



**UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS**

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

TEMA:

DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE RED PARA LA RED DE ÁREA LOCAL DEL EDIFICIO CENTRAL DE LA UNIVERSIDAD TÉCNICA DEL NORTE EN BASE AL MODELO DE GESTIÓN OSI CON EL PROTOCOLO SNMP.

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN

ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTORA: JESSICA ESTEFANÍA BÁEZ CHEZA

DIRECTOR: ING. FABIÁN CUZME

IBARRA-ECUADOR
2017



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
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 formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO	
Cédula de Identidad	100360118-2
Apellidos y Nombres	Báez Cheza Jessica Estefanía
Dirección	Av. 17 de Julio 5-26
E-mail	jebaezc@utn.edu.ec
Teléfono Fijo	062602997
Teléfono Móvil	0939374645
DATOS DE LA OBRA	
Título	DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE RED PARA LA RED DE ÁREA LOCAL DEL EDIFICIO CENTRAL DE LA UNIVERSIDAD TÉCNICA DEL NORTE EN BASE AL MODELO DE GESTIÓN OSI CON EL PROTOCOLO SNMP.

Autor	Báez Cheza Jessica Estefanía
Fecha	17 de julio de 2017
Programa	Pregrado
Título por el que se aspira:	Ingeniería en Electrónica y Redes de Comunicación
Director	Ing. Fabián Geovanny Cuzme Rodríguez

2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, JESSICA ESTEFANÍA BÁEZ CHEZA, con cédula de identidad Nro. 100360118-2, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma 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 de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior artículo 144.

3.- CONSTANCIAS

El auto 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 titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, al 17 día del mes de julio del 2017

.....


Jessica Estefanía Báez Cheza

100360118-2



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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

Yo, JESSICA ESTEFANÍA BÁEZ CHEZA, con cédula de identidad Nro. 100360118-2, manifiesto 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 autor del trabajo de grado denominado: “DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE RED PARA LA RED DE ÁREA LOCAL DEL EDIFICIO CENTRAL DE LA UNIVERSIDAD TÉCNICA DEL NORTE EN BASE AL MODELO DE GESTIÓN OSI CON EL PROTOCOLO SNMP.”, que ha sido desarrollado para optar el título de Ingeniería en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, al 17 día del mes de julio del 2017

A handwritten signature in blue ink, reading "Jessica Báez", is written over a horizontal dotted line.

Jessica Estefanía Báez Cheza

1003601182-2



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Jessica Estefanía Báez Cheza, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos 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.

A handwritten signature in blue ink, reading "Jessica Báez Cheza", is written over a horizontal dotted line.

Jessica Estefanía Báez Cheza

100360118-2



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que la Tesis “DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE RED PARA LA RED DE ÁREA LOCAL DEL EDIFICIO CENTRAL DE LA UNIVERSIDAD TÉCNICA DEL NORTE EN BASE AL MODELO DE GESTIÓN OSI CON EL PROTOCOLO SNMP” ha sido realizada en su totalidad por la señorita: JESSICA ESTEFANÍA BÁEZ CHEZA portadora de la cédula de identidad N° 100360118-2; previo a la obtención del Título de Ingeniera en Electrónica y Redes de Comunicación, bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.

A handwritten signature in black ink, appearing to read "Fabián Geovanny Cuzme Rodríguez", is written over a horizontal line.

Ing. Fabián Geovanny Cuzme Rodríguez.

Cédula: 131152701-2

Director de Tesis

AGRADECIMIENTO

A mis padres que día a día supieron apoyarme para lograr las metas que me propuse, por su paciencia y amor, gracias.

Agradezco a la Universidad Técnica del Norte, a la Facultad de Ingeniería en Ciencias Aplicadas, y docentes de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, por haber compartido sus conocimientos, experiencias y valores, para crecer como buenos profesionales. A mi director de tesis Ing. Fabián Cuzme, por su paciencia, guía y apoyo para el desarrollo de mi tesis.

De manera muy especial quiero expresar mi agradecimiento a la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, Ing. Vinicio Guerra, ya que sin su colaboración no hubiera sido posible la finalización de este proyecto.

A todos mis amigos, que siempre tuvieron palabras de aliento para lograr la realización de este proyecto.

DEDICATORIA

Este proyecto lo dedico a mis padres Raúl y María y a mi hermano Wilmer, quienes me han sabido apoyar en cada etapa de mi vida. Con su esfuerzo, 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.

Jessica Báez

CONTENIDO

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE	ii
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.....	v
DECLARACIÓN	vi
CERTIFICACIÓN	vii
AGRADECIMIENTO.....	viii
DEDICATORIA	ix
CONTENIDO	x
RESUMEN.....	xxv
ABSTRACT	xxvii
PRESENTACIÓN	xxix
CAPÍTULO I.....	1
1. ANTECEDENTES	1
1.1. Tema	1
1.2. Problema	1
1.3. Objetivos.....	2
1.3.1. Objetivo General	2
1.3.2. Objetivos Específicos	2

1.4.	Alcance	3
1.5.	Justificación	5
CAPÍTULO II		7
2.	Marco teórico	7
2.1.	Conceptos generales.....	7
2.1.1.	Administrar.....	7
2.1.2.	Gestionar	7
2.1.3.	Gestión de red.....	8
2.2.	Elementos de la gestión de red.....	9
2.2.1.	Gestor	9
2.2.2.	Agente	9
2.2.3.	Dispositivo administrado.....	9
2.3.	Procesos de gestión de red	9
2.3.1.	Monitoreo	10
2.3.2.	Control.....	11
2.4.	Modelos de gestión de red	11
2.4.1.	Modelo de gestión TMN	11
2.4.2.	Modelo de gestión ISO.....	13
2.4.2.1.	Gestión de configuraciones	13
2.4.2.2.	Gestión de rendimiento.....	14

2.4.2.3.	Gestión de fallos	15
2.4.2.4.	Gestión de contabilidad	15
2.4.2.5.	Gestión de seguridad	16
2.4.3.	Modelo de gestión Internet.....	16
2.5.	Protocolos de gestión	16
2.5.1.	CMIP	17
2.5.2.	SNMP	17
2.5.2.1.	Versiones SNMP	18
2.5.2.2.	Arquitectura SNMP	20
2.5.2.3.	Funcionamiento SNMP	21
2.5.2.4.	Elementos de SNMP.....	22
2.5.2.4.1.	Estación de gestión	22
2.5.2.4.2.	Agente de gestión	23
2.5.2.4.3.	Protocolo de gestión de red	23
2.5.2.4.4.	Base de información de gestión.....	23
2.5.2.5.	Mensajes SNMP	25
2.5.2.5.1.	PDU de los mensajes SNMP	27
2.5.2.6.	Comunidades SNMP	28
2.5.3.	RMON.....	29
2.6.	Herramientas de gestión.....	30

2.6.1.	Pandora FMS.....	30
2.6.2.	CiscoWorks.....	31
2.6.3.	HP Openview	31
2.6.4.	PRTG Network Monitor.....	32
2.6.5.	Nagios.....	32
2.6.6.	Zabbix.....	33
2.6.7.	Cacti	34
2.6.8.	Zenoss.....	34
2.7.	Herramientas complementarias al software de gestión.....	35
2.7.1.	Ping.....	35
2.7.2.	Traceroute.....	35
2.7.3.	Nessus.....	35
2.7.4.	Wireshark	36
2.7.5.	Tripwire.....	36
2.7.6.	Swatch	37
2.8.	Políticas de administración	37
CAPÍTULO III.....		40
3.	Situación actual.....	40
3.1.	Universidad Técnica del Norte	40
3.1.1.	Ubicación	40

3.1.2.	Estructura Organizacional	41
3.1.3.	Misión y visión	42
3.1.4.	Red de datos interna	42
3.2.	Edificio Central de la UTN	45
3.2.1.	Equipos de telecomunicaciones	47
3.2.1.1.	Cuarto de Equipos	47
3.2.1.2.	Planta baja	52
3.2.1.3.	Planta alta 1	52
3.2.1.4.	Planta alta 2	54
3.2.1.5.	Planta alta 3	55
3.2.1.6.	Planta alta 4	55
3.3.	Entrevista	57
3.4.	Encuesta	58
3.4.2.	Resultados	61
3.5.	Requerimientos del software de gestión	70
3.6.	Selección del software de monitoreo	71
3.6.1.	Estándar ISO/IEC/IEEE 29148:2011	72
3.6.2.	Comparación y elección de software	73
3.6.3.	Software Zabbix	76
3.6.3.1.	Requerimientos de hardware	78

3.7.	Selección del hardware de gestión de red	79
3.7.1.	Análisis de crecimiento de equipos de conmutación.	79
3.7.2.	Requerimientos del servidor de gestión de red	80
CAPÍTULO IV		83
4.	Implementación.....	83
4.1.	Establecimiento de Políticas	83
4.2.	Manual de Procedimientos.....	94
4.2.1.	Manual de procedimientos para la gestión de configuraciones.....	94
4.2.2.	Manual de procedimientos para la gestión de fallos	98
4.2.3.	Manual de procedimientos para la gestión de contabilidad	101
4.2.4.	Manual de procedimientos para la gestión de prestaciones	104
4.2.5.	Manual de procedimientos para la gestión de seguridad.....	107
4.3.	Implementación del modelo de gestión de red	110
4.3.1.	Implementación de Gestión de configuraciones	115
4.3.1.1.	Registro de configuraciones	115
4.3.1.2.	Inventarios	116
4.3.2.	Implementación de Gestión de fallos	117
4.3.2.1.	Gestión proactiva.....	117
4.3.2.2.	Gestión reactiva	118
4.3.2.2.1.	Detección de fallos	118

4.3.2.2.2.	Aislamiento y diagnóstico del fallo	123
4.3.2.2.3.	Solución de la falla	123
4.3.3.	Implementación de Gestión de prestaciones	123
4.3.3.1.	Monitoreo de interfaces de red	124
4.3.3.2.	Disponibilidad	126
4.3.3.2.1.	Monitoreo del Portal Web de la UTN	126
4.3.3.3.	Límites de rendimiento	129
4.3.3.3.1.	Switches	129
4.3.3.3.2.	Firewall	130
4.3.3.3.3.	Servidores	131
4.3.3.3.4.	Resumen de límites de rendimiento	131
4.3.4.	Implementación de Gestión de contabilidad	132
4.3.4.1.	Monitoreo de uso de memoria	132
4.3.4.2.	Monitoreo de uso de CPU	133
4.3.4.3.	Monitoreo del espacio de disco	133
4.3.5.	Implementación de Gestión de seguridad	135
4.3.5.1.	Acceso al servidor de gestión	135
4.3.5.2.	Dispositivos gestionados	138
4.4.	Análisis Costo-Beneficio	140
4.4.1.	Software	140

4.4.2. Hardware	141
4.4.3. Presupuesto total	141
4.4.4. Beneficios.....	142
CONCLUSIONES	144
RECOMENDACIONES	146
GLOSARIO.....	148
BIBLIOGRAFÍA.....	151
ANEXO A. Características técnicas de los equipos.....	156
ANEXO B. Encuesta.....	164
ANEXO C. Entrevista.....	169
ANEXO D. Especificación de Requerimientos de software.....	173
ANEXO E. Formulario de reportes de fallos	180
ANEXO F. Instalación de CentOS 7.....	181
ANEXO G. Instalación del servidor Zabbix	187
ANEXO H. Configuración del protocolo SNMP.....	195
ANEXO I. Instalación del agente en CentOS 6.8	198
ANEXO J. Instalación de Nessus.....	200
ANEXO K. Manual del administrador.....	203
ANEXO L. Instalación de OTRS.....	216
ANEXO M. Plantilla de registro de configuraciones.....	226

ANEXO N. Acta de entrega de Manual de políticas y procedimientos 227

ÍNDICE DE FIGURAS

Figura 1. Niveles funcionales del modelo TMN	12
Figura 2. Esquema de una red gestionada con SNMP	22
Figura 3. Intercambio de mensajes en SNMPv1	26
Figura 4. Mensaje SNMP	27
Figura 5. Ubicación de la UTN	40
Figura 6. Organigrama Estructural de la UTN.....	41
Figura 7. Diseño físico de la red UTN	44
Figura 8. Campus UTN "El Olivo"	45
Figura 9. Topología física del Data Center	48
Figura 10. Frecuencia de problemas en la red.....	62
Figura 11. Atención a problemas	63
Figura 12. Tiempo de solución del problema.....	64
Figura 13. Servicios de la red interna UTN	65
Figura 14. Página Web de la red interna UTN.....	66
Figura 15. Portafolio virtual de la red interna UTN.....	67
Figura 16. Servicio de Internet.....	68
Figura 17. Grado de satisfacción con la labor de la DDTI.....	69
Figura 18. Pantalla principal de Zabbix	77
Figura 19. Diagrama de gestión	110
Figura 20. Inventario de equipos.....	117
Figura 21. Ciclo de vida de incidencia de fallos	118
Figura 22. Alarmas visuales.....	119
Figura 23. Mapa del sistema de gestión	120

Figura 24. Configuración de alertas vía e-mail	121
Figura 25. Alertas vía e-mail.....	121
Figura 26. Dashboard de OTRS	122
Figura 27. Tráfico entrante y saliente de interfaces del switch.....	124
Figura 28. Tráfico entrante y salientes de interfaz "DMZ" de firewall ASA.....	125
Figura 29. Tráfico en la interfaz del servidor Zabbix	125
Figura 30. Reportes de disponibilidad	126
Figura 31. Ítems del escenario web.....	127
Figura 32. Estado de HTTP service	127
Figura 33. Velocidad de carga del portal web UTN	128
Figura 34. Tiempo de respuesta del portal web UTN	129
Figura 35. Fallo en la conexión hacia www.utn.edu.ec	129
Figura 36. Monitoreo del uso de memoria de un switch.....	133
Figura 37. Monitoreo del uso de CPU	133
Figura 38. Utilización de disco en el servidor DHCP	134
Figura 39. Utilización de disco en la partición /boot del servidor DHCP.....	134
Figura 40. Utilización de disco de la partición /home del servidor DHCP	135
Figura 41. Usuarios de Zabbix	136
Figura 42. Configuración de la cuenta de usuario Admin	136
Figura 43. Permisos de usuario	137
Figura 44. Registro de auditoría.....	138
Figura 45. Plantillas Nessus	139
Figura 46. Escaneo básico de la red	139

Figura 47. Detalles de la vulnerabilidad en Nessus	140
--	-----

ANEXO A

Figura A 1. Switch WS-C4510R+E	156
Figura A 2. Switch WS-C4503-E L3	157
Figura A 3. Switch WS-CBS3020-HPQ	158
Figura A 4. Switch WS-C2960-48TC-L	158
Figura A 5. Switch WS-C2960-24TC-L	159
Figura A 6. Switch WS-C3850-48T.....	160
Figura A 7. Switch WS-C2960X-48TS-L.....	161
Figura A 8. Switch Nexus 5548	161
Figura A 9. Switch WS-C2960S-24PS-S.....	162
Figura A 10. Cisco ASA 5520	163

ANEXO F

Figura F 1. Instalación de CentOS 7	181
Figura F 2. Selección de idioma.....	181
Figura F 3. Destino de instalación.....	182
Figura F 4. Selección de dispositivos.....	182
Figura F 5. Resumen de instalación	183
Figura F 6. Red y nombre de host	183
Figura F 7. Reconocimiento de la interfaz de red	184
Figura F 8. Comenzar instalación	184
Figura F 9. Ajustes de usuario.....	185
Figura F 10. Configuración de contraseña root.....	185

Figura F 11. Finalización de instalación	186
--	-----

ANEXO G

Figura G 1. Instalación de Zabbix	189
Figura G 2. Comprobación de requisitos previos.....	190
Figura G 3. Detalles de la base de datos	190
Figura G 4. Detalles del servidor	191
Figura G 5. Resumen de la pre-instalación	191
Figura G 6. Instalación frontend	192
Figura G 7. Inicio de sesión	192
Figura G 8. Panel de Zabbix	193

ANEXO J

Figura J 1. Descarga de Nessus	200
Figura J 2. Pantalla principal de instalación de Nessus	200
Figura J 3. Configuraciones de cuenta de Nessus	201
Figura J 4. Activación del producto Nessus.....	201
Figura J 5. Log en Nessus	201
Figura J 6. Pantalla principal de Nessus.....	202

ANEXO K

Figura K 1. Grupos de usuarios.....	203
Figura K 2. Users groups	203
Figura K 3. Privilegios de grupos	204
Figura K 4. Creación de usuario	204
Figura K 5. Detalles de usuario.....	205
Figura K 6. Hosts	205

Figura K 7. Configuración de host.....	206
Figura K 8. Ingreso de la comunidad SNMP	207
Figura K 9. Adición de plantillas	207
Figura K 10. Host añadido	208
Figura K 11. Latest data	208
Figura K 12. Plantillas.....	209
Figura K 13. Crear ítem	209
Figura K 14. Parámetros del ítem	210
Figura K 15. Gráficos.....	210
Figura K 16. Parámetros del gráfico	211
Figura K 17. Creación de host para web escenario	212
Figura K 18. Adición de plantilla HTTP.....	212
Figura K 19. Creación de escenario	213
Figura K 20. Configuración del escenario	213
Figura K 21. Steps.....	214
Figura K 22. Parámetros del step	214
Figura K 23. Adición del step	215
Figura K 24. Escenarios activados	215
Figura K 25. Datos obtenidos en el escenario.....	215

ÍNDICE DE TABLAS

Tabla 1 Diferencias SNMP v1,v2 y v3	18
Tabla 2. PDU de GetRequest, GetNextRequest, SetRequest, GetResponse.....	27
Tabla 3. Equipos del Data center	48
Tabla 4. Switches Planta baja.....	52
Tabla 5. Switches planta alta 1	53
Tabla 6. Switches planta alta 2.....	54
Tabla 7. Switches planta alta 3.....	55
Tabla 8. Switches planta alta 4.....	56
Tabla 9. Comparación de software en base al SRS.....	75
Tabla 10. Requerimientos de hardware para CentOS 7	78
Tabla 11. Requerimientos de hardware de Zabbix.....	79
Tabla 12. Incremento de equipos de conmutación anual	79
Tabla 13. Comparación de equipos	81
Tabla 14. Especificaciones técnicas de IBM 3200.....	111
Tabla 15. Clasificación de fallos en Zabbix.....	123
Tabla 16. Límites de rendimiento	132
Tabla 17. Costos de Software.....	141
Tabla 18. Presupuesto total	141

RESUMEN

La administración de redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y debidamente documentada. Tiene como objetivo mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, así como hacer uso eficiente de la red y utilizar mejor los recursos de la misma. Hoy en día las instituciones públicas dependen más que nunca de su infraestructura informática. La disponibilidad constante, sin interrupciones, y el rendimiento óptimo de la red, se han convertido en factores fundamentales ya que el más pequeño problema con la red puede tener efectos negativos.

La red interna del Edificio Central de la Universidad Técnica del Norte, al tener una gran cantidad de usuarios es una red que está sujeta a cambios e inconvenientes frecuentes. La complejidad de la red hace que la tarea de mantener el correcto funcionamiento de la misma sea difícil. Al suscitarse un problema en alguno de los componentes de la red, éste no se notifica de manera automáticamente, además es necesario que el administrador de red y su equipo de trabajo verifiquen personalmente el funcionamiento de los equipos para encontrar la falla. Otro inconveniente es que al no tener registros que acerca de los eventos que se producen en la red no se pueden aplicar medidas preventivas.

Se implementa un modelo de gestión de red en el Edificio Central de la Universidad Técnica del Norte en base a las áreas funcionales que contempla el modelo de gestión de red ISO/OSI, siendo éstas: Gestión de configuraciones, gestión de fallos, gestión de contabilidad, gestión de prestaciones y gestión de seguridad. Mediante la implementación de software de distribución libre se consigue un sistema de gestión de red que cubre las cinco áreas funcionales mencionadas,

brindando una red continuamente monitoreada, en donde los problemas que se pueden suscitar son detectados a brevedad. Se establecen políticas y manuales de procedimientos en concordancia con las cinco áreas funcionales que propone el modelo de gestión de red ISO/OSI, para que sirvan como guía para la adecuada utilización del sistema de gestión de red y sus componentes.

ABSTRACT

Network management is a set of techniques aimed at maintaining an operational network, efficient, secure, constant monitored and with adequate and properly documented planning. It aims to improve the continuity in the operation of the network with the proper use of control and monitoring, as well as to make efficient use of the network and to make better use of its resources. Today, public institutions depend more than ever on their IT infrastructure. Constant uninterrupted availability and optimal network performance have become critical factors and the smallest problem with the network can have negative effects.

The internal network of the Central building of Universidad Técnica del Norte, which has a large number of users, is a network that is subject to frequent changes and drawbacks. The complexity of red makes the task of keeping the correct operation of the sea difficult. When a problem arises in the network components, this is not the notification automatically, it is also necessary that the administrator of red and his work team personally verified the operation of the equipment to find the fault. Another drawback is that there are no records that on the events that occur in the red cannot apply preventive measures.

A network management model is implemented in the Central building of the Technical University of North in the base of the functional areas that contemplate the management model of the ISO / OSI network, being these: Configuration management, fault management, management Accounting, performance management and security management. By implementing the distribution software freely, a red management system is achieved that covers the five functional areas mentioned, providing a continuously monitored network, where problems that can be created are detected briefly. Policies and procedures manuals are established in accordance with the five

functional areas proposed by the ISO / OSI red management model, for which they serve as a guide for the convenient application of the red management system and its components.

PRESENTACIÓN

El presente proyecto se desarrolló con el fin de mejorar la disponibilidad de la red de datos del Edificio Central de la Universidad Técnica del Norte, mediante la implementación del modelo de gestión de red ISO/OSI abarcando todas sus áreas funcionales.

Durante el desarrollo de este proyecto, se analizó la información referente a la gestión de redes, protocolo SNMP, modelo de gestión de red ISO/OSI y sus áreas funcionales. Se realizó un levantamiento de información acerca de la red de datos del Edificio Central de la UTN, para conocer su situación actual.

Una vez analizada la situación actual de la red, se procede a implementar un software de gestión de red, en base a los requerimientos de la misma y en concordancia con las cinco áreas funcionales del modelo de gestión de red ISO/OSI.

Se establecen políticas y manuales de procedimientos para que sirvan como guía para la adecuada utilización del sistema de gestión de red y sus componentes.

CAPÍTULO I

1. ANTECEDENTES

En este capítulo se presenta el modelo de anteproyecto previamente aprobado, el cual contiene la propuesta realizada para la implementación del proyecto.

1.1. Tema

Diseño e implementación de un modelo de gestión de red para la red de área local del Edificio Central de la Universidad Técnica del Norte en base al modelo de gestión OSI con el protocolo SNMP.

1.2. Problema

Las instituciones educativas por lo general manejan redes de datos complejas debido al gran número de usuarios que tienen que soportar. Estas redes están sujetas a constantes problemas y cambios, lo cual dificulta al administrador mantener la red en correcto funcionamiento. En la actualidad existen herramientas, modelos y protocolos que pueden ser implementados en una red para lograr una administración eficiente aun cuando se susciten problemas en la misma.

La red de datos alámbrica del Edificio Central de la Universidad Técnica del Norte cuenta con una numerosa cantidad de usuarios, quienes diariamente hacen uso de dispositivos conectados a la red para desempeñar actividades administrativas, adicionalmente este Edificio cuenta con los equipos de core y de distribución que permiten tanto la conexión hacia la nube de Internet como la conexión de la red de datos de toda la institución. Al presentarse un problema dentro de la red éste no se notifica de manera automática e inmediata, además es necesario que el o los encargados de administrar la misma verifiquen personalmente el funcionamiento de los equipos para encontrar la falla. Otro inconveniente es que no se pueden aplicar medidas preventivas puesto que no se

generan registros que detallen la información acerca de configuraciones, fallas, seguridad, contabilidad y rendimiento de los dispositivos que participan en la red.

Por los antecedentes citados es necesario implementar un modelo que permita administrar y gestionar eficientemente la red de área local del Edificio Central de la Universidad Técnica del Norte y sus recursos para solucionar los problemas en menor tiempo, mejorando así el servicio que se presta a los usuarios de la red.

1.3. Objetivos

Se detalla el objetivo general y los objetivos específicos

1.3.1. Objetivo General

Plantear un modelo de administración y gestión de la red de área local del Edificio Central de la Universidad Técnica del Norte, a través de la implementación de una herramienta de gestión, en base al modelo de gestión OSI con el protocolo SNMP, para mejorar el rendimiento de la red.

1.3.2. Objetivos Específicos

Analizar el modelo de gestión de red OSI y del protocolo SNMP para aplicarlo en la red de área local del Edificio Central de la Universidad Técnica del Norte.

Realizar el levantamiento de la situación actual de la red de área local del Edificio Central de la Universidad Técnica del Norte, para conocer los requerimientos de administración de la red.

Determinar políticas de gestión que se ajusten a las necesidades de la red para cumplir con las áreas que se definen en el modelo de gestión de red OSI.

Analizar herramientas de administración y gestión Open Source para definir cuál es la idónea para realizar la administración de la red según los requerimientos que ésta tenga.

Realizar la implementación de una herramienta de administración en la red alámbrica del Edificio Central para realizar el monitoreo de sus recursos.

Realizar un análisis Costo-beneficio para determinar qué tan factible es la implementación de la herramienta de gestión.

1.4. Alcance

Se propone un modelo de administración y gestión en la red de área local del Edificio Central de la Universidad Técnica del Norte con una herramienta Open Source utilizando como base el modelo de gestión ISO/OSI y el protocolo SNMP que permita monitorear la red para conocer su estado mediante el intercambio de información entre gestor y agente.

Inicialmente se realiza una investigación acerca del modelo de gestión ISO/OSI. De esta manera se conoce el papel que cumple cada una de sus áreas funcionales. También se investiga acerca del protocolo SNMP.

Se recopila información acerca del estado físico y lógico actual de la red alámbrica del Edificio Central de la Universidad Técnica del Norte, dentro de lo que se destaca la ubicación y modo de interconexión de los equipos de red, así como su direccionamiento IP. Los datos encontrados se utilizan para definir los requerimientos de la red en cuanto a la administración.

Se determina las políticas de gestión necesarias respecto a la administración de la red y de los procedimientos que se deben seguir para cumplir con los requerimientos de la red. Estas políticas se definen también en base al modelo ISO/OSI y sus áreas funcionales: gestión de fallos, gestión de configuraciones, gestión de contabilidad, gestión de rendimiento y gestión de seguridad.

Se analizan diferentes herramientas de gestión de redes, en base a sus características se elige a la herramienta que cumple en el mayor grado con las necesidades de la red y con las áreas funcionales del modelo ISO/OSI. La comparativa se realiza entre herramientas Open Source porque como institución pública se promueve el uso de este tipo de plataformas.

Se realizan las respectivas configuraciones para poner en funcionamiento la herramienta de administración en el Edificio de Central de la Universidad Técnica del Norte, con el fin de empezar con el proceso de administración y que sea un punto de partida para la implementación en otras facultades y dependencias de la institución. La gestión se realiza sobre los dispositivos de acceso y de distribución, mediante la habilitación de los protocolos correspondientes para permitir la comunicación entre el gestor y los agentes. A continuación, se detallan las áreas funcionales que cubre el modelo de gestión:

En la gestión de fallos se realizan los procesos adecuados para detectar, aislar y corregir problemas que pueden suscitarse en los equipos de la red. La notificación de fallas se hace en tiempo real mediante alarmas y el envío de un correo electrónico al administrador de la red para que se pueda dar con una solución lo más pronto posible.

Con respecto a la gestión de configuración, se realiza el levantamiento de información de la red para conocer su estado físico y lógico. En base a las políticas de gestión se realizan los procedimientos de reconfiguración, cambios y adición de elementos de red dentro del sistema de gestión.

En gestión de contabilidad se ejecuta el proceso de medición del grado de utilización de los recursos de la red por parte de los usuarios para comprobar que haya una distribución adecuada de los mismos. Esta área incluye el inventario de los equipos sujetos a la monitorización.

En la gestión de prestaciones se realiza la medición del rendimiento de la red mediante el monitoreo de indicadores de prestaciones, los cuales se orientan al grado de satisfacción de usuarios y al grado de utilización de recursos y servicios. Se establecen los niveles mínimos a los que debe llegar el rendimiento de la red.

La gestión de seguridad se realiza mediante la protección del sistema de administración y gestión contra ingresos no autorizados lo cual sirve para garantizar confidencialidad. Únicamente quien administre de la red tiene acceso a este sistema, recibe las alertas y puede realizar las configuraciones necesarias.

Cada una de las áreas funcionales descritas anteriormente tiene su respectivo manual de procedimientos, el mismo que se entrega al administrador de la red.

Tomando en cuenta los resultados obtenidos tras la implementación del software de administración, se realiza un análisis costo-beneficio con el fin de conocer la factibilidad del proyecto.

1.5. Justificación

En nuestro país el Gobierno Nacional ha contribuido al desarrollo de los proyectos tecnológicos a través del cumplimiento del objetivo 11 del Plan Nacional del Buen Vivir 2013-2017, en el cual se promueve el uso intensivo de las tecnologías de la información y comunicación en beneficio de la ciudadanía. La Universidad Técnica del Norte al ser una entidad educativa pública requiere de la implementación de un modelo de gestión de red, especialmente en su Edificio Central ya que es aquí donde se realizan las actividades administrativas de la institución y además se alojan los equipos de core y de distribución cuyo funcionamiento es crítico para garantizar la disponibilidad de toda la red de la Universidad Técnica del Norte.

Actualmente las políticas de Estado establecen que en todas las entidades de administración pública utilicen herramientas Open Source en sus sistemas, según el decreto 1014 firmado en el año 2008. Este por este motivo que la propuesta de administración se realiza con este tipo de herramientas.

En una red es importante conocer constantemente el estado de los recursos que la conforman, con la finalidad de prevenir problemas y anticiparse a los efectos que produce una falla en la red y que perjudican las actividades de los usuarios. Al implementar una herramienta de administración el administrador de la red es capaz de encontrar una solución a tiempo, en caso de que suceda un fallo o en el mejor de los casos una solución proactiva. Una vez implementada la herramienta de gestión de red se logrará prestar un mejor servicio lo cual beneficiará tanto a los usuarios como al administrador de la red de datos del Edificio Central de la Universidad técnica del Norte.

La importancia de este proyecto radica en la aplicación de los conocimientos adquiridos durante el transcurso de mi carrera universitaria con énfasis en el área de las redes de comunicación. La implementación de este proyecto está enfocada en dejar un trabajo que beneficie a la Universidad Técnica del Norte, siendo más específico a la red de datos que maneja el área administrativa de esta institución

CAPÍTULO II

2. Marco teórico

En este capítulo se presentan los conceptos generales sobre administración y gestión de red, se analizan los modelos y protocolos de gestión de red. Adicionalmente se analizan algunas herramientas que se utilizan para monitorear una red.

2.1. Conceptos generales

En este apartado se presentan los conceptos de: administrar, gestionar y gestión de red.

2.1.1. Administrar

El término administrar se refiere a una serie de acciones que se ejecutan por una organización para conseguir fines determinados. "La administración es el conjunto de las funciones o procesos básicos (planificar, organizar, dirigir, coordinar y controlar) que, realizados convenientemente, repercuten de forma positiva en la eficacia y eficiencia de la actividad realizada en la organización" (Diez de Castro, García del Junco, Martín Jiménez, & Perriñez Cristóbal, 2000, pág. 4). Los objetivos que persigue la administración se enfocan en obtener el mejor rendimiento de determinado recurso.

2.1.2. Gestionar

De acuerdo a Villamayor y Lamas (1998), "Gestionar es una acción integral, entendida como un proceso de trabajo y organización en el que se coordinan diferentes miradas, perspectivas y esfuerzos, para avanzar eficazmente hacia objetivos asumidos institucionalmente" (Villamayor & Lamas, 1998). Por lo tanto, la gestión hace referencia a los procesos realizados conjuntamente por los miembros de una organización para alcanzar determinados objetivos.

2.1.3. Gestión de red

La gestión de red, según Barba Martí (1999) engloba diferentes aspectos como la planificación organización, supervisión y control de los elementos de un sistema de comunicaciones con el objetivo de dar un determinado nivel de servicio bajo cierto costo. La gestión de red se enfoca básicamente en proveer una mejor disponibilidad y rendimiento del sistema.

A medida que una red de datos crece y se hace más compleja requiere aún más de un adecuado sistema de gestión que permita dar el mejor servicio posible. Por lo general en redes de gran tamaño se presenta el problema de la heterogeneidad provocado por la implementación de equipos de distintos fabricantes. Este tipo de empresas no pueden optar por soluciones propietarias de gestión, sino más bien deben buscar soluciones de estándares abiertos que les permitan asegurar la compatibilidad dentro del sistema de gestión (Barba, 1999). Para dar solución a este problema se crearon los protocolos de gestión SNMP (Simple Network Management Protocol) y CMIP (Common Management Information Protocol).

La gestión de redes parte de los recursos humanos, quienes para lograr obtener una red eficiente emplean una serie de herramientas diseñadas para ello y también se basan en metodologías. Organismos internacionales de estandarización como la ITU-T son los encargados de proporcionar estas recomendaciones, en este sentido para la gestión de telecomunicaciones, se definió el estándar TMN (por sus siglas en inglés Telecommunications Management Network). (Barba, 1999)

En la organización de la gestión se tiene el control operacional, en el cual todas las operaciones realizadas deben ser registradas para que posteriormente las analice el administrador de la red. De acuerdo a Barba (1999), estas operaciones incluyen la recolección de datos referentes a las prestaciones, contabilidad, evaluación de alarmas, diagnóstico de fallos, la puesta a punto de los

elementos de la red, ejecución de pruebas preventivas y configuraciones de software. El seguimiento y la elaboración de informes acerca de las tareas de control operacional se realizan con el fin de garantizar la calidad de servicio pues se llevan registros acerca de los problemas que ocurren en la red, mantenimiento de inventario, mantenimiento de configuraciones, evaluación de tráfico control de ° y contabilidad.

2.2. Elementos de la gestión de red

La gestión de red consta de tres elementos: Agentes, Gestores y Dispositivos Administrado.

2.2.1. Gestor

También se le denomina Sistema de gestión de redes o por sus siglas en Ingles Network Management Station (NMS). El Gestor, se encarga de realizar la supervisión y control permanente de los dispositivos gestionados. En una red puede haber uno o más gestores según sus requerimientos.

2.2.2. Agente

El agente es el software de administración de red que se encuentra en el dispositivo para que pueda ser gestionado. El agente alberga a las MIB (base de datos local de información de administración), las cuales se organizan en jerarquías y se traducen al formato adecuado según el protocolo de administración que se esté ejecutando.

2.2.3. Dispositivo administrado

Es el dispositivo que posee un agente SNMP para poder ser administrado. Estos dispositivos pueden ser: routers, servidores, switches, bridges, hubs, computadoras e impresoras.

2.3. Procesos de gestión de red

Dentro de la gestión de red se lleva a cabo dos procesos: Monitoreo y Control.

2.3.1. Monitoreo

El proceso de monitoreo se basa en funciones de lectura que se encargan de mantener la información del comportamiento de la red.

La monitorización es usada para obtener información acerca de las gestiones de prestaciones, fallos, contabilidad y a veces de la gestión de configuraciones.

La monitorización es un proceso que se compone de varios pasos. En primer lugar, se define la información que será monitorizada, un método de acceso a esta información, un diseño de mecanismos para monitorización y por último el procesamiento de la información de gestión obtenida durante la monitorización (Barba, 1999).

En la monitorización la información puede clasificarse en estática, dinámica y estadística. De acuerdo con Barba (1999), la información estática es aquella que se almacena en el dispositivo monitorizado, mientras que la información dinámica es almacenada en el dispositivo o en otros equipos especializados. Por otra parte, la información estadística se obtiene a partir de la información dinámica y se encuentra en el mismo lugar.

La monitorización se realiza cuando el gestor efectúa un sondeo o polling accediendo de manera periódica a la información de gestión que almacenan los dispositivos gestionados, es decir que estos simplemente deberán responder al gestor cuando lo necesite. Otro mecanismo consiste en que el dispositivo gestionado envíe notificaciones bajo ciertas circunstancias, se denomina event reporting y su ventaja es que genera menos tráfico en la red comparado con el mecanismo de sondeo (Barba, 1999). Es posible obtener un método mixto mediante la combinación de los dos mecanismos anteriores.

2.3.2. Control

Luego de realizar el monitoreo de la red y obtener datos relevantes de administración, el siguiente paso es utilizar el proceso de control para analizar el comportamiento de la red y definir las directrices adecuadas para asegurar su buen desempeño.

El control tiene su función en la gestión de configuración y gestión de seguridad. En el proceso de control se definen funciones de escritura, es decir que se modifican parámetros en los equipos gestionados.

2.4. Modelos de gestión de red

La gestión de red está basada en modelos, Varela (2003) señala tres modelos:

- Arquitectura TMN
- Gestión de red OSI
- Gestión de Internet

2.4.1. Modelo de gestión TMN

TMN (Telecommunications Managed Network) es el modelo de administración de red desarrollado por la Unión Internacional de Telecomunicaciones (ITU). Esta infraestructura está diseñada para lograr la comunicación e interconectividad entre sistemas de telecomunicaciones heterogéneos. TMN se limita únicamente a soluciones de gestión de red que cumplen estrictamente con los estándares fijados por la ITU.

Varela (2003), define las siguientes funciones del modelo de gestión TMN:

- Administración remota de los elementos del sistema.
- Proveer al cliente una interfaz amigable y de fácil interacción.

- Incrementar la automatización al momento de solucionar problemas que involucren a los clientes y servicios.
- Brindar integración e interoperabilidad entre diferentes protocolos y tecnologías.

El modelo TMN tiene una estructura jerárquica dividida en niveles definidos para brindar escalabilidad, eficiencia y operación óptima en la administración y gestión de empresas y redes de telecomunicaciones (Varela, 2003). La Figura 2 muestra los niveles lógicos de administración definidos por el modelo TMN. Cada uno de estos niveles tiene sus determinadas funciones y reglas. Los niveles más bajos desempeñan funciones específicas mientras que los niveles superiores se encargan de una serie de funciones mucho más amplia.

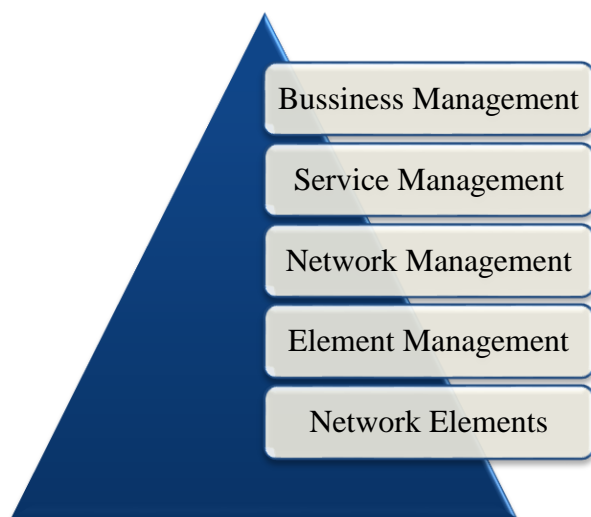


Figura 1. Niveles funcionales del modelo TMN

Fuente: (Varela, 2003)

2.4.2. Modelo de gestión ISO

La International Organization for Standardization (ISO) desarrolló un modelo de gestión de red, el cual consta de cinco áreas funcionales:

- Gestión de configuraciones
- Gestión de rendimiento
- Gestión de fallos
- Gestión de contabilidad
- Gestión de seguridad

2.4.2.1. Gestión de configuraciones

La gestión de configuraciones se encarga de mantener la información acerca de la configuración actual de los equipos de la red. La información de la gestión de configuraciones indica que está instalado, donde está instalado, como está conectado, quien es el responsable de cada cosa y como comunicarse con él (Alarcón, 2007). La importancia de esta gestión radica en que una mala configuración de los elementos de la red puede causar que ésta tenga un mal desempeño o en el peor de los casos no funcione.

Millán Tejedor (1999) afirma que la gestión de configuración consiste en la realización de tres tareas fundamentales:

- Recolección automatizada de datos sobre el inventario y estado de la red, tales como versiones software y hardware de los distintos componentes.
- Cambio en la configuración de los recursos.
- Almacenamiento de los datos de configuración.

2.4.2.2. *Gestión de rendimiento*

También puede ser llamada gestión de prestaciones, se enfoca en garantizar niveles adecuados de rendimiento de la red. La gestión de rendimiento requiere información acerca del tráfico, tasas de errores, utilización, esto se obtiene a través del monitoreo constante de la red. Tras recolectar los datos se pueden generar informes cuya información es útil para mejorar el funcionamiento de la red (Alarcón, 2007). Para garantizar los niveles de rendimiento requeridos se deben tomar las siguientes medidas:

- **Disponibilidad:** es el porcentaje de tiempo que una red, dispositivo o aplicación se encuentra disponible para el usuario.
- **Tiempo de respuesta:** indica el tiempo que tarda en aparecer la respuesta en el terminal del usuario cuando éste realiza una acción.
- **Fiabilidad:** porcentaje de tiempo en el que no se presentan errores en la transmisión de información.

Por otra parte, la gestión de prestaciones según Millán Tejedor (1999), se basa en cuatro tareas:

- Recogida de datos o variables indicadoras de rendimiento, tales como el throughput¹ de la red, los tiempos de respuesta o latencia, la utilización de la línea, etc.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.

¹ Throughput: Velocidad real de transporte de datos a través de una red telemática, el cual normalmente se mide en Mbit/s y siempre será inferior al ancho de banda.

- Determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

2.4.2.3. *Gestión de fallos*

La gestión de fallos conlleva identificar, aislar y resolver la falla que pueda presentarse en la red. Esta gestión aporta mayor fiabilidad a la red debido a que un fallo puede comprometer el buen funcionamiento de una parte o a toda la red.

De acuerdo a Millán (1999), la gestión de problemas de red implica las siguientes tareas:

- Determinación de los síntomas del problema.
- Aislamiento del fallo.
- Resolución del fallo.
- Comprobación de la validez de la solución en todos los subsistemas importantes de la red.
- Almacenamiento de la detección y resolución del problema.

2.4.2.4. *Gestión de contabilidad*

Se refiere a la contabilidad de la utilización de la red y sus servicios (Facturación). En esta gestión es posible monitorear la carga de usuarios, el tipo y nivel de tráfico que circula habitualmente por un puerto.

Alarcón (2007), afirma que las tareas que se deben realizar en la gestión de contabilidad son:

- Recolección de datos sobre la utilización de los recursos.
- Establecimiento de cuotas.
- Cobro a los usuarios con las tarifas derivadas de la utilización de los recursos.

2.4.2.5. Gestión de seguridad

Se enfoca en proporcionar un grado de seguridad a la red. Esta área engloba distintos servicios como: autenticación, confidencialidad, control de acceso e integridad.

Según Millán (1999), entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Identificación de recursos sensibles en la red, tales como ficheros o dispositivos de comunicaciones.
- Determinación de las relaciones entre los recursos sensibles de la red y los grupos de usuarios.
- Monitorización de los puntos de acceso a los recursos sensibles de red.
- Almacenamiento de los intentos de acceso no autorizados a estos recursos, para su posterior análisis.

2.4.3. Modelo de gestión Internet

Los fabricantes, en su mayoría, son capaces de soportar estándares de gestión SNMP. En el modelo TCP/IP el protocolo de gestión de red es SNMP, el cual utiliza los servicios que ofrece TCP/IP.

2.5. Protocolos de gestión

De acuerdo con Millán (2004), los protocolos de gestión más importantes son SNMP y CMIP. La utilización de más de un protocolo de gestión simultáneamente no es recomendable, ya que tal combinación incrementaría la complejidad de la red.

2.5.1. CMIP

El protocolo de gestión CMIP se desarrolló en base al protocolo SNMP corrigiendo sus falencias, por lo que se considera un protocolo más eficiente. Sin embargo, según afirma Millán (2004), el protocolo CMIP no ha tenido mucho uso en las redes empresariales pues no todas tienen la capacidad de realizar una implementación completa debido a su complejidad, la cual conlleva altos costos. En contraste CMIP tiene mayor uso en redes de operadoras de telecomunicación.

El protocolo CMIP permite desarrollar tareas más complejas con respecto a SNMP, pero también puede presentar ciertos inconvenientes. La desventaja de usar CMIP para el usuario es que se utiliza diez veces más recursos de red respecto a SNMP (Millán, 2004). Esto quiere decir que se requiere mayor capacidad de procesamiento y de memoria en los routers y servidores. En cuanto al desarrollo de nuevas aplicaciones, CMIP resulta un protocolo muy complejo por lo que se requieren programadores más experimentados.

2.5.2. SNMP

SNMP fue el primer protocolo de gestión creado en 1988. Se trata de un protocolo de capa aplicación cuyo origen fue provisional, sin embargo, llegó a convertirse en el estándar de facto debido a su masiva utilización en redes empresariales (Millán, 2004). SNMP al ser un protocolo sencillo ayuda a reducir tiempo y costos al momento de desarrollar nuevas aplicaciones y actualizaciones.

SNMP trabaja comúnmente sobre el protocolo UDP y tiene la ventaja de soportar otros protocolos como OSI CLNS, DDP, AppleTalk, entre otros. De acuerdo a Millán (2004), una desventaja que presenta SNMP es su alto consumo de ancho de banda en entornos de red extendidos, lo cual dificulta la optimización del tráfico de la red.

En términos de seguridad el protocolo SNMP inicialmente presentaba un alto grado de vulnerabilidad frente a ataques debido a mecanismos de autenticación demasiado débiles y falta de cifrado (Millán, 2004). Sin embargo, estas y otras falencias se solucionaron en la tercera versión del protocolo.

2.5.2.1. Versiones SNMP

- **SNMPv1:** Diseñado a mediados de los 80. Fue una solución temporal hasta la llegada de protocolos de gestión de red más completos.
- **SNMPv2:** Es la evolución del protocolo SNMP que apareció en el año 1993. A diferencia de la primera versión SNMPv2 cuenta con un mayor número de colecciones de datos, códigos de error y operaciones.
- **SNMPv3:** Es la última versión del protocolo SNMP creada en 1997. Esta versión no es un reemplazo de sus antecesoras SNMPv1 y SNpv2, sino que debe ser usada en conjunto con éstas para proveer mejores prestaciones en cuanto a seguridad y administración.

Las principales diferencias entre las versiones SNMP se muestran en la Tabla 1.

Tabla 1 Diferencias SNMP v1, v2 y v3

	SNMPv1	SNMPv2	SNMPv3
Estándares	RFC-1155.1157.1212	RFC-1441,1452 RFC-1909.1910 RFC- 1901 a 1908	RFC-1902 a 1908, RFC-2271 a 2275
Versión	Fue la primera versión de SNMP	SNMPv2 existe en al menos tres	actualmente Es la versión más nueva

		variantes, SNMPv2c, SNMPv2u y SNMPv2	
Seguridad	Ninguna seguridad	No mejoró la seguridad	Su principal característica es la mejora en la seguridad
Complejidad	Limitaciones en rendimiento y seguridad	Más potente pero más complejo que en la primera versión	Se centra en mejorar el aspecto de la seguridad
Tipos de paquetes	<ul style="list-style-type: none"> • Get-Request • Get-Next-Request • Set Request • Get Response 	<ul style="list-style-type: none"> • Get-Request • Get-Bulk-Request • Get-Next-Request • Set Request • Inform-Response • SNMP v2 Trap 	Las funciones básicas de v3 son de v1 y v2. La versión 3 tiene un nuevo formato de mensaje SNMP
Secuencias de comunidad en texto plano	Si	Si	No
Encriptación de tráfico	No	Si	Si

Fuente: (SolarWinds, 2013) y (Ques10, 2014)

2.5.2.2. *Arquitectura SNMP*

Según el RFC 1157 la arquitectura SNMP es un conjunto de estaciones gestionadas y elementos de red. Las estaciones de gestión de red ejecutan aplicaciones que se encargan de monitorear y controlar los elementos de la red. Los elementos de red son dispositivos tales como hosts, gateways, servidores, y dispositivos similares, los cuales poseen agentes de gestión responsables de desempeñar las funciones de gestión de red solicitadas por las estaciones de gestión de red. El protocolo SNMP se utiliza para intercambiar información entre las estaciones de gestión y los agentes instalados en los elementos de red.

Case, Fedor, Schoffstall, & Davin (1990), afirman que los objetivos de la arquitectura SNMP son:

- Minimizar la cantidad y complejidad de las funciones de gestión ejecutadas por el agente de administración. Se reduce el costo de desarrollo de software para el agente. El grado de función de gestión se incrementa, permitiendo el uso óptimo de los recursos de Internet e imponiendo el menor número de restricciones sobre la sofisticación y forma de las herramientas de administración. Y se facilitan las funciones de administración para los desarrolladores de herramientas de gestión.
- Hacer que el paradigma funcional para control y monitoreo sea lo suficientemente extensible como para acomodar aspectos adicionales, posiblemente aspectos no anticipados de funcionamiento de la red y administración.
- Lograr que la arquitectura sea lo más independiente posible de la arquitectura y mecanismos de hosts y gateways particulares.

2.5.2.3. Funcionamiento SNMP

SNMP opera con el protocolo de transporte TCP/IP. Básicamente el funcionamiento de SNMP se basa en obtener y almacenar. La información se obtiene mediante la colección de MIB (por sus siglas en inglés, Management Information Base), este proceso consiste preguntar a cada dispositivo su estado actual y realizar una copia de esta información en el dispositivo gestionado y en su MIB local (Millán , 2004). De esta manera el gestor obtiene la información del agente.

El esquema y funcionamiento de la arquitectura SNMP se muestran en la Figura 2. El agente mantiene información del elemento gestionado referente a su estado y configuración. Utilizando el protocolo de gestión SNMP el gestor ordena al agente realizar operaciones en base a los datos obtenidos en la gestión. Si un dispositivo gestionado presenta alguna anomalía, su agente enviará notificaciones al gestor sin que este lo haya solicitado permitiendo así que el sistema de gestión actúe en consecuencia.

