



**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**  
**FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**  
**CARRERA TELECOMUNICACIONES**

**IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RED  
BASADO EN FCAPS PARA LA PRESTACIÓN DEL SERVICIO DE  
ACCESO A INTERNET DE LA EMPRESA INTERTEC DEL  
CANTÓN RIOBAMBA.**

**Trabajo de Integración Curricular**  
Tipo: Proyecto Técnico

Presentado para optar al grado académico de:  
**INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y  
REDES**

**AUTOR:** MAURO SEBASTIÁN SAGÑAY LEÓN  
**DIRECTOR:** Ing. DIEGO FERNANDO VELOZ CHERREZ MSc.

Riobamba – Ecuador

2023

© 2023, Mauro Sebastián Sagñay León

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.

Yo, Mauro Sebastián Sagñay León, declaro que el presente Trabajo de Integración Curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Integración Curricular; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 13 de abril de 2023



**Mauro Sebastián Sagñay León**

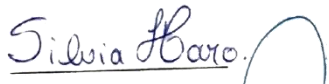
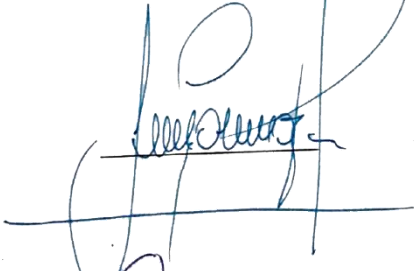
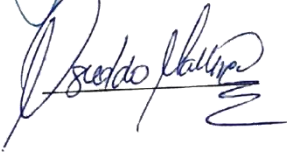
**060515101-8**

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

**FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**

**CARRERA TELECOMUNICACIONES**

El Tribunal del Trabajo de Integración Curricular certifica que: El Trabajo de Integración Curricular; Tipo: Proyecto Técnico, **“IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RED BASADO EN FCAPS PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET DE LA EMPRESA INTERTEC DEL CANTÓN RIOBAMBA”**, realizado por el señor: **MAURO SEBASTIÁN SAGÑAY LEÓN**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	FECHA
Dra. Silvia Mariana Haro Rivera <b>PRESIDENTE DEL TRIBUNAL</b>		2023-04-13
Ing. Diego Fernando Veloz Cherrez MSc. <b>DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR</b>		2023-04-13
Ing. Oswaldo Geovanny Martínez Guashima <b>ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR</b>		2023-04-13

## **DEDICATORIA**

A mis padres y hermanas, quienes estuvieron siempre presente de manera incondicional en mis fracasos y triunfos a lo largo de mi vida, cuyo apoyo a sido un pilar fundamental para cumplir con esta etapa.

Mauro Sebastián  
Sagñay León

## **AGRADECIMIENTO**

Agradezco a los docentes de la FIE - ESPOCH quienes con su conocimiento supieron ofrecerme una formación académica íntegra de calidad, a la empresa RIOBIT/INTERTEC por su colaboración para la realización de este trabajo, del mismo modo a mi director Ing. Diego Veloz por su acompañamiento en el desarrollo y culminación del presente Trabajo de Titulación y por último a mis compañeros y amigos que supieron brindar su ayuda y conocimiento para llevar a cabo este logro.

Mauro Sebastián  
Sagñay León

## ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS.....	xiii
ÍNDICE DE ILUSTRACIONES.....	xiv
ÍNDICE DE ANEXOS.....	xvii
RESUMEN.....	xviii
SUMMARY.....	xix
INTRODUCCIÓN.....	1

### CAPÍTULO I

1. DIAGNÓSTICO DE PROBLEMA.....	3
1.1. Identificación del problema.....	3
1.1.1. <i>Antecedentes de la empresa</i> .....	3
1.1.2. <i>Justificación Teórica</i> .....	4
1.2. Beneficiarios directos e indirectos.....	4
1.2.1. <i>Beneficiarios directos</i> .....	4
1.2.2. <i>Beneficiarios indirectos</i> .....	4
1.3. Localización del proyecto.....	5
1.4. Objetivos.....	5
1.4.1. <i>General</i> .....	5
1.4.2. <i>Específicos</i> .....	6

### CAPÍTULO II

2. MARCO TEÓRICO.....	7
2.1. Definición, Servicios y Arquitectura de un ISP.....	7
2.1.1. <i>Características que debe cumplir un ISP</i> .....	7
2.1.2. <i>ISP Inalámbrico</i> .....	8
2.1.3. <i>Servicios de un ISP</i> .....	8
2.1.3.1. <i>Servicio DNS (Domain Name Server)</i> .....	8
2.1.3.2. <i>Servicio FTP (File Transfer Protocol)</i> .....	9
2.1.3.3. <i>Servicio de Web Hosting</i> .....	9
2.1.3.4. <i>Servicio de Voz sobre IP</i> .....	9
2.1.3.5. <i>Servicio de Video sobre IP</i> .....	9

<b>2.1.4. Arquitectura de un ISP.....</b>	<b>9</b>
<b>2.1.5. Red de Acceso .....</b>	<b>12</b>
2.1.5.1. Línea de acceso por Fibra óptica .....	12
2.1.5.2. Línea de acceso Híbridas (HFC, HybridFiber Coaxial).....	13
2.1.5.3. Líneas de acceso inalámbricas .....	13
<b>2.1.6. Red de concentración o de borde.....</b>	<b>15</b>
<b>2.1.7. Red de troncal o backbone .....</b>	<b>15</b>
<b>2.1.8. Red de Gestión .....</b>	<b>15</b>
<b>2.2. Infraestructura de red.....</b>	<b>16</b>
<b>2.2.1. Clasificación de una red.....</b>	<b>16</b>
2.2.1.1. Según el acceso de los usuarios.....	16
2.2.1.2. Según la cobertura .....	16
2.2.1.3. Según su topología .....	17
<b>2.2.2. Componentes de una Infraestructura de red. ....</b>	<b>18</b>
<b>2.3. Sistema de gestión de red .....</b>	<b>19</b>
<b>2.3.1. Modelos de gestión de red.....</b>	<b>19</b>
2.3.1.1. Modelo de gestión TMN .....	20
2.3.1.2. Modelo de gestión OSI (FCAPS).....	20
2.3.1.3. Modelo de gestión de Internet .....	21
<b>2.3.2. Elementos de un sistema de gestión de redes .....</b>	<b>22</b>
2.3.2.1. Gestor.....	22
2.3.2.2. Agente.....	22
2.3.2.3. Protocolo de comunicación .....	23
2.3.2.4. Base de Información de Gestión (MIB) .....	23
<b>2.4. Protocolo Simple de Gestión de Red (SNMP).....</b>	<b>25</b>
<b>2.4.1. Funcionamiento del protocolo SNMP .....</b>	<b>25</b>
<b>2.4.2. Versiones SNMP.....</b>	<b>26</b>
<b>2.4.3. Mensaje SNMP.....</b>	<b>27</b>
<b>2.4.4. Comandos básicos .....</b>	<b>28</b>
<b>2.4.5. GetRequest.....</b>	<b>29</b>
<b>2.4.6. GetNextRequest .....</b>	<b>29</b>
<b>2.4.7. SetRequest.....</b>	<b>29</b>
<b>2.4.8. GetResponse.....</b>	<b>29</b>
<b>2.4.9. Trap.....</b>	<b>29</b>
<b>2.4.10. GetBulkRequest.....</b>	<b>30</b>
<b>2.4.11. InformRequest.....</b>	<b>30</b>



<b>2.5. Modelo de gestión ISO/FACPS.....</b>	<b>30</b>
<b>2.5.1. Gestión de Fallos / Fault.....</b>	<b>31</b>
2.5.1.1. <i>Gestión de fallos pasiva.....</i>	32
2.5.1.2. <i>Gestión de fallos activa.....</i>	32
<b>2.5.2. Gestión de Configuración / Configuration.....</b>	<b>32</b>
<b>2.5.3. Gestión de Contabilidad / Administración.....</b>	<b>33</b>
<b>2.5.4. Gestión de Rendimiento / Performance.....</b>	<b>33</b>
<b>2.5.5. Gestión de Seguridad / Security.....</b>	<b>33</b>
<b>2.6. Servidor.....</b>	<b>34</b>
<b>2.6.1. Funcionamiento.....</b>	<b>34</b>
<b>2.6.2. Tipo de servidores.....</b>	<b>35</b>
2.6.2.1. <i>Servidor de archivos.....</i>	35
2.6.2.2. <i>Servidor proxy.....</i>	35
2.6.2.3. <i>Servidor de base de datos.....</i>	35
2.6.2.4. <i>Servidor web.....</i>	36
2.6.2.5. <i>Servidor DNS.....</i>	36
2.6.2.6. <i>Servidor de aplicaciones.....</i>	36
2.6.2.7. <i>Servidores de Supervisión y administración.....</i>	36
<b>2.6.3. Ubuntu Server LTS.....</b>	<b>36</b>
<b>2.7. Herramientas de monitoreo de red.....</b>	<b>37</b>
<b>2.7.1. Nagios Core.....</b>	<b>38</b>
2.7.1.1. <i>Requerimientos mínimos para la instalación de Nagios Core.....</i>	40

## CAPÍTULO III41

<b>3. MARCO METODOLÓGICO.....</b>	<b>41</b>
<b>3.1. Situación actual de la empresa.....</b>	<b>41</b>
3.1.1. <i>Portafolio de servicios.....</i>	41
3.1.2. <i>Topología de la red de Intertec.....</i>	42
<b>3.2. Requerimientos que debe cubrir el sistema de gestión de red.....</b>	<b>43</b>
<b>3.3. Implementación de la herramienta de monitoreo Nagios Core.....</b>	<b>44</b>
3.3.1. <i>Instalación del software Nagios Core.....</i>	44
3.3.2. <i>Configurando Nagios Core.....</i>	47
3.3.2.1. <i>Archivo de Configuración Principal / Main Configuration File.....</i>	48
3.3.2.2. <i>Archivos de Recursos / Resource Files.....</i>	48
3.3.2.3. <i>Archivos de Definición de Objetos / Object Definition Files.....</i>	48

