4. Switch 3COM 5500 SI

Fuente: Recuperado de <http://www.sct-systems.com/catalog/e550048poe-gigabit-port-managed-switches-p-1502.html>

Tabla B 3. Características técnicas Switch 3COM 5500 SI

CARACTERÍSTICAS	
Conexión GAD-I	Utilizado para interconectar los segmentos de red del edificio principal.
Tipo de dispositivo	- Conmutador Capas 2, 3
Dimensiones	- Altura: 43,6 mm; anchura: 440 mm; fondo: 270 mm
Apilado	- Hasta 8 switches mediante puertos Gigabit Ethernet
Modo de comunicación	Half-Full dúplex en todos los puertos
Fuente de alimentación	- Soporta múltiples modos de alimentación: sólo AC, AC y DC, y sólo DC
Memoria	-
Procesador	-
Puertos	- 48 Fast Ethernet - 10/100 Mbps BASE T/TX - 4 Gigabit Ethernet - 1000 Mbps BASE-X SPF
Descripción de capas	- Capa 2: IEEE 802.Q VLANs, 802.3ad, control de flujo 802.3x full-duplex, STP 802.1D, RSTP 802.1w, - Capa 3: Enrutamiento estático/dinámico, RIPv1/v2, OSPF, ARP, interfaces virtuales.
Administración	- 3Com Network Supervisor, 3Com Network Director, 3Com Enterprise Management Suite - Otro tipo de administración: GUI basada en web, SNMP 1, SNMP 2, SNMP 3, Telnet, CLI, RMON-1 (estadísticas, histórico, alarmas, eventos).

Fuente: Adaptado de datasheets de los equipos

❖ Switch 3COM 4500

En la Tabla B 4 se puntualiza brevemente las características técnicas del dispositivo de red que se indica en la Figura B 5:



Figura B 5. Switch 3COM 4500

Fuente: Recuperado de <http://www.sct-systems.com/catalog/e450048-port-managed-switches-p-1496.html>

Tabla B 4: Características técnicas Switch 3COM 4500

CARACTERÍSTICAS	
Conexión GAD-I	Utilizado para interconectar los segmentos de red del edificio principal.
Tipo de dispositivo	- Conmutador Capas 2, 3
Dimensiones (P x A x L)	- 26.92 x 43.94 x 4.32 cm
Apilado	- Hasta 8 switches mediante puertos Gigabit Ethernet
Modo de comunicación	- El modo duplex en todos los puertos se negocian automáticamente
Memoria	- SDRAM: 64 MB - FLASH: 8 MB
Procesador	-
Puertos	- 48 Fast Ethernet - 10/100 Mbps - 2 Gigabit Ethernet - 1000BASE-T (mediante RJ45), o 1000Base-X "SFP" ³² .
Descripción de capas	- Soporta 802.1x, Clase de Servicio / Calidad de Servicio (CoS/QoS) 802.1p, ACL, VLAN - Enrutamiento dinámico con RIP. - Los switches detectan y ajustan las conexiones de cables cruzados o directos mediante la funcionalidad "Auto MDI/MDIX".
Administración	- A través de 3Com Network Supervisor, 3Com Network Director ó 3Com Enterprise Management Suite - Otro tipo de administración: GUI basada en web, SNMP 1, SNMP 2, SNMP 3, Telnet, CLI, RMON-1 (estadísticas, histórico, alarmas, eventos),

Fuente: Adaptado de datasheets de los equipos

❖ Switch 3COM 4250T

En la Tabla B 5 se puntualiza brevemente las características generales del dispositivo de red que se indica en la Figura B 6:

³² SFP.- Transceptor utilizado para conectar equipos de comunicaciones de datos.



Figura B 6. 3Com SuperStack 3 Switch 4250T

Fuente: Recuperado de <http://apacelli.com/3com-switch-4250t-48-port-plus-2-10-100.jpg>

Tabla B 5: Características técnicas 3Com SuperStack 3 Switch 4250T

CARACTERÍSTICAS	
Conexión GAD-I	Utilizado para interconectar los segmentos de red del edificio principal. Este switch se conecta en cascada con el switch SW3C-RACK1-4250 a través de los puertos Giga.
Dimensiones	Ancho 44 cm x Altura 27.4 cm x Profundidad 4.4 cm
Tipo de dispositivo	Conmutador Capa 2
Modo de comunicación	- Semiduplex, dúplex pleno
Fuente de alimentación	- Integrado
Memoria	-
Procesador	-
Puertos	- 48 Fast Ethernet -10BASE-T/100BASE-TX - 2 Gigabit Ethernet - 10/100/1000 BASE-T
Velocidad de transferencia de datos	- 100Mbps
Descripción de capas	- Control de flujo, conmutador MDI/MDI-X, soporte VLAN , apilable - Cumplimiento de normas IEEE 802.1Q, IEEE 802.1P, IEEE 802.1w. - Administración: configuración basada en web, SNMP 1. O a través de 3Com Network Supervisor, 3Com Network Director, 3Com Enterprise Management Suite.

Fuente: Adaptado de datasheets de los equipos

❖ Switch CISCO CATALYST 2960 (24/48 PUERTOS)

En la Tabla B 6 se puntualiza brevemente las características técnicas del dispositivo de red que se indica en la Figura B 7:



Figura B 7. Switch CISCO CATALYST 2960

Fuente: Recuperado de <http://www.cisco.com/c/products/switches/catalyst-2960-series-switches.html>

Tabla B 6. Características técnicas Switch CISCO CATALYST 2960

CARACTERÍSTICAS	
Conexión	Utilizados para interconectar los segmentos de red del edificio principal.
Tipo de dispositivo	- Conmutador Capa 2
Dimensiones	- Ancho 44.5 cm x Profundidad 23.6 cm x Altura 4.4 cm
Fuente de alimentación	- Fuente de alimentación - interna
Memoria	- RAM: 64 MB - FLASH: 32MB
Procesador	- Single core
Puertos	- Fast Ethernet 24/48 -10/100 Mbps - Gigabit Ethernet: 2- 10/100/1000 Mbps - Puertos auxiliares 2 SFP (mini-GBIC)
Velocidad de transferencia de datos	- 10/100 Mbps
Modo de comunicación	- Full dúplex
Características generales	- Encapsulación IEEE 802.1Q VLAN, IEEE 802.1p, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab - Soporta QoS - Protocolos de gestión: Telnet, RMON 2, RMON 1, SNMP 1, SNMP 3, SNMP 2c, TFTP, SSH - Protocolos de red admitidos: ACL, ARP, DiffServ, IGMP, IP, RADIUS, SSH, TCP, UDP, DHCP, TFTP

Fuente: Adaptado de datasheets de los equipos

Anexo C: Resultados del monitoreo del tráfico de datos.

Dentro de este Anexo esta un ejemplo de los datos obtenidos con el software de monitoreo Ntop, el que ayudó a determinar los servidores activos de la entidad. En la Figura C 1 se presenta los resultados obtenidos del total de datos enviados 66,2 MBytes y recibidos 29,8 MBytes del servidor de Repositorios.

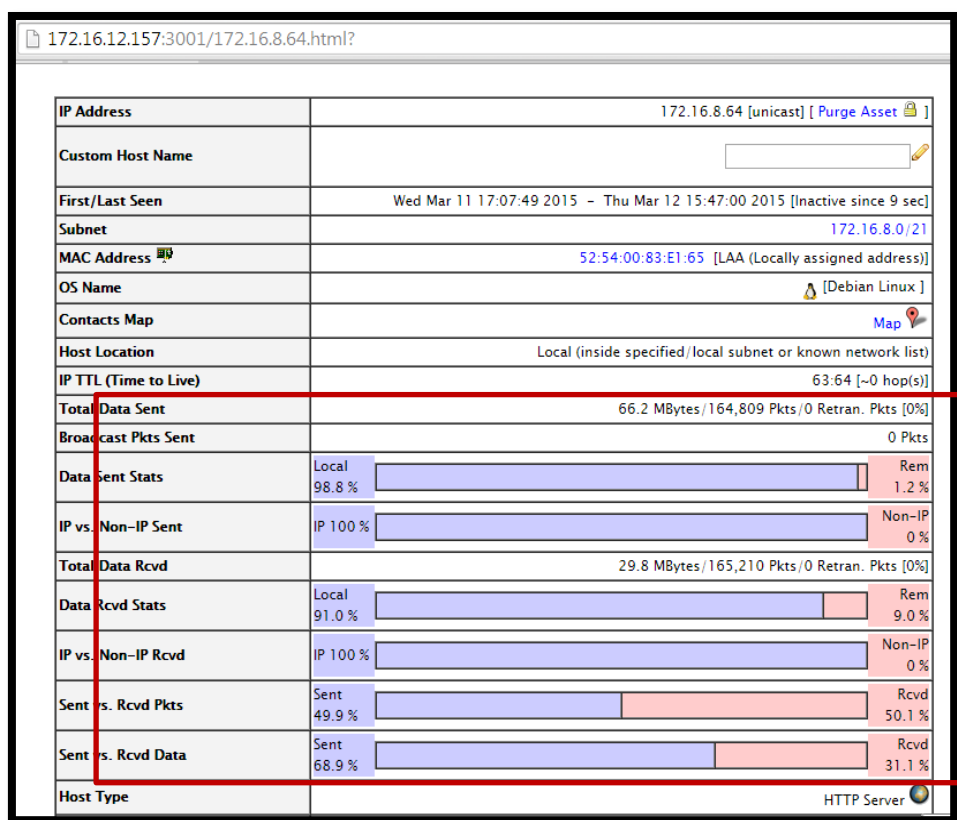


Figura C 1. Datos de Servidor de Repositorios

Fuente: Captura propia de software Ntop

La Figura C 2 muestra los protocolos que más utiliza este servidor: TCP, Mail_POP y HTTP:

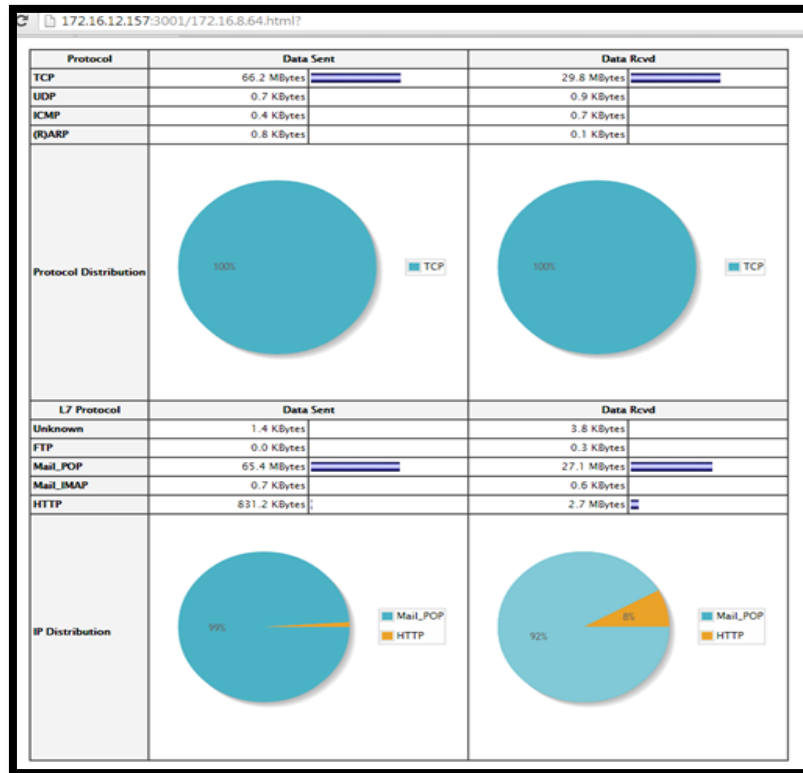


Figura C 2. Datos de Servidor de Repositorios
Fuente: Captura propia de software Ntop

En la Figura C 3 Ntop muestra los puertos utilizados por el servidor de Repositorios:

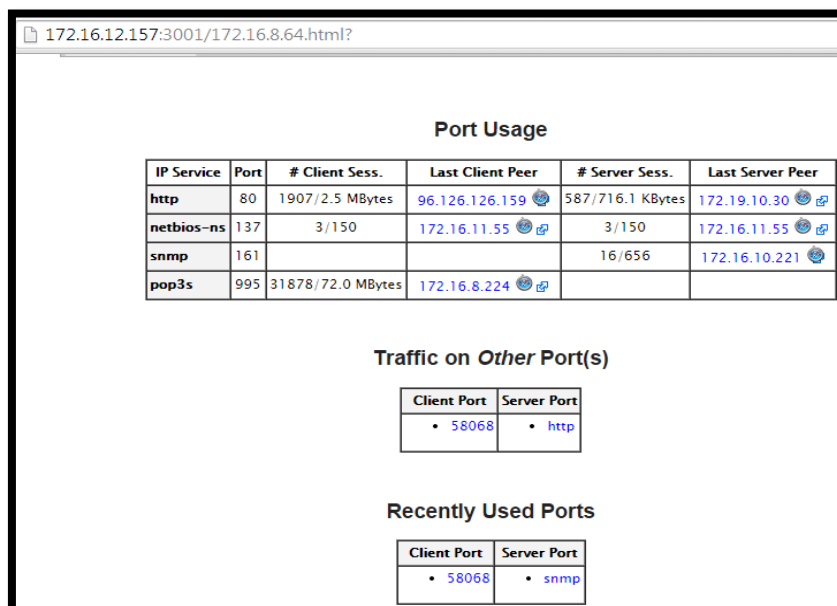


Figura C 2. Datos de Servidor de Repositorios
Fuente: Captura propia de software Ntop

Anexo D: Elección del software de gestión en base al estándar

IEEE 830

D.1. Elección de Software de Gestión.

Este software tiene como objetivo ayudar a los administradores a mantener monitoreados los eventos que se susciten en la red, detectar problemas antes que afecten a los usuarios. Además para el análisis se toma en cuenta los requerimientos de la entidad y entre ellos está el costo de adquisición e implementación el cual debe ser bajo; por tal razón debe poseer una licencia de GNU (General Public License), que es una licencia de Software Libre que asegure actualizaciones y soporte. Por lo tanto en el presente Anexo se describe cada software de gestión a evaluar; se expone las características, funcionalidades, desventajas y requerimientos del sistema.

D.1.1. Pandora FMS



Figura D.1. Logo Pandora FMS

Pandora FMS (Flexible Monitoring System o Sistema de Monitoreo Flexible) es un software de monitorización Open Source para gestión de infraestructura TI desarrollado desde el año 2003 actualmente es dirigido y financiado por Ártica Soluciones Tecnológicas, permite recoger datos de cualquier fuente y medir el estado de cualquier sistema o servicio, (Pandora FMS Enterprise, 2014).

a. Características

- Gestiona todo tipo de dispositivos de red, sistemas operativos, servidores, aplicaciones y sistemas hardware como; bases de datos, cortafuegos, proxies servidores web, VPN, routers, Switches, etc.
- Soporta todos los estándares SNMP.
- Permite establecer alertas sobre umbrales y enviar notificaciones mediante email y SMS.
- Trabaja sobre una base de datos de forma que genera informes, estadísticas, niveles de adecuación de servicio (SLA).

b. Funcionalidades

A continuación se presenta algunas de las funcionalidades de Pandora FMS en su edición OpenSource (Pandora FMS Enterprise, 2014):

Cuenta con:

- Monitorización de rendimiento y disponibilidad
- Gestión de eventos
- Administración por línea de comandos
- Alta disponibilidad
- Consola visual personalizable
- Agentes multiplataforma para Windows, Linux, HP-UX, Solaris, BSD, AIX
- Agentes para Android y sistemas empotrados
- La interfaz de usuario se encuentra en un entorno 100% Web.
- Consola Web ligera para móviles
- Detección de topología de red y autodescubrimiento de nivel 2 y 3
- Soporte IPv6

- Consola SSH/Telnet
- Soporta la monitorización de cualquier dispositivo con protocolo SNMP
- Arquitectura modular y escalar

No cuenta con:

- Gestión centralizada de recursos
- Monitorización de servicios
- Monitorización remota descentralizada de alta capacidad
- Gestión remota de agentes
- Virtualización
- Escalabilidad
- Inventario remotos
- Plugins³³ VMware, Oracle, Websphere
- Personalización de informes

c. Desventajas

- No es recomendable utilizar Pandora FMS en entornos virtualizados, ya que tiene unos requisitos de acceso a disco muy estrictos. En el caso de hacerlo, es imprescindible asignar disco independiente, así como RAM y CPU. En estos entornos es recomendable usar discos SAN (Artica Soluciones Tecnológicas, 2012).
- La versión libre no contiene todos los módulos de monitoreo.

³³ Plugin.- Es una aplicación que añade funcionalidades adicionales en un programa informático, que es ejecutado mediante el software principal, con el que interactúa a través de una determinada interfaz.

- Pandora FMS no es un sistema de tiempo real, es un software de monitorización general de aplicaciones y sistemas en entornos cuya criticidad no sea el tiempo real.

d. Requerimientos del sistema

A continuación se muestran los requerimientos que necesita este software de gestión (Pandora FMS, 2014):

Tabla D 1: Requerimientos para el sistema Pandora FMS

Parámetros	Requerimientos
Tamaño del Hardware	<ul style="list-style-type: none"> • Hasta 500 agentes o 5000 módulos; 4 GB de RAM y un único CPU de 2 GHz. Disco duro rápido 7200 rpm o equivalente. • Hasta 2000 agentes o 10000 módulos: 8 GB de RAM y un cpu doble de 2,5 HGz y un disco duro rápido 7200rpm o más.
Sistemas Operativos	<ul style="list-style-type: none"> ▪ Para el servidor y la consola: SUSE Linux, Debian, Ubuntu o RHEL/CentOS.
Agentes	<ul style="list-style-type: none"> ▪ AIX 5.x, Solaris, HP-UX11.x, Linux, BSD, Windows NT4, 2000, XP, 2003, Vista y 7, Android y dispositivos empotrados.

Fuente: Elaboración propia basada en características de software Pandora FMS

D.1.2. ZABBIX



Figura D.2. Logo Zabbix

Zabbix es un software de monitoreo con gestión centralizada de código abierto con licencia GPL versión 2 diseñado para la máxima disponibilidad y rendimiento de los componentes de una infraestructura de TI. Posee monitoreo en tiempo real, donde

decenas de miles de servidores, máquinas virtuales y dispositivos de red pueden ser monitoreados simultáneamente (Olups, 2010).

a. Características

A continuación se puntualiza las características más relevantes que tiene este software (Zabbix, 2014):

- Interfaz Web centralizada eficaz y flexible fácil de usar.
- Todo dentro de la red se puede controlar: el rendimiento y la disponibilidad de los servidores, aplicaciones web, bases de datos, equipos de red.
- Mejorar la calidad de los servicios y reducir los costos de operación al evitar el tiempo de inactividad.
- Envío de notificaciones vía correo electrónico y/o SMS.
- Posibilidad de supervisar directamente SNMP (v1, 2 y 3).
- Informes SLA en tiempo real.

b. Funcionalidades

- Permite la visualización de resúmenes, mapas, gráficos, pantallas, etc.
- Agentes Multiplataforma para Windows, Linux, AIX, FreeBSD, HP-UX, Solaris.
- Supervisa protocolos como; SSH, HTTP, NTP, SMTP, POP, FTP, IMAP, NNTP entre otros.
- Recolección de datos a través de agentes Zabbix, agentes SNMP, sin agentes
- Scripts personalizados en lenguajes de programación Perl, Python, Ruby

- Permite el monitoreo en entornos virtuales
- Detección de problemas en base a definiciones de umbrales flexibles.
- Detección automática de dispositivos.
- Manejo de plantillas de configuración exportables/importables.
- Autenticación segura de los usuarios, esquema de permisos de usuario y administrador flexible.

c. Desventajas

- Zabbix tiene una configuración compleja.
- La documentación es irregular.
- No cuenta con una comunidad de soporte actualizada.

d. Requerimientos del sistema

Los requisitos de hardware son muy variables dependiendo de la configuración (Zabbix SIA, 2008):

Tabla D 2: Requerimientos para el sistema Zabbix

Parámetros	Requerimientos
Tamaño del Hardware	<ul style="list-style-type: none"> • Pequeña hasta 20 host; 256 MB de RAM, CPU PII 350 MHz y disco duro de 40 GB. • Mediana hasta 500 host; 2 GB de RAM, CPU AMD Athlon 3200 y disco duro de 80 GB. • Grande hasta 1000 host; 4 GB de RAM, CPU Intel Dual Core 6400 y Disco Duro de 100 GB. • Muy Grande hasta 10000; 8 GB de RAM, CPU Intel Xeon 2x y disco duro de 120 GB.
Sistemas Operativos	<ul style="list-style-type: none"> • Zabbix funciona con las siguientes plataformas; SUSE Linux, FreeBSD, Solaris, Open BSD, HP-UX.
Agentes	<ul style="list-style-type: none"> ▪ Windows (2000, 2003, XP, Vista), Linux, Solaris, FreeBSD, AIX.

Fuente: Elaboración propia basada en características de software ZABBIX

D.1.3. CACTI



Figura D.2. Logo Cacti

Cacti es un software de monitorización de código abierto, con la ayuda de RRDtool³⁴ y MySQL almacena toda la información necesaria para brindar una representación gráfica de alto rendimiento, además es totalmente configurable a través de su interfaz web. Se puede tener información en tiempo real de los dispositivos gestionados (routers, switches o servidores, tráfico de interfaces, carga de cpu, temperatura, etc) (Urban, 2011, págs. 1,2).

a. Características

- Para la recolección de datos, Cacti usa scripts y comandos externos, así como las 3 versiones de SNMP.
- Proporciona un esquema rápido de obtención de datos remotos.
- Manejo avanzado de plantillas
- Generación de gráficos en red
- Consola de administración vía web completamente en PHP
- Permite reportar comportamientos vía email y SMS

³⁴RRDtool.- Es un sistema de base de datos que permiten almacenar y representar gráficamente datos en intervalos temporales.

b. Funcionalidades

A continuación se indican algunas funcionalidades que posee Cacti además de ser un software enfocado en la medición del desempeño de una red:

- Alerta mediante el manejo de umbrales
- Monitoreo en tiempo real de fuentes de datos específicos
- Creación y envío de informes programados
- Registro y análisis de sistema
- Realizar copias de seguridad de configuración de red
- Integración de otros software de gestión de red

c. Desventajas

- La configuración de interfaces es tediosa
- Configurar la arquitectura de plugins no es trivial
- Hacer actualizaciones puede ser complejo
- Solamente muestra estadísticas y gráficas de las máquinas.
- No monitorea el uso de memoria, disco o CPU de un servidor

D.1.4. NAGIOS



Figura D.4: Logo Nagios Core

Nagios Core es un software de monitoreo de código abierto, utilizado para comprobar la conectividad entre los hosts y asegurar que los servicios de red estén funcionando correctamente, permite identificar y resolver problemas de una

infraestructura de TI, asegurando que los sistemas, aplicaciones, servicios y procesos estén funcionando adecuadamente, en el caso de un fallo, puede alertar el problema al personal técnico, lo que permite remediar los procesos antes de que afecten a los usuarios finales (Kocjan, 2008).

a. Características

- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Envío de notificaciones personalizadas cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (Vía email, pager, Jabber, SMS).
- Interfaz web para observar el estado de la red actual, notificaciones, historial de problemas, archivos de registros, etc.
- Reportes y estadísticas del estado de disponibilidad de servicios y hosts.
- Monitorización de factores ambientales a través de sondas físicas (temperatura, humedad relativa, luminosidad, líneas de tensión, etc.).
- Arquitectura simple de integración que permita a los usuarios desarrollar fácilmente sus propios agentes de chequeo de servicios y recursos.
- Nagios marca el estándar en la industria de monitoreo a grandes niveles
- Permite controlar la red informática y solucionar problemas antes que los usuarios los detecten.
- Nagios es un sistema estable, escalable, con soporte y extensible.

b. Funcionalidades

- Diseño de Plugins totalmente personalizables para adaptar el sistema acorde a nuestras necesidades.
- Detallado informe gráfico y textual, diario, semanal, mensual, etc., del comportamiento de los sistemas a monitorizarse.
- Uso de su interface web que permite ver información detallada de los estados de los distintos componentes, reconocer problemas de forma rápida.
- Permite reiniciar automáticamente aplicaciones que hayan fallado, servicios y equipos.
- Permite planificar las capacidades de los componentes a través del monitoreo.
- Permite generar reportes de disponibilidad SLA (Service Level Agreements), y reportes históricos de alertas y notificaciones. Además permite ver las tendencias de los informes a través de la integración con Cactus y RRD.
- Múltiples usuarios pueden acceder a la interface web, además cada usuario puede tener una vista única y restringida.
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando herramientas como (Bash, C++, Perl, Ruby, Python, PHP, C#, Java, etc.).

c. Desventajas

- Nagios necesita acceso SSH o un addon (NRPE) para supervisar funcionamiento interno del sistema remoto (archivos abiertos, los procesos en ejecución, la memoria, etc).
- La interfaz web es de sólo lectura.

d. Requerimientos del sistema

En la Tabla D 3 se indica los requerimientos que necesita Nagios:

Tabla D 3: Requerimientos para el software Nagios

Parámetros	Requerimientos
Tamaño del Hardware	<ul style="list-style-type: none"> • Hasta 20 host y 250 servicios; 40 GB disco duro, (1-4) GB de RAM y CPU Cores (1-2). • Hasta 100 host y 500 servicios; 80 GB disco duro, (4-8) GB de RAM y CPU Cores (2-4). • Más de 500 host y 2500 servicios; 120 GB disco duro, (más de 8) GB de RAM y CPU Cores (> 4).
Sistemas Operativos	<ul style="list-style-type: none"> ▪ Cualquier equipo que este ejecutando Linux y con compilador C
Agentes	<ul style="list-style-type: none"> ▪ AIX 5.x, Solaris, HP-UX11.x, Linux, BSD, Windows NT4, 2000, XP, 2003, Vista y 7, Android

Fuente: Elaboración propia basada en características de software Nagios

D.2. Especificación de Requisitos para el Software de Gestión

D.2.1. Introducción.

Este documento de Especificaciones de Requisitos de Software creado por el estándar IEEE 830, es la base del desarrollo técnico del software de gestión a implementarse dentro de una infraestructura virtual en la entidad.

D.2.2. Propósito.

La ERS tiene como propósito brindar todos los requerimientos, funcionalidades y restricciones que el software de gestión deberá cumplir para poder realizar la implementación del presente proyecto. Se definirá las especificaciones de una forma entendible, clara, completa, consistente, verificable y modificable que ayudará a elegir un software de gestión con un rendimiento y disponibilidad estables.

D.2.3. Ámbito

El software de gestión que se implementará además de ser estable y robusto debe estar basado en software libre y ser compatible con un entorno virtualizado. El software

de gestión también deberá permitir una administración centralizada y escalable además de brindar ciertas funcionalidades que ayuden a mejorar el desempeño actual de la red.

D.2.4. Definiciones, Acrónimos y Abreviaturas

D.2.4.1. Definiciones

Término	Definición
Entorno Virtualizado	Cada sistema operativo puede residir en una maquina propia independiente como si fuera una computadora física, todo esto controlado por un hipervisor.
Especificación de Requisitos Software	Es un conjunto de requerimientos que describen la funcionalidad que el software debe tener para cumplir con los objetivos de implementación.

D.2.4.2. Acrónimos

Acrónimo	Definición
IEEE	Institute of Electrical and Electronic Engineers ó Instituto de Ingenieros Eléctricos y Electrónicos
ERS	Especificación de Requisitos Software
SMS	Short Message Service ó Servicio de Mensajes Cortos
GPL	General Public License o Licencia Pública General

D.2.4.3. Abreviaturas

Abreviatura	Definición
Std	Estándar
REQ	Requisito

D.2.5 Referencias

- IEEE-STD-830-1998.- Especificaciones de los Requisitos del Software

D.2.6. Descripción general

D.2.6.1. Perspectiva del Producto

El software de gestión puede ser instalado en una plataforma con sistema operativo con licencia GPL³⁵ ya sea en una infraestructura física o virtual donde este deberá tener la misma funcionalidad y estabilidad, pero tomando en cuenta los requerimientos del mismo y de la entidad o empresa además el software deberá interactuar con las áreas funcionales de un modelo de gestión.