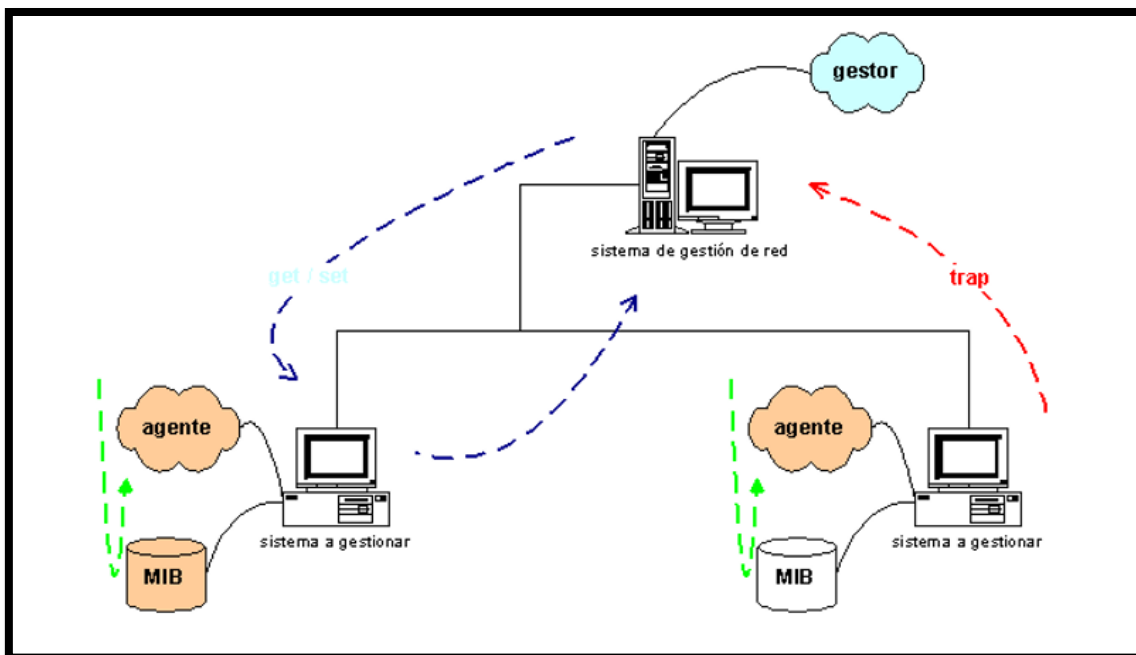


Figura 2. Esquema de una red gestionada con SNMP

Fuente: Recuperado de: <http://www.ramonmillan.com/tutoriales/snmpv3.php>

2.5.2.4. Elementos de SNMP

Stallings (2004), afirma que los elementos fundamentales del modelo de gestión SNMP son:

- Estación de gestión
- Agente de gestión
- Base de información de gestión
- Protocolo de gestión de red

2.5.2.4.1. Estación de gestión

NMS (Network Management System) también denominado Administrador SNMP es la entidad encargada de enviar peticiones al agente para poder obtener su información. El NMS ejecuta el monitoreo de la red mediante la recuperación del valor de las MIBs, responde a las peticiones del usuario y puede cambiar o modificar la configuración de un agente o hacer que este ejecute una

determinada acción (Stallings, 2004). La información que recoge la estación de gestión se registra y analiza de tal forma que sea de utilidad para el administrador de la red.

Según los requerimientos, una red puede necesitar más de una aplicación de gestión. De acuerdo con Stallings (2004), es necesario que el nodo que desempeña la función de NMS sea una estación con suficiente memoria RAM para que se puedan ejecutar todas las aplicaciones de administración que deben correr al momento. Las aplicaciones de administración de red se denominan NMA (por sus siglas en inglés, Network Management Station), este es el software alojado en el NMS que presenta una interfaz de usuario al administrador de la red.

2.5.2.4.2. *Agente de gestión*

El agente es el encargado de responder a las peticiones de monitorización y control que provienen desde una estación gestora. También es posible que éste provea información importante al NMS sin que dicha acción haya sido solicitada.

2.5.2.4.3. *Protocolo de gestión de red*

Para que exista comunicación entre la estación gestora y el agente se necesita un protocolo de gestión de red. Para las redes TCP/IP se utiliza el protocolo SNMP. Stallings (2004), afirma que las funciones fundamentales del protocolo de gestión de red SNMP son: get, set y notify.

2.5.2.4.4. *Base de información de gestión*

La MIB (Management Information Base) permite tener acceso a la información de gestión que se encuentra almacenada en la memoria interna del dispositivo gestionado. Las MIB tienen estructura en árbol, lo cual permite manejar diferentes grupos de objetos. (Huidrobo, 2005)

Los dispositivos gestionados mantienen valores para un número de variables y los reportan cuando el NMS los solicita, el agente puede reportar datos como, por ejemplo, el número de bytes

y paquetes que entran y salen del dispositivo (Cisco, 2007). Cada variable se conoce como un objeto gestionado, el cual es todo lo que un agente puede tener acceso e informar al NMS.

Todos los objetos gestionados están contenidos en la MIB. Estos pueden ser modificados o leídos para proporcionar información sobre los dispositivos e interfaces de red. De acuerdo a Cisco (2007), el NMS es capaz de controlar un dispositivo gestionado mediante el envío de un mensaje al agente de dicho dispositivo, en cual se ordene que el dispositivo modifique el valor de sus variables.

Las MIB pueden ser estándar o de empresa. Las MIB estándar están definidas por IETF (Internet Engineering Task Force) y publicadas como RFC. Las MIB de empresa están definidas por otras organizaciones.

El estándar MIB es MIB-II, es decir, la segunda versión de SNMP MIB.

Según CISCO (2007), la MIB es un árbol en el cual las hojas representan ítems individuales de datos denominados objetos o variables. Un ejemplo de objeto puede ser un contador o estado de protocolo. Un MIB object está compuesto de los siguientes valores:

- **Object type:** Identifica el tipo de MIB object.
- **Syntax:** Identifica el tipo de dato del objeto.
- **Access:** Identifica el máximo nivel de acceso.
- **Status:** El estado del objeto administrado.
- **Description:** Provee una descripción textual del objeto administrado.

Cada objeto en la MIB tiene un Object Identifier (OID), el cual es usado por el NMS para solicitar al agente el valor de un objeto. Un OID está compuesto por una secuencia de números

enteros que identifica de forma única a un objeto gestionado por la definición de una ruta de acceso al mismo mediante una estructura de árbol conocido como árbol de registro o árbol OID (SNMP agent MIB Reference, 2007). Si un agente requiere acceder a un determinado objeto, se recorre el árbol OID para encontrarlo.

2.5.2.5. Mensajes SNMP

Los mensajes en SNMP pueden clasificarse en tres tipos: lectura, escritura y notificación.

Los mensajes de lectura son información recuperada desde los objetos gestionados por un agente, indican la situación actual del dispositivo obtenida mediante el monitoreo. En este grupo están los mensajes Get.

Los mensajes de escritura son aquellos en los que el administrador ordena crear o cambiar la configuración de las instancias de un objeto administrado. En este grupo están los mensajes Set.

Las notificaciones son mensajes enviados por un agente hacia el administrador para informar la aparición de una anomalía en el dispositivo gestionado. Estos son los Traps.

La Figura 3 muestra cómo se ejecuta la comunicación entre el gestor y el agente. El intercambio de los mensajes SNMP se realiza desde el gestor hacia al agente y viceversa dependiendo del tipo de mensaje.

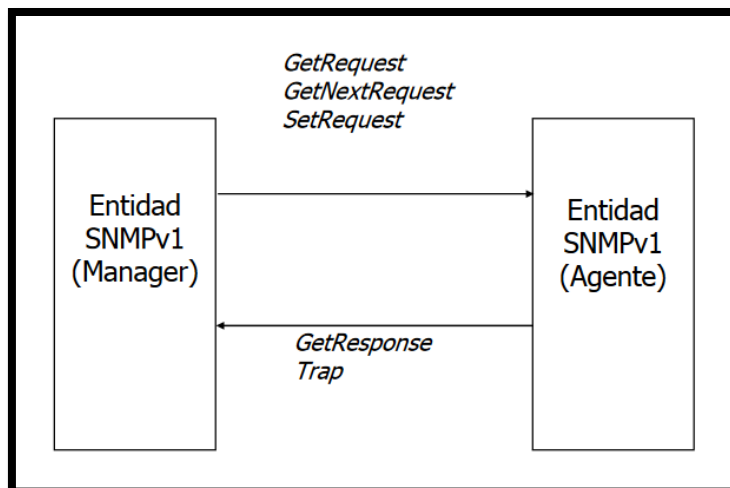


Figura 3. Intercambio de mensajes en SNMPv1

Fuente: Recuperado de: <http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/SNMP.pdf>

Mensajes desde el nodo de gestión:

GetRequest: Obtener el valor de objetos MIBs

GetNextRequest: Obtener el valor de un objeto MIB y puede moverse en la tabla MIB.

SetRequest: Escribe el valor de las instancias de un objeto.

GetBulkRequest: Similar a la operación GetNext, obtiene el valor de un bloque grande de datos

InformRequest: El gestor proporciona valores MIB a otro gestor.

Mensajes desde el agente:

GetResponse: Respuestas de los agentes a los NMS, cuyo contenido es el valor solicitado.

Trap: Mensaje o notificación enviada desde el agente hacia el NMS para informar sobre un evento.

2.5.2.5.1. PDU de los mensajes SNMP

De acuerdo a García (1998), el mensaje SNMP consta de los campos: versión, comunidad y PDU. La estructura del mensaje se muestra en la Figura 4:

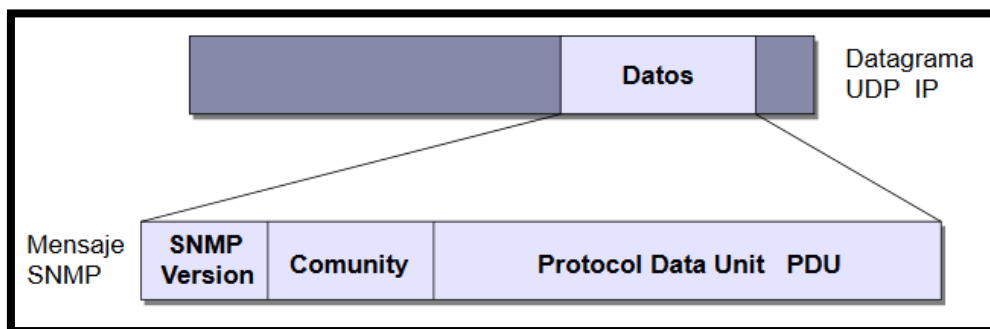


Figura 4. Mensaje SNMP

Fuente: (García Yague, 1998)

- **Version:** Versión del protocolo SNMP
- **Community:** Este campo cumple la función de enviar la identificación básica del usuario. Se usa para controlar el acceso no autorizado a un elemento SNMP.
- **Protocol Data Unit (PDU):** En este campo se envían las peticiones que el usuario desea realizar sobre un determinado dispositivo y los mensajes que envía el agente hacia el usuario.

El PDU de los mensajes *GetRequest*, *GetNextRequest*, *SetRequest*, *GetResponse* se muestran en la Tabla 2. Según IBM (2014), están compuestos de los siguientes campos:

Tabla 2. PDU de *GetRequest*, *GetNextRequest*, *SetRequest*, *GetResponse*

Version	Community name	PDU type	Request ID	Error status	Error index	Variable binding list
---------	----------------	----------	------------	--------------	-------------	-----------------------

Fuente: (IBM, 2014)

- **Version:** La versión de SNMP.

- **Community name:** Nombre de la comunidad en donde se generó el PDU. Este valor puede sobrepasar los 255 caracteres.
- **PDU type:** Tipo de PDU contenido en el mensaje SNMP, puede ser: GETREQUEST, GETNEXTREQUEST, SETREQUEST y GETRESPONSE.
- **Request ID:** Un número usado para distinguir diferentes peticiones y asociarles con su respuesta correspondiente.
- **Error status:** Indica si un error a ocurrido mientras el agente estaba procesando una petición.
- **Error index:** Usado para proveer información adicional identificando qué variable de la lista causó el error.
- **Variable binding list:** Una simple lista de asignaciones de variables, que son los emparejamientos de los nombres de las variables MIB con sus valores correspondientes.

2.5.2.6. *Comunidades SNMP*

Se denomina comunidad (community) a un conjunto de gestores y a los objetos gestionados. A las comunidades se les asignan nombres, de tal forma que este nombre junto con cierta información adicional sirva para validar un mensaje SNMP y al emisor del mismo. Por ejemplo, si se tienen dos identificadores de comunidad "total" y "parcial", se podría definir que el gestor que use el identificador "total" tenga acceso de lectura y escritura a todas las variables de la base de administración de información, MIB (Management Information Base), mientras que el gestor con nombre de comunidad "parcial" sólo pueda acceder para lectura a ciertas variables del MIB.

2.5.3. RMON

RMON (Remote Monitor) es una especificación realizada por IETF para la monitorización remota en redes de área local. Funciona en base al modelo cliente/servidor, en donde el cliente es el software ejecutado en la estación gestora y el servidor es el agente, encargado de generar la información en base al tráfico de la red (Garzón Villar, Leyva Cortés, Prieto Tinoco, & Sampalo de la Torre, 2007).

RMON se encarga de definir las funciones necesarias para la supervisión de la red y las interfaces de comunicación entre la plataforma de gestión SNMP y los agentes que se encuentran en los dispositivos gestionados (Huidrobo, 2005). RMON le da la posibilidad al administrador de vigilar el tráfico y generar datos estadísticos.

El RFC 1271 define la siguiente clasificación de objetos:

- **Alarmas:** Los usuarios pueden configurar alarmas para un objeto gestionado, cualquiera que sea.
- **Estadísticas:** Mantener utilización de bajo nivel y estadísticas de error.
- **Historias:** Análisis de tendencias en base a las instrucciones de usuarios tomando en cuenta la información contenida en las estadísticas.
- **Filtros:** Memoria para paquetes entrantes y un número cualquiera de filtros que son definidos por los usuarios.
- **Ordenadores:** Tabla estadística que contiene información acerca de los datos transmitidos y recibidos, se basa en las direcciones MAC.
- **Principales Hosts:** Estadísticas de los ordenadores que designa el usuario, para que solo se reciba información útil.

- **Matriz de tráfico:** Información acerca de errores y utilización de la red.
- **Captura de paquetes:** Definición de buffers en la captura de paquetes.
- **Sucesos:** Define objetos de umbral ascendente, descendente y acoplamiento de paquetes, para los cuales se puede realizar interrupciones.

2.6. Herramientas de gestión

Actualmente existe una gran variedad de herramientas de gestión, las cuales tienen diferentes características y funcionalidades. Pueden encontrarse soluciones libres y propietarias.

2.6.1. Pandora FMS

Pandora FMS es una herramienta de monitorización para todo tipo de empresas, especialmente para grandes entornos, en los cuales ayuda a detectar tempranamente los problemas que pueden presentarse en la red a través de la gestión de servidores, comunicaciones y aplicaciones. Pandora FMS posee además un sistema de informes que permite evaluar el nivel de cumplimiento del sistema y reportar la información a los clientes (PandoraFMS, 2016). Las características principales de Pandora FMS son:

- Autodescubrimiento de la topología de la red.
- Agentes multiplataforma para Windows, HP-UX, Solaris, BSD, AIX y Linux
- Monitorización de disponibilidad y rendimiento.
- Consola visual personalizable
- Monitorización de red (SNMP,WMI,TCP,ICMP) IPv5 e IPv6.
- Monitorización de SNMP a través de polling y traps.
- Conexión SSH/Telnet a equipos desde una interfaz web.

2.6.2. CiscoWorks

CiscoWorks LAN Management Solution (LMS) es un conjunto integrado de funciones de administración diseñadas para simplificar la configuración, administración, monitoreo y solución de problemas desarrollado por Cisco networks. CiscoWorks LMS permite al operador de la red realizar la gestión a través de una interfaz basada en navegador, a la cual se puede acceder en cualquier momento desde cualquier lugar que se encuentre dentro de la red (Cisco, 2014). Las principales áreas funcionales son:

- Supervisión y solución de problemas
- Gestión de auditoría
- Generación de reportes
- Generación de inventarios
- Centros de trabajo
- Administración centralizada

2.6.3. HP Openview

HP Openview es un conjunto de software de administración de equipos empresariales o servicios electrónicos desarrollado por Hewlett-Packard (HP). Generalmente los programas de HP Openview se venden a clientes de servidores empresariales HP 9000 y e3000. Openview es utilizado para administrar aplicaciones, disponibilidad de dispositivos, estado de la red, rendimiento, mantenimiento de servicios, programas y recursos de almacenamiento (TechTarget, 2006). Algunas de las características de HP Openview son:

- Una función Gráfica de monitoreo de rendimiento en tiempo real.

- Función de acercamiento que provee una visualización más detallada de métricas o gráficos en un periodo de tiempo específico.
- Múltiples opciones de gráficos, incluyendo linear y exponencial, todos con niveles de confianza.
- Generación de reportes flexible, permitiendo la exportación de datos a formatos comunes.

2.6.4. PRTG Network Monitor

PRTG Network Monitor es una solución unificada para la gestión y monitorización de red desarrollada por Paessler AG. PRTG se ejecuta en una máquina con Windows, recolectando las estadísticas de las estaciones, software entre otros equipos que se hayan designado o autodetectado. También permite recolectar y visualizar datos históricos. Incluye gráficas en tiempo real y reportes costumizados (Paessler, 2014). Algunas de las características de PRTG son:

- Monitorización de ancho de banda, uso, tiempo de actividad y de SLA.
- Adecuado para redes de distintos tamaños.
- Monitorización de redes/ubicaciones múltiples con solo una licencia.
- API basada en HTTP para comunicación con otras aplicaciones.
- Descubrimiento automático de la red y configuración de sensores (IPv4 e IPv6).

2.6.5. Nagios

Nagios es un software de código abierto diseñado para la supervisión continua y automática en sistemas informáticos o Tecnologías de Infraestructura de Comunicaciones. Está escrito bajo General Public License (GNU) y se enfoca principalmente en vigilar el comportamiento de hosts y servicios de red (Nagios, 2012). Las características principales de Nagios son:

- Monitoreo de servicios de red.
- Monitoreo de recursos como CPU, Memoria, Discos, etc.
- Permite definir contactos para el envío de notificaciones.
- Permite el manejo de eventos de manera proactiva.
- Log de eventos.
- Visualización a través de una interfaz web.
- Multiplataforma.

2.6.6. Zabbix

Zabbix es un software de código abierto diseñado para la monitorización de red. Con esta herramienta es posible recopilar una amplia gama de datos de miles de servidores, máquinas virtuales y dispositivos de red simultáneamente. Cuenta con almacenamiento de datos, características flexibles de visualización (vistas panorámicas, mapas, gráficos, pantallas, etc), así como formas muy variadas de analizar los datos con el fin de alertar los problemas que aparecen (Zabbix, 2016). Algunas de las características de Zabbix son:

- Detección automática de servidores y dispositivos de red
- Software de servidores para Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X
- Monitorización sin agentes
- Autenticación de usuario
- Permisos de usuario flexibles
- Interfaz web
- Notificación por correo electrónico.

2.6.7. Cacti

Cacti es una solución gráfica que permite monitorizar dispositivos conectados a una red que tengan activado el protocolo SNMP. Cacti provee un modelo avanzado de plantillas, múltiples métodos de adquisición de datos y funciones de gestión de usuarios (Cacti, 2015). Puede monitorear redes complejas con miles de dispositivos y se distribuye bajo licencia GPL. Algunas de sus características son:

- Usa RRDtool, PHP, y MySQL.
- Permite agregar ilimitado número de elementos para cada gráfico.
- Permite definir scripts personalizados.
- Permite organizar la información en estructuras jerárquicas
- Construido en soporte SNMP
- Permite crear usuarios y añadir permisos

2.6.8. Zenoss

Zenoss una herramienta de monitoreo de red que proporciona las funcionalidades necesarias para gestionar eficazmente la configuración, estabilidad, rendimiento de redes, servidores y aplicaciones a través de un único paquete de software integrado. Cuenta con una versión libre y dos versiones comerciales. Sus principales características son:

- Detección automática de dispositivos
- Tiene una interfaz web.
- Generación automática de eventos
- Envío de correos electrónicos y SMS.
- Dashboard personalizado

- Genera informes multigráfico

2.7. Herramientas complementarias al software de gestión

Además de los sistemas de monitorización y control que se mencionaron en el apartado anterior, existe un sinnúmero de herramientas que complementan la administración de red ejecutando tareas más simples como la gestión de logs, análisis de paquetes, análisis de vulnerabilidades, etc.

2.7.1. Ping

Ping (Packet Internet Groper) es un comando que se utiliza generalmente para detectar problemas en la accesibilidad de dispositivo. Usa dos mensajes, solicitudes de eco ICMP y respuestas de eco ICMP para determinar si un host remoto se encuentra activo. Este comando también calcula el tiempo necesario para recibir la respuesta de eco.

2.7.2. Traceroute

El comando traceroute se usa con el objetivo de detectar los trayectos que toman los paquetes hacia un destino remoto y también, indica dónde deja de funcionar el ruteo. Traceroute se encarga de registrar la fuente de cada mensaje “tiempo excedido” ICMP para indicar una traza de la trayectoria que el paquete tomó para llegar a su destino (CISCO, 2016).

2.7.3. Nessus

Nessus es una plataforma de análisis de vulnerabilidades. Nessus permite a los usuarios programar exploraciones a través de varios escáneres, utilizar asistentes para crear políticas, programar escaneos y enviar resultados mediante correo electrónico (Tenable Network Security, 2016). Las características de Nessus incluyen:

- Descubrimiento de activos de alta velocidad
- Evaluación de vulnerabilidad

- Detección de malware / botnet
- Auditoría de Configuración y Cumplimiento
- Escaneo y auditoría de plataformas virtualizadas.

2.7.4. Wireshark

Wireshark es un software analizador de paquetes de código abierto que permite al usuario capturar y leer información de aplicaciones como Sniffer, Snoop y Microsoft network monitor. Tanto la descarga como la instalación de Wireshark se realizan de manera gratuita, además puede usarse para la solución de problemas de red, comunicaciones y análisis de red. La herramienta fue lanzada en mayo de 2006 con el nombre Ethereal, sin embargo, tuvo que ser renombrado a Wireshark poco después debido a un problema de marcas registradas (Wireshark, 2015). Este software tiene las siguientes características principales:

- Capacidad para escribir y leer en varios formatos de captura.
- Exporta informes en texto plano, CSV, PostScript y XML.
- Puede analizar VoIP.
- Captura datos en vivo de muchos tipos de red e interfaces.
- Dispone de un sistema de filtrado

2.7.5. Tripwire

Es una herramienta Open Source de seguridad e integridad de datos, es utilizado para monitorizar cambios en los ficheros de un sistema y alertar sobre ello. Este software monitorea rutinariamente la integridad de una gran cantidad de archivos utilizando la firma digital de los archivos y directorios contra una base de datos de éstos en un momento previo (TripWire, 2016). Este es un proceso pesado que por lo general se ejecuta en intervalos.

2.7.6. Swatch

Es un programa para gestión de logs en sistemas UNIX. Swatch monitorea los archivos de registro y actúa para filtrar los datos no deseados y toma una o más acciones especificadas por el usuario (SecuriTeam, 2001). Esta herramienta puede monitorear la información a medida que se anexa al archivo de registro y alertar a los administradores del sistema inmediatamente acerca de problemas graves del sistema en el momento que aparecen.

2.8. Políticas de administración

Para la implementación de un sistema de gestión de red es necesario establecer políticas de acuerdo a los objetivos de la organización. En la actualidad no existe un documento oficial en donde se definan las políticas de gestión necesarias en la red de datos de una institución de educación superior.

Barba y Guerrero (2008), definen que una política es un conjunto de directivas o reglas especificadas por el administrador para gestionar ciertos aspectos de los resultados deseados de las interacciones entre usuarios, entre aplicaciones, y entre usuarios y aplicaciones.

Núñez y Caicedo (2005), definen las siguientes directrices para la implementación de políticas en las áreas: Gestión de fallos, gestión de configuraciones, gestión de rendimiento y gestión de seguridad.

Gestión de fallos:

- El sistema de administración debe recolectar la información de los dispositivos administrados cada cinco minutos.
- Los componentes principales de la red deben estar configurados para enviar alertas al administrador de la red.

- Al encontrarse una falla es necesario definir procedimientos que permitan solucionarla, por lo cual es necesario catalogar las fallas, indicando su nombre y su causa.
- Las fallas deben reportarse en la interfaz del sistema de administración junto con un sonido para poder alertar al administrador de red.
- Una vez notificada la falla se debe seguir un procedimiento para manejarla siguiendo los siguientes pasos:

Notificación: El administrador es notificado de la falla.

Asignación: El administrador asigna el caso a una persona, la cual deberá revisar la falla y determinar su origen.

Resolución: La persona encargada del caso soluciona la falla.

Finalización: La persona encargada del caso realiza la documentación del proceso que se hizo para resolver la falla.

Gestión de configuraciones:

Se deben tener pautas para estandarizar:

- Compra de equipos de comunicaciones. - Para facilitar la recolección y procesamiento de datos, los equipos deben tener una misma (MIB).
- Direccionamiento de red y nombre de equipos. - Establecer un direccionamiento de red común para todos los equipos de red usando distintos rangos de direcciones. En cuanto a los nombres de los dispositivos se debe establecer la nomenclatura para cada tipo de dispositivo.

- Configuración básica del dispositivo. - La configuración básica comprende: nombre del dispositivo, dirección de red, clave de acceso y protocolo de administración. Si se usa SNMP se debe definir la comunidad de lectura, escritura y el servidor.

Gestión de prestaciones

Se debe recolectar de cada equipo:

- Dispositivos de comunicaciones. - Uso de procesador, uso de memoria, uso de las interfaces de comunicación.
- Servidores. - Uso del procesador, uso de memoria, uso de interfaces de comunicación, porcentaje de uso de cada partición del servidor.

CAPÍTULO III

3. Situación actual

En este apartado se realiza el levantamiento de información de la red de datos del Edificio Central de la UTN, mediante la inspección del lugar, entrevista al administrador de red y encuesta a los usuarios de la misma. Se realiza la elección del software de monitoreo de acuerdo a los requerimientos de la red.

3.1. Universidad Técnica del Norte

La Universidad Técnica del Norte es una institución de educación superior cuya labor se enfoca en el desarrollo académico e investigativo del país, en especial en la zona UNO, correspondiente a las provincias: Imbabura, Carchi, Esmeraldas y Sucumbíos.

3.1.1. Ubicación

La institución está domiciliada en la ciudad de Ibarra, ubicada en la Avenida 17 de Julio 5-21 y General José María Córdova sector “EL Olivo”. Esta dirección se visualiza en la Figura 5.

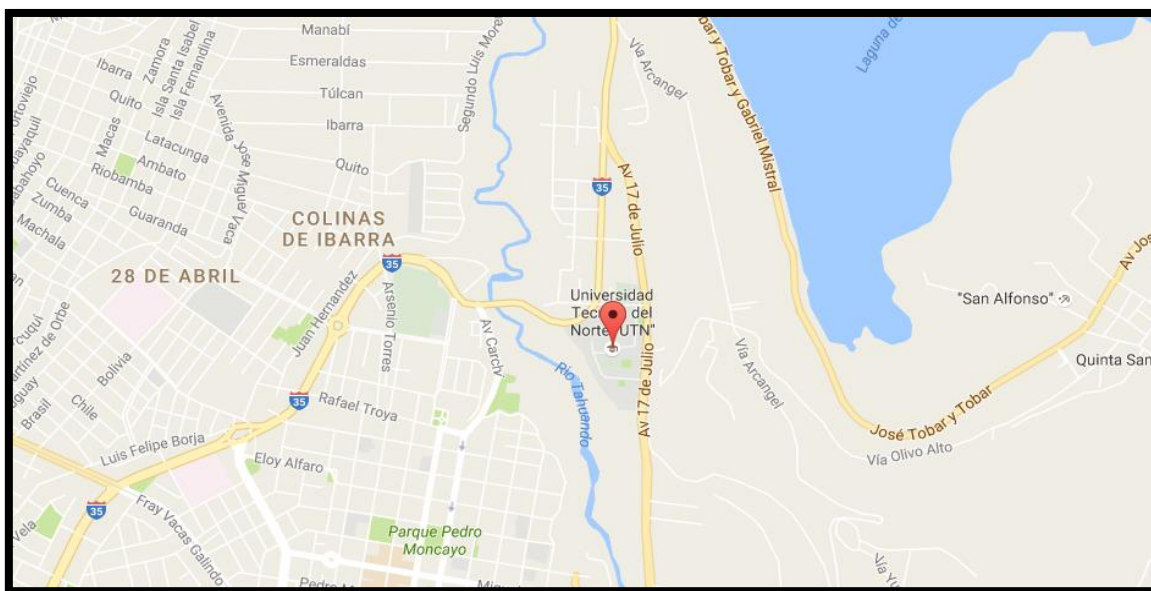


Figura 5. Ubicación de la UTN

Fuente: Recuperado de Google Maps

3.1.2. Estructura Organizacional

Para el cumplimiento de sus actividades académicas, administrativas, de investigación y de vinculación con la sociedad, la Universidad Técnica del Norte se encuentra estructurado por el Honorable Consejo Universitario, quien es la máxima autoridad normativa y administrativa de la institución; Rectorado, máxima autoridad ejecutiva y representante legal; Vicerrectorado Académico, encargado de las diferentes unidades y centros educativos; Vicerrectorado Administrativo, encargado del adecuado funcionamiento de la universidad en sus aspectos administrativos y otras áreas de apoyo. La Figura 6 muestra el organigrama estructural de la UTN en base a estatuto orgánico disponible en el portal web de la institución.

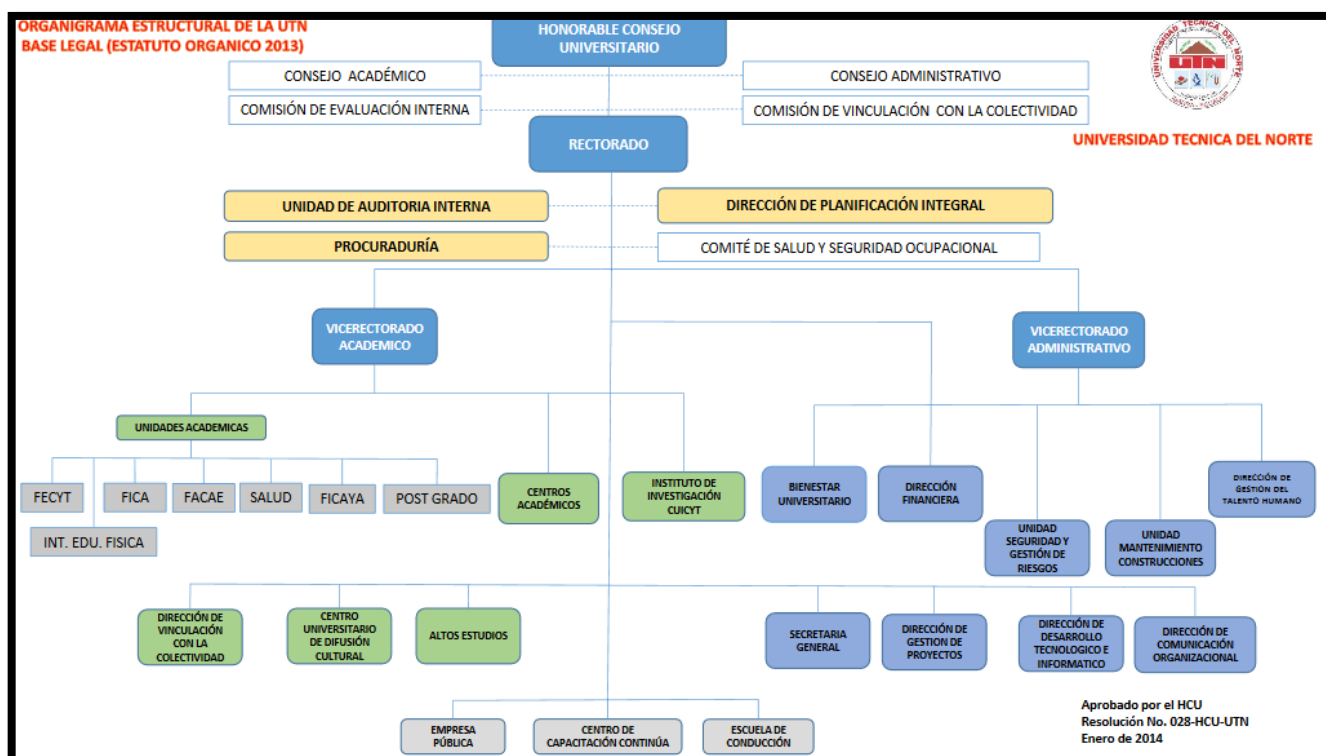


Figura 6. Organigrama Estructural de la UTN.

Fuente: recuperado de http://www.utn.edu.ec/web/uniportal/wp-content/uploads/2016/06/a1_organigrama_estructural_utn.pdf

3.1.3. Misión y visión

La Universidad Técnica del Norte ha definido la siguiente misión y visión.

Misión

“La Universidad Técnica del Norte es una institución de educación superior, pública y acreditada, forma profesionales de excelencia, críticos, humanistas líderes y emprendedores con responsabilidad social; genera, fomenta y ejecuta procesos de investigación, de transferencia de saberes, de conocimientos científicos, tecnológicos y de innovación; se vincula con la comunidad, con criterios de sustentabilidad para contribuir al desarrollo social, económico, cultural y ecológico de la región y del país.” (UTN, s.f.)

Visión

“La Universidad Técnica del Norte, en el año 2020, será un referente regional y nacional en la formación de profesionales, en el desarrollo de pensamiento, ciencia, tecnología, investigación, innovación y vinculación, con estándares de calidad Internacional en todos sus procesos; será la respuesta académica a la demanda social y productiva que aporta para la transformación y la sustentabilidad” (UTN, s.f.)

3.1.4. Red de datos interna

La Universidad Técnica del Norte cuenta con una red de datos desplegada hacia todas las dependencias de la institución, provee un servicio de Internet con un ancho de banda simétrico de 600Mbps. Para las instalaciones externas al campus universitario, el servicio se distribuye desde los enlaces de radio, que parten desde el core principal hasta los switches ubicados en cada dependencia. (DDTI, 2016). La red de la UTN tiene un diseño lógico basado en una red jerárquica de tres capas.

El proveedor de Internet proporciona un router de borde marca cisco de la serie 7604 que se conecta internamente a la red de la institución.

El router de borde a su vez se conecta a un Cisco ASA 5520, equipo que desempeña la función de firewall y es el encargado de la seguridad de la red, garantizando confidencialidad, autenticidad, integridad de los datos y prevención de intrusos.

La capa de core de la red de datos de la UTN está conformada por dos switches de Core Catalyst 4506-E, los cuales permiten administrar las comunicaciones y garantizan el correcto funcionamiento de la red. Uno de estos equipos se encuentra ubicado en el cuarto de equipos de la Dirección de Desarrollo Tecnológico e Informático (DDTI), en la planta baja del Edificio Central y otro dentro del cuarto de equipos de la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

Las diferentes dependencias del campus universitario se conectan con el Edificio Central mediante enlaces de fibra óptica para tener conectividad a Internet. Adicionalmente se tienen enlaces redundantes con el equipo de core ubicado en la FICA.

En la institución se encuentran instalados enlaces de radio punto a punto desde la torre ubicada en el Edificio Central hacia cada una de las dependencias externas al campus universitario tales como: Granjas Yuyucocha y La Pradera, Colegio Universitario, Guardería, Facultad de Ciencias de la Salud (Antiguo Hospital) y la Planta Textil.

La *Figura 7* muestra el diseño físico de la red de datos de la institución.

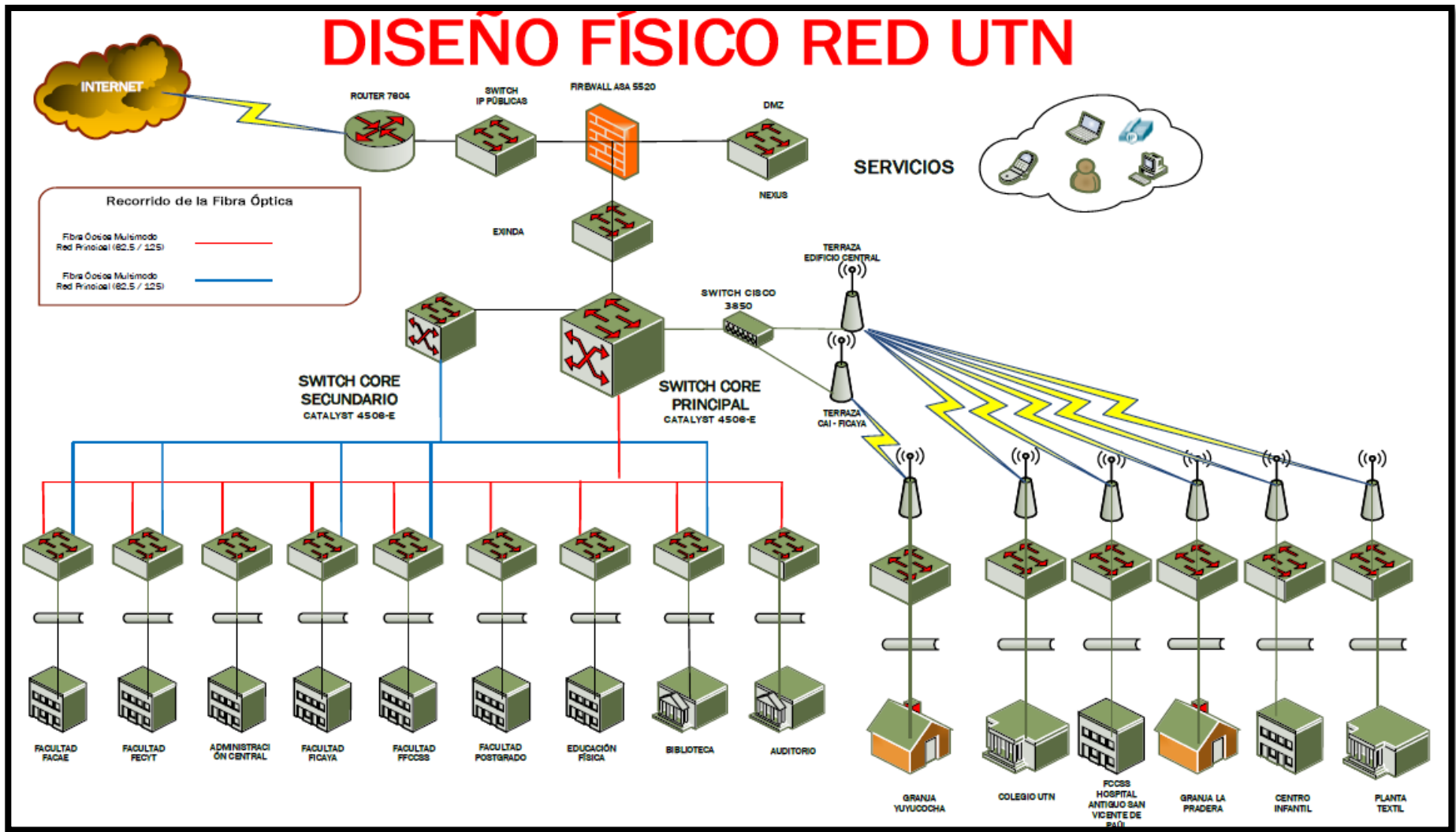


Figura 7. Diseño físico de la red UTN

Fuente: DDTI

3.2. Edificio Central de la UTN

El Edificio Central de la Universidad Técnica del Norte concentra la mayor parte de las actividades administrativas de la institución. Su ubicación, dentro del campus universitario se presenta en la Figura 7.



Figura 8. Campus UTN "El Olivo"

Fuente: Recuperado de http://www.utn.edu.ec/web/uniportal/?page_id=2015

El Edificio Central consta de las siguientes dependencias:

Planta baja

- Oficina del estudiante
- Dirección de Desarrollo Tecnológico e Informático
- Dpto. Vinculación con la Colectividad

- Transporte
- Instituto de altos estudios
- Almacén bodega

Planta alta 1

- Rectorado
- Vicerrectorado Académico
- Vicerrectorado Administrativo
- Relaciones públicas y coordinación cultural

Planta alta 2

- Sala José Martí
- Sala Francisco de Orellana
- Planeamiento integral
- Cubículos de investigación
- Sala de reuniones
- Comisión General de Evaluación
- CUICYT

Planta alta 3

- Dirección de Coordinación Internacional
- Procuraduría
- Televisión universitaria UTN
- Radio Universitaria

- Sala Simón Bolívar
- Departamento de Mantenimiento y Construcciones

Planta alta 4

- Departamento Financiero
- Departamento de Relaciones Humanas

3.2.1. Equipos de telecomunicaciones

En este apartado se presenta la disposición física de los equipos y sus principales características. La descripción se realiza por cada planta del Edificio, empezando por el cuarto de equipos o data center.

3.2.1.1. Cuarto de Equipos

De acuerdo a la información proporcionada en (DDTI, 2016), se detalla que dentro del Edificio Central de la UTN se encuentra el data center que es el espacio para los equipos de telecomunicaciones, aquí se encuentra un switch de core principal CISCO Catalyst 4510, switches de distribución, servidores, racks etc. La topología física del data center se muestra en la Figura 9.

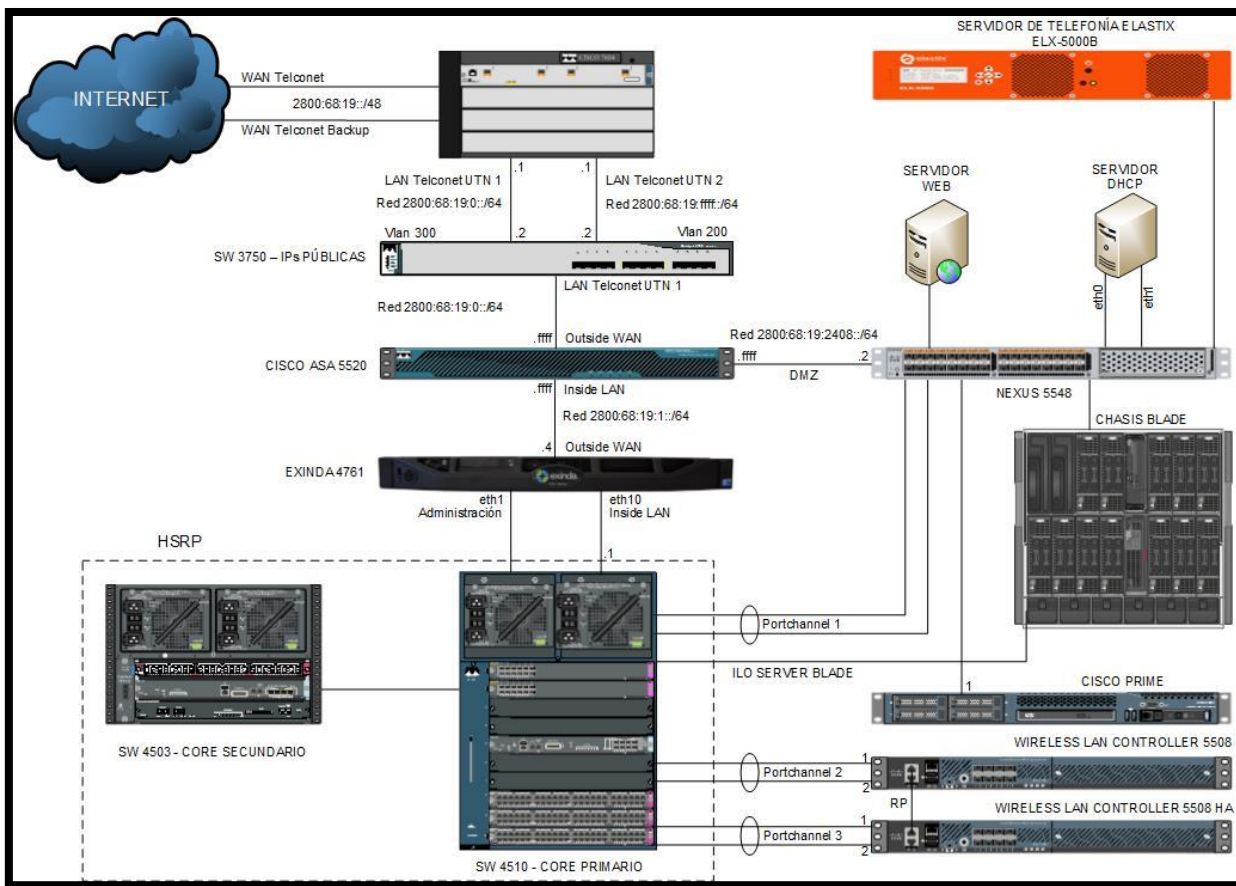


Figura 9. Topología física del Data Center

Fuente: DDTI

A continuación, en la Tabla 3, se muestra el detalle de los equipos, características y función que desempeñan dentro del Data Center.

Tabla 3. Equipos del Data center

EQUIPOS	CARACTERÍSTICAS	FUNCIÓN
Router Cisco 7604	<ul style="list-style-type: none"> - 4 slots - Alto rendimiento de conmutación de etiquetas IP (MPLS) para redes MAN y WAN 	Es el equipo de borde que permite la salida a Internet.

Switch Cisco 3750	<ul style="list-style-type: none"> - Administrable - Capa 2 y 3 	Equipo donde están configuradas las direcciones IP públicas.
Cisco Asa 5520	<ul style="list-style-type: none"> - Protección firewall - Equilibrio de carga - Soporte VLAN - Alta disponibilidad 	Desempeña la función de firewall en la red. Provee servicios de seguridad, con alta disponibilidad y conectividad Gigabit Ethernet.
Exinda 4761	<ul style="list-style-type: none"> - Diseñado para oficinas centrales. - Capacidad de 1Gbps - Almacenamiento de datos de 385 GB 	Equipo administrador de ancho de banda. Asigna dinámicamente el ancho de banda a las aplicaciones de que más lo necesitan.
Switch Cisco 4510	<ul style="list-style-type: none"> - Administrable - 10 slots - Capa 2 y 4 	Equipo de core primario, desde donde se conectan los enlaces a todas las dependencias internas de la universidad.
Switch Cisco 4503	<ul style="list-style-type: none"> - Administrable - 3 slots - Capa 2 y 4 	Equipo de core secundario cuya configuración es similar a la del switch de core primario dando redundancia.
Switch Nexus 5548	<ul style="list-style-type: none"> - Administrable - 32 puertos SFP - Capa 2 y 3 	Switch de alta disponibilidad donde se conectan todos los servidores de la DMZ.

Servidor Elastix	<ul style="list-style-type: none"> - Soporte para hardware de telefonía - Módulo de centro de llamadas 	<p>Servidor de telefonía encargado de establecer las conexiones entre las terminales de la institución, o de hacer que se cursen las llamadas al exterior.</p>
<hr/>		
Chasis Blade C7000	<ul style="list-style-type: none"> - Capacidad de hasta 16 blades almacenamiento y/o servidores. - Módulos opcionales de interconexión de almacenamiento y de red redundantes. - Puede administrarse como un entorno unificado. 	<p>Equipo donde se encuentran todos los aplicativos de la institución.</p>
<hr/>		
Cisco Prime	<ul style="list-style-type: none"> - Ofrece soporte para 802.11ac - Capacidades de gestión de ciclos de vida de redes fijas e inalámbricas convergentes. - Gestión convergente para facilitar la supervisión, 	<p>Equipo que permite administrar la red inalámbrica</p>

			resolución de problemas y generación de informes
Wireless controller 5508	LAN	- Soporta más de 500 Access points y 7000 clientes. - Diseñado para 802.11ac y 802.11n - Máximo throughput de 8Gbps	Equipo en él que se configura la red inalámbrica de la institución. Se encuentra en estado activo
Wireless controller 5508 HA	LAN	- Soporta más de 500 Access points y 7000 clientes. - Diseñado para 802.11ac y 802.11n - Máximo throughput de 8Gbps - Una fuente de alimentación redundante para garantizar la máxima disponibilidad	Equipo de alta disponibilidad en él que se configura la red inalámbrica de la institución. Se encuentra en estado pasivo

Fuente: DDTI

3.2.1.2. *Planta baja*

En la planta baja se encuentran las dependencias: Oficina del estudiante, Dirección de Desarrollo Tecnológico e Informático, Dpto. Vinculación con la Colectividad, Transporte, Instituto de altos estudios, Almacén bodega.

El rack de este piso se ubica en una bodega de la parte izquierda del Edificio, contiene un switch que se especifica en la Tabla 4.

Tabla 4. Switches Planta baja

ELEMENTO	NOMBRE	CARACTERÍSTICAS	DESCRIPCIÓN
Switch Cisco WS-C2960- 48TC-L	SW-ATENEA	- Administrable - 48 puertos fast ethernet - Capa 2	46 puertos Fast Ethernet se utilizan para conectar usuarios finales dentro del Edificio Central. 1 puerto fast ethernet se usa para proveer conectividad a la copiadora que se encuentra fuera del Edificio. 1 puerto fast ethernet se usa para conectar una cámara de seguridad Se utiliza una interfaz Gigabit Ethernet para conectarse al switch de core principal mediante fibra óptica.

Fuente: DDTI

3.2.1.3. *Planta alta 1*

En la Planta 1 se encuentran: Rectorado, Vicerrectorado Académico, Vicerrectorado Administrativo, Relaciones públicas y coordinación cultural.

El rack de ese piso se ubica dentro del Rectorado y aloja a dos switches que se especifican en la Tabla 5.