3.3.2.4. Archivos de Configuración CGI / CGI Configuration File .....	48
<b>3.3.3. Objetos en Nagios .....</b>	<b>48</b>
3.3.3.1. Definición de objetos .....	49
3.3.3.2. Definición de un host .....	49
3.3.3.3. Definición de un servicio .....	50
<b>3.3.4. Instalación de PNP4Nagios para la generación de gráficos .....</b>	<b>50</b>
<b>3.3.5. Monitoreo de Equipos .....</b>	<b>54</b>
3.3.5.1. Monitoreo de pérdida de paquetes y RTA.....	55
3.3.5.2. Monitoreo de información de estatus mediante SNMP.....	55
<b>3.3.6. Gráficas de Tráfico.....</b>	<b>56</b>
<b>3.3.7. Topología de Red.....</b>	<b>56</b>
<b>3.3.8. Integración de Notificaciones .....</b>	<b>56</b>
3.3.8.1. Utilización de Telegram con Nagios Core.....	57
3.3.8.2. Creación de un bot en Telegram.....	57
3.3.8.3. Envío de notificaciones de Nagios con Telegram .....	58
<b>3.3.9. WinSCP .....</b>	<b>59</b>
<b>3.4. Establecimiento de políticas de gestión de red.....</b>	<b>60</b>
3.4.1. Descripción de las políticas .....	60
3.4.2. Desarrollo de las políticas de gestión de red .....	60
3.4.3. Generalidades .....	60
3.4.4. Niveles Organizacionales .....	61
3.4.5. Vigencia .....	61
3.4.6. Referencia.....	61
3.4.7. Políticas de gestión de red para la empresa Intertec.....	62
3.4.8. Términos y definiciones.....	63
<b>3.5. Desarrollo de políticas de gestión de red para la empresa Intertec .....</b>	<b>63</b>
3.5.1. Política de gestión de red.....	63
3.5.2. Política de gestión de fallos .....	64
3.5.3. Políticas de gestión de configuración.....	65
3.5.4. Política de gestión de contabilidad / administración.....	66
3.5.5. Políticas de gestión de desempeño / performance .....	67
3.5.6. Políticas de gestión de seguridad.....	67
 <b>CAPÍTULO IV69</b>	
<b>4. RESULTADOS.....</b>	<b>69</b>

<b>4.1. Cumplimiento de parámetros FCAPS .....</b>	<b>69</b>
<b>4.2. Implementación en Gestión de Fallas .....</b>	<b>69</b>
<b>4.2.1. Manejo de Fallas .....</b>	<b>69</b>
4.2.1.1. <i>Detección de Fallas.....</i>	69
4.2.1.2. <i>Aislamiento de Fallas.....</i>	71
4.2.1.3. <i>Corrección de Fallas.....</i>	72
4.2.1.4. <i>Envío de notificaciones de alerta.....</i>	74
4.2.1.5. <i>Filtrado de alertas.....</i>	74
4.2.1.6. <i>Generación de Alertas.....</i>	75
<b>4.2.2. Pruebas de Diagnóstico .....</b>	<b>76</b>
<b>4.2.3. Manejo de Errores.....</b>	<b>76</b>
4.2.3.1. <i>Estadísticas de errores .....</i>	76
<b>4.3. Implementación en Gestión de Configuración .....</b>	<b>77</b>
<b>4.3.1. Supervisar y hacer cumplir las normas de entrada y salida de equipos. ....</b>	<b>77</b>
4.3.1.1. <i>Entrada de equipos al sistema de gestión.....</i>	77
4.3.1.2. <i>Configuración SNMP .....</i>	78
<b>4.3.2. Conservar los datos de configuración y mantenimiento en un inventario actualizado de todos los componentes de la red.....</b>	<b>78</b>
4.3.2.1. <i>Backup de seguridad de configuración de red.....</i>	79
4.3.2.2. <i>Registro e informe de cambios en las configuraciones.....</i>	80
<b>4.3.3. Configuración remota. ....</b>	<b>80</b>
<b>4.4. Implementación en Gestión de Contabilidad / Administración .....</b>	<b>81</b>
<b>4.4.1. Administración del uso de recursos de red.....</b>	<b>81</b>
4.4.1.1. <i>Establecimiento de usuarios autorizados. ....</i>	81
4.4.1.2. <i>Establecimiento de cronograma de ventanas de mantenimiento para los distintos equipos.....</i>	82
<b>4.5. Implementación en Gestión de Rendimiento .....</b>	<b>82</b>
<b>4.5.1. Captura de datos o variables indicadoras de rendimiento .....</b>	<b>82</b>
4.5.1.1. <i>Establecimiento de los parámetros de rendimiento .....</i>	82
<b>4.5.2. Análisis de los datos para determinar los niveles deseados de rendimiento .....</b>	<b>83</b>
4.5.2.1. <i>Parámetros medidos en equipos del Core .....</i>	84
4.5.2.2. <i>Parámetros medidos en equipos Concentradores.....</i>	86
4.5.2.3. <i>Parámetros medidos en los equipos Punto a Punto (PTP).....</i>	88
4.5.2.4. <i>Parámetros medidos en los equipos Radio Base (RB).....</i>	91
4.5.2.5. <i>Medición de parámetros en servidores.....</i>	93
<b>4.5.3. Generación de Reportes.....</b>	<b>93</b>

4.5.3.1. <i>Reporte de disponibilidad</i> .....	93
4.5.3.2. <i>Reporte de Tendencia</i> .....	94
4.5.3.3. <i>Reporte de Alertas</i> .....	94
<b>4.6. Implementación en Gestión de Seguridad</b> .....	<b>96</b>
4.6.1. <i>Encriptado de la información</i> .....	96
4.6.2. <i>Establecimiento de procesos de autenticación</i> .....	97
4.6.3. <i>Control de acceso a los recursos</i> .....	98
<b>4.7. Cumplimiento de las políticas de gestión de red</b> .....	<b>99</b>
<b>4.8. Implementación final del sistema de gestión de red</b> .....	<b>103</b>
4.8.1. <i>Establecimiento de grupos de host</i> .....	103
4.8.2. <i>Obtención de Reportes</i> .....	107
4.8.3. <i>Generación de Alertas</i> .....	108
4.8.4. <i>Generación de Notificaciones</i> .....	110
4.8.5. <i>Visualización de configuración de host</i> .....	111

**CONCLUSIONES**

**RECOMENDACIONES**113

**BIBLIOGRAFÍA**

**ANEXOS**

## ÍNDICE DE TABLAS

<b>Tabla 1-1:</b> Datos geográficos de la empresa Intertec. ....	5
<b>Tabla 1-2:</b> Estándares de la especificación de redes inalámbricas. ....	14
<b>Tabla 2-2:</b> Clasificación de las redes según su cobertura. ....	17
<b>Tabla 3-2:</b> Comparativa de las versiones SNMP. ....	26
<b>Tabla 4-2:</b> Comparativa entre las diferentes herramientas de monitoreo de código abierto. ....	37
<b>Tabla 1-3:</b> Servicios que ofrece la empresa Intertec. ....	41
<b>Tabla 2-3:</b> Simbología de red utilizada. ....	42
<b>Tabla 3-3:</b> Descripción de los requerimientos de monitoreo que necesita la empresa. ....	43
<b>Tabla 1-4:</b> Jerarquía de alertas dependiendo de su criticidad/nivel de prioridad en Nagios. ....	72
<b>Tabla 2-4:</b> Métodos de configuración remota que utiliza la empresa. ....	81
<b>Tabla 3-4:</b> Definición de parámetros de rendimiento. ....	82
<b>Tabla 4-4:</b> Generación de usuarios y sus respectivos privilegios. ....	99
<b>Tabla 5-4:</b> Nivel de cumplimiento en porcentaje a las políticas de gestión de red. ....	99

## ÍNDICE DE ILUSTRACIONES

<b>Ilustración 1-1:</b>	Logotipo de la empresa Intertec. ....	3
<b>Ilustración 2-1:</b>	Fachada principal de la empresa Intertec. ....	3
<b>Ilustración 3-1:</b>	Mapa de Georreferenciación de la empresa Intertec. ....	5
<b>Ilustración 1-2:</b>	Arquitectura de general de un ISP. ....	10
<b>Ilustración 2-2:</b>	Arquitectura general de un ISP Inalámbrico (WISP). ....	11
<b>Ilustración 3-2:</b>	Ejemplo de fibra óptica, donde se aprecia los hilos y el revestimiento. ....	12
<b>Ilustración 4-2:</b>	Arquitectura de una red de acceso PON. ....	13
<b>Ilustración 5-2:</b>	Arquitectura de una red de acceso inalámbrica. ....	14
<b>Ilustración 6-2:</b>	Arquitectura de una red de gestión de un ISP. ....	16
<b>Ilustración 7-2:</b>	Diseño de Topología tipo Bus. ....	17
<b>Ilustración 8-2:</b>	Topología de red tipo estrella. ....	18
<b>Ilustración 9-2:</b>	Topología de red tipo anillo. ....	18
<b>Ilustración 10-2:</b>	Arquitectura lógica por capas de TMN. ....	20
<b>Ilustración 11-2:</b>	Elementos de gestión de red. ....	22
<b>Ilustración 12-2:</b>	Árbol MIB. ....	24
<b>Ilustración 13-2:</b>	Formato de consultas y respuestas SNMP. ....	27
<b>Ilustración 14-2:</b>	Estructura SNMP PDU. ....	28
<b>Ilustración 15-2:</b>	Estructura de un PDU en un Trap. ....	29
<b>Ilustración 16-2:</b>	Modelo funcional FCAPS por la ISO para la gestión de redes. ....	31
<b>Ilustración 17-2:</b>	Solicitud de Servicios. ....	35
<b>Ilustración 18-2:</b>	Logotipo de Nagios Core. ....	39
<b>Ilustración 1-3:</b>	Topología General de la red de la empresa Intertec. ....	42
<b>Ilustración 2-3:</b>	Página Inicial de la herramienta de monitoreo Nagios Core. ....	47
<b>Ilustración 3-3:</b>	Funcionamiento de la herramienta Nagios Core. ....	47
<b>Ilustración 4-3:</b>	Integración de PNP4Nagios en la interfaz web de Nagios Core. ....	53
<b>Ilustración 5-3:</b>	Interfaz web de PNP4Nagios. ....	54
<b>Ilustración 6-3:</b>	Topología Lógica de la red de la empresa que se visualiza en el software Nagios. ....	56
<b>Ilustración 7-3:</b>	Inicio de la conversación con BotFather para la creación de un bot. ....	57
<b>Ilustración 1-4:</b>	Detección de falla en el keepalive de PING en el host PTP_GLL_SE_01. ....	69
<b>Ilustración 2-4:</b>	Registro de la pérdida de paquetes en el equipo PTP_GLL_SE_01. ....	70
<b>Ilustración 3-4:</b>	Registro del RTA en el equipo PTP_GLL_SE_01. ....	70
<b>Ilustración 4-4:</b>	Ruido presente en el equipo RB_ESP_SO_01 en un lapso de 4 horas. ....	71