D.2.6.2. Funciones del Producto

Manejar una interfaz Web ininteligible

- Posee una interfaz fácil de interpretar, configurar e implementar manteniendo la funcionalidad de las áreas de gestión.

Manejar disponibilidad y estabilidad

- Permitir constantemente el monitoreo de dispositivos gestionados.

D.2.6.3. Restricciones

- El software de gestión debe soportar el monitoreo de diferentes modelos de dispositivos de red gestionados entre ellos: Cisco, 3Com, Mikrotik.
- El software de gestión debe ser compatible con varios Sistemas Operativos.
- El software de gestión será específicamente software libre y deberá permitir el uso de otras herramientas que también serán libres.

³⁵ GPL.- Licencia Pública General, permite a un usuario modificar, copiar, estudiar un software que mantenga este tipo de licencia.

D.2.7. Requisitos Específicos

D.2.7.1. Interfaces Externas

En esta sección se establecen los requisitos que definen la comunicación entre las personas encargadas de la administración de la red y el software de gestión.

D.2.7.1.1. Interfaces de usuario

REQ#1: Administración

El software de gestión deberá brindar al usuario administrador una consola de administración centralizada en la cual se podrá observar el estado de los dispositivos gestionados.

D.2.8. Requisitos Funcionales

REQ#2: Compatibilidad de Virtualización

El software debe ser compatible con un sistema de virtualización, requerimiento fundamental para su implementación.

REQ#3: Monitoreo de recursos hardware

El software deberá monitorear (uso de CPU, uso de memoria, uso de disco, interfaces de red activas) de los servidores y dispositivos de red Switches, Routers, host.

REQ#4: Manejo de alertas

El software debe generar alertas cuando sobrepasen umbrales previamente definidos.

REQ#5: Soporte de envío de correo electrónico y SMS

El software deberá enviar mensajes SMS y correos electrónicos informando cuando ocurra un fallo en algún dispositivo gestionado que sea considerado como prioritario.

REQ#6: Generación de reportes

El software deberá emitir reportes (informes, historiales, datos estadísticos) de los dispositivos gestionados.

REQ#7: Soporte SNMP

El software deberá soportar el envío de información mediante SNMP.

REQ#8: Soporte de varios Sistemas Operativos

El software debe permitir monitorear servidores remotos con sistemas operativos Windows y Linux con sus respectivos agentes.

REQ#9: Documentación suficiente

El software deberá poseer información suficiente y clara, de una comunidad que lo respalde.

REQ#10: Seguridad del software

El software debe proporcionar seguridad en cuanto al manejo de contraseña y permiso de usuarios para acceder al sistema.

REQ#11: Performance

El funcionamiento de los dispositivos monitoreados no se debe ver afectado por nuevas funciones instaladas en los mismos.

REQ#12: Usabilidad

El software de gestión deberá ser de fácil uso, configuración e implementación y mantenimiento.

REQ#13: Estabilidad

El software de gestión debe ser instalado en una versión estable y disponible actualmente no debe ser de prueba.

REQ#14: Disponibilidad

El software debe estar disponible y con un total rendimiento las 24 horas del día los siete días de la semana debido a que será instalado en una entidad donde cursa información de usuarios todo el tiempo.

D.2.9. Selección de Software.

D.2.9.1. Valorización de los Requerimientos.

Después de haber determinado los requerimientos para la selección del software de gestión, se procede a establecer un puntaje para cada requerimiento y poder encontrar la mejor solución para la implementación de este proyecto.

REQ#1: Administración

- 0 No posee ninguna interfaz de administración
- 1 Posee una interfaz de administración

REQ#2: Compatibilidad de Virtualización

- 0 No soporta la instalación en un sistema virtualizado
- 1 Soporta la instalación en un sistema virtualizado

REQ#3: Monitoreo de recursos hardware

- 0 No realiza monitoreo de recursos hardware
- 1 Realiza monitoreo de recursos hardware

REQ#4: Manejo de alertas

- 0 No soporta el manejo de alertas con establecimiento de umbrales
- 1 Soporta el manejo de alertas con establecimiento de umbrales

REQ#5: Soporte de envío de correo electrónico y SMS

- 0 No soporta el envío de correo electrónico ni SMS
- 1 Soporta el envío de correo electrónico.
- 2 Soporta el envío de correo electrónico y SMS.

REQ#6: Generación de reportes

- 0 No permite generar reportes
- 1 Permite generar reportes

REQ#7: Soporte SNMP

- 0 No Soporta SNMP
- 1 Soporta SNMP

REQ#8: Soporte de varios Sistemas Operativos

- 0 No soporta a sistemas operativos como Windows y Linux
- 1 Soporta a sistemas operativos como Windows y Linux

REQ#9: Documentación suficiente

- 0 No existe documentación
- 1 Existe poca documentación
- 2 Existe documentación

REQ#10: Seguridad del software

- 0 No posee autorización de acceso al software
- 1 Posee autorización de acceso al software

REQ#11: Performance

- 0 Los equipos gestionados se ven afectados por nuevas funciones instaladas
- 1 Los equipos gestionados no se ven afectados por nuevas funciones instaladas

REQ#12: Usabilidad

- 1 No es de fácil uso, configuración y mantenimiento
- 2 Es de fácil uso, configuración y mantenimiento

REQ#13: Estabilidad

- 0 El software no es estable
- 1 El software es estable

REQ#14: Disponibilidad

- 0 No está disponible las 24 horas del día los 7 días de la semana
- 1 Está disponible las 24 horas del día los 7 días de la semana

D.2.9.2. Evaluación para cada solución de Virtualización

Tabla D 4: Evaluación de Software de Gestión

Requerimientos	Pandora FMS	Zabbix	Cacti	Nagios
REQ#1	1	1	1	1
REQ#2	0	0	1	1
REQ#3	1	1	0	1
REQ#4	1	1	1	1
REQ#5	2	2	2	2
REQ#6	1	1	1	1
REQ#7	1	1	1	1
REQ#8	1	1	1	1
REQ#9	1	1	1	2
REQ#10	1	1	1	1
REQ#11	1	1	1	1
REQ#12	1	1	2	1
REQ#13	0	0	0	1
REQ#14	1	1	1	1
Total	13	13	14	<u>16</u>

Fuente: Elaboración propia basada en estándar IEEE 830

**Anexo E: Manual de Instalación y Configuración del Software
de Gestión Nagios**

**MANUAL DE
INSTALACIÓN Y
CONFIGURACIÓN DEL
SOFTWARE DE
GESTIÓN NAGIOS**



E.1. Manual de Instalación del Software de Gestión Nagios

E.1.1. Especificaciones generales de Nagios.

Como se observa en la Figura E 1, Nagios presenta un núcleo que forma la lógica de control el cual contiene el software necesario para realizar la monitorización de los servicios y dispositivos de red. Además hace uso de diversos componentes que vienen dentro de su paquete de instalación, y puede hacer uso de otros componentes realizados por terceras personas. Realiza su labor basándose en una gran cantidad de pequeños módulos software que realizan chequeos en la red. Muestra los resultados de la monitorización y del uso de los diversos componentes en una interfaz web a través de un conjunto de CGI's³⁶ y de un conjunto de páginas HTML que vienen incorporadas. Al compilar Nagios guardará los históricos en una base de datos para que al detener y reanudar el servicio de monitorización, todos los datos sigan como estaban, sin cambios.

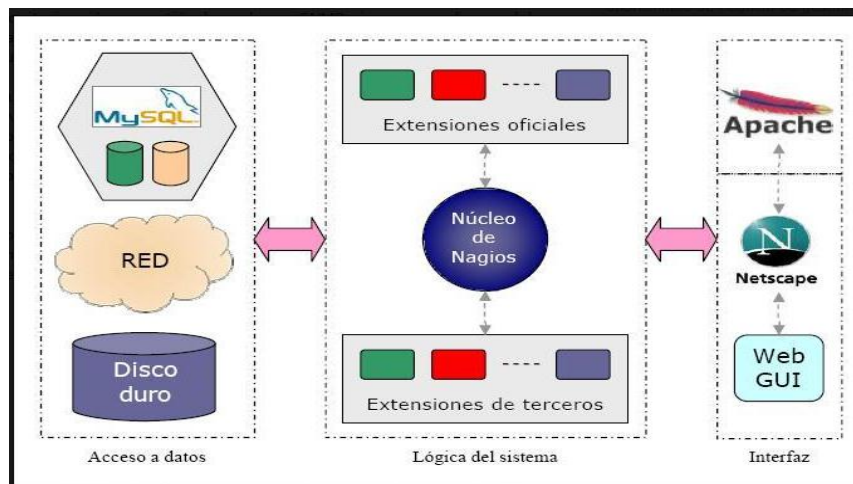


Figura E 1. Estructura de Nagios

Fuente: (Guerrero Pantoja, 2011)

E.1.1.1. Descripción de archivos y directorios que posee Nagios.

³⁶ CGI (Common Gateway Interface).- En español Interfaz de Entrada Común que permite a un cliente de un navegador web solicitar datos de un programa ejecutado en un servidor

Entre los archivos principales que contiene Nagios se puntualizan a continuación los siguientes:

1. **Archivo de configuración principal.-** Este archivo es (`nagios.cfg`) contiene una serie de directivas que afectan la manera cómo funciona el demonio Nagios. Este archivo de configuración se lee tanto por el demonio de Nagios y los CGIs.
2. **Archivos de recursos.-** Utilizados para almacenar macros definidos por el administrador. El objetivo principal de tener archivos de recursos es utilizarlos para almacenar información de configuración confidencial como pueden ser claves, sin ponerlos a disposición de los CGIs.
3. **Archivos de definición de objetos.-** Dentro de estos archivos se define todo lo que se desea monitorear y cómo se desea monitorear cada uno de los dispositivos gestionados. Se puede especificar uno o más archivos de definición de objeto mediante el **cfg_file** que se encuentra dentro del archivo de configuración principal.

3.1. Objetos. Se utilizan para definir los hosts, servicios, grupos de host, contactos, comandos, etc., como está descrito a continuación:

- **Host.-** Los host son dispositivos físicos de la red (servidores, enrutadores), tienen una dirección de algún tipo por ejemplo (IP o MAC). Tienen uno o más servicios asociados con ellos.
- **Grupos de Host (Host groups).-** Son grupos de uno o más host los cuales pueden hacer más fácil ver el estado de ciertos dispositivos relacionados entre sí, mediante la interfaz Web de Nagios y de esta forma simplificar la configuración.

- **Comandos (Commands).**- Estos comandos se utilizan para indicar a Nagios que Plugins se deben ejecutar para llevar a cabo: chequeo de host y servicios, notificaciones, eventos.
- **Servicios (Services).**- Los servicios están relacionados con los host y estos pueden ser atributos como (carga de CPU, uso de disco, etc).
- **Grupo de Servicios (Service Groups).**- Al igual que host groups simplifican la configuración y facilitan ver en la interfaz web de Nagios el estado de los servicios relacionados.
- **Contactos (Contacts).**- Se refiere a las personas a las cuales se les notificará de algún suceso anormal que pase en los dispositivos de red y posee las siguientes características:
 - Los contactos deben tener uno o más métodos de comunicación por ejemplo el software genera (mensajes SMS a celulares, correo electrónico, etc)
 - Los contactos reciben las notificaciones de las máquinas y de servicios de los cuales son responsable.
- **Grupos de Contactos (Contacts groups).**- Son grupos de uno o más contactos.
- **Periodos de tiempo (Time periods).**- Se utiliza para determinar cuando los host y servicios pueden ser monitoreados y cuando los contactos pueden recibir notificaciones.
- **Plantillas (Templates).**- Son archivos que permiten simplificar la configuración de dispositivos de red y servicios.

4. Archivos de configuración CGI.- Archivos que permite al administrador peticionar datos de aplicaciones ejecutadas en Nagios y visualizarlas en su interfaz web.

5. Directorios principales de Nagios.

Se describe a continuación los subdirectorios que están ubicados en

/usr/local/nagios:

- **bin.-** En este directorio está el ejecutable Nagios que es el programa que se ejecuta en segundo plano.
- **etc.-** Este directorio guarda toda la configuración que se realiza para el correcto funcionamiento de Nagios, es decir los archivos en los que especifica los host y servicios a monitorear, comandos a utilizar para el monitoreo, periodos de tiempo para chequeo y contactos de notificación.
- **libexec.-** Este directorio almacena todos los Plugins ejecutables que serán utilizados para ejecutar los servicios, estos pueden ser archivos binarios o scripts escritos en lenguaje c, php, bash, perl, etc.
- **sbin.-** En este directorio están ubicados los archivos ejecutables CGI que permiten solicitar información de un programa, los mismos que se encuentran ejecutándose en un servidor web, estos archivos hacen posible la visualización de la interfaz web de Nagios.
- **share.-** En este directorio se almacena la información que se mostrará en la interfaz web como logos, imágenes, páginas de inicio y documentación de ayuda.
- **var.-** Dentro de este directorio se guarda un registro de toda la información como resultado de la ejecución de la monitorización como es: estadísticas de los chequeos, logs, información que se está ejecutando.

A continuación se presenta paso a paso la instalación detallada de Nagios y sus Plugins:

E.1.2. Instalación de gestor Nagios

Para realizar todas las instalaciones y configuraciones se debe ingresar en un terminal en modo usuario **root** e ingresar la clave de superusuario, ejecutar:

```
# su
```

1. Instalación de requerimientos previos:

- a) Para instalar Apache 2 y PHP versión 5 ejecutar:

```
# apt-get install apache2
```

```
# apt-get install php5
```

- b) Crear fichero info.php para comprobar la instalación anterior:

```
# cd /var/www
```

```
# echo '<?php phpinfo() ?>' > info.php
```

- c) Para instalar el paquete Perl ejecutar:

```
# apt-get install libperl-version-perl
```

- d) Reiniciar servicio Apache:

```
# /etc/init.d/apache2 restart
```

- e) Instalar el paquete GCC de compilación necesario:

```
# apt-get install build-essential
```

- f) Se instala las librerías necesarias para jpeg, png:

```
# apt-get install libjpeg62 libjpeg62-dev libpng12-0 libpng12-dev
```

- g) Se instala la librería GD:

Ingresar al directorio **/tmp** para descargar ahí el siguiente paquete para complementar la configuración de Nagios:

```
# cd /tmp
```

Descargar el paquete mediante la herramienta wget:

```
# wget -c https://bitbucket.org/libgd/gd-libgd/downloads/libgd-2.1.0.tar.gz
```

Descomprimir e ingresar a la carpeta descargada para configurarla:

```
# tar -xf libgd-2.1.0.tar.gz
```

```
# cd libgd-2.1.0
```

```
# ./configure
```

```
# make install
```

h) Instalar modulo GD de PHP.

```
# apt-get install php5-gd
```

i) Reiniciar Apache y comprobar mediante la URL de info.php que estén las librerías de GD instaladas.

```
# /etc/init.d/apache2 restart
```

```
# http://ip.servidor/info.php
```

j) Instalar el módulo SNMP de perl.

```
# perl -MCPAN -e "install Net::SNMP" (.. a cualquier pregunta responder yes)
```

2. Configuración de Nagios:

j) Se crea la cuenta del usuario Nagios y la asignación de contraseña:

```
# useradd nagios
```

```
# passwd nagios <Clave de usuario>
```

k) Crear los grupos de Nagios.

```
# groupadd nagios
```

Crear un nuevo grupo llamado nagcmd para permitir comandos externos:

```
# groupadd nagcmd
```

- l) Asignar los usuarios a sus respectivos grupos.

```
# usermod -G nagios nagios
```

```
# usermod -G nagcmd nagios
```

```
# usermod -G nagcmd www-data
```

- m) Descargar las fuentes de Nagios como se indica a continuación en el siguiente directorio:

```
# cd /tmp
```

```
# wget http://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.0.4/nagios-4.0.4.tar.gz/download?use_mirror=hivelocity
```

- n) Descomprimir el paquete nagios-4.0.4.tar.gz anteriormente descargado e ingresar al mismo:

```
# tar -xf nagios-4.0.4.tar.gz
```

```
# cd nagios-4.0.4/
```

Ejecutar el script de configuración de Nagios colocando el nombre del grupo que se creó donde mostrara la siguiente pantalla que se observa en la figura:

```
# ./configure --with-command-group=nagcmd
```

```
172.16.8.202 - PuTTY
config.status: creating html/Makefile
config.status: creating module/Makefile
config.status: creating worker/Makefile
config.status: creating worker/ping/Makefile
config.status: creating sdata/Makefile
config.status: creating daemon-init
config.status: creating t/Makefile
config.status: creating t-tap/Makefile
config.status: creating include/config.h
config.status: creating lib/sprintf.h
config.status: creating lib/iobroker.h
Creating sample config files in sample-config/ ...

*** Configuration summary for nagios 4.0.4 03-14-2014 ***:
General Options:
Nagios executable: nagios
Nagios user/group: nagios,nagios
Command user/group: nagios,nagcmd
Event Broker: yes
Install ${prefix}: /usr/local/nagios
Lock file: ${prefix}/var/nagios.lock
Check result directory: ${prefix}/var/spool/checkresults
Init directory: /etc/init.d
Apache conf.d directory: /etc/apache2/conf.d
Mail program: /usr/bin/mail
Host OS: linux-gnu
IOBroker Method: spoll

Web Interface Options:
HTML URL: http://localhost/nagios/
CGI URL: http://localhost/nagios/cgi-bin/
Traceroute (used by WAP): /usr/sbin/traceroute

Review the options above for accuracy. If they look okay,
type 'make all' to compile the main program and CGIs.

root@debbadmin:/tmp/nagios-4.0.4# ./configure --with-command-group=nagcmd
```

Figura E 1: Configuración de grupos

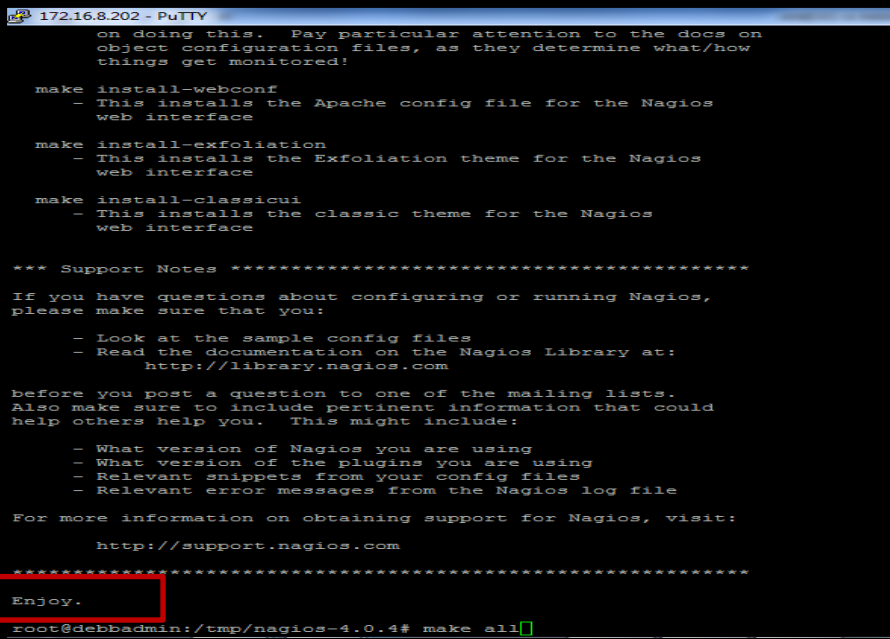
La Tabla E 1 explica la funcionalidad de los comandos de instalación y a continuación se ejecutan los mismos:

Tabla E 1: Descripción de comandos para el proceso de instalación de Nagios.

Comando	Funcionalidad
make all	Compila Nagios
make install	Instala archivos de los principales programas CGI y HTML
make install-init	Instala scripts para configurar Nagios como un servicio del sistema
make install-config	Instala la configuración de Nagios
make install-commandmode	Instala y configura el archivo de comandos externos
make install-webconf	Instala y configura el archivo de configuración de Nagios para Apache, para la visualización de la interfaz web.

Fuente: Elaboración propia basada en parámetros de instalación de Nagios

make all



```

172.16.8.202 - PuTTY
on doing this. Pay particular attention to the docs on
object configuration files, as they determine what/how
things get monitored!

make install-webconf
- This installs the Apache config file for the Nagios
web interface

make install-xfoliation
- This installs the Exfoliation theme for the Nagios
web interface

make install-classicui
- This installs the classic theme for the Nagios
web interface

*** Support Notes *****
If you have questions about configuring or running Nagios,
please make sure that you:
- Look at the sample config files
- Read the documentation on the Nagios Library at:
  http://library.nagios.com

before you post a question to one of the mailing lists.
Also make sure to include pertinent information that could
help others help you. This might include:
- What version of Nagios you are using
- What version of the plugins you are using
- Relevant snippets from your config files
- Relevant error messages from the Nagios log file

For more information on obtaining support for Nagios, visit:
http://support.nagios.com

*****
Enjoy.
root@debbadmin:/tmp/nagios-4.0.4# make all

```

Figura E 2: Compilación de Nagios

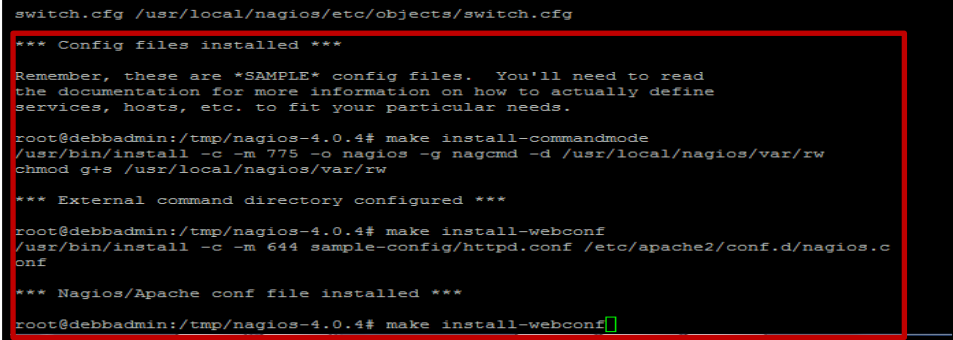
make install

make install-init

make install-config

```
# make install-commandmode
```

```
# make install-webconf
```



```
switch.cfg /usr/local/nagios/etc/objects/switch.cfg
*** Config files installed ***
Remember, these are *SAMPLE* config files. You'll need to read
the documentation for more information on how to actually define
services, hosts, etc. to fit your particular needs.

root@debbadmin:/tmp/nagios-4.0.4# make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

root@debbadmin:/tmp/nagios-4.0.4# make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/conf.d/nagios.c
onf

*** Nagios/Apache conf file installed ***

root@debbadmin:/tmp/nagios-4.0.4# make install-webconf
```

Figura E 3: Compilación de Nagios (1)

- o) Aquí se crea un usuario (**nagiosadmin**) http para el acceso vía web a Nagios:

```
# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Aquí es donde se puede hacer mas usuarios para el ingreso al software de gestion

- p) Reiniciar el Apache para que actualice el último cambio.

```
# /etc/init.d/apache2 restart
```

- q) Crear enlace para que Nagios arranque el inicio automáticamente.

```
# ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

- r) Comprobar configuración y reinicio de Nagios.

Con este comando se verifica que las configuraciones e instalación de Nagios en

Debian está correcta:

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

- s) En este punto ya está instalado Nagios y sin errores por lo tanto iniciar el servicio.

```
# /etc/init.d/nagios start
```

- t) Entrar a la interfaz web mediante la URL de Nagios.

```
# http://ip.servidor/nagios/
```

Ingresar el nombre de usuario (nagiosadmin) y la contraseña que se configuro anteriormente.