Tabla 5. Switches planta alta 1

ELEMENTO	NOMBRE	CARACTERÍSTICAS	DESCRIPCIÓN
Switch Cisco WS-C2960- 48TC-L	SW-CRATOS	<ul style="list-style-type: none"> - Administrable - 48 puertos fast ethernet - Capa 2 	<p>47 puertos Fast Ethernet se utilizan para conectar usuarios finales dentro del Edificio.</p> <p>Un puerto Fast Ethernet para conectar al Access point ubicado en el vicerrectorado administrativo.</p> <p>Se usa una interfaz Gigabit Ethernet para conectarse al switch de core principal mediante fibra óptica.</p> <p>Se usa una interfaz Gigabit Ethernet para conectarse al SW-CRONOS.</p>
Switch Cisco WS-C2960- 24TC-L	SW-CRONOS	<ul style="list-style-type: none"> - Administrable - 24 puertos fast ethernet - Capa 2 	<p>Se usa 20 puertos Fast Ethernet para conectar a usuarios finales.</p> <p>Se usa 3 puertos Fast Ethernet para conectar cámaras de vigilancia.</p> <p>Un puerto Fast Ethernet para conectar al Access point ubicado en el rectorado.</p> <p>Se usa una interfaz Gigabit Ethernet para conectarse al SW-CRATOS.</p>

Fuente: DDTI

3.2.1.4. Planta alta 2

Sala José Martí, Sala Francisco de Orellana, Planeamiento integral, Cubículos de investigación, Sala de reuniones, Comisión General de Evaluación, CUICYT.

El rack de este piso está ubicado en la sala José Martí, en él se ubican dos switches, cuyos detalles se muestran en la Tabla 6.

Tabla 6. Switches planta alta 2

ELEMENTO	NOMBRE	CARACTERÍSTICAS	DESCRIPCIÓN
Switch Cisco WS-C2960- 48TC-L	SW-ERIS	<ul style="list-style-type: none"> - Administrable - 48 puertos fast ethernet - Capa 2 	<p>Los 48 puertos Fast Ethernet se utilizan para conectar usuarios finales.</p> <p>Se usa una interfaz Gigabit Ethernet para conectarse al switch de core principal mediante fibra óptica.</p> <p>Se usa una interfaz Gigabit Ethernet para conectarse hacia el SW-EROS</p>
Switch Cisco WS-C2960- 48TC-L	SW-EROS	<ul style="list-style-type: none"> - Administrable - 48 puertos fast ethernet - Capa 2 	<p>Se usa 47 puertos Fast Ethernet para conectar a usuarios finales.</p> <p>Un puerto Fast Ethernet para conectar un Access Point.</p> <p>Se usa una interfaz Gigabit Ethernet para conectarse al SW-ERIS.</p>

Fuente: DDTI

3.2.1.5. *Planta alta 3*

Dirección de Coordinación Internacional, Procuraduría, Televisión universitaria UTN, Radio Universitaria, Sala Simón Bolívar, Departamento de Mantenimiento y Construcciones.

El rack de este piso se encuentra ubicado dentro del departamento Televisión universitaria. La Tabla 7 muestra las características de los switches de acceso de la planta alta 3

Tabla 7. Switches planta alta 3

ELEMENTO	NOMBRE	CARACTERÍSTICAS	DESCRIPCIÓN
Switch Cisco WS-C2960- 48TC-L	SW-HADES	<ul style="list-style-type: none"> - Administrable - 48 puertos fast ethernet - Capa 2 	<p>47 puertos Fast Ethernet se utilizan para conectar usuarios finales.</p> <p>1 puerto fast ethernet se conecta a la DMZ.</p> <p>Se usa una interfaz Gigabit Ethernet para conectarse hacia el SW-ANDROMEDA</p>

Fuente: DDTI

3.2.1.6. *Planta alta 4*

En esta planta se encuentran las siguientes dependencias: Departamento Financiero, Departamento de Relaciones Humanas.

El rack de este piso se ubica en una bodega y contiene 3 switches que se especifican en la Tabla 8.

Tabla 8. Switches planta alta 4

ELEMENTO	NOMBRE	CARACTERÍSTICAS	DESCRIPCIÓN
Switch Cisco WS-C3850- 48T	SW- ANDROMEDA	- Administrable - 48 puertos Gigabit ethernet - Capa 2 y 3	<p>20 puertos Gigabit ethernet para usuarios finales.</p> <p>3 puertos Gigabit ethernet para cámaras de seguridad.</p> <p>2 puertos Gigabit ethernet para la conexión de Access Points.</p> <p>5 puertos Gigabit ethernet para enlaces con las dependencias externas: Centro infantil, planta textil, antiguo hospital, granja La Pradera y Colegio universitario.</p> <p>Puertos Gigabit ethernet para enlaces con los switches: SW-ARTEMISA, SW-HERA y SW-HADES mediante cable UTP categoría 6.</p> <p>1 puerto Gigabit ethernet para el enlace con el switch de core central mediante fibra óptica.</p>
Switch Cisco WS-C2960X- 48TS-L	SW- ARTEMISA	- Administrable - 48 puertos fast ethernet	42 interfaces Gigabit ethernet para usuarios finales.

		- Capa 2	1 interfaz Gigabit ethernet para la conexión con el switch SW-ANDROMEDA.
			5 puertos Gigabit Ethernet libres.
Switch Cisco	SW-HERA	- Administrable	47 puertos Fast Ethernet para
WS-C2960-		- 48 puertos fast ethernet	usuarios finales
48TC-L		- Capa 2	1 puerto Fast Ethernet para conectarse con el switch SW-ANDROMEDA.

Fuente: DDTI

3.3. Entrevista

Con la finalidad de obtener información acerca de la administración de la red de datos del Edificio Central se realiza una entrevista al Ingeniero Vinicio Guerra, quien desempeña el puesto de Administrador de red en la Dirección de Desarrollo Tecnológico e Informático.

En la entrevista se realizaron las siguientes preguntas abiertas enfocadas a las áreas funcionales del modelo de gestión de red ISO/OSI:

Gestión de configuraciones

- ¿Se sigue un procedimiento establecido para solventar una falla en la red, adicionar equipos, realizar configuraciones, etc?
- ¿Se realiza algún tipo de documentación de los distintos eventos que se presentan en la red y de las configuraciones que se realizan sobre los dispositivos?

Gestión de fallos

- ¿Qué tipo de problemas son los más frecuentes dentro de la red de datos del Edificio Central?
- ¿Qué mecanismos utiliza para la detección de fallos en la red?
- ¿Cuánto tiempo demora en detectar una falla en la red y solucionarla?

Gestión de contabilidad

- ¿Se realizan inventarios periódicamente de los equipos de red del Edificio Central?

Gestión de prestaciones

- ¿Se generan periódicamente registros acerca del rendimiento de los dispositivos de red?
- ¿Cómo califica usted la disponibilidad de los servicios que provee la red de datos de la UTN?

Gestión de seguridad

- En cuanto a la seguridad, ¿Cómo se maneja el acceso a los dispositivos de red del Edificio Central?
- ¿Qué equipos considera usted, tienen mayor necesidad de ser monitoreados?

Las respuestas a la entrevista realizada se encuentran en el ANEXO C.

3.4. Encuesta

Se realizan encuestas con el objetivo de conocer la satisfacción de los usuarios sobre la red interna de datos de la UTN. Los usuarios encuestados fueron en su mayoría de la planta administrativa de la institución que se encuentra en el Edificio Central.

Para determinar el tamaño de la muestra, es decir, el número de sujetos necesarios para que los datos obtenidos de la encuesta sean representativos de la población se utiliza la ecuación 1:

$$n = \frac{NZ^2p(1-p)}{Ne^2 + Z^2p(1-p)}$$

Donde:

n= muestra número de personas a ser encuestadas

N= Población total (950)

Z= Nivel de confianza de los encuestados (1,64)

e= Margen de error máximo (10%)

p= Probabilidad de ocurrir el evento, recomendado 50%

Para la realización de esta encuesta se toma en cuenta al personal docente y administrativo de la institución puesto que son quienes dependen del buen funcionamiento de la red de datos para desempeñar sus actividades laborales. De acuerdo al Departamento de Recursos Humanos de la UTN, entre la planta administrativa y planta docente se tiene un total de 950 empleados, siendo ésta la población total.

El nivel de confianza es el valor obtenido mediante niveles de confianza. Su valor es una constante, el valor mínimo aceptado para considerar la investigación como confiable es de 1.96, equivalente al 95%. (Ochoa, 2013)

El margen de error es una estadística que expresa la cantidad de error de muestreo aleatorio en los resultados de una encuesta, se puede elegir un margen de error del 1 % al 10 % según la encuesta (Ochoa, 2013). No es recomendable incrementar el margen de error por encima del 10 %.

La probabilidad de ocurrir el evento es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que $p=0.5$ que es la opción más segura. (Ochoa, 2013)

Reemplazando valores en la Ec. 1, el valor de la muestra (número de encuestas a realizar) es de 64.

$$n = \frac{950 \cdot (1,64)^2 \cdot 0,5 \cdot (1 - 0,5)}{950 \cdot 0,1^2 + (1,64)^2 \cdot 0,5 \cdot (1 - 0,5)} = 64 \text{ encuestas}$$

Al estar en constante uso de la red, los usuarios perciben con mayor facilidad las deficiencias de la misma, es por ello que las preguntas de la encuesta se enfocan en dos áreas del modelo de gestión de red FCAPS: Gestión de fallos y gestión de rendimiento. El formato de la encuesta realizada se encuentra en el ANEXO B.

3.4.1. Criterios de encuesta para la gestión de fallos:

En el área de gestión de fallos las preguntas se realizaron en torno a la frecuencia con la que se presentan problemas en la red, atención a problemas notificados por el personal y tiempo de solución de dichos problemas, en concordancia con las actividades que abarcan esta gestión según el modelo ISO/OSI. Por lo tanto, las preguntas son las siguientes:

- ¿Con qué frecuencia, usted considera que ocurre un problema en la red de datos de la UTN?

- Cuando reporta un problema en la red de datos, ¿Cuál es el tiempo aproximado de espera antes de ser atendido por el personal de la DDTI?
- ¿Cuál es el tiempo aproximado que tarda el personal de la DDTI en solucionar un problema en la red de datos de la UTN?

Criterios de encuesta para la gestión de rendimiento:

En cuanto a la gestión de rendimiento, las preguntas se realizaron en torno a la satisfacción con el servicio de Internet, grado de funcionalidad de los servicios de red que provee la UTN. Finalmente se evalúa el grado de satisfacción con la labor que desempeña la DDTI.

- escoja el grado de funcionalidad del servicio de E-mail que provee la UTN.
- escoja el grado de funcionalidad de la Página web que provee la UTN.
- escoja el grado de funcionalidad de su Portafolio virtual al que accede.
- ¿Cómo califica usted el servicio de Internet?
- En general ¿cuál es su nivel de satisfacción con el servicio recibido por parte de la DDTI?

3.4.2. Resultados

A continuación, se analizan los datos recopilados en las encuestas realizadas a los usuarios de la red.

Pregunta 1: ¿Con qué frecuencia, usted considera que ocurre un problema en la red de datos de la UTN?

Acerca de la frecuencia con la que ocurren problemas en la red, se presentaron cuatro alternativas cuyos porcentajes se visualizan en la Figura 10. El 39% de los encuestados

respondieron que ocurre un problema más de una vez al día; por otra parte, el 33% contestaron que los problemas se presentan tan sólo una vez a la semana.

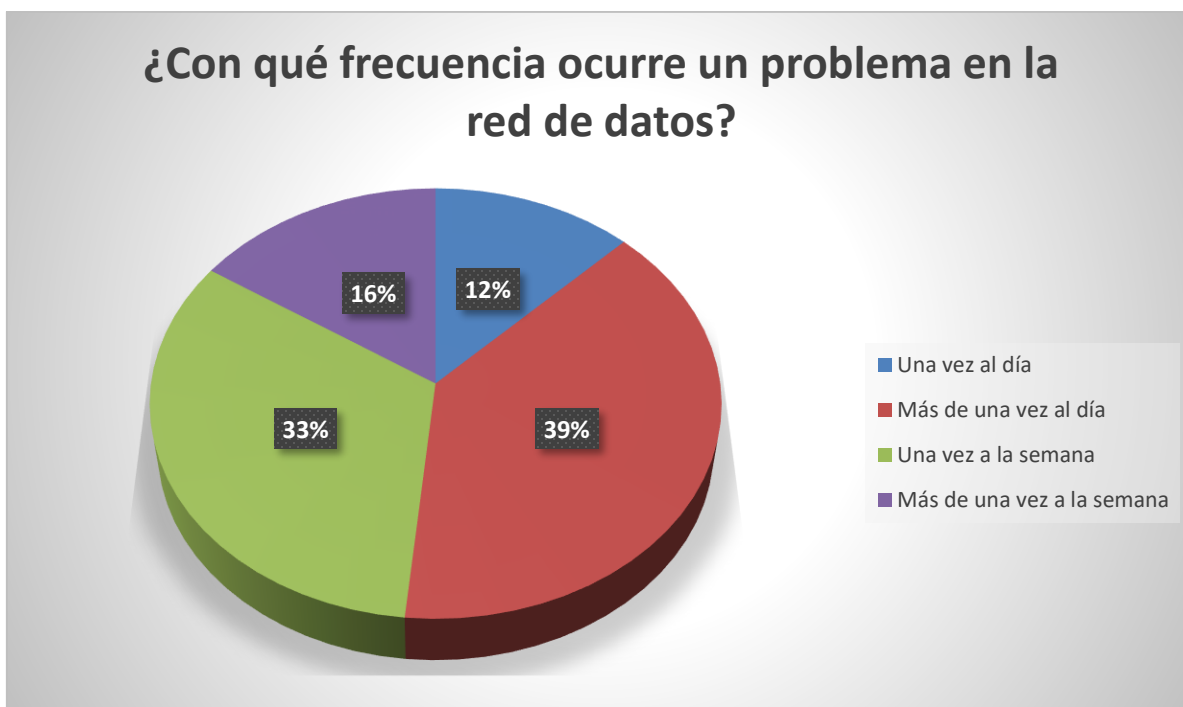


Figura 10. Frecuencia de problemas en la red

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

Esta pregunta evidencia que la aparición de problemas en la red es bastante frecuente día a día, lo cual causa molestias a los usuarios de la red, pues sus actividades se ven interrumpidas. En base a este resultado es necesario que se realicen acciones proactivas para evitar fallos en la red en la medida que sea posible.

Pregunta 2: Cuando reporta un problema en la red de datos, ¿Cuál es el tiempo aproximado de espera antes de ser atendido por el personal de la DDTI?

Según se muestra en la Figura 11, el 41% de los usuarios considera que la atención a problemas se realiza en 10 minutos, el 33% respondió que el tiempo de espera es de 30 minutos. El 20% de los encuestados manifestó que la atención se da en 1 hora y el 6% en un día.

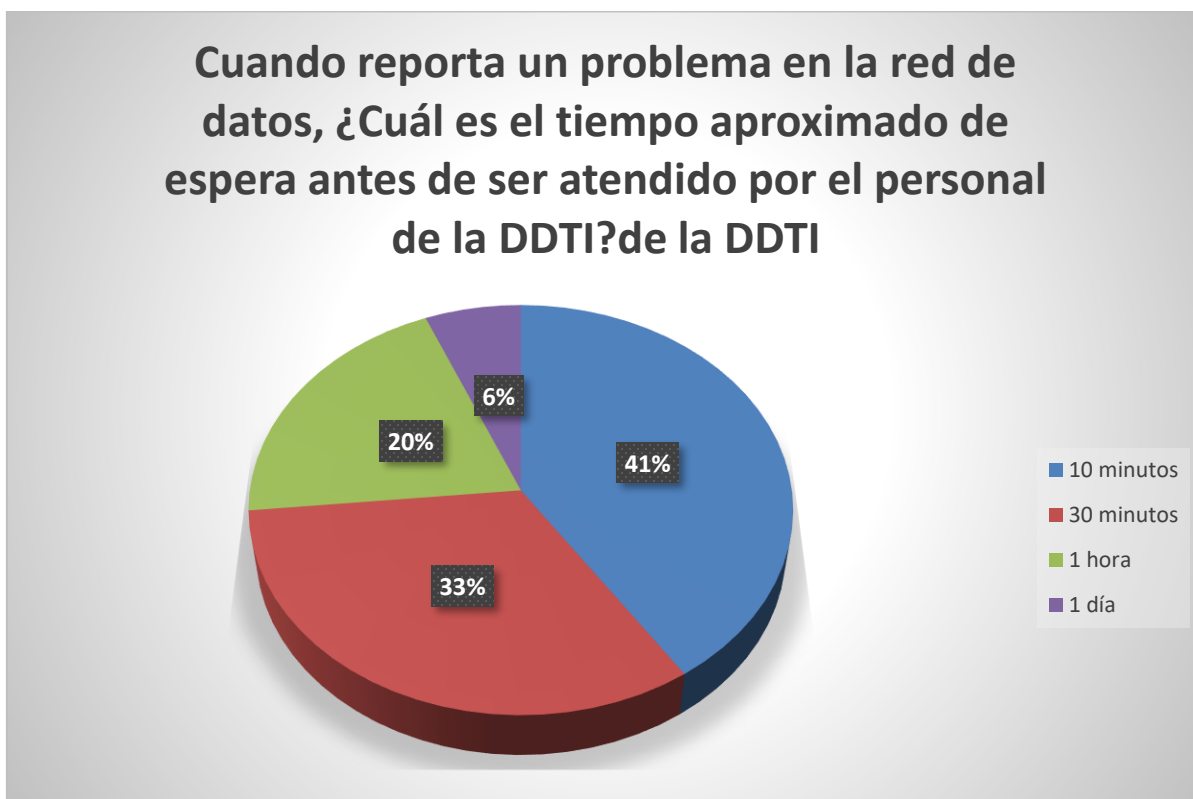


Figura 11. Atención a problemas

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

En base al resultado de esta pregunta se determina que la mayoría de los usuarios deben esperar entre 10 a 30 minutos a ser atendidas cuando reportan un problema, indicando que la atención es lo más inmediata posible.

Pregunta 3: ¿Cuál es el tiempo aproximado que tarda el personal de la DDTI en solucionar un problema en la red de datos de la UTN?

La Figura 12 muestra que el 33% de los encuestados, expresan que la resolución de problemas se realiza en 30 minutos, mientras que el 25% contestó que el tiempo es de una hora

aproximadamente. El 22% de los encuestados respondió que la solución de problemas tarda un día y otro 17% señaló que dicha solución se realiza en tan solo 10 minutos. Un reducido porcentaje de 3% de encuestados indicó que en una semana se da la solución a los problemas.

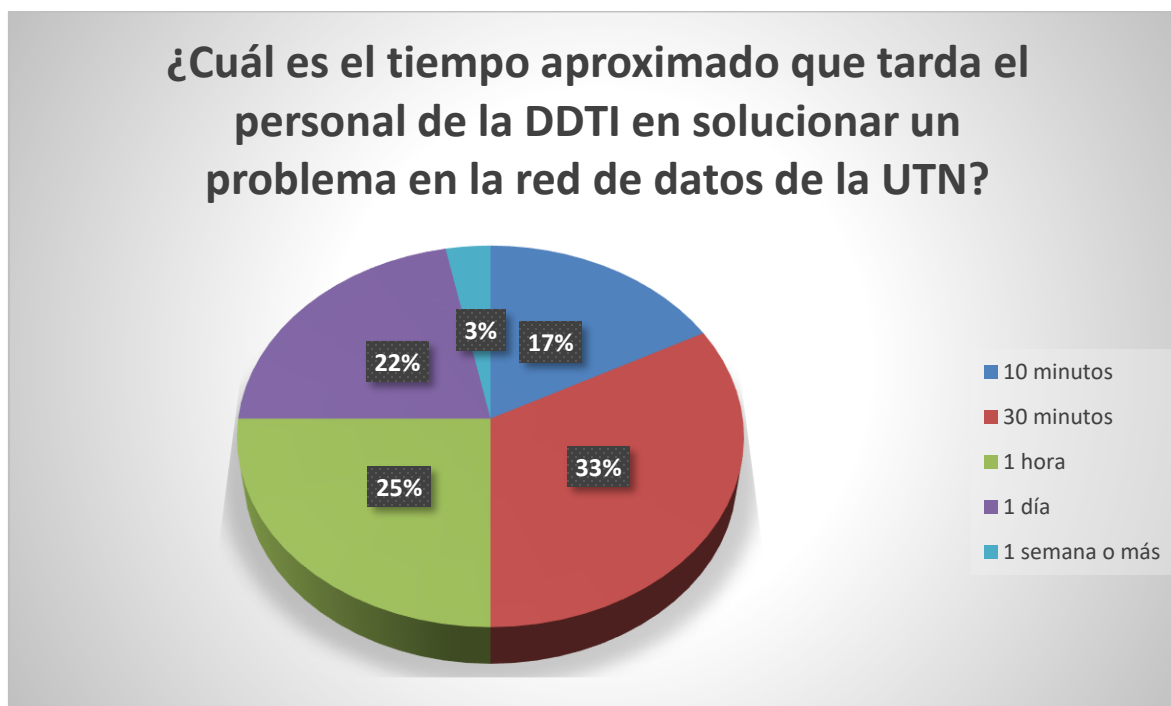


Figura 12. Tiempo de solución del problema

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

El análisis de los resultados obtenidos de este ítem indica que la mayor parte de los problemas son resueltos en tiempos de treinta minutos a una hora. Cabe recalcar que el tiempo de solución depende del tipo de problema con el que se esté tratando, por lo que los periodos de tiempo más reducidos corresponden a problemas pequeños mientras que los periodos de tiempos más grandes corresponden a problemas de mayor complejidad que se resuelven en un día, una semana o más. Para mejorar estos resultados se requiere establecer procedimientos que permitan minimizar el tiempo en que se soluciona el inconveniente, además de registros que detallen cómo se solucionan los problemas más recurrentes de la red.

Pregunta 4: Escoja el grado de funcionalidad del servicio de E-mail que provee la UTN

Respecto a los servicios que ofrece la red interna de la UTN se preguntó si éstos funcionan correctamente, presentan fallas o definitivamente no funcionan. La mayor parte de los encuestados con un porcentaje de 58% expresaron que el servicio funciona correctamente, como se evidencia en la Figura 13. El 37% de los encuestados señaló que los servicios fallan muy rara vez y el 5% expresó que fallan con mucha frecuencia.

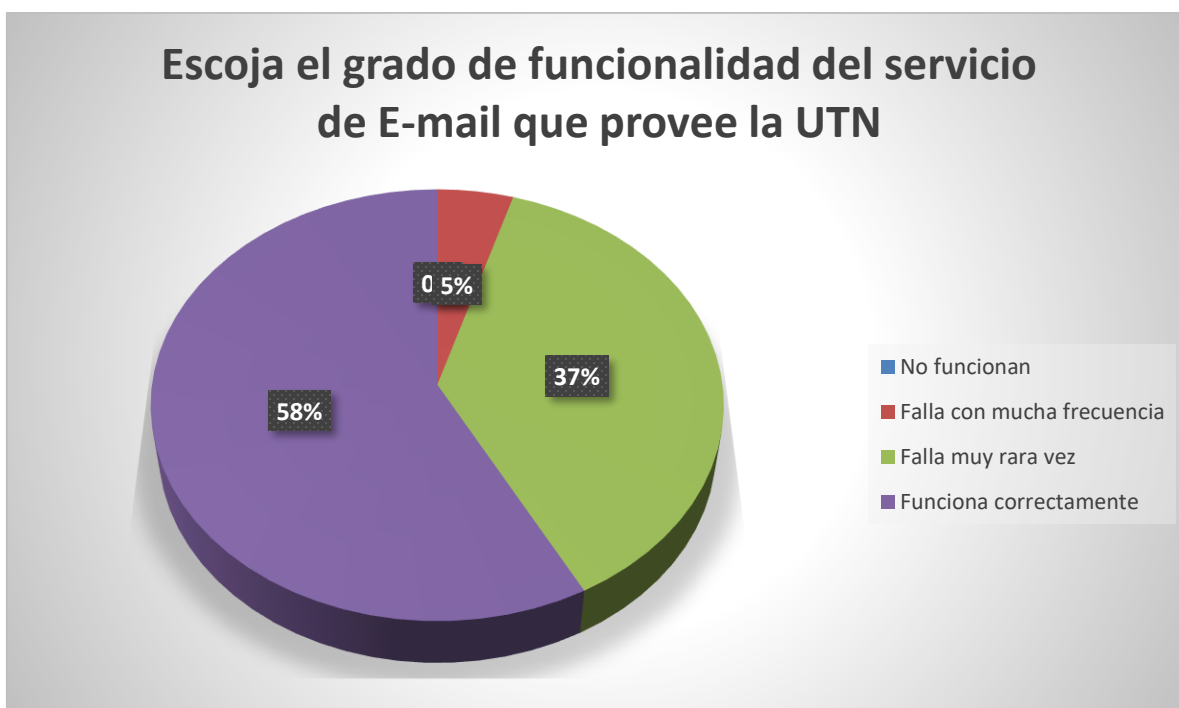


Figura 13. Servicios de la red interna UTN

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

En general se puede decir que el funcionamiento del servicio de E-mail es aceptable, ya que la mayor parte de las personas encuestadas señaló que este funciona correctamente o falla muy rara vez.

Pregunta 5: Escoja el grado de funcionalidad de la Página web que provee la UTN

El 56% de los encuestados expresaron que el Portal Web de la UTN falla muy rara vez, como se muestra en la Figura 14. El 38% de los encuestados señalaron que el Portal Web funciona correctamente, mientras el 6% de ellos expresó que falla con mucha frecuencia.

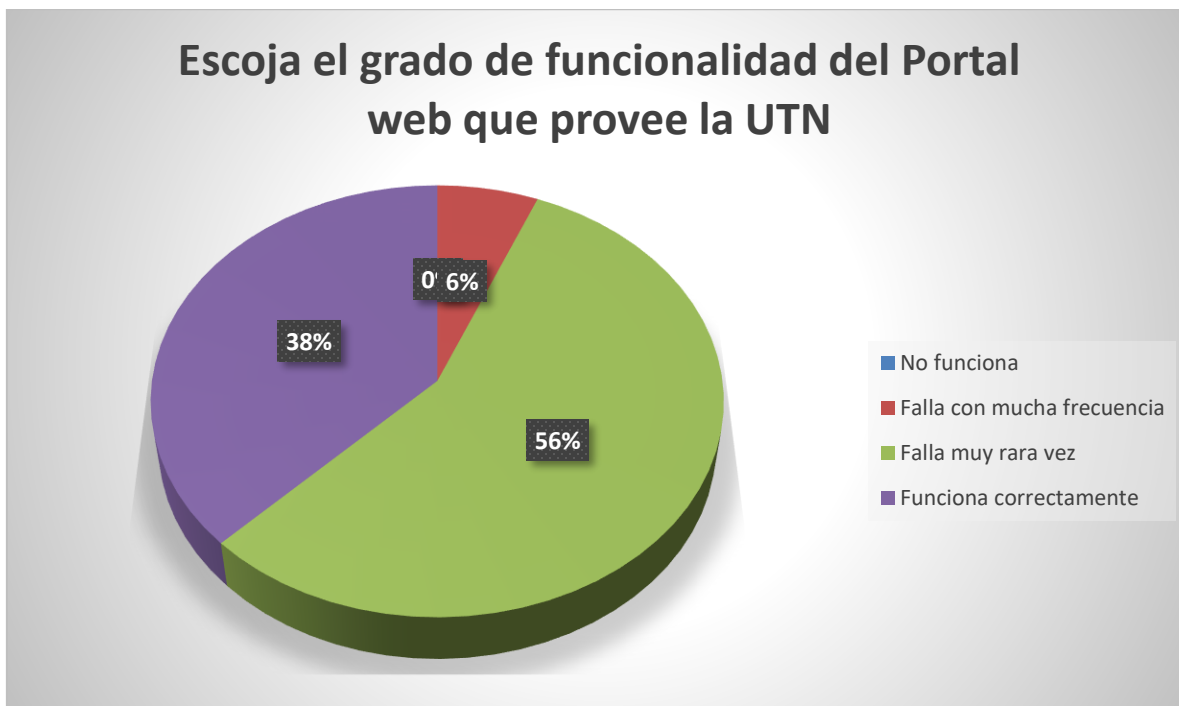


Figura 14. Página Web de la red interna UTN

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

De acuerdo a los datos obtenidos en este ítem, la gran mayoría de usuarios encuestados percibe que el funcionamiento del Portal Web es aceptable pues no se presentan fallas de manera frecuente.

Pregunta 6: Escoja el grado de funcionalidad de su Portafolio virtual al que accede

La mayor parte de los encuestados y con un porcentaje de 59%, expresaron que este servicio falla muy rara vez, como se evidencia en la Figura 15. El 28% de los encuestados señaló que los servicios funcionan correctamente y el 13% expresó que fallan con mucha frecuencia.

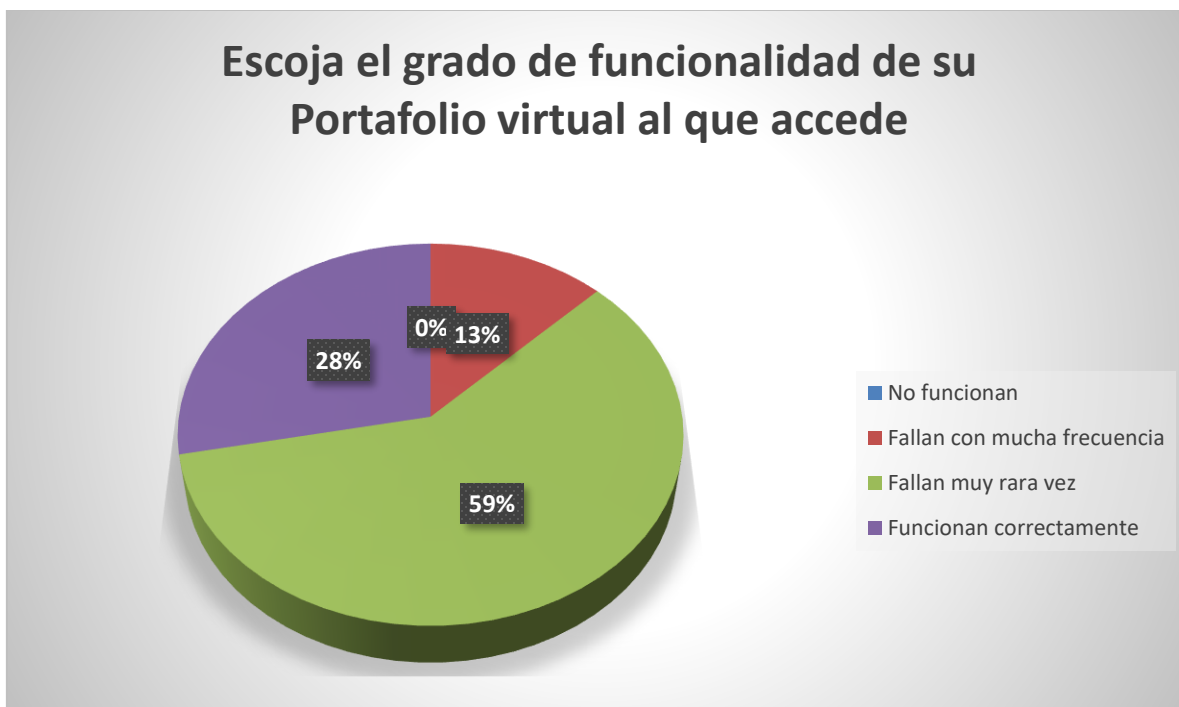


Figura 15. Portafolio virtual de la red interna UTN

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

Los resultados de esta pregunta indican que el servicio de Portafolio virtual, según los usuarios, tiene un funcionamiento aceptable la mayoría de tiempo.

Pregunta 7: ¿Cómo califica usted el servicio de Internet?

El servicio de Internet fue calificado como Bueno por la mayor parte de los encuestados con el porcentaje de 55%, esto se evidencia en la Figura 16. El 26% de las personas a las que se les aplicó

la encuesta calificaron el servicio de Internet como Regular, el 11% lo calificaron como Ineficiente y con menor cantidad el 8% lo calificó como Muy bueno.

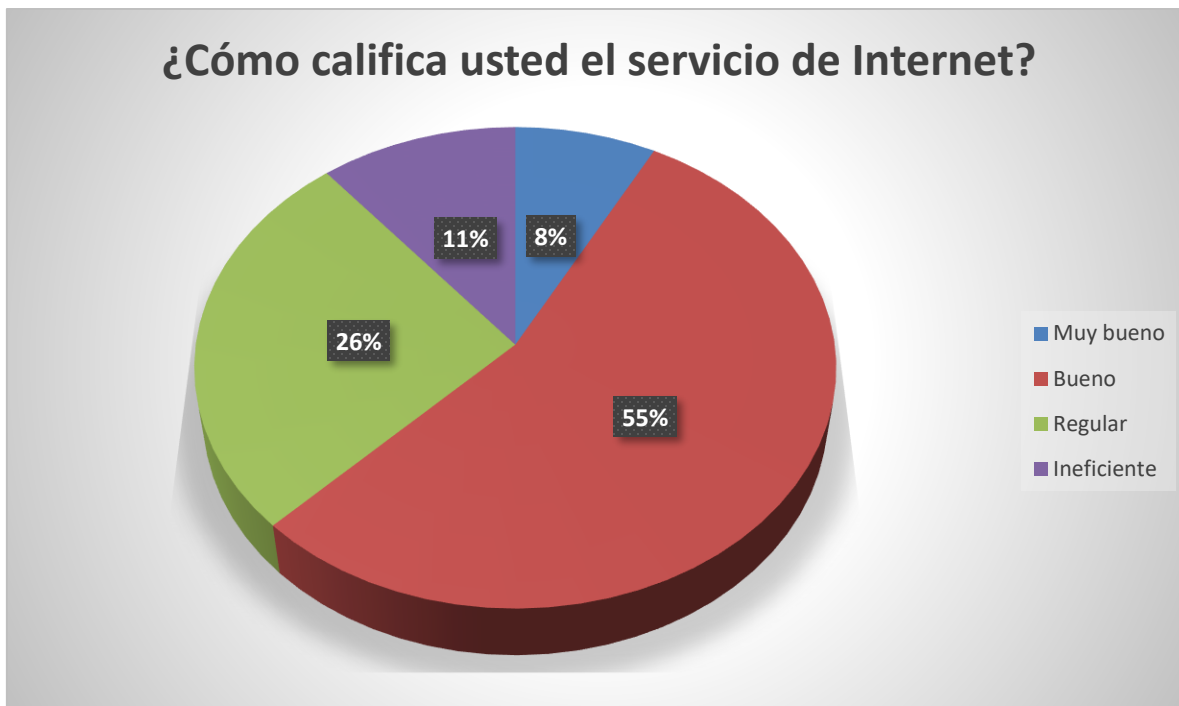


Figura 16. Servicio de Internet

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

El servicio de Internet en general ha sido calificado como Bueno, a pesar de no ser excelente, para la mayoría de usuarios este servicio no presenta muchos inconvenientes.

Pregunta 8: En general ¿cuál es su nivel de satisfacción con el servicio recibido por parte de la DDTI?

Respecto al grado de satisfacción de los usuarios acerca del desempeño de quienes conforman la DDTI, el 69% expresaron que están satisfechos como se muestra en Figura 17. El 22% expresaron que están Poco satisfechos con la labor de la DDTI y el 9% señaló que se están muy satisfechos.



Figura 17. Grado de satisfacción con la labor de la DDTI

Fuente: Encuestas realizadas a usuarios de la red interna de la UTN

El resultado de este ítem demuestra que la gran mayoría de personas encuestadas están satisfechas con la labor que realiza la DDTI.

Análisis general

Para el análisis general de los resultados obtenidos tanto en la entrevista como en la encuesta, se tomó en cuenta los aspectos más relevantes, determinando cuáles son las áreas que requieren más atención.

La atención que se da a los usuarios al momento de notificar una falla, generalmente toma pocos minutos. En cuanto al tiempo de solución de problemas, difiere dependiendo del problema y por lo tanto de la complejidad del mismo.

Los problemas más comunes son los referentes al servicio de Internet, ya sea por la falta de acceso o baja calidad. La percepción de los usuarios acerca de este servicio en su mayoría es buena, sin embargo, hay usuarios que no se encuentran conformes.

La disponibilidad de los aplicativos que provee la red de la UTN es buena la mayor parte del tiempo, salvo ciertas incidencias que se presentan en periodos donde la cantidad de usuarios intentando acceder al servicio es muy grande.

No se maneja ningún tipo de reportes acerca del rendimiento y usabilidad de la red, los cuales son necesarios para realizar diagnósticos y planificaciones futuras para mejorar el desempeño de la red.

No se realizan registros acerca de las configuraciones que se ejecutan en los equipos de la red, tampoco se documentan los fallos y procedimientos de solución.

3.5. Requerimientos del software de gestión

En base a la información obtenida en los apartados anteriores (Site survey, encuesta y entrevista) se obtienen los siguientes requerimientos para el sistema de gestión de red:

Autodescubrimiento de la red. Es muy importante que el software de monitoreo sea capaz de descubrir de forma automática las redes y los elementos que las forman.

Monitorización remota. Es fundamental que la herramienta de monitoreo de red de la posibilidad de acceder a equipos de forma remota, para no tener que desplazarse al sitio físico donde se encuentra el equipo.

Notificaciones y alertas. En caso de encontrarse una falla, el software debe notificarla inmediatamente, ya sea desde la interfaz de usuario o en el mejor de los casos enviando un correo electrónico al administrador de la red.

Generación de reportes. El software debe ser capaz de emitir reportes (informes, historiales y datos estadísticos) acerca de los dispositivos gestionados, para su posterior análisis.

Visualización en forma gráfica. Ver la información de la red de manera gráfica para un mejor entendimiento e interpretación. Esta característica es esencial para conocer el estado en tiempo real de los dispositivos gestionados.

Seguridad. La seguridad es vital, ya que la información que va a gestionar la herramienta de monitoreo será muy importante y en muchos casos confidencial. Por esta razón, el sistema de monitoreo de red debe tener una buena seguridad para que no se pueda acceder a los datos que almacena.

Disponibilidad. El sistema deberá estar en funcionamiento las 24 horas del día todos los días para emitir alertas en cualquier momento que se produzca un fallo.

Escalabilidad. Se debe poder añadir más elementos al sistema de gestión de red en caso de que sea necesario. El ingresar nuevos dispositivos no debe afectar el desempeño del sistema de gestión de red.

3.6. Selección del software de monitoreo

Actualmente existen varias opciones para el control y monitoreo de una red. Es fundamental seleccionar el software que brinde las prestaciones necesarias y cumpla los requerimientos de la red, para esta selección se utiliza el estándar IEEE 29148.

3.6.1. Estándar ISO/IEC/IEEE 29148:2011

Es un estándar internacional creado en 2011 que define disposiciones para procesos y productos en relación a la ingeniería de requerimientos para sistemas, productos y servicios a través del ciclo de vida. Este estándar es el reemplazo de la norma IEEE 830-1998.

ISO/IEC/IEEE 29148:2011 provee características y atributos de los requerimientos, proporciona además guías para la aplicación de requerimientos y procesos de gestión. Puede utilizarse independientemente o en conjunto con otras normas.

De acuerdo con la ISO/IEC/IEEE 29148:2011 la especificación de los requisitos debe realizarse según la parte del sistema para la que el requisito está definido. Para este trabajo se utilizó la Especificación de Requerimientos de Software (por su acrónimo en inglés SRS).

El SRS es una especificación para un programa o set de programas que desempeña ciertas funciones en un determinado ambiente. ISO/IEC/IEEE 29148:2011 propone el siguiente ejemplo de SRS:

1. Introducción

1.1. Propósito

1.2. Alcance

1.3. Visión general del producto

1.3.1. Perspectiva del producto

1.3.2. Funciones del product

1.3.3. Características del usuario

1.3.4. Limitaciones

1.4. Definiciones

2. Referencias
3. Requisitos específicos
 - 3.1. Interfaces externas
 - 3.2. Funciones
 - 3.3. Requisitos de usabilidad
 - 3.4. Requisitos de rendimiento
 - 3.5. Requisitos de base de datos
 - 3.6. Atributos del Sistema de software
 - 3.7. Información de soporte
4. Verificación
5. Apéndices
 - 5.1. Dependencias
 - 5.2. Acrónimos y abreviaturas

Introducción: Es la introducción del documento, contiene el propósito del SRS y su alcance.

Descripción general: En esta sección se establecen los lineamientos en las subsecciones de: perspectiva del software, funciones del software, características de usuario y limitaciones.

Referencias: Se mencionan las referencias usadas para la realización del documento.

Requerimientos del software: En esta sección se detalla las interfaces externas, requisitos funcionales, requisitos de usabilidad, requisitos de rendimiento y atributos del software.

3.6.2. Comparación y elección de software

La Tabla 9 muestra la comparación de software de gestión en base a los requisitos obtenidos en el SRS, el cual se detalla en el ANEXO D.

Para la comparación se tomó en cuenta cinco herramientas de gestión de red. De acuerdo a PandoraFMS (2016), algunas de las mejores herramientas de monitoreo de redes (gratis y de pago) que existen actualmente en el mercado son:

- Nagios
- Zabbix
- Zenoss
- Pandora FMS
- Cacti

Tabla 9. Comparación de software en base al SRS

REQUISITOS	CÓDIGO	DESCRIPCIÓN	NAGIOS	ZABBIX	ZENOSS	PANDORA FMS	CACTI
Requisitos funcionales	RQ1	Monitorización de manera remota	Si	Si	Si	Si	Si
	RQ2	Autodescubrimiento de la red	No	Si	Si	Si	No
	RQ3	Notificaciones y alertas	Si	Si	Si	Si	Si
	RQ4	Generación de Reportes	Si	Si	Si	Si	No
	RQ5	Visualización gráfica	Si	Si	Si	Si	Si
Requisitos de Usabilidad	RQ6	Fácil instalación, configuración y uso	No	Si	No	Si	Si
Atributos del sistema	RQ7	Ingreso al sistema con usuario y contraseña	Si	Si	Si	Si	Si
	RQ8	Funcionamiento del sistema las 24h del día	Si	Si	Si	Si	Si
	RQ9	Añadir más componentes al sistema	Si	Si	Si	Si	Si
		Cumplimiento total de requisitos	77.7%	100%	88.8%	100%	77.7%

Fuente: Autora

De acuerdo a la Tabla 9 tanto el software Zabbix como Pandora FMS cumplen con los requerimientos establecidos en el SRS. Para la realización de este proyecto se ha optado por utilizar la herramienta Zabbix, debido a que es una plataforma 100% libre y no requiere de actualizaciones a versiones Enterprise como Pandora FMS.

3.6.3. Software Zabbix

Zabbix es un software basado en código abierto que permite a las empresas tomar control de la disponibilidad y uso de recursos de los servicios de información para atender incidencias y mitigar en la medida posible la aparición de problemas, a través del monitoreo de servidores, aplicaciones y servicios de red, generando alertas ante situaciones que requieren atención (Alkaid, 2015). De acuerdo a (Alkaid, 2015), Zabbix cuenta entre otras con las siguientes funcionalidades:

- **Recolección de Datos**

Zabbix ofrece diferentes métodos para la recolección de datos de los ítems monitoreados: Agente Zabbix, SNMP, Prueba Remota, Monitoreo a la Medida, Máquinas Virtuales, Escenarios Web, Aplicaciones Java, Motores de Bases de Datos, Rendimiento de Recursos.

- **Detección de Incidencias**

Luego de recibir los datos, se realiza una evaluación para determinar la aparición de incidencias en base a una serie de criterios configurados. Posteriormente se clasifica la incidencia dependiendo de su nivel de criticidad, y generando notificaciones.

- **Visualización de Datos**

Zabbix cuenta con una interfaz de usuario en la Web en la cual se puede realizar la configuración de los dispositivos monitoreados e ítems recolectados. También permite visualizar

incidencias, eventos y el histórico de comportamiento, presentando la información en forma de gráficos o listas detalladas. La pantalla principal de Zabbix se puede observar en la Figura 18.

- **Plantillas Avanzadas**

Zabbix incorpora una serie de plantillas en las que cada una posee ítems, eventos, disparadores, notificaciones, dashboards, facilitando la configuración. El usuario también puede definir sus propias plantillas

- **Auto Descubrimiento**

Zabbix puede encontrar elementos que conforman la red de manera automática y tomar acciones como agregar hosts, enviar notificaciones, ejecutar scripts remotos, etc. También puede detectar sistemas de archivos, interfaces de red, etc.

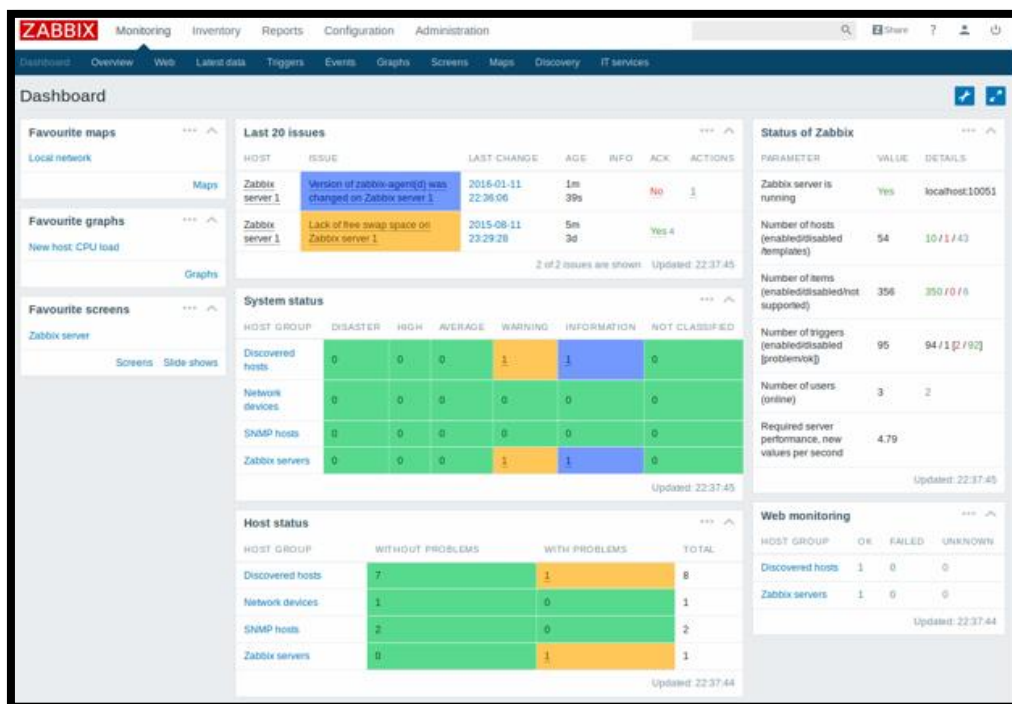


Figura 18. Pantalla principal de Zabbix

Fuente: Recuperado de: <http://www.zabbix.com/screenshots>

Zabbix es soportado en las siguientes plataformas:

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Windows (Zabbix agent)

3.6.3.1. *Requerimientos de hardware*

El software de monitoreo será instalado en el sistema operativo CentOS 7. Los requerimientos de hardware de este S.O. con la arquitectura x86 se muestran en la Tabla 10.

Tabla 10. Requerimientos de hardware para CentOS 7

Requerimiento	Mínimo	Recomendado
Memoria	1GB	2GB
Espacio de disco	20 GB	40GB
Procesador	226Mhz	226Mhz

Fuente: <https://documentation.cpanel.net/display/ALD/Installation+Guide+-+System+Requirements>

Zabbix y especialmente la base de datos Zabbix pueden requerir recursos significativos de la CPU dependiendo del número de parámetros supervisados y del motor de base de datos elegido.

La Tabla 11 proporciona los requerimientos mínimos de hardware en base al tamaño de la empresa para Zabbix.

Tabla 11. Requerimientos de hardware de Zabbix

Nombre	Plataforma	CPU/Memoria	Disco duro	Hosts monitoreados
<i>Pequeño</i>	CentOS	Dispositivo virtual	40GB	100
<i>Mediana</i>	CentOS	2 CPU cores/2GB	80GB	500
<i>Grande</i>	RedHat Enterprise Linux	4 CPU cores/8GB	100GB	>1000
<i>Muy grande</i>	RedHat Enterprise Linux	8 CPU cores/16GB	120GB	>10000

Fuente: <https://www.zabbix.com/documentation/3.0/manual/installation/requirements>

De acuerdo al número de hosts a monitorear, que en este caso es menor a 500, el nivel de configuración recomendada para el entorno en donde se desarrolla este proyecto es mediano

3.7. Selección del hardware de gestión de red

Se definen los requerimientos para el hardware de gestión de red y se determina el equipo más factible.

3.7.1. Análisis de crecimiento de equipos de conmutación.

Actualmente se tienen 101 equipos de conmutación, entre switches de core y acceso, no obstante, considerando el crecimiento que tendrá la infraestructura de la red, se procede a determinar la tasa de crecimiento aplicando la ecuación (2). La Tabla 12 muestra el incremento de equipos de conmutación en los últimos cinco años.

Tabla 12. Incremento de equipos de conmutación anual

Año	Equipos de conmutación
2012	79
2013	81
2014	81
2015	93
2016	101

Fuente: DDTI

Aplicando la fórmula:

$$Tasa\ de\ crecimiento = \frac{Presente - Pasado}{Pasado} \times 100\% \quad (2)$$

$$Tasa\ de\ crecimiento\ 5\ años = \frac{101 - 79}{79} \times 100\%$$

$$Tasa\ de\ crecimiento\ 5\ años = 27,84\%$$

Se obtiene que, hubo un crecimiento del 27,84% de equipos de conmutación durante un periodo de cinco años. Por lo tanto, se prevee que la cantidad de equipos de conmutación para los próximos cinco años será de 129.




3.7.2. Requerimientos del servidor de gestión de red

Una vez identificados los requerimientos de la herramienta Zabbix, se determinó que el sistema requiere de un dispositivo físico, el equipo adecuado para alojar el software debe presentar las siguientes características mínimas:

- CPU de 2 cores.
- Tamaño mínimo de memoria de 2GB
- Contar con una interfaz GigabitEthernet.
- Disco duro de 80GB
- Permitir la instalación de distribuciones Linux.