<b>Ilustración 5-4:</b>	Topología dinámica usada en Nagios para aislar una falla. ....	71
<b>Ilustración 6-4:</b>	Estado del servicio monitoreado cuando se da un error. ....	73
<b>Ilustración 7-4:</b>	Mensajes recibidos en la app de Telegram sobre la recuperación de los equipos después de una caída de conexión (izquierda) y del nivel de ruido en un equipo (derecha). ....	73
<b>Ilustración 8-4:</b>	Recuperación de Hosts registrada en el Log de Nagios. ....	73
<b>Ilustración 9-4:</b>	Menú para filtrar las alertas por el tipo y por host. ....	74
<b>Ilustración 10-4:</b>	Filtrado de las alertas de host y de servicio de acuerdo a su criticidad. ....	75
<b>Ilustración 11-4:</b>	Medición del parámetro del ruido en el equipo RB_CHA_NO_01. ....	75
<b>Ilustración 12-4:</b>	Servicios monitoreados en el equipo GUA_GMT_01. ....	76
<b>Ilustración 13-4:</b>	Histograma de alertas ocurridas en el equipo GUA_GMT_01 desde el 17 de Nov hasta el 18 de Dic de 2022. ....	76
<b>Ilustración 14-4:</b>	Archivos de configuración alojados en el servidor FTP. ....	78
<b>Ilustración 15-4:</b>	Verificación en el servidor FTP de los archivos backups de los equipos concentradores. ....	80
<b>Ilustración 16-4:</b>	Acceso a WinSCP mediante SSH. ....	81
<b>Ilustración 17-4:</b>	Inicio de sesión en la Nagios Core. ....	81
<b>Ilustración 18-4:</b>	Rangos de tiempo para visualizar los gráficos de desempeño de red. ....	84
<b>Ilustración 19-4:</b>	Parámetros medidos en el host GAU_GMT_01 ubicado en el Core. ....	84
<b>Ilustración 20-4:</b>	Carga del CPU en el GUA_GMT_01 ubicado en el Core. ....	85
<b>Ilustración 21-4:</b>	Memoria del equipo Usada. ....	85
<b>Ilustración 22-4:</b>	Captura de los tiempos de PING y de las pérdidas de paquetes en el equipo. .....	86
<b>Ilustración 23-4:</b>	Medición de parámetros en el equipo Concentrador RIO_CORONA_REAL_01. ....	86
<b>Ilustración 24-4:</b>	Carga del CPU en el equipo RIO_CORONA_REAL_01. ....	87
<b>Ilustración 25-4:</b>	Memoria usada en el equipo RIO_CORONA_REAL_01. ....	87
<b>Ilustración 26-4:</b>	Tiempo de Ping y pérdida de paquetes en el equipo RIO_CORONA_REAL_01. ....	88
<b>Ilustración 27-4:</b>	Parámetros medidos en el equipo Punto a Punto PTP_ESP_SE_01. ....	88
<b>Ilustración 28-4:</b>	Intensidad de señal del equipo PTP_ESP_SE_01. ....	89
<b>Ilustración 29-4:</b>	Ruido de fondo captado en el equipo PTP_ESP_SE_01. ....	89
<b>Ilustración 30-4:</b>	Nivel de Señal a Ruido SNR del equipo PTP_ESP_SE_01. ....	90
<b>Ilustración 31-4:</b>	Tasa de transmisión del equipo PTP_ESP_SE_01. ....	90
<b>Ilustración 32-4:</b>	Tasa de recepción del equipo PTP_ESP_SE_01. ....	90
<b>Ilustración 33-4:</b>	Parámetros medidos en el equipo Radio Base RB_GLL_SE_01. ....	91

<b>Ilustración 34-4:</b> Intensidad de señal en el equipo RB_GLL_SE_01.....	91
<b>Ilustración 35-4:</b> Nivel de SNR en el equipo RB_GLL_SE_01.....	92
<b>Ilustración 36-4:</b> Nivel de ruido captado en el equipo RB_GLL_SE_01.....	92
<b>Ilustración 37-4:</b> Medición de parámetros en el servidor NPERF.....	93
<b>Ilustración 38-4:</b> Tipos de reportes disponibles. ....	93
<b>Ilustración 39-4:</b> Reporte de disponibilidad del equipo PTP_ESP_SE_01. ....	94
<b>Ilustración 40-4:</b> Reporte de tendencia del equipo PTP_ESP_SE_01.....	94
<b>Ilustración 41-4:</b> Historial de alertas generadas en Nagios Core, en el período de una hora. ....	95
<b>Ilustración 42-4:</b> Resumen de los equipos que más alertas han generado en los últimos 7 días. .....	95
<b>Ilustración 43-4:</b> Histograma de la variación de estados ocurridos en equipo BH_GLL_RAY en el período de 7 días. ....	96
<b>Ilustración 44-4:</b> Verificación de acceso a Nagios mediante SSH para una conexión segura. .	97
<b>Ilustración 45-4:</b> Creación de credenciales para los diferentes equipos de la red.....	97
<b>Ilustración 46-4:</b> Configuración de RADIUS en equipos Mikrotik. ....	98
<b>Ilustración 47-4:</b> Mensaje de error obtenido cuando se intenta el acceso a secciones no autorizadas.....	99
<b>Ilustración 48-4:</b> Lista Hostgroup 1 generada en la infraestructura de red.....	103
<b>Ilustración 49-4:</b> Lista Hostgroup 2 generada en la infraestructura de red.....	104
<b>Ilustración 50-4:</b> Lista Hostgroup 3 generada en la infraestructura de red.....	104
<b>Ilustración 51-4:</b> Lista Hostgroup 4 generada en la infraestructura de red.....	105
<b>Ilustración 52-4:</b> Lista de Hosts dados de Alta. ....	105
<b>Ilustración 53-4:</b> Lista de todos los servicios del host respectivo. ....	106
<b>Ilustración 54-4:</b> Vista resumida del estatus de todos los hostgrups .....	106
<b>Ilustración 55-4:</b> Resumen del estatus de los servicios de todos.....	107
<b>Ilustración 56-4:</b> Reporte de disponibilidad del host BH-CEB-RAY por 7 días.....	107
<b>Ilustración 57-4:</b> Tendencia del status del host en el periodo de 7 días. ....	108
<b>Ilustración 58-4:</b> Generación y almacenamiento de todas las alertas ocurridas en el host y servicios.....	109
<b>Ilustración 59-4:</b> Lista de opciones para obtener un reporte de las Alertas ocurridas. ....	109
<b>Ilustración 60-4:</b> Reporte de la Alertas generadas en el periodo de 7 días.....	110
<b>Ilustración 61-4:</b> Reporte de las notificaciones enviadas. ....	110
<b>Ilustración 62-4:</b> Visualización de la configuración de todos los hosts.....	111



## **ÍNDICE DE ANEXOS**

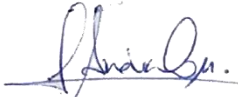
- ANEXO A:** FORMATO PARA EL CONTROL Y MANTENIMIENTO
- ANEXO B:** MANUAL DE UTILZACION DE NAGIOS CORE
- ANEXO C:** PROPUESTA PARA LA IMPLEMENTACIÓN DE NAGIOS CORE
- ANEXO D:** ACUERDO DE CONFIDENCIALIDAD

## RESUMEN

La empresa Proveedor de Servicios de Internet Intertec no cuenta con una gestión de red adecuada del servicio de acceso a internet, ocasionando problemas en la calidad y disponibilidad del mismo, afectando a la detección y resolución de fallas, además de que las decisiones que toma la gerencia, se realiza de forma casi empírica, por lo tanto, el objetivo del presente Trabajo de Integración Curricular fue implementar un sistema de gestión de red basado en el modelo de gestión FCAPS para la prestación del servicio de acceso a internet de la empresa Intertec del cantón Riobamba. En la metodología se utilizó un diseño secuencial, donde inicialmente se formuló las necesidades de gestión de la empresa mediante entrevistas con la gerencia, luego se investigó los parámetros para la implementación del modelo FCAPS; con estos datos se procedió a desarrollar políticas de gestión de red, las mismas que brindan un guía para la implementación del sistema de gestión. Cumpliendo con esta metodología se implementó el software de monitoreo Nagios Core además de otras herramientas, donde se enfocó en cumplir con las políticas establecidas basadas en el modelo FCAPS, de esta manera la empresa Intertec pudo obtener un sistema de gestión de red para el adecuado monitoreo del servicio de acceso a Internet. Por lo cual, se concluye que se pudo implementar un sistema de gestión de red basado en el modelo FCAPS mediante el desarrollo de políticas para cumplir con los parámetros de las cinco áreas funcionales del modelo, esto se pudo observar a través de una tabla donde se especifica el nivel de cumplimiento que se ha dado a las políticas.

**Palabras clave:** <GESTION DE RED>, <MONITOREO DE RED>, <POLÍTICAS DE GESTIÓN>, <TELECOMUNICACIONES>, <PROTOCOLO SNMP>, <MODELO DE GESTIÓN DE RED FCAPS >, <NAGIOS CORE (SOFTWARE)>.

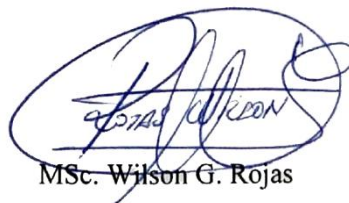


  
0541-DBRA-UPT-2023

## SUMMARY

The Internet Service Provider company Intertec does not have an adequate network management of the Internet access service, causing problems in its quality and availability, affecting the detection and resolution of failures, in addition to the decisions made by the management, is carried out almost empirically, therefore, the objective of this Curricular Integration Work was to implement a network management system based on the FCAPS management model for the provision of the Internet access service of the company Intertec in Riobamba parish. In the methodology, a sequential design was used, where initially the management needs of the company were formulated through interviews with management, then the parameters for the implementation of the FCAPS model were investigated; with these data we proceeded to develop network management policies, which provide a guide for the implementation of the management system. Complying with this methodology, the Nagios Core monitoring software was implemented in addition to other tools, where it focused on complying with the established policies based on the FCAPS model, in this way the Intertec company was able to obtain a network management system for adequate monitoring. of the Internet access service. Therefore, it is concluded that a network management system based on the FCAPS model could be implemented through the development of policies to comply with the parameters of the five functional areas of the model, this could be observed through a table where specifies the level of enforcement that has been given to the policies.

**Keywords:** <NETWORK MANAGEMENT>, <NETWORK MONITORING>, <MANAGEMENT POLICIES>, <TELECOMMUNICATIONS>, <SNMP PROTOCOL>, <FCAPS NETWORK MANAGEMENT MODEL>, <NAGIOS CORE(SOFTWARE)>.



MSc. Wilson G. Rojas

C.I. 0602361842

## INTRODUCCIÓN

Los modelos de gestión para las redes de comunicaciones fueron desarrollados con el fin de proporcionar un monitoreo adecuado de los recursos de una infraestructura tecnológica para brindar un servicio adecuado y eficiente.