3. Instalación de Plugins de Nagios

- a) Descargar los Plugins como se indica a continuación en el siguiente directorio:

```
# cd /tmp

# wget https://www.nagios-plugins.org/download/nagios-plugins-2.0.tar.gz
```

- b) Descomprimir el paquete *nagios-plugins-2.0.tar.gz* anteriormente descargado e ingresar al mismo:

```
# cd /tmp

# tar -xf nagios-plugins-2.0.tar.gz

# cd nagios-plugins-2.0/
```

- c) Compilar e instalar los Plugins como se muestra en la Figura E 4:

```
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

```
checking for wctype_t... yes
checking for wctrans_t... yes
checking whether wctype is declared without a macro... yes
checking whether wctrans is declared without a macro... yes
checking whether towctrans is declared without a macro... yes
checking for stdint.h... (cached) Yes
configure: creating ./config.status
config.status: creating gl/Makefile
config.status: creating nagios-plugins.spec
config.status: creating Makefile
config.status: creating tap/Makefile
config.status: creating lib/Makefile
config.status: creating plugins/Makefile
config.status: creating lib/tester/Makefile
config.status: creating plugins-root/Makefile
config.status: creating plugins-scripts/Makefile
config.status: creating plugins-scripts/subst
config.status: creating plugins-scripts/utills.pm
config.status: creating plugins-scripts/utills.sh
config.status: creating perlmoda/Makefile
config.status: creating test.pl
config.status: creating pkg/solaris/pkginfo
config.status: creating po/Makefile.in
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing libtool commands
config.status: creating po/POFILES
config.status: creating po/POFILES
config.status: creating po/Makefile
--with-apt-get-command: /usr/bin/apt-get
--with-ping6-command: /bin/ping6 -n -U -w %d -c %d %s
--with-ping-command: /bin/ping -n -U -w %d -c %d %s
--with-iptables: yes
--with-mysqld: no
--with-openssl: yes
--with-openssl: no
--enable-extra-opts: yes
--with-perl: /usr/bin/perl
--enable-perl-modules: no
--with-cgiurl: /nagios/cgi-bin
--with-trusted-path: /bin:/sbin:/usr/bin:/usr/sbin
--enable-libtap: no
root@debbadmin: /tmp/nagios-plugins-2.0#
```

Figura E 4: Compilación de Nagios (3)

```
# make
```

```
# make install
```


E.1.2.1. Instalación de Agente SNMP

La presente instalación se realizó en el gestor y en los agentes para establecer comunicación entre ellos:

1. Instalar requerimientos previos y el demonio snmpd

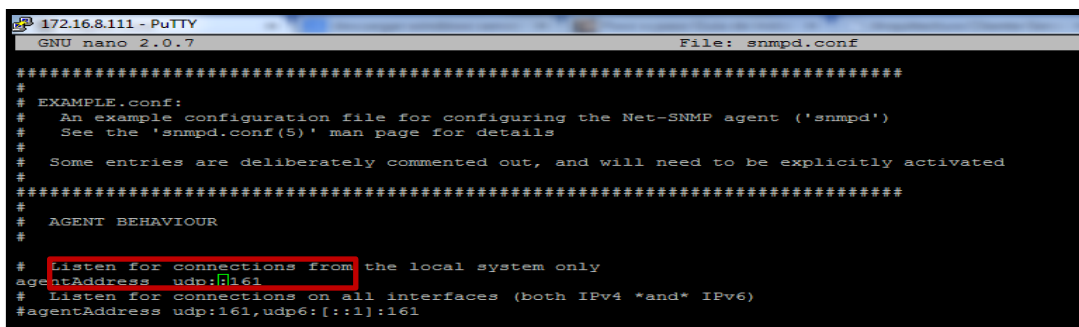
```
# apt-get install libsnmp-perl
```

```
# apt-get install snmp
```

```
# apt-get install snmpd
```

2. Editar el archivo que está en el directorio /etc/snmp, borrar 127.0.0.1 que está en la línea agentAddress udp:127.0.0.1:161:

```
# nano /etc/snmp/snmpd.conf
```



```
#####
#
# EXAMPLE.conf:
#   An example configuration file for configuring the Net-SNMP agent ('snmpd')
#   See the 'snmpd.conf(5)' man page for details
#
#   Some entries are deliberately commented out, and will need to be explicitly activated
#####
#
# AGENT BEHAVIOUR
#
# Listen for connections from the local system only
agentAddress udp:161
# Listen for connections on all interfaces (both IPv4 *and* IPv6)
#agentAddress udp:161,udp6:[::1]:161
```

Figura E 5. Configuración de SNMP en Linux

3. Editar el archivo que está en el directorio /etc/snmp y cambiar **system only** por **all**

```
# nano /etc/snmp/snmpd.conf
```

```

172.16.8.111 - PuTTY
GNU nano 2.0.7 File: snmpd.conf
#####
#
# ACCESS CONTROL
#
view systemonly included .1.3.6.1.2.1.1 # system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.25.1
#rocommunity public localhost # Full access from the local host
rocommunity public default # Default access to basic system info
# Full access from an example network
# Adjust this network address to match your local
# settings, change the community string,
# and check the 'agentAddress' setting above
#rocommunity secret 10.0.0.0/16 # Full read-only access for SNMPv3
# Full write access for encrypted requests
# Remember to activate the 'createUser' lines above
#ruser authPrivUser priv
# It's no longer typically necessary to use the full 'com2sec/group/access' configuration
# [(ou)user and [(o)community, together with suitable views, should cover most requirements

```

Figura E 6. Configuración de SNMP en Linux (1)

- Ingresar al archivo `snmp.conf` que está en el siguiente directorio y agregar un `#` en la línea `mibs` :

```
# nano /etc/snmp/snmp.conf
```

```

172.16.8.111 - PuTTY
GNU nano 2.0.7 File: snmp.conf
#
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
#mibs :

```

Figura E 7. Configuración del archivo snmp.conf

Dentro de este bloque se detalla la configuración que complementan el funcionamiento de Nagios como son: PNP4Nagios para poder realizar las gráficas de ancho de banda de cada interfaz, PostFix para realizar el envío de correos y SMStools para realizar el envío de mensajes de texto.

G.1.2.2. Configuración detallada para la instalación de PNP4Nagios.

Para instalar el complemento `pnp4nagios` el servidor Nagios debe estar funcionando correctamente:

- Acceder en modo `root` al servidor Nagios e instalar los siguientes paquetes:

```
# apt-get install php5 rrdtool librrds-perl
```

```
# apt-get install librrdtool-oo-perl, python-rrdtool, rddtool-dbg, rrdtool-tcl,
rrdcached
```

```
# apt-get install librrd-ruby1.9.1, librrd4, librrdp-perl, librrds-dev, rrdcollect
```

2. Instalar el paquete pnp4nagios

a) Descargar el paquete desde la siguiente página:

```
#wget http://sourceforge.net/projects/pnp4nagios/files/PNP-0.6/pnp4nagios-
0.6.21.tar.gz/download
```

4. Descomprimir los archivos de PNP4 e ingresar al directorio:

```
# tar -xf pnp4nagios-0.6.21.tar.gz
```

```
# cd pnp4nagios-0.6.21
```

b) Compilar e instalar el paquete pnp4nagios:

```
#!/configure
```

```
# make all
```

```
root@debbadmin:~/pnp4nagios-0.6.21# make all
cd ./src && make
make[1]: se ingresa al directorio '/root/pnp4nagios-0.6.21/src'
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o utils.o utils.c
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o config.o config.c
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o logging.o logging.c
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -o npcd npcd.o utils.o config.o logging.o -lpthread
gcc -fPIC -g -O2 -DHAVE_CONFIG_H -DNSCORE -o npcdmod.o npcdmod.o -shared -fPIC
make[1]: se sale del directorio '/root/pnp4nagios-0.6.21/src'
cd ./share && make
make[1]: se ingresa al directorio '/root/pnp4nagios-0.6.21/share'
make[1]: No se hace nada para `all'.
make[1]: se sale del directorio '/root/pnp4nagios-0.6.21/share'
cd ./scripts && make
make[1]: se ingresa al directorio '/root/pnp4nagios-0.6.21/scripts'
make[1]: No se hace nada para `all'.
make[1]: se sale del directorio '/root/pnp4nagios-0.6.21/scripts'
chmod a+r ./contrib/ssi/status-header.ssi

*** Compile finished ***

make install
- This installs the main program and HTML files

make fullinstall
- This installs the main program, runlevel scripts, config and HTML files

Enjoy.
root@debbadmin:~/pnp4nagios-0.6.21#
```

Figura E 8: Compilación de PNP4nagios

Para instalar y copiar todos los elementos en sus lugares correspondientes en el sistema se ficheros:

```
# make install
```

```

172.16.8.202 - PuTTY
checking for rrdtool... /usr/bin/rrdtool
checking rrdtool path /usr/bin/rrdtool... yes
checking for executable Bit on /usr/bin/rrdtool... yes
checking for linker flags for loadable modules... -shared
checking for Perl Module Time::HiRes... yes
checking for Perl Module Getopt::Long... yes
checking for optional Perl Module RRDs... yes
configure: creating ./config.status
config.status: creating subst
config.status: creating Makefile
config.status: creating share/Makefile
config.status: creating lib/Makefile
config.status: creating scripts/Makefile
config.status: creating src/Makefile
config.status: creating sample-config/Makefile
config.status: creating man/Makefile
config.status: creating include/config.h

*** Configuration summary for pnp4nagios-0.6.21 03-24-2013 ***

General Options:
-----
Nagios user/group:          nagios nagios
Install directory:         /usr/local/pnp4nagios
HTML Dir:                  /usr/local/pnp4nagios/share
Config Dir:                 /usr/local/pnp4nagios/etc
Location of rrdtool binary: /usr/bin/rrdtool Version 1.4.7
RRDs Perl Modules:         FOUND (Version 1.4007)
RRD Files stored in:       /usr/local/pnp4nagios/var/perfdata
process_perfdata.pl logfile: /usr/local/pnp4nagios/var/perfdata.log
Perfdata files (NPCD) stored in: /usr/local/pnp4nagios/var/spool

Web Interface Options:
-----
HTML URL:                  http://localhost/pnp4nagios
Apache Config File:        /etc/apache2/conf.d/pnp4nagios.conf

Review the options above for accuracy.  If they look okay,
type 'make all' to compile.
root@debbadmin:~/pnp4nagios-0.6.21#

```

Figura E 9: Compilación de PNP4nagios (1)

Con este comando se asegura que los ficheros de configuración process_perfdata.pl y npcd se copien en etc/pnp:

```

# make install-config
# make install-webconf
# ldconfig

```

```

*** Main program, Scripts and HTML files installed ***

Please run 'make install-webconf' to install the
web configuration file

Please run 'make install-config' to install sample
configuration files

Please run 'make install-init' if you want to use
BULK Mode with NPCD

root@debbadmin:~/pnp4nagios-0.6.21#

```

Figura E 10: Compilación de PNP4nagios (2)

c) Ahora se necesita el módulo de reescritura activa en apache:

```

# cd /etc/apache2/mods-enable/
# ln -s ../mods-available/rewrite.load rewrite.load

```

d) Configurar nagios.cfg, buscar el parámetro process_performance_data e introducir los datos a continuación.

```

# cd /usr/local/nagios/etc/

```

```

# nano nagios.cfg

process_performance_data=1
# *the template definition differs from the one in the original nagios.cfg
service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata
service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$
\tHOSTNAME::$HOSTNAMES$\tSERVICEDESC::$SERVICEDESC$\tSER
VICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$S
ERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATET
YPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTATE$\tSERVICES
TATETYPE::$SERVICESTATETYPE$

service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-perfdata-file
# *** the template definition differs from the one in the original nagios.cfg
host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$
\tHOSTNAME::$HOSTNAMES$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOS
TCHECKCOMMAND::$HOSTCHECKCOMMAND$\tHOSTSTATE::$HOSTST
ATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$
host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file

```

- e) Acceder al archivo `commands.cfg` e introducir los datos en el final del archivo:

```

# cd /usr/local/nagios/etc/objects/commands.cfg

define command {
    command_name    process-service-perfdata-file
    command_line    /bin/mv /usr/local/pnp4nagios/var/service-perfdata
                   /usr/local/pnp4nagios/var/spool/service-
                   perfdata.$TIMET$
}

define command {
    command_name    process-host-perfdata-file

```

```

command_line      /bin/mv /usr/local/pnp4nagios/var/host-perfdata
                  /usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$
    }

```

f) Ajustar la configuración mediante los siguientes pasos:

```

# cd /usr/local/pnp4nagios/etc
# mv process_perfdata.cfg-sample process_perfdata.cfg
# mv npcd.cfg-sample npcd.cfg

```

g) Reiniciar apache y acceder a la interfaz de pnp4Nagios

```

# /etc/init.d/apache2 restart
# http://IP_Servidor/pnp4nagios/

```

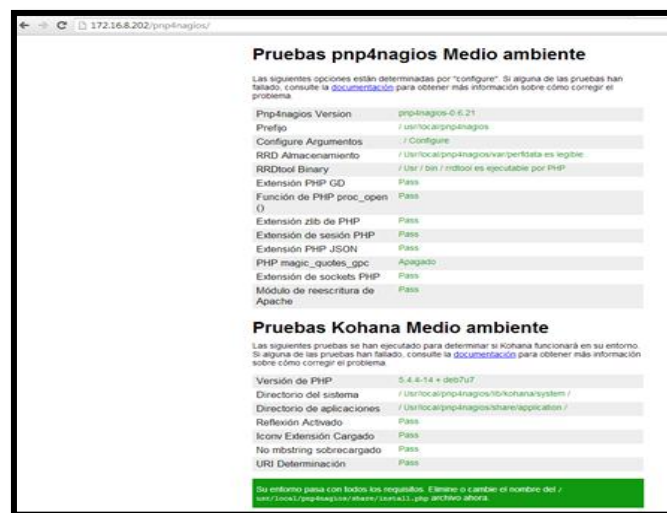


Figura E 11. Prueba de instalación

nota: Verificar que todas las dependencias estén en OK.

h) Ajustes de la página pnp4nagios

```

# cd /usr/local/pnp4nagios/share
# mv install.php install.php-old

```

i) Iniciar el servicio

```

# /usr/local/pnp4nagios/bin/npcd -d -f /usr/local/pnp4nagios/etc/npcd.cfg

```

j) Ingresar al directorio /etc/rc.local y agregar la siguiente línea:

nano /usr/local/pnp4nagios/bin/npcd -d -f /usr/local/pnp4nagios/etc/npcd.cfg

```

172.16.8.202 - PuTTY
GNU nano 2.2.6 Fichero: rc.local

#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

nano /usr/local/pnp4nagios/bin/npcd -d -f /usr/local/pnp4nagios/etc/npcd.cfg
exit 0

```

Figura E 12. Configuración del archivo rc.local

k) Integrar las interfaces de Nagios en PNP4NAGIOS

Acceder al archivo templates.cfg que está en el directorio /usr/local/nagios/etc/objects e introducir el siguiente código:

```

define service{
    name                servicio-pnp
    action_url
    /pnp4nagios/index.php/graph?host=$HOSTNAME&srv=$SERVICEDESC$
    register            0
}

define host{
    name                host-pnp
    action_url
    /pnp4nagios/index.php/graph?host=$HOSTNAME&srv=_HOST_
    register            0
}

```

l) Verificar que no exista ningún error, y reiniciar nagios:

```

# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

# /etc/init.d/nagios restart

```



```
# make install-plugin
# make install-daemon
# make install-daemon-config
# make install-xinetd
```

- d) Acceder y editar el archivo de configuración de xinetd que está en el directorio `/etc/xinetd.d/nrpe` para aceptar peticiones.

```
# nano /etc/xinetd.d/nrpe
only_from = 127.0.0.1 <<ip_servidor_nagios>>
```

- e) Editar el archivo que se encuentra en el directorio `/etc/services` y añadir el puerto de NRPE para poder identificar las conexiones

```
# nano /etc/xinetd.d/nrpe
nrpe          5666/tcp     # NRPE
```

- f) Reiniciar el demonio xinetd

```
# /etc/init.d/xinetd restart
```

- g) Probar el funcionamiento de nrpe localmente y remotamente.

```
# netstat -ant | grep 5666
```

La salida en el terminal debe mostrar la siguiente línea:

```
tcp          0 0 0.0.0.0:5666      0.0.0.0:* LISTEN
```

- h) Chequear si el plugin NRPE se ha instalado correctamente

```
# /usr/local/nagios/libexec/check_nrpe -H localhost
```

El resultado es el siguiente:

```
NRPE v2.15
```

E.1.2.4. Instalación detallada del servidor de correo electrónico

En esta parte se realiza paso a paso la instalación de PostFix:

1. Instalar mail. Comando que Nagios usará para el envío de mail.

```
# apt-get install mailutils
```

2. Crear enlace para el comando mail

```
# ln -s /usr/bin/mail /bin/mail
```

3. Instalar postfix como medio de transporte para el envío de correo.

```
# apt-get install postfix
```

Elegir la opción “Internet Site”. El sistema de correo se configura con el sistema externo para una cuenta de correo de Gmail.

4. Copiar la configuración original del postfix.

```
# cp -p /etc/postfix/main.cf /etc/postfix/main.cf.original
```

5. Crear la configuración para Gmail.

```
# echo "" > /etc/postfix/main.cf
```

6. Ingresar los siguientes datos dentro del fichero.

```
# nano -w /etc/postfix/main.cf
```

```
relayhost = [smtp.gmail.com]:587
```

```
smtp_use_tls = yes
```

```
smtp_tls_CAfile = /etc/postfix/cacert.pem
```

```
smtp_sasl_auth_enable = yes
```

```
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
```

```
smtp_sasl_security_options = noanonymous
```

7. Generar el fichero con la autenticación con el siguiente contenido.

```
# nano -w /etc/postfix/sasl/passwd
```

```
[smtp.gmail.com]:587 usuario@gmail.com:<contraseña>
```

Reemplazar la cuenta de correo y contraseña por la cuenta valida de Gmail.

8. Asignar permisos adecuados.

```
# chmod 600 /etc/postfix/sasl/passwd
```

- Transformar el fichero passwd a un fichero indexado hash.

```
# postmap /etc/postfix/sasl/passwd
```

- Añadir la autoridad certificadora.

```
# cat /etc/ssl/certs/Equifax_Secure_CA.pem >> /etc/postfix/cacert.pem
```

- Reiniciar postfix.

```
# /etc/init.d/postfix restart
```

- Probar el envío de correo.

```
# mail -s "el.asunto" usuario@gmail.com
```

CTRL+D (para enviarlo)

E.1.2.5. Instalación detallada para el envío de SMS.

Para el envío de mensajes de texto se requiere de la instalación de un paquete llamado smstools como se indica a continuación:

- Descargar el paquete smstools-3.3.1.15.tar.gz

```
# tar -xf smstools-3.3.1.15tar.gz
```

- Ingresar y compilar el paquete

```
# cd smstools3
```

```
# Make install
```

- Ingresar al directorio /etc/smsd.conf

Configurar el dispositivo móvil añadiendo la siguiente línea: device =
/etc/ttyACM0

- Iniciar el servicio sms3

```
# /etc/init.d/sms3 start
```

```
# /etc/init.d/sms3 restart
```

5. Probar el funcionamiento del envío de SMS

```
# sendsms +593992xxxxxx "Mensaje de Prueba"
```

6. Interconectar al usuario Nagios con SMS Server, para lo cual se ejecuta el siguiente comando:

```
# chown -R nagios.nagios /var/spool/sms
```

7. Para verificar la información de propiedad de Nagios ejecutar el siguiente comando:

```
# ls -la /var/spool/sms
```

8. Todo se ha realizado correctamente, el resultado debe ser el siguiente:

```
# drwxr-xr-x 5 nagios nagios 4096 May 1 11:59 .
```

```
# drwxr-xr-x 17 root root 4096 May 1 11:59 ..
```

```
# drwxr-xr-x 2 nagios nagios 4096 May 1 23:36 checked
```

```
# drwxr-xr-x 2 nagios nagios 4096 May 1 11:44 incoming
```

```
# drwxr-xr-x 2 nagios nagios 4096 May 1 23:36 outgoing
```

9. Configurar el archivo `commands.cfg` que se encuentra en el directorio `/usr/local/nagios/etc/objects` con la siguiente información :

```
define command{
```

```
    command_name    notify-host-by-sms
```

```
    command_line    /usr/bin/printf "%b" ""***** Nagios ***** Host:
```

```
$HOSTNAME$, State: $HOSTSTATE$, Address:$HOSTADDRESS$, Info:
```

```
$HOSTOUTPUT$, Date/Time:$LONGDATETIME$" /usr/local/bin/sendsms
```

```
$CONTACTPAGER$
```

```
}
```

```
define command{
```

```
    command_name    notify-service-by-sms
```

```

command_line /usr/bin/printf "%b" ""***** Nagios *****" Service:
$SERVICEDESC$, Host: $HOSTALIAS$, Address: $HOSTADDRESS$, State:
$SERVICESTATE$, Date/Time: $LONGDATETIME$"/usr/local/bin/sendsms
$CONTACTPAGER$

}

```

E.1.3. Instalación de agentes en los dispositivos gestionados.

En esta sección se explica detalladamente la instalación de agentes necesarios en los dispositivos gestionados para establecer la comunicación con el gestor Nagios:

F.1.3.1. Instalación de agente SNMP en switches Cisco.

Para configurar SNMP en un switch cisco se debe hacer lo siguiente:

1. Entrar en el modo de configuración exec privilegiado ingresando enable y contraseña:

```
Switch> enable
```

```
Contraseña: xxxxxx
```

```
Switch#
```

2. Entrar en el modo de configuración global:

```
Switch# configure terminal
```

```
Switch (config)#
```

3. Definir y crear una comunidad de solo lectura (RO, Read-Only) con la siguiente sintaxis:

```
Switch(config)# snmp-server community nombre_comunidad
```

```
[view nombre_vista ] [ro/rw]
```

Por defecto, si no se especifican los parámetros opcionales, se facilita el acceso de solo lectura a toda la MIB y a todo los host.

```
Switch (config)# snmp-server community imi ro
```

Con este comando se agrega la comunidad imi con permisos de solo lectura.

4. Se configura el switch para enviar notificaciones SNMP a NMS con la siguiente

Sintaxis:

```
Switch(config)# snmp-server host NombreHost[traps/informs][version {1 | 2c  
/ 3 [auth | noauth | priv]} ] NombreComunidad [udp-port numero_puerto]  
[tipo_notificación]
```

Con NombreHost se identifica la dirección IP del gestor.

```
Switch (config)# snmp-server host 172.16.x.x version 2c imi
```

5. Salir del modo de configuración y guardar la configuración:

```
Switch(config)# exit
```

```
Switch# copy-running startup-config
```

6. Comprobar la configuración SNMP

Para comprobar que llegue la información SNMP del Switch al servidor se ejecuta el comando snmpwalk que es emitido por NMS para recuperar la información de administración de los dispositivos monitorizados: `snmpwalk -v -2c -c imi 172.x.x.x`

Nota. Al emplear el comando *snmp-server community* se habilitan automáticamente SNMPv1 y SNMPv2.

E.1.3.2. Instalación de agente SNMP en switches 3COM

Aquí se presenta la configuración de SNMP en switch de la serie 3COM:

- m) Ingresar en modo de configuración con **system-view** y configurar SNMP mediante el comando **snmp-agent community**, configurar la comunidad debido

a que el gestor solo necesita la opción de lectura se ha configurado la opción **read**.

```
<4500G>system-view
System View: return to User View with Ctrl+Z.
[4500G]snmp-agent community read imi
```

Figura E 14. Captura propia instalación de SNMP en switch 3Com

n) Con el comando `display > current-configuration` se puede observar la configuración realizada en el Switch y en la Figura E 15 se indica la configuración realizada y por defecto de SNMP.

```
#
snmp-agent
snmp-agent local-engineid 8000002B03001AC1A3EFC1
snmp-agent community read imi
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version all
```

Figura E 15. Captura propia resultado de instalación de SNMP

E.1.3.3. Instalación de agente SNMP en Enlaces Inalambricos Mikrotik

En la Figura E 16 se indica la configuración de SNMP en dispositivos Mikrotik:

1. Desplegar la pestaña **IP** donde aparece **SNMP**
2. Habilitar en el campo “**Enable**” para habilitar SNMP y click en **Apply**



Figura E 16. Captura propia instalación de SNMP en Mikrotik

3. La Figura E 17 indica como añadir una comunidad para SNMP, dar click en **Communities > Add New**

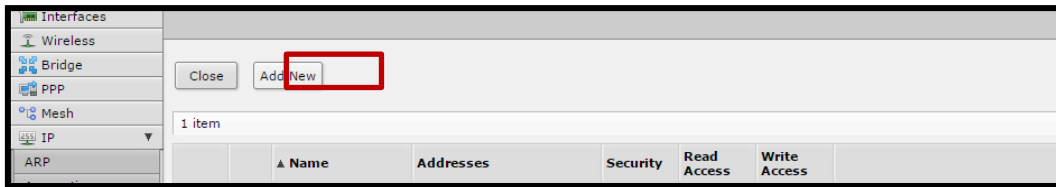


Figura E 17. Captura propia instalación de SNMP en Mikrotik (1)

4. En la Figura E 18 muestra que en el campo **Name** se debe agregar un nombre a la comunidad y activar **Read Access** porque el gestor solo necesita leer los OID del dispositivo.
5. Finalmente dar click en **Apply** para guardar cambios de configuración.

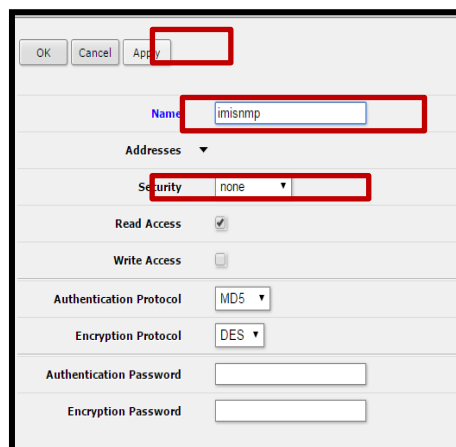


Figura E 18. Captura propia instalación de SNMP en Mikrotik (2)

E.1.3.4. Instalación de agente NRPE en servidores con software libre.

2. Se crea la cuenta del usuario Nagios y la asignación de contraseña:

```
# useradd nagios
```

```
# passwd nagios <Clave de usuario>
```

3. Crear los grupos de Nagios.

```
# groupadd nagios
```

Crear un nuevo grupo llamado nagcmd para permitir comandos externos:


```
# groupadd nagcmd
```

4. Asignar los usuarios a sus respectivos grupos.

```
# usermod -G nagios nagios
```

```
# usermod -G nagcmd nagios
```

```
# usermod -G nagcmd www-data
```

5. Plugins de Nagios

- a) Descargar los Plugins de Nagios

```
# cd /tmp
```

```
# wget https://www.nagios-plugins.org/download/nagios-plugins-1.5.tar.gz
```

- b) Descomprimir el paquete *nagios-plugins-2.0.tar.gz* anteriormente descargado e ingresar al mismo:

```
# cd /tmp
```

```
# tar -xf nagios-plugins-2.0.tar.gz
```

```
# cd nagios-plugins-2.0/
```

Compilar los Plugins:

```
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

Instalar los Plugins

```
# make
```

```
# make install
```

6. Instalar el paquete del demonio xinetd

```
# apt-get install xinetd libssl-dev
```

7. NRPE daemon

- i) Descargar NRPE

```
# cd /tmp
```

```
# wget http://sourceforge.net/projects/nagios/files/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz
```

- j) Descomprimir el paquete y acceder al directorio.

```
# tar -xf nrpe-2.15.tar.gz
# cd nrpe-2.15/
```

- k) Compilar e instalar el paquete nrpe como se muestra en la Figura G 12.

```
#!/configure
# make install-plugin
# make install-daemon
# make install-daemon-config
# make install-xinetd
```

- l) Acceder y editar el archivo de configuración de xinetd que está en el directorio `/etc/xinetd.d/nrpe` para aceptar peticiones.

```
# nano /etc/xinetd.d/nrpe
only_from = 127.0.0.1 <<ip_servidor_nagios>>
```

- m) Editar el archivo que se encuentra en el directorio `/etc/services` y añadir el puerto de NRPE para poder identificar las conexiones

```
# nano /etc/xinetd.d/nrpe
nrpe          5666/tcp      # NRPE
```

- n) Reiniciar el demonio xinetd

```
#!/etc/init.d/xinetd restart
```

- o) Probar el funcionamiento de nrpe localmente y remotamente.

```
# netstat -ant | grep 5666
```

La salida en el terminal debe mostrar la siguiente línea:

```
tcp          0 0 0.0.0.0:5666      0.0.0.0:* LISTEN
```

p) Chequear si el plugin NRPE se ha instalado correctamente

```
# /usr/local/nagios/libexec/check_nrpe -H localhost
```

El resultado es el siguiente:

```
NRPE v2.15
```

F.1.3.5. Instalación de agente NSCLIENT++ en servidores con sistema operativo Windows Server 2003, 2008, 7, 8.

Es necesario un agente para establecer comunicación con el sistema operativo Windows y para eso esta disponible NSClient++ versión 0.3.9 de 64 y 32 bits vigente, a continuación se presenta paso a paso su previa instalación.

1. Pantalla de inicio del asistente de instalación. Pulsar en Next.

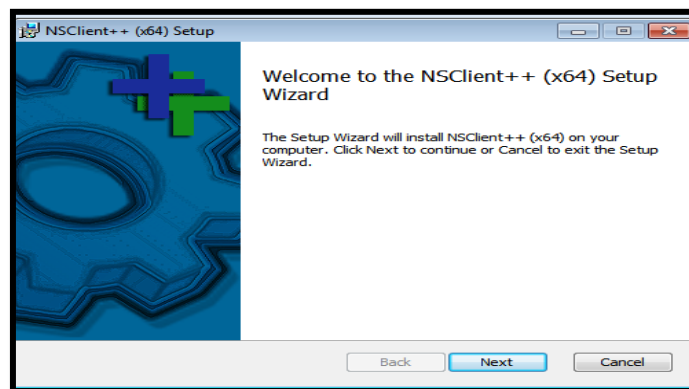


Figura E 19. Pantalla de instalación NSClient++

2. Aceptar la licencia GNUv2 y pulsar en Next.

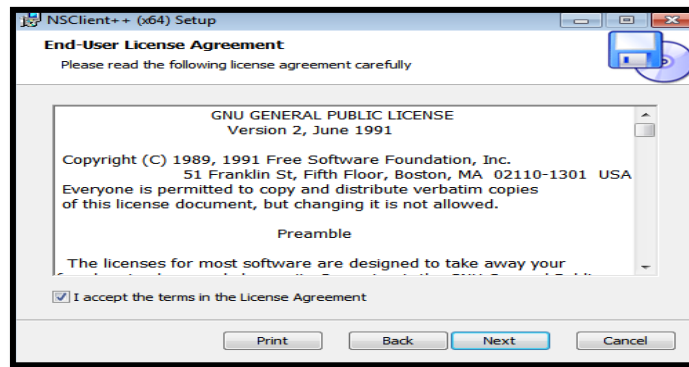


Figura E 20. Pantalla de instalación NSClient++ (1)

3. Seleccionar todo para instalar (por defecto). Pulsar en Next.

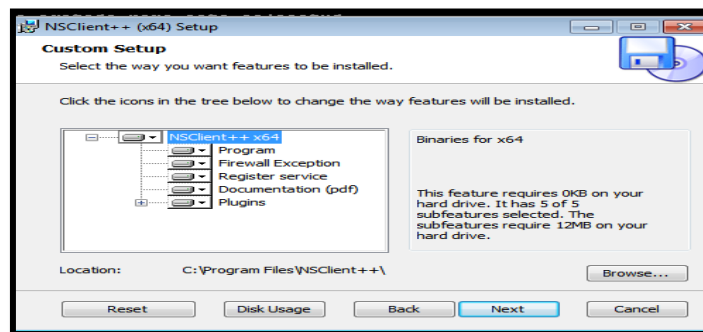


Figura E 21. Pantalla de instalación NSClient++ (2)

4. En la ventana de la Figura E 22 se debe asignar la dirección IP del servidor Nagios donde se enviará la información requerida y el asignar contraseña es opcional Marcar las opciones que se indican en la pantalla. Pulsar en Next.