En la Tabla 13, se muestra una comparativa entre varios servidores existentes en el mercado de diferentes fabricantes, tomando en cuenta que cubran los requerimientos antes mencionados. Esto se realiza con el fin de determinar el equipo adecuado para la instalación del software de gestión Zabbix.

Tabla 13. Comparación de equipos

	HP ProLiant ML110 G5	IBM System x3100 M5	Dell PowerEdge T20
			
Fabricante	HP	IBM	DELL
CPU	Intel Xeon 3065 / 2.33 GHz	Intel Xeon 3.10GHz	Intel Xeon E3-1225 v3 3.2 GHz
Número de cores	Dual-Core	Dual-Core	Quad-Core
Máximo tamaño de memoria	8GB	8GB	32GB
Memoria instalada	2GB	8GB	4GB
Memoria Cache	L2 cache - 4 MB	L2 cache - 4 MB	L3 Cache 8MB L3 Cache
Disco duro	1 TB HDD 7200 rpm	1 TB HDD 7200 rpm	1TB HDD 7200 rpm
Protocolo de enlace de datos	Ethernet, Fast Ethernet, Gigabit Ethernet	Ethernet, Fast Ethernet, Gigabit Ethernet	Ethernet, Fast Ethernet, Gigabit Ethernet
Precio	\$1392,38	\$1223,60	\$862,31

Fuente: Adaptado de: <https://www.cnet.com/products/hp-proliant-ml110-g5-xeon-3065-2-33-ghz-monitor-none-series/>,
<https://www.amazon.com/System-E3-1220-3-10GHz-Mini-tower-5457ECU/dp/B00M0VRJ8S> y
https://www.amazon.com/gp/offer-listing/B011ZB45LM/ref=dp_olp_new_mbc?ie=UTF8&condition=new,
https://harddrivesdirect.com/product_info.php?products_id=200171

De acuerdo a las características que se presentan en Tabla 13, el equipo más óptimo es el servidor Dell PowerEdge T20 debido a que cumple y supera los requerimientos mínimos de CPU,

disco duro y memoria, lo cual asegura la escalabilidad del sistema de gestión de red. Esto da la posibilidad de que se adicionen nuevos dispositivos en el futuro sin que esto afecte al rendimiento del gestor.

CAPÍTULO IV

4. Implementación

En este capítulo se establecen las políticas de gestión de red y manuales de procedimientos. Se detalla la implementación del modelo y se realiza un análisis costo-beneficio.

4.1. Establecimiento de Políticas

Las políticas de gestión de red se basan en las cinco áreas funcionales del modelo de gestión ISO/OSI que se describen en el apartado 2.4.2. A continuación, se presenta un manual que contiene cada una de las políticas de gestión de red para la Universidad Técnica del Norte, cuya función es la de definir las reglas pertinentes para asegurar el buen uso del sistema de gestión de red. El acta de entrega de Políticas de gestión de red y manual de procedimientos se encuentra en el ANEXO N.

UNIVERSIDAD TÉCNICA DEL NORTE		
POLÍTICAS DE GESTIÓN PARA LA RED DE DATOS DEL EDIFICIO CENTRAL		
DE LA UTN		
	Elaborado por:	Jessica Báez
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Juan Carlos García, Director de DDTI
	Versión:	1.0
	Fecha:	16/02/2017

I. PROPÓSITO

El presente documento permitirá definir las políticas de gestión de red que deben ser cumplidas por el encargado de la administración de red de la institución para garantizar el buen uso y funcionamiento del sistema de gestión de red.

II. CONCEPTOS PREVIOS

- **Gestión de red**

La gestión de red consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando su funcionamiento.

- **Políticas de gestión de red**

Consiste en un manual que permite al administrador de la red manejar de forma ordenada cualquier suceso que pueda presentarse en la red.

III. NIVELES ORGANIZACIONALES

- a) **Director.** - Autoridad de nivel superior de la Dirección de Desarrollo Tecnológico e informático de la UTN.
- b) **Administrador de red.** - Persona encargada de administrar los recursos de red de la institución. Bajo su administración corresponde la aceptación de las políticas de gestión de red.

IV. GENERALIDADES

- a) El administrador de la red de datos deberá cumplir las políticas definidas en este documento, en cuanto al uso del sistema de gestión de red.

- b) Las políticas definidas en este documento podrán ser actualizadas en caso de requerirlo, siempre y cuando se ajusten a las áreas funcionales del modelo de gestión de red ISO/OSI.

V. VIGENCIA

Las políticas expuestas en el presente documento entrarán en vigencia desde el momento en que tenga la aprobación del Administrador de red de la UTN. Estas reglas estarán sujetas a las modificaciones que el Administrador de red considere pertinentes.

VI. REFERENCIA

Debido a que actualmente no existe un formato para las políticas de gestión de red, se ha tomado como referencia la tesis realizada en el GAD de Ibarra por Viviana Ayala, en el año 2015.

VII. ESTRUCTURA DE LAS POLÍTICAS DE GESTIÓN

1. Políticas de gestión de red

- 1.1. Objetivo de las políticas de gestión de red
- 1.2. Compromiso de las autoridades

2. Gestión de configuraciones

- 2.1. Ingreso de dispositivos a la red de datos
- 2.2. Configuración de dispositivos

3. Gestión de fallos

- 3.1. Manejo de fallos
- 3.2. Documentación de fallos

4. Gestión de contabilidad

- 4.1. Inventario de los dispositivos gestionados

5. Gestión de prestaciones

5.1.Reportes de rendimiento

6. Gestión de seguridad

6.1.Acceso al sistema de gestión de red

6.2.Acceso a los dispositivos gestionados

VIII. TÉRMINOS Y DEFINICIONES

DDTI: Dirección de Desarrollo Tecnológico e Informático, Departamento encargado de las TIC's en la UTN.

Dispositivo de red: Es el hardware que hace posible la comunicación entre las computadoras que hay en una red.

Fallo: Circunstancia de fallar o no funcionar una cosa como debía o se esperaba.

Red de datos: Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.


Reporte: Un reporte es un escrito que se desarrolla con el objetivo de dar a conocer algo. Estos documentos permiten la difusión de diferentes clases de datos con distintos fines u objetivos.

SNMP: Simple Network Management Protocol. Es un protocolo de la capa de aplicación perteneciente a la familia de protocolos TCP/IP que facilita el intercambio de información de administración entre dispositivos de red.

Gestor: Es el dispositivo encargado de realizar la supervisión y control permanente de los dispositivos gestionados.


Agente: Es el software de administración de red que se encuentra en el dispositivo para que pueda ser gestionado.


POLÍTICAS DE GESTIÓN DE RED

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	1. Política de gestión de red
	Control	1.1. Objetivo de las políticas de gestión de red
	Encargado	Administrador de red
<p>Art. 1. Brindar la información necesaria acerca del sistema de gestión de red a las personas encargadas de la administración de red, quienes deben cumplir con las políticas propuestas para mejorar la disponibilidad de la red identificando los problemas que se suscitan en los dispositivos con la mayor brevedad posible.</p>		

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	1. Política de gestión de red
	Control	1.2. Compromiso de las autoridades
	Encargado	Administrador de red
<p>Art. 2. El administrador de red, como responsable de la elaboración de Políticas de gestión de red para el Edificio Central de la UTN, toma el compromiso de revisión y socialización de las políticas definidas en el presente documento.</p>		

POLÍTICAS DE GESTIÓN DE CONFIGURACIONES


	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	2. Gestión de configuraciones
	Control	2.1.Ingreso de equipos a la red
	Encargado	Administrador de red
<p>Art. 3. La DDTI deberá tener un inventario propio de equipos de red. Al ingresar un nuevo dispositivo se deberá documentar su información, tomando en cuenta las características más importantes del equipo.</p> <p>Art. 4. A todos los dispositivos que se adicionen se les debe activar el protocolo SNMP (siempre y cuando lo soporten) y configurar la comunidad de gestión, para que éstos puedan ser monitoreados.</p>		

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	2. Gestión de configuraciones
	Control	2.2.Configuración de equipos
	Encargado	Administrador de red
<p>Art. 5. Únicamente el administrador de la red y quienes estén previamente autorizados podrán realizar configuraciones sobre los dispositivos de red.</p> <p>Art. 6. Se deberá mantener respaldos de las configuraciones realizadas en los dispositivos de red, en caso de que haya pérdida de información o desconfiguraciones accidentales.</p> <p>Art. 7. Antes de realizar una configuración sobre un elemento de la red, la persona encargada de ello deberá realizar un respaldo de la última configuración correcta del dispositivo.</p>		

Art. 8. Toda configuración de los equipos de red deberá ser documentada, para que haya un registro de los cambios que se realizan.

El formato correspondiente al registro y configuración de equipos se encuentran en el manual de gestión de configuraciones, en el ANEXO M.


POLÍTICAS DE GESTIÓN DE FALLOS

UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio
	Control
	Encargado
<p>Art. 9. El equipo de tecnología de la DDTI hará uso de la interfaz del software de administración de red para verificar si se ha detectado un fallo en la red y proceder al aislamiento y solución del mismo.</p> <p>Art. 10. El administrador de red podrá asignar a otra persona del equipo de tecnología de la DDTI para que se encargue del aislamiento y solución de la falla.</p> <p>Art. 11. La persona designada a un determinado fallo deberá dar solución al problema en el menor tiempo posible y de acuerdo a las características del problema que se presente, para evitar inconvenientes en las labores que desempeñan los usuarios de la red.</p> <p>Tomando como base el tipo de fallo reportado y del diagnóstico de la búsqueda y resolución de problemas, se establece un sistema de asignación de prioridades según el estado del servicio.</p> <ul style="list-style-type: none"> • Prioridad 1 (Crítico): El equipo está fuera de servicio, inestable o con interrupciones repetitivas durante breves periodos de tiempo. Requiere acción inmediata por parte del 	


administrador para restablecer el servicio a condiciones operativas normales de funcionamiento.

- **Prioridad 2 (Error):** El servicio presenta degradación en la calidad. Requiere de acción inmediata del administrador de red siempre y cuando no haya alertas de Prioridad 1.
- **Prioridad 3 (Aviso):** No requiere inmediata atención por parte del administrador de red. Notificación de algún tipo de impacto en el servicio a causa de actividades programadas como: mantenimiento, cambios y adición de equipos.
- **Prioridad 4 (Notificación, Información):** Información referente al servicio. No genera ningún impacto sobre el servicio, por lo que no requiere de ninguna acción por parte del administrador de red.


Prioridad	Fallo	Tiempo de solución
1/crítico	Caída total del servicio	Se permitirá la solución del problema de 0 a 1 hora.
2/error	Alerta del dispositivo Desconocido	Se permitirá la solución del problema de 2 a 4 horas.
3/aviso	Alerta del Servicio Parcialmente Caído	Se permitirá la solución del problema dentro de 24 horas.
4/información	Dispositivo Funcionando	Se permitirá la solución del problema dentro de 48 horas.

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	3. Gestión de fallos
	Control	3.2.Documentación de fallos
	Encargado	Administrador de red
<p>Art. 12. Se deberán documentar tanto los fallos ocurridos como la solución de los mismos, para que la próxima vez que ocurran se tenga un proceso ya establecido que permita dar con la solución con mayor prontitud.</p>		


POLÍTICAS DE GESTIÓN DE CONTABILIDAD

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	4. Gestión de Contabilidad
	Control	4.1.Inventario de los dispositivos gestionados
	Destinatario	Administrador de red
<p>Art. 13. La herramienta de gestión de red se utilizará para generar registros sobre la utilización de los recursos de red como: disco duro, memoria y CPU de los dispositivos monitoreados, estadísticas de interfaces y estadísticas de protocolos.</p> <p>Art. 14. El administrador de red podrá obtener reportes del uso de recursos de red monitoreados mediante la herramienta de gestión de red, de forma mensual y anual, en el momento que él lo requiera.</p> <p>Art. 15. No se realizará ningún tipo de tarificación a los usuarios.</p>		

POLÍTICAS DE GESTIÓN DE PRESTACIONES

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	5. Gestión de Prestaciones
	Control	5.1. Reportes de rendimientos
	Destinatario	Administrador de red
<p>Art. 16. El administrador de red podrá generar reportes en el momento que considere necesario para obtener información acerca de los recursos monitoreados: tráfico de interfaces, tiempos de respuesta y disponibilidad.</p> <p>Art. 17. Se establecerá umbrales de aceptación, bajo los cuales los equipos de red trabajen correctamente.</p> <p>Art. 18. Los reportes deberán ser analizados para futuras mediciones y pronóstico acerca de los dispositivos de red.</p>		

POLÍTICAS DE GESTIÓN DE SEGURIDAD


	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	6. Gestión de Seguridad
	Control	6.1. Acceso al sistema de gestión de red
	Destinatario	Administrador de red
<p>Art. 19. El administrador de red tendrá la potestad de crear nuevas cuentas de usuario para ingresar al sistema de gestión con los privilegios que considere prudentes.</p>		

Art. 20. Únicamente los responsables del componente tecnológico podrán acceder a sistema de gestión de red a través de un usuario y contraseña.

Art. 21. En caso de haber notificaciones vía correo electrónico, estas sólo se enviarán al administrador de la red.

Art. 22. El administrador de red podrá realizar las configuraciones que crea convenientes en el sistema de gestión.

El ingreso al sistema de gestión de red se muestra en el manual de gestión de seguridad en el apartado 4.2.5.

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	6.Gestión de Seguridad
	Control	6.2.Acceso a los dispositivos gestionados
	Destinatario	Administrador de red
<p>Art. 23. El acceso a los dispositivos gestionados debe ser realizado mediante el uso de contraseñas asignadas previamente por el responsable de la red.</p> <p>Art. 24. Únicamente los usuarios autorizados tendrán las claves de acceso para ingresar a los dispositivos gestionados.</p>		

4.2. Manual de Procedimientos

El presente manual de procedimientos está estructurado en base a cada área funcional del estándar de gestión red ISO/OSI, el cual deberá ser utilizado por el personal encargado de la administración de red para diagnosticar y corregir problemas de manera oportuna. El acta de entrega de Políticas y Manual de procedimientos se encuentra en el ANEXO N.

4.2.1. Manual de procedimientos para la gestión de configuraciones

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE CONFIGURACIONES		
	Elaborado por:	Jessica Báez
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Juan Carlos García, Director de DDTI
	Versión:	1.0
	Fecha:	16/02/2017

Objetivo. - Presentar el procedimiento a seguir cuando se requiere adicionar un nuevo dispositivo a la red y realizar sus respectivas configuraciones para que desempeñe sus funciones dentro de la red.

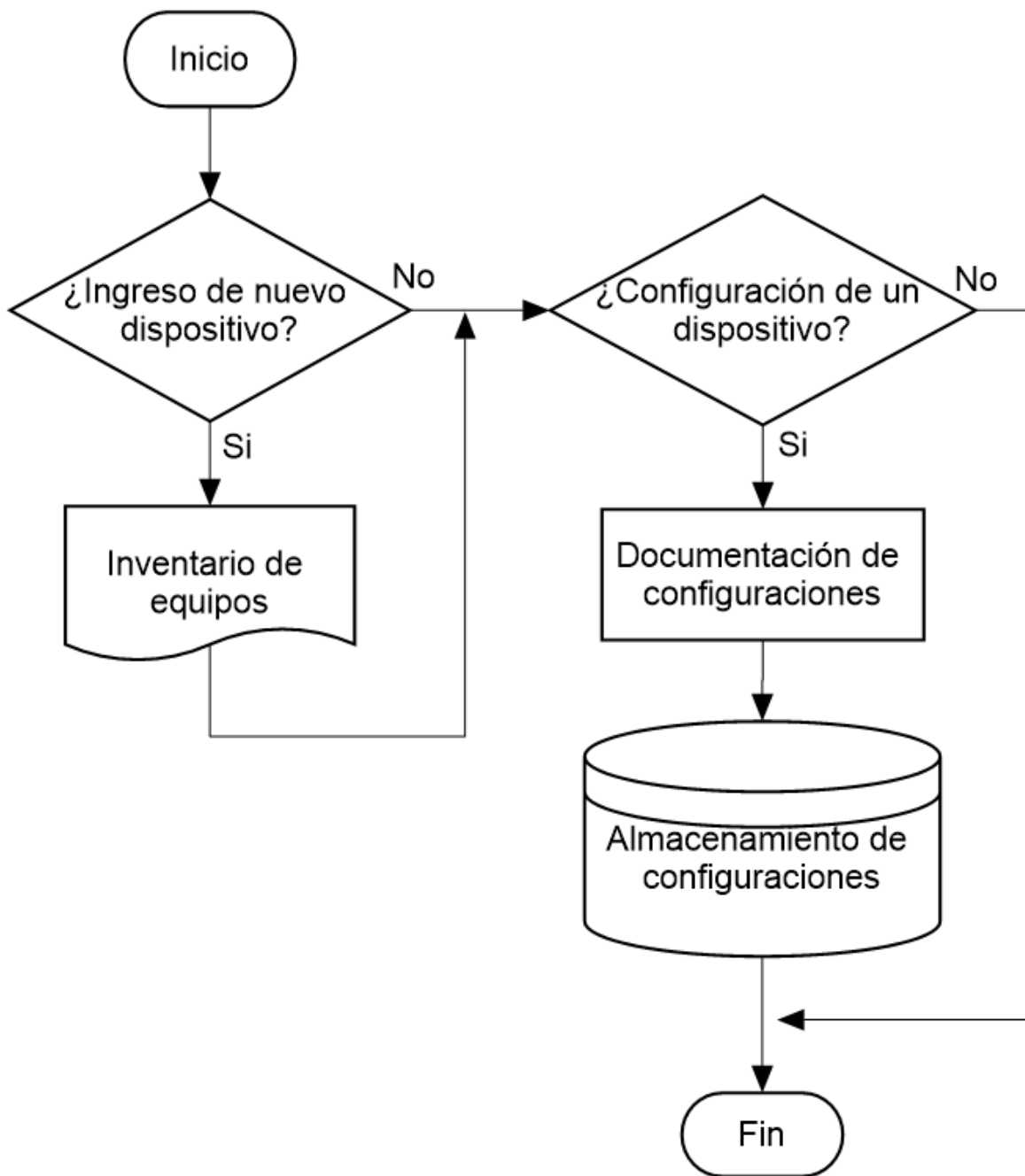
Alcance. - Este manual esta realizado para ingresar nuevos dispositivos en la red de datos del Edificio Central, este procedimiento se aplica a todos los dispositivos de red que se agreguen desde que el presente manual entre en vigencia. Adicionalmente se presentarán los formatos para documentar tanto el ingreso de nuevos dispositivos como la configuración de los mismos.

Descripción del procedimiento

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Ingreso de equipos	<p>1) Verificar que el equipo funcione correctamente.</p> <p>2) Registrar el dispositivo en el inventario que provee la herramienta Zabbix teniendo en cuenta la siguiente información:</p> <ul style="list-style-type: none"> • Tipo de equipo • Nombre del Equipo • Dirección IP y máscara de Red • Marca y modelo • Número de Serie • Ubicación del Equipo • Fecha de Ingreso • Responsable del equipo • Proveedor • Fabricante • Soporte y garantía 	Administrador de red
2	Configuración de equipos	<p>1) Realizar la configuración del equipo incluyendo:</p> <ul style="list-style-type: none"> • Configuraciones básicas de seguridad. • Configuraciones de adaptación a la red en base a la función que cumplirá el dispositivo. 	Administrador de red

		2) Habilitar el protocolo SNMP y configurar la comunidad de gestión para que pueda ser monitoreado.	
3	Documentación de configuraciones	<ol style="list-style-type: none"> 1) Obtener respaldos de las configuraciones de los equipos gestionados. 2) Almacenar los respaldos en el cloud institucional del administrador de red. 3) Registrar los detalles de la configuración realizada en la plantilla que se propone en el ANEXO . 4) En caso de desconfiguración de los equipos gestionados, cargar sus respectivos respaldos. 	Administrador de red

Flujograma



4.2.2. Manual de procedimientos para la gestión de fallos

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE FALLOS		
	Elaborado por:	Jessica Báez
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Juan Carlos García, Director de DDTI
	Versión:	1.0
	Fecha:	16/02/2017

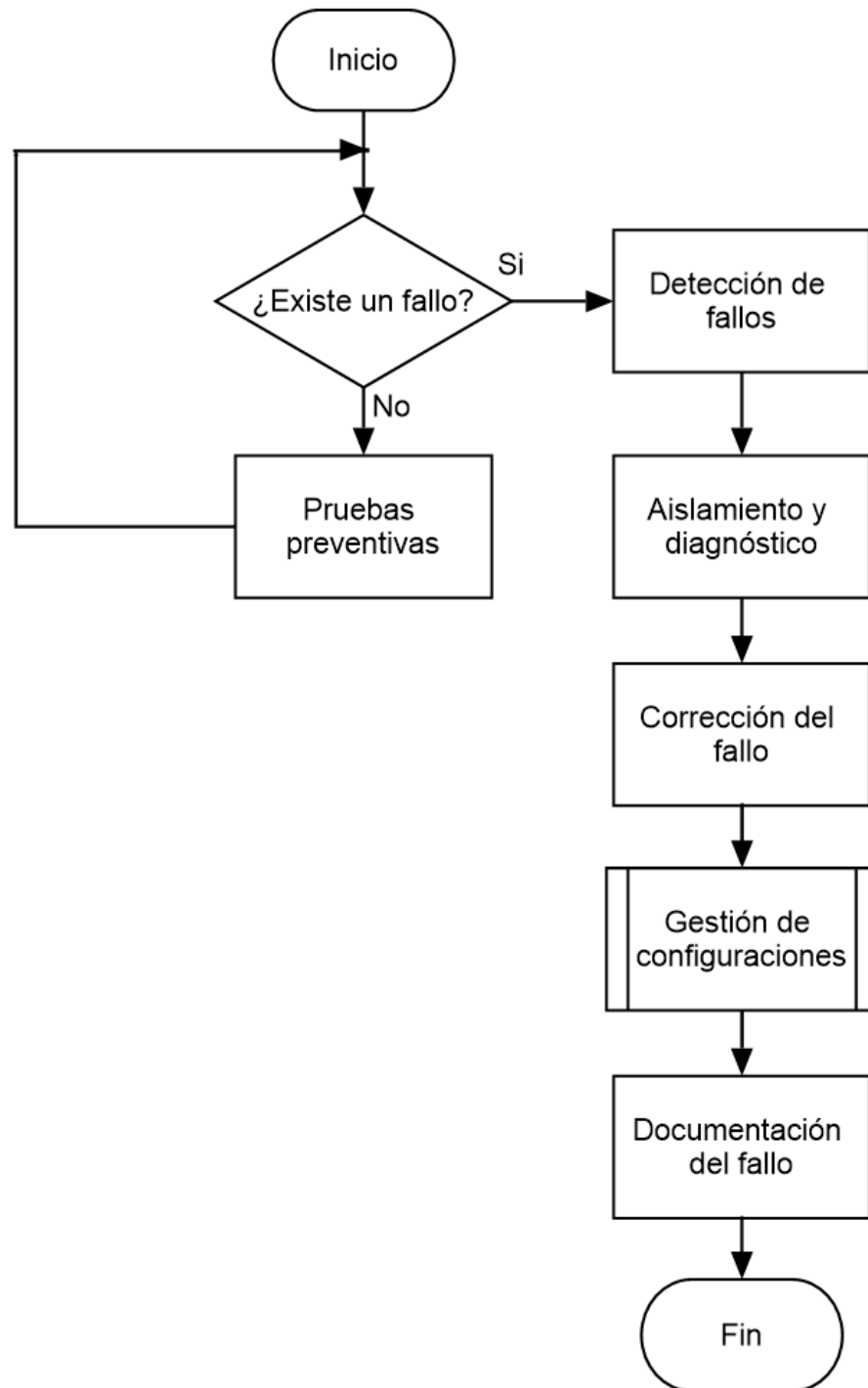
Objetivo. - Presentar el proceso a seguir para la detección, aislamiento y solución de fallos que se susciten dentro de la red, para mejorar el tiempo de respuesta ante este tipo de eventualidades

Alcance. - Este manual esta realizado para ser aplicado en todos los dispositivos gestionados, cubriendo áreas estratégicas; este procedimiento se aplica a los fallos en general que se presenten en la red.

En caso de existir un fallo, este se documentará junto con su respectiva solución para que en caso de que vuelva a presentarse se conozca el procedimiento para solucionarlo eficazmente.

Descripción del procedimiento

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Detección del fallo	<ol style="list-style-type: none"> 1) Planificar y crear ambientes de prueba. 2) Usar la interfaz del software de gestión para verificar el estado de los equipos. 3) Permanecer alerta a las notificaciones que envía el sistema de gestión. 4) Crear un ticket en la aplicación OTRS. 	Encargado del componente tecnológico
2	Aislamiento y diagnóstico del fallo	<ol style="list-style-type: none"> 1) Identificar el origen del fallo. 2) Diagnosticar el problema. 	Encargado del componente tecnológico
3	Corrección del fallo	<ol style="list-style-type: none"> 1) Realizar un respaldo de la configuración del equipo. 2) Identificar la solución del problema. 3) Corregir el problema. 4) Cerrar el ticket que corresponde a la incidencia solucionada. 	Encargado del componente tecnológico
4	Documentación de fallos	<ol style="list-style-type: none"> 1) Documentar el problema ocurrido 2) Detallar el proceso realizado para la solución del problema según la plantilla establecida en el ANEXO E. 	Encargado del componente tecnológico

Flujograma

4.2.3. Manual de procedimientos para la gestión de contabilidad

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE CONTABILIDAD		
	Elaborado por:	Jessica Báez
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Juan Carlos García, Director de DDTI
	Versión:	1.0
	Fecha:	16/02/2017

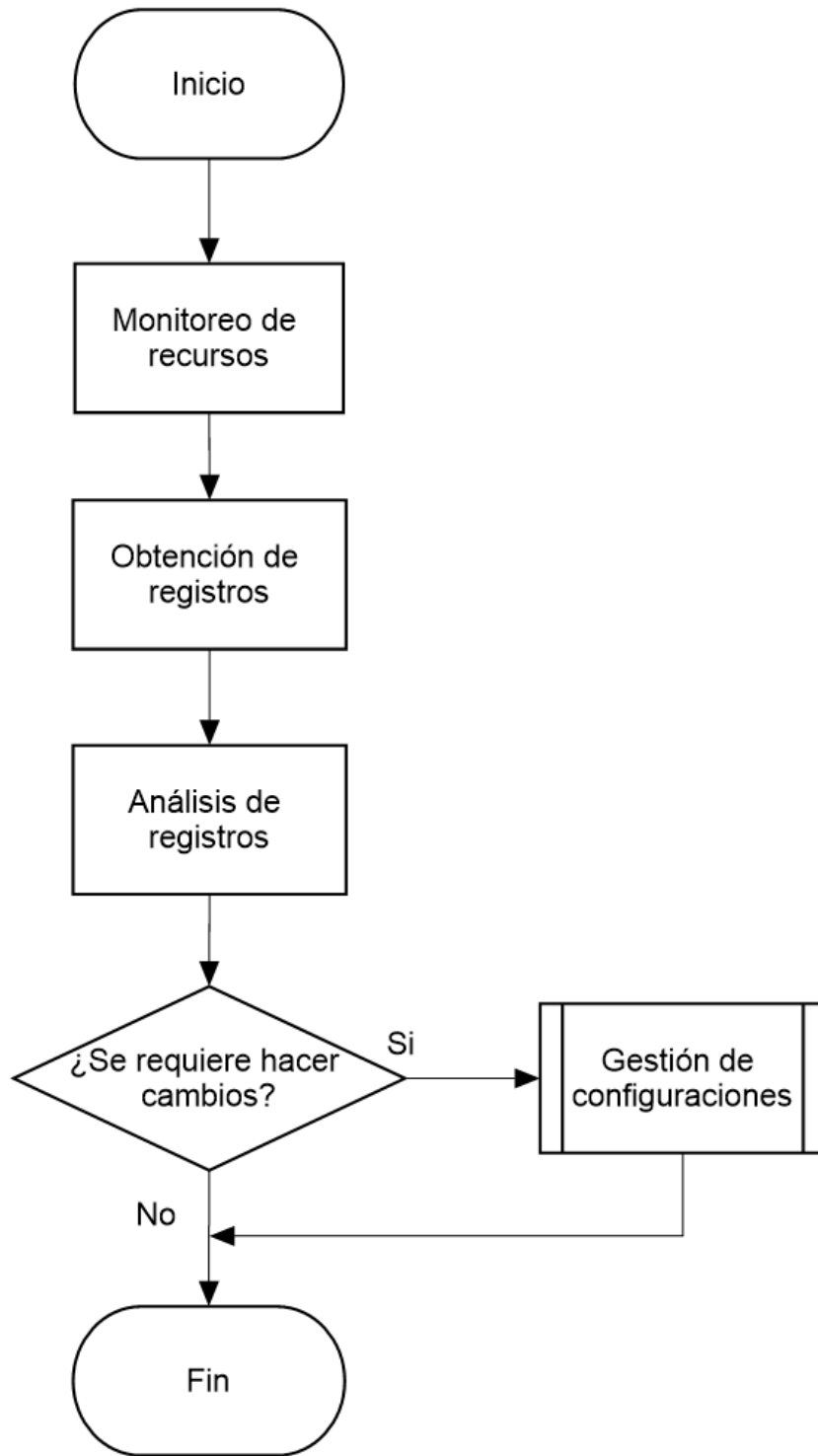
Objetivo. - Presentar el procedimiento a seguir para recolectar la información acerca de la utilización de recursos de la red y la obtención de reportes presentados por el software de gestión, para conocer de manera constante el desempeño de la red.

2. Alcance. – En este manual se presentan los procesos a seguir para medir la utilización de los recursos de la red y generación de reportes acerca de los dispositivos ingresados en el sistema de gestión de red.

Descripción del procedimiento

Nº	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Obtención de reportes	1) Monitoreo de los recursos de la red: <ul style="list-style-type: none"> • Memoria • CPU 	Encargado del componente tecnológico

		<ul style="list-style-type: none">• Estadísticas del tráfico en interfaces <ol style="list-style-type: none">2) Determina el reporte o historial en base al tiempo de funcionamiento que se quiera adquirir, ya sea semanal o mensual.3) Generar los reportes en formato PDF e imprimirlos en caso de ser necesario.4) Analizar los reportes.5) Si se determina que debe hacerse un cambio, pasar al proceso de gestión de configuraciones.	
--	--	--	--

Flujograma

4.2.4. Manual de procedimientos para la gestión de prestaciones

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE PRESTACIONES		
	Elaborado por:	Jessica Báez
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Juan Carlos García, Director de DDTI
	Versión:	1.0
	Fecha:	16/02/2017

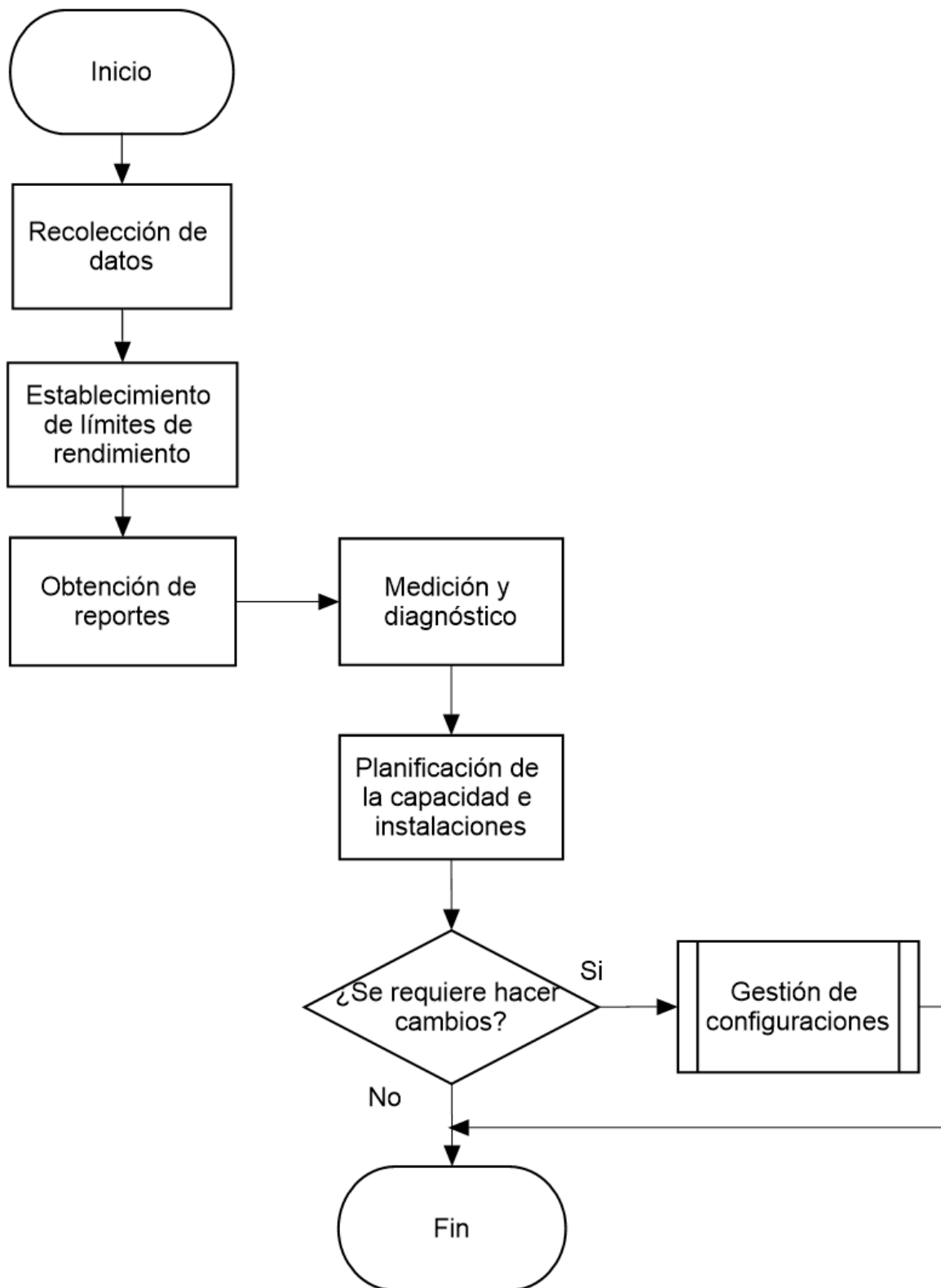
Objetivo. - Presentar el procedimiento a seguir para recolectar la información del tráfico generado en la red y la obtención de reportes presentados por el software de gestión, para conocer de manera constante el desempeño de la red.

2. Alcance. – En este manual se presentan los procesos a seguir para el escaneo del tráfico y generación de reportes acerca de los dispositivos ingresados en el sistema de gestión de red.

Descripción del procedimiento

Nº	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Recolección de datos	1) Usar la interfaz del software de gestión para visualizar de manera gráfica el desempeño de los dispositivos de la red.	Encargado del componente tecnológico

		<p>Se tomarán en cuenta los siguientes indicadores:</p> <ul style="list-style-type: none"> • Tráfico de interfaces • Tiempos de respuesta • Disponibilidad porcentual <p>2) Establecer umbrales bajo los cuales se considere un rendimiento de la red aceptable.</p>	
2	Generación de reportes	<p>1) Se generarán reportes de manera semanal o mensual, según lo requiera el director de DDTI.</p> <p>2) Los reportes se mantendrán de manera digital y se imprimirán sólo en el caso de ser necesario.</p> <p>3) Los reportes deberán ser evaluados para su posterior pronóstico.</p> <p>4) De acuerdo al pronóstico obtenido se realizará la planificación de capacidad e instalaciones.</p> <p>5) Si se determina que debe hacerse un cambio, pasar al proceso de gestión de configuraciones.</p>	Encargado del componente tecnológico

Flujograma

4.2.5. Manual de procedimientos para la gestión de seguridad

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE SEGURIDAD		
	Elaborado por:	Jessica Báez
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Juan Carlos García, Director de DDTI
	Versión:	1.0
	Fecha:	16/02/2017

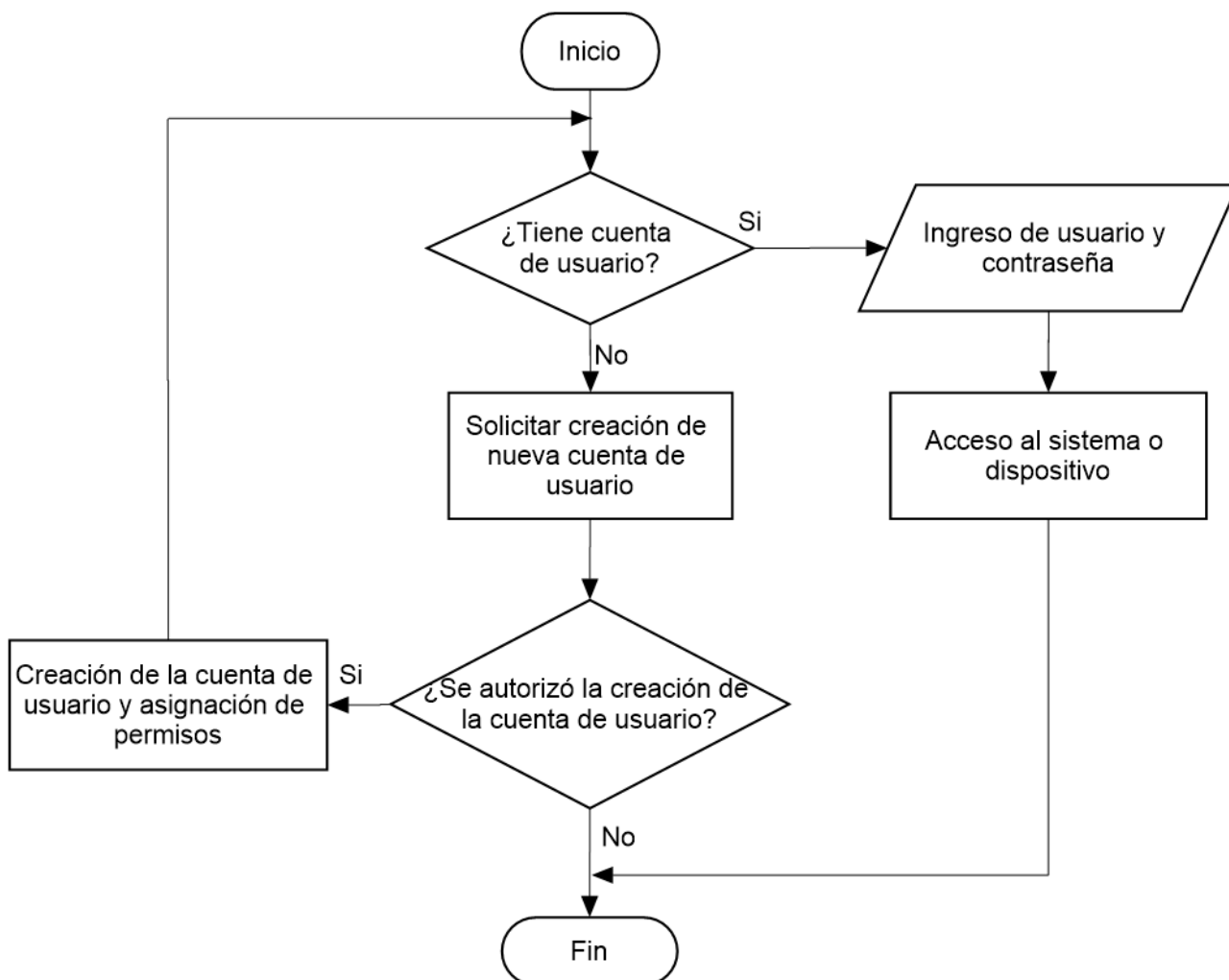
Objetivo. - Presentar el procedimiento a seguir para el acceso al sistema de gestión y dispositivos gestionados.

Alcance. - Este manual es la guía de procesos para el acceso al sistema de gestión de red y dispositivos monitoreados.

Descripción del procedimiento

Nº	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Acceso al software de gestión	1) El administrador de red creará nuevas cuentas de usuario en caso de requerirlo, previo a la autorización del Director de la DDTI.	Administrador de red

		<p>2) El nombre de usuario se creará a partir del primer nombre y primer apellido</p> <p>3) Únicamente quienes tengan cuentas de usuario podrán acceder al sistema de gestión de red.</p> <p>4) El administrador podrá realizar configuraciones dentro del sistema de gestión de red.</p>	
2	Acceso a los dispositivos gestionados	1) El administrador de red podrá acceder a los dispositivos gestionados mediante el uso de contraseñas que se manejan actualmente en los equipos.	Administrador de red

Flujograma

4.3. Implementación del modelo de gestión de red

Se detalla la implementación del modelo de gestión de red, conformado por el gestor, agentes y protocolo de gestión. Se desarrolla la implementación para cada una de las áreas funcionales del sistema de gestión de red ISO/OSI.

La Figura 19 muestra un esquema del sistema de gestión de red implementado en este proyecto, identificando a la estación gestora y a los dispositivos inicialmente gestionados. Los dispositivos representados con “OK”, son los que forman parte del sistema de gestión.

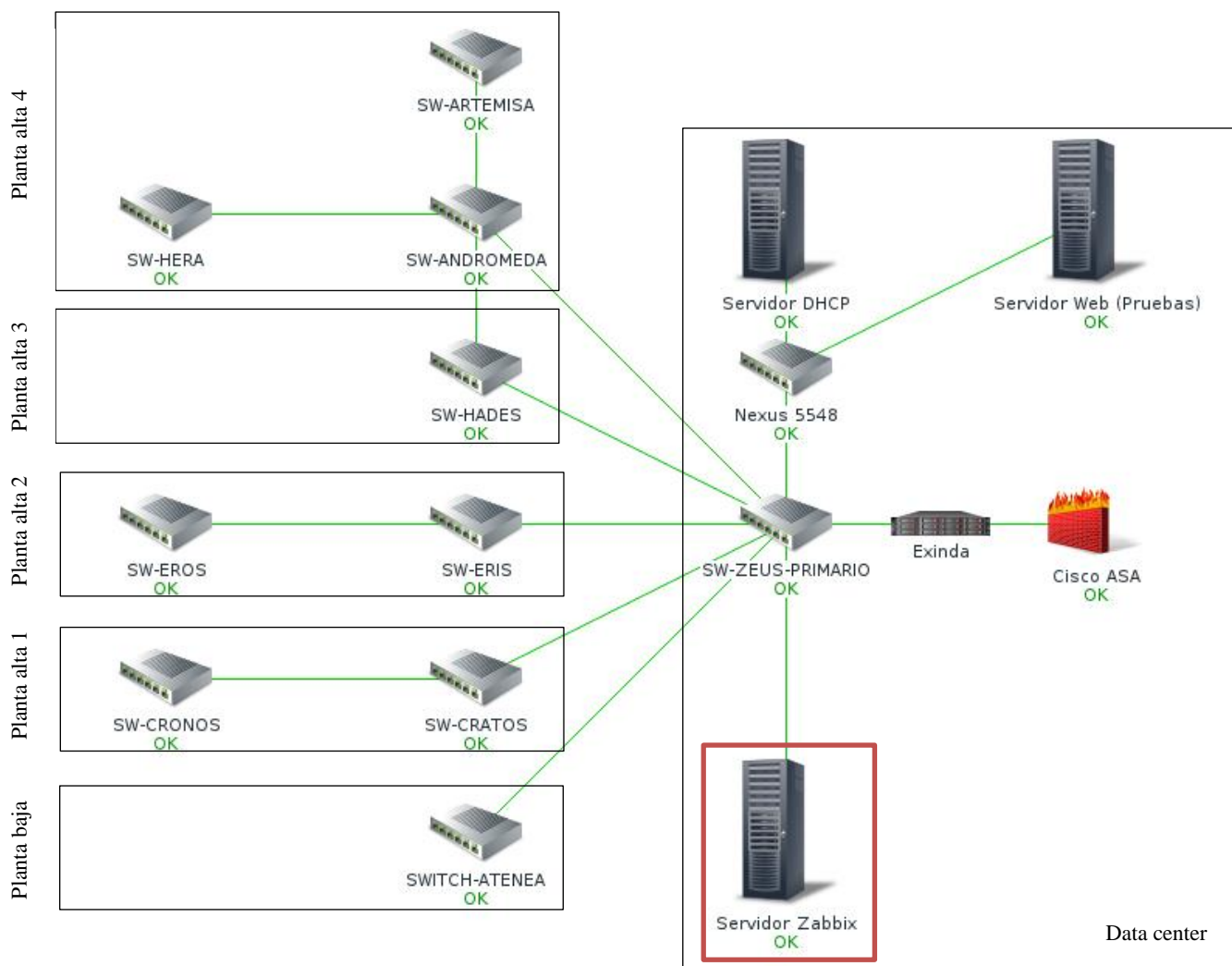


Figura 19. Diagrama de gestión

Fuente: Captura de Zabbix

Configuración del gestor

En vista de que la institución dispone de un servidor IBM 3200 M2 con las características descritas en la Tabla 14, se realizará la implementación de la estación gestora en dicho equipo, sin embargo, en el mercado existen otros equipos con mejores prestaciones, que cumplen con todos los requerimientos de hardware definidos para el funcionamiento del software Zabbix.

Tabla 14. Especificaciones técnicas de IBM 3200

Procesador	<ul style="list-style-type: none"> • Core 2 Duo E4600 3 GHz. • Optimizado para EM64T para soportar aplicaciones de 32 ó 64 bits
Memoria	<ul style="list-style-type: none"> • 2 GB de memoria RAM
Tamaño L2 cache	<ul style="list-style-type: none"> • 6144 KB
CD y DVD drives	<ul style="list-style-type: none"> • DVD-ROM
Slots	<ul style="list-style-type: none"> • Cinco slots de expansión: <ul style="list-style-type: none"> ○ 2 32-bit/33 MHz PCI ○ 2 PCI-Express ○ Opcional, 64-bit/133 MHz PCI-X
Networking	<ul style="list-style-type: none"> • Full-duplex integrado 10/100/1000 Mbps Ethernet
Video	<ul style="list-style-type: none"> • Controlador gráfico ATI ES1000 integrado con memoria de vídeo de 16 MB.
Fuente de alimentación	<ul style="list-style-type: none"> • Una Fuente de alimentación fija de 400 W.
Puertos	<ol style="list-style-type: none"> 1) 6 USB 2) Gigabit Ethernet con RJ-45 3) 2 puertos seriales
Configuración	<ul style="list-style-type: none"> • Minitorre para pequeñas y medianas empresas (opcionalmente montable en rack)

Fuente: <https://www-947.ibm.com/support/entry/portal/docdisplay?lnocid=migr-5074147>

De acuerdo a los requerimientos del software Zabbix descritos en la Tabla 11, se procede a la instalación de dicha herramienta en el equipo IBM 3200 asignado por el Administrador de red. El SO establecido como estándar por la DDTI dentro de sus políticas es CentOS7, por lo tanto, para el servidor de gestión se tendrá como software base el sistema operativo CentOS7.

La instalación del servidor de gestión de Red basado en Zabbix 3.0 implementado en el presente proyecto, se detalla en el ANEXO F describiendo los siguientes pasos:

1. Añadir los repositorios oficiales de Zabbix 3.0
2. Instalación de Zabbix 3.0 Server, agente y web front-end
3. Instalar MariaDB Server, habilitarlo e iniciarlo
4. Crear la base de datos y usuarios de Zabbix
5. Importar esquema inicial y datos
6. Configurar Zabbix Server
7. Configuración de PHP
8. Agregar reglas de Firewall y Selinux
9. Habilitar e iniciar el servidor Zabbix, agente y servicio HTTPD
10. Terminar la instalación a través de la interfaz web

Configuración de los dispositivos gestionados

En los dispositivos de red es necesario habilitar el protocolo SNMP para que puedan ser monitoreados por el software de gestión de red.

El software Zabbix permite monitorear la red mediante SNMPv1, SNMPv2 y SNMPv3. La versión del protocolo de gestión de red a implementarse es la SNMPv2c, la cual es una sub-versión de SNMPv2. Se eligió esta versión debido a que es ampliamente usada en los sistemas de gestión

de red, tiene mejores características que la primera versión y su configuración es simple. No se consideró la implementación de SNMPv3 debido a que, a pesar de agregar mecanismos de seguridad más robustos, los cálculos criptográficos causan un incremento de carga de CPU provocando que el software de gestión corra más lento (SNMP Research International, Inc., 2003).

- **Switches serie Catalyst**

El primer paso es establecer conexión con el dispositivo, para esto se usó la aplicación Putty. Se requiere únicamente establecer la dirección IP del equipo y el puerto de comunicación que en este caso es el 23 para poder acceder vía Telnet.

Es necesario saber si el dispositivo tiene habilitado el protocolo SNMP. El comando *show snmp* indica si el protocolo de gestión está habilitado, así como la comunidad.

En caso de que el protocolo no esté habilitado es necesario configurar la cadena comunidad con el comando, en donde RO corresponde a la función Read-Only. La cadena *public* corresponde al nombre de la comunidad de gestión, por motivos de seguridad es recomendable cambiarla por otra cadena.

```
snmp-server community public RO
```

Estas configuraciones sirven tanto para switches como para routers de la serie Catalyst

- **Cisco Asa 5500**

- Verificar si el protocolo SNMP está habilitado. De forma predeterminada, el servidor SNMP está habilitado.

```
snmp-server enable
```

- Especifica el destinatario de una notificación SNMP.

```
snmp-server host interface_name ip_address [trap | poll] [community text]
[version 1 | 2c] [udp-port port]
```

Identifica el nombre y la dirección IP del administrador NMS. La palabra clave *trap* limita el NMS a recibir traps solamente. La palabra clave de *poll* limita el NMS a las solicitudes de sondeo.

-Configurar la comunidad

```
snmp-server community community-string
```

- **Servidores**

En el caso del servidor Web y DHCP, éstos se encuentran instalados sobre el sistema operativo CentOS 6.8. Para monitorear este tipo de servicios se requiere de la instalación de una agente de gestión para que éste recoja información y se la envíe a la estación gestora.