El término gestión de redes es determinado por la suma de las políticas, procedimientos de diseño o planeación, configuración, intervención y monitoreo de elementos que forman parte de una red con el objetivo de certificar el eficiente y efectivo uso de los recursos, todo este proceso se evidenciará en la calidad de los servicios ofrecidos. (Terán, 2017).

Anteriormente los modelos de gestión de red eran desarrollados de tal manera que prestaban soluciones y mecanismos propietarios de distintos fabricantes, así entonces la gestión solo se podría realizar sobre los equipos y dispositivos del mismo proveedor. Para resolver esta problemática a principios de la década de los 90 se estandarizaron los primeros modelos de gestión de red de comunicaciones, estos definían protocolos y procedimientos aplicables a las distintas infraestructuras tecnológicas sin considerar el fabricante o proveedor. Existen tres modelos estándar que son actualmente los más extendidos en el mercado.

- Arquitectura TMN (Telecommunications Management Network).
- Modelo de gestión OSI (FCAPS).
- Modelo de gestión de Internet.

Estos tres modelos sirven como base para el desarrollo de sistemas de gestión dirigido a solucionar las distintas necesidades de las infraestructuras tecnológicas, estos sistemas son de gran importancia dentro de las redes grandes y medianas, pues su uso adecuado conlleva a un mejoramiento continuo de la calidad de servicio entregado en el usuario final.

Para realizar las operaciones de gestión se deben cumplir tareas, como detectar fallas, aislarlas y resolverlas en un tiempo mínimo posible en un bajo costo; cuando se presente un cambio de configuración no se afecte en gran medida el servicio; predecir posibles puntos de falla y evitarlos o en su defecto minimizarlos. (Martín & León de Mora, 2014).

La implementación de un sistema de gestión de red en las empresas proveedoras de internet es de gran importancia pues su giro de negocio radica en brindar el servicio de acceso a internet con la mayor calidad posible, mediante un sistema de gestión de red se logra establecer umbrales de

calidad y poder monitorear de mejor manera los posibles desperfectos que lleguen a afectar el normal funcionamiento del servicio.

## CAPÍTULO I

### 1. DIAGNÓSTICO DE PROBLEMA

#### 1.1. Identificación del problema

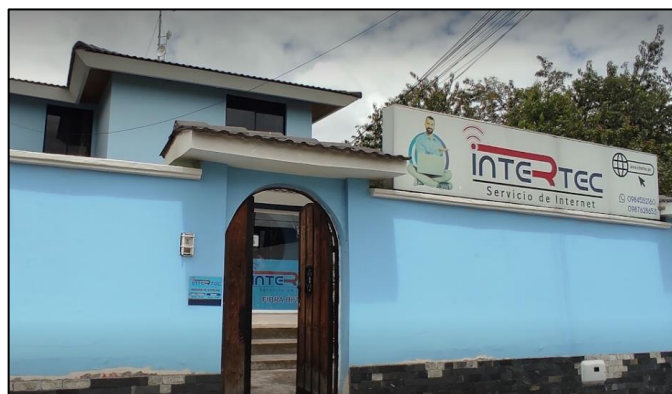
##### 1.1.1. Antecedentes de la empresa

Intertec es una empresa proveedora de servicios de internet, establecida en el año 2019 en la ciudad de Riobamba, recientemente ha experimentado un crecimiento importante del número de abonados al servicio de acceso a internet por lo que la gerencia de la empresa ha implementado nuevos equipos de red para satisfacer la creciente demanda, sin embargo los procedimientos de gestión y monitoreo de la red han sido descuidados, principalmente debido a que la empresa cuenta con personal reducido por lo que todos los esfuerzos de los mismos se enfocaban en tareas como el despliegue de la red, administración de clientes y los ámbitos financieros, entre otros aspectos. Esto da como evidencia la falta de un sistema de gestión que brinden un apoyo para garantizar tanto la calidad como la estabilidad de los servicios suministrados.



**Ilustración 1-1:** Logotipo de la empresa Intertec.

Fuente: Intertec, 2022



**Ilustración 2-1:** Fachada principal de la empresa Intertec.

Fuente: Intertec, 2022

### ***1.1.2. Justificación Teórica***

En este trabajo lo que se propone es desarrollar un apoyo para la administración y gestión de los equipos de red y su funcionamiento, que actúe además como un factor para la toma de decisiones por parte de la gerencia de la empresa Intertec. Este apoyo consiste en el diseño e implementación de un sistema de gestión de red desarrollado bajo el modelo FCAPS.

El uso de este modelo de gestión de redes, brinda un marco para simplificar los procesos para la administración, monitoreo y seguridad de las mismas, para esto se divide en cinco áreas funcionales, de aquí proviene del nombre del modelo.

- Gestión de Fallos (Fault).
- Gestión de Contabilidad (Accounting).
- Gestión de Configuración (Configuration).
- Gestión de Rendimiento (Performance)
- Gestión de Seguridad (Security)

De esta manera se puede contar con procesos adecuados para mejorar la disponibilidad del servicio, optimización de tiempos de atención a fallas, mejoramiento de niveles de la calidad de servicio de acceso a internet que percibe el cliente, además de proporcionar métricas adecuadas para la toma de decisiones por parte de los operadores de red.

## **1.2. Beneficiarios directos e indirectos**

### ***1.2.1. Beneficiarios directos***

Los beneficiarios directos de este proyecto técnico corresponden al proveedor de servicios de internet Intertec al optimizar los procesos de monitoreo de la infraestructura de red de la empresa para mejorar la calidad del servicio de acceso a internet.

### ***1.2.2. Beneficiarios indirectos***

Una vez el sistema de gestión de red sea implementado, los beneficiarios indirectos corresponden a los abonados de la empresa Intertec pues mejora la calidad de servicio percibida por el usuario final.

### 1.3. Localización del proyecto

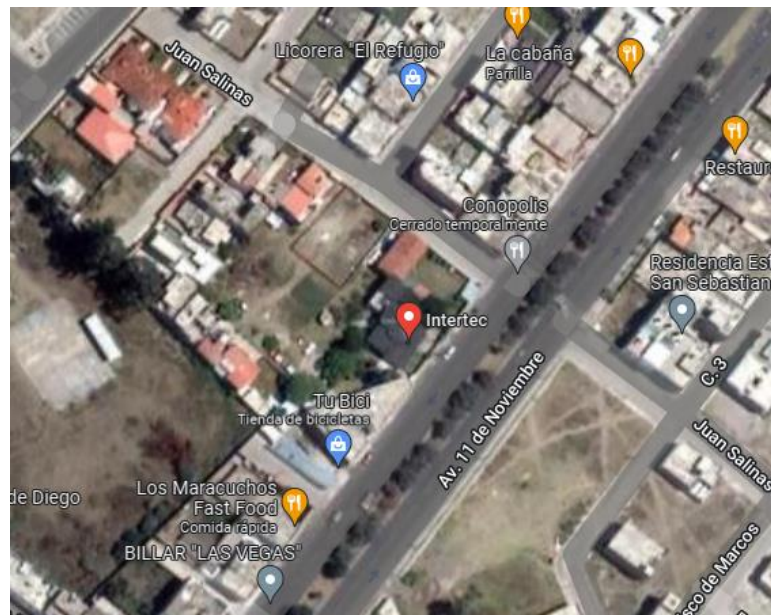
La implementación del sistema de gestión de red se realizó en el core de la infraestructura de red, dentro de las instalaciones de la empresa Intertec la misma que se ubica en la ciudad de Riobamba, provincia de Chimborazo, cuyos datos geográficos se indican en la Tabla 1-1.

**Tabla 1-1:** Datos geográficos de la empresa Intertec.

<b>Ubicación</b>	Av. 11 de Noviembre y Juan Salinas
<b>Coordenadas</b>	1°39'33,8"S 78°40'25,0"O
<b>Latitud</b>	-1,659399
<b>Longitud</b>	-78,673596
<b>Altitud</b>	2754 m.s.n.m.

Fuente: Google Maps, 2022

Realizado por: Sagñay, Mauro, 2022



**Ilustración 3-1:** Mapa de Georreferenciación de la empresa Intertec.

Realizado por: Google Maps, 2022.

### 1.4. Objetivos

#### 1.4.1. General

Implementar un sistema de gestión de red basado en FCAPS para la prestación del servicio de acceso a internet de la empresa Intertec del cantón Riobamba.



#### ***1.4.2. Específicos***

- Investigar los distintos modelos de gestión de red haciendo énfasis en el modelo FCAPS para desarrollar un sistema que pueda administrar la infraestructura de red de la empresa Intertec.
- Determinar los parámetros del modelo de gestión de red FCAPS para satisfacer las necesidades de gestión de la empresa Intertec mediante el diagnóstico actual de infraestructura de red.
- Implementar el sistema de gestión de red utilizando el modelo de gestión FCAPS en la infraestructura de la empresa Intertec para monitorear el servicio de acceso a internet y la detección de fallas.
- Evaluar el rendimiento del sistema de gestión de red mediante la realización de pruebas de funcionalidad para calibrar correctamente el sistema.

## CAPÍTULO II

### 2. MARCO TEÓRICO

#### 2.1. Definición, Servicios y Arquitectura de un ISP

En décadas anteriores el acceso a internet era dotado por medio de la red telefónica a través de dispositivos conocidos como módems, lo que permitía aprovechar la infraestructura de comunicaciones que provee las compañías telefónicas. Actualmente el transporte de datos de los clientes se lo realiza a través de redes dedicadas operadas por empresas que brindan entre otros servicios el acceso a internet.

Un Proveedor de Servicios de Internet, (ISP, por sus siglas en inglés) se trata de una empresa u compañía que suministra el servicio de acceso internet a usuarios finales, mediante distintas tecnologías como DSL, Cable módem, Dial-up, Wifi, Fibra óptica, por mencionar los más comunes. Además de este servicio también puede dar soporte a otros como e-mail, web hosting, DNS, FTP, VoIP, entre otros. (Maruri & Vargas, 2021, p.16).

Un ISP en su rol como empresa debe ser responsable del correcto funcionamiento de las distintas conexiones a Internet y de los servicios que ofrece, para ello dentro de su infraestructura de red debe contar con equipos necesarios para cumplir con la factibilidad técnica, relevancia, escalabilidad y alta disponibilidad. Esto se puede cumplir con la implementación de servidores orientados a los diferentes servicios y con un esquema de red bien estructurado. (Silva, 2012, p.2).

##### 2.1.1. Características que debe cumplir un ISP

Las siguientes características son necesarias para el correcto funcionamiento de un ISP y garantizan un nivel de servicio adecuado en el usuario final.