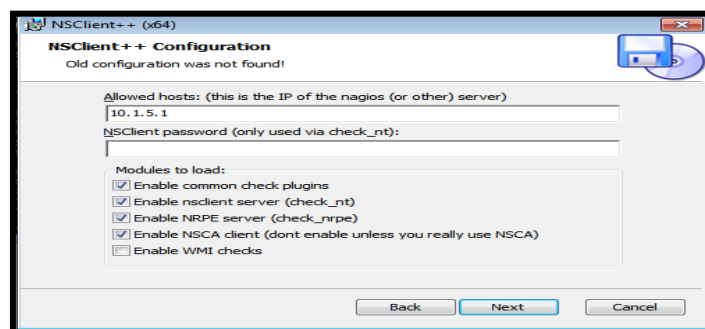


Figura E 22. Pantalla de instalación NSClient++ (3)

5. En la siguiente pantalla pulsar **Install** para que se instale la aplicación y, después de la instalación de los ficheros, marcar que se inicie el servicio y pulsar **Finish**.

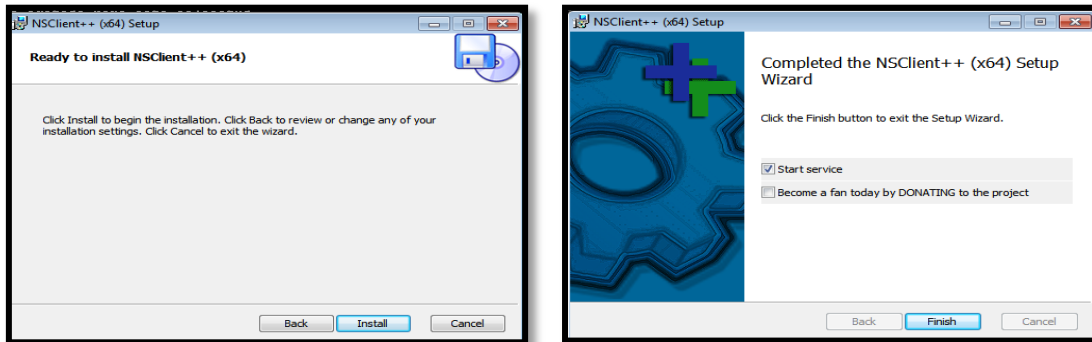


Figura E 23. Fin de instalación NSClient++

6. Por último comprobar que el servicio está iniciado automáticamente. Ir a Inicio > Equipo > Click derecho Administrar > Servicios y Aplicaciones > Servicios. Ir al servicio NSClient++ y configurar para que se inicie automáticamente. Después pulsar Iniciar.

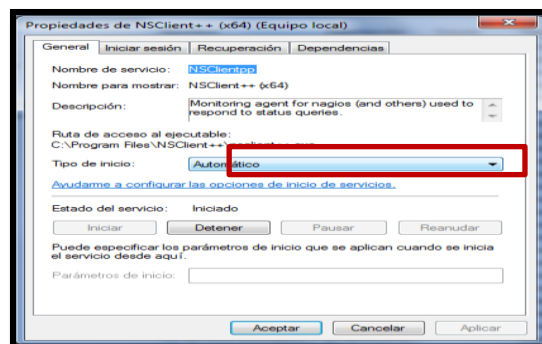


Figura E 24. Fin de instalación NSClient++

7. Configurar el archivo NSC.ini, que está ubicado en: C:\Program Files\NSClient++. Descomentar las líneas con los módulos dll y dejar comentado solamente el NRPEListener.dll, de la siguiente manera:

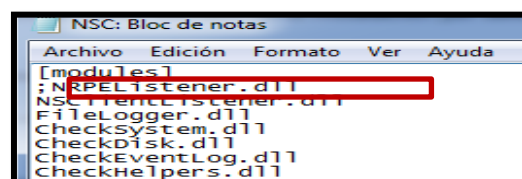


Figura E 25. Configuración de Archivo NSC.ini

Además en la línea: **NSCLIENT PORT NUMBER** descomentar la línea y modificar este puerto con el número "1248", por motivos de incompatibilidad. Guardar y salir.

Nota. Abrir el puerto 12489, 1248 (de igual forma en objects/commands cambiar el puerto).

F.2. Manual de Configuración del Software de Gestión Nagios

F.2.1 Configuración de switches dentro de Nagios.

1. Ingresar a un terminal en modo root.

```
#su
```

```
#contraseña de superusuario
```

2. Se crea el nuevo archivo **sw-cisco-core-4503E.cfg** en los directorios de:

```
#nano /usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

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

```
cfg_file=/usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

3. Configuración de plantillas para switches.

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 2: Plantilla para switches

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	generic-dispositivo-sw	Define nombre asignando a la plantilla
notifications_enabled	1	Define notificaciones: 1-Activa, 0-Desactiva
event_handler_enabled	1	Define control de eventos del sistema: 1-Activa, 0-Desactiva
flap_detection_enabled	1	Define detección de flapeo: 1-Activa, 0-Desactiva
process_perf_data	1	Define proceso de rendimiento: 1-Activa, 0-Desactiva
retain_status_information	1	Conservar la información de estado en los reinicios del programa: 1-Activa, 0-Desactiva
retain_nonstatus_information	1	Retiene la información sin estado en los reinicios del programa 1-Activa, 0-Desactiva
notification_period	24x7	Define periodo de tiempo que enviará notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

Tabla E 3: Plantilla para switches (1)

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	generic-switches	Define nombre asignando a la plantilla
use	generic-dispositivo-sw	Define nombre de la plantilla a heredar

check_period	24x7	Define periodo de chequeo
check_interval	5	Define intervalo de tiempo en minutos entre cada chequeo
retry_interval	1	Define reintentos de chequeo de estado en intervalos de minutos
max_check_attempts	10	Número de veces que chequea el comando, comprueba el estado Up/Down del dispositivo y después notifica
check_command	check-switch-ping	Nombre del comando que comprueba el estado del dispositivo
notification_period	24x7	Nombre de la plantilla que especifica el periodo de notificación
notification_interval	5	Define periodo de tiempo entre cada notificación enviada
notification_options	d, r	Tipo de notificación a enviar d:down, r:recovery, u:unreachable
contacts	Administrador-Nagios	Define nombre a quien notificará Nagios
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

4. Definición de switches.

Ingresar al directorio y archivo para cambiar los valores en las líneas que están con negrita:

```
#cd /usr/local/nagios/etc/objects/Switches/
```

```
#nano /usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

Tabla E 4: Definir switches

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
use	generic-switches	Define nombre de la plantilla a heredar
host_name	SW-CORE	Define nombre del dispositivo
alias	Switch Core	Define nombre descriptivo del dispositivo que aparece en la interfaz web
address	172.x.x.x	Define dirección IP del dispositivo
hostgroups	switches	Define en nombre del grupo al que pertenece el dispositivo
icon_image	switch40.gif	Define la imagen utilizada como icono en la interfaz web
statusmap_image	switch40.gd2	Define la imagen utilizada en el mapa de red de la interfaz
}		Finaliza proceso de definición

Falat poner parents

5. Creación de grupos de switches.

Se define el nombre del grupo de switches al que pertenecerá el nuevo switch que se integre al software de gestión es decir sea este Cisco o 3Com, en el siguiente directorio:


```
#nano /usr/local/nagios/etc/objects/Switches/hostgroup-switches.cfg
```

Tabla E 5: Crear grupo de switches

Parámetros	Valor Asignado	Descripción
define hostgroup {		Inicia proceso de definición
hostgroup_name	switches	Define nombre del grupo
alias	switches-cisco-imi	Define nombre descriptivo que aparece en la interfaz web
}		Finaliza proceso de definición

6. Configuración de plantillas para servicios de switches.

Definir una plantilla para switches en el directorio:

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

Tabla E 6: Plantilla para servicios de switches

Parámetros	Valor Asignado	Descripción
define service{		[Inicia proceso de definición]
name	generic-service-sw	Definición de nombre de plantilla para servicios
active_checks_enabled	1	Define chequeo de servicio activos. 1: Activa, 0: Desactiva
passive_checks_enable	1	Define chequeo de servicio pasivos. 1: Activa, 0:Desactiva
check_freshness	0	Por default desactiva los chequeos pasivos de frescura
notifications_enabled	1	Notificaciones para los servicios. 1: Activa, 0: Desactiva
event_handler_enabled	1	Controlador de eventos para servicios. 1: Activa, 0: Desactiva]
flap_detection_enabled	1	Define la habilitación de flapeo. 1: Activa, 0: Desactiva
process_perf_data	1	Define procesamiento del rendimiento de los datos. 1: Activa, 0: Desactiva
retain_status_information	1	Almacena información sobre el estado de los servicios antes de un reinicio. 1: Activa, 0: Desactiva
is_volatile	0	Define este servicio como no volátil
check_period	24x7	Define el nombre de la plantilla con el periodo de tiempo para el chequeo
max_check_attempts	3	Define máxima cantidad de chequeos
normal_check_interval	3	Define intervalo de tiempo a programar los chequeos en (min)
retry_check_interval	3	Define intervalo de tiempo para un re-chequeo en (min)
contacts	Administrador	Define nombre de contacto
notification_options	w, u, c, r	Define cuando enviar notificaciones de w: warning, c: critical
notification_interval	5	Define intervalo de envío de notificación
notification_period	24x7	Define nombre de plantilla con el periodo para notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

7. Configuración de comandos

En el siguiente directorio configurar comandos para luego concatenarlos con la definición de servicios:

```
#nano /usr/local/nagios/etc/objects/commands.cfg
```

Tabla E 7: Configurar comandos

Parámetros	Valor Asignado	Descripción
define command{		Inicia proceso de definición
command_name	check-switch-ping	Define nombre de comando
command_line	\$USER1\$/check_ping -H \$HOSTADDRESS\$ -w \$ARG1\$ -c \$ARG2\$ -p 5	Define sintaxis de ejecución del comando con su respectivo plugin
}		Finaliza proceso de definición

Breve Descripción:

El comando es ‘\$USER1\$/check_ping’, donde ‘\$USER1\$’ es una macro de Nagios que define donde se encuentran los plugins de Nagios (asignados en el directorio ‘/usr/local/nagios/libexec’); ‘check-switch-ping’ es el nombre del plugin. \$ARG1\$ y \$ARG2\$ son macros que definen los valores de advertencia y critico del plugin.

A continuación se describe cada plugin utilizado en la implementación de switches:

Tabla E 8: Descripción de sintaxis de plugins

Línea de comando	Sintaxis de plugins
command_line	\$USER1\$/check_ping -H \$HOSTADDRESS\$ -w \$ARG1\$ -c \$ARG2\$ -p 5
command_line	\$USER1\$/check_catalyst_load.pl -s \$HOSTADDRESS\$ -C \$ARG1\$ -w \$ARG2\$ -c \$ARG3\$
command_line	\$USER1\$/check_catalyst_mem.pl -s \$HOSTADDRESS\$ -C \$ARG1\$ -w \$ARG2\$ -c \$ARG3\$
command_line	\$USER1\$/check_catalyst_flash.pl -s \$HOSTADDRESS\$ -C \$ARG1\$ -w \$ARG2\$ -c \$ARG3\$
command_line	\$USER1\$/check_catalyst_fans.pl -s \$HOSTADDRESS\$ -C \$ARG1\$
command_line	\$USER1\$/check-cisco.pl -H \$HOSTADDRESS\$ -C \$ARG1\$ -t ps
command_line	\$USER1\$/check_iftraffic43.pl -H \$HOSTADDRESS\$ -C imi -i 3 -b 100 -u m -w \$ARG2\$ -c \$ARG3\$
command_line	\$USER1\$/check_snmp_env.pl -H \$HOSTADDRESS\$ -o \$ARG1\$ -C \$ARG2\$ -T cisco

8. Definición de servicios

Con la información descrita en el paso 7 se continúa con la definición de servicios que verificará el nuevo switch ingresado a Nagios dentro del directorio:

```
#nano /usr/local/nagios/etc/objects/Switches/sw-cisco-core-4503E.cfg
```

Tabla E 9: Definir servicios

Parámetros	Valor Asignado	Descripción
define service{		Inicia proceso de definición
use	generic-service-sw	Define el nombre de plantilla a heredar
host_name	SW-CORE	Define nombre del dispositivo
service_description	01. PING	Define nombre del servicio a verificar
check_command	check_ping!200.0,20%!400.0,40%	Define el comando que realiza la ejecución del servicio
}		Finaliza proceso de definición

A continuación se describe cada plugin con sus valores asignados en la línea `check_command`:

Tabla E 10: Descripción de valores asignados a plugins

check_command	Sintaxis	Descripción
check_ping!	200.0,20%!400.0,40%	Si el tiempo de ida y vuelta (RTT) de la respuesta PING es mayor que 200 ms (pero menor de 400 ms) Nagios marcará un estado de Advertencia y si el RTT es superior a 400 ms Nagios marcará un estado Crítico . Si mas de 20% (pero menos de 40% por ciento) de solicitudes de ping no reciben respuesta Nagios marcará un estado de Advertencia y si mas del 40% de solicitudes de ping no reciben respuesta Nagios marcará un estado Crítico .
check_catalyst_load.pl!	-C imisnmp -w 70,70,70 -c 80,80,80	Verifica el uso de CPU y Nagios marcará un estado de Advertencia si el uso es mayor de 80% y un estado Crítico si es mayor de 90%
check_catalyst_mem.pl!	-C imisnmp -w 30% -c 20%	Verifica el uso de memoria RAM y Nagios marcará un estado de Advertencia cuando tenga solamente un 20% libre y un estado Crítico cuando tenga un 10% libre.
check_catalyst_flash.pl!	-C imisnmp -w 30% -c 20%	Verifica el uso de memoria Flash y Nagios marcará un estado de Advertencia cuando tenga solamente un 20% libre y un estado Crítico cuando tenga un 10% libre.
check_catalyst_fans.pl!	-C imisnmp	Verifica el estado de los ventiladores
check-cisco.pl!	-C imisnmp -t ps	Verifica el estado de la fuente de alimentación
check_iftraffic43.pl!	-C imisnmp -i 3 -b 100 -u m -w 40% -c 50%	Verifica el tráfico que cursa por la interfaz GigabitEthernet 1/1/1, Nagios muestra un estado de Advertencia si el tráfico supera al 70% y un estado Crítico si supera el 80%.
check_snmp_env!	-C imisnmp -o 1.3.6.1.2.1.47.1.1.1.2.6	Verifica el estado del sensor de temperatura

Nota.- Para configurar una nueva interfaz en un switch, se debe conocer el OID perteneciente a la nueva interfaz, mediante el comando

```
#snmpwalk -v 2c -c imi 172.x.x.x ifDescr
```

F.2.2 Configuración de enlaces inalámbricos dentro de Nagios.

1. Ingresar a un terminal en modo root.

```
#su
```

```
#contraseña de superusuario
```

2. Se crea el nuevo archivo **enlace_mikrotik_imi.cfg** en los directorios de:

```
#nano
```

```
/usr/local/nagios/etc/objects/Enlaces_Inalambricos/enlace_mikrotik_imi.cfg
```

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

```
cfg_file=/usr/local/nagios/etc/objects/
```

```
Enlaces_Inalambricos/enlace_mikrotik_imi.cfg
```

3. Configuración de plantillas para enlaces inalámbricos.

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 11: Plantilla para enlaces inalámbricos

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	generic-enlaces	Define nombre asignando a la plantilla
notifications_enabled	1	Define notificaciones: 1-Activa, 0-Desactiva
event_handler_enabled	1	Define control de eventos del sistema: 1-Activa, 0-Desactiva
flap_detection_enabled	1	Define detección de flapeo: 1-Activa, 0-Desactiva
process_perf_data	1	Define proceso de rendimiento: 1-Activa, 0-Desactiva
retain_status_information	1	Conservar la información de estado en los reinicios del programa: 1-Activa, 0-Desactiva
retain_nonstatus_information	1	Retiene la información sin estado en los reinicios del programa 1-Activa, 0-Desactiva]
notification_period	24x7	Define periodo de tiempo que enviará notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

Tabla E 12: Plantilla para enlaces inalámbricos (1)

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	generic-mikrotik	Define nombre asignando a la plantilla
use	generic-enlaces	Define nombre de la plantilla a heredar
check_period	24x7	Define periodo de chequeo
check_interval	5	Define intervalo de tiempo en minutos entre cada chequeo

retry_interval	1	Define reintentos de chequeo de estado en intervalos de minutos
max_check_attempts	10	Número de veces que chequea el comando, comprueba el estado Up/Down del dispositivo y después notifica
check_command	check-mikrotik-ping	Nombre del comando que comprueba el estado del dispositivo
notification_period	24x7	Nombre de la plantilla que especifica el periodo de notificación
notification_interval	5	Define periodo de tiempo entre cada notificación enviada
notification_options	d, r	Tipo de notificación a enviar d:down, r:recovery, u:unreachable
contacts	Administrador	Define nombre a quien notificará Nagios
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

4. Definición de enlaces inalámbricos.

Ingresar al archivo para cambiar los valores en las líneas que están con negrita:

```
#nano
```

```
/usr/local/nagios/etc/objects/Enlaces_Inalambricos/enlace_mikrotik_imi.cfg
```

Tabla E 13: Definir enlace inalámbrico

Parámetros	Valor Asignado	Descripción
define host{		[Inicia proceso de definición]
use	generic-mikrotik	Define nombre de la plantilla a heredar
host_name	Mikrotik-IMI	Define nombre del dispositivo
alias	Enlace Mikrotik IMI	Define nombre descriptivo del dispositivo que aparece en la interfaz web
address	172.x.x.x	[Define dirección IP del dispositivo
hostgroups	Enlaces Inalambricos	Define en nombre del grupo al que pertenece el dispositivo
icon_image	wifi.gif	Define la imagen utilizada como icono en la interfaz web
statusmap_image	wifi.gd2	Define la imagen utiliza en el mapa de red de la interfaz
}		Finaliza proceso de definición

5. Creación de grupo para enlaces inalámbricos.

En el siguiente directorio:

```
#nano /usr/local/nagios/etc/objects/Enlaces-Inalambricos/hostgroup-enlaces-
inalambricos.cfg
```

Tabla E 14: Crear grupo de enlace inalámbrico

Parámetros	Valor Asignado	Descripción
define hostgroup {		Inicia proceso de definición

hostgroup_name	Enlaces Inalambricos	Define nombre del grupo
alias	Enlaces Inalambricos imi	Define nombre descriptivo que aparece en la interfaz web
}		Finaliza proceso de definición

6. Configuración de plantillas para servicios de enlaces inalámbricos.

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 15: Plantilla para servicios de enlace inalámbrico

Parámetros	Valor Asignado	Descripción
define service{		[Inicia proceso de definición]
name	generic-service-mikrotik	Definición de nombre de plantilla para servicios
active_checks_enabled	1	Define chequeo de servicio activos. 1: Activa, 0: Desactiva
passive_checks_enable	1	Define chequeo de servicio pasivos. 1: Activa, 0:Desactiva
check_freshness	0	Por default desactiva los chequeos pasivos de frescura
notifications_enabled	1	Notificaciones para los servicios. 1: Activa, 0: Desactiva
event_handler_enabled	1	Controlador de eventos para servicios. 1: Activa, 0: Desactiva]
flap_detection_enabled	1	Define la habilitación de flapeo. 1: Activa, 0: Desactiva
process_perf_data	1	Define procesamiento del rendimiento de los datos. 1: Activa, 0: Desactiva
retain_status_information	1	Almacena información sobre el estado de los servicios antes de un reinicio. 1: Activa, 0: Desactiva
is_volatile	0	Define este servicio como no volátil
check_period	24x7	Define el nombre de la plantilla con el periodo de tiempo para el chequeo
max_check_attempts	3	Define máxima cantidad de chequeos
normal_check_interval	3	Define intervalo de tiempo a programar los chequeos en (min)
retry_check_interval	3	Define intervalo de tiempo para un re-chequeo en (min)
contacts	Administrador	Define nombre de contacto
notification_options	w, u, c, r	Define cuando enviar notificaciones de w: warning, c: critical
notification_interval	5	Define intervalo de envío de notificación
notification_period	24x7	Define nombre de plantilla con el periodo para notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

7. Configuración de comandos

En el siguiente directorio configurar comandos para luego concatenarlos con la definición de servicios:

```
#nano /usr/local/nagios/etc/objects/commands.cfg
```

Tabla E 16: Configurar comandos

Parámetros	Valor Asignado	Descripción
define command{		[Inicia proceso de definición]
command_name	check-mikrotik-señal	[Define nombre de comando]
command_line	\$USER1\$/check_mikrotik_signal -H \$HOSTADDRESS\$ -c \$ARG1\$ -P 2c	[Define sintaxis de ejecución del comando con su respectivo plugin]
}		Finaliza proceso de definición

A continuación se describe cada plugin utilizado en la implementación de switches:

Tabla E 17: Descripción de sintaxis de plugins

Línea de comando	Sintaxis de plugins
command_line	\$USER1\$/check_ping -H \$HOSTADDRESS\$ -w \$ARG1\$ -c \$ARG2\$ -p 5
command_line	\$USER1\$/check_mikrotik_signal -H \$HOSTADDRESS\$ -C \$ARG1\$ -P 2c
command_line	\$USER1\$/check_mikrotik_users.pl -H \$HOSTADDRESS\$ -C \$ARG1\$ -w \$ARG2\$ -c \$ARG3\$ -P 2c
command_line	\$USER1\$/check_snmp -H \$HOSTADDRESS\$ -o \$ARG1\$ -C \$ARG2\$

8. Definición de servicios

Con la información descrita en el paso 7 se continúa con la definición de servicios que verificará el nuevo switch ingresado a Nagios dentro del directorio:

```
#nano
```

```
/usr/local/nagios/etc/objects/Enlaces_Inalambricos/enlace_mikrotik_imi.cfg
```

Tabla E 18: Definir servicios

Parámetros	Valor Asignado	Descripción
define service{		[Inicia proceso de definición]
use	generic-service-mikrotik	Define el nombre de plantilla a heredar
host_name	Enlace Mikrotik IMI	Define nombre del dispositivo
service_description	01. Mikrotik dBm	Define nombre del servicio a verificar
check_command	check_mikrotik_signal!imi	Define el comando que realiza la ejecución del servicio
}		Finaliza proceso de definición

A continuación se describe cada plugin con sus valores asignados en la línea `check_command`:

Tabla E 18: Descripción de valores asignados a plugins

check_command	Sintaxis	Descripción
check_ping!	200.0,20%!400.0,40%	Si el tiempo de ida y vuelta (RTT) de la respuesta PING es mayor que 200 ms (pero menor de 400 ms) Nagios marcará un estado de Advertencia y si el RTT es superior a 400 ms Nagios marcará un estado Crítico . Si mas de 20% (pero menos de 40% por ciento) de solicitudes de ping no reciben respuesta Nagios marcará un estado de Advertencia y si mas del 40% de solicitudes de ping no reciben respuesta Nagios marcará un estado Crítico .
check_mikrotik_signal!	-C imisnmp	Verifica el nivel de señal en dBm
check_mikrotik_users.pl!	-C imisnmp -w 20 -c 30	Verifica el número de clientes conectados y si sobrepasa de los 20 notificará como advertencia y si sobrepasa los 30 notificará como crítico.
check_snmp!	- o 1.3.6.1.2.1.25.2.3.1.3.1.131073 - C imisnmp	Verifica el estado de funcionamiento de la memoria principal y disco

E.2.3 Configuración de servidores Linux dentro de Nagios.

1. Ingresar a un terminal en modo root.