Inicialmente se intentó instalar un agente de la versión 3.0 de Zabbix para que esté acorde con la versión implementada en la estación gestora, sin embargo, esta versión no fue soportada por el sistema operativo. Para solucionar este inconveniente se procedió a instalar una versión la última versión compatible con CentOS 6.8, que es el agente 2.2.

El procedimiento para instalar el agente Zabbix en CentOS 6.8 se resume en los siguientes pasos:

1. Añadir el repositorio de Zabbix
2. Instalar el agente Zabbix
3. Editar el archivo de configuración del agente para, principalmente, definir la dirección IP de la estación gestora

4. Reiniciar el agente
5. Configurar las iptables para que permita la entrada y salida de información de gestión.
6. Reiniciar las iptables

La instalación detallada del agente se muestra en el ANEXO I.

4.3.1. Implementación de Gestión de configuraciones

Dentro de la gestión de configuraciones se tiene el registro de las configuraciones e inventario de los equipos monitoreados.

4.3.1.1. Registro de configuraciones

Se propone una plantilla en formato Excel para registrar todas las configuraciones realizadas sobre los dispositivos gestionados.

La plantilla permite el ingreso de la siguiente información:

- **Información general**

Consta del número de configuración, asignado desde el 1 en adelante. Fecha y hora de la configuración con el formato dd/mm/aa y 00h00 respectivamente.

- **Información del dispositivo**

Se debe identificar el tipo de dispositivo, ya sea switch de core, switch de acceso, servidor o firewall. También debe constar el nombre asignado al equipo y su ubicación teniendo en cuenta la dependencia a la que pertenece y la planta donde se encuentra el rack.

- **Responsable de la configuración**

Registrar el nombre de la persona responsable de la configuración.

- **Justificación**

Se debe redactar la justificación para realizar la configuración, es decir, el porqué es importante ejecutar dicha tarea.

- **Configuración realizada**

Se menciona brevemente la configuración realizada como, por ejemplo: cambio de dirección IP, creación de Access lists, cambio de contraseña, creación de iptables, etc.

- **Observaciones**

Se detalla de manera amplia la configuración realizada y se mencionan cualquier otra información que sea importante.

La plantilla para el registro de configuraciones se encuentra en el ANEXO M.

4.3.1.2. Inventarios

Zabbix da la facilidad de realizar inventarios de los equipos, al añadir un nuevo dispositivo al sistema de gestión de red se debe ingresar toda la información conocida del dispositivo. De esta manera el dispositivo quedará registrado en el sistema como se muestra en la Figura 20 y se puede acceder a dicha información en cualquier momento.

The screenshot shows the Zabbix web interface. At the top, there is a navigation bar with the Zabbix logo and menu items: Monitoring, Inventory, Reports, Configuration, and Administration. Below this is a sub-menu with 'Overview' and 'Hosts'. The main content area is titled 'Host inventory' and has two tabs: 'Overview' and 'Details'. The 'Details' tab is active, displaying the following information:

- Type: Switch Cisco
- Type (Full details): Switch Cisco WS-C4510R+E
- Name: SW-ZEUS-PRIMARIO
- Alias: SW-ZEUS-PRIMARIO
- OS: Cisco IOS XE
- OS (Full details): C2960-LANBASEK9-M
- OS (Short): Version 12.2(50)SE4
- Contact: Administrador de red
- Location: Data Center - Edificio Central
- Chassis: 10 Slots
- Model: WS-C4510R+E
- Date HW installed: Compiled Fri 26-Mar-10 09:14

Figura 20. Inventario de equipos

Fuente: Captura Zabbix

4.3.2. Implementación de Gestión de fallos

La gestión de fallos puede ser proactiva o reactiva.

4.3.2.1. Gestión proactiva

La gestión proactiva consiste en anticiparse a un fallo antes de que suceda. Una forma de realizar gestión proactiva es a través de pruebas preventivas. Algunas herramientas que se pueden utilizar son:

- **Ping:** Comando utilizado para comprobar la conectividad punto a punto mediante el protocolo ICMP.
- **Traceroute:** Comando utilizado para comprobar la conectividad salto a salto.

- **Snmwalk:** Sirve para verificar la conexión hacia los dispositivos gestionados desde el servidor Zabbix.

4.3.2.2. *Gestión reactiva*

La gestión de fallos reactiva se realiza a través del monitoreo constante de los recursos de la red con el fin de detectar los fallos que se producen. Esta gestión cumple con un proceso de ciclo de vida de incidencias de fallo, el cual se muestra en Figura 21.

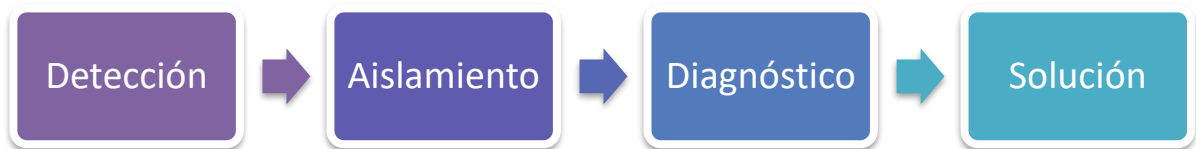


Figura 21. Ciclo de vida de incidencia de fallos

Fuente: Autora

4.3.2.2.1. *Detección de fallos*

La interfaz web del software Zabbix presenta alarmas visuales cada vez que se superen los umbrales de rendimiento definidos para los dispositivos de la red, como se muestra en la Figura 22.

Host	Trigger	Severity	Number of status changes
SW-CRATOS	Operational status was changed on interface FastEthernet0/19	Information	2
SW-ZEUS-PRIMARIO	Operational status was changed on SW-ZEUS-PRIMARIO interface GigabitEthernet8/3	Information	2
SW-ZEUS-PRIMARIO	Operational status was changed on SW-ZEUS-PRIMARIO interface GigabitEthernet8/17	Information	2
SW-ZEUS-PRIMARIO	Operational status was changed on SW-ZEUS-PRIMARIO interface GigabitEthernet8/28	Information	2
SW-ZEUS-PRIMARIO	Operational status was changed on SW-ZEUS-PRIMARIO interface GigabitEthernet10/16	Information	2
SW-ZEUS-PRIMARIO	Operational status was changed on SW-ZEUS-PRIMARIO interface GigabitEthernet10/16--Controlled	Information	2
SW-ZEUS-PRIMARIO	Operational status was changed on SW-ZEUS-PRIMARIO interface GigabitEthernet10/16--Uncontrolled	Information	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Operational Status change	Warning	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Operational Status change	Warning	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Operational Status change	Warning	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Operational Status change	Warning	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Operational Status change	Warning	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Operational Status change	Warning	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Speed Change	Warning	2
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Speed Change	Warning	2
SW-ZEUS-PRIMARIO	Operational status was changed on SW-ZEUS-PRIMARIO interface GigabitEthernet10/14--Controlled	Information	1
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO - CPU utilization too high	Average	1
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO - Spanning Tree Topology Changed	High	1
SW-ZEUS-PRIMARIO	SW-ZEUS-PRIMARIO Interface Speed Change	Warning	1

Figura 22. Alarmas visuales

Fuente: Captura de Zabbix

Adicionalmente se ha creado un mapa en la herramienta Zabbix que permite monitorizar la infraestructura de la red que se encuentra gestionada. Los íconos están enlazados a los dispositivos sujetos a monitorización, por lo que, si ocurre un problema, éste se muestra con la palabra “Problem” tal y como lo indica la Figura 23. Si el dispositivo no tiene problema alguno se visualiza la palabra “OK”. En caso de fallar un enlace, éste cambia de color verde a rojo, indicando la desconexión de los dispositivos.

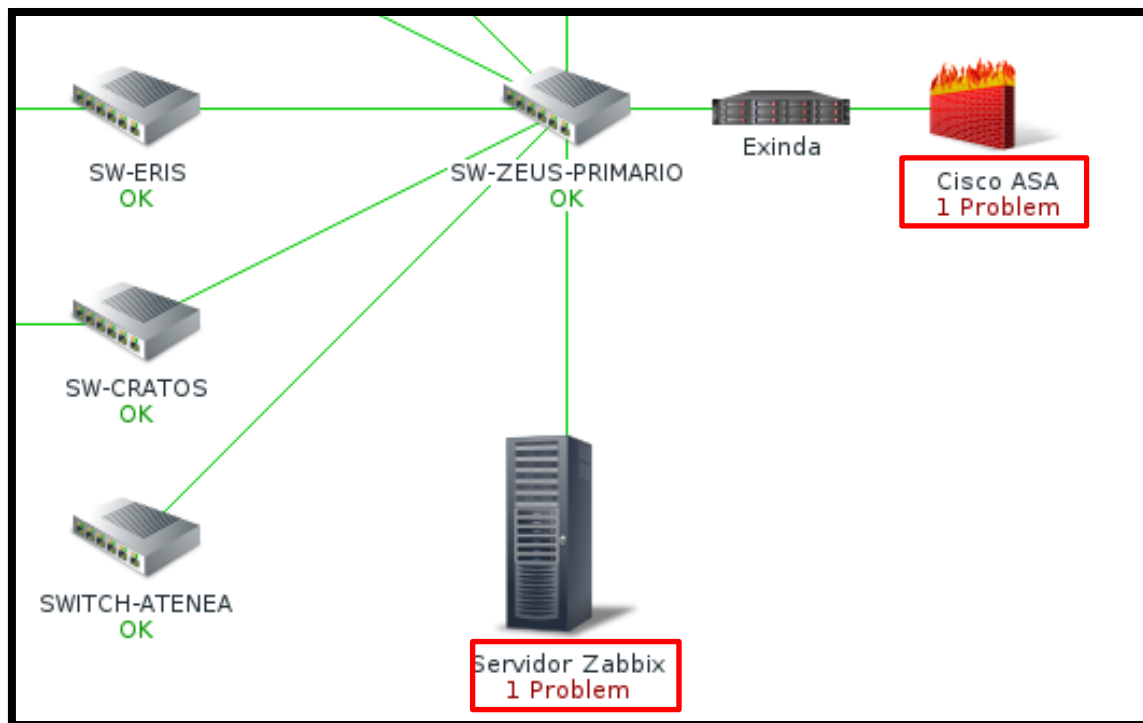


Figura 23. Mapa del sistema de gestión

Fuente: Captura de Zabbix

Alerta vía e-mail

El software Zabbix permite configurar alertas vía e-mail que se envían automáticamente cuando ocurre un evento en cualquiera de los dispositivos gestionados. Para el envío de correos se ha configurado en Zabbix una cuenta de Gmail, desde la cual se envían todas las alertas. La Figura 24 muestra la configuración del SMTP email para Zabbix.

The screenshot shows the 'Media types' configuration page in Zabbix. The 'Name' field is set to 'SMTPMail'. The 'Type' is 'Email'. The 'SMTP server' is 'smtp.gmail.com', 'SMTP server port' is '587', 'SMTP helo' is 'gmail.com', and 'SMTP email' is 'zabbixutn@gmail.com'. 'Connection security' is set to 'None', 'Authentication' is 'Normal password', and 'Username' is 'zabbixutn@gmail.com'. There is a 'Change password' button. The 'Enabled' checkbox is checked. At the bottom, there are buttons for 'Update', 'Clone', 'Delete', and 'Cancel'.

Figura 24. Configuración de alertas vía e-mail

Fuente: Captura de Zabbix

Las alertas se envían desde la cuenta zabbixutn@gmail.com hacia el correo institucional del Administrador de red. La Figura 25 muestra distintas alertas que se han enviado, el correo más reciente indica que una interfaz del SWITCH CRATOS ha cambiado su estado operacional a “down”

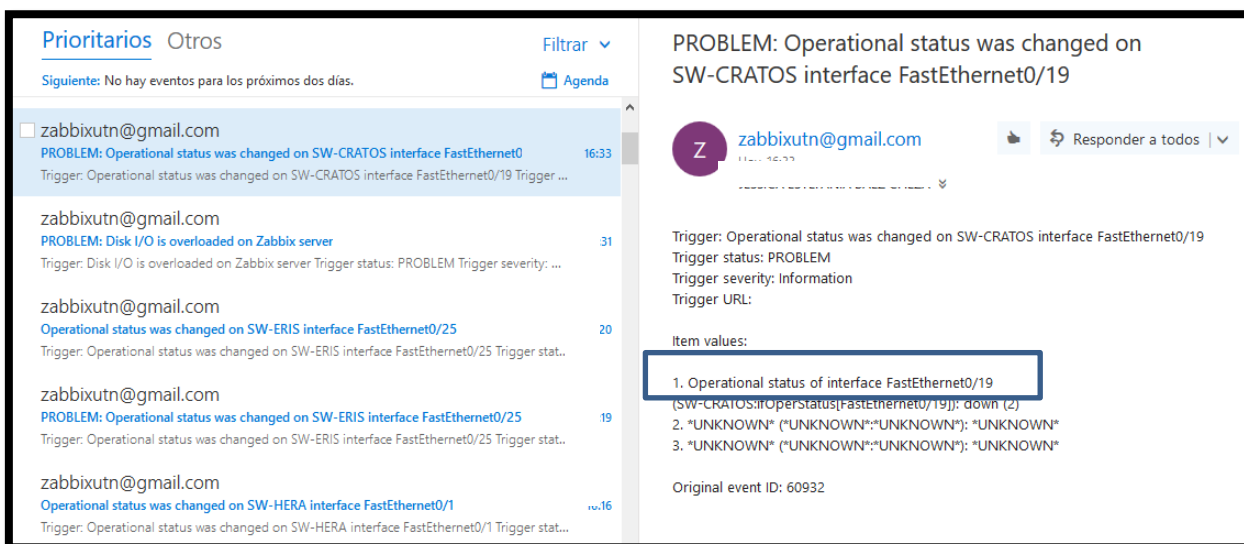


Figura 25. Alertas vía e-mail

Fuente: Captura de www.outlook.com

Registro del fallo

Cuando se notifica un fallo se propone utilizar la aplicación OTRS (Open-source Ticket Request System) como sistema de tickets. OTRS es un sistema libre que cualquier institución puede utilizar para asignar identificadores únicos llamados tickets a solicitudes de servicio o de información, de forma de facilitar el seguimiento y manejo de dichas solicitudes, así como cualquier otra interacción con sus clientes o usuarios. Se distribuye bajo la licencia GNU. La Figura 26 muestra el panel principal de la aplicación OTRS, se puede observar los tickets generados con sus respectivos detalles.

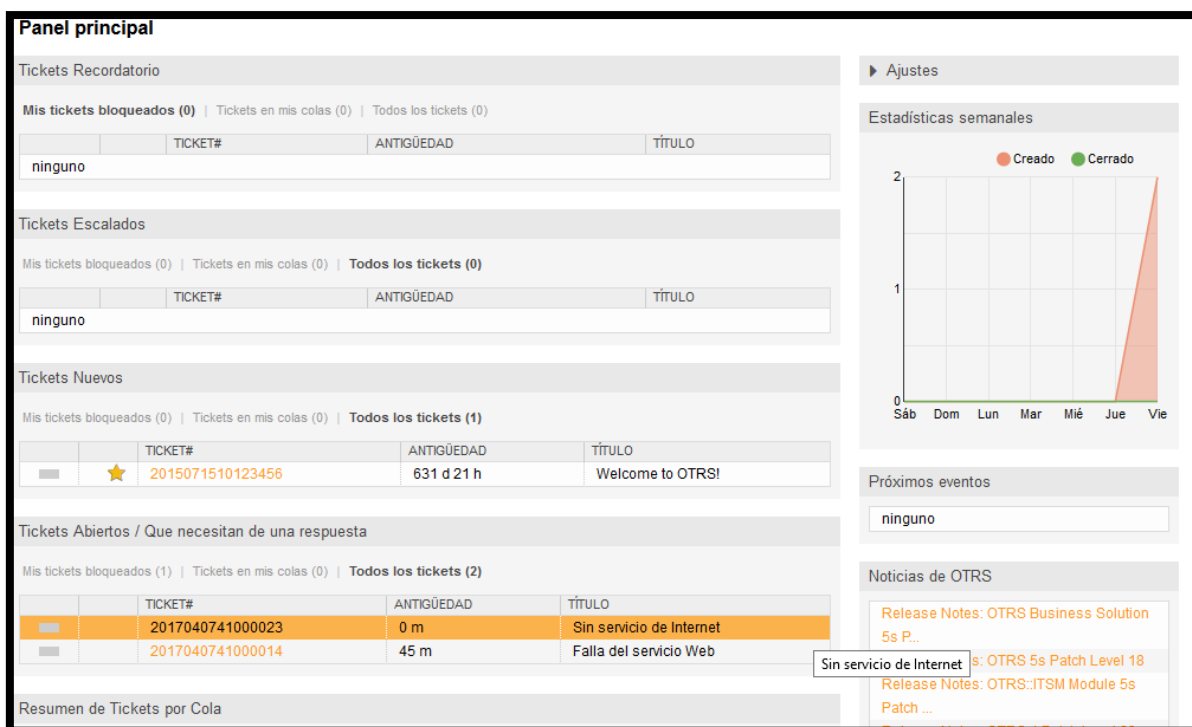


Figura 26. Dashboard de OTRS

Fuente: Captura de OTRS





Adicionalmente, la aplicación OTRS permite exportar reportes en formato csv acerca de los tickets generados, en donde se detalla toda la información de los mismos.

En el ANEXO L se detallan los pasos para la instalación y configuración de la aplicación OTRS.

4.3.2.2.2. Aislamiento y diagnóstico del fallo

Dependiendo de la gravedad del problema, se tienen diferentes grados de severidad representados por colores, los cuales se muestran en la Tabla 15. El nivel de severidad se puede asignar libremente de acuerdo al criterio del administrador de red.

Tabla 15. Clasificación de fallos en Zabbix

Nº	Severidad	Color	Descripción
2	Información		El dispositivo está funcionando
3	Aviso		Alerta del dispositivo.
4	Error		Aviso de error en el dispositivo
5	Crítico		Caída total del servicio

Fuente: Elaboración propia basada en la herramienta Zabbix

4.3.2.2.3. Solución de la falla

Cuando ya se conoce el diagnóstico de la falla que se ha suscitado en un equipo el siguiente paso es solucionarlo en el menor tiempo posible. En este paso es fundamental utilizar la plantilla de notificación de fallos que se encuentra en el ANEXO E, en donde se debe detallar tanto el problema como la solución para que en eventos futuros se siga dicho procedimiento.

4.3.3. Implementación de Gestión de prestaciones

En la gestión de prestaciones se tienen distintos reportes acerca del rendimiento de la red, mediante gráficas y estadísticas.

4.3.3.1. Monitoreo de interfaces de red

Mediante la utilización de las plantillas SNMP incluidas en el servidor Zabbix es posible descubrir las interfaces de los dispositivos de red. Se indica el estado de la interfaz, tráfico y errores.

En la sección de gráficos es posible observar tanto el tráfico entrante como el saliente de una interfaz de un switch de acceso, como se observa en la Figura 27. Este parámetro está medido en bps.

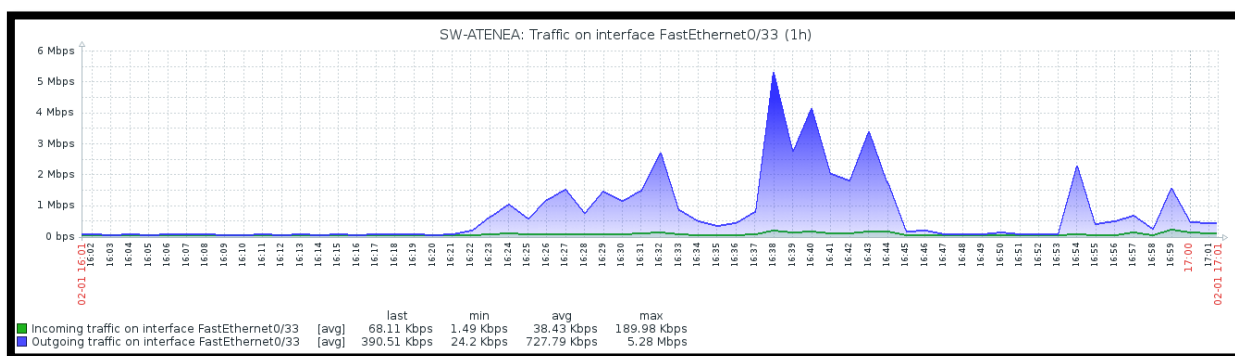


Figura 27. Tráfico entrante y saliente de interfaces del switch

Fuente: Captura de Zabbix

De manera similar se monitorea el tráfico de las interfaces del Firewall ASA 5520. La Figura 28 muestra el tráfico entrante y saliente medido en bps de la interfaz del firewall que se conecta a la DMZ. Se puede observar que el tráfico entrante, representado con el color verde, es superior a la cantidad de tráfico saliente.

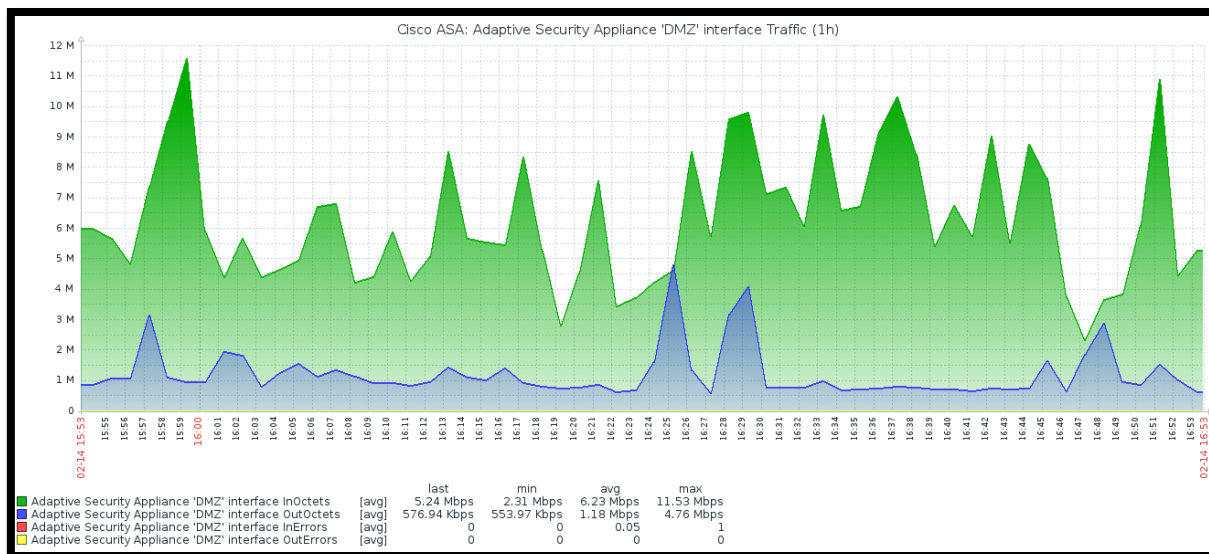


Figura 28. Tráfico entrante y salientes de interfaz "DMZ" de firewall ASA.

Fuente: Captura de Zabbix

Es fundamental monitorear también el tráfico del servidor de monitoreo, ya que esto permite conocer qué cantidad de tráfico se adiciona a la red cuando el sistema de gestión de red está en funcionamiento. En la Figura 29 se presenta el tráfico entrante y saliente durante una hora, se puede observar que la cantidad de tráfico que envía el servidor y el que recibe por parte de los dispositivos gestionados es similar la mayoría del tiempo, aunque se puede llegar a tener picos superiores a los 50Kbps.

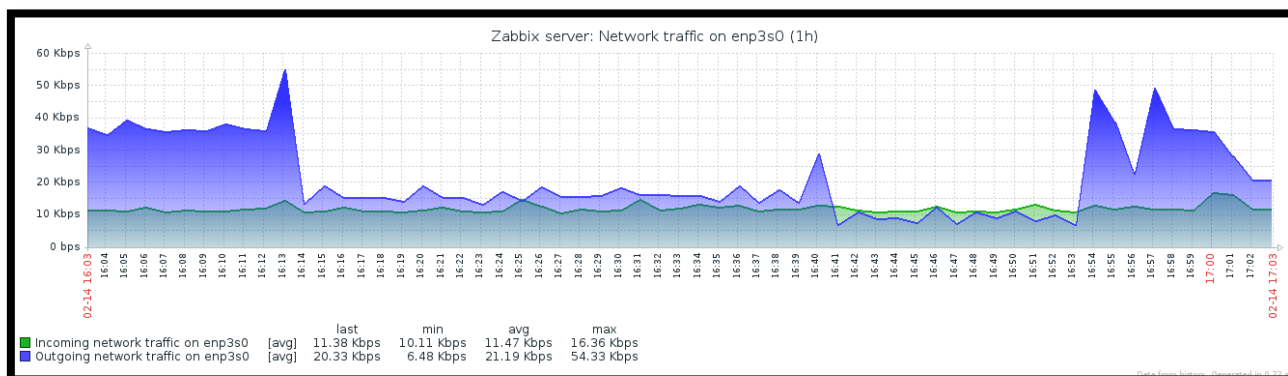


Figura 29. Tráfico en la interfaz del servidor Zabbix

Fuente: Captura de Zabbix

4.3.3.2. Disponibilidad

La herramienta Zabbix permite visualizar la disponibilidad de los dispositivos monitoreados en la red. Como se evidencia en la Figura 30, la interfaz muestra de manera porcentual la disponibilidad y los problemas de cada interfaz de los equipos de red.

Host	Name	Problems	Ok
SW-ATENEA	Incoming traffic sw atenea		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/2		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/3		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/4		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/5		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/6		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/7		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/8		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/9		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/10		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/11		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/12		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/13		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/14		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/15		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/16	0.1520%	99.8480%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/17		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/18		100.0000%
SW-ATENEA	Operational status was changed on SW-ATENEA interface FastEthernet0/19	0.7600%	99.2400%

Figura 30. Reportes de disponibilidad

Fuente: Captura de Zabbix

4.3.3.2.1. Monitoreo del Portal Web de la UTN

Zabbix tiene la opción de crear escenarios web para monitorear aplicaciones HTTP y HTTPS. Se creó un escenario para el portal web de la UTN con su respectiva dirección: <http://www.utn.edu.ec/web/uniportal/>. Este tipo de monitorización se realiza externamente sin la instalación de un agente o la activación del protocolo SNMP.

La Figura 31 muestra los ítems que se monitorean en el escenario web asignado al portal web de la institución. Los ítems con mayor relevancia corresponden al estado del servicio, velocidad

de descarga y tiempo de respuesta, de los cuales se puede obtener la última revisión, valor más reciente, cambio respecto al valor anterior y un gráfico.

Name	Last check ▼	Last value	Change	
HTTP (5 items)				
Download speed for scenario "http://www.utn.edu.ec/web/uniportal/".	2017-02-13 01:27:09	47.89 KBps	+4.69 KBps	Graph
Download speed for step "www.utn.edu.ec" of scenario "http://www.utn.edu.ec/web/uniportal/".	2017-02-13 01:27:09	47.89 KBps	+4.69 KBps	Graph
Failed step of scenario "http://www.utn.edu.ec/web/uniportal/".	2017-02-13 01:27:09	0		Graph
Response code for step "www.utn.edu.ec" of scenario "http://www.utn.edu.ec/web/uniportal/".	2017-02-13 01:27:09	200		Graph
Response time for step "www.utn.edu.ec" of scenario "http://www.utn.edu.ec/web/uniportal/".	2017-02-13 01:27:09	1s 632ms	-170ms	Graph

Figura 31. Ítems del escenario web

Fuente: Captura de Zabbix

- **Estado del servicio HTTP**

Este ítem es fundamental para conocer la disponibilidad del portal web. Si el servicio HTTP está corriendo, es decir en estado *up*, el valor del ítem será 1 como se muestra en la Figura 32. En caso de que el servicio se desactive se tendrá el valor 0.

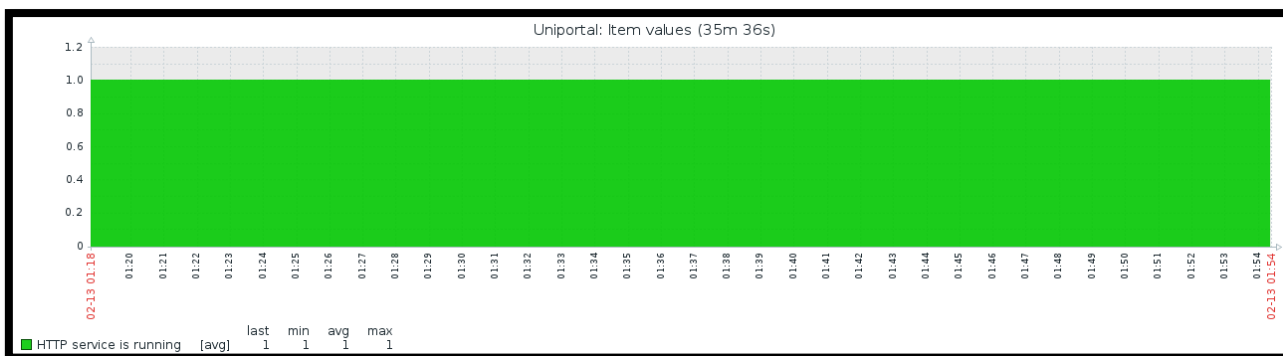


Figura 32. Estado de HTTP service

Fuente: Captura de Zabbix

- **Velocidad de descarga**

Mediante este ítem es posible conocer la velocidad de descarga del portal web en bytes por segundo y evaluar su rendimiento. En la Figura 33 se presentan las velocidades de carga obtenidas durante 25 minutos.

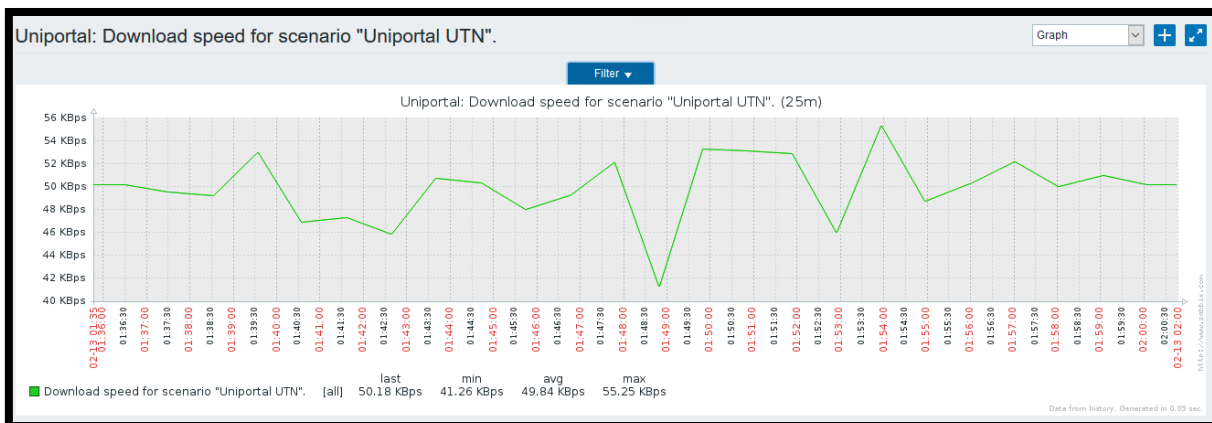


Figura 33. Velocidad de carga del portal web UTN

Fuente: Captura de Zabbix

Tiempo de respuesta

El tiempo que tarda cada página Web en cargarse se denomina *tiempo de respuesta*, el cual se cuenta desde el comienzo de la solicitud hasta que se ha transferido toda la información. De acuerdo a Hernández (2015), los periodos razonables de carga de un sitio web son:

- Carga rápida, en menos de 2 segundos.
- Carga normal, entre 2 y 4 segundos.
- Carga lenta, más de 5 segundos.

La Figura 34 presenta los tiempos de carga del portal UTN durante 26 minutos. En la gráfica se puede apreciar que el tiempo de respuesta no sobrepasa los 2 segundos, lo que significa que en ese lapso de tiempo la carga fue rápida.

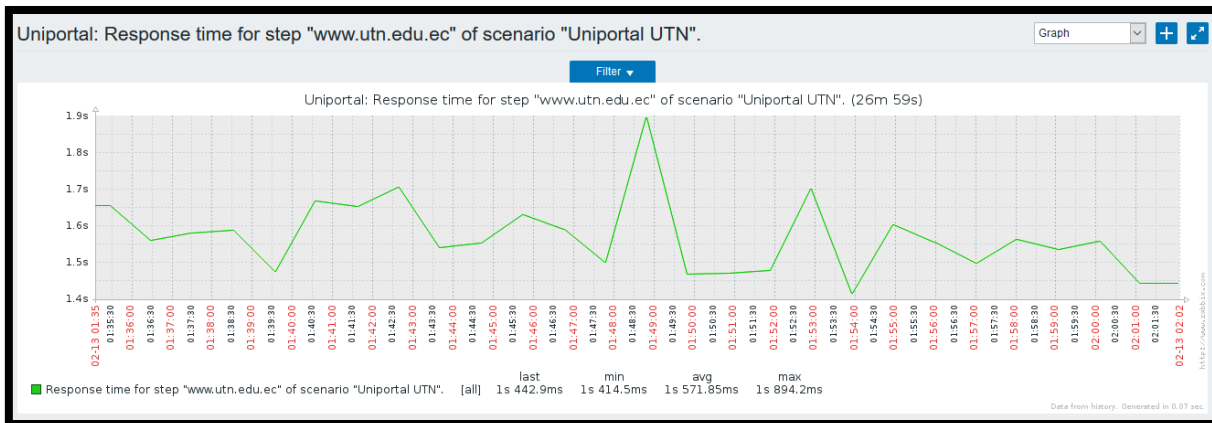


Figura 34. Tiempo de respuesta del portal web UTN

Fuente: Captura de Zabbix

Cuando no se tiene respuesta desde el sitio web, el software de monitoreo muestra un mensaje de error como se muestra en la Figura 35. En este caso también se envía una alerta vía e-mail al encargado del sitio web.

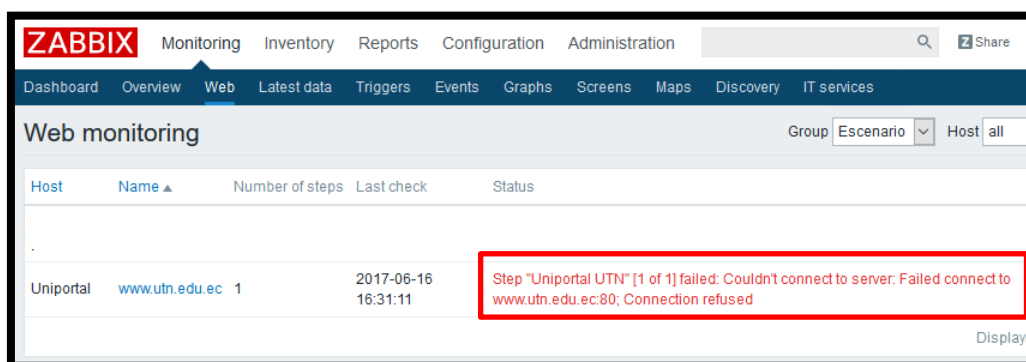


Figura 35. Fallo en la conexión hacia www.utn.edu.ec

Fuente: Captura de Zabbix

4.3.3.3. Límites de rendimiento

Se establecen los límites de rendimiento para cada tipo de dispositivo monitoreado en la red

4.3.3.3.1. Switches

Se considera que por debajo del 70% de utilización de la CPU es aceptable en un switch (Cisco, 2016). Una utilización sostenida de la CPU de más del 70% es potencialmente problemática.

Mientras que el switch puede parecer que funciona bien en este nivel de utilización de la CPU, su capacidad de reaccionar a los eventos dinámicos de la red se ve comprometida. En base a esto se define 70% como umbral de advertencia y 80% como umbral de criticidad.

En algunas implementaciones de red, una CPU con alto nivel de usabilidad es normal. En general, cuanto mayor es la red de Capa 2 o Capa 3, mayor es la demanda en la CPU para procesar tráfico relacionado con la red. Estos son ejemplos de operaciones que tienen el potencial de causar una alta utilización de la CPU:

- Spanning Tree
- Actualizaciones de la tabla de enrutamiento IP
- Comandos de Cisco IOS
- Otros eventos que causan alta utilización de CPU

En las operaciones mencionadas, la alta utilización de la CPU es normal y no causa problemas de red. La alta utilización de la CPU se convierte en un problema cuando el conmutador no funciona como se esperaba.

En cuanto al uso de memoria, de acuerdo a Cisco (2016) debe estar libre por lo menos el 20% de memoria. En base a este criterio se definen los umbrales de 70% y 80% de uso de memoria para la notificación de advertencia y criticidad respectivamente.

4.3.3.3.2. *Firewall*

Una vez que el ASA alcanza el 70% de uso de la CPU, la latencia a través del ASA aumenta lentamente. Cuando el uso de la CPU es más del 80%, el ASA comienza a soltar paquetes (Cisco, 2016). Por lo tanto, los umbrales son 70% y 80% para advertencia y criticidad respectivamente.

Para el uso de memoria se toma en cuenta el criterio expuesto para los switches, siendo un uso de 70% advertencia y 80% criticidad.

4.3.3.3.3. *Servidores*

De acuerdo a Microsoft (2005), la utilización de CPU de un servidor en horas de actividad máxima debe mantener una carga del 60%. Si la utilización de CPU sobrepasa el 75% de forma continua, se considera que el rendimiento del procesador es un cuello de botella.

Algunos de los factores por los cuales la utilización de CPU de un servidor afecta al rendimiento son:

- La velocidad de reloj del procesador, medida en megahercios (MHz) o gigahercios (GHz).
- El número de procesadores.
- El tipo de procesador.

Respecto a la utilización de memoria, cuando ésta se acerca al 100%, el servidor no aceptará aplicaciones que consuman memoria y adicionalmente se tardará más tiempo en ejecutar las aplicaciones que ya estén solicitadas por esta razón el umbral de memoria no debe sobrepasar del 70% de ser utilizada (Microsoft, 2011). En base a este criterio se definirá un umbral del 60% en modo de advertencia antes de llegar al 70%.

4.3.3.3.4. *Resumen de límites de rendimiento*

La Tabla 16 muestra un resumen de los umbrales establecidos para cada tipo de dispositivo monitoreado en la red.

Tabla 16. Límites de rendimiento

Dispositivo	Parámetro	Umbral de advertencia	Umbral de criticidad
Switches	Uso de CPU	70%	80%
	Uso Memoria	70%	80%
Firewall	Uso de CPU	70%	80%
	Uso Memoria	70%	80%
Servidor	Uso de CPU	60%	75%
	Uso Memoria	60%	70%

Fuente: Autora

4.3.4. Implementación de Gestión de contabilidad

En esta área funcional se recolecta información acerca de la utilización de la red, para que posteriormente se puedan obtener registros acerca de los recursos utilizados.

4.3.4.1. Monitoreo de uso de memoria

El uso de memoria es un recurso muy importante que se debe monitorear, ya que un excesivo consumo de memoria puede perjudicar el rendimiento del dispositivo. Zabbix permite visualizar de manera gráfica este recurso, mostrando tanto la memoria disponible como la memoria utilizada. La Figura 36 muestra el uso de memoria de un Switch Cisco, la porción verde indica la cantidad de memoria utilizada y la porción roja muestra la cantidad de memoria disponible medida en Mb.

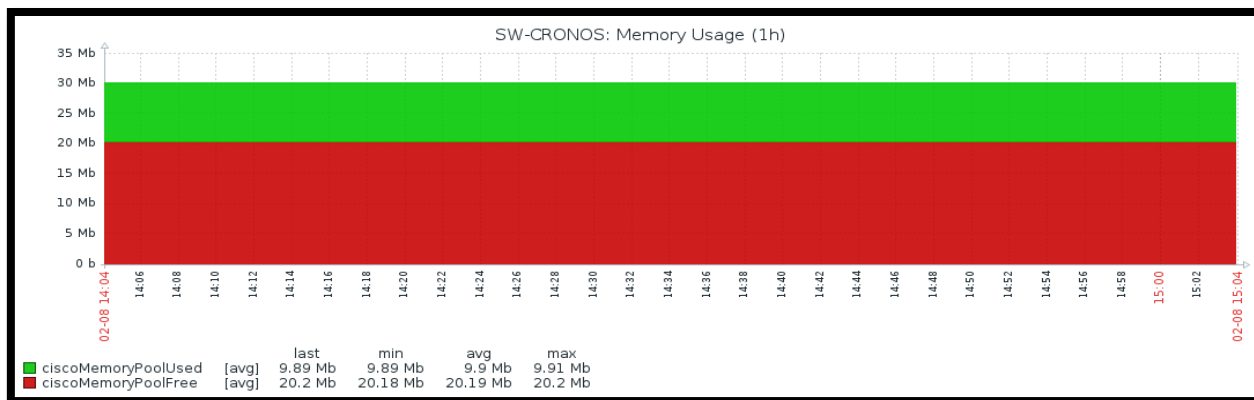


Figura 36. Monitoreo del uso de memoria de un switch

Fuente: Captura de Zabbix

4.3.4.2. Monitoreo de uso de CPU

Zabbix muestra de manera gráfica el porcentaje de CPU que está utilizando el dispositivo en tiempo real. La Figura 37 muestra el monitoreo del uso de CPU de un dispositivo, se puede observar que el consumo es prácticamente bajo por lo que no se genera ningún tipo de alerta.

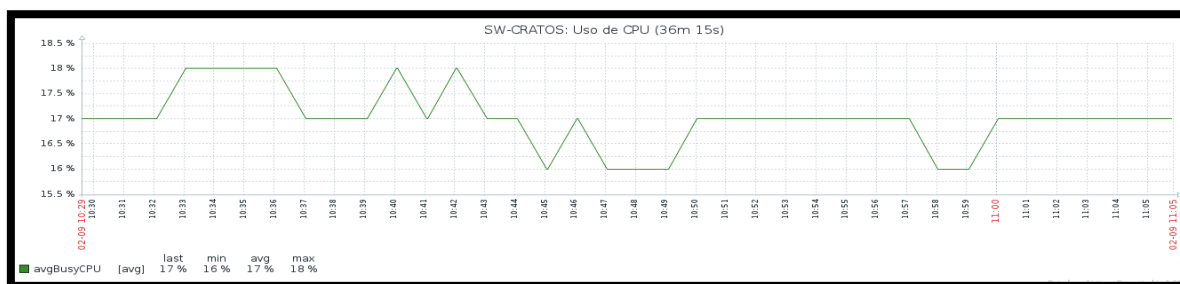


Figura 37. Monitoreo del uso de CPU

Fuente: Captura de Zabbix

4.3.4.3. Monitoreo del espacio de disco

- **Espacio de disco total**

El espacio de disco utilizado y disponible se monitorea en los servidores DHCP y Web. La Figura 38 presenta el uso de disco en el servidor DHCP medido en GB, también se muestra de manera porcentual indicando que el 88% del disco está libre

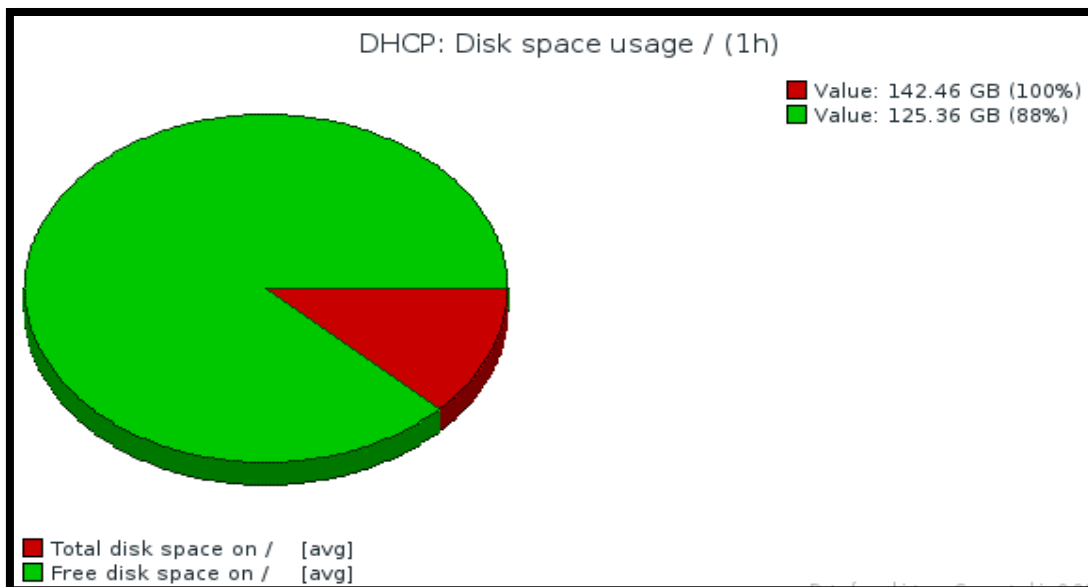


Figura 38. Utilización de disco en el servidor DHCP

Fuente: Captura de Zabbix

- **Espacio de disco en la partición /boot**

De acuerdo a la información obtenida por Zabbix, en el servidor DHCP se tiene una partición /boot, la Figura 39 muestra la utilización de disco de dicha partición.

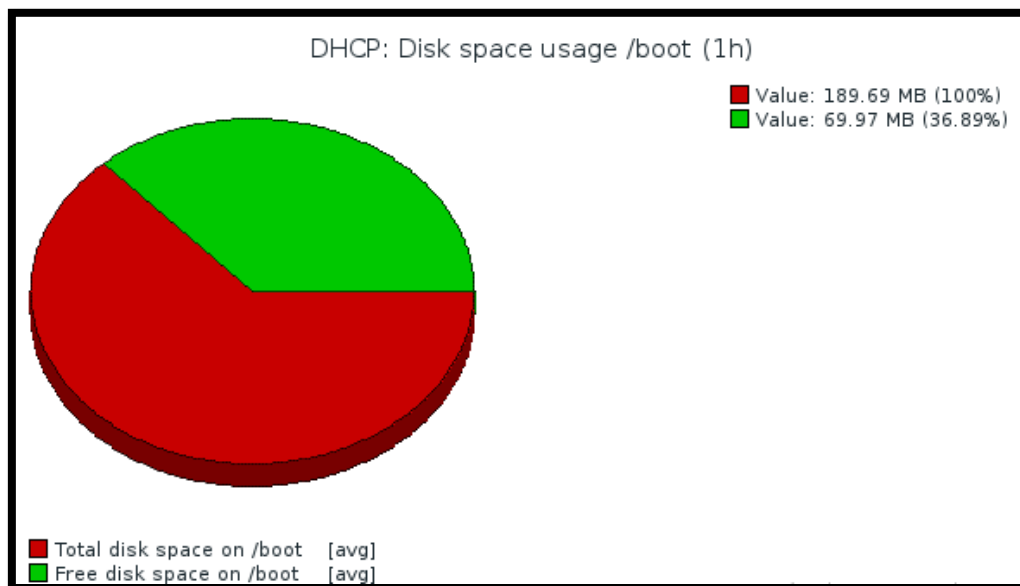


Figura 39. Utilización de disco en la partición /boot del servidor DHCP

Fuente: Captura de Zabbix

- **Espacio de disco en la partición /home**

Dentro del servidor DHCP se tiene una partición de disco /home. La utilización de disco de esta partición se muestra en la Figura 40. Se puede observar que el 94% de la partición está libre.

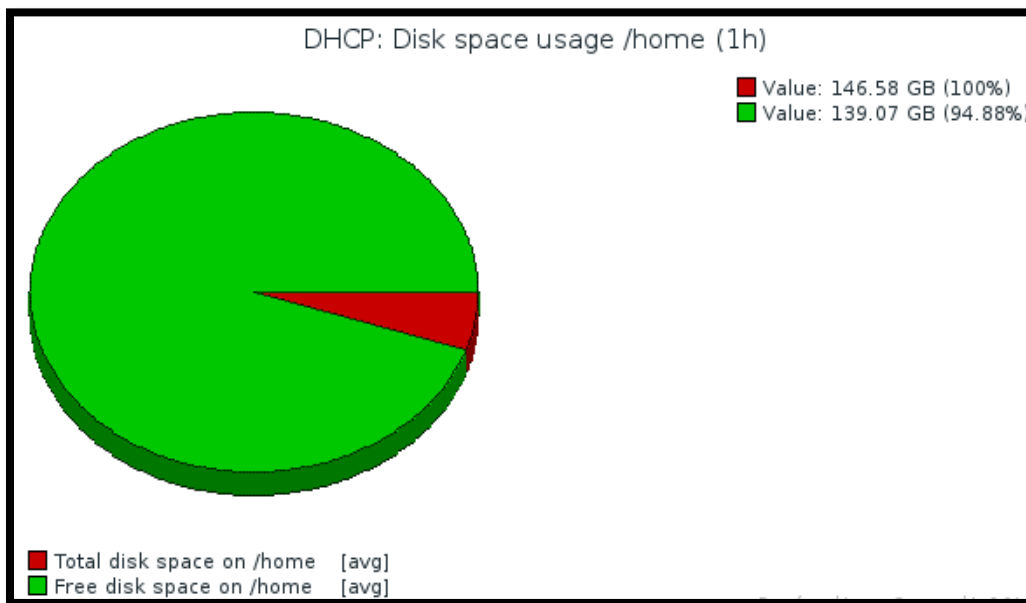


Figura 40. Utilización de disco de la partición /home del servidor DHCP

Fuente: Captura de Zabbix

4.3.5. Implementación de Gestión de seguridad

La gestión de seguridad es la encargada de manejar el acceso al sistema de gestión de red y a los dispositivos gestionados.

4.3.5.1. Acceso al servidor de gestión

El acceso a la interfaz frontend de Zabbix se hace mediante una PC conectada a la red local, ingresando en el navegador la dirección IP del servidor seguida de “/zabbix”.

El primer paso para dar seguridad al frontend del sistema de gestión de red es cambiar la contraseña por defecto del usuario Admin, ya que ésta será la cuenta para el Administrador de la red de la UTN. La Figura 41 muestra los usuarios que aparecen por defecto en el servidor Zabbix

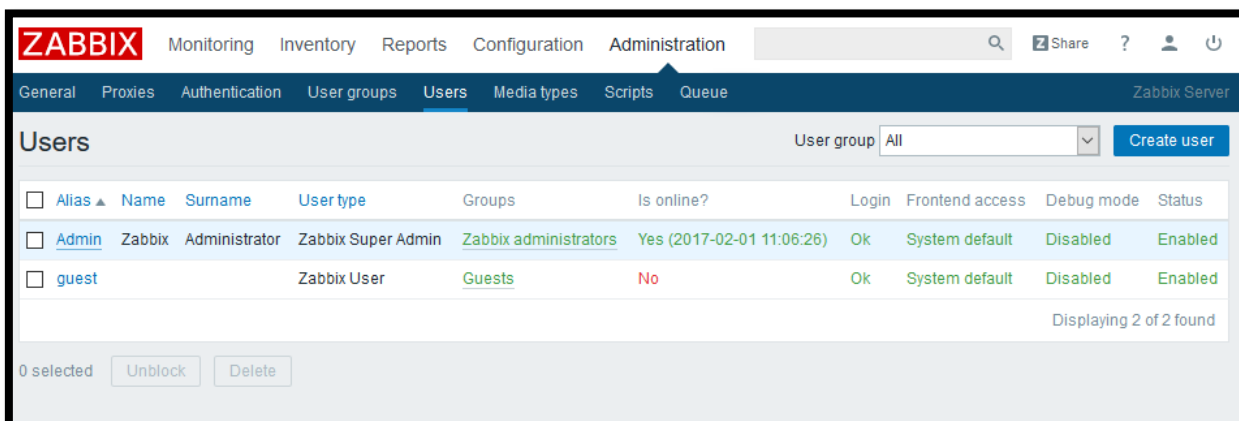


Figura 41. Usuarios de Zabbix

Fuente: Captura de Zabbix

Como se muestra en la Figura 42, es posible realizar el cambio de contraseña del usuario Admin ya que por defecto esta es “zabbix”.

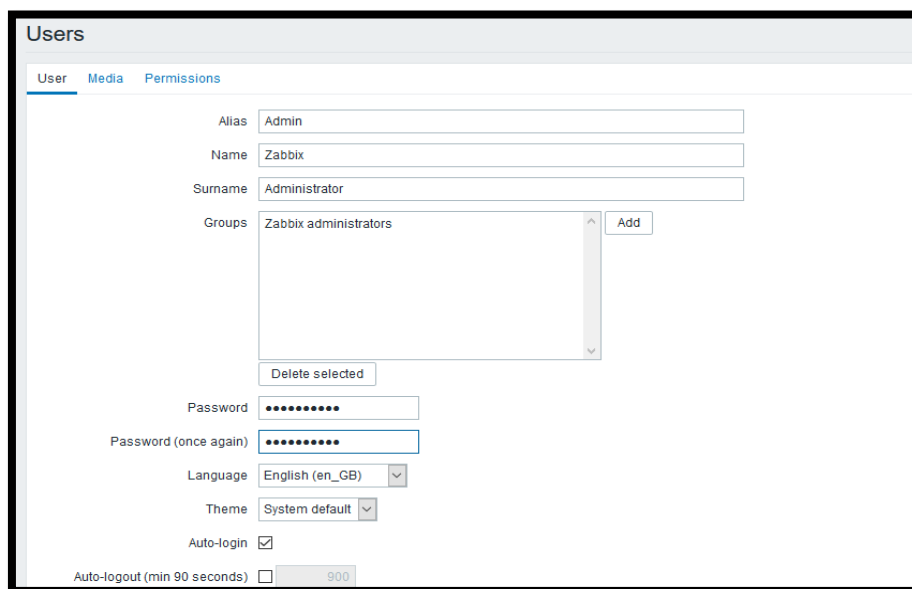


Figura 42. Configuración de la cuenta de usuario Admin

Fuente: Captura de Zabbix

El usuario Admin tiene todos los permisos de lectura y escritura sobre los hosts como se evidencia en la Figura 43. Estos permisos no pueden ser cambiados para el usuario Admin, pero para el resto de usuarios sí.

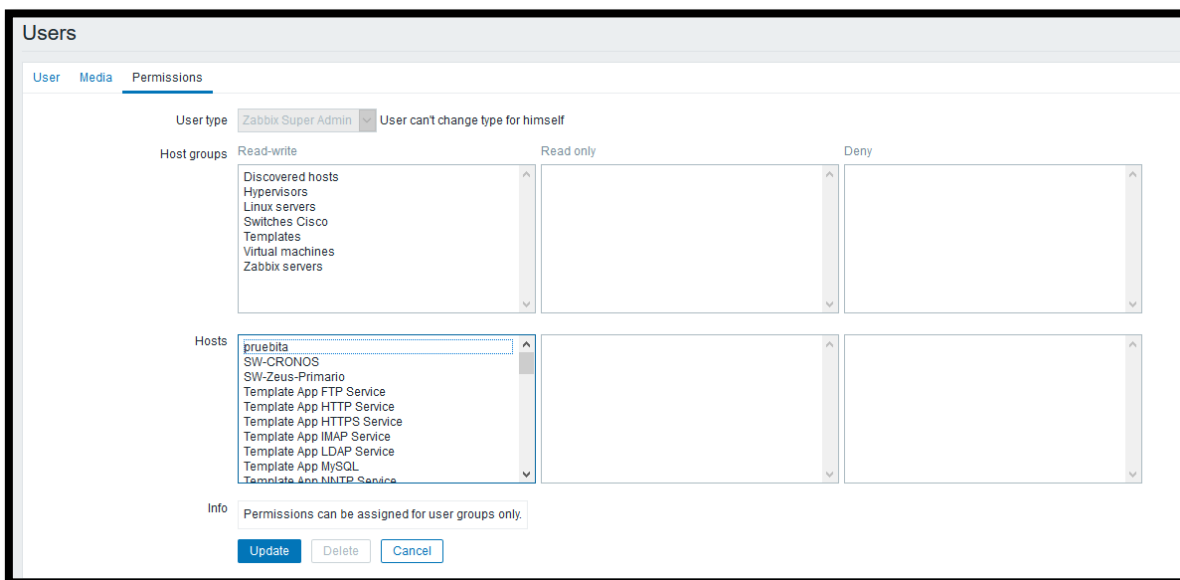


Figura 43. Permisos de usuario

Fuente: Captura de Zabbix

Únicamente el usuario Admin podrá crear nuevos usuarios para accedan al sistema de gestión con determinados permisos. La creación de usuarios se detalla en el Manual de Administrador (ANEXO K).

En la sección Reportes, los usuarios pueden ver los registros de los cambios realizados en el frontend.

En la Figura 44 se puede ver el registro de auditoría de varios cambios realizados en el frontend. Se puede usar el filtro, situado debajo de la barra de registro de auditoría, para restringir los registros por usuario, tipo de actividad, recurso afectado y el período de tiempo.

Time	User	IP	Resource	Action	ID	Description	Details
2017-06-19 15:10:59	Admin	172.	Web scenario	Updated	0		Web scenario [www.utn.edu.ec] [1] Host [Uniportal]
2017-06-19 15:10:12	Admin	172.	Web scenario	Updated	0		Web scenario [Nube] [2] Host [Cloud portal]
2017-06-16 16:50:33	Admin	172.	Screen	Updated	25	www.utn.edu.ec	Cell changed screen itemid "91" resource type "1"
2017-06-16 16:49:58	Admin	172.	Screen	Updated	25	www.utn.edu.ec	Cell changed screen itemid "90" resource type "1"
2017-06-16 16:48:24	Admin	172.	Screen	Updated	25	www.utn.edu.ec	Cell changed screen itemid "90" resource type "1"
2017-06-16 15:09:06	Admin	172.	Host	Added	10142	Wireless Lan Controller	
2017-06-16 15:09:05	Admin	172.	Trigger	Added	24467	Utilización de CPU superior a 70%	
2017-06-16 15:09:05	Admin	172.	Trigger	Added	24468	Utilización de CPU superior a 80%	

Figura 44. Registro de auditoría

Fuente: Captura de Zabbix

El acceso al backend del servidor Zabbix se realiza mediante ssh, generalmente usando la aplicación Putty. Es necesario poner una contraseña segura en el usuario root de CentOS, ya que allí se encuentran las configuraciones del servidor.

4.3.5.2. Dispositivos gestionados

Para la seguridad en los dispositivos gestionados se propone utilizar la herramienta Nessus, que es una plataforma de análisis de vulnerabilidades. Particularmente la versión Nessus home es una distribución sin costo que permite escanear una red a través de la utilización de distintas plantillas, las cuales pueden verse en la Figura 45, únicamente las plantillas etiquetadas con el texto *UPDATE* no están disponibles en la versión libre.

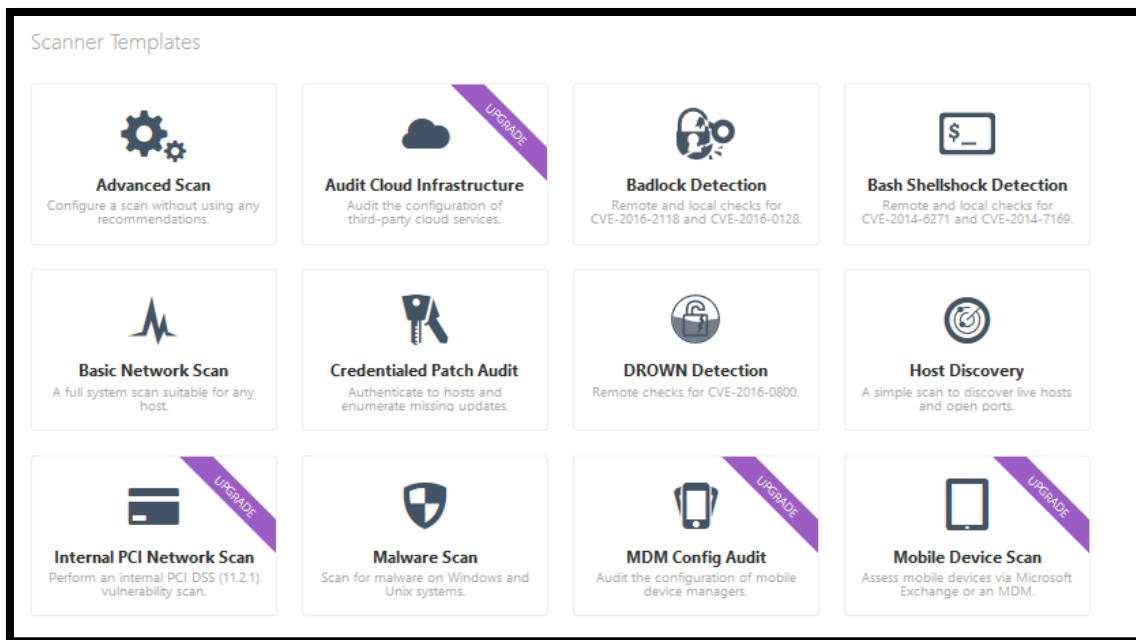


Figura 45. Plantillas Nessus

Fuente: Captura de Nessus

Para realizar un escaneo es necesario seleccionar una de las plantillas y configurar ciertos parámetros como el rango de direcciones IP que se quiere escanear. El escaneo puede programarse o ejecutarse manualmente. La Figura 46 muestra un escaneo básico de la red, las vulnerabilidades encontradas están representadas por los colores que se ven en la imagen.



Figura 46. Escaneo básico de la red

Fuente: Captura de Nessus

Dentro de cada vulnerabilidad encontrada, Nessus presenta una descripción detallada de la misma junto con una solución. En el caso del escaneo de la *Figura 47*, se tiene el reporte de los puertos abiertos en un switch de acceso siendo éstos: 22, 80 y 443.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

Port 22/tcp was found to be open

Port	Hosts
22 / tcp / ssh	172.

Port 80/tcp was found to be open

Port	Hosts
80 / tcp / www	172.

Port 443/tcp was found to be open

Port	Hosts
443 / tcp / www	172.

Figura 47. Detalles de la vulnerabilidad en Nessus

Fuente: Captura de Nessus

4.4. Análisis Costo-Beneficio

En esta sección se realizó un análisis costo-beneficio con el fin de conocer los gastos y beneficios que se obtiene por la realización de este proyecto. Se analizaron tanto los costos de hardware como de software.

4.4.1. Software

El costo de software se determina tomando en cuenta las tres herramientas implementadas, con Zabbix como el software principal de gestión de red y OTRS y Nessus como software

complementario para la gestión de fallos y gestión de seguridad respectivamente. Adicionalmente se toma en cuenta el costo de implementación del software, para esto se ha tomado como referencia la capacitación en software libre, la cual tiene un costo de \$300 de acuerdo a la empresa ecuatoriana de capacitación Saslibre (2017). La Tabla 17 muestra el total de costos de software.

Tabla 17. Costos de Software

Software	Costo
Licencia Zabbix	0,00
Licencia OTRS	0,00
Licencia Nessus	0,00
Capacitación en Software libre	300,00
Total	300,00

Fuente: Autora

4.4.2. Hardware

El costo de hardware se obtiene tomando en cuenta el servidor elegido en el apartado 3.7.2, cuyo valor es de \$862,31.

4.4.3. Presupuesto total

Se determina el presupuesto total que corresponde a los costos de implementación de este proyecto, teniendo en cuenta los costos totales de hardware y de software detallados en los apartados anteriores, esto se muestra en la Tabla 18.

Tabla 18. Presupuesto total

Descripción	Presupuesto
Costos de Software	\$300,00

Costos de Hardware	\$862,31
Total	\$1162,31

Fuente: Autora

4.4.4. Beneficios

La encuesta que se muestra en el ANEXO B, se realizó antes y después de la implementación del sistema de gestión de red para verificar la obtención de beneficios tras la implementación del proyecto. Los resultados de ambas encuestas fueron comparados obteniendo lo siguiente:

El 47% de usuarios expresaba que la solución a problemas se realizaba entre 1 hora y un día, dicha cifra se redujo en 15%, denotando que los problemas se resuelven en lapsos de entre 10 a 30 minutos.

El 39% de los usuarios manifestaba que ocurrían fallos más de una vez al día, este número se redujo en un 12%, indicando que los problemas ocurren con menor frecuencia.

La valoración del servicio de Internet como “Muy bueno” se incrementó de 8% a 17%, Lo cual indica la mejora del servicio.

La valoración de la labor de la DDTI como “Muy satisfactoria” se incrementó de 9% a 19%. Indicando cierta mejora en la satisfacción del usuario.

La implementación de este proyecto presenta múltiples beneficios para el administrador de red, usuarios y para la infraestructura de red.

Beneficios para el administrador:

- Puede detectar fallos en la red con mayor prontitud.
- Puede llevar un inventario de equipos de manera más fácil.

- Puede obtener reportes acerca del rendimiento de la red para realizar pronósticos y planificar futuras configuraciones.
- Mejora la disponibilidad del sistema.

Beneficios para el usuario:

- Tienen una red más estable con mayor disponibilidad.
- Se solucionan los problemas en menor tiempo, por lo que aumenta su tiempo de productividad.

Beneficios para la infraestructura de red:

- Se tiene una infraestructura con recursos más eficientes.
- Se puede dimensionar mejor la capacidad de procesamiento de los equipos de red.

La implementación de este proyecto con herramientas de distribución libre representa un considerable beneficio para la red de datos del Edificio Central de la UTN, para el personal encargado de la administración de dicha red y para los usuarios, quienes obtienen una red constantemente monitoreada. El mayor beneficio es para el personal técnico encargado de la administración de la red de datos de la UTN pues se les permite agilizar la detección y solución de fallos, reduciendo el uso de los recursos.

CONCLUSIONES

La gestión de red en la red de datos del Edificio Central de la Universidad Técnica del Norte es fundamental, ya que permite al administrador de la red supervisar el rendimiento de la misma, de manera que se detecte con prontitud los problemas que se presentan y puedan ser resueltos a tiempo.

El análisis de la información referente a la gestión de red y en especial al modelo de gestión ISO/OSI es útil para conocer los criterios que deben tomarse en cuenta para la implementación del modelo basado en las cinco áreas funcionales: Gestión de configuraciones, gestión de fallos, gestión de rendimiento, gestión de contabilidad y gestión de seguridad.

A través del levantamiento de información de la red de datos interna del Edificio Central de la Universidad Técnica del Norte, es posible conocer los requerimientos relacionados con la administración y gestión de red, como autodescubrimiento de la red, generación de alertas, generación de reportes y visualización gráfica, entre otros. Dichos requerimientos se toman en cuenta para la implementación del modelo.

Las políticas de gestión de red y manuales de procedimientos para cada una de las áreas funcionales del modelo ISO/OSI constituyen una guía para una gestión de red organizada.

El análisis costo-beneficio evidencia la factibilidad del proyecto, se destaca el gasto ahorrado al utilizar herramientas de distribución libre y los beneficios que genera este proyecto tanto para el administrador de red como para los usuarios.

Se comprobó el funcionamiento del sistema de gestión de red en todas las áreas funcionales comprendidas en el modelo ISO/OSI, con lo cual se determinó que la implementación del proyecto

se desempeña correctamente, permitiendo tener una red continuamente monitoreada, en la que además se presentan alarmas ante diferentes eventualidades.

RECOMENDACIONES

Al momento de adquirir un nuevo dispositivo de red, es aconsejable asegurarse que el equipo tenga soporte SNMP en por lo menos la versión 2, para que éste pueda ser integrado al sistema de gestión de red y por lo tanto esté sujeto a la monitorización constante de sus recursos.

Asignar los recursos necesarios de memoria en el servidor Zabbix, para que el sistema de gestión de red mantenga un nivel de rendimiento adecuado a pesar de que se adicionen nuevos dispositivos.

El encargado de la monitorización de red debe revisar de manera constante los fallos que puedan producirse y no ignorar las alertas generadas por el software de gestión, para que los problemas no avancen a niveles críticos.

Es necesario utilizar las plantillas propuestas tanto para la notificación de fallos como para el control de configuraciones para obtener registros acerca de estas actividades que puedan ayudar a identificar y solucionar problemas futuros.

Implementar herramientas complementarias al software de gestión, que permitan cubrir de manera más amplia determinadas áreas funcionales del modelo de gestión de red ISO/OSI, en caso de que el software principal no lo haga.

El presente modelo de gestión no debe quedar como una propuesta, se recomienda al personal encargado de la administración de red utilizar el software implementado, así como acatarse a las políticas y manual de procedimientos que se detallan en este proyecto.

Se sugiere al personal encargado de la administración y gestión de red capacitarse en nuevas herramientas que se presenten a futuro, para que se actualice el sistema implementado aprovechando los beneficios del desarrollo tecnológico.

Se recomienda a futuro, volver a analizar las políticas y manual de procedimientos con el fin de realizar cambios que contribuyan a la mejora y actualización del sistema de gestión de red propuesto inicialmente.

Verificar de manera continua que el nodo de gestión esté disponible, en caso de que se presente un evento fortuito que pueda interrumpir su funcionamiento, como por ejemplo, una interrupción de energía eléctrica.

GLOSARIO

C

Cisco: Empresa dedicada a la fabricación, mantenimiento, comercialización y consultoría de equipos de telecomunicaciones.

CMIP: *Common Management Information Protocol* es el Protocolo de administración de red basado en el modelo OSI y definido por las recomendaciones la ITU-T.

I

ICMP: Internet Control Message Protocol es el protocolo de control y notificación de errores de Internet.

IP: Internet Protocol, protocolo para la comunicación de datos digitales, cuya funcionalidad se ubica en la capa de red del modelo OSI.

ISO: Es la Organización Internacional para la Estandarización, encarga de regular normas para la fabricación, comercio y comunicación en los sectores industriales.

ITU: Unión Internacional de Telecomunicaciones es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), su labor es la de regular las telecomunicaciones entre las distintas administraciones y empresas operadoras a nivel internacional.

ITU-T: Es uno de los tres sectores de la ITU; que coordina las normas de telecomunicaciones.

M

MIB: Management Information Base o en español Base de datos local de información de gestión

N

NMA: Network Management Application es el software que se instala en el NMS.

NMS: Network Management Station es la estación encargada de la monitorización en un sistema de gestión.

O

OID: Object Identifier es una cadena de tamaño variable de números.

OSI: Open system interconnection es un modelo de referencia para los protocolos de la red de arquitectura en capas.

P

PDU: Unidad de datos de protocolo, usado para el intercambio de datos entre las mismas capas de dos computadores.

Polling: Consulta constante hacia un dispositivo sin el uso de interrupciones.

R

RAM: Random Access Memory

RFC: Request for Comment, son una serie de publicaciones que contienen notas técnicas y organizativas sobre Internet. Abarcan varios aspectos de la creación de redes de computadoras, como protocolos, procedimientos, programas y conceptos.

RMON: Estándar utilizado para la monitorización remota de redes.

S

SNMP: Simple Network Management Protocol. es un protocolo de la capa de aplicación perteneciente a la familia de protocolos TCP/IP que facilita el intercambio de información de administración entre dispositivos de red.

SRS: Especificación de Requisitos Software.

T

TCP/IP: Transmission Control Protocol/Internet Protocol es un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

U

UDP: *User Datagram Protocol* es un protocolo de la capa de transporte no orientado a conexión basado en el intercambio de datagramas.

BIBLIOGRAFÍA

Alarcón, R. (2007). Gestión y administración de redes como eje temático de investigación.

Avances Investigación en Ingeniería(7), 104-113.

Alkaid. (2015). *Alkaid*. Recuperado el 20 de Enero de 2017, de <https://alkaid.cr/productos/zabbix>

Barba Martí, A. (1999). *Gestión de red* (1 ed.). Edicions UPC.

Barba, A., & Guerrero, J. A. (Junio de 2008). Arquitectura de referencia de gestión de red basada en políticas para un entorno integrado 3G-WLAN. *IEEE LATIN AMERICA TRANSACTIONS*, 6(2), 230-232.

Cacti. (2015). *Cacti*. Recuperado el 23 de Noviembre de 2016, de <http://www.cacti.net/>

Case, J., Fedor, M., Schoffstall, M., & Davin, J. (Mayo de 1990). RFC 1157. *A Simple Network Management Protocol (SNMP)*. Obtenido de <https://www.rfc-editor.org/rfc/rfc1157.txt>

Cisco. (29 de Junio de 2007). Recuperado el 4 de Octubre de 2016, de http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/pgw/7/mibs/guide/7MIB_Ch1.htm
1

Cisco. (Agosto de 2014). *Cisco*. Recuperado el 23 de Octubre de 2016, de http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/ciscoworks-lan-management-solution-4-0/data_sheet_c78-610760.html

Cisco. (16 de Marzo de 2016). *Cisco*. Obtenido de http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/cpu_util.html

Cisco. (13 de Junio de 2016). *Cisco*. Obtenido de <http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113185-asaperformance.html#anc7>

CISCO. (17 de Octubre de 2016). *CISCO*. Recuperado el 1 de Noviembre de 2016, de http://www.cisco.com/cisco/web/support/LA/102/1025/1025374_ext_ping_trace.html

Diez de Castro, E. P., García del Junco, J., Martín Jiménez, F., & Periañez Cristóbal, R. (2000). *Administración y dirección*. Madrid: McGraw-Hill.

ebay. (s.f.). *ebay*. Obtenido de <http://www.ebay.com/bhp/ibm-tower-server>

García Yague, A. (Agosto de 1998). *Gestión SNMP*. Recuperado el 23 de Octubre de 2016, de OLICOM The Network Company: <http://www.ccapitalia.net/descarga/docs/1998-gestion-snmp-v1.pdf>

Garzón Villar, L., Leyva Cortés, E., Prieto Tinoco, J., & Sampalo de la Torre, M. (2007). *Cuerpo de Profesores de Enseñanza Secundaria. Informática. Temario*. (Vol. IV). Mad S.L.

Hernández, A. (29 de Septiembre de 2015). *Marketing Digital*. Obtenido de <http://alfredohernandezdiaz.com/2015/09/29/como-medir-optimizar-velocidad-pagina-web/>

Hewlett Packard Enterprise. (s.f.). *Hewlett Packard Enterprise*. Recuperado el 20 de Octubre de 2016, de <https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=PERFMINFO>

Huidrobo, J. (2005). *Sistemas Telemáticos*. Paraninfo.

IBM. (2014). *IBM Knowledge Center*. Recuperado el 5 de Octubre de 2016, de http://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.13/gtpc1/pdus.html

Microsoft. (25 de Octubre de 2005). *Microsoft*. Obtenido de [https://technet.microsoft.com/es-es/library/bb124583\(v=exchg.65\).aspx](https://technet.microsoft.com/es-es/library/bb124583(v=exchg.65).aspx)

Millán , R. (2004). *Ramon Millán*. Recuperado el 5 de Octubre de 2016, de <http://www.ramonmillan.com/tutoriales/snmpv3.php>

Millán Tejedor, R. (1999). *CONSULTORÍA ESTRATÉGICA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES*. Recuperado el 4 de Octubre de 2016, de <http://www.ramonmillan.com/tutoriales/gestionred.php>

Millán Tejedor, R. J. (Mayo de 2004). Tendencias en gestión de red. *Comunicaciones World*, 54-56.

Nagios. (2 de Septiembre de 2012). *Nagios*. Recuperado el 20 de Octubre de 2016, de <http://www.nagios-cl.org/que-es-nagios>

Ochoa, C. (11 de Noviembre de 2013). *Netquest*. Obtenido de www.netquest.com

Oracle. (28 de Septiembre de 2007). Recuperado el 23 de Octubre de 2016, de https://docs.oracle.com/cd/E13203_01/tuxedo/tux100/snmpmref/1tmib.html

Paessler. (2014). *Paessler*. Recuperado el 23 de Octubre de 2016, de The Network Monitoring Company:

https://www.es.paessler.com/prtg?utm_source=google&utm_medium=cpc&utm_campaign=ROW_ES_Search-

[Brand_exact_1&utm_adgroup=prtg&utm_adnum=98646590790&utm_keyword=prtg&utm_term=prtg](https://www.es.paessler.com/prtg?utm_source=google&utm_medium=cpc&utm_campaign=ROW_ES_Search-Brand_exact_1&utm_adgroup=prtg&utm_adnum=98646590790&utm_keyword=prtg&utm_term=prtg)

tm_device=c&utm_position=1t1&utm_campaignid=412618590&utm_adgroupid=28411
503030&utm_targeti

Paessler. (2016). *Paessler*. Obtenido de <https://www.paessler.com/partners/prtg-training>

PandoraFMS. (23 de Octubre de 2016). *Pandora FMS*. Recuperado el 6 de Octubre de 2016, de www.pandorafms.com

Ques10. (Diciembre de 2014). *Ques10*. Recuperado el 28 de Octubre de 2016, de <http://www.ques10.com/p/3301/compare-between-snmp-v1-snmp-v2-and-snmp-v3/>

SecuriTeam. (6 de Septiembre de 2001). *SecuriTeam*. Recuperado el 28 de Octubre de 2016, de <http://www.securiteam.com/tools/5RP062K5HM.html>

SNMP Research International, Inc. (2003). *SNMP Research International, Inc.* Obtenido de Secure your network: <http://www.snmp.com/>

SolarWinds. (2013). A Guide to understanding SNMP. *SOLARWINDS TECH TIPS*, 5-6. Recuperado el 8 de Noviembre de 2016, de http://web.swcdn.net/creative/pdf/techtips/A_Guide_to_Understanding_SNMP.pdf

Stallings, W. (2004). *FUNDAMENTOS DE SEGURIDAD EN REDES* (2 ed.). Madrid: PEARSON EDUCACIÓN.

TechTarget. (Enero de 2006). *TechTarget*. Recuperado el 23 de Octubre de 2016, de <http://searchitoperations.techtarget.com/definition/HP-OpenView>

Tenable Network Security. (2016). *Tenable Network Security*. Recuperado el 8 de Noviembre de 2016, de <https://www.tenable.com/products/nessus/select-your-operating-system>

TripWire. (Marzo de 2016). *TripWire*. Recuperado el 18 de Noviembre de 2016, de <http://www.tripwire.com/>

UTN. (s.f.). *UTN Uniportal*. Recuperado el 21 de Diciembre de 2016, de http://www.utn.edu.ec/web/uniportal/?page_id=2008

Varela, C. (2003). Gestión integrada de telecomunicaciones y el modelo TMN de la ITU. *Revista de Tecnología*, 2(1), 20-24. Obtenido de http://www.uelbosque.edu.co/sites/default/files/publicaciones/revistas/revista_tecnologia/volumen2_numero1/gestion_integrada_telecomunicaciones2-1.pdf

Villamayor, C., & Lamas, E. (1998). *Gestión de la radio comunitaria y ciudadana*. Quito.

Wireshark. (2015). *Wireshark*. Recuperado el 18 de Noviembre de 2016, de <http://wireshark.com/wireshark-reviews-downloads.html>

Zabbix. (2016). *Zabbix*. Recuperado el 23 de Noviembre de 2016, de The Enterprise-class Monitoring Solution for Everyone: <http://www.zabbix.com/product>

ANEXO A. Características técnicas de los equipos

• SWITCHES

WS-C4510R+E



Figura A 1. Switch WS-C4510R+E

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/switches/catalyst-4510r-e-switch/model.html>

Slots	10
Slots para tarjetas de línea	8
Supervisor engine slots	2
Ancho de banda por slot	48Gbps
PoE Universal (UPOE)	Sí
PoE+(30W)	Sí
Rendimiento	Comutación IPv4: 250 Mpps Comutación IPv6: 125 Mpps
Procesador	1.5GHz
Autenticación	(SSH), RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Cumplimiento de normas	IEEE 802.3af, IEEE 802.3x, IEEE 802.1ae, IEEE 802.3at
Dimensiones (h,a,p)	61.84x43.97x31.70cm
Unidades de rack	14
Soporte SNMP	SNMPv1, v2c y v3

Switch WS-C4503-E L3



Figura A 2. Switch WS-C4503-E L3

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/switches/catalyst-4503-e-switch/model.html>

Slots	3
Slots para tarjetas de línea	2
Supervisor engine slots	1
Ancho de banda por slot	48Gbps
PoE Universal (UPOE)	Sí
PoE+(30W)	Sí
Rendimiento	Conmutación IPv4: 250 Mpps Conmutación IPv6: 125 Mpps
Procesador	1.5GHz
Autenticación	(SSH), RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Cumplimiento de normas	IEEE 802.3af, IEEE 802.3x, IEEE 802.1ae, IEEE 802.3at
Dimensiones (h,w,d)	31.12 x 43.97 x 31.70 cm
Unidades de rack	7U
Soporte SNMP	SNMPv1, v2c y v3

Fuente: http://www.almacen-informatico.com/CISCO_Catalyst-4510R-E-WS-C4510RE-S7-96V-_1090897_p.htm

Switch WS-CBS3020-HPQ



Figura A 3. Switch WS-CBS3020-HPQ

Fuente: Recuperado de: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-blade-switch-3020-hp/product_data_sheet0900aecd804a3d81.html

Slots de expansión	4
Número de puertos de red (RJ-45)	4
Tecnología de red	10/100/1000Base-T
Tecnología Ethernet	Gigabit
Tecnología de almacenamiento	DDR SDRAM
Memoria RAM	128 MB
Memoria Flash	32MB
Puerto de administración	Sí
Rendimiento	Conmutación a 48Gbps
Autenticación	RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Dimensiones (h,w,d)	1.1"x7.6"x10.5"
Gestión remota	CLI , RMON 1 , RMON 2 , SNMP 1 , SNMP 2c , SNMP 3 , Telnet

Fuente: http://www.manucomp.com/cisco_catalogue/Switches/WS-CBS3020-HPQ.html

Switch WS-C2960-48TC-L



Figura A 4. Switch WS-C2960-48TC-L

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/switches/catalyst-2960-48tc-l-switch/model.html>

Modelo	LAN Base Layer 2
Puertos	48 puertos Ethernet 10/100

Ancho de banda de conmutación	32Gbps
Paquetes por segundo (Mpps)	10.1
PoE	No
VLAN IDs	4000
Direcciones MAC Unicast	8000
Rendimiento	Capacidad switching 16 Gbps
Memoria flash	32MB
Memoria DRAM	64MB
Memoria RAM	128MB
MTU	Sobre los 9000 bytes
Auenticación	RADIUS , TACACS+
Dimensiones (h,w,d)	4.4 x 44.5 x 23.6 cm.
Gestión remota	CLI , RMON 1 , RMON 2 , SNMP 1 , SNMP 2c , SNMP 3 , Telnet

Fuente: <http://www.cisco.com/c/en/us/support/switches/catalyst-2960-48tc-l-switch/model.html>

Switch WS-C2960-24TC-L



Figura A 5. Switch WS-C2960-24TC-L

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/switches/catalyst-2960-24tc-l-switch/model.html>

Modelo	LAN Base Layer 2
Puertos	24 puertos Ethernet 10/100
Interfaces uplink	2 (SFP o 1000BASE-T)
Ancho de banda de conmutación	32Gbps
Paquetes por segundo (Mpps)	6.5
PoE	No
VLAN IDs	4000
Direcciones MAC Unicast	8000
Rendimiento	Capacidad switching 16 Gbps
Memoria flash	64MB
Memoria DRAM	64MB
Memoria RAM	128MB

MTU	Sobre los 9000 bytes
Auenticación	RADIUS , TACACS+
Dimensiones (h,w,d)	4.4cm x 45.0 cm x 24.2 cm.
Gestión remota	CLI , RMON 1 , RMON 2 , SNMP 1 , SNMP 2c , SNMP 3 , Telnet

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-plus-series-switches/data_sheet_c78-728003.html

Switch WS-C3850-48T



Figura A 6. Switch WS-C3850-48T

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/switches/catalyst-3850-48t-e-switch/model.html>

Tipo	Switch capa 3
Puertos	48
Tecnología Ethernet	Gigabit Ethernet
Tecnología de red	10/100/1000Base-T
PoE	Si
Rendimiento	Capacidad switching 176 Gbps
Memoria flash	2GB
Memoria RAM	4GB
Memoria DRAM	8GB
Auenticación	Kerberos , RADIUS , Secure Shell (SSH) , TACACS+
Dimensiones (h,w,d)	4,57x44,45x44.95cm
Unidades de Rack	1U
Gestión remota	CLI , RMON 1 , RMON 2 , SNMP 1 , SNMP 2c , SNMP 3 , SSH , Telnet

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/data_sheet_c78-720918.html

Switch WS-C2960X-48TS-L



Figura A 7. Switch WS-C2960X-48TS-L

Fuente: <http://www.cisco.com/c/en/us/support/switches/catalyst-2960x-48ts-l-switch/model.html>

Modelo	LAN Base Layer 2
Puertos	48 x 10/100/1000 + 4 x Gigabit SFP
Interfaces uplink	4 x 1G SFP
VLAN IDs	4000
MTU	9198 Bytes
Rendimiento	Capacidad switching 216 Gbps
Memoria flash	128MB
Memoria RAM	512MB
Procesador	600 MHz Dual Core
Autenticación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Dimensiones (h,w,d)	4.5 cm x 44.5 cm x 27.9 cm
Gestión remota	SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, HTTP, TFTP, SSH, CLI

Fuente: <http://www.cisco.com/c/en/us/support/switches/catalyst-2960x-48ts-l-switch/model.html>

Switch Nexus 5548



Figura A 8. Switch Nexus 5548

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/switches/nexus-5548up-switch/model.html>

Tráfico soportado	Capa 2 y Capa 3
Puertos	32 x SFP+
Tamaño de tabla de dirección MAC	32K de entradas
DRAM	8GB
NVRAM	6MB
Procesador	1.7 GHz (dual core)
Autenticación	MS-CHAP , RADIUS , TACACS+

Algoritmo de encriptación	AES
Dimensiones (h,w,d)	4.32cm x 43.9cm x 74.93cm
Unidades de rack	1U
Gestión remota	CLI , RMON , SNMP 1 , SNMP 2 , SNMP 3 , SSH-2 , Telnet

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5548p-switch/white_paper_c11-622479.html

Switch WS-C2960S-24PS-S



Figura A 9. Switch WS-C2960S-24PS-S

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/switches/catalyst-2960s-24ts-s-switch/model.html>

Puertos	24 x 10/100/1000 + 4 x SFP
Paquetes por segundo	6.5 Mpps
PoE	Si
Rendimiento	Capacidad de switching de 176Gps
Memoria Flash	64MB
RAM	128MB
Autenticación	Secure Shell (SSH), RADIUS, TACACS+
Algoritmo de encriptación	SSL
Dimensiones (h,w,d)	4.5 x 44.5 x 29.9 cm.
Gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html

- FIREWALL

Cisco ASA 5520



Figura A 10. Cisco ASA 5520

Fuente: Recuperado de: <http://www.cisco.com/c/en/us/support/security/asa-5520-adaptive-security-appliance/model.html>

Puertos	4 Gigabit Ethernet y 1 Fast Ethernet
Rendimiento	Capacidad del cortafuegos: 450 Mbps Capacidad de VPN (3DES/AES): 225 Mbps Tasa de conexiones: 12.000 conexiones por segundo
Memoria Flash	256MB
RAM	2GB
Autenticación	Secure Shell (SSH), RADIUS, TACACS+
Algoritmo de cifrado	DES, Triple DES, AES
Dimensiones (h,w,d)	4.45 cm x 36.2 cm x 20.04 cm.
Protocolo de Gestión	SNMP 1, SNMP 2, SNMP 3, SNMP 2c

Fuente: <http://www.cisco.com/c/en/us/support/security/asa-5520-adaptive-security-appliance/model.html>

ANEXO B. Encuesta
Formato de encuesta

UNIVERSIDAD TÉCNICA DEL NORTE

**ENCUESTA DIRIGIDA A LOS USUARIOS DE LA RED DE DATOS DEL EDIFICIO CENTRAL DE LA
UTN**

Fecha: _____ Dpto. o área: _____

La presente encuesta se elaboró con el objetivo de determinar el nivel de satisfacción de los usuarios de la red interna del Edificio Central y evaluar el trabajo de la Dirección de Desarrollo Tecnológico e Informativo (DDTI).

La encuesta consta de 9 preguntas, emita su criterio marcando con una X en la opción que usted considere correcta.

¿Con qué frecuencia, usted considera que ocurre un problema en la red de datos de la UTN?

- Una vez al día
- Más de una vez al día
- Una vez a la semana
- Más de una vez a la semana

Cuando reporta un problema en la red de datos, ¿Cuál es el tiempo aproximado de espera antes de ser atendido por el personal del DDTI?

- 10 minutos
- 30 minutos
- 1 hora
- 1 día

¿Cuál es el tiempo aproximado que tarda el personal del DDTI en solucionar un problema en la red de datos de la UTN?

- 10 minutos
- 30 minutos
- 1 hora
- 1 día
- 1 semana

Escoja el grado de funcionalidad del servicio de E-mail que provee la UTN

- No funciona
- Falla con mucha frecuencia
- Falla muy rara vez
- Funciona correctamente

Escoja el grado de funcionalidad de la Página web que provee la UTN

- No funciona
- Falla con mucha frecuencia
- Falla muy rara vez
- Funciona correctamente

Escoja el grado de funcionalidad de su Portafolio virtual al que accede

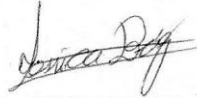
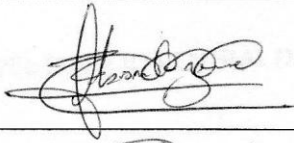
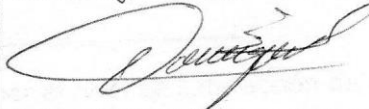
- No funciona
- Falla con mucha frecuencia
- Falla muy rara vez
- Funciona correctamente

¿Cómo califica usted el servicio de Internet?

- Muy bueno
- Bueno
- Regular
- Ineficiente

En general ¿cuál es su nivel de satisfacción con el servicio recibido por parte del DDTI?

- Muy Satisfecho
- Satisfecho
- Poco Satisfecho
- No satisfecho

Elaborado por:	Jessica Báez	
Aprobado por:	Ing. Fabián Cuzme, Msc Director de tesis	
	Ing. Mauricio Domínguez, Msc Co-director de tesis	

UNIVERSIDAD TÉCNICA DEL NORTE

ENCUESTA DIRIGIDA A LOS USUARIOS DE LA RED DE DATOS DEL EDIFICIO CENTRAL DE LA
UTNFecha: 20/12/2016Dpto. o área: Tesorería

La presente encuesta se elaboró con el objetivo de determinar el nivel de satisfacción de los usuarios de la red interna del Edificio Central y evaluar el trabajo de la Dirección de Desarrollo Tecnológico e Informativo (DDTI).

La encuesta consta de 8 preguntas, emita su criterio marcando con una X en la opción que usted considere correcta.

¿Con qué frecuencia, usted considera que ocurre un problema en la red de datos de la UTN?

- Una vez al día
- Más de una vez al día
- Una vez a la semana
- Más de una vez a la semana

Cuando reporta un problema en la red de datos, ¿Cuál es el tiempo aproximado de espera antes de ser atendido por el personal del DDTI?

- 10 minutos
- 30 minutos
- 1 hora
- 1 día

¿Cuál es el tiempo aproximado que tarda el personal del DDTI en solucionar un problema en la red de datos de la UTN?

- 10 minutos
- 30 minutos
- 1 hora
- 1 día
- 1 semana

Escoja el grado de funcionalidad del servicio de E-mail que provee la UTN

- No funciona
 Falla con mucha frecuencia
 Falla muy rara vez
 Funciona correctamente

Escoja el grado de funcionalidad de la Página web que provee la UTN

- No funciona
 Falla con mucha frecuencia
 Falla muy rara vez
 Funciona correctamente

Escoja el grado de funcionalidad de su Portafolio virtual al que accede

- No funciona
 Falla con mucha frecuencia
 Falla muy rara vez
 Funciona correctamente

¿Cómo califica usted el servicio de Internet?

- Muy bueno
 Bueno
 Regular
 Ineficiente

En general ¿cuál es su nivel de satisfacción con el servicio recibido por parte del DDTI?

- Muy Satisfecho
 Satisfecho
 Poco Satisfecho
 No satisfecho

ANEXO C. Entrevista UNIVERSIDAD TÉCNICA DEL NORTE

Entrevista dirigida al administrador de red de la UTN

Fecha de la entrevista: 15 de febrero de 2017

La presente entrevista se elaboró con el objetivo de conocer la situación actual de la red de datos del Edificio Central de la UTN, con respecto a la administración de red. Las siguientes preguntas se realizan en concordancia con las cinco áreas del modelo de gestión de red ISO/OSI: gestión de configuraciones, gestión de fallos, gestión de contabilidad, gestión de prestaciones y gestión de seguridad.

GESTIÓN DE CONFIGURACIONES

- **¿Se sigue un procedimiento establecido para solventar una falla en la red, adicionar equipos, realizar configuraciones, etc?**

Se siguen ciertos procedimientos, pero actualmente no existe un manual de procedimientos debidamente aprobado por el Honorable Consejo Universitario.

- **¿Se realiza algún tipo de documentación de los distintos eventos que se presentan en la red y de las configuraciones que se realizan sobre los dispositivos?**

No se realiza ningún tipo de documentación, sin embargo, cuando se suscita un fallo considerable éste se notifica vía quipux.

GESTIÓN DE FALLOS

- **¿Qué tipo de problemas son los más frecuentes dentro de la red de datos del Edificio Central?**

Las páginas web a los que acceden los usuarios cargan lentamente debido al número de peticiones que se generan. Además, se presentan ocasionalmente problemas con el servidor DNS que tiene la institución.

Otro problema común es la manipulación de los cables de red por parte de los usuarios.

- **¿Qué mecanismos utiliza para la detección de fallos en la red?**

Se utiliza el Firewall Cisco ASA, para detectar fallos generados por ataques cibernéticos. Otra forma de detectar fallos es a través de la notificación de los usuarios de la red.

- **¿Cuánto tiempo demora en detectar una falla en la red y solucionarla?**

No hay un tiempo estimado, porque dependería del problema que se haya generado. Cuando es un fallo menor puede ser solucionado inmediatamente de manera remota, mientras que, si el problema es más grave, es necesario desplazarse hacia el sitio donde se ha reportado el fallo.

GESTIÓN DE CONTABILIDAD

- **¿Se realizan inventarios periódicamente de los equipos de red del Edificio Central?**

Si se tienen inventarios de los equipos, se maneja información como: dirección IP máscara de red, gateway, usuario, contraseña, ubicación, marca, modelo y nombre.

GESTIÓN DE PRESTACIONES

- **¿Se generan periódicamente registros acerca del rendimiento de los dispositivos de red?**

Actualmente no se realizan ese tipo de registros.

- **¿Cómo califica usted la disponibilidad de los servicios que provee la red de datos de la UTN?**

Se considera que la disponibilidad a dichos servicios es muy buena.

GESTIÓN DE SEGURIDAD

- **En cuanto a la seguridad, ¿Cómo se maneja el acceso a los dispositivos de red del Edificio Central?**

El acceso es a través de un usuario y contraseña, estas credenciales sólo se manejan por el equipo de trabajo del área de redes y comunicaciones de la DDTI.

- **¿Cuenta actualmente con un mecanismo de monitoreo de red?**

Con respecto a la seguridad, se utiliza el dispositivo Cisco ASA para detectar ciertos ataques, aunque no es suficiente. Se utiliza el equipo Cisco Prime para monitorizar la red Inalámbrica.

- **¿Qué equipos considera usted, tienen mayor necesidad de ser monitoreados?**

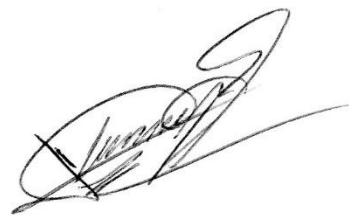
Los equipos que tienen más necesidad de ser monitoreados son: Switch de core, Firewall y Exinda.

- **¿Qué características fundamentales considera usted, que debería tener el software de gestión de red a implementarse?**

Es fundamental que el software de gestión de red tenga una interfaz fácil de usar, que envíe notificaciones por correo electrónico y que tenga escalabilidad y compatibilidad con diferentes tecnologías.



Srta. Jessica Báez
Estudiante



Ing. Vinicio Guerra
Administrador de red

ANEXO D. Especificación de Requerimientos de software

**ESPECIFICACIÓN DE REQUERIMIENTOS DE SOFTWARE
PARA LA GESTIÓN DE RED EN EL EDIFICIO CENTRAL DE LA
UTN**



UNIVERSIDAD TÉCNICA DEL NORTE

JESSICA BÁEZ

IBARRA, 2017

HISTORIAL DE CAMBIOS

FECHA	SECCIÓN MODIFICADA	DESCRIPCIÓN	RESPONSABLE
10/12/2016	Todas	Creación de todas las secciones	Jessica Báez

CONTENIDO

1. Introducción
 - 1.1. Propósito del software
 - 1.2. Alcance del software
2. Descripción general del software
 - 2.1. Perspectiva del software
 - 2.2. Funciones del software
 - 2.3. Características del usuario
 - 2.4. Limitaciones
3. Referencias
4. Requerimientos del software
 - 4.1. Interfaces externas
 - 4.2. Requisitos funcionales
 - 4.3. Requisitos de usabilidad
 - 4.4. Requisitos de rendimiento
 - 4.5. Atributos del software
5. Acrónimos

1. Introducción

Este documento ha sido estructurado de acuerdo a las especificaciones definidas por ISO/IEC/IEEE 29148:2011 para la Especificación de Requisitos de Software con el fin definir de forma clara los requerimientos para la implementación de un software de gestión de red en el Edificio Central de la Universidad Técnica del Norte.

1.1. Propósito

El software a especificarse tiene el propósito de realizar la monitorización y control de los equipos de red del Edificio Central de la Universidad Técnica del Norte.

1.2. Alcance

El software de gestión de red debe tener las funciones necesarias para poder cubrir las cinco áreas funcionales del modelo de gestión de red ISO/OSI: Gestión de configuraciones, gestión de fallos, gestión de contabilidad, gestión de prestaciones y gestión de seguridad.

2. Descripción General

En esta sección se describe la perspectiva del producto, funciones del producto, características del usuario, limitaciones del producto y definiciones.

2.1.1. Perspectiva

El software a especificarse debe ser compatible con los modelos de equipos de red existentes en el Edificio Central de la UTN, que en su mayoría son de marca Cisco. Además, debe tener una interfaz de usuario amigable e intuitiva.

2.1.2. Funciones

- Autodescubrimiento de la red
- Monitorización
- Notificaciones y alertas
- Inventariar componentes
- Visualización en forma gráfica

2.1.3. Características del usuario

- *Administrador de red:* Ingeniero en Electrónica y redes de Comunicación, Responsable Infraestructura Tecnológica | Desarrollo Tecnológico e Informático

2.1.4. Limitaciones

- El software debe ser Open Source.
- El software debe soportar el protocolo de gestión de red SNMP.
- Debe ser compatible con los equipos de red presentes en la misma.

2.2. Definiciones

- *Especificación de Requisitos Software:* Conjunto de requerimientos que describen la funcionalidad que el software debe tener para cumplir con los objetivos de implementación.
- *Open Source:* Open Source o código abierto es el software distribuido y desarrollado libremente.

3. Referencias

- Systems and software engineering — Life cycle processes — Requirements engineering. ISO/IEC/IEEE 29148

4. Requisitos Específicos

4.1. Interfaces externas

El administrador de la red podrá acceder al sistema remotamente desde un PC o computador portátil utilizando su cuenta de usuario. Desde allí podrá visualizar el estado de la red, así como ejecutar las acciones relacionadas al control de red.

4.2. Requisitos Funcionales

- *RQ1: Autodescubrimiento de la red.* El software debe ser capaz de encontrar los dispositivos conectados en la red.
- *RQ2: Monitorización y control.* El software debe recuperar la información de los agentes en tiempo real. Además, debe tener la posibilidad de realizarlo de manera remota.
- *RQ3: Notificaciones y alertas.* En caso de encontrarse una falla, el software debe notificarla inmediatamente, ya sea desde la interfaz de usuario o en el mejor de los casos enviando un correo electrónico al administrador de la red.
- *RQ4: Generación de reportes.* El software debe ser capaz de emitir reportes (informes, historiales y datos estadísticos) acerca de los dispositivos gestionados.
- *RQ5: Visualización en forma gráfica.* Ver la información de la red de manera gráfica para un mejor entendimiento e interpretación.

4.3.Requisitos de usabilidad

- *RQ6*: El software deberá ser de fácil instalación, configuración y uso.

4.4.Requisitos de rendimiento

El funcionamiento de los dispositivos monitoreados no debe ser afectado por nuevas funciones instaladas en los mismos.


4.5. Atributos del sistema

- *RQ7: Seguridad*. El administrador de la red estará autorizado para acceder al sistema de gestión, mediante un *login* y *password*.
- *RQ8: Disponibilidad*. El sistema deberá estar en funcionamiento las 24 horas del día todos los días para emitir alertas en cualquier momento que se produzca un fallo.
- *RQ9: Escalabilidad*. Se debe poder añadir más elementos al sistema de gestión de red en caso de que sea necesario.

5. Acrónimos

- *IEEE*: Institute of Electrical and Electronic Engineers ó Instituto de Ingenieros Eléctricos y Electrónicos.
- *ERS*: Especificación de Requisitos Software.
- *SNMP*: Protocolo simple de administración de red.

ANEXO E. Formulario de reportes de fallos

	UNIVERSIDAD TÉCNICA DEL NORTE			
	FORMATO ÚNICO DE REPORTES DE FALLOS			
	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO			
Número de reporte:		Fecha del reporte:		
Área/ Departamento:		Fecha de solución:		
Reportado por:		Tiempo empleado:		
Solucionado por:				
Tipo de fallo:				
	Red	Servicios	Otros _____	
Nivel de prioridad:	Crítico	Error	Aviso	Notificación
Detalle del dispositivo:				
Tipo de dispositivo	Descripción	Marca	Modelo	
Detalle del problema:				
Detalle de la solución:				

ANEXO F. Instalación de CentOS 7

- 1) Entrar a la primera opción: Install CentOS 7

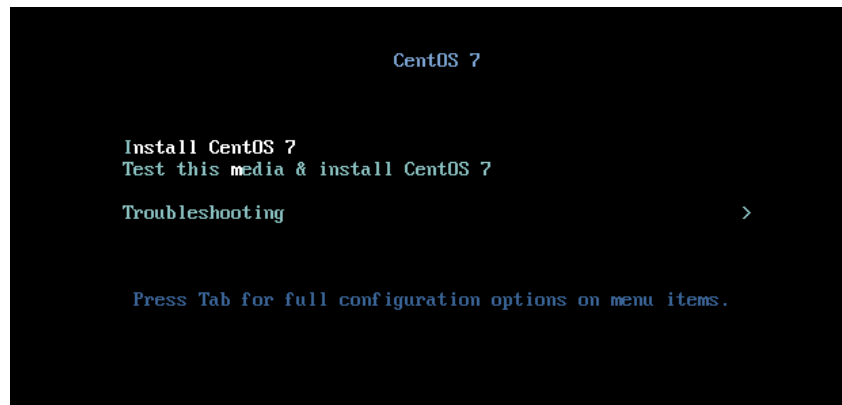


Figura F 1. Instalación de CentOS 7

Fuente: Captura de CentOS

- 2) Elegir el idioma y dar clic en *Continuar*

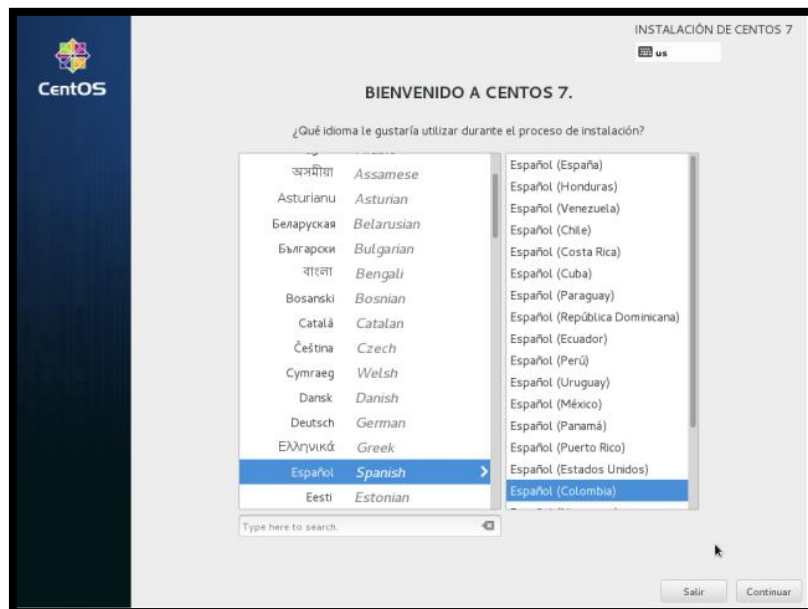


Figura F 2. Selección de idioma

Fuente: Captura de CentOS

- 3) En la pantalla de Resumen de Instalación dar clic en *Destino de la instalación*

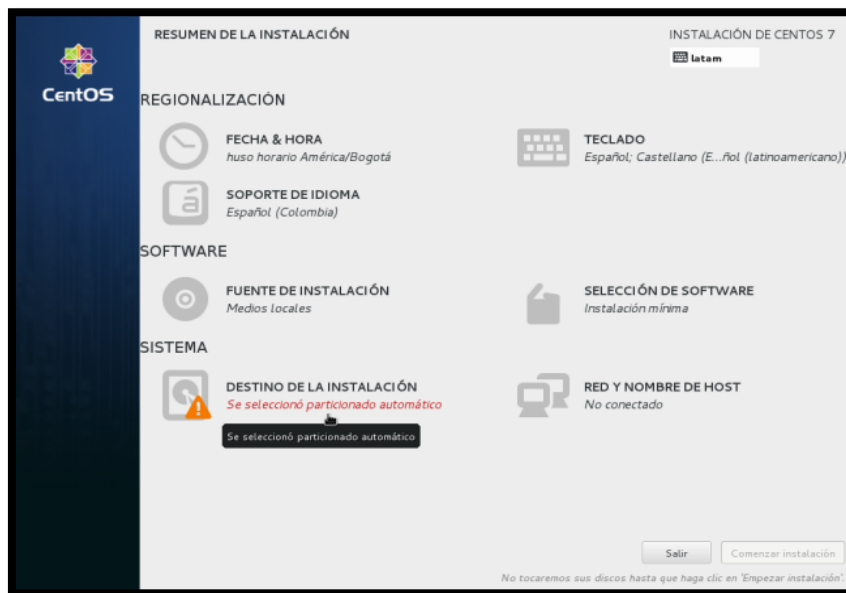


Figura F 3. Destino de instalación

Fuente: Captura de CentOS

- 4) Se podrán ver los discos en los que es posible instalar, generalmente será un único disco, debe estar seleccionado. Hacer clic en el botón *Listo*



Figura F 4. Selección de dispositivos

Fuente: Captura de CentOS

- 5) En la pantalla de Resumen de instalación, dar clic en **Red y nombre de host**



Figura F 5. Resumen de instalación

Fuente: Captura de CentOS

- 6) Escribir el nombre del host de la forma `host.dominio` y hacer clic en **Configurar**. En la ventana que sale a continuación se debe activar la opción **Conectarse automáticamente a esta red cuando esté disponible**. Hacer clic al botón **Guardar**

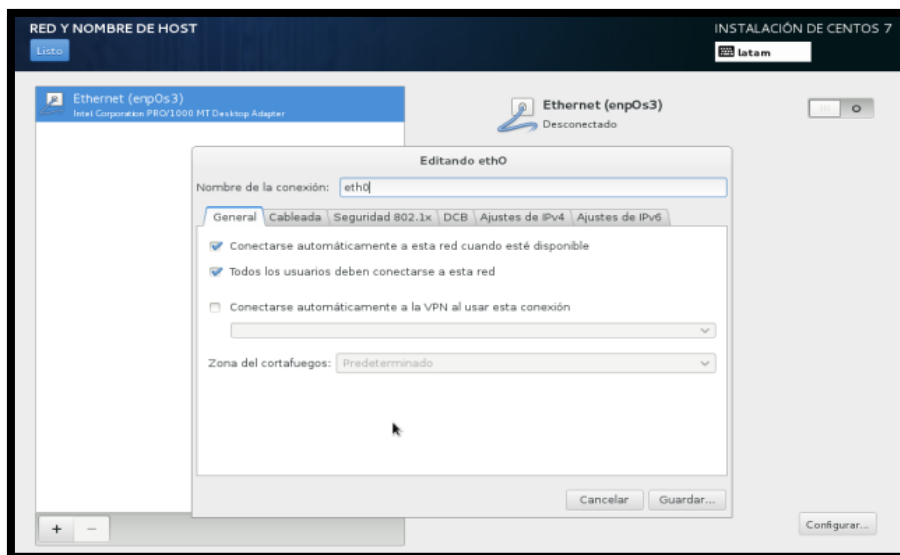


Figura F 6. Red y nombre de host

Fuente: Captura de CentOS

- 7) El equipo se conectará a la red y mostrará los datos obtenidos por DHCP. Hacer clic en *Listo*

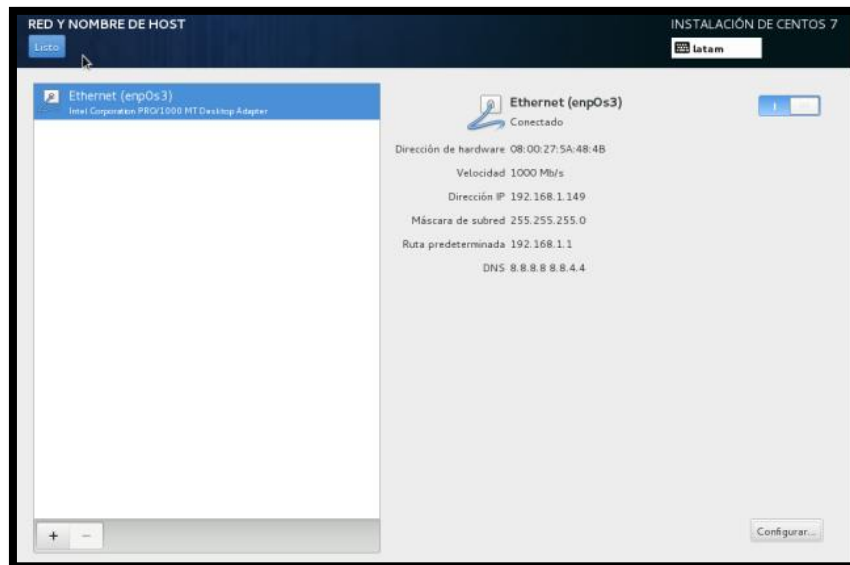


Figura F 7. Reconocimiento de la interfaz de red

Fuente: Captura de CentOS

- 8) Clic al botón *Comenzar instalación*.

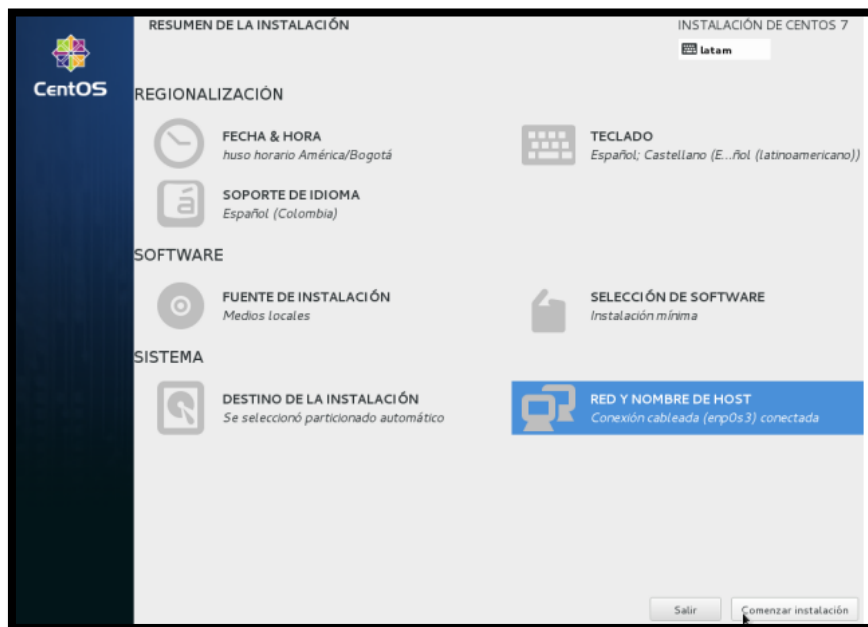


Figura F 8. Comenzar instalación

Fuente: Captura de CentOS

- 9) Durante la instalación, se realiza la configuración de usuario. Hacer clic en ***Contraseña de root***

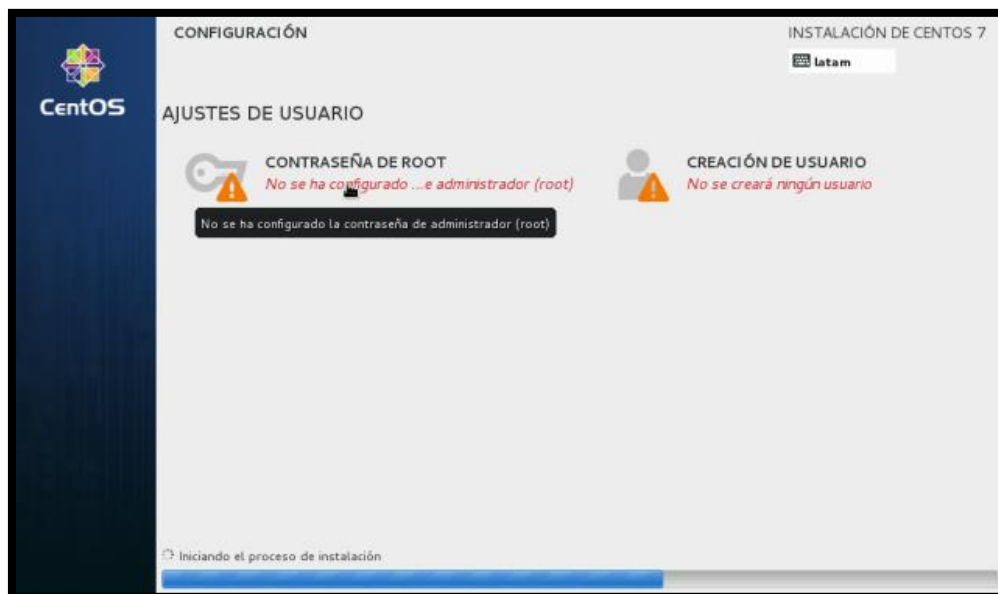


Figura F 9. Ajustes de usuario

Fuente: Captura de CentOS

- 10) La contraseña debe escribirse dos veces

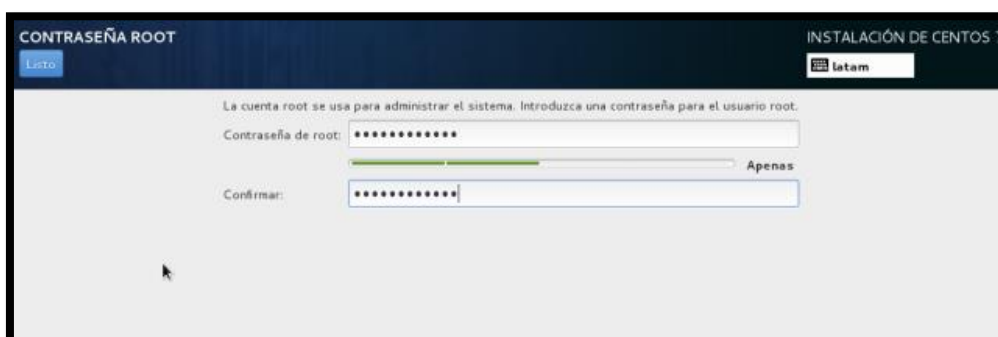


Figura F 10. Configuración de contraseña root

Fuente: Captura de CentOS

11) Cuando se acabe la instalación dar clic en *reiniciar*



Figura F 11. Finalización de instalación

Fuente: Captura de CentOS

12) Una vez se reinicie la maquina será posible ingresar con la contraseña de root

ANEXO G. Instalación del servidor Zabbix

1) Añadir los repositorios oficiales de Zabbix 3.0 CentOS 7

```
# rpm -ivh http://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm
```

2) Desactivar SELinux

SELinux es un módulo de seguridad del kernel de Linux que forma parte de las instalaciones estándar de CentOS. Lo siguiente sólo debe realizarse en un entorno de prueba, ya que normalmente se desea que SELinux esté configurado correctamente.

```
# setenforce 0
# sed -i 's/^SELINUX=.*SELINUX=disabled/g' /etc/selinux/config
```

3) Instalación de Zabbix 3.0 Server, agente y web front-end

```
# yum -y install zabbix-server-mysql zabbix-web-mysql zabbix-agent
```

4) Instalar MariaDB Server, habilitarlo e iniciarlo

```
# yum -y install mariadb-server mariadb
# systemctl enable mariadb.service
# systemctl start mariadb.service
```

5) Asegure su instalación de MariaDB

```
# mysql_secure_installation
```

El script preguntará si desea cambiar la contraseña de root del servidor MariaDB, puede cambiarse más tarde. Responda "Sí" a las 4 preguntas restantes.

6) Crear la base de datos y usuarios de Zabbix

Esto creará su base de datos Zabbix y un usuario llamado 'zabbix' con la <contraseña> que especifique. Este usuario será el utilizado por su servidor Zabbix y el web front-end.

```
# mysql -uroot -p
MariaDB> create database zabbix character set utf8 collate utf8_bin;
MariaDB> grant all privileges on zabbix.* to zabbix@localhost identified by
'<password>';
MariaDB> quit;
```

7) Importar esquema inicial y datos

Zabbix necesita configurar correctamente su base de datos 'zabbix' y también crear tablas para su uso.

```
# /usr/share/doc/zabbix-server-mysql-*/
# gunzip create.sql.gz
#mysql -u root -p zabbix < create.sql
```

8) Configurar Zabbix Server

```
# vi /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbix
```

9) Especifique el huso horario de su web front-end

```
# vi /etc/httpd/conf.d/zabbix.conf
```

10) Configuración de PHP

```
# vi /etc/php.ini
max_execution_time = 600
max_input_time = 600
memory_limit = 256M →512M
post_max_size = 32M
upload_max_filesize = 16M
```

```
date.timezone = Asia/Kolkata
```

11) Permitir los puertos en el Firewall

```
# firewall-cmd --permanent --add-port=10050/tcp
# firewall-cmd --permanent --add-port=10051/tcp
# firewall-cmd --permanent --add-port=80/tcp
# firewall-cmd --reload
# firewall-cmd --permanent --add-service=http
# systemctl restart firewalld
```

12) Establezca la regla de Selinux a continuación.

```
# setsebool -P httpd_can_connect_zabbix=1
```

13) Habilite e inicie su servidor Zabbix, agente y servicio HTTPD

```
# systemctl enable zabbix-server
# systemctl enable zabbix-agent
# systemctl enable httpd
# systemctl start zabbix-server
# systemctl start zabbix-agent
# systemctl start httpd
```

Compruebe que puede acceder a su web front-end abriendo un navegador y señalándolo a:

```
http://<your-server-ip>/zabbix/
```

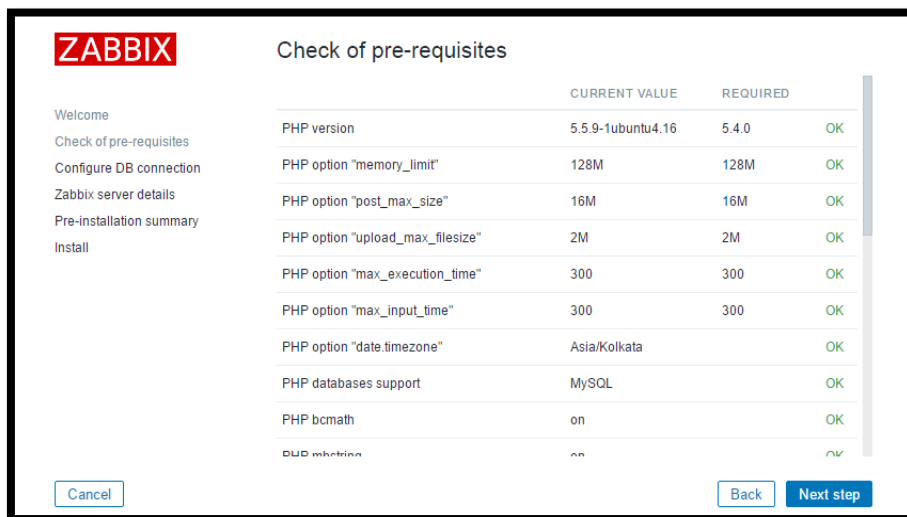


Figura G 1. Instalación de Zabbix

Fuente: Captura de Zabbix

14) Compruebe los requisitos previos

Compruebe si su sistema tiene todos los paquetes necesarios, si todo está bien haga clic en Siguiente.



ZABBIX Check of pre-requisites

	CURRENT VALUE	REQUIRED	
PHP version	5.5.9-1ubuntu4.16	5.4.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	Asia/Kolkata		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK

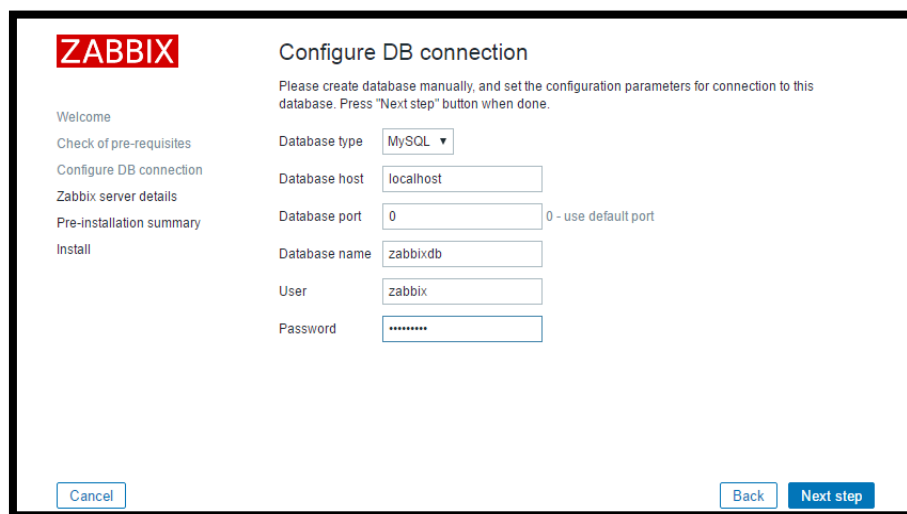
Buttons: Cancel, Back, Next step

Figura G 2. Comprobación de requisitos previos

Fuente: Captura de Zabbix

15) Configurar la conexión de DB

Introduzca los detalles de la base de datos



ZABBIX Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

Database type:

Database host:

Database port: 0 - use default port

Database name:

User:

Password:

Buttons: Cancel, Back, Next step

Figura G 3. Detalles de la base de datos

Fuente: Captura de Zabbix

16) Detalles del servidor Zabbix

ZABBIX Zabbix server details

Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional).

Host

Port

Name

Cancel Back Next step

Figura G 4. Detalles del servidor

Fuente: Captura de Zabbix

17) Resumen de la preinstalación

En este paso se mostrará el resumen que ha introducido los pasos anteriores, por lo que simplemente haga clic en Siguiente.

ZABBIX Pre-installation summary

Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Database type MySQL

Database server localhost

Database port default

Database name zabbixdb

Database user root

Database password *****

Zabbix server localhost

Zabbix server port 10051

Zabbix server name Zabbix Server

Cancel Back Next step

Figura G 5. Resumen de la pre-instalación

Fuente: Captura de Zabbix

18) Instalación

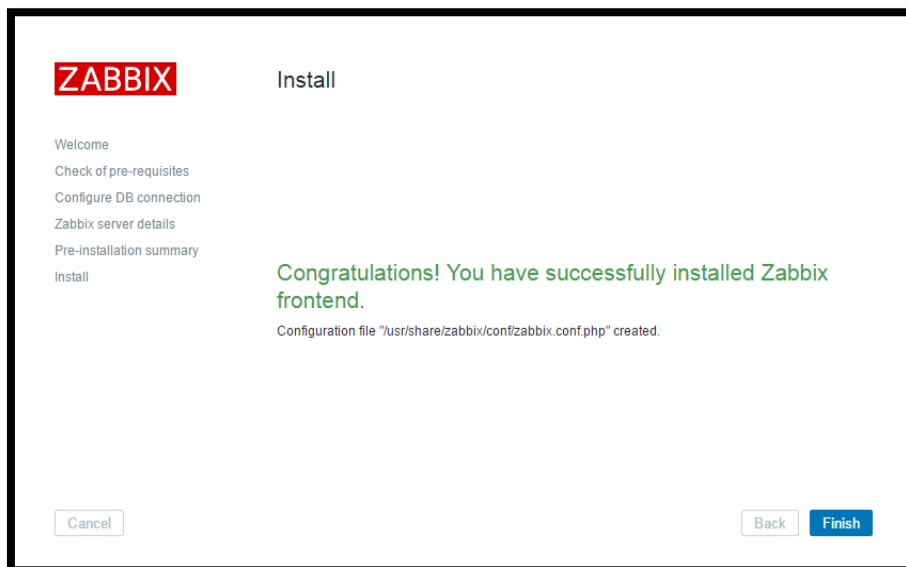


Figura G 6. Instalación frontend

Fuente: Captura de Zabbix

19) Inicio de sesión

Inicie sesión en Zabbix utilizando las credenciales por defecto.

Username: Admin
Password: zabbix

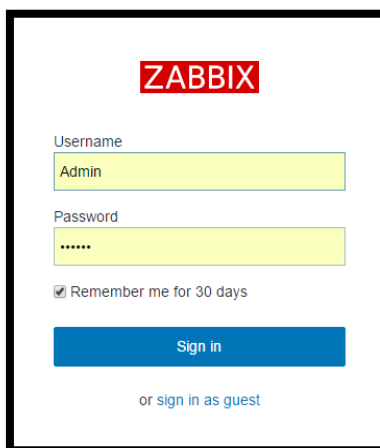


Figura G 7. Inicio de sesión

Fuente: Captura de Zabbix

Después de iniciar sesión con éxito, obtendrá el panel de zabbix como a continuación.

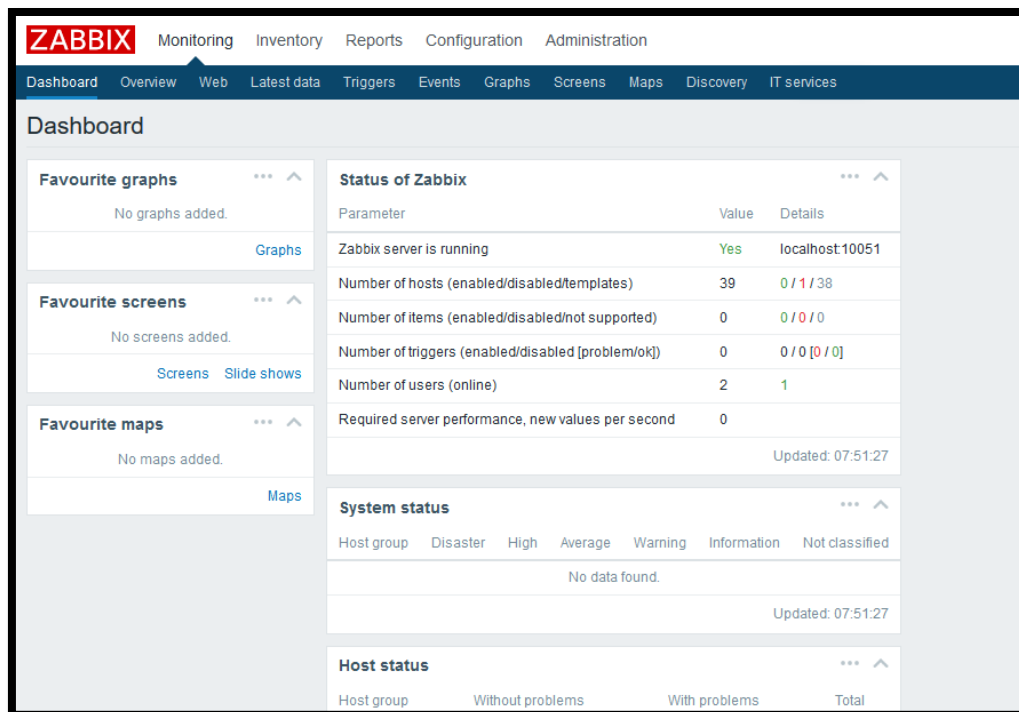


Figura G 8. Panel de Zabbix

Fuente: Captura de Zabbix

Habilitar SNMP en Zabbix

1) Instalar snmp en CentOS 7 con el siguiente comando

```
Yum -y install net-snmp net-snmp-utils
```

2) Configurar el archivo snmp.conf con la comunidad que se va a monitorear y la dirección IP del servidor

```
Vi /etc/snmp/snmpd.conf
```

```
rocommunity public 192.168.20.3
```

```
rocommunity public 127.0.0.1
```

3) Reiniciar el servicio

```
Systemctl restart snmpd.service
```

4) Comprobar conexión y reiniciar los servicios

```
Snmwalk -v 2c -c public ipswitch
```

```
Systemctl restart httpd.service
```

```
Systemctl restart Zabbix-server.service
```

ANEXO H. Configuración del protocolo SNMP

- **Equipos Cisco Catalyst**

Este procedimiento es el mismo para los routers y los conmutadores Cisco Catalyst de Cisco IOS.

Habilitar las comunidades SNMP

- 1) Establecer conexión vía telnet con el Switch o router. Puede usarse la aplicación Putty.
- 2) Ingresar al modo enable ingresando la contraseña respectiva.

```
Router>enable
Password:
Router#
```

- 3) Mostrar la configuración en ejecución y buscar la información SNMP:

```
Router#show running-config
Building configuration...
....
....
```

- 4) Ingresar al modo de configuración

```
Router#configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#
```

- 5) Utilice los siguientes comandos para habilitar la comunidad public Read-Only (RO) y la comunidad private Read-write (RW):

```
Router(config)#snmp-server community public RO
Router(config)#snmp-server community private RW
```

- 6) Salir del modo de configuración y guarde la configuración modificada en la memoria

RAM no volátil (NVRAM):

```
Router(config)#exit
Router#write memory
Building configuration...
[OK]
Router#
```


Verificar las comunidades SNMP

- 7) Compruebe que hay conectividad TCP / IP entre el servidor administración de red (NMS) y el router o switch:

```
ping <IP adress>
```

- 8) Ingresar nuevamente al modo enable del dispositivo y mostrar la configuración en ejecución para buscar la información SNMP:

```
Router#show running-config
....
....
snmp-server community public RO
snmp-server community private RW
....
....
```

- **Configuración del protocolo SNMP en equipos Cisco Asa 5500**

- 1) Utilizar el siguiente comando para verificar si el protocolo SNMP está habilitado. De forma predeterminada, el servidor SNMP está habilitado.

```
snmp-server enable
```

- 2) Especificar el destinatario de una notificación SNMP.

```
snmp-server host interface_name ip_address [trap | poll] [community text]
[version 1 | 2c] [udp-port port]
```

- 3) Indicar la interfaz desde la que se envían los traps. Identifica el nombre y la dirección IP del administrador NMS o SNMP que puede conectarse al ASA. La palabra clave *trap* limita el NMS a recibir traps solamente. La palabra clave de *poll* limita el NMS a las solicitudes de envío (sondeo) solamente. De forma predeterminada, los traps SNMP están habilitados. De forma predeterminada, el puerto UDP es 162. La cadena de comunidad es una clave

secreta compartida entre el ASA y el NMS. La comunidad predeterminada es "pública". El ASA utiliza esta clave para determinar si la petición SNMP entrante es válida.

4) Configurar la comunidad

```
snmp-server community community-string
```

5) Habilitar traps

```
Snmp-server enable traps [all | syslog | snmp [trap] [...] | entity [trap]  
[...]] | ipsec [trap] [...] | remote-access [trap]]
```

ANEXO I. Instalación del agente en CentOS 6.8

1) Agregar Repositorio Requerido

Antes de instalar Zabbix Agent configure el repositorio zabbix yum utilizando los siguientes comandos de acuerdo a la versión requerida y el sistema operativo.

```
rpm -ivh http://repo.zabbix.com/zabbix/2.2/rhel/6/x86_64/zabbix-release-2.2-1.el6.noarch.rpm
```

2) Instalar el Agente de Zabbix

Usar el siguiente comando para instalar el agente Zabbix en su sistema Linux.

```
yum install zabbix-agent
```

3) Editar la configuración del agente de Zabbix

Como el agente zabbix se ha instalado correctamente en nuestro sistema remoto. Ahora solo necesitamos configurar el agente zabbix agregando el servidor IP zabbix en su archivo de configuración `/etc/zabbix/zabbix_agentd.conf`

```
vi /etc/zabbix/zabbix_agentd.conf
```

```
Server=[zabbix server ip]  
Hostname=[ Hostname of client system ]
```

4) Reiniciar el Agente de Zabbix

Después de agregar el servidor IP de Zabbix en el archivo de configuración, reinicie el servicio del agente utilizando el comando:

```
/etc/init.d/zabbix-agent restart  
/etc/init.d/zabbix-agent start
```

Para que el servicio se inicie automáticamente al encender el dispositivo utilizar el siguiente comando

```
chkconfig zabbix-agent on
```

5) Configurar iptables

Se deben añadir las siguientes reglas al firewall para que permite el paso de información de gestión.

```
vi /etc/sysconfig/iptables
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 10050 -j ACCEPT  
-A INPUT -m state --state NEW -m tcp -p tcp --dport 10051 -j ACCEPT
```

6) Reiniciar iptables

Reiniciar las iptables para que entren en funcionamiento las nuevas reglas

```
service iptables restart
```

ANEXO J. Instalación de Nessus

- 1) Descargar el paquete de instalación correspondiente según el sistema operativo en el siguiente link.

<https://www.tenable.com/products/nessus/select-your-operating-system>

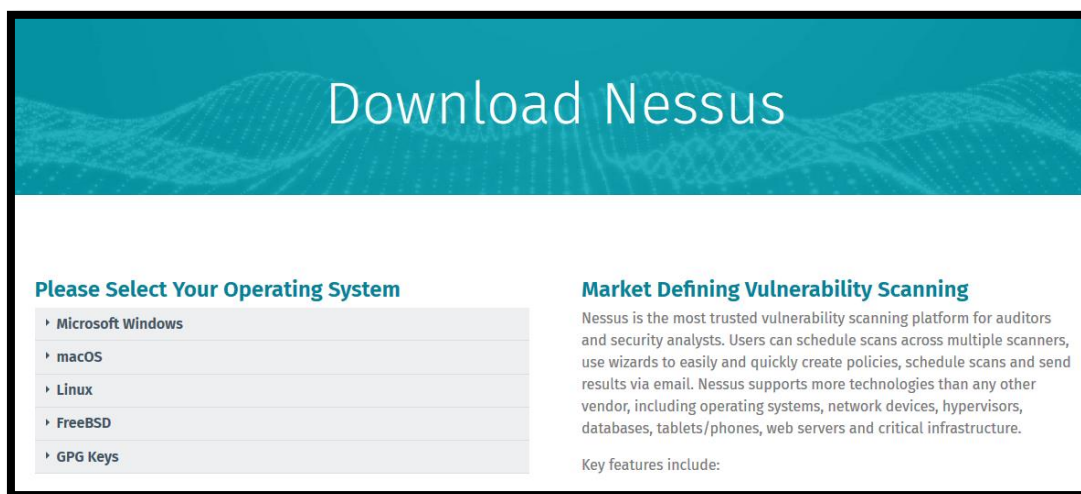


Figura J 1. Descarga de Nessus

Fuente: Recuperado de: <https://www.tenable.com/products/nessus/select-your-operating-system>

- 2) Luego de descargar y ejecutar el instalador entrar a la dirección: <https://localhost:8834/>

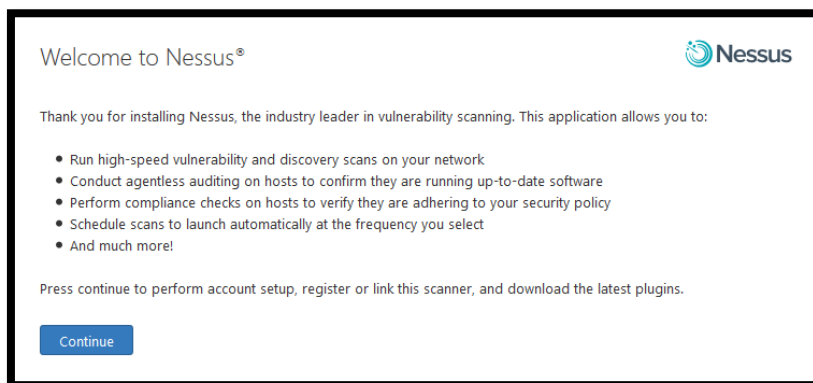


Figura J 2. Pantalla principal de instalación de Nessus

Fuente: Captura de Nessus

- 3) Acceder a la siguiente ventana, donde hay que configurar la cuenta de administrador.

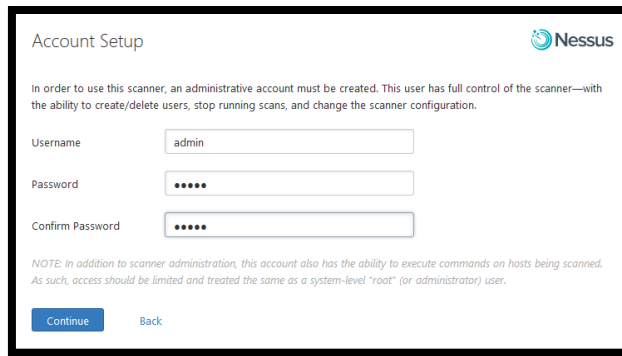


Figura J 3. Configuraciones de cuenta de Nessus

Fuente: Captura de Nessus

4) Se solicita elegir el tipo de activación, en este caso es Nessus Home

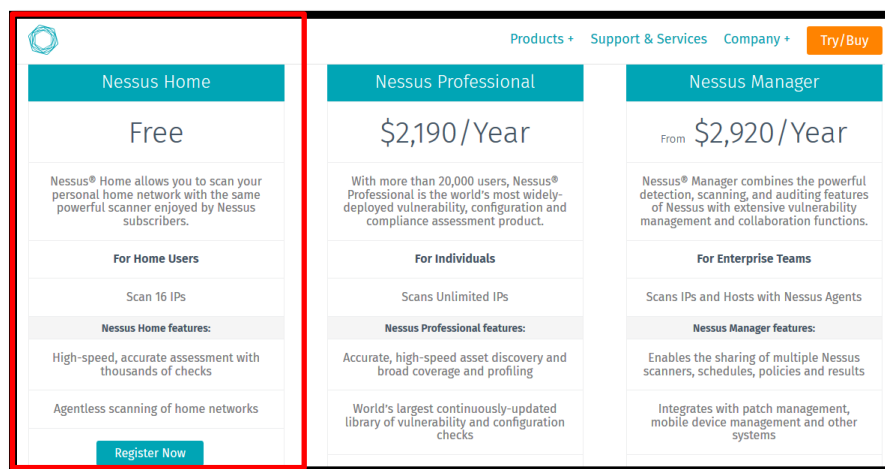


Figura J 4. Activación del producto Nessus

Fuente: Recuperado de: <https://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>

5) El paso siguiente es entrar al programa en modo administrador.

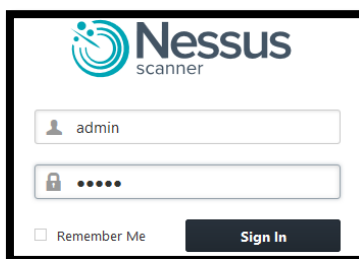


Figura J 5. Log en Nessus

Fuente: Captura de Nessus

6) Se podrá acceder a la interfaz y comenzar a hacer escaneos en la red

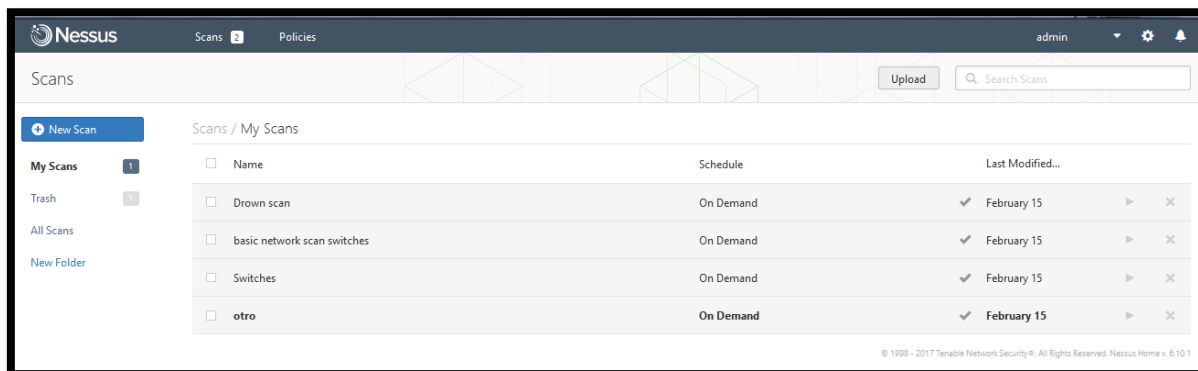


Figura J 6. Pantalla principal de Nessus

Fuente: Captura de Nessus

ANEXO K. Manual del administrador

1. Creación de grupos de usuarios y usuarios:

- 1) Antes de crear un usuario se debe crear un Grupo de Usuarios o usar uno de los grupos ya existentes. Para el caso de que se requiera crear un nuevo grupo ingresar en la interfaz Web a *Administración* → *User Groups* → *Create User group*

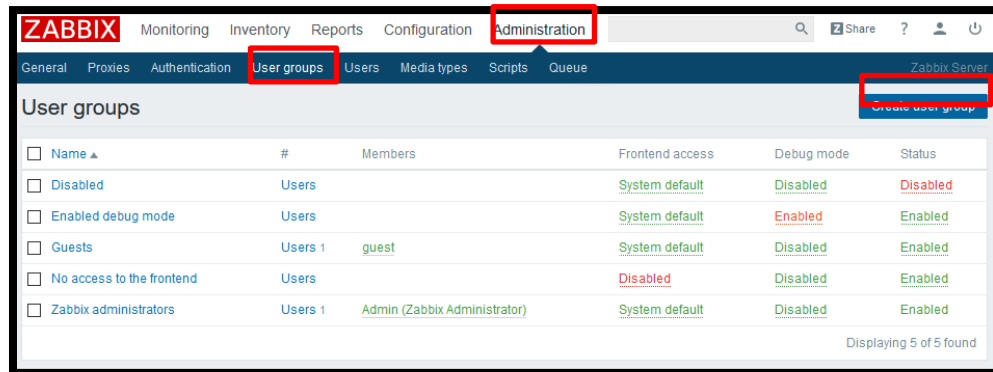


Figura K 1. Grupos de usuarios

Fuente: Captura de Zabbix

- 2) En la siguiente ventana se podrá configurar el nombre del grupo, activar el acceso al frontend del servidor y habilitar al grupo. En la pestaña Permissions se podrán añadir los permisos de lectura y escritura.

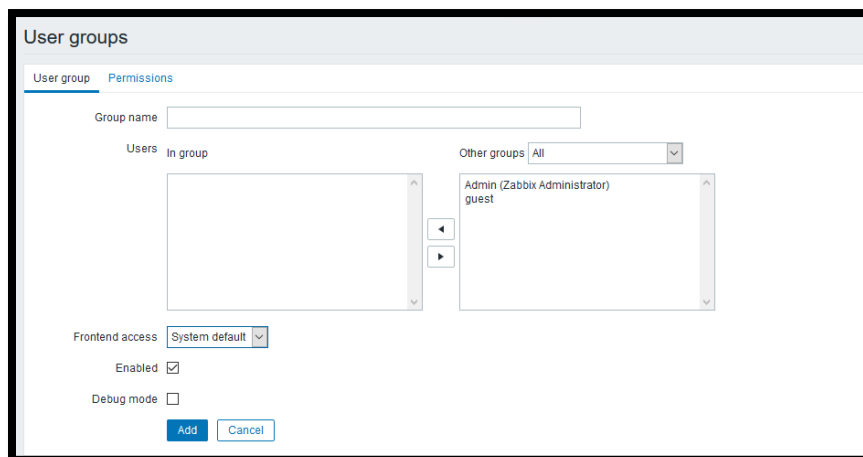


Figura K 2. Users groups

Fuente: Captura de Zabbix

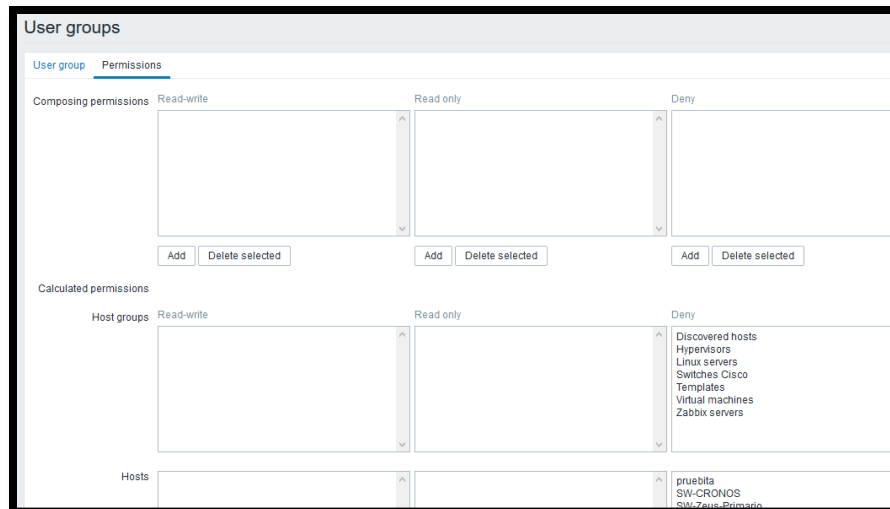


Figura K 3. Privilegios de grupos

Fuente: Captura de Zabbix

- 3) Una vez creado el grupo se prosigue a crear un nuevo usuario que pertenezca a cualquiera de los grupos y por lo tanto goce de los permisos otorgados a dicho grupo de usuarios.

Para esto acceder a *Administración* → *Users* → *Create User*

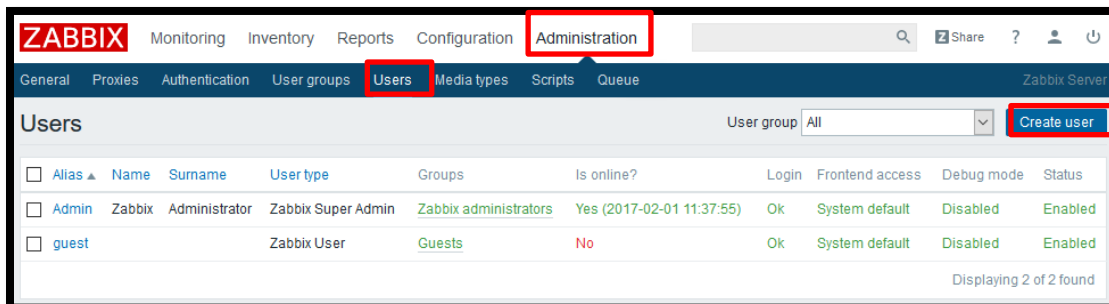


Figura K 4. Creación de usuario

Fuente: Captura de Zabbix

- 4) En la siguiente ventana se deben configurar principalmente: alias, nombre, apellido, grupo, contraseña del usuario. Una vez ingresada toda la información pulsar el botón *Add*.

The screenshot shows the 'Users' configuration page in Zabbix. The 'User' tab is active. The form contains the following fields and values:

- Alias: ECarrión
- Name: Edison
- Surname: Carrión
- Groups: Zabbix administrators
- Password: [masked]
- Password (once again): [masked]
- Language: English (en_GB)
- Theme: System default
- Auto-login:
- Auto-logout (min 90 seconds): 900
- Refresh (in seconds): 30

Figura K 5. Detalles de usuario

Fuente: Captura de Zabbix

2. Creación de hosts

El host son los dispositivos que van a ser monitoreados, antes de crear el host es necesario que el dispositivo ya tenga activado al protocolo SNMP y configurada la comunidad de gestión.

- 1) Para crear un nuevo host ingresar en la interfaz web a: *Configuración* → *Hosts* → *Create host*

The screenshot shows the Zabbix web interface. The 'Configuration' menu is highlighted in red, and the 'Hosts' sub-menu is selected. The 'Create host' button is also highlighted in red. The page displays a table of existing hosts with columns for Name, Applications, Items, Triggers, Graphs, Discovery, Web, Interface, Templates, Status, Availability, and Agent encryption.

Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info
SW-CRONOS	Applications 2	Items 230	Triggers 28	Graphs 28	Discovery 1	Web		Template SNMP Device (Template SNMP Generic, Template SNMP Interfaces)	Enabled	ZBX, SNMP, JMX, IPMI	NONE	
SW-Zeus-Primario	Applications 2	Items 4342	Triggers 542	Graphs 542	Discovery 1	Web		Template SNMP Device (Template SNMP Generic, Template SNMP Interfaces)	Enabled	ZBX, SNMP, JMX, IPMI	NONE	
Zabbix server	Applications 11	Items 63	Triggers 42	Graphs 10	Discovery 2	Web		Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Disabled	ZBX, SNMP, JMX, IPMI	NONE	

Figura K 6. Hosts

Fuente: Captura de Zabbix

- 2) En la pestaña *Host* se podrá configurar el nombre del dispositivo, en este ejemplo se trata del SWITCH-ATENEA. Se debe añadir al host a un determinado grupo, en este caso el grupo es *Switches Cisco* sin embargo se puede añadir a otro grupo ya existente o crear uno nuevo en el campo *New group*.

Si se trata de un dispositivo de red se debe remover el campo *Agent Interfaces*. Luego dirigirse a *SNMP interfaces* y configurar la dirección IP del dispositivo. El puerto 161 está configurado por defecto.

Si se trata de otro tipo de dispositivos que requieren la instalación de un agente, la configuración se realiza en *Agent interfaces*, en donde se configura la dirección IP.

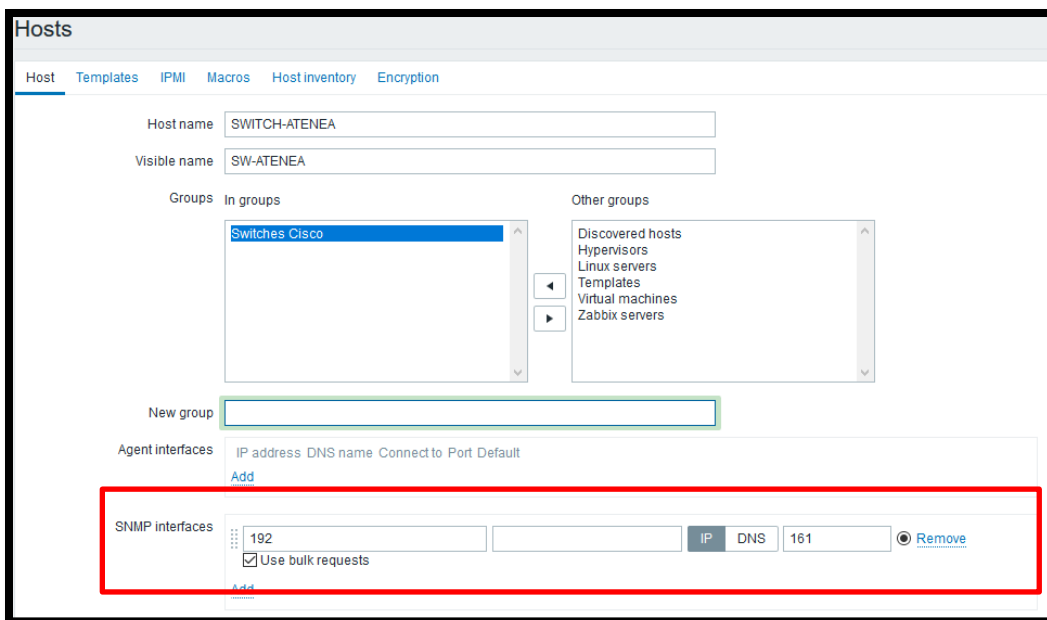


Figura K 7. Configuración de host

Fuente: Captura de Zabbix

- 3) Dirigirse a la pestaña *Macros*. En el campo *Macro* ingresar: `{$SNMP_COMMUNITY}`. En el campo *Value* se debe ingresar el nombre de la comunidad de gestión que está configurada en el dispositivo a monitorear.

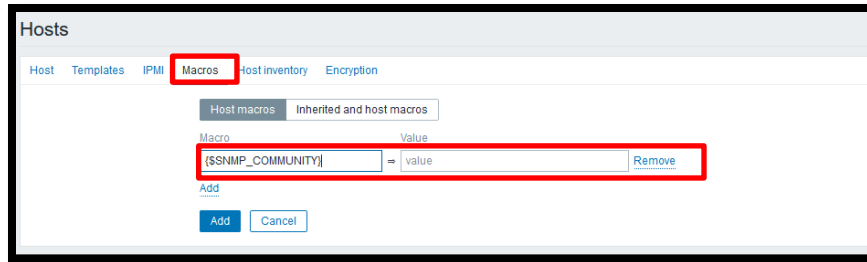


Figura K 8. Ingreso de la comunidad SNMP

Fuente: Captura de Zabbix

- 4) Dirigirse a la pestaña *Templates*, en donde se pueden añadir plantillas ya configuradas para los distintos tipos de host que se pueden monitorear con Zabbix. Al tratarse de un dispositivo que se monitorea mediante el protocolo SNMP se seleccionará la plantilla *Template SNMP Device*. Una vez seleccionadas las plantillas necesarias pulsar *Add*.

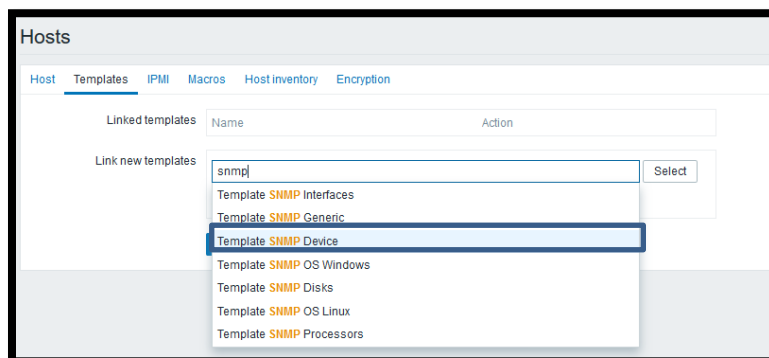


Figura K 9. Adición de plantillas

Fuente: Captura de Zabbix

- 5) Cuando se haya añadido el host aparecerá la siguiente ventana en donde se podrá constatar que el host ha sido creado.

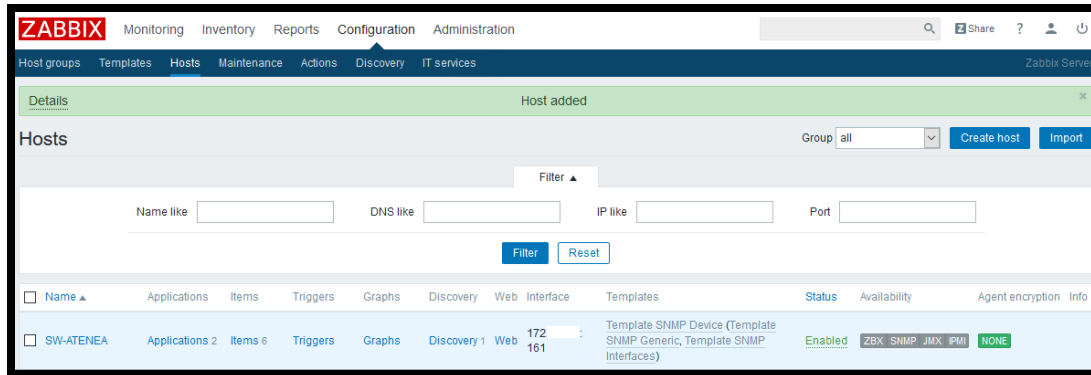


Figura K 10. Host añadido

Fuente: Captura de Zabbix

- 6) Inmediatamente no se tendrán información del dispositivo ya que le toma al software alrededor de una hora para reconocer todas las interfaces. Cuando haya terminado el reconocimiento ingresar a *Monitoring* → *Latest Data*. Al seleccionar al host se desplegará la siguiente información.

<input type="checkbox"/> Device uptime	2017-02-01 12:24:03	2 days, 04:31:12	+00:01:00	Graph
Interfaces (4337 items)				
<input type="checkbox"/> Admin status of interface FastEthernet1	2017-02-01 12:24:03	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/1	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/1--Controlled	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/1--Uncontrolled	2017-02-01 12:24:03	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/2	2017-02-01 12:24:03	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/2--Controlled	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/2--Uncontrolled	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/3	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/3--Controlled	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/3--Uncontrolled	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/4	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/4--Controlled	2017-02-01 12:24:03	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/4--Uncontrolled	2017-02-01 12:24:02	up (1)		Graph
<input type="checkbox"/> Admin status of interface GigabitEthernet1/5	2017-02-01 12:24:02	up (1)		Graph

Figura K 11. Latest data

Fuente: Captura de Zabbix

3. Creación de ítems

Los ítems se pueden crear para un host en específico o para una plantilla. Es recomendable crear el ítem dentro de una plantilla, para que éste pueda ser usado en múltiples usuarios similares.

- 1) Para crear un ítem dentro de una plantilla es necesario dirigirse a Configuration → Templates y seleccionar la plantilla en donde se va a crear el ítem

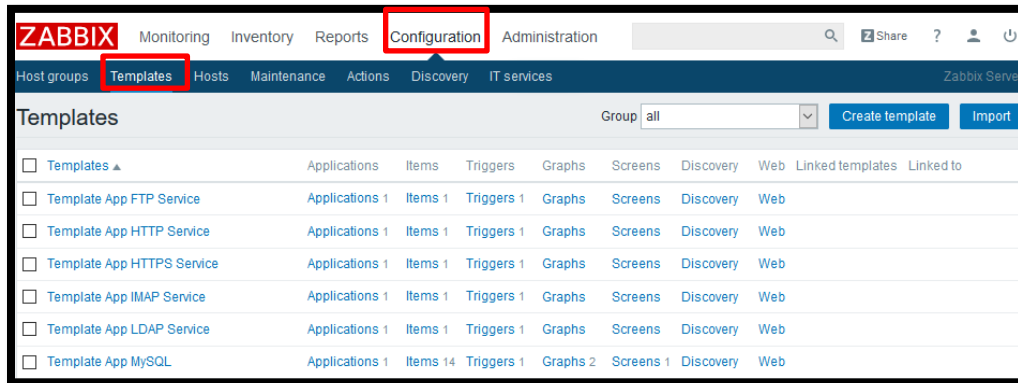


Figura K 12. Plantillas

Fuente: Captura de Zabbix

- 2) Ubicarse en la pestaña *Items* y presionar el botón *Create item*

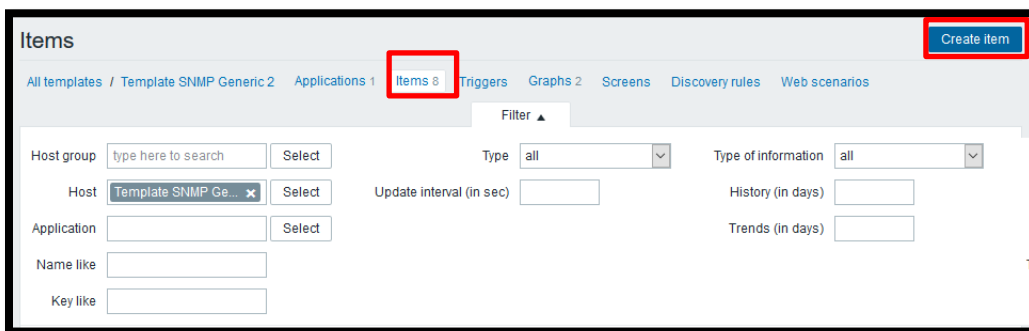


Figura K 13. Crear ítem

Fuente: Captura de Zabbix

- 3) Se desplegará una pantalla para configurar los parámetros del ítem. En este ejemplo se ven los parámetros para crear un ítem que recoja información acerca de la memoria del dispositivo. El parámetro más importante es el SNMP OID.

The screenshot shows the configuration form for a Zabbix item named 'ciscoMemoryPoolFree'. The form includes the following fields and options:

- Name: ciscoMemoryPoolFree
- Type: SNMPv2 agent
- Key: CISCO-MEMORY-POOL-MIB-ciscoMemoryPoolFree
- SNMP OID: 1.3.6.1.4.1.9.9.48.1.1.1.6.1
- SNMP community: utn
- Port: 161
- Type of information: Numeric (unsigned)
- Data type: Decimal
- Units: b
- Use custom multiplier: 1
- Update interval (in sec): 300
- Custom intervals table:

Type	Interval	Period	Action
Flexible	Scheduling	50	1-7,00:00-24:00
- History storage period (in days): 30
- Trend storage period (in days): 365
- Store value: As is
- Show value: As is

Figura K 14. Parámetros del ítem

Fuente: Captura de Zabbix

4. Creación de gráficos

- 1) Dentro de un host o una plantilla seleccionar la pestaña *Graphs* y presionar el botón *Create graph*

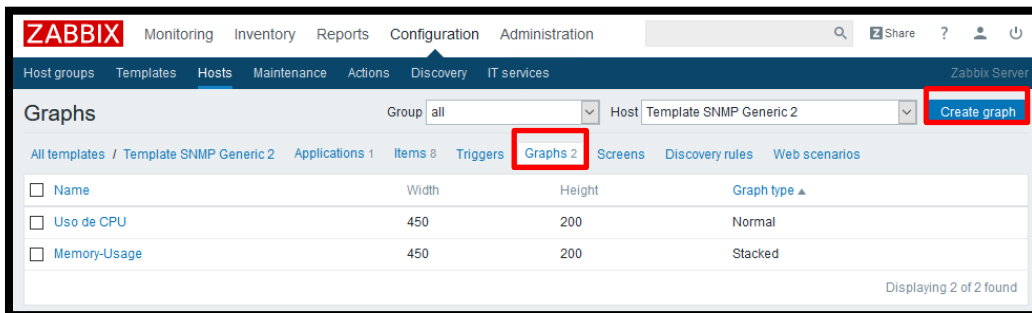


Figura K 15. Gráficos

Fuente: Captura de Zabbix

- 2) Configurar los parámetros del gráfico. Este ejemplo es la creación de un gráfico de la memoria de un dispositivo, por lo que para generar el gráfico se añadieron los ítems de memoria utilizada y de memoria libre.

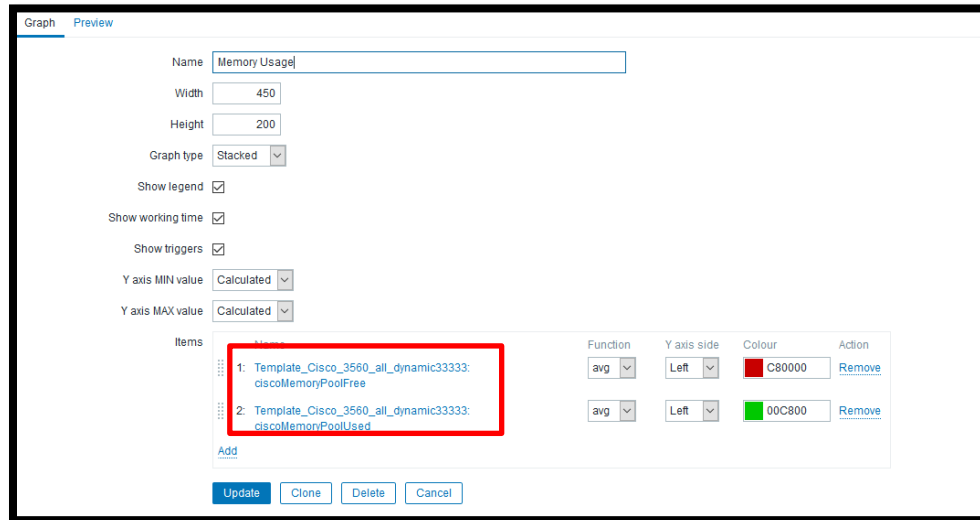


Figura K 16. Parámetros del gráfico

Fuente: Captura de Zabbix

5. Creación de escenarios web

Los escenarios web sirven para monitorear sitios web de manera externa sin la necesidad de instalar un agente o activar el protocolo SNMP en el servidor.

- 1) Primero se debe crear un nuevo host, únicamente hay que configurar el nombre y grupo. No se añade ninguna dirección IP.

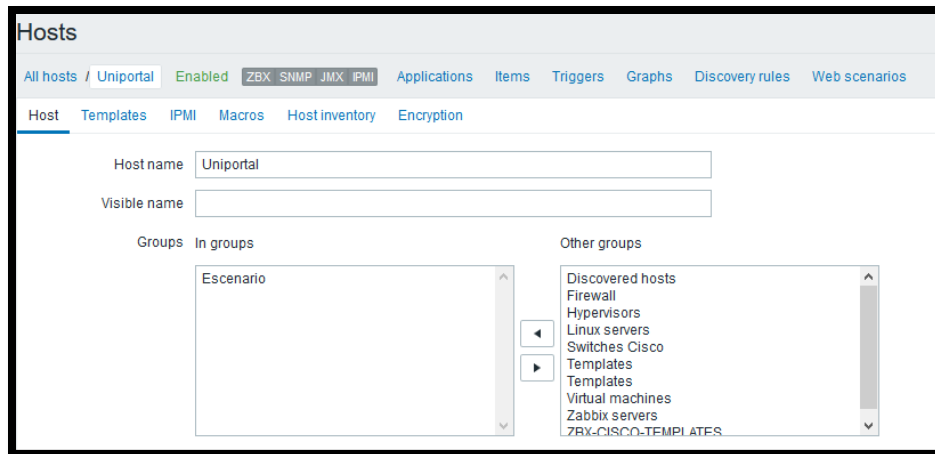


Figura K 17. Creación de host para web escenario

Fuente: Captura de Zabbix

- 2) Enlazar el host a la plantilla de monitoreo HTTP. También puede añadirse una plantilla para HTTPS.

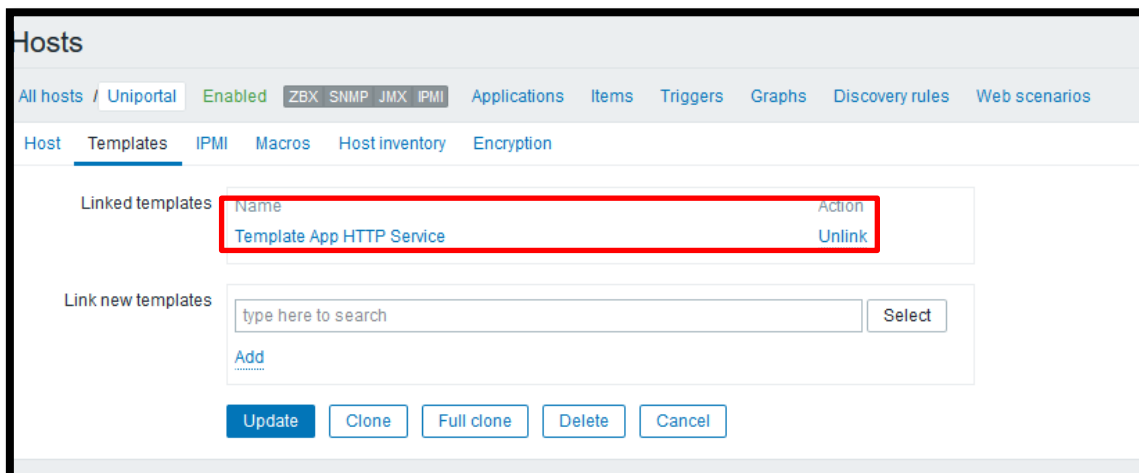


Figura K 18. Adición de plantilla HTTP

Fuente: Captura de Zabbix

- 3) Se procede a crear un escenario web dentro del host

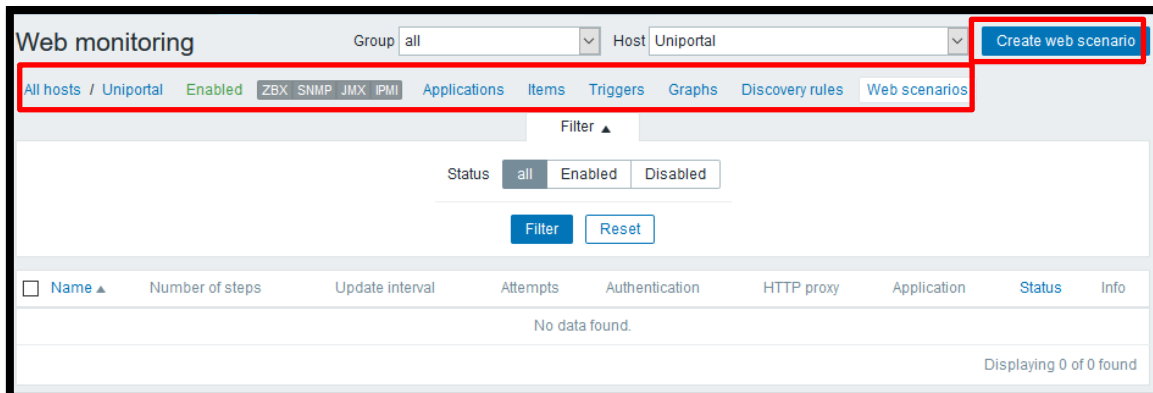


Figura K 19. Creación de escenario

Fuente: Captura de Zabbix

- 4) Configurar los parámetros del escenario. Es necesario que se seleccione la aplicación HTTP service

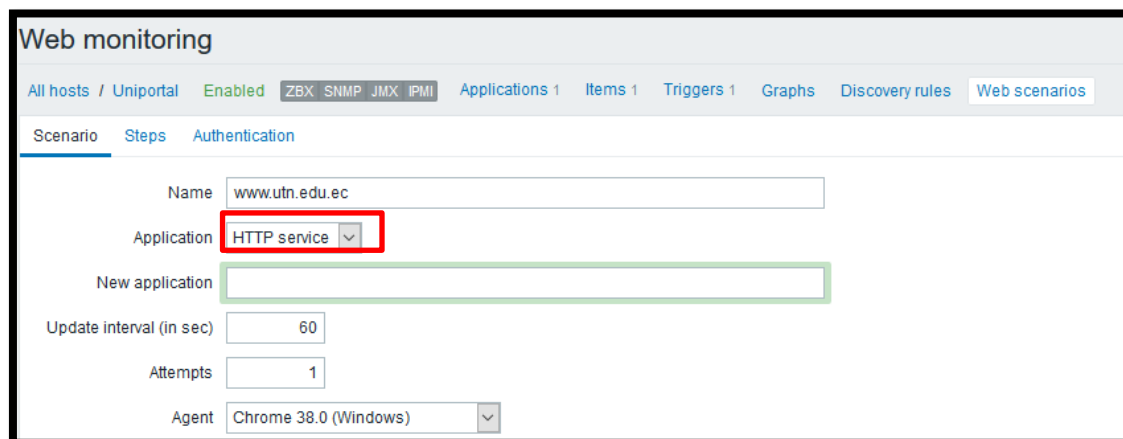


Figura K 20. Configuración del escenario

Fuente: Captura de Zabbix

- 5) Crear los pasos del escenario ubicándose en *Steps* → *Add*

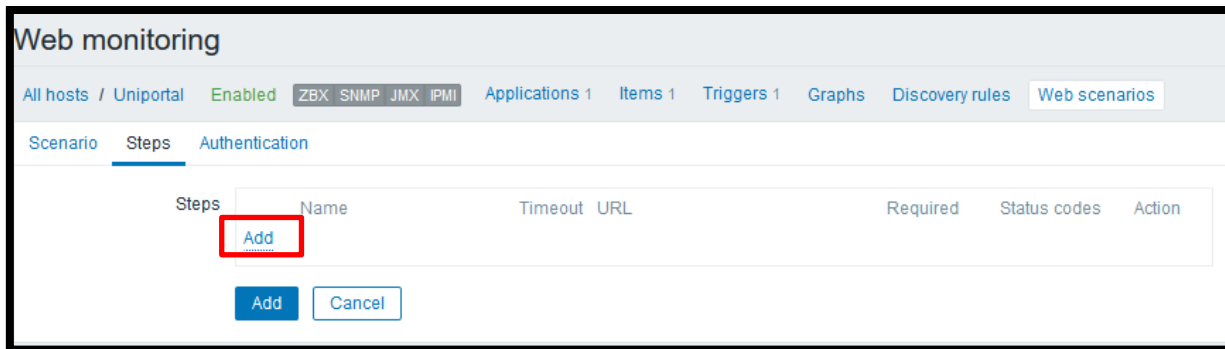


Figura K 21. Steps

Fuente: Zabbix

- 6) Parecerá otra ventana en donde se configura principalmente el URL del sitio Web. También es necesario fijar un valor de 200 en *Required status codes*.

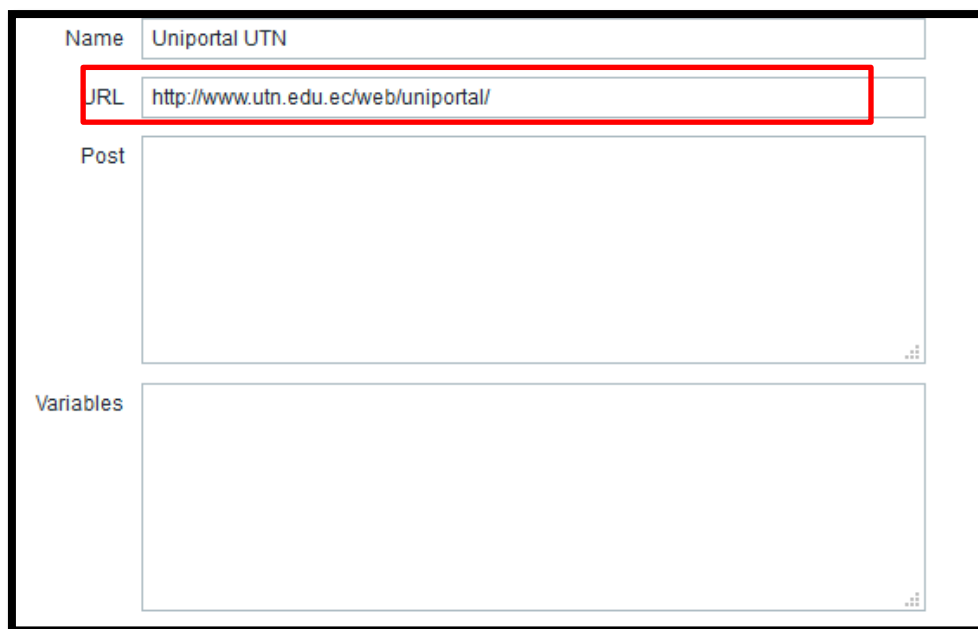


Figura K 22. Parámetros del step

Fuente: Captura de Zabbix

- 7) Al pulsar *Add*, el step se habrá creado con los parámetros configurados.

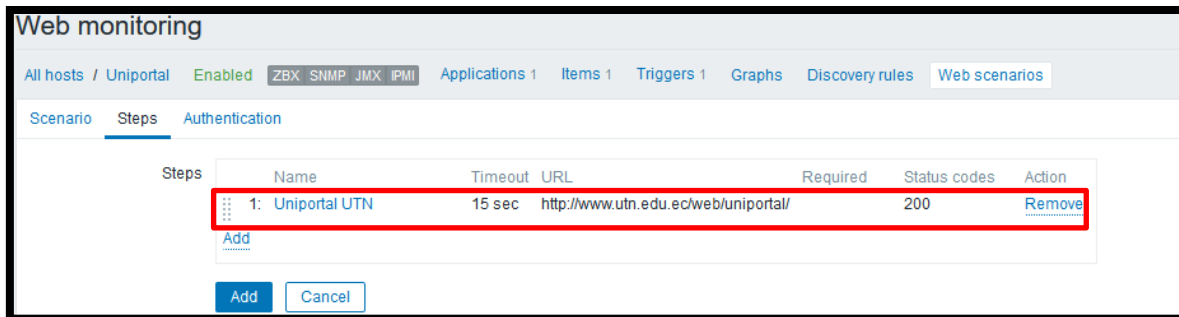


Figura K 23. Adición del step

Fuente: Zabbix

8) El escenario se habrá creado

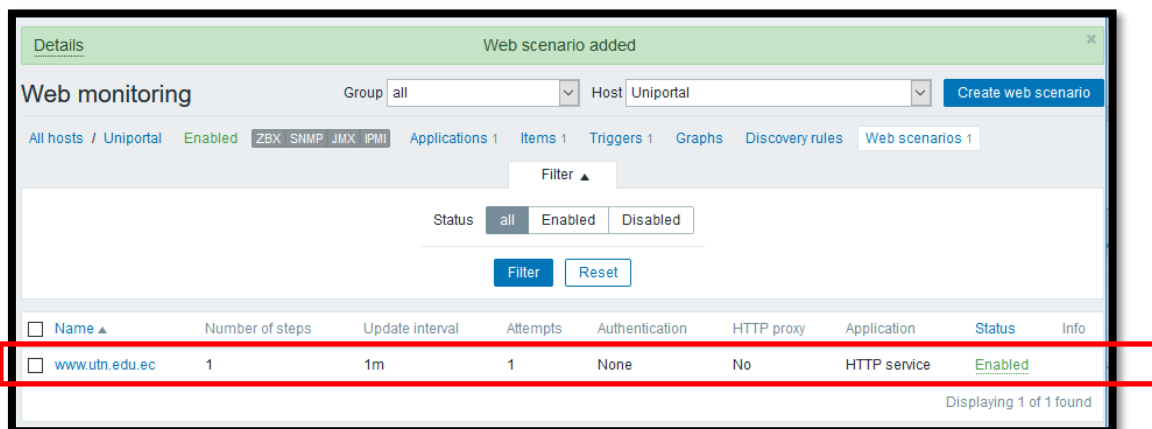


Figura K 24. Escenarios activados

Fuente: Zabbix

Dentro de la ventana *Latest Data* será posible ver los datos recogidos del sitio Web

Name	Last check	Last value	Change
HTTP service (6 Items)			
Download speed for scenario "www.utn.edu.ec".	2017-02-16 12:44:46	61.57 KBps	-500 Bps Graph
Download speed for step "Uniportal UTN" of scenario "www.utn.edu.ec".	2017-02-16 12:44:46	61.57 KBps	-500 Bps Graph
Failed step of scenario "www.utn.edu.ec".	2017-02-16 12:44:46	0	Graph
HTTP service is running	2017-02-16 12:45:23	Up (1)	Graph
Response code for step "Uniportal UTN" of scenario "www.utn.edu.ec".	2017-02-16 12:44:46	200	Graph
Response time for step "Uniportal UTN" of scenario "www.utn.edu.ec".	2017-02-16 12:44:46	1s 269.6ms	+10ms Graph

Figura K 25. Datos obtenidos en el escenario

Fuente: Zabbix

ANEXO L. Instalación de OTRS

1) Actualizar el Sistema Operativo

```
yum -y update
```

2) Instalar Apache

```
yum -y install epel-release  
yum -y install httpd mod_perl
```

3) Configurar la autoiniciación de Apache

```
/sbin/chkconfig httpd on  
service httpd start  
firewall-cmd --zone=public --add-port=80/tcp --permanent  
firewall-cmd --reload
```

4) Instalar MaríaDB

```
yum -y install mariadb mariadb-server  
/sbin/chkconfig mariadb on  
service mariadb start  
mysql_secure_installation
```

5) Editar el archivo /etc/my.cnf

```
vi /etc/my.cnf  
    max_allowed_packet = 20M  
    query_cache_size = 32M  
    innodb_log_file_size = 256M
```

6) Resetear MariaDB con los siguientes comandos

```
service mariadb stop  
rm /var/lib/mysql/ib_logfile0  
rm /var/lib/mysql/ib_logfile1  
service mariadb start
```

7) Instalar SEMANAGE

```
yum install policycoreutils-python
```

8) Descargar OTRS

```
yum -y install wget bzip2
```

9) Acceder a la carpeta /opt y descargar los paquetes

```
cd /opt
wget https://ftp.otrs.org/pub/otrs/otrs-5.0.18.tar.bz2
```

10) Descomprimir con los siguientes comandos

```
tar jxvpf otrs-5.0.18.tar.bz2
mv otrs-5.0.18 otrs
```

11) Crear un usuario OTRS

```
useradd -d /opt/otrs/ -c 'OTRS user' otrs
usermod -G apache otrs
```

12) Instalar los módulos Perl con los siguientes comandos

```
cd /opt/otrs
```

```
sudo yum -y install "perl(ExtUtils::MakeMaker)" "perl(Sys::Syslog)" "perl(Archive::Tar)"
"perl(Archive::Zip)" "perl(Crypt::Eksblowfish::Bcrypt)" "perl(Crypt::SSLeay)"
"perl(Date::Format)" "perl(DBD::Pg)" "perl(Encode::HanExtra)" "perl(IO::Socket::SSL)"
"perl(JSON::XS)" "perl(Mail::IMAPClient)" "perl(IO::Socket::SSL)" "perl(ModPerl::Util)"
"perl(Net::DNS)" "perl(Net::LDAP)" "perl(Template)" "perl(Template::Stash::XS)"
"perl(Text::CSV_XS)" "perl(Time::Piece)" "perl(XML::LibXML)" "perl(XML::LibXSLT)"
"perl(XML::Parser)" "perl(YAML::XS)"
```

13) Realizar la configuración y asignación de permisos

```
sudo -i
cd /opt/otrs/
cp Kernel/Config.pm.dist Kernel/Config.pm

ln -s /opt/otrs/scripts/apache2-httpd.include.conf
/etc/httpd/conf.d/zzz_otrs.conf
/opt/otrs/bin/otrs.SetPermissions.pl --web-group=apache
systemctl restart httpd.service
```

14) Deshabilitar SELINUX

```
vi /etc/selinux/config
```

```
SELINUX=disabled
```

15) Instalar OTRS vía Web

Digitar la dirección IP del servidor OTRS seguido de /otrs/installer.pl

Seleccionar Next

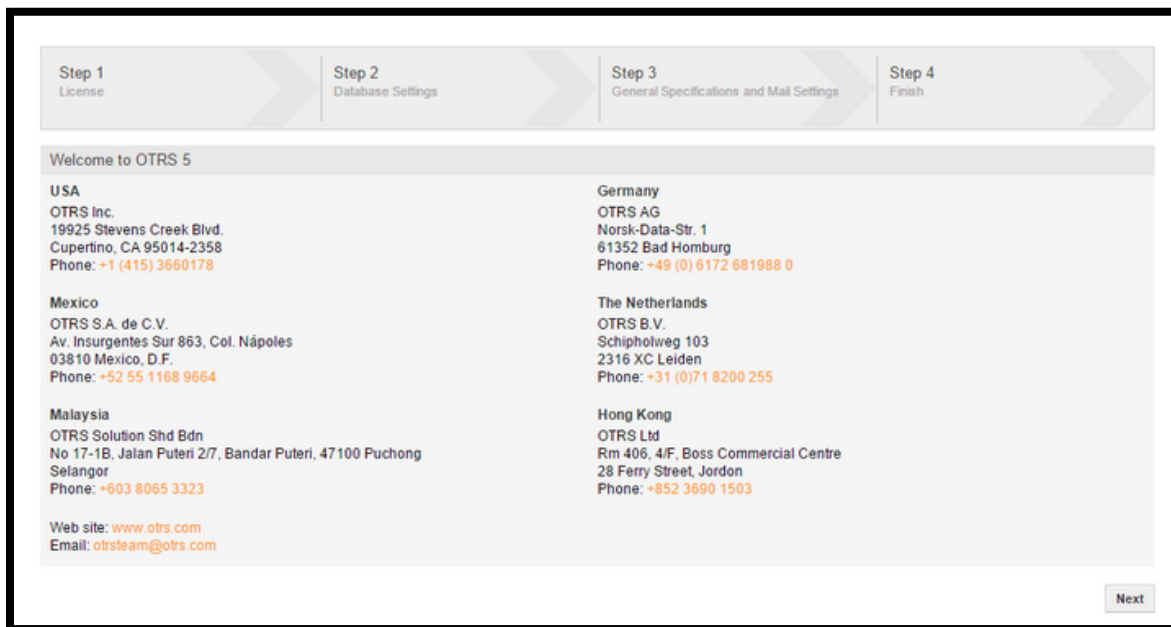


Figura L.1. Inicio de la instalación OTRS

Fuente: Captura de OTRS

Hacer Clic en “Accept license and continue”

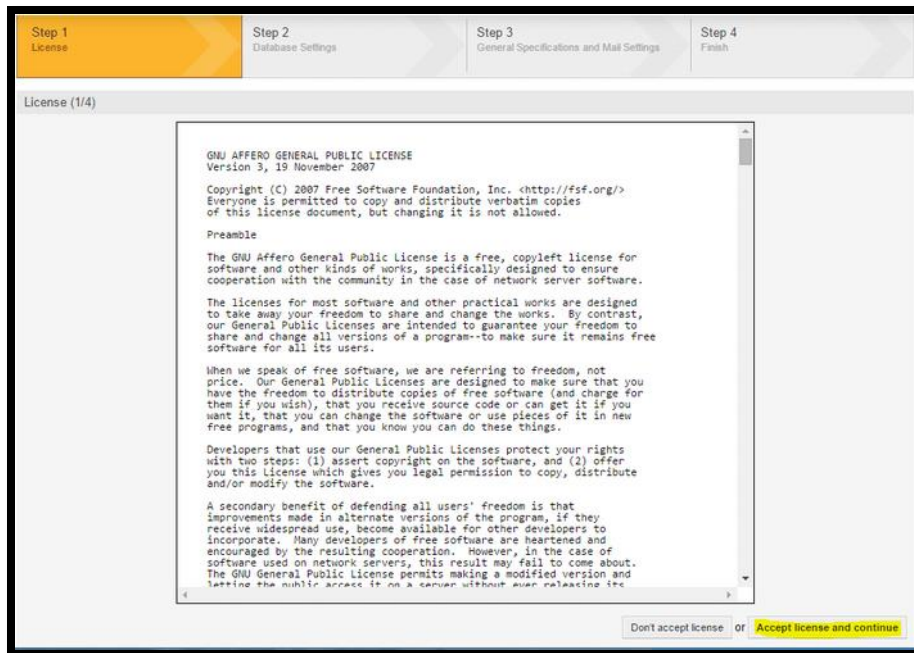


Figura L 2. Licencia OTRS

Fuente: Captura de OTRS

Seleccionar MySQL y marcar la opción “Create a new database for OTRS”

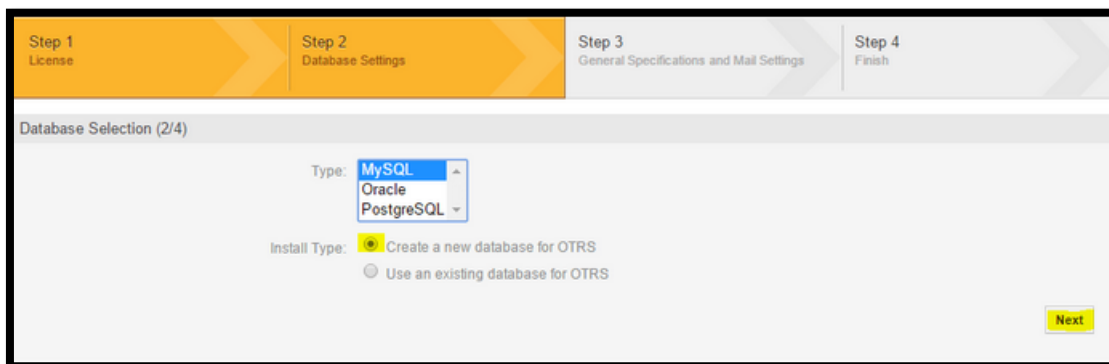


Figura L 3. Configuración de base de datos

Fuente: Captura de OTRS

Digitar la contraseña de root y seleccionar “Check database settings”

Figura L 4. Configuración MySQL

Fuente: Captura de OTRS

Ingresar la contraseña del usuario otrs y seleccionar Next.

Figura L 5. Verificación de configuración de la base de datos

Fuente: Captura de OTRS

Si la instalación es exitosa se tendrá la siguiente imagen

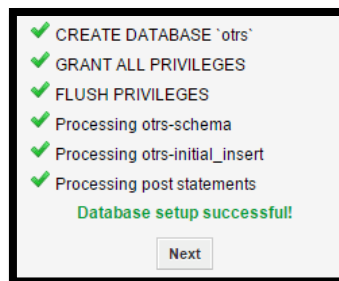


Figura L 6. Revisión de requerimientos

Fuente: Captura de OTRS

Al finalizar se presentará la página de inicio, usuario y contraseña

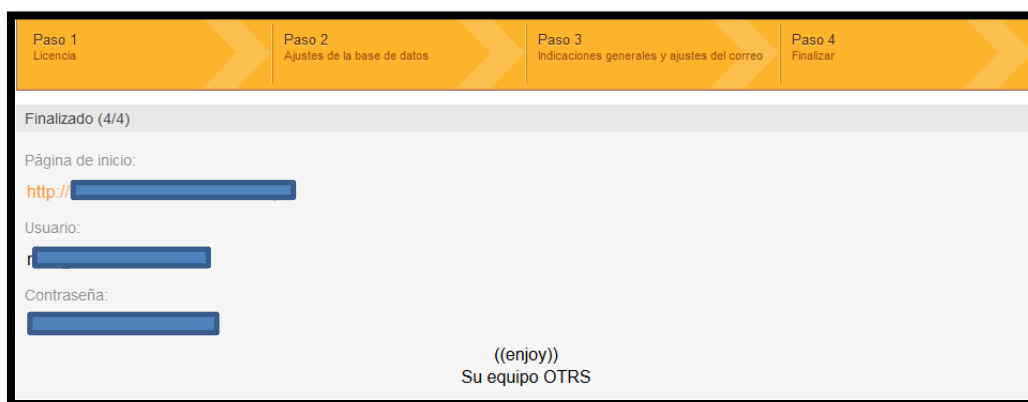


Figura L 7. Final de la instalación.

Fuente: Captura de OTRS

Ingreso a OTRS a través del usuario y contraseña presentados en el paso anterior

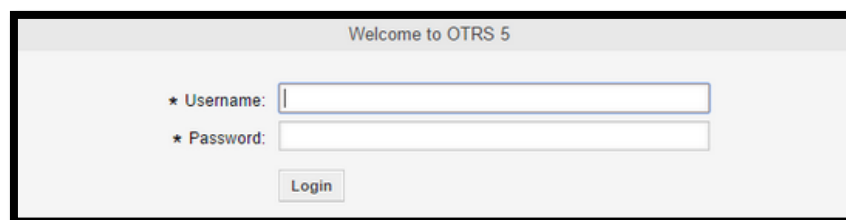


Figura L 8. Ingreso a la aplicación OTRS

Fuente: OTRS

Al acceder se puede visualizar el Dashboard del servidor

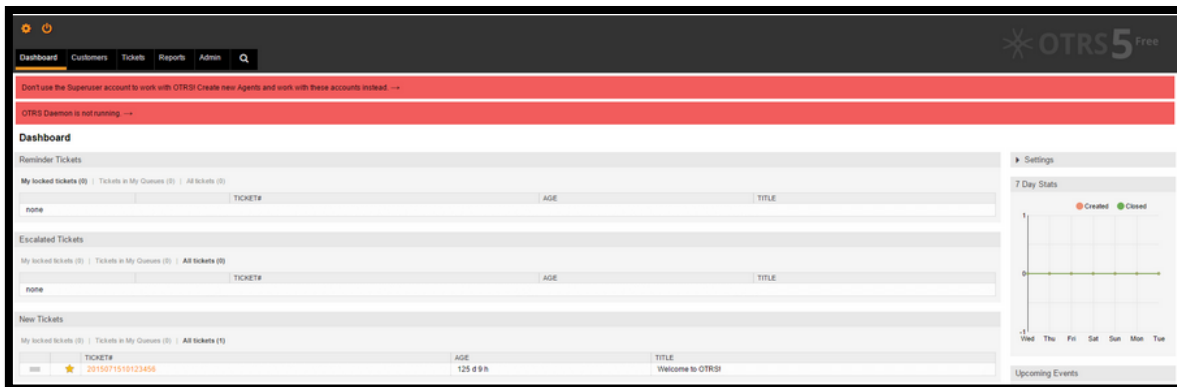


Figura L 9. Dashboard de OTRS

Fuente: OTRS

Configuración del Daemon

```
sudo cp /opt/otrs/var/cron/otrs_daemon.dist /opt/otrs/var/cron/otrs_daemon
```

```
sudo /opt/otrs/bin/Cron.sh start otrs
```

Creación de usuarios clientes

Seleccionar la pestaña *Clientes* y la opción *Añadir usuario cliente*

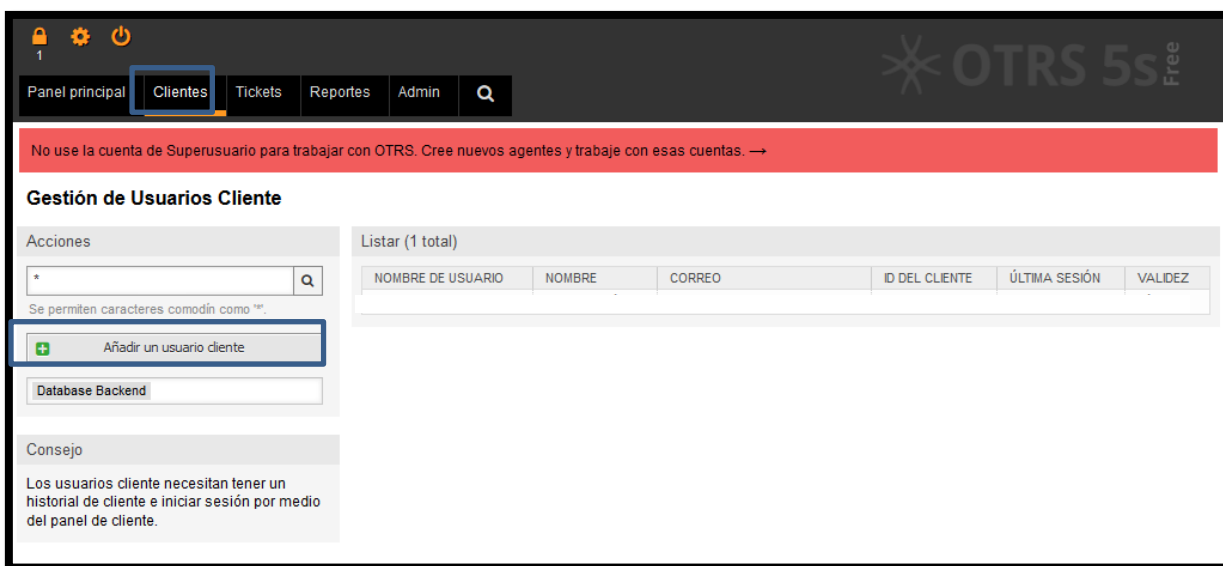


Figura L 1. Clientes

Fuente: Captura de OTRS

Llenar los campos referentes a la información del cliente

The screenshot shows a web interface titled "Gestión de Usuarios Cliente". On the left, there are navigation buttons: "Ir a la vista general" and "Volver a los resultados de la búsqueda". Below these is a "Consejo" section with a message: "Los usuarios cliente necesitan tener un historial de cliente e iniciar sesión por medio del panel de cliente." The main area is titled "Añadir Usuario Cliente" and contains a form with the following fields: "Título o saludo:", "* Nombre:", "* Apellido:", "* Nombre de usuario:", "Contraseña:", "* Correo:", and "* ID del cliente:". The form fields are highlighted with a blue border.

Figura L 2. Información del cliente

Fuente: OTRS

Creación de tickets

Para crear un Nuevo ticket es necesario ubicarse en la pestaña *Tickets* → *Nuevo Ticket por correo*.



Figura L 3. Creación de Tickets

Fuente: OTRS

Se deben llenar los campos necesarios para proporcionar información del ticket, como el usuario, asunto y descripción.

Crear un nuevo ticket por correo electrónico

Todos los campos marcados con un asterisco (*) son obligatorios.

* De la cola:

* Al usuario cliente:

Copia:

Copia oculta:

ID del cliente:

Propietario:

* Asunto:

Opciones: [Libreta de direcciones] [Usuario del cliente]

* Texto:

Formato Fuente Tam... Fuente HTML

Información del cliente
ninguno

Figura L 4. Detalles del ticket

Fuente: Captura de OTRS

El usuario puede encontrarse en *[Usuario del cliente]*, en donde se proporciona una lista de todos los usuarios que se han agregado hasta el momento.

Gestión de Usuarios Cliente

Acciones

*

Se permiten caracteres comodín como *.

Consejo

Los usuarios cliente necesitan tener un historial de cliente e iniciar sesión por medio del panel de cliente.

Listar (1 total)

NOMBRE DE USUARIO	NOMBRE	CORREO	ID DEL CLIENTE	ÚLTIM

Figura L 5. Selección del usuario cliente

Fuente: Captura de OTRS

Creación de Reportes

Al seleccionar la pestaña *Reportes* se accede a las estadísticas acerca de los tickets generados. Al seleccionar el botón *Ejecutar ahora*, es posible obtener las estadísticas con todos los detalles en formato csv.

Estadísticas » Vista general

Acciones

+ Añadir

Importar

Estadísticas

1-11 de 11

STAT#	TÍTULO	OBJETO	EXPORTAR	BORRAR	EJECUTAR
10001	List of tickets closed last month	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora
10002	New Tickets	TicketAccumulation	EXPORTAR	BORRAR	EJECUTAR ahora
10003	List of open tickets, sorted by time left until response deadline expires	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora
10004	List of tickets closed, sorted by response time.	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora
10005	List of tickets created last month	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora
10006	List of the most time-consuming tickets	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora
10007	List of open tickets, sorted by time left until escalation deadline expires	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora
10008	List of tickets closed, sorted by solution time	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora
10009	Overview about all tickets in the system	TicketAccumulation	EXPORTAR	BORRAR	EJECUTAR ahora
10010	List of open tickets, sorted by time left until solution deadline expires	Ticketlist	EXPORTAR	BORRAR	EJECUTAR ahora

Figura L 6. Creación de reportes

Fuente: OTRS

ANEXO N. Acta de entrega de Manual de políticas y procedimientos

Ibarra, 20 de junio del 2017

Señor

Ing. Juan Carlos García

DIRECTOR DDTI

De mis consideraciones:

Yo, JESSICA ESTEFANÍA BÁEZ CHEZA estudiante de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, en calidad de autora del proyecto de grado "DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE RED PARA LA RED DE ÁREA LOCAL DEL EDIFICIO CENTRAL DE LA UNIVERSIDAD TÉCNICA DEL NORTE EN BASE AL MODELO DE GESTIÓN OSI CON EL PROTOCOLO SNMP", actualmente tesista en la Dirección de Desarrollo Tecnológico e Informático cordialmente solicito, me permita hacer la entrega de las Políticas y Manuales de Procedimientos de Administración y gestión de red realizado en beneficio de la red Universitaria, con la finalidad de que esta información sea divulgada hacia los encargados en las áreas de infraestructura de red y aplicaciones, para que sea revisado y aplicado.

Atentamente,



Jessica Estefanía Báez Cheza

C.I: 1003601182

RECIBIDO 20 JUN 2017
161433 (12)