- Factibilidad Técnica: se refiere a disponer de los recursos tecnológicos, ya sea equipos o dispositivos, de vanguardia para dar soporte a los servicios que se ofrece, de tal manera que la infraestructura de red del ISP no se vuelva obsoleta a corto plazo.
- Relevancia: un ISP deberá poder resolver los problemas de conexión en el usuario final sin que se imponga soluciones demasiado costosas o muy complejas.
- Escalabilidad: La arquitectura de un ISP debe ser capaz de aumentar su tamaño, dependiendo del crecimiento del número de abonados y del tráfico de la red.

- Alta disponibilidad: Los servicios que ofrece un ISP deberán estar operativos las 24 horas del día, los siete días de la semana por todo el año.

En la actualidad existe una gran variedad de ISP, los más grandes poseen infraestructuras más sofisticadas y robustas, mientras que los más pequeños pueden llegar a ser cliente de otro ISP mayor. Los elementos fundamentales en la arquitectura de un ISP son los siguientes:

- Canal de acceso ISP a Internet.
- Intranet y banco de servicios.
- Canal de acceso Cliente a ISP
- Mecanismos de administración y seguridad.

### **2.1.2. ISP Inalámbrico**

También denominado WISP, por sus siglas en inglés, se trata de un Proveedor de Servicios de Internet que usa enlaces inalámbricos para dotar de conexión a sus clientes y de esta manera brindar sus servicios, ya sea con enlaces punto a punto o punto multipunto, esta tecnología se utiliza debido a la complejidad de levantar líneas cableadas dedicadas, por su alto costo o porque no existe factibilidad técnica para su montaje. (Yacelga, 2017, p.45).

Dentro de los principales requisitos que se deben cumplir para los diferentes enlaces inalámbricos de un WISP, tenemos los siguientes.

- Deberá existir línea de vista directa entre la antena del WISP que brinda el servicio y la ubicación donde se encuentra el cliente.
- El cliente debe estar dentro del rango máximo de alcance de la antena del WISP.
- Generalmente esta tecnología utiliza las bandas de frecuencia no licenciadas, que son de 2.4 GHz o en la de 5 GHz, aunque puede variar según las regulaciones locales.

### **2.1.3. Servicios de un ISP**

Estos servicios dependen directamente de los recursos tecnológicos que posee un ISP, entre los principales servicios se encuentran los siguientes.

#### **2.1.3.1. Servicio DNS (Domain Name Server)**

Este servicio tiene la función principal de traducir o resolver nombres asociados a las direcciones IP y viceversa, con el fin de poder localizar y direccionar estos equipos en la red.

#### *2.1.3.2. Servicio FTP (File Transfer Protocol)*

Este protocolo se utiliza para la transferencia de archivos, en este se define de qué manera los datos son transferidos sobre una red TCP/IP. FTP permite que los dispositivos remotos puedan compartir archivos de manera independiente a al sistema de archivos que posea tanto el cliente como el servidor, de esta manera se logra una transferencia eficaz de datos.

#### *2.1.3.3. Servicio de Web Hosting*

Provee a los clientes un sistema adecuado para almacenar información, imágenes, video o cualquier contenido accesible vía Internet. El ISP deberá tener la capacidad de proporcionar un espacio de almacenamiento dentro de sus servidores.

#### *2.1.3.4. Servicio de Voz sobre IP*

También denominado VoIP, (por sus siglas en inglés), se trata de la operación de hacer que la voz viaje a través de internet mediante un protocolo IP, esto implica que la voz se codifica en forma digital y se envía a través de la red de telefonía convencional o PSTN (Public Switched Telephone Network).

#### *2.1.3.5. Servicio de Video sobre IP*

Se trata de la transmisión de audio y video a través de la red del ISP, básicamente se dividen en tres categorías, Video broadcasting, Video on Demand y Videoconferencia, solamente el último se trata de una transmisión full-duplex, los dos primeros corresponden a una transmisión unidireccional. (Pachar, 2010, p.29)

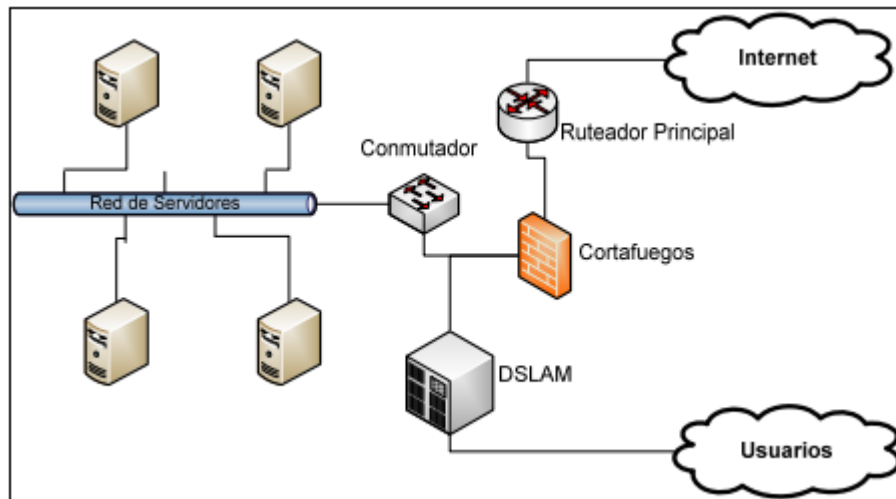
#### **2.1.4. Arquitectura de un ISP**

Los Proveedores de Servicios de Internet deben poseer los recursos tecnológicos tanto en hardware como en software para garantizar el acceso a los servicios que este ofrece a sus abonados. A medida que aumenta la demanda de servicios, la red de un ISP se vuelve más compleja y con mayor número de elementos de red, para definir una estructura, lo que se hace es dar tareas específicas a routers particulares, lo que genera la siguiente división.

- Routers de concentración o de borde: proporciona acceso a la red a los clientes individuales, estos equipos soportan un elevado número de puertos con una velocidad relativa baja que se conecta a los clientes.

- Routers troncales o de backbone: se encargan del transporte óptimo entre los nodos de la red, envían paquetes a gran velocidad de un dominio de red a otro o incluso de un proveedor a otro.

La correcta implementación de estos equipos de red, debe generar una adecuada calidad de servicio, para lo cual los ISP deben poseer elementos de red de alta escalabilidad y fiabilidad, además de enlaces de alta capacidad.



**Ilustración 1-2:** Arquitectura de general de un ISP.

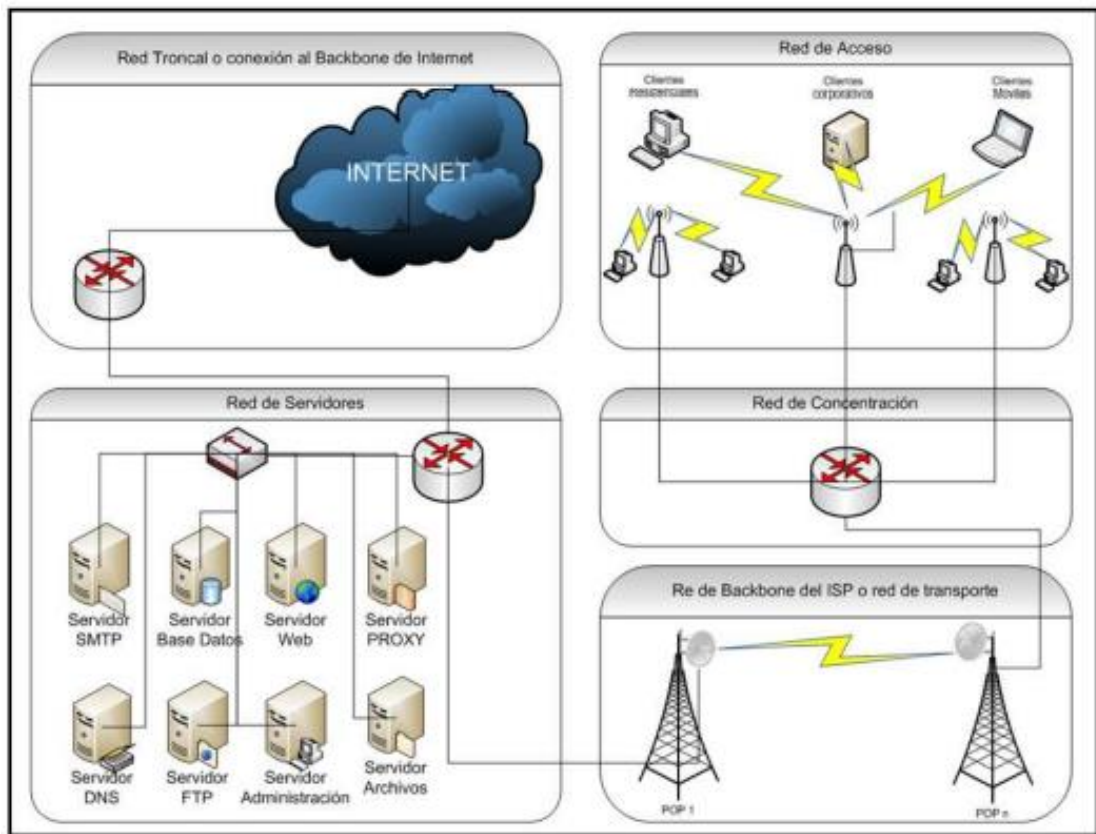
**Fuente:** Lasso, J. & Paucar, L., 2010, p.38.

En la Ilustración 1-2, se aprecia la infraestructura básica de un ISP, con su salida a Internet mediante un Router Principal y su Red de Acceso para usuarios, por la cual los abonados podrán acceder a la red interna de Servidores que ofrezca el ISP. De una manera general la arquitectura de un Proveedor de Servicios de Internet se compone de cuatro estructuras o niveles, las cuales son.

- Red de acceso
- Red de concentración
- Red troncal o backbone
- Red de gestión.

Estas tres estructuras a su vez están conformadas por diferentes dispositivos y equipos adecuadas para su propósito, la interconexión de estas tres redes se utiliza como el transporte de los datos generados por el usuario final hacia el backbone de internet, sobre esta red también es por donde el ISP brinda sus servicios desde sus servidores propios.

En lo que corresponde a un ISP inalámbrico (WISP) la arquitectura no varía en grandes rasgos, la diferencia fundamental radica en que generalmente en la red troncal y de acceso se utiliza enlaces radioeléctricos para su interconexión, como se muestra en la siguiente Ilustración 2-2.



**Ilustración 2-2:** Arquitectura general de un ISP Inalámbrico (WISP).

**Fuente:** Pachar, F., 2010, p.25.

La tecnología utilizada para el levantamiento de estos enlaces inalámbricos depende muchas veces del diseño específico que realiza el ISP, la elección de una tecnología u otra va de la mano con los recursos físicos en antenas y equipos adecuados para su puesta en marcha. Otro factor que influye para elegir un tipo de sistema inalámbrico es la naturaleza del entorno en donde se lleva a cabo la implementación del WISP, además de un estudio adecuado de demanda de tráfico que llegue a generarse.

Al igual que un ISP tradicional, en un ISP inalámbrico, se debe monitorear constantemente cada radioenlace de la red para evitar las caídas imprevistas y la interrupción del servicio, ya sea por factores naturales como las condiciones climáticas y accidentes, o por falla de los equipos de red, el Proveedor de Servicios de Internet deberá garantizar el arreglo de estos desperfectos en el menor tiempo posible y la reanudación de los servicios, sin que estos costos sean recargados al cliente final.

### 2.1.5. Red de Acceso

Se trata del tramo final de la infraestructura de red del ISP que se conecta con los usuarios finales, se definen varios tipos de redes de acceso, dependiendo de la tecnología utilizada.

- Líneas de usuario conmutados (Dial UP)
- Líneas de Usuario Dedicados.
- Línea Digital de Suscriptor (xDSL)
- Líneas de acceso Híbridas, Fibra coaxial
- Líneas de acceso Inalámbricas.

Varias de estas tecnologías ya han quedado obsoletas y actualmente los más utilizados son los enlaces inalámbricos, ya sean radioeléctricos o satelitales, los enlaces de fibra óptica, los enlaces por cable coaxial, o las redes híbridas.

#### 2.1.5.1. Línea de acceso por Fibra óptica

Actualmente es la tecnología más usada para las redes de acceso, este sistema de comunicaciones está conformado por hilos finísimos de vidrio de alta pureza, recubiertos por un material de protección de plástico adecuado para soportar daños del entorno exterior.



**Ilustración 3-2:** Ejemplo de fibra óptica, donde se aprecia los hilos y el revestimiento.

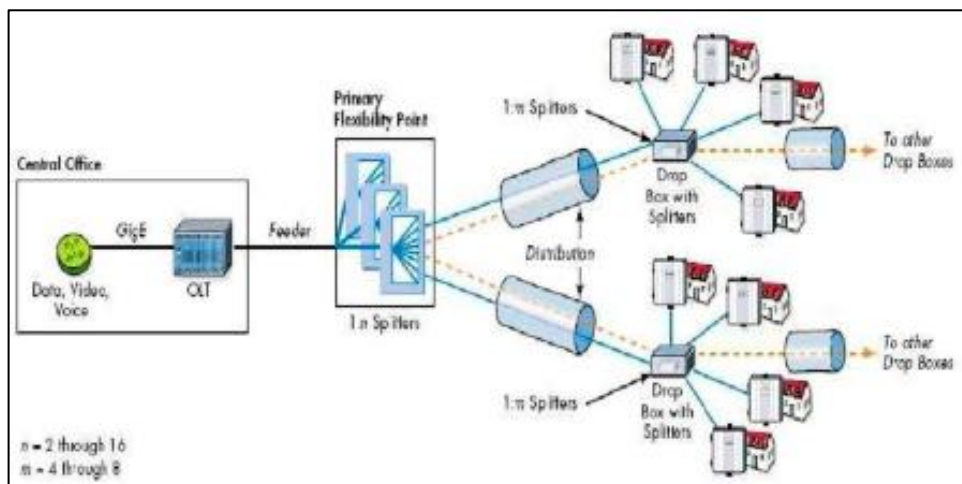
**Fuente:** Prieto, J., 2014, p.7.

La fibra óptica ha ganado protagonismo en las redes de comunicaciones, pues sus características favorables, permiten la transmisión de grandes cantidades de datos y la entrega de un mayor abanico de aplicaciones por un mismo medio de transmisión. Entre las principales propiedades de la fibra óptica tenemos. (Prieto, 2014, p.7).

- Gran capacidad de transmisión.

- Baja atenuación de la señal óptica.
- Inmunidad frente a las interferencias electromagnéticas.
- Los cables de fibra óptica son pequeños, ligeros y flexibles, con una vida útil superior a otros conductores convencionales.
- Baja coste de producción debido a la abundancia de la materia prima para su construcción.

Las redes PON (Pasive Optical Network) son las más utilizadas para el despliegue de una red de acceso con fibra óptica debido a su gran fiabilidad y bajo coste inicial. La red utiliza un transmisor de fibra único ubicado en un nodo principal de la red, desde aquí se reparte por toda el área hasta ramificarse en redes de distribución más pequeñas, las cuales llevan la fibra a cada una de las edificaciones, de ser necesario la red se ramifica dando lugar a una red de dispersión que llega a cada uno de los abonados residenciales, esto se puede observar en la siguiente Ilustración.



**Ilustración 4-2:** Arquitectura de una red de acceso PON.

**Fuente:** Prieto, J. 2014, p.59.

#### 2.1.5.2. Línea de acceso Híbridas (HFC, HybridFiber Coaxial)

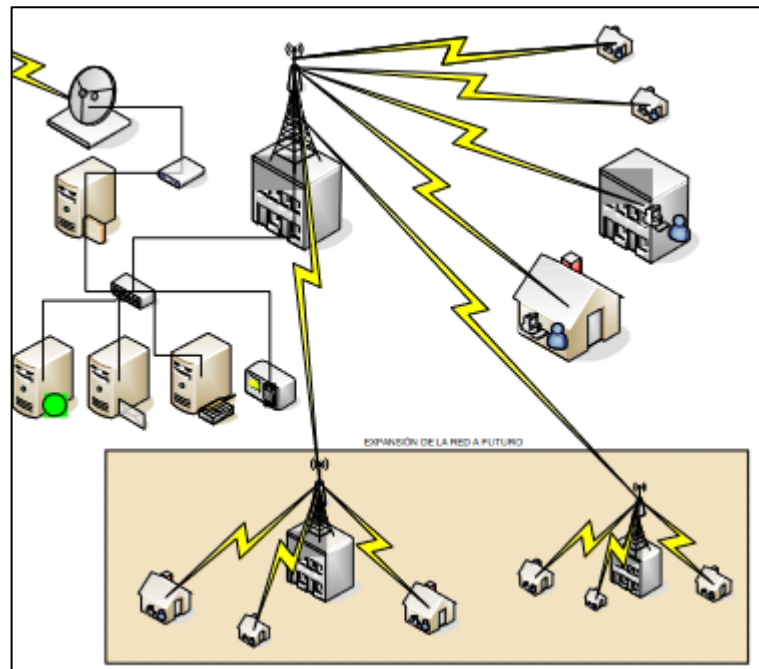
Como su nombre lo indica está conformada por tecnología de Fibra óptica y de cable coaxial, las redes HFC proveen y de un gran ancho de banda que permite el despliegue de un abanico de servicios de valor agregado de telecomunicaciones, además se incluye la distribución de señales de TV analógica y digital.

#### 2.1.5.3. Líneas de acceso inalámbricas

Este tipo de redes se implementan mediante la utilización de ondas de radio, microondas, satelitales o infrarrojos, el levantamiento del enlace radioeléctrico se realiza mediante la utilización de antenas y equipos de transmisión adecuados; también se puede clasificar a las redes inalámbricas como públicas o privadas, las primeras son aquellas que se despliegan en bandas no licenciadas y por lo tanto no es necesario algún tipo de pago para su uso, mientras que las segundas



se deberán pagar al órgano regulador para concesionar la banda de frecuencias para su posterior explotación. (Aguaiza, 2016, p.38).



**Ilustración 5-2:** Arquitectura de una red de acceso inalámbrica.

Fuente. Pachar, F., 2010, p.17.

La mayoría de redes inalámbricas utilizadas por los ISP se basan en el estándar IEEE 802.11.x, este define la tecnología utilizada para el despliegue de redes inalámbricas de área local y área metropolitana, a lo largo de los años este estándar ha evolucionado con el objetivo de soportar mejores velocidades de transmisión, mayor seguridad y escalabilidad, en la actualidad existen numerosas versiones de este estándar los cuales se resumen en la Tabla 1-2.

**Tabla 1-2:** Estándares de la especificación de redes inalámbricas.

Estándar	Característica	Banda	Velocidad
802.11	Legacy	IR/ 2.4 GHz	1-2 Mbps
802.11 a	Inclusión de la banda 5GHz	5 GHz	54 Mbps
802.11 b	Gran crecimiento comercial	2.4 GHz	11 Mbps
802.11 g	Revisión de b	2.4 GHz	54 Mbps
802.11 h	Revisión de a para Europa	5 GHz	54 Mbps
802.11 i	Mejoras de seguridad ( WPA, WPA2)	-	-
802.11 e	Mejoras en QoS (EDCA y HCCA)	-	-
802.11 n	Inclusión MIMO	2.4 y 5 GHz	> 600 Mbps
802.11 s	Inclusión de redes mash		
802.11 ac	Revisión del n	5 GHz	1 Gbps

802.11 ad	Alto Throughput	>60 GHz	-
802.11 af	White - Wi-Fi	Frecuencias huecas de TV	-

**Fuente:** Estado del arte 802.11, sf.

**Realizado por:** Yacelga, J., 2017, p.23.

Otro de los protocolos que se usan para el despliegue de redes inalámbricas es el IEEE 802.16, también llamado WiMAX, este estándar utiliza técnicas MIMO para lograr altas tasas de transferencia, mediante la codificación y codificación avanzada, llegando así hasta los 75 Mbps teóricos, esta tecnología es adecuada para ofrecer servicios de telecomunicaciones a zonas rurales, ya que puede trabajar en diferentes anchos de banda desde 1.25 hasta 20 MHz. (Yacelga, 2017, pp.23-24).

#### **2.1.6. Red de concentración o de borde.**

Se trata del medio de comunicación entre la red de acceso y la red troncal, se encarga principalmente de agregar las conexiones de los clientes en los puntos de presencia del proveedor (PoP). Los routers de esta red son escalables y tienen gran capacidad de ancho de banda, además de contar con una alta densidad de puertos para dar soporte al creciente número de clientes, en estos routers también se ofrecen servicios de valor agregado como VPN, Firewall, políticas de calidad de servicio, entre otros. (Silva, 2012, pp.13-14)

#### **2.1.7. Red de troncal o backbone**

Esta red permite la interconexión con otros proveedores y salida a Internet, un ISP puede llegar a tener uno o varios enlaces WAN, ya sea Frame Relay, ATM, MPLS, enlaces satelitales, entre otros. Su función principal es la de conmutar el tráfico procedente de las redes de menor jerarquía, la red backbone es la encargada de llevar grandes cantidades de tráfico de manera confiable con altas velocidades y con la menor latencia posible. (Silva, 2012, p.12)

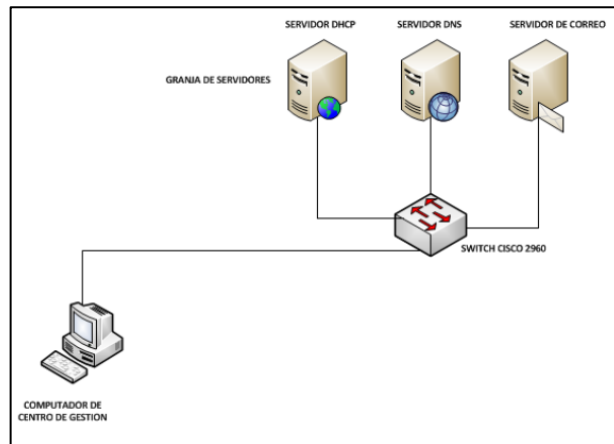
#### **2.1.8. Red de Gestión**

Para separar las funciones de administración de los equipos de acceso al cliente, en la oficina central se debe configurar las siguientes redes de área local:

- LAN de servidores de aplicación.
- LAN de servidores de administración.
- LAN de dispositivos de acceso.

Para realizar las tareas se debe utilizar un computador o servidor como centro de gestión, debido a que los servidores de la empresa necesitan cumplir con las propiedades de alta disponibilidad y alto desempeño para dotar una calidad de servicio adecuada en el usuario final. (Silva, 2012, p.13).

Este equipo de gestión formaría parte de la red junto con los servidores, como se muestra en la Ilustración 6-2.



**Ilustración 6-2:** Arquitectura de una red de gestión de un ISP.

**Fuente:** Yacelga, J., 2017, p.66.

## 2.2. Infraestructura de red

Una red se considera a un conglomerado de dispositivos activos conectados entre sí, cuyo propósito fundamental es el de compartir recursos como, información, programas, o ingreso a bases de datos, entre otros, pero físicamente ubicados en otro punto de conexión. En lo que respecta a una infraestructura de red de un ISP, su composición conlleva routers interconectados por enlaces de comunicación, las redes más simples están formadas por unos pocos routers de propósito general interconectados por enlaces propios o alquilados. (Sáenz de Viguera, 2002, p.2).

### 2.2.1. Clasificación de una red

En general una red informática se clasifica tomando en cuenta diferentes características como son el tipo de acceso a los usuarios, la cobertura, el tipo de medio y la topología.

#### 2.2.1.1. Según el acceso de los usuarios

Una red puede considerarse pública si puede acceder cualquier usuario, mientras que en una red privada solo puede acceder un grupo restringido de personas.

#### 2.2.1.2. Según la cobertura

En ésta se determina la distancia que abarca el diseño de la red, como se observa en la siguiente Tabla 2-2.

**Tabla 2-2:** Clasificación de las redes según su cobertura.

Distancia máxima.	Área de uso	Clasificación
1m	Metro cuadrado	PAN (Red de Área Personal)
10 m	Habitación	LAN (Red de Área Local)
100 m	Edificio	
1 km	Campus	CAN (Red de Área de Campus)
10 km	Ciudad	MAN (Red de Área Metropolitana)
100 km	País	WAN (Red Área Amplia)
1000 km	Continente	
1000 km	Planeta	INTERNET

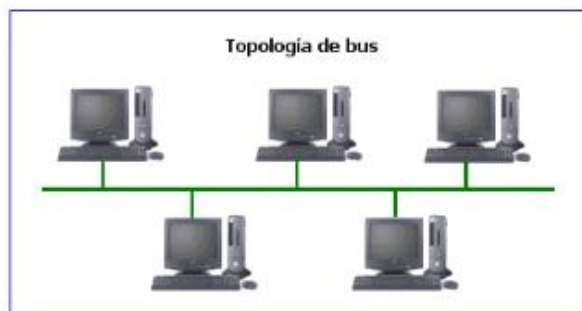
**Fuente:** Zayas & Sao Áviles, 2002.

**Realizado por:** Aguaiza, D., 2016, p.20.

### 2.2.1.3. Según su topología

Se denomina a la ubicación física que se les da a los equipos dentro de la red, puede haber más de un tipo, a lo que se le denomina mixto, existen tres tipos básicos de topologías que se muestran a continuación.

- Bus: en esta topología un ordenador o estación transmite la información mientras el resto está escuchando, es decir, uno envía y todas las demás reciben la información. como se observa en la Ilustración 7-2, consiste de una conexión formada por un único cable con un terminal en cada extremo. (Aguaiza, 2016, p.21)



**Ilustración 7-2:** Diseño de Topología tipo Bus.

**Fuente:** Barragán A., 2012, p.21.

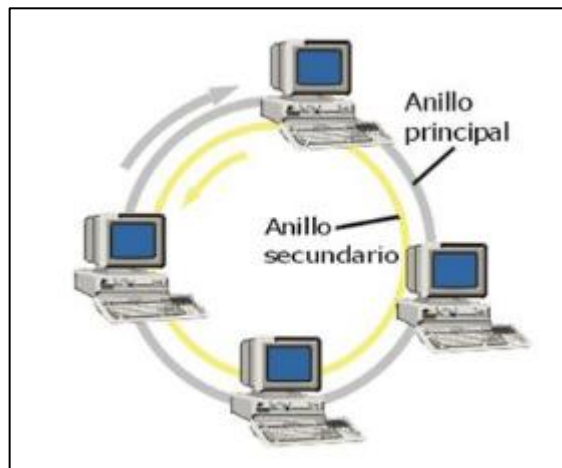
- Estrella: para esta topología se emplea un dispositivo de conexión de redes como un punto común en el centro, como un Hub, Switch o Router, al cual se le conectan los demás elementos de red y por el cual se realizan todas las comunicaciones en la misma, como se observa en la Ilustración 8-2.



**Ilustración 8-2:** Topología de red tipo estrella.

**Fuente:** Barragán A., 2012, p.22.

- Anillo: para esta topología cada estación recibe el nombre de nodos, los mismo que hacen la función de receptor y repetidor, captando la información de su antecesor y retransmitiéndola a su sucesor, como se aprecia en la Ilustración 9-2.



**Ilustración 9-2:** Topología de red tipo anillo.

**Fuente:** Barragán A., 2012, p.23.

### **2.2.2. Componentes de una Infraestructura de red.**

Para conformar una infraestructura de red es necesario la inclusión de ciertos elementos básicos, según el estudio realizado por (Zayas & Sao Áviles, 2002, pp.5 - 6), se puede definir a estos elementos de manera general en tres elementos principales:

- Nodos o estaciones finales: mediante estos, los usuarios finales se comunican a la red utilizando alguna topología de red.

- Cables de red: su función radica en conectar los diferentes nodos y dispositivos físicos de la red. Existe un gran número de tipo de cable cuyas características depende de los requerimientos solicitados para la implementación de una red.
- Dispositivos de interconexión de redes: se encarga de conectar segmentos de red, de igual manera existen varios tipos dependiendo de las necesidades de diseño de la red, se emplean diferentes equipos como repetidores, hubs, switches, routers, Gateway, entre otros.

### **2.3. Sistema de gestión de red**

Se considera como un sistema de gestión de red de datos, al conjunto de herramientas para monitorizar y controlar la red de forma integrada, de tal manera que la red entera se puede considerar como una arquitectura global y unificada, con direcciones y etiquetas asignadas a cada dispositivo. Los elementos activos que componen la infraestructura de red proporcionan una retroalimentación al centro de control de red, una realimentación regular de información de estado. (Solís, 2014, p.199).

Los elementos que se pueden gestionar con este sistema son los siguientes:

- Redes y subredes
- Estructura de red
- Elementos de red como switches, routers, etc.
- Equipos finales como PC, hosts, servidores, dispositivos de almacenamiento.

Un gestor de red, también conocido como una aplicación de gestión de red (Network Management Application o NMA), permite al personal autorizado mediante una interfaz gráfica la intercomunicación hacia equipos locales y remotos mediante un protocolo de gestión de red a nivel de aplicación, como SNMP, también es posible la utilización de plataformas desarrolladas para el monitoreo de red, como es el caso de PRTG Network Monitor, Solarwinds, Manage Engine, Nagios, entre otros, que muestran un análisis de rendimiento de los nodos conectados a la red como la obtención de información de los nodos conectados, registro de incidencias y fallos de los equipos instalados. (Terán, 2020, p.11).

#### **2.3.1. Modelos de gestión de red**

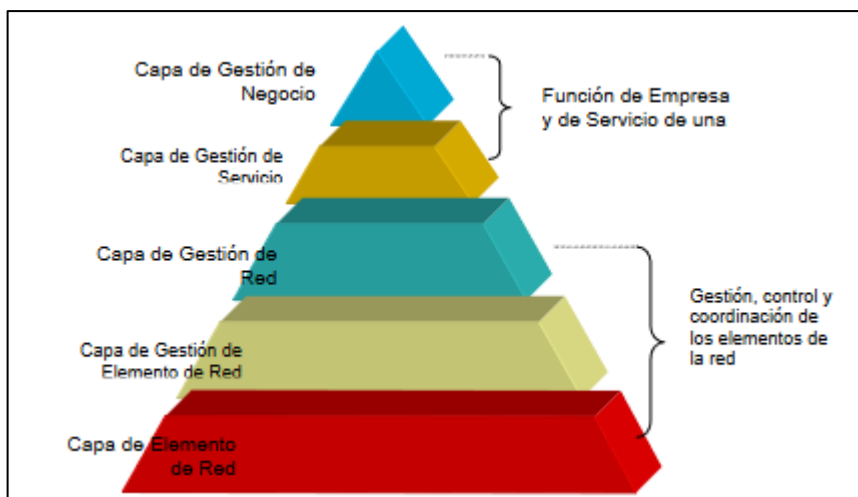
Para desarrollar las distintas operaciones de gestión se deben cumplir tareas como, detectar fallas, aislarlas y resolver en un tiempo mínimo posible, en un bajo costo; cuando se presenta un cambio de configuración no se afecte en gran medida el servicio; predecir posibles puntos de falla y evitarlos o en su efecto minimizarlos (Martín & León de Mora, 2014,).

Actualmente se han desarrollado varios modelos de gestión, de los más extendidos son:

- Modelo TMN (Telecommunications Management Network)
- Modelo de gestión OSI (FCAPS)
- Modelo de gestión de Internet

#### 2.3.1.1. Modelo de gestión TMN

Desarrollado por la Unión Internacional de Telecomunicaciones ITU-T en su sector de normalización, define una lista de capas o niveles de gestión para poder abordar la gran complejidad de la gestión de redes de telecomunicaciones. Descritos en la recomendación UIT-T M.3010 (Logical Layered Architecture), se define una estructura jerárquica que permite proporcionar niveles de gestión en los cuales cada uno agrupa un conjunto de funciones, donde las capas superiores utilizan los servicios proporcionados por las capas inferiores, formando una estructura piramidal, como se observa en la Ilustración 10-2, en este modelo las funciones se organizan de acuerdo al nivel de responsabilidad. (Padilla, 2015, p.8)



**Ilustración 10-2:** Arquitectura lógica por capas de TMN

Fuente: Garrido G., 2003, p.24

#### 2.3.1.2. Modelo de gestión OSI (FCAPS)

Fue establecida por la ISO como una guía para definir un conjunto de protocolos abiertos, en su norma ISO/IEC 7498-4 se establece como un estándar para la gestión de redes basadas en la arquitectura OSI de siete capas. El modelo OSI/FCAPS define cinco áreas para la gestión, denominadas áreas funcionales, de ahí su nombre; gestión de Fallos (Faults), gestión de Configuración (Configuration), gestión de Contabilidad (Accounting), gestión de Rendimiento (Performance), gestión de Seguridad (Security). (Padilla, 2015, pp.4-5)

- La Gestión de Fallos consiste en la monitorización o seguimiento del sistema gestionado con el fin de detectar posibles problemas, y las políticas de actuación en caso de fallas para su recuperación.
- La Gestión de Configuración incluye las tareas relacionadas con la toma de información de la red, modificación del comportamiento de los dispositivos y almacenamiento de la información que determina este comportamiento.
- La Gestión de Contabilidad posibilita la determinación de los costos asociados a la utilización de los recursos y la asignación de sus correspondientes cargas.
- La Gestión de Rendimiento realiza la evaluación del comportamiento de los elementos de red, mediante la obtención de estadísticas que incluyen para qué se utiliza la red y que tan eficientemente se está usando.
- La Gestión de Seguridad controla el acceso a los recursos, protección de la información en tránsito, incluye gestión de claves, firewalls y logs de seguridad.

#### *2.3.1.3. Modelo de gestión de Internet*

La organización IEFT (Internet Engineering Task Force), ha definido la recomendación SNMP para facilitar la gestión de redes, este último protocolo consta de un conjunto de funciones diseñadas para las redes basadas en el modelo TCP/IP, este modelo permite a los administradores de red aislar y monitorear el estado y rendimiento de las redes corporativas.

Su funcionamiento se basa en una arquitectura cliente-servidor, donde se define un Gestor o NMS que se encarga de recolectar información de gestión de los distintos elementos de red, los mismos que a través de un Agente envían información almacenada en su base de datos local llamada MIB (Management Information Base).

El protocolo de comunicación que se utiliza en este modelo es el SNMP (Simple Network Management Protocol), este es ampliamente utilizado y ha evolucionado a través de sus tres versiones que incluyen mejoras significativas como son la inclusión de autenticación y privacidad. (Padilla, 2015, pp.7-8)



### 2.3.2. Elementos de un sistema de gestión de redes

Básicamente dentro de una red de comunicaciones para realizar las tareas de gestión se basan en una comunicación gestor – agente, es decir, se utiliza un equipo dedicado al seguimiento, control y monitoreo de la red, con el objetivo de garantizar una adecuada Calidad de Servicio.

Los elementos que se incluyen en la gestión de redes principalmente son los siguientes.

- El gestor.
- El agente.
- El protocolo de gestión.
- La base de información de gestión, MIB.



**Ilustración 11-2:** Elementos de gestión de red.

Fuente: Guzmán, A., 2016.

#### 2.3.2.1. Gestor

Es el encargado de realizar las funciones de monitoreo de la red a través de una interfaz gráfica que permita la intercomunicación con los equipos dentro de la red local de la empresa, así también como los equipos remotos, mediante un protocolo de gestión de red a nivel de aplicación. (Terán, 2020, p.11).

#### 2.3.2.2. Agente

Se le denomina también como la entidad de gestión de red, se trata de un software que permite la gestión dentro de cada nodo de la red, este tiene las siguientes funciones.

- Recolectar información sobre las actividades realizadas sobre la red.
- Almacenar la información recolectada de manera local.

- Responder a las peticiones de un gestor, generalmente se encarga del envío de estadísticas del estado y funcionamiento de un nodo, información del dispositivo de red, configuración entre otros.

#### *2.3.2.3. Protocolo de comunicación*

Es el encargado de llevar la información de cada consulta realizada por el gestor a un agente y su respectiva respuesta, mediante este protocolo es posible la comunicación de todo el sistema de gestión de la red, con este protocolo es posible realizar una gran cantidad de acciones, como dar a conocer desde eventos e incidencias dentro de los distintos equipos, hasta fallos en los enlaces de la red. Entre los principales protocolos de comunicación para gestión de red, se mencionan los principales:

- Protocolo Simple de Administración de Red (SNMP, por sus siglas en inglés) perteneciente a los protocolos TCP/IP, es de gran demanda en los sectores empresariales debido a su alta compatibilidad con la mayoría de dispositivos de red que existen en el mercado.
- Protocolo de Administración de Información Común (CMIP, por sus siglas en inglés), forma parte de los protocolos de la familia OSI desarrollado por la ISO, se creó para reemplazar a SNMP, pues presenta una mejor seguridad y flexibilidad.
- Netflow es un protocolo de gestión de red perteneciente a Cisco, permite la recolección de información para monitorear del tráfico de red, este protocolo solo es soportado por equipos Cisco y algunos sistemas operativos de software libre como Linux. (Terán, 2020, p.12).

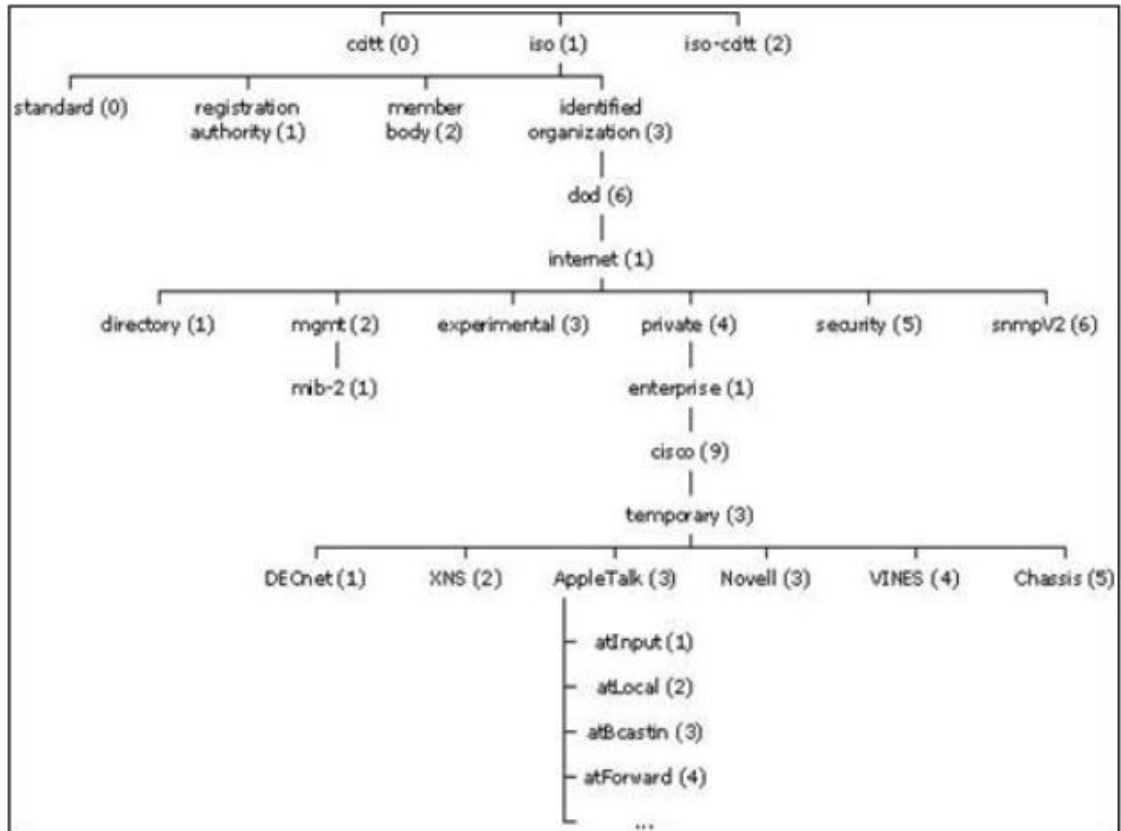
#### *2.3.2.4. Base de Información de Gestión (MIB)*

Se trata de una compilación de información que está ubicada jerárquicamente, esta base de datos es consultada mediante un protocolo de comunicación por parte del gestor, básicamente se compone de objetos administrados y referidos por identificadores de objetos. (Terán, 2017, p.16).

Los objetos administrados están compuestos de una o más instancias de objeto, que básicamente se tratan de variables, existen dos tipos de objetos, los escalares y tabulares.

- Objetos escalares: estos definen una simple instancia de objeto
- Objetos Tabulares: definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un identificador de objeto (OID, por sus siglas en inglés) únicamente identifica a un objeto administrado en la jerarquía MIB, esta se representa mediante un árbol cuya raíz superior pertenecen a diferentes organizaciones estándar, mientras que los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas.



**Ilustración 12-2:** Árbol MIB.

Fuente: Terán, R., 2017, p.17

Los fabricantes pueden definir sus propias ramas privadas que incluyen los objetos administrados para sus propios productos, las MIBs que no estén estandarizadas, generalmente están localizadas en la rama experimental. La parte más importante del árbol MIB, para la administración se encuentra en el grupo mib-2, los cuales son los siguientes.

- System (1);
- Interfaces (2);
- AT (3);
- IP (4);
- ICMP (5);

TCP (6);  
UDP (7);  
EGP (8);  
Transmission (10);  
SNMP (11);

Para la notación de la estructura de una MIB, se describe mediante el estándar Notación Sintáctica Abstracta 1 (Abstract Syntax Notation One). (Mejía, 2019, p.37)

#### **2.4. Protocolo Simple de Gestión de Red (SNMP)**

SNMP por sus siglas en inglés, se trata de un protocolo desarrollado por el IETF para el monitoreo fácil y permanente de la red, funciona en base a la comunicación gestor – agente, usando el método de solicitud y respuesta se intercambia información de tres tipos, de estado, advertencia y alarma.

En cada dispositivo gestionado se ejecuta, en todo momento, un componente de software llamado agente que reporta información a través de SNMP con el gestor. Los gestores muestran esta información en forma de variables. El protocolo también permite realizar tareas de gestión de activos, así como la modificación y ejecución de nueva configuración de forma remota de estas variables. Las variables accesibles a través de SNMP están organizadas en jerarquías, las mismas