```
#su
```

```
#contraseña de superusuario
```

2. Se crea el nuevo archivo *serv_debbrepositorios.cfg* en los directorios de:

```
#nano
```

```
/usr/local/nagios/etc/objects/Servidores_Virtuales/serv_debbrepositorios.cfg
```

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

```
cfg_file=/usr/local/nagios/etc/objects/Servidores_Virtuales/
```

```
serv_debbrepositorios.cfg
```

3. Configuración de plantillas para servidores virtuales.

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 19: Plantilla para servidores virtuales

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	generic-virtual	Define nombre asignando a la plantilla
notifications_enabled	1	Define notificaciones: 1-Activa, 0-Desactiva
event_handler_enabled	1	Define control de eventos del sistema: 1-Activa, 0-Desactiva
flap_detection_enabled	1	Define detección de flapeo: 1-Activa, 0-Desactiva
process_perf_data	1	Define proceso de rendimiento: 1-Activa, 0-Desactiva
retain_status_information	1	Conservar la información de estado en los reinicios del programa: 1-Activa, 0-Desactiva
retain_nonstatus_information	1	Retiene la información sin estado en los reinicios del programa 1-Activa, 0-Desactiva]
notification_period	24x7	Define periodo de tiempo que enviará notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

Tabla E 20: Plantilla para servidores virtuales (1)

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	servidores-virtuales	Define nombre asignando a la plantilla
use	generic-virtual	Define nombre de la plantilla a heredar
check_period	24x7	Define periodo de chequeo
check_interval	5	Define intervalo de tiempo en minutos entre cada chequeo
retry_interval	1	Define reintentos de chequeo de estado en intervalos de minutos
max_check_attempts	10	Número de veces que chequea el comando, comprueba el estado Up/Down del dispositivo y después notifica
check_command	check-servidores-ping	Nombre del comando que comprueba el estado del dispositivo
notification_period	24x7	Nombre de la plantilla que especifica el periodo de notificación
notification_interval	5	Define periodo de tiempo entre cada notificación enviada
notification_options	d, r	Tipo de notificación a enviar d:down, r:recovery, u:unreachable
contacts	Administrador	Define nombre a quien notificará Nagios
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

4. Definición de servidor virtual

Ingresa al archivo para cambiar los valores en las líneas que están con negrita:

```
#nano
```

```
/usr/local/nagios/etc/objects/Servidores_Virtuales/serv_debbrepositorios.cfg
```

Tabla E 21: Definir servidores virtuales

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
use	servidores-virtuales	Define nombre de la plantilla a heredar
host_name	debbrepositorios	Define nombre del dispositivo
alias	Servidor de Repositorios	Define nombre descriptivo del dispositivo que aparece en la interfaz web
address	172.x.x.x	Define dirección IP del dispositivo
parent	HP BL 460 G6	Define el nombre del dispositivo al que pertenece
hostgroups	Servidores Virtuales	Define el nombre del grupo al que pertenece el dispositivo
icon_image	debian.gif	Define la imagen utilizada como icono en la interfaz web
statusmap_image	debian.gd2	Define la imagen utiliza en el mapa de red de la interfaz
}		Finaliza proceso de definición

5. Creación de grupos de servidores virtuales.

En el siguiente directorio:

```
#nano /usr/local/nagios/etc/objects/Servidores_Virtuales/hostgroups.cfg
```

Tabla E 22: Definir grupo de servidore virtuales

Parámetros	Valor Asignado	Descripción
define hostgroup {		Inicia proceso de definición
hostgroup_name	Servidores Virtuales	Define nombre del grupo
alias	Servidores-virtuales-imi	Define nombre descriptivo que aparece en la interfaz web
}		Finaliza proceso de definición

6. Configuración de plantillas para servicios.

Ingresar al archivo:

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 23: Plantilla para servicios de servidores virtuales

Parámetros	Valor Asignado	Descripción
define service{		[Inicia proceso de definición]
name	generic-service-virtuales	Definición de nombre de plantilla para servicios
active_checks_enabled	1	Define chequeo de servicio activos. 1: Activa, 0: Desactiva
passive_checks_enable	1	Define chequeo de servicio pasivos. 1: Activa, 0:Desactiva
check_freshness	0	Por default desactiva los chequeos pasivos de frescura
notifications_enabled	1	Notificaciones para los servicios. 1: Activa, 0: Desactiva
event_handler_enabled	1	Controlador de eventos para servicios. 1: Activa, 0: Desactiva]
flap_detection_enabled	1	Define la habilitación de flapeo. 1: Activa, 0: Desactiva

process_perf_data	1	Define procesamiento del rendimiento de los datos. 1: Activa, 0: Desactiva
retain_status_information	1	Almacena información sobre el estado de los servicios antes de un reinicio. 1: Activa, 0: Desactiva
is_volatile	0	Define este servicio como no volátil
check_period	24x7	Define el nombre de la plantilla con el periodo de tiempo para el chequeo
max_check_attempts	3	Define máxima cantidad de chequeos
normal_check_interval	3	Define intervalo de tiempo a programar los chequeos en (min)
retry_check_interval	3	Define intervalo de tiempo para un re-chequeo en (min)
contacts	Administrador	Define nombre de contacto
notification_options	w, u, c, r	Define cuando enviar notificaciones de w: warning, c: critical
notification_interval	5	Define intervalo de envío de notificación
notification_period	24x7	Define nombre de plantilla con el periodo para notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

7. Configuración de comandos

En el siguiente directorio configurar comandos para luego concatenarlos con la definición de servicios:

```
#nano /usr/local/nagios/etc/objects/commands.cfg
```

Tabla E 24: Configurar comandos

Parámetros	Valor Asignado	Descripción
define command{		[Inicia proceso de definición]
command_name	check-mikrotik-señal	[Define nombre de comando]
command_line	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$	[Define sintaxis de ejecución del comando con su respectivo plugin]
}		Finaliza proceso de definición

A continuación se describe cada plugin utilizado en la implementación de servidores Linux sean físicos o virtuales, dentro del directorio:

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

Tabla E 25: Descripción de sintaxis de plugins

Línea de comando	Sintaxis de plugins
command_line	<code>\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$</code>
command_line	<code>\$USER1\$/check_disk -w \$ARG1\$ -c \$ARG2\$ -p \$ARG3\$</code>
command_line	<code>\$USER1\$/check_swap -w \$ARG1\$ -c \$ARG2\$</code>
command_line	<code>\$USER1\$/check_snmp_mem.pl -H \$HOSTADDRESS\$ -c \$ARG1\$ -p 161 -w \$ARG2\$ -c \$ARG3\$</code>
command_line	<code>\$USER1\$/check_load -w \$ARG1\$ -c \$ARG2\$</code>

Tabla E 26: Descripción de sintaxis de plugins (1)

Línea de comando	Sintaxis de plugins
command[check_sda1] =	<code>/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /</code>
command[check_swap] =	<code>/usr/local/nagios/libexec/check_swap -w 20% -c 10%</code>
command[check_mem] =	<code>/usr/local/nagios/libexec/check_snmp_mem.pl -H \$HOSTADDRESS\$ -C imi -w 70,75 -c 80, 85</code>
command[check_load] =	<code>/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20</code>

8. Definición de servicios

Con la información descrita en el paso 7 se continúa con la definición de servicios que verificará el nuevo switch ingresado a Nagios dentro del directorio:

```
#nano
```

```
/usr/local/nagios/etc/objects/Servidores_Virtuales/serv_debbrepositorios.cfg
```

Tabla E 27: Definir servicios

Parámetros	Valor Asignado	Descripción
<code>define service{</code>		[Inicia proceso de definición]
<code>use</code>	<code>generic-service-virtuales</code>	Define el nombre de plantilla a heredar
<code>host_name</code>	<code>debbrepositorios</code>	Define nombre del dispositivo
<code>service_description</code>	<code>01. Espacio de Disco</code>	Define nombre del servicio a verificar
<code>check_command</code>	<code>check_nrpe!check_sda1!20%!10%!/</code>	Define el comando que realiza la ejecución del servicio
<code>}</code>		Finaliza proceso de definición

A continuación se describe cada plugin con sus valores asignados en la línea `check_command`:

Tabla E 28: Descripción de valores asignados a plugins

check_command	Sintaxis	Descripción
check_ping!	200.0,20%!400.0,40%	Si el tiempo de ida y vuelta (RTT) de la respuesta PING es mayor que 200 ms (pero menor de 400 ms) Nagios marcará un estado de Advertencia y si el RTT es superior a 400 ms Nagios marcará un estado Crítico . Si mas de 20% (pero menos de 40% por ciento) de solicitudes de ping no reciben respuesta Nagios marcará un estado de Advertencia y si mas del 40% de solicitudes de ping no reciben respuesta Nagios marcará un estado Crítico .
check_nrpe!	check_sda!20%!10%!/	Verifica el espacio de disco y Nagios marcará un estado de Advertencia cuando tenga solamente un 20% libre y un estado Crítico cuando tenga un 10% libre.
check_nrpe!	check_swap!20!10!	Verifica el uso de memoria Swap y Nagios marcará un estado de Advertencia cuando tenga solamente un 20% libre y un estado Crítico cuando tenga un 10% libre.
check_nrpe!	check_mem!	Verifica el uso de memoria Swap y Nagios marcará un estado de Advertencia cuando tenga un 70% de uso y un estado Crítico cuando tenga un 80% de uso.
check_nrpe!	check_load!	Verifica el uso de CPU y Nagios marcará un estado de Advertencia si el uso es mayor de 80 y un estado Crítico si es mayor de 90%

E.2.4 Configuración de servidores Windows dentro de Nagios.

1. Ingresar a un terminal en modo root.

```
#su
```

```
#contraseña de superusuario
```

2. Se crea el nuevo archivo **serv07_Olympo.cfg** en los directorios de:

```
#nano /usr/local/nagios/etc/objects/Servidores_Fisicos/serv07_Olympo.cfg
```

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

```
cfg_file=/usr/local/nagios/etc/objects/Servidores_Fisicos/serv07_Olympo.cfg
```

3. Configuración de plantillas para servidores Windows

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 29: Plantilla para servidores físicos

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	generic-fisicos	Define nombre asignando a la plantilla
notifications_enabled	1	Define notificaciones: 1-Activa, 0-Desactiva
event_handler_enabled	1	Define control de eventos del sistema: 1-Activa, 0-Desactiva
flap_detection_enabled	1	Define detección de flapeo: 1-Activa, 0-Desactiva
process_perf_data	1	Define proceso de rendimiento: 1-Activa, 0-Desactiva
retain_status_information	1	Conservar la información de estado en los reinicios del programa: 1-Activa, 0-Desactiva
retain_nonstatus_information	1	Retiene la información sin estado en los reinicios del programa 1-Activa, 0-Desactiva]
notification_period	24x7	Define periodo de tiempo que enviará notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

Tabla E 30: Plantilla para servidores físicos (1)

Parámetros	Valor Asignado	Descripción
define host{		Inicia proceso de definición
name	generic-serv-fisicos	Define nombre asignando a la plantilla
use	generic-fisicos	Define nombre de la plantilla a heredar
check_period	24x7	Define periodo de chequeo
check_interval	5	Define intervalo de tiempo en minutos entre cada chequeo
retry_interval	1	Define reintentos de chequeo de estado en intervalos de minutos
max_check_attempts	10	Número de veces que chequea el comando, comprueba el estado Up/Down del dispositivo y después notifica
check_command	check-fisicos-ping	Nombre del comando que comprueba el estado del dispositivo
notification_period	24x7	Nombre de la plantilla que especifica el periodo de notificación
notification_interval	5	Define periodo de tiempo entre cada notificación enviada
notification_options	d, r	Tipo de notificación a enviar d:down, r:recovery, u:unreachable
contacts	Administrador	Define nombre a quien notificará Nagios
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

4. Definición de servidores Windows

Ingresa al archivo para cambiar los valores en las líneas que están con negrita:

```
#nano /usr/local/nagios/etc/objects/Servidores_Fisicos/serv07_Olympo.cfg
```

Tabla E 31: Definir servidor Windows

Parámetros	Valor Asignado	Descripción
define host{		[Inicia proceso de definición]
use	generic-serv-fisicos	Define nombre de la plantilla a heredar
host_name	ser07_Olympo	Define nombre del dispositivo
alias	Servidor Olympo	Define nombre descriptivo del dispositivo que aparece en la interfaz web
address	172.x.x.x	[Define dirección IP del dispositivo
hostgroups	Servidores Fisicos	Define en nombre del grupo al que pertenece el dispositivo
icon_image	win40.gif	Define la imagen utilizada como icono en la interfaz web
statusmap_image	win40.gd2	Define la imagen utiliza en el mapa de red de la interfaz
}		Finaliza proceso de definición

5. Creación de grupos de servidores físicos.

Dentro del directorio:

```
#nano /usr/local/nagios/etc/objects/Servidores_Fisicos/hostgroups.cfg
```

Tabla E 32: Crear grupo de servidores físicos

Parámetros	Valor Asignado	Descripción
define hostgroup {		Inicia proceso de definición
hostgroup_name	Servidore Fisicos	Define nombre del grupo
alias	Servidores-fisicos-imi	Define nombre descriptivo que aparece en la interfaz web
}		Finaliza proceso de definición

6. Configuración de plantillas para servicios.

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 33: Plantilla para servicios de servidores virtuales

Parámetros	Valor Asignado	Descripción
define service{		[Inicia proceso de definición]
name	generic-service-fisicos	Definición de nombre de plantilla para servicios
active_checks_enabled	1	Define chequeo de servicio activos. 1: Activa, 0: Desactiva
passive_checks_enable	1	Define chequeo de servicio pasivos. 1: Activa, 0:Desactiva
check_freshness	0	Por default desactiva los chequeos pasivos de frescura
notifications_enabled	1	Notificaciones para los servicios. 1: Activa, 0: Desactiva
event_handler_enabled	1	Controlador de eventos para servicios. 1: Activa, 0: Desactiva]
flap_detection_enabled	1	Define la habilitación de flapeo. 1: Activa, 0: Desactiva
process_perf_data	1	Define procesamiento del rendimiento de los datos. 1: Activa, 0: Desactiva
retain_status_information	1	Almacena información sobre el estado de los servicios

		antes de un reinicio. 1: Activa, 0: Desactiva
is_volatile	0	Define este servicio como no volátil
check_period	24x7	Define el nombre de la plantilla con el periodo de tiempo para el chequeo
max_check_attempts	3	Define máxima cantidad de chequeos
normal_check_interval	3	Define intervalo de tiempo a programar los chequeos en (min)
retry_check_interval	3	Define intervalo de tiempo para un re-chequeo en (min)
contacts	Administrador	Define nombre de contacto
notification_options	w, u, c, r	Define cuando enviar notificaciones de w: warning, c: critical
notification_interval	5	Define intervalo de envío de notificación
notification_period	24x7	Define nombre de plantilla con el periodo para notificaciones
register	0	Solo define una plantilla no un verdadero dispositivo
}		Finaliza proceso de definición

7. Configuración de comandos

En el siguiente directorio configurar comandos para luego concatenarlos con la definición de servicios:

```
#nano /usr/local/nagios/etc/objects/commands.cfg
```

Tabla E 34: Configurar comandos

Parámetros	Valor Asignado	Descripción
define command{		[Inicia proceso de definición]
command_name	check_nt	[Define nombre de comando]
command_line	\$USER1\$/check_nt -H \$HOSTADDRESS\$ -p 1248 -v \$ARG1\$ \$ARG2\$	[Define sintaxis de ejecución del comando con su respectivo plugin]
}		Finaliza proceso de definición

8. Definición de servicios

Con la información descrita en el paso 7 se continúa con la definición de servicios que verificará el nuevo switch ingresado a Nagios dentro del directorio:

```
#nano /usr/local/nagios/etc/objects/Servidores_Fisicos/serv07_Olympo.cfg
```

Tabla E 35: Plantilla para servicios de servidores virtuales

Parámetros	Valor Asignado	Descripción
define service{		[Inicia proceso de definición]
use	generic-service-fisicos	Define el nombre de plantilla a heredar
host_name	serv07_Olympo	Define nombre del dispositivo
service_description	01. Memoria RAM	Define nombre del servicio a verificar
check_command	check_nt!MEMUSE! -w 80 -c 90	Define el comando que realiza la ejecución del servicio
}		Finaliza proceso de definición

A continuación se describe cada plugin con sus valores asignados en la línea check_command:

Tabla E 36: Plantilla para servicios de servidores virtuales

check_command	Sintaxis	Descripción
check_ping!	200.0,20%!400.0,40%	Si el tiempo de ida y vuelta (RTT) de la respuesta PING es mayor que 200 ms (pero menor de 400 ms) Nagios marcará un estado de Advertencia y si el RTT es superior a 400 ms Nagios marcará un estado Crítico . Si mas de 20% (pero menos de 40% por ciento) de solicitudes de ping no reciben respuesta Nagios marcará un estado de Advertencia y si mas del 40% de solicitudes de pig no reciben respuesta Nagios marcará un estado Crítico .
check_nt!	CPULOAD! -l 5,70,75,10,80,85	Verifica el uso de CPU y Nagios marcará como estado de Advertencia cuando el uso este en el 75% y Crítico cuando el uso este en 85%.
check_nt!	MEMUSE! w 80 -c 90	Verifica el uso de memoria RAM y Nagios marcará un estado de Advertencia cuando tenga solamente un 20% libre y un estado Crítico cuando tenga un 10% libre.
check_nt!	USEDISKSPACE! -l C -w 80 -c 90	Verifica el espacio de disco y Nagios marcará un estado de Advertencia cuando tenga solamente un 20% libre y un estado Crítico cuando tenga un 10% libre.

F.2.5 Configuración de contactos

1. Configuración de plantilla para contactos

Para que Nagios pueda enviar notificaciones al administrador de la red configurar otra plantilla para contactos en el mismo directorio:

```
#nano /usr/local/nagios/etc/objects/templates.cfg
```

Tabla E 37: Plantilla para contactos

Parámetros	Valor Asignado	Descripción
define contact{		Inicia proceso de definición
name	generic-contact-alertas	Nombre asignado a la plantilla de contacto
service_notification_period	24x7	Periodo de tiempo de notificaciones de servicios
host_notification_period	24x7	Periodo de tiempo de notificaciones para dispositivos
service_notification_options	w,u,c,r,s	Opciones de notificaciones por servicio
host_notification_options	d,u,r,f,s	Opciones de notificaciones por dispositivo
service_notification_commands	notify-service-by-email,notify-service-by-sms	Comando de notificaciones a utilizar por el servicio
host_notification_commands	notify-service-by-email,notify-service-by-sms	Comando de notificaciones a utilizar por el dispositivo
}		Finaliza proceso de definición

2. Definición de comandos

```
#nano /usr/local/nagios/etc/objects/commands.cfg
```

Tabla E 38: Configurar comandos de notificación

Parámetros	Valor Asignado	Descripción
define command{		[Inicia proceso de definición]
command_name	notify-host-by-email	[Define nombre de comando]
command_line	/usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: \$NOTIFICATIONTYPE\$\nHost: \$HOSTNAME\$\nState: \$HOSTSTATES\$\nAddress:	[Define sintaxis de ejecución del comando con su respectivo plugin]
}		Finaliza proceso de definición

3. Definición de contacto

En el archivo *#nano /usr/local/nagios/etc/objects/contacts.cfg*, se define el número de teléfono celular y cuenta de correo electrónico del administrador a quien se le envía las notificaciones:

Tabla E 39: Definición de contacto

Parámetros	Valor Asignado	Descripción
define contact{		Inicia proceso de definición
contact_name	Administrador	Define nombre de contacto
use	generic-contact-alertas	Define nombre de plantilla de contacto a utilizar
alias	Administrador Nagios	Define nombre descriptivo
pager	+59399xxxxxxx	Define el número de teléfono celular del contacto
email	nagiosgadi@gmail.com	Define cuenta de correo electrónico del contacto
}		Finaliza proceso de definición

F.2.6 Configuración de tiempos

En el archivo ubicado en el directorio:

#nano /usr/local/nagios/etc/objects/timeperiods.cfg

Tabla E 40: Defición de tiempo

Parámetros	Valor Asignado	Descripción
define timeperiod{		Inicia proceso de definición
timeperiod_name	24x7	Define nombre de tiempo
alias	24 Horas del día, 7 días de la semana	Define nombre descriptivo
sunday	00:00 – 24:00	Define horario del día Domingo
monday	00:00 – 24:00	Define horario del día Lunes
tuesday	00:00 – 24:00	Define horario del día Martes
wednesday	00:00 – 24:00	Define horario del día Miércoles
thursday	00:00 – 24:00	Define horario del día Jueves
friday	00:00 – 24:00	Define horario del día Viernes
saturday	00:00 – 24:00	Define horario del día Sábado
}		Finaliza proceso de definición

E.3. Interfaz Web de Nagios Core

Abrir un navegador para ingresar a la interfaz de gestión de Nagios e ingresar la dirección IP que está asignada al servidor de la siguiente forma *http://172.x.x.x/nagios* e ingresar su respectivo nombre de usuario y su contraseña como se observa en la Figura E 41:

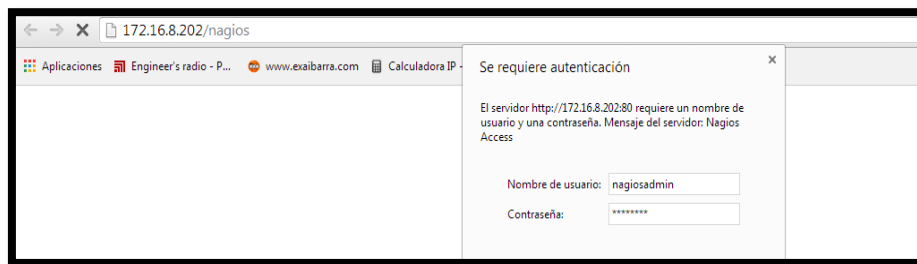


Figura E 41. Autenticación para ingresar al servidor Nagios

Después de haber realizado la autenticación ingresar a la interfaz Web de Nagios Core como se indica en la Figura E 42, donde le permite al administrador supervisar el estado actual de la red. Mediante CGI y scripts PHP permite una visión del rendimiento de todos los hosts y servicios que se están monitoreando. A continuación se explica cada una de las opciones que presenta el software de gestión en el menú que se ubica en la parte izquierda.



Figura E 42. Interfaz Web de Nagios Core 4.0.4

1. Estado actual / Current Status

La pantalla de la Figura E 43 ofrece un resumen sobre el estado actual de funcionamiento tanto de los hosts y servicios.

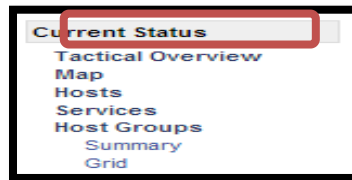


Figura E 43. Vínculo Current Status

a) Panorama táctico / Tactical Overview

Al ingresar en la opción **Tactical Overview** aparece la pantalla que se muestra en la Figura E 44 donde se puede observar un resumen del monitoreo.

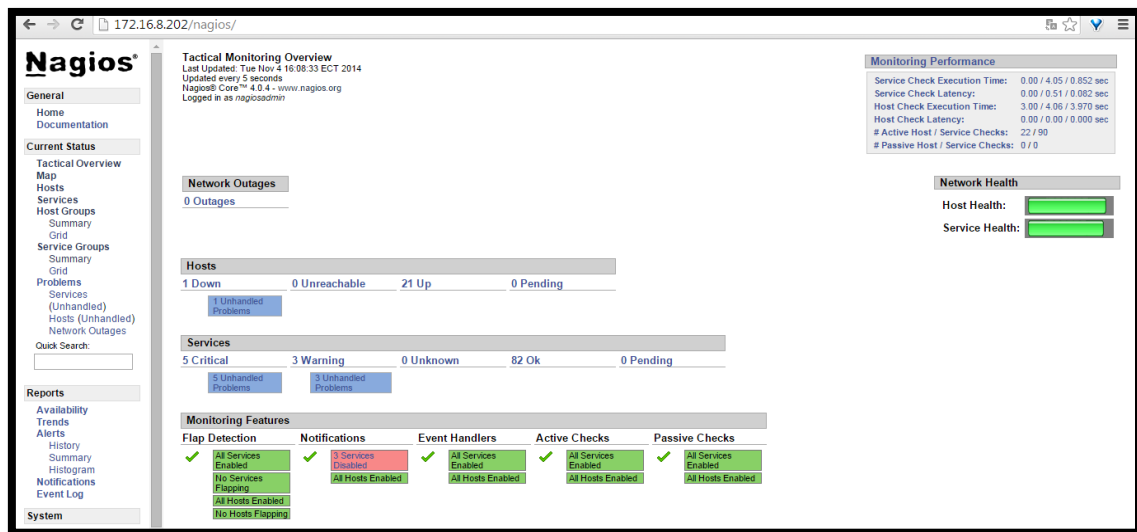


Figura E 44. Resumen del estado de la red

b) Mapa / Map

Al ingresar en la opción **Map** aparece la pantalla que indica la Figura E 45 donde presenta el mapa de los dispositivos que se están monitoreando, donde se observa claramente los que estén activos e inactivos.

c) Equipos / Host

La Figura E 45 indica la lista de los dispositivos gestionados por Nagios donde se observa los que estén activos e inactivos y al dar click en alguno de ellos podrá observar los servicios que cada uno tiene configurado.

Host	Status	Last Check	Duration	Status Information
SW-2960-RACK2-01	UP	08-31-2014 08:17:23	81d 20h 9m 32s	PING OK - Packet loss = 0%, RTA = 2.86 ms
SW-2960POE-CULT-S1	UP	08-31-2014 08:16:03	65d 13h 48m 39s	PING OK - Packet loss = 0%, RTA = 0.78 ms
SW-2960POE-RACK2-01	UP	08-31-2014 08:17:25	81d 20h 9m 30s	PING OK - Packet loss = 0%, RTA = 0.80 ms
SW-2960POE-RACKS1-03-EA	UP	08-31-2014 08:17:26	81d 20h 9m 26s	PING OK - Packet loss = 0%, RTA = 0.81 ms
SW-4500-CORE	UP	08-31-2014 08:20:23	81d 20h 9m 30s	PING OK - Packet loss = 0%, RTA = 1.53 ms
Server-Nagios	UP	08-31-2014 08:18:41	215d 6h 4m 26s	PING OK - Packet loss = 0%, RTA = 0.03 ms
deb103	UP	08-31-2014 08:17:33	98d 22h 38m 4s	PING OK - Packet loss = 0%, RTA = 0.37 ms
debbfirewall	UP	08-31-2014 08:20:22	128d 2h 52m 10s	PING OK - Packet loss = 0%, RTA = 1.27 ms
deblade01	UP	08-31-2014 08:19:47	102d 0h 7m 39s	PING OK - Packet loss = 0%, RTA = 0.28 ms
deblade03	UP	08-31-2014 08:19:49	128d 2h 53m 44s+	PING OK - Packet loss = 0%, RTA = 0.25 ms
deblade04	UP	08-31-2014 08:16:49	127d 3h 54m 59s	PING OK - Packet loss = 0%, RTA = 0.41 ms
debbquipux	DOWN	08-31-2014 08:20:25	127d 3h 54m 56s	CRITICAL - Host Unreachable (172.16.8.89)
debbrepositorios	UP	08-31-2014 08:20:22	128d 2h 51m 20s	PING OK - Packet loss = 0%, RTA = 1.88 ms
debbservicios	UP	08-31-2014 08:16:55	128d 2h 51m 37s	PING OK - Packet loss = 0%, RTA = 0.70 ms
debbweb	UP	08-31-2014 08:20:09	127d 3h 54m 55s	PING OK - Packet loss = 0%, RTA = 0.74 ms
debbdocumental	UP	08-31-2014 08:18:53	146d 1h 15m 57s	PING OK - Packet loss = 0%, RTA = 0.71 ms
debbmapserver	UP	08-31-2014 08:17:14	127d 3h 54m 55s	PING OK - Packet loss = 0%, RTA = 0.76 ms
debbpostgis	UP	08-31-2014 08:20:23	127d 2h 52m 45s	PING OK - Packet loss = 0%, RTA = 1.78 ms
freenas	UP	08-31-2014 08:16:10	104d 17h 53m 55s	PING OK - Packet loss = 0%, RTA = 0.75 ms
ncorreo	UP	08-31-2014 08:20:22	67d 5h 39m 39s	PING OK - Packet loss = 0%, RTA = 0.57 ms
pg01	UP	08-31-2014 08:17:29	98d 22h 38m 4s	PING OK - Packet loss = 0%, RTA = 0.43 ms
svea2960p101-EA	UP	08-31-2014 08:17:03	98d 22h 37m 41s	PING OK - Packet loss = 0%, RTA = 1.42 ms

Figura E 45. Listado de los equipos monitoreados

d) Services / Servicios

La Figura E 46 indica todos los servicios que se han configurado en cada dispositivo monitoreado, cada servicio indica su estado de criticidad (OK, WARNING, CRITICAL, UNKNOWN):

Host	Service	Status	Start Time	Duration	Attempts	Details
SERV/DOR HP DL 380 G5	01. PING	OK	04-01-2015 09:59:48	0d 0h 30m 5s	1/4	PING OK - Packet loss = 0%, RTA = 1.05 ms
SW-2960-RACK2-01	01. PING	OK	04-01-2015 10:04:35	14d 16h 49m 4s	1/3	PING OK - Packet loss = 0%, RTA = 0.82 ms
	02. Memoria RAM	OK	04-01-2015 10:04:14	14d 16h 48m 39s	1/3	OK: Driver text: valid, Used: 40B Free: 1048536B (99%)/ I/O: valid, Used: 1647532B Free: 2546772B (60%)/ Processor: valid, Used: 9509024B Free: 23979824B (71%)
	03. Memoria Flash	OK	04-01-2015 10:04:35	14d 16h 49m 31s	1/3	OK: Onboard system FLASH: Size: 27996208 Free: 16785408 (59%) Status: available VPP: installed!
	04. Carga de CPU	OK	04-01-2015 10:03:55	14d 16h 48m 57s	1/3	OK: CPU0: 6% 6% 6% !
	05. Ventilador	OK	04-01-2015 10:04:37	14d 16h 49m 3s	1/3	OK: Switch#1, Fan#1: normal
	06. Fuente de Alimentacion	OK	04-01-2015 10:04:33	14d 16h 48m 35s	1/3	PS: OK - 1 PS are running all good
SW-2960-RACK2-02	01. PING	OK	04-01-2015 09:59:59	13d 18h 38m 22s	1/3	PING OK - Packet loss = 0%, RTA = 1.29 ms
	02. Memoria RAM	OK	04-01-2015 10:04:14	13d 18h 37m 53s	1/3	OK: Driver text: valid, Used: 40B Free: 1048536B (99%)/ I/O: valid, Used: 1649396B Free: 2544908B (60%)/ Processor: valid, Used: 9527132B Free: 23961716B (71%)
	03. Memoria Flash	OK	04-01-2015 10:03:54	13d 18h 37m 54s	1/3	OK: Onboard system FLASH: Size: 27996208 Free: 16785408 (59%) Status: available VPP: installed!
	04. Carga de CPU	OK	04-01-2015 10:04:15	3d 13h 23m 25s	1/3	OK: CPU0: 6% 6% 6% !
	05. Ventilador	OK	04-01-2015 10:04:33	13d 18h 38m 21s	1/3	OK: Switch#1, Fan#1: normal
	06. Fuente de Alimentacion	OK	04-01-2015 10:04:34	13d 18h 37m 52s	1/3	PS: OK - 1 PS are running all good
SW-2960POE-CULT-01	01. PING	OK	04-01-2015 10:04:39	0d 18h 20m 29s	1/3	PING OK - Packet loss = 0%, RTA = 1.00 ms
	02. Memoria RAM	OK	04-01-2015 10:04:01	12d 22h 35m 43s	1/3	OK: Driver text: valid, Used: 40B Free: 1048536B (99%)/ I/O: valid, Used: 1641672B Free: 2544440B (60%)/ Processor: valid, Used: 9004856B Free: 28147884B (74%)
	03. Memoria Flash	OK	04-01-2015 10:04:14	12d 22h 35m 57s	1/3	OK: Onboard system FLASH: Size: 27996208 Free: 17231360 (61%) Status: available VPP: installed!
	04. Carga de CPU	OK	04-01-2015 10:04:10	12d 22h 35m 42s	1/3	OK: CPU0: 6% 6% 6% !
	05. Ventilador	OK	04-01-2015 10:04:18	12d 22h 36m 13s	1/3	OK: Switch#1, Fan#1: normal
	06. Fuente de Alimentacion	OK	04-01-2015 10:03:51	13d 18h 34m 16s	1/3	PS: OK - 1 PS are running all good
SW-2960POE-RACK1-02	01. PING	OK	04-01-2015 10:00:40	6d 18h 44m 7s	1/3	PING OK - Packet loss = 0%, RTA = 3.09 ms
	02. Memoria RAM	OK	04-01-2015 10:04:15	6d 18h 30m 45s	1/3	OK: Driver text: valid, Used: 40B Free: 1048536B (99%)/ I/O: valid, Used: 1666012B Free: 2528232B (60%)/ Processor: valid, Used: 11233260B Free: 19105660B (62%)
	03. Memoria Flash	OK	04-01-2015 10:04:35	6d 18h 30m 13s	1/3	OK: Onboard system FLASH: Size: 27996208 Free: 16800384 (57%) Status: available VPP: installed!
	04. Carga de CPU	OK	04-01-2015 10:04:09	6d 18h 30m 40s	1/3	OK: CPU0: 23% 25% 25% !
	05. Ventilador	OK	04-01-2015 10:03:58	6d 18h 30m 5s	1/3	OK: Switch#1, Fan#1: normal
	06. Fuente de Alimentacion	OK	04-01-2015 10:04:03	6d 18h 44m 6s	1/3	PS: OK - 1 PS are running all good
SW-2960POE-RACK2-01	01. PING	OK	04-01-2015 10:04:17	13d 18h 30m 52s	1/3	PING OK - Packet loss = 0%, RTA = 5.06 ms
	02. Memoria RAM	OK	04-01-2015 10:04:34	13d 18h 32m 7s	1/3	OK: Driver text: valid, Used: 40B Free: 1048536B (99%)/ I/O: valid, Used: 1682500B Free: 2531804B (60%)/ Processor: valid, Used: 11214232B Free: 19125888B (63%)

Figura E 46. Servicios de los dispositivos monitoreados

e) Grupos de equipos / Hostgroup

La Figura E 47 indica los grupos de dispositivos configurados de acuerdo a sus características de funcionamiento.

Current Network Status				Host Status Totals				Service Status Totals				
Last Updated: Tue Nov 4 16:10:20 ECT 2014 Updated every 5 seconds Nagios® Core™ 4.0.4 - www.nagios.org Logged in as nagiosadmin				Up	Down	Unreachable	Pending	Ok	Warning	Unknown	Critical	Pending
				21	1	0	0	82	3	0	5	0
View Service Status Detail For All Host Groups View Host Status Detail For All Host Groups View Status Summary For All Host Groups View Status Grid For All Host Groups				All Problems		All Types		All Problems		All Types		
				1	22			8	90			
Service Overview For All Host Groups												
servidores-fisicos-imi (serv-fisicos)				servidores-virtuales-imi (serv-virtuales)				switch-cisco-imi (switches-cisco)				
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions	
deblade01	UP	No matching services	[Icons]	Servidor-Nagios	UP	6 OK	[Icons]	SW-2960-RACK2-01	UP	6 OK	[Icons]	
deblade03	UP	No matching services	[Icons]	deb103	UP	3 OK	[Icons]	SW-2960POE-CULT-01	UP	6 OK	[Icons]	
deblade04	UP	No matching services	[Icons]	debbfirewall	UP	2 OK	[Icons]	SW-2960POE-RACK2-01	UP	6 OK	[Icons]	
pg01	UP	3 OK	[Icons]	debbquipux	DOWN	3 OK	[Icons]	SW-2960POE-RACKS1-03-EA	UP	6 OK	[Icons]	
				debbrepositorios	UP	2 OK	[Icons]	SW-4500-CORE	UP	15 OK	[Icons]	
				debbrepositorios	UP	1 WARNING	[Icons]	swea2960p101-EA	UP	4 CRITICAL	[Icons]	
				debbweb	UP	4 OK	[Icons]					
				debdocumental	UP	3 OK	[Icons]					
				debmappoint	UP	3 OK	[Icons]					
				debpostgis	UP	3 OK	[Icons]					
				freenas	UP	No matching services	[Icons]					
				ncorreo	UP	2 OK	[Icons]					
					UP	1 WARNING	[Icons]					

Figura E 47. Servicios de los dispositivos monitoreados

f) Resumen / Summary

En la Figura E 48 se observa un resumen del estado del grupo de host y servicios

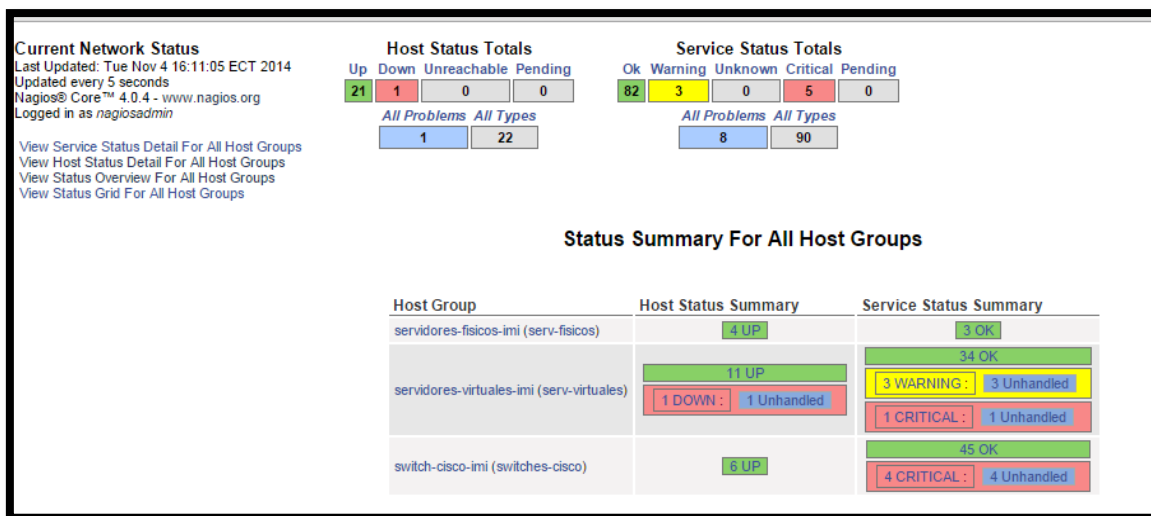


Figura E 48. Grupos de dispositivos monitoreados

g) Red / Grid

La Figura E 49 muestra el estado de todos los dispositivos gestionados en su orden de grupos en el que se encuentran.

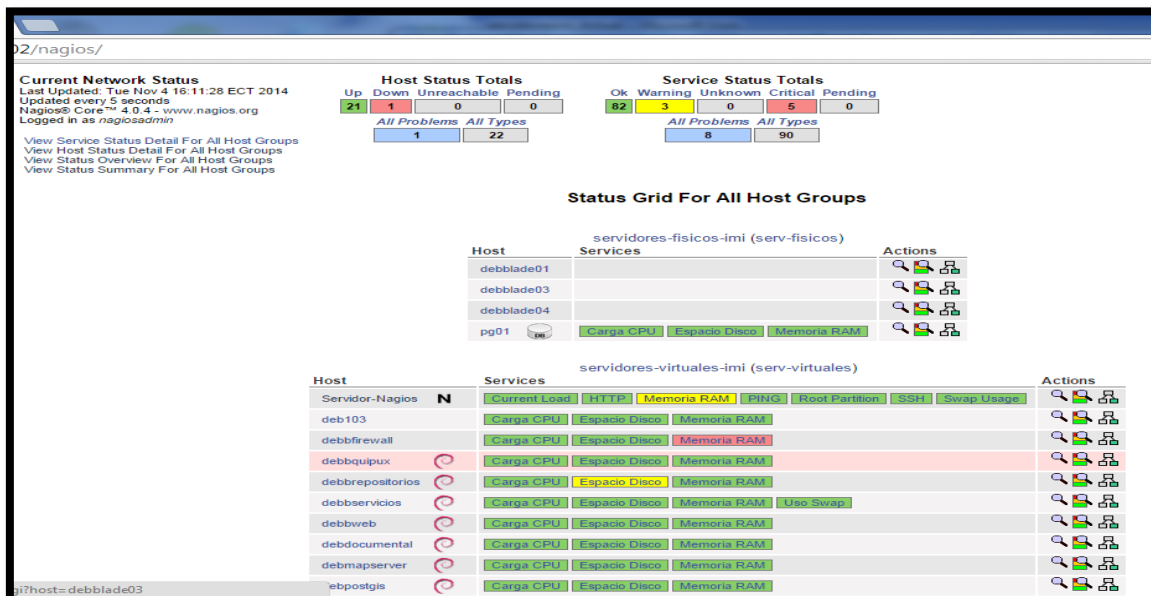


Figura E 49. Servicios monitoreados

h) Problemas / Problem

La Figura E 50 muestra una lista de los equipos que se encuentran en un estado (CRITICAL o WARNING) con su respectivo servicio.

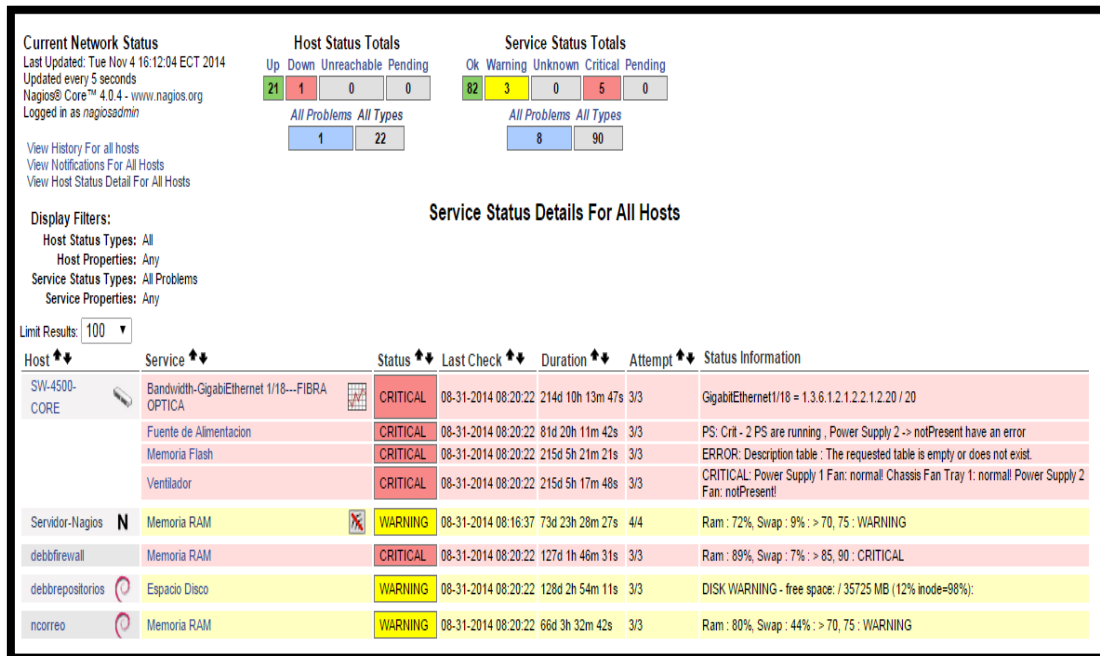


Figura E 50: Dispositivos en problemas

2. Reportes / Reports

Al ingresar en cada vínculo de la Figura E 51 Nagios presenta un resumen sobre el estado actual de funcionamiento tanto de hosts como servicios, presenta una fácil visualización e interpretación de informes de disponibilidad.

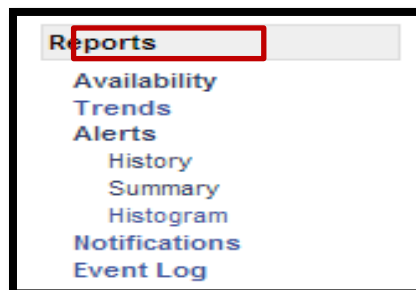
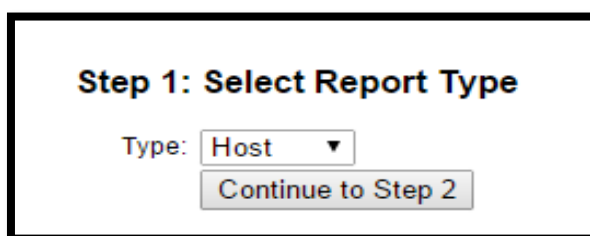


Figura E 51. Reportes

a) Disponibilidad / Availability

Este vínculo muestra el tiempo de actividad, estadísticas de un dispositivo, de un grupo de dispositivos, servicio es útil como una métrica rápida de disponibilidad general, para cumplir con los términos de un acuerdo de nivel de servicio.

1. Seleccionar el tipo de informe que se quiere generar sea para un hosts, hostGroup, servicio:

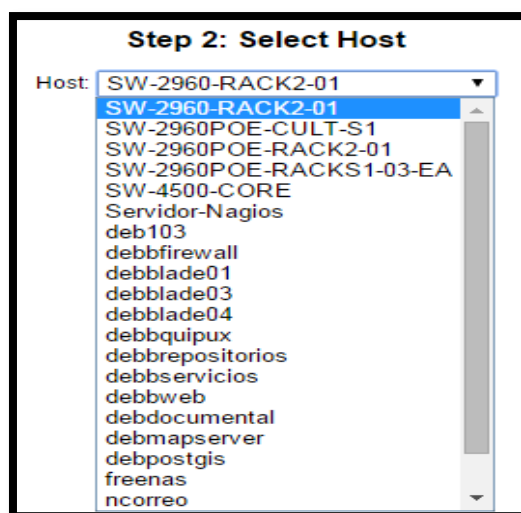


Step 1: Select Report Type

Type: ▼

Figura E 52. Seleccionar dispositivos o servicios

2. Seleccionar que dispositivo o servicio específico sobre el que se desea sacar el informe, o eventualmente optar por ejecutar por todos los host, hostgroups, servicios:



Step 2: Select Host

Host: ▼

- SW-2960-RACK2-01
- SW-2960POE-CULT-S1
- SW-2960POE-RACK2-01
- SW-2960POE-RACKS1-03-EA
- SW-4500-CORE
- Servidor-Nagios
- deb103
- debbfirewall
- deblade01
- deblade03
- deblade04
- debbquipux
- debbrepositorios
- debbservicios
- debbweb
- debdocumental
- debmapsver
- debpostgis
- frenas
- ncorreo

Figura E 54. Seleccionar dispositivo o servicio específico

3. La Figura E 55 define algunas opciones para el informe y hacer clic en crear informe:

Step 3: Select Report Options

Report period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Host State:

Backtracked Archives (To Scan For Initial States):

Suppress image map:

Suppress popups:

Figura E 55. Crear informe de disponibilidad

Tabla E 41: Descripción de Reporte

Parámetro	Descripción	Descripción (1)
Report period	Today, Last 24 Hours, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last 31 Days, Last Month, This Year, Last Year o Custom Report Period	Todos los días, últimas 24 horas, esta semana, últimos 7 días, última semana, este mes, últimos 31 días, último mes, este año, último año o reporte de tiempo personalizado.
If Custom	Start Date (inclusive)	Fecha inicio (completo)
Report Period	End Date (inclusive)	Fecha fin (completo)

Anexo F: Base de Datos para la Gestión de Fallos

A continuación se presenta una base de datos de los posibles problemas que pueden presentar los dispositivos de la red del GAD-Ibarra, los cuales provocan que un servicio sobrepase sus niveles normales de funcionamiento. Después de haber realizado el monitoreo por diez meses se ha tomado como guía los problemas que se pueden repetir en un futuro.

F.1. Fallos producidos en Switches.

F.1.1. Fallos que presentan un estado de advertencia:

Se genera este estado cuando se presenta una alerta de color amarillo y debe dirigirse a los siguientes pasos:

1. Detectar

Detecta que algunos switch están sobre los umbrales establecidos de advertencia lo que quiere decir que se debe tomar medidas de precaución antes de que los umbrales pasen a un estado crítico.

2. Aislar y Diagnosticar

El dispositivo presenta estados de advertencia para los siguientes parámetros: carga de CPU, memoria RAM, memoria flash, fuente de alimentación, ventiladores, interfaces de red.

F.1.2. Fallos que presentan un estado Crítico.

Cuando se presente este tipo de alerta se procede a realizar los siguientes pasos:

1. Detectar

Se identifica el dispositivo que ha presentado este estado.

2. Aislar

Cuando el dispositivo presenta una alerta de color **ROJO** representa un estado crítico donde pueden suceder por dos situaciones:

- ✓ El dispositivo esta abajo es decir está en estado **DOWN** o en estado **UNREACHABLE** (INESTABLE), por lo que ha perdido conectividad no responde a ninguna petición de PING.


SW-2960POE-RACKS1-03-EA	 DOWN	04-01-2015 10:24:50	29d 23h 31m 17s	PING CRITICAL - Packet loss = 100%
-------------------------	--	---------------------	-----------------	------------------------------------

Figura F 1. Representa estado DOWN

- ✓ El dispositivo puede presentar estados críticos de: carga de CPU, memoria RAM, memoria Flash, fuente de alimentación ó ventiladores.

05. Ventilador	CRITICAL	04-01-2015 10:23:53	15d 0h 13m 31s	3/3	CRITICAL: Power Supply 1 Fan: normal Chassis Fan Tray 1: normal Power Supply 2 Fan: notPresent!
06. Fuente de Alimentacion	CRITICAL	04-01-2015 10:24:15	15d 0h 13m 11s	3/3	PS: Crit - 2 PS are running , Power Supply 2 -> notPresent have an error

Figura F 2. Representa estado CRÍTICO

3. Diagnosticar

- ✓ Una de las razones que provoca un elevado consumo de carga de CPU es la presencia de broadcast, debido a que se reenvían las mismas tramas constantemente entre todos los switches en el bucle, la CPU del switch debe procesar una gran cantidad de datos, esto disminuye el rendimiento del switch cuando llega tráfico legítimo.
- ✓ El problema que provoca el broadcast es realmente considerable porque un host atrapado en un bucle de red es inaccesible para otros hosts de la red. Además, debido a los constantes cambios en la tabla de direcciones MAC, el switch no sabe cuál es el puerto por el que debe reenviar las tramas de unidifusión.

- ✓ También la presencia de broadcast inunda la red utilizando ancho de banda innecesariamente.
- ✓ Otro de los problemas que puede causar un elevado consumo de CPU es que SNMP este continuamente peticionando grandes cantidades de información.
- ✓ Fallos que tiene origen en una mala configuración del entorno como puede ser spanning-tree defectuosos, enlaces redundantes, port mirroring, etc. En establecidas ocasiones puede tratarse de ataques introducidos por terceros que pretenden dejar sin servicio mediante un ataque DoS, explorar tráfico mediante envenenamiento ARP.

4. Corregir

- ✓ Al reducir el tamaño del dominio de Broadcast, los dispositivos de red funcionan más eficazmente.
- ✓ Se procederá a corregir mediante troubleshooting de switch en el caso de CISCO con los siguientes comandos para reconocer que procesos están consumiendo el uso de CPU:
 - Show processs cpu
 - show processes cpu sorted | exclude 0.00%
 - Show processes cpu sorted
- ✓ Al excluir algunas MIBs del monitoreo, el CPU baja.
- ✓ Mediante una configuración correcta de agregación de enlaces, spanning tree para evitar bucles en la red.

F.1.3. Fallos que presentan un estado de desconocido.

Este tipo de alerta solo se presenta por fallas de configuración en los dispositivos agentes y en el gestor por lo tanto se procede a realizar lo siguiente:

1. Detectar

Cuando el dispositivo presenta una alerta de color **NARANJA** representa un estado **INALCAZABLE/UNREACHABLE**.

2. Aislar

Este estado se puede presentar por dos situaciones:

- ✓ Un dispositivo es inalcanzable

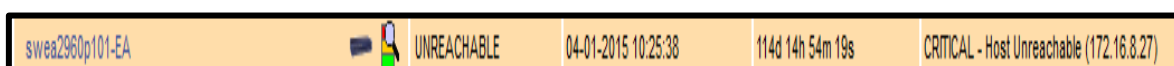


Figura F3. Representa estado UNREACHABLE/INALCANZABLE

- ✓ Los servicios configurados en el dispositivo es decir en los siguientes: carga de CPU, memoria RAM, memoria Flash, fuente de alimentación, ventiladores

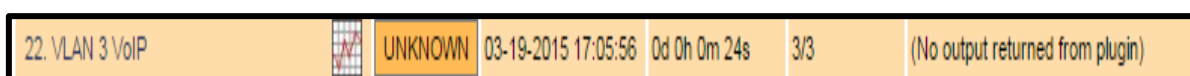


Figura F4. Representa estado UNKNOW/DESCONOCIDO

3. Diagnosticar

- ✓ Muchos sistemas se estabilizan si son reiniciados.
- ✓ No reconoce el OID asignado al servicio.
- ✓ Existe un error en el plugin asignado al servicio.

4. Corregir

- ✓ Corregir errores en los Plugins utilizados para el funcionamiento de los servicios.
- ✓ Asignarle el OID correcto para el servicio que se desea monitorear.

F.1.1.4. Fallos que presentan un estado de Pendiente.

Cuando se presente este tipo de alerta se procede a realizar lo siguiente:

1. Detectar

Cuando el dispositivo presenta una alerta de color **GRIS** representa un estado **PENDIENTE** donde sucede lo siguiente:

- ✓ Cuando se ingresa un nuevo dispositivo a Nagios inicialmente aparece en este estado mientras espera, para ejecutar una comprobación de que el host está activo.

Load	PENDING	N/A	0d 0h 0m 10s+	1/3	Service check scheduled for Tue Feb 24 14:35:57 ECT 2015
Memoria Flash	PENDING	N/A	0d 0h 0m 10s+	1/3	Service check scheduled for Tue Feb 24 14:36:16 ECT 2015

Figura F5: Representa estado de PENDIENTE

2. Diagnosticar

- ✓ En los próximos minutos se debe cambiar a color verde para indicar que ha pasado el control y el nuevo host está en UP, es decir está activo y con sus respectivos servicios.
- ✓ Si la prueba de verificación falló y Nagios Core no fue capaz de obtener una respuesta de algún servicio o máquina después de tres intentos, por cualquier razón, entonces el estado pasaría a **CRÍTICO**.
- ✓ No establece conectividad el agente con el gestor por falta de configuración de SNMP.
- ✓ Verificar si la dirección IP está asignada correctamente.

3. Corregir

- ✓ Si no está correctamente asignada la dirección IP proceder a asignar la IP que le pertenece al dispositivo.

- ✓ Verificar que el gestor establezca conectividad con el agente SNMP mediante el comando (*snmpwalk -v -2c -c comunidad 172.x.x.x*).
- ✓ Si el gestor no puede obtener la información de OID de una MIB del dispositivo proceder a configurar SNMP agente en el mismo.

F.2. Fallas producidas en los servidores

F.2.1. Fallos que presentan un estado de advertencia

Este tipo de alerta solo se presenta por fallas en los dispositivos agentes por lo tanto se procede a realizar lo siguiente:

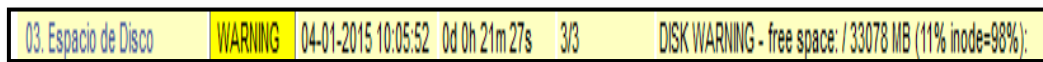


Figura F 6. Representa estado de ADVERTENCIA

1. Detectar

Cuando el dispositivo presenta una alerta de color **AMARILLO** representa un estado de **ADVERTENCIA** donde puede suceder lo siguiente:

- ✓ Se detecta esta alerta solo en los servicios configurados en el dispositivo más no en el equipo es decir en los siguientes: carga de CPU, memoria RAM, memoria Swap, espacio disco.

2. Diagnosticar

- ✓ La advertencia puede estar en color amarillo si la memoria RAM o la memoria Swap están dentro de los umbrales asignados.

3. Corregir

- ✓ Tomar medidas antes de que llegue a un estado crítico

F2.2. Falla que presenta un estado Crítico.

Este tipo de alerta solo se presenta por fallas en los dispositivos agentes por lo tanto se procede a realizar lo siguiente:

1. Detectar

Cuando el dispositivo presenta una alerta de color **ROJO** representa un estado de **CRÍTICO**, identificar inmediatamente en la topología de Nagios.

2. Aislar

Puede suceder por dos situaciones:

- ✓ El dispositivo esta abajo es decir está en estado **DOWN** o en estado **UNREACHABLE**

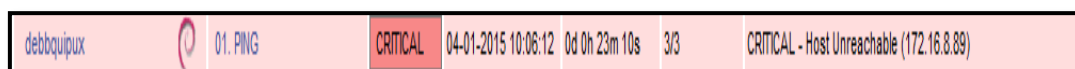


Figura F 7. Representa estado down en un servidor

- ✓ Los servicios configurados en el dispositivo es decir los siguientes: carga de CPU, memoria RAM, memoria Swap, espacio disco están abajo **DOWN**.

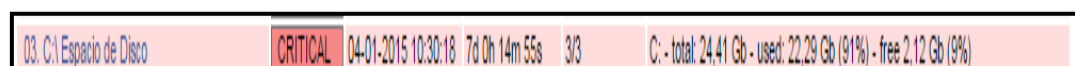


Figura F 8. Representa estado crítico en un servidor

3. Diagnosticar

- ✓ Si el dispositivo este abajo es decir está en estado **DOWN** o en estado **UNREACHABLE**, significa que ha perdido conectividad.
- ✓ Cual fue la causa que generó la desconexión del dispositivo:
 - Desconexión de luz eléctrica.
 - Cambio de direccionamiento.

- Equipo temporalmente suspendido por migración hacia un nuevo servidor sea físico o virtual.
- En proceso de actualización.
- Cambio de elementos hardware (memoria, CPU, disco) de los dispositivos.
- Cable de red roto o deteriorado.
- Errores de configuración en los equipos.

4. Corregir

- ✓ Ampliación o sustitución de los componentes afectados.
- ✓ El administrador debe mantenerse informado sobre las actualizaciones y parches que tenga que instalar.

F.2.3. Fallos que presenten un estado de desconocido.

Este tipo de alerta solo se presenta por fallas de configuración en los dispositivos agentes y en el gestor por lo tanto se procede a realizar lo siguiente:

1. Detectar

Cuando el dispositivo presenta una alerta de color **NARANJA** representa un estado **DESCONOCIDO** donde puede suceder lo siguiente:

- ✓ Se detecta esta alerta solo en los servicios configurados en el dispositivo mas no en el equipo es decir en los siguientes: carga de CPU, memoria RAM, memoria Swap, espacio disco.

2. Diagnosticar

- ✓ No reconoce el OID asignado al servicio.
- ✓ Existe un error en el plugin asignado al servicio.

3. Corregir

- ✓ Corregir errores en los Plugins utilizados para el funcionamiento de los servicios (buscar el error en el plugin que tenia) dos formas por consola y la paginadel plugin
- ✓ Asignarle el OID correcto para el servicio que se desea monitorear.

F.2.4. Falla que presentan un estado Pendiente

Cuando se presente este tipo de alerta se procede a realizar lo siguiente:

1. Detectar

Cuando el dispositivo presenta una alerta de color **GRIS** representa un estado **PENDIENTE** donde sucede lo siguiente:

- ✓ Cuando se ingresa un nuevo dispositivo a Nagios Inicialmente aparece en este estado mientras espera, para ejecutar una comprobación de que el host está activo.

2. Diagnosticar

- ✓ En los próximos minutos se debe cambiar a color verde para indicar que ha pasado el control y el nuevo host está en UP, es decir está activo y con sus respectivos servicios.

- ✓ Si la prueba de verificación falló y Nagios Core no fue capaz de obtener una respuesta de algún servicio o máquina después de tres intentos, por cualquier razón, entonces el estado pasaría a CRÍTICO.
- ✓ No establece conectividad el agente con el gestor por falta de configuración de SNMP.
- ✓ Verificar si la dirección IP está asignada correctamente

3. Corregir

- ✓ Si no está correctamente asignada la dirección IP proceder a asignar la IP que le pertenece al dispositivo.
- ✓ Verificar que el gestor establezca conectividad con el agente SNMP mediante el comando (*snmpwalk -v -2c -c comunidad 172.x.x.x*).
- ✓ Si el gestor no puede obtener la información de OID del dispositivo proceder a configurar el agente SNMP como se muestra en el Anexo E ítem E 1.2.1 y NRPE como se muestra en el Anexo E ítem E 1.2.3.

Anexo G: Test de rendimiento de la red mediante Ntop y Wireshark

Al presentarse un inconveniente en el switch de acceso que tiene conectividad con el área de TIC se procedió a realizar el respectivo monitoreo del tráfico, para determinar la causa del problema que satura el switch y este a su vez afecta el rendimiento del switch core.

G.1. Configuración del puerto mirroring

Para el monitoreo del tráfico entrante y saliente que genera las interfaces del switch core se configuró un puerto mirroring en el puerto GigabitEthernet 1/4, que es el encargado de duplicar todo el tráfico que genera las interfaces activas y enviarlo al host donde está conectado e instalado el software de monitoreo Ntop y Wireshark. Los comandos de configuración en el switch son los siguientes:

```
Switch(config)#monitor session 1 source interface gigabitethernet 1/1-24 both
```

```
Switch(config)#monitor session 1 destination interface gigabitethernet 1/4
```

G.2. Resultados del análisis del tráfico

Se realizó la captura del tráfico mediante el software Wireshark en el puerto MDF-45 ubicado en la Unidad de TIC; durante cinco días, desde el 26 de Febrero hasta el 4 de Marzo del 2015, por un lapso de 15 minutos diarios y en horarios elegidos de forma aleatoria para conocer el tráfico TCP, UDP y otros que circulan por la red sin configuración de SNMP y durante 5 días, desde el 5 de Marzo hasta el 11 de Marzo del 2015, por un lapso de 15 minutos diarios y en horarios elegidos de forma aleatoria para conocer el tráfico TCP, UDP y otros que circulan por la red con configuración de

SNMP. El resumen de estos resultados se muestra a continuación en las Tablas G 1 y G 2:

Tabla G 1. Tráfico SW-CORE sin configuración SNMP

TRÁFICO SIN CONFIGURACIÓN DE SNMP SW-CORE			
Fecha (dd-mm-aa)	Tráfico TCP	Tráfico UDP	Otro tipo de tráfico
Jueves 26-02-2015	18,70 %	81,12 %	0,18 %
Viernes 27-02-2015	13,63 %	84,71 %	2,05 %
Lunes 02-03-2015	15,26%	82,60%	2,14%
Martes 03-03-2015	10,07 %	86,96%	3,06 %
Miércoles 04-03-2015	9,84 %	87,76 %	2,40 %

Fuente: Datos capturados de software Wireshark

Tabla G 2. Tráfico SW-CORE con configuración SNMP

TRÁFICO CON CONFIGURACIÓN DE SNMP SW-CORE			
Fecha (dd-mm-aa)	Tráfico TCP	Tráfico UDP	Otro tipo de tráfico
Jueves 05-03-2015	55,50 %	44,35 %	0,15 %
Viernes 06-03-2015	12,65 %	84,49 %	2,87 %
Lunes 09-03-2015	19,17 %	79,07 %	1,76 %
Martes 10-03-2015	19,82 %	78,44 %	1,74 %
Miércoles 11-03-2015	22,17 %	76,74 %	1,09 %

Fuente: Datos capturados de software Wireshark

También se realizó la captura del tráfico mediante el software Ntop como indica la Tabla G3 el porcentaje de tráfico Unicast, Broadcast y Multicast consumido sin configuración de SNMP y en la Tabla G 4 el porcentaje de tráfico Unicast, Broadcast y Multicast consumido con configuración de SNMP.

Tabla G 3. Tráfico SW-CORE sin configuración SNMP

TRÁFICO SIN CONFIGURACIÓN DE SNMP SW-CORE			
Fecha (dd-mm-aa)	Unicast	Broadcast	Multicast
Jueves 26-02-2015	85,2%	11,0%	3,8%
Viernes 27-02-2015	92,4%	5,9%	1,7%
Lunes 02-03-2015	89,7%	7,2%	3,2%
Martes 03-03-2015	90,5%	6,7%	2,8%
Miércoles 04-03-2015	90,6%	6,8%	2,7 %

Fuente: Datos capturados de software Ntop

Tabla G 4. Tráfico SW-CORE

TRÁFICO CON CONFIGURACIÓN DE SNMP SW-CORE			
Fecha (dd-mm-aa)	Unicast	Broadcast	Multicast
Jueves 05-02-2015	91,6 %	6,1 %	2,3 %
Viernes 06-03-2015	95,6 %	3,2 %	1,3 %
Lunes 09-03-2015	90,6%	6,7%	2,7%
Martes 10-03-2015	91,2%	6,4%	2,5%
Miércoles 11-03-2015	91,3 %	6,4 %	2,4 %

Fuente: Datos capturados de software Ntop

En la gráfica de la Figuras G 1 se indica el tráfico Unicast, Broadcast y Multicast del día viernes 27-02-2015 y en la Figura G 2 se indica el tráfico Unicast, Broadcast y Multicast del día viernes 06-03-2015 tomadas desde Ntop en la pestaña **Summary**
>Traffic > eth0

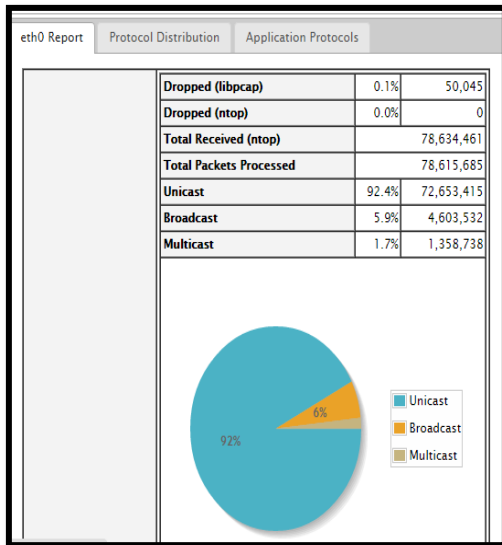


Figura G1: Captura propia de software Ntop

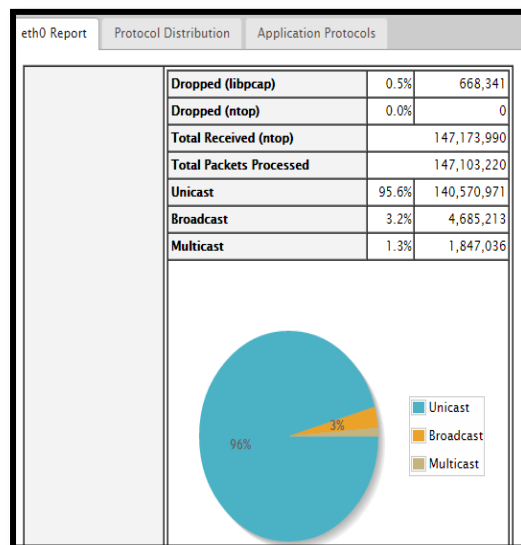


Figura G 2: Captura propia de software Ntop

En la gráfica de la Figura G 3 se indica el tráfico TCP, UDP y otros del día viernes 27-02-2015 y en la Figura G 4 se indica el tráfico TCP, UDP y otros del día viernes 06-03-2015 tomadas desde Wireshark en la pestaña **Statistics > IP Protocol Types** y **Statistics > IO Graph**.

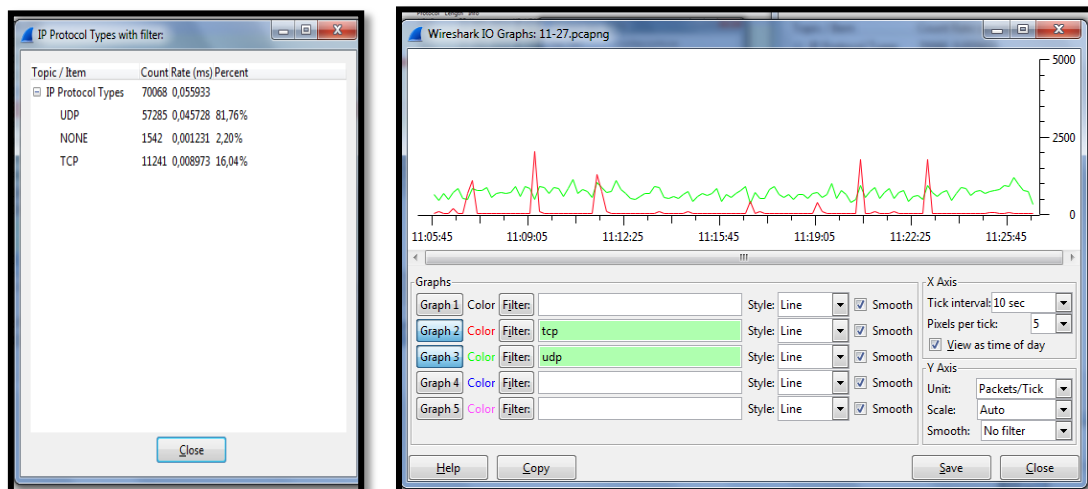


Figura G 3: Captura propia de software Ntop

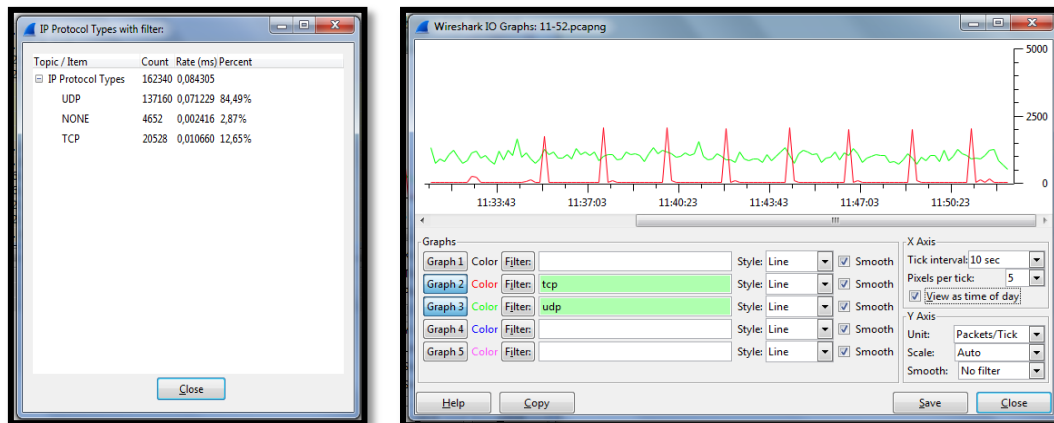


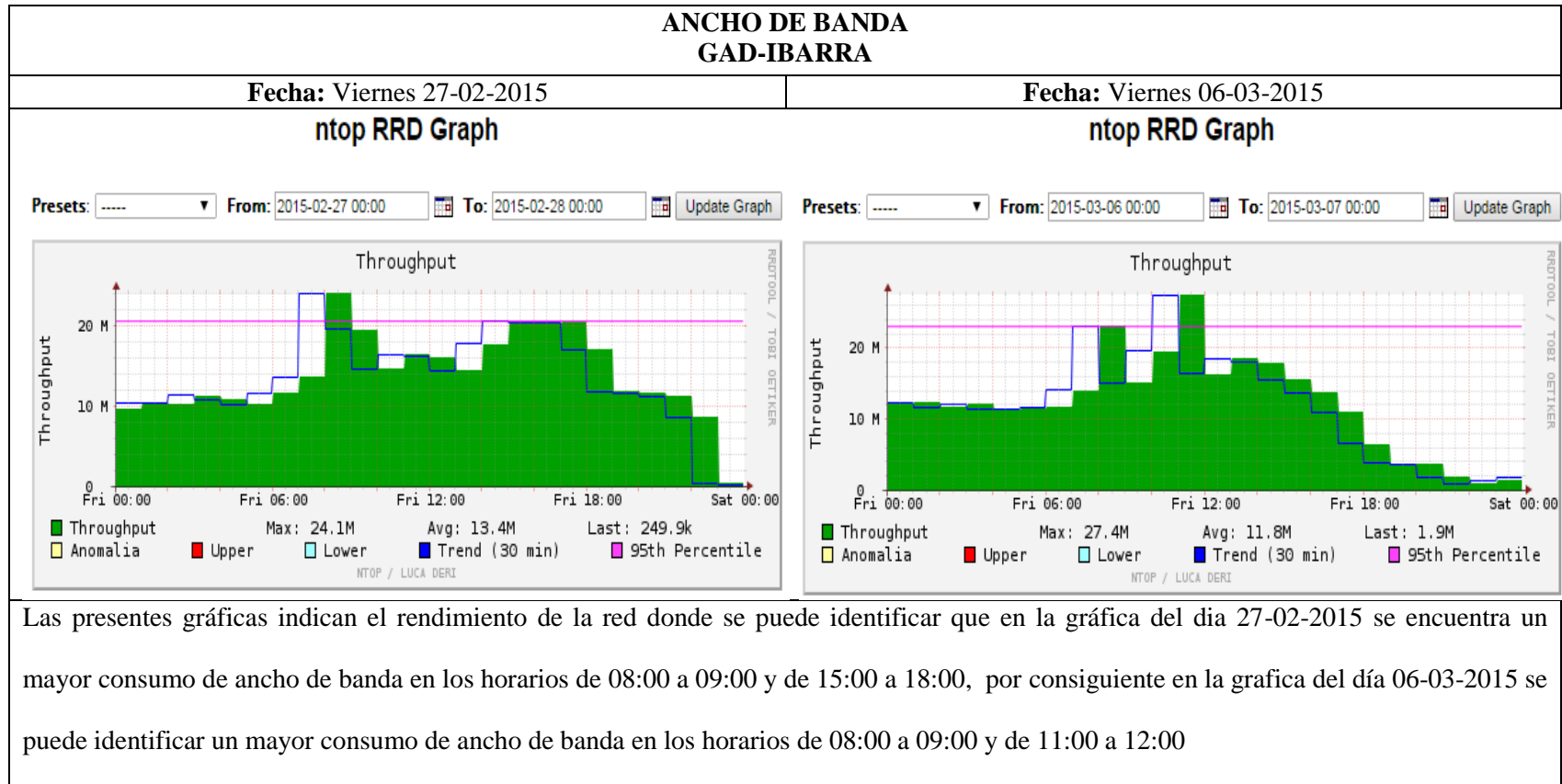
Figura G 4: Captura propia de software Ntop

G.3 Medición del tráfico de datos

Se realizó el siguiente análisis con la finalidad de obtener información acerca del tráfico que cursa por la red y de esta forma conocer su estado, para considerar el rendimiento que posee la misma antes de la implementación del proyecto. A continuación se presenta un análisis del rendimiento de la red para comprobar que al implementar el modelo de gestión en la red del GAD-Ibarra este no afectará su rendimiento y disponibilidad.

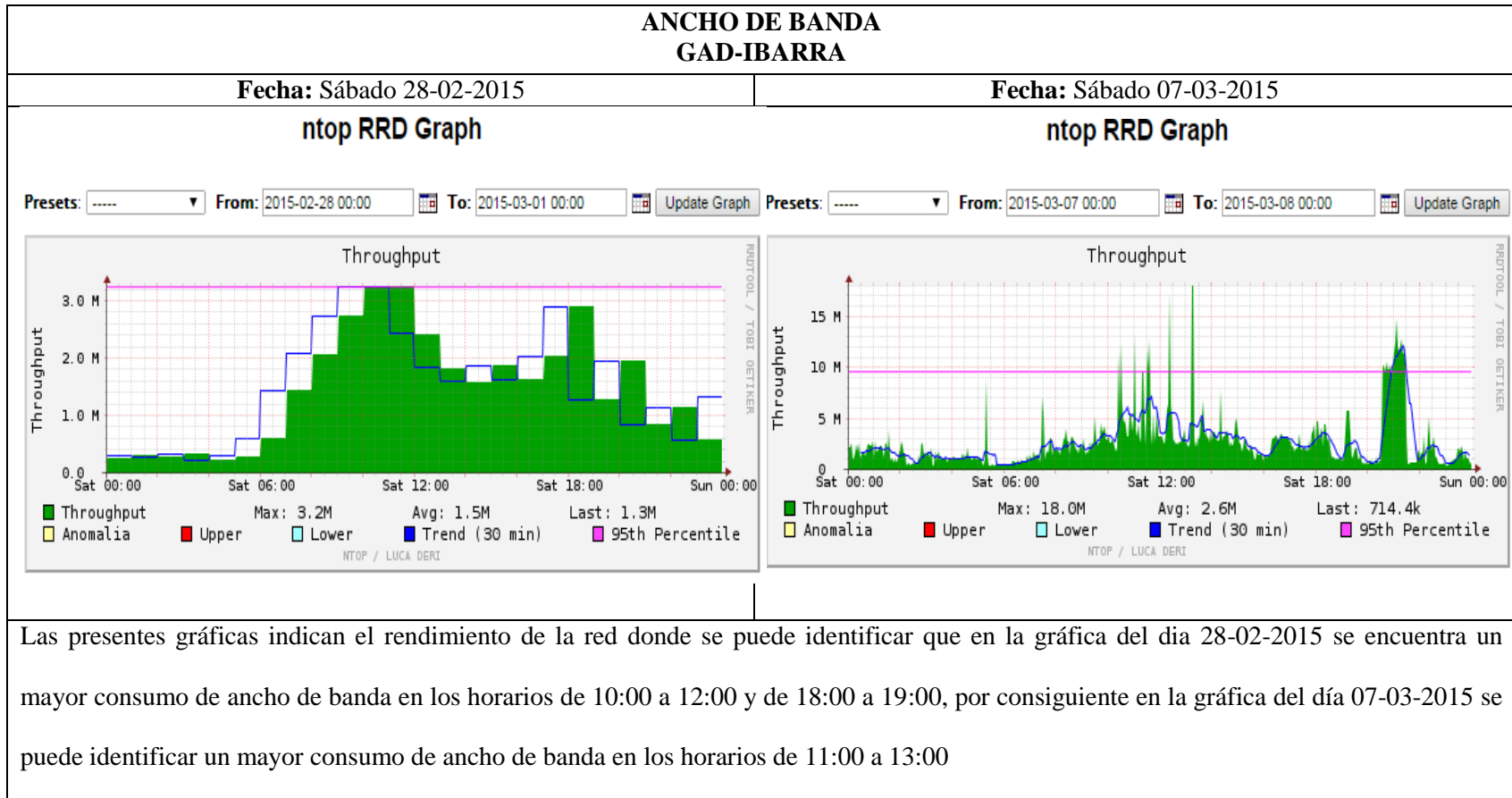
En las Tablas G 5, G 6, G 7, G 8, G 9, G 10 se puede observar el throughput de la red capturado sin configuración de SNMP en los días 27 de Febrero hasta el 05 de Marzo del 2015 y capturado con configuración de SNMP en los días desde el 06 de Marzo hasta el 12 de Marzo del 2015.

Tabla G 5: Throughput de la red del GAD-Ibarra los días Viernes 27-02-2015 y Viernes 06-03-2015



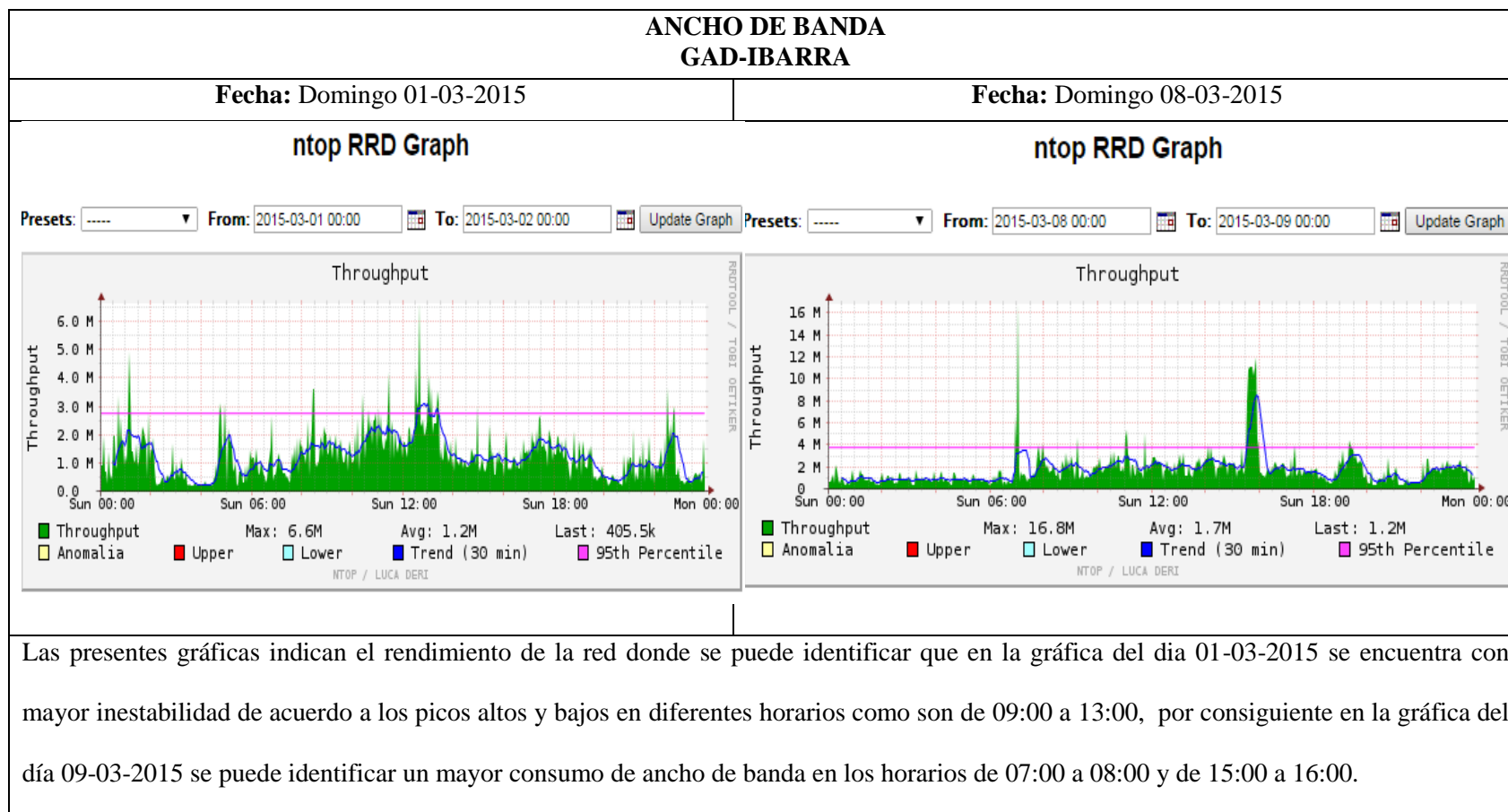
Fuente: Datos capturados de software Ntop

Tabla G 6: Throughput de la red del GAD-Ibarra los días Sábado 28-02-2015 y Sábado 07-03-2015



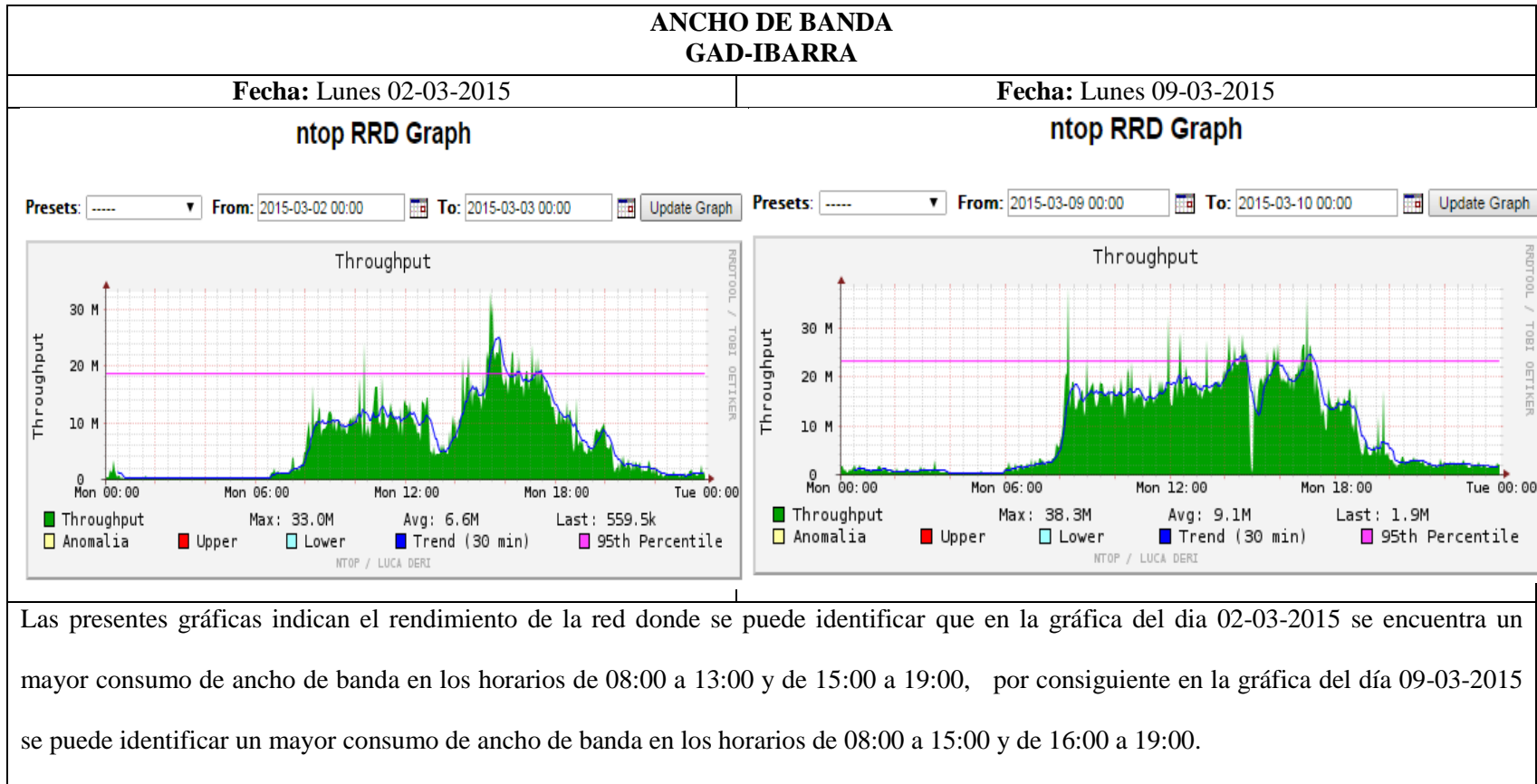
Fuente: Datos capturados de software Ntop

Tabla G 7: Throughput de la red del GAD-Ibarra los días Domingo 01-03-2015 y Domingo 08-03-2015



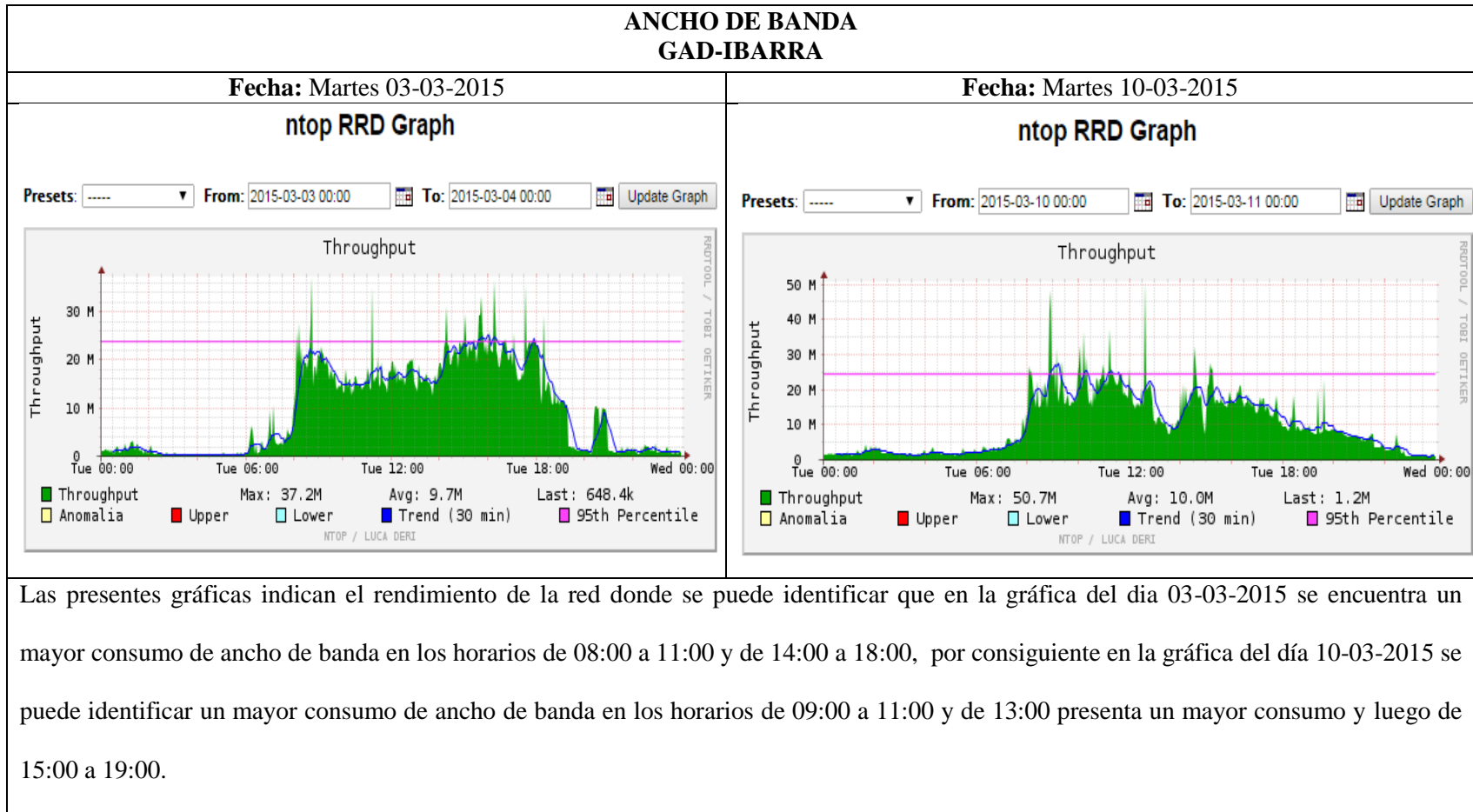
Fuente: Datos capturados de software Ntop

Tabla G 8: Throughput de la red del GAD-Ibarra los días Lunes 02-03-2015 y Lunes 09-03-2015



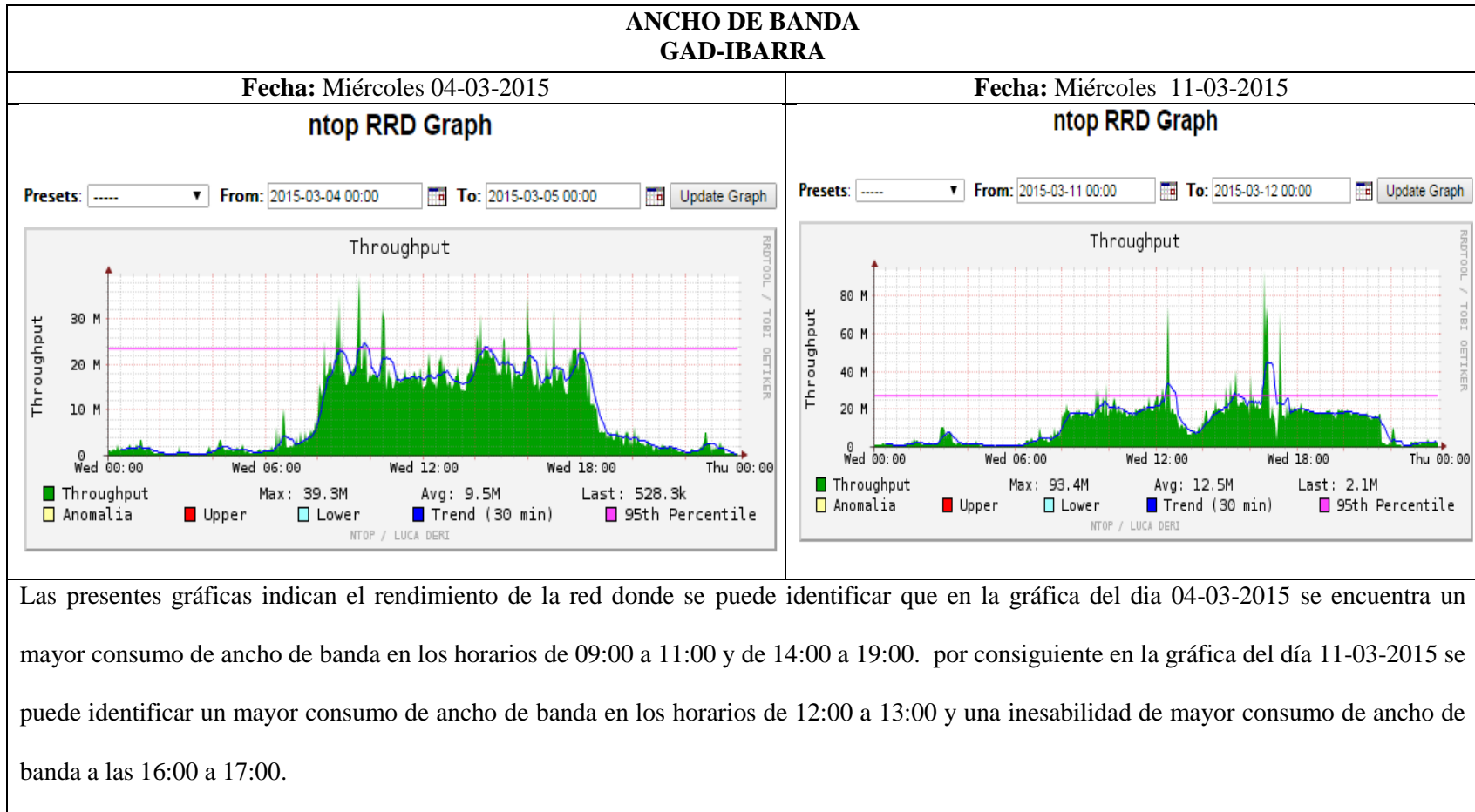
Fuente: Datos capturados de software Ntop

Tabla G 9: Throughput de la red del GAD-Ibarra los días Martes 03-03-2015 y Martes 10-03-2015



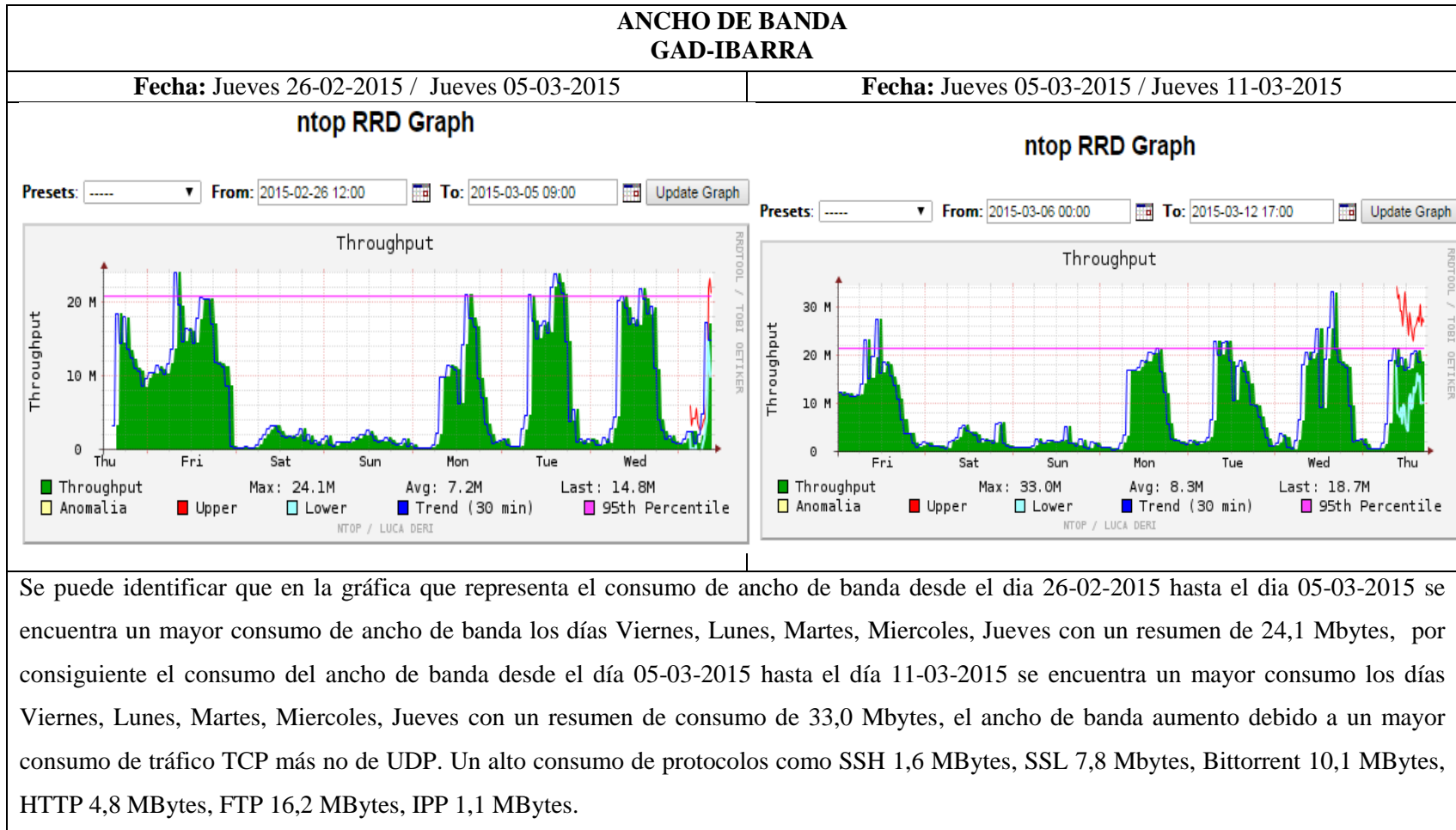
Fuente: Datos capturados de software Ntop

Tabla G 10: Throughput de la red del GAD-Ibarra los días Miércoles 04-03-2015 y Miércoles 11-03-2015



Fuente: Datos capturados de software Ntop

Tabla G 11: Throughput de la red del GAD-Ibarra los días Jueves 26-02-2015/05-03-2015 y Jueves 05-03-2015/11-03-2015



Fuente: Datos capturados de software Ntop

Anexo H: Simulación del proyecto implementado en la red del GAD-Ibarra con el software GNS3

A través de la simulación se puede indicar la captura de paquetes del proyecto implementado en la red de la entidad, debido a que en el servidor virtual no era posible implementar la herramienta Wireshark para poder verificar el sondeo de SNMP.

En la Figura H 1 se puede observar la topología realizada en el simulador y en las Tablas H 1, 2 y 3 indican el direccionamiento utilizado para la simulación:

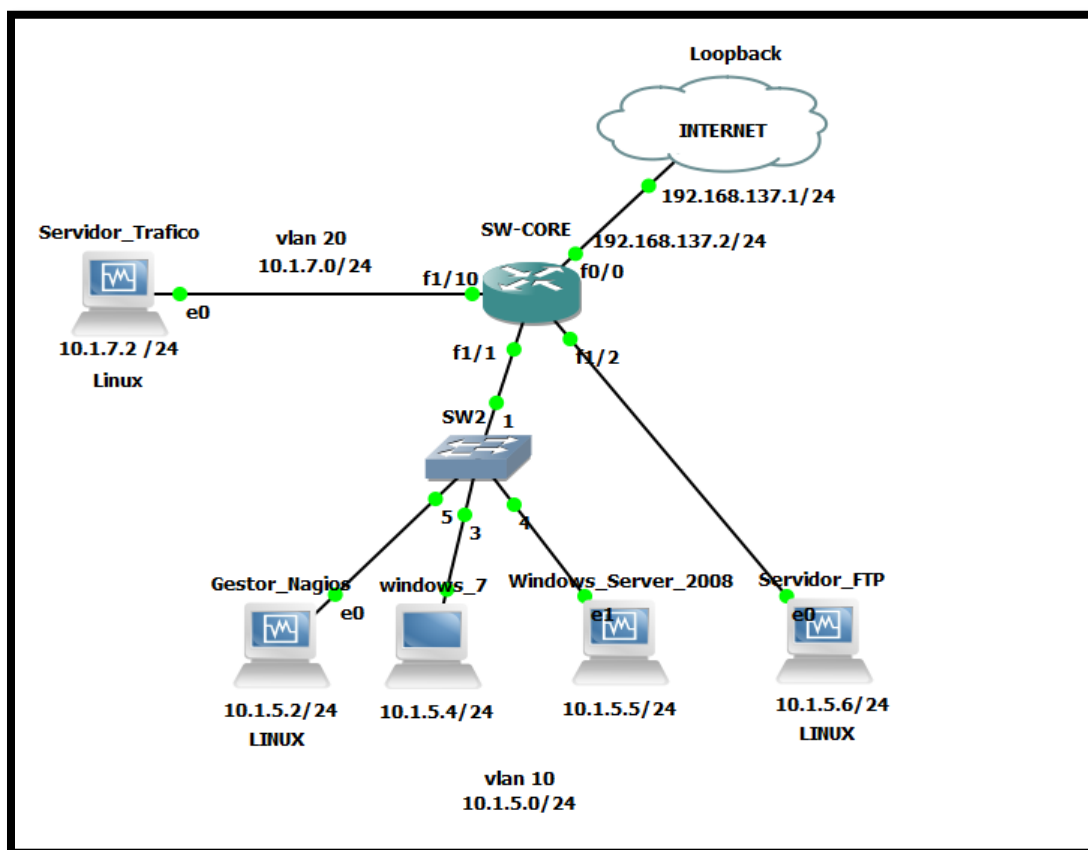


Figura H 1. Topología realizada en simulador GNS3

Fuente: Captura propia de software GNS3

Tabla H 1. Direccionamiento de vlan del switch

Nombre del Switch	Dirección IP de VLAN	Máscara de Subred	Nombres y Números de Vlan	Asignación de puertos del Switch
SW-CORE	10.1.5.1	255.255.255.0	VLAN 10 Administración	Fa1/1 - 1/5
	10.1.7.1	255.255.255.0	VLAN 20 de Tráfico	Fa 1/10

Tabla H 2. Direccionamiento del switch

Nombre del Switch	Interfaces	Dirección IP	Máscara de Subred
SW-CORE	Fa 0/0	192.168.137.2	255.255.255.0

Tabla H 3. Direccionamiento de host

Host	Dirección IP	Máscara de subred	Gateway
PC-Nagios	10.1.5.2	255.255.255.0	10.1.5.1
PC-Linux	10.1.5.3	255.255.255.0	10.1.5.1
PC-Windows Server 2003	10.1.5.4	255.255.255.0	10.1.5.1
PC-Windows 7	10.1.5.5	255.255.255.0	10.1.5.1
PC-Trafico	10.1.7.2	255.255.255.0	10.1.7.1

H.1. Configuración del Router

El router debe tener configurado los siguientes parámetros:

- **Nateo.**- Para establecer conectividad desde la red interna hacia la red de internet.
- **Vlans.**- Se crea vlan's para establecer la conexión con la red interna debido a las características que presenta el router **3700** de GNS3 que es el único que posee el módulo **NM-16ESW** que cumple con los parámetros que se necesita para simular el proyecto.
- **Port Mirroring.**- Esta configuración se realiza para analizar el tráfico que cursa por la red simulada.

A continuación se indica la configuración detallada en el router:

```
SW-CORE(config)#interface fastEthernet 0/0
SW-CORE(config-if)#ip address 192.168.137.2 255.255.255.0
SW-CORE(config-if)#ip nat outside
SW-CORE(config-if)#no shutdown

SW-CORE(config)#interface fastEthernet 1/1
SW-CORE(config-if)# switchport access vlan 10
SW-CORE(config-if)#exit

SW-CORE(config)#interface fastEthernet 1/2
SW-CORE(config-if)# switchport access vlan 10
SW-CORE(config-if)#exit

SW-CORE(config)#interface fastEthernet 1/10
SW-CORE(config-if)# switchport access vlan 20
SW-CORE(config-if)#exit

SW-CORE(config)#interface vlan 10
SW-CORE(config-if)# ip address 10.1.5.1 255.255.255.0
SW-CORE(config-if)# ip nat inside
SW-CORE(config)#ip default-gateway 10.1.5.1

SW-CORE(config)#interface vlan 20
SW-CORE(config-if)# ip address 10.1.7.1 255.255.255.0
SW-CORE(config-if)# ip nat inside
SW-CORE(config)#ip default-gateway 10.1.7.1

SW-CORE(config)#ip route 0.0.0.0 0.0.0.0 192.168.137.1
SW-CORE(config)#ip route 10.1.5.0 255.255.255.0 fastEthernet 1/1
SW-CORE(config)#ip route 10.1.7.0 255.255.255.0 fastEthernet 1/10

SW-CORE(config)#access-list 1 permit 10.1.5.0 0.0.0.255
SW-CORE(config)#access-list 2 permit 10.1.7.0 0.0.0.255

SW-CORE(config)#ip nat inside source list 1 interface fastEthernet 0/0 overload
SW-CORE(config)#ip nat inside source list 2 interface fastEthernet 0/0 overload
SW-CORE(config)#ip domain-lookup
```

H.2. Resultados

En esta parte solo se muestra resultados obtenidos de la simulación, porque las configuraciones de gestor y agente son exactamente iguales como se explicó en el Anexo E. En la Figura H 2 se puede observar los mensajes que genera SNMP (get-request, get-response, get-next-request) entre el gestor Nagios y sus respectivos agentes además indica la versión y comunidad configuradas en el dispositivo gestionado.

No.	Time	Source	Destination	Protocol	Length	Info
90	44.261665000	10.1.5.2	192.168.137.2	SNMP	134	get-request 1.3.6.1.2.1.2.2.1.5.1 1.3.6.1.2.1.2.2.1.8.1 1.3.6.1.2.1.31.1
91	44.329891000	192.168.137.2	10.1.5.2	SNMP	149	get-response 1.3.6.1.2.1.2.2.1.5.1 1.3.6.1.2.1.2.2.1.8.1 1.3.6.1.2.1.31.1
447	218.093212000	10.1.5.2	192.168.137.2	SNMP	134	get-request 1.3.6.1.2.1.2.2.1.5.5 1.3.6.1.2.1.2.2.1.8.5 1.3.6.1.2.1.31.1
448	218.190292000	192.168.137.2	10.1.5.2	SNMP	145	get-response 1.3.6.1.2.1.2.2.1.5.5 1.3.6.1.2.1.2.2.1.8.5 1.3.6.1.2.1.31.1
479	232.876169000	10.1.5.2	192.168.10.1	SNMP	91	get-next-request 1.3.6.1.4.1.14988.1.1.1.2.1.3
480	232.919666000	192.168.10.1	10.1.5.2	SNMP	108	get-response 1.3.6.1.4.1.14988.1.1.1.2.1.3.80.183.195.183.81.149.6
481	232.921255000	10.1.5.2	192.168.10.1	SNMP	102	get-next-request 1.3.6.1.4.1.14988.1.1.1.2.1.3.80.183.195.183.81.149.6
482	232.939549000	192.168.10.1	10.1.5.2	SNMP	109	get-response 1.3.6.1.4.1.14988.1.1.1.2.1.4.80.183.195.183.81.149.6
632	292.103917000	10.1.5.2	192.168.137.2	SNMP	86	getBulkRequest 1.3.6.1.4.1.9.9.48.1.1.1.2
635	293.420560000	192.168.137.2	10.1.5.2	SNMP	755	get-response 1.3.6.1.4.1.9.9.48.1.1.1.2.1 1.3.6.1.4.1.9.9.48.1.1.1.2.2 1.3.6.1.4.1.9.9.48.1.1.1.2.3
636	293.426992000	10.1.5.2	192.168.137.2	SNMP	125	get-request 1.3.6.1.4.1.9.9.48.1.1.1.4.2 1.3.6.1.4.1.9.9.48.1.1.1.5.2 1.3.6.1.4.1.9.9.48.1.1.1.5.3

Frame 90: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0

Ethernet II, Src: CadmusCo_23:f9:f3 (08:00:27:23:f9:f3), Dst: c2:00:13:1c:00:00 (c2:00:13:1c:00:00)

Internet Protocol Version 4, Src: 10.1.5.2 (10.1.5.2), Dst: 192.168.137.2 (192.168.137.2)

User Datagram Protocol, Src Port: 26081 (26081), Dest Port: snmp (161)

Simple Network Management Protocol

- version: v2c (1)
- community: imi
- data: get-request (0)

```

0000  c2 00 13 1c 00 00 08 00 27 23 f9 f3 08 00 45 00  ..... '#...E.
0010  00 78 00 00 40 00 40 11 e1 c7 0a 01 05 02 c0 a8  ..x.@.@.....
0020  89 02 90 75 00 a1 00 64 a6 8d 30 5a 02 01 01 04  .....d..0Z...
0030  03 69 6d 69 a0 50 02 04 22 a5 39 67 02 01 00 02  ..iml.P.+.9g...
0040  01 00 30 42 30 0e 06 0a 2b 06 01 02 01 02 02 01  ..0B0...+.....

```

Figura H 2. Mensajes que genera SNMP entre gestor y agentes

Fuente: Captura propia de software Wireshark

La Figura H 3 muestra la conexión que se establece cuando Nagios envía una notificación de correo electrónico a una cuenta de Gmail.

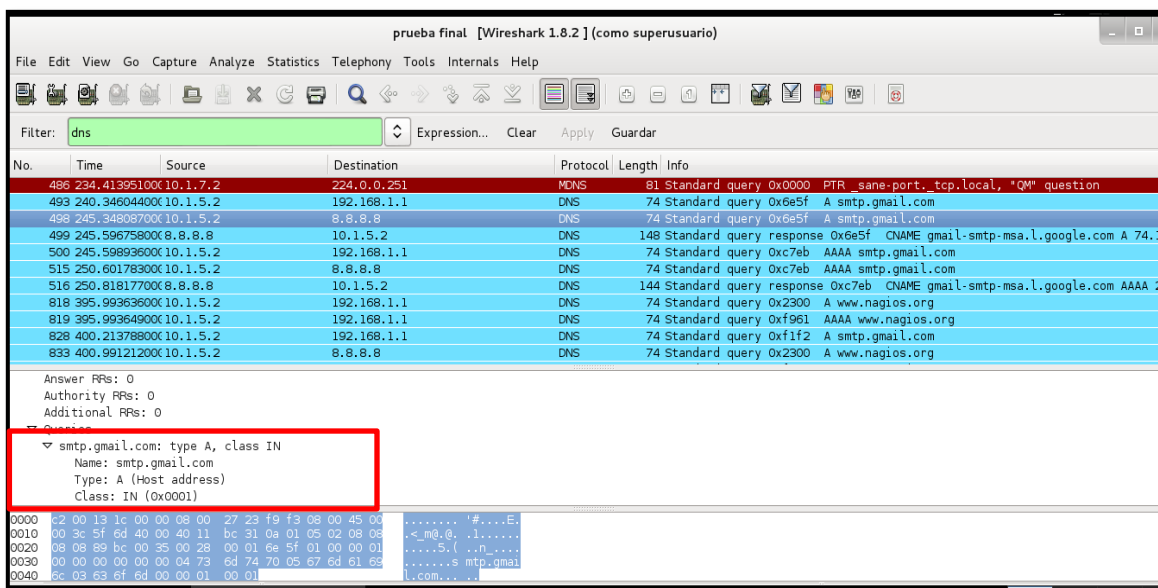


Figura H 3. Envío de correo desde Nagios a cuenta Gmail

Fuente: Captura propia de software Wireshark

La Figura H 4 muestra el log que genera Nagios al enviar una notificación de correo electrónico mediante el comando (*notify-service-by-email*) el cual genera el texto que debe ser enviado a la cuenta de correo del administrador de la red. Al igual que sms, mediante el comando (*notify-service-by-sms*).

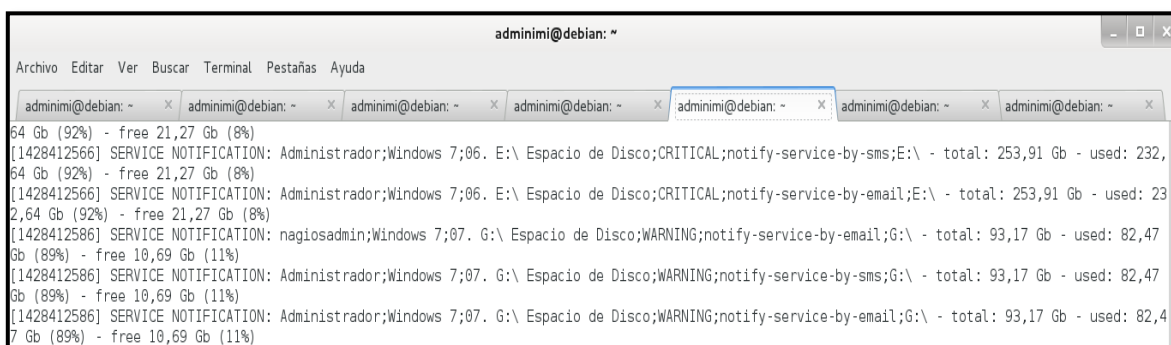


Figura H 4. Log de envío de notificaciones

Fuente: Captura propia de software Nagios



Ibarra, 07 de Abril del 2015

CERTIFICACIÓN

Señores:

UNIVERSIDAD TÉCNICA DEL NORTE

Presente.

De mis consideraciones.-

Siendo auspiciantes del Proyecto de Tesis de la Srta. Viviana Elizabeth Ayala Yandún con CI. 100306856-4, quien desarrolló su trabajo con el tema “**MODELO DE GESTIÓN DE RED FUNCIONAL EN LA RED LOCAL DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA BASADO EN EL ESTÁNDAR ISO**”, me es grato informar que se han superado con satisfacción las pruebas técnicas de implementación y el cumplimiento del modelo de gestión, por lo que se recibe el proyecto como culminado. Una vez recibida la documentación respectiva, nos comprometemos a continuar utilizándolo en beneficio de nuestra entidad.

La Srta. Viviana Elizabeth Ayala Yandún, puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,



Lic. Miguel Tobar

HARDWARE Y COMUNICACIONES

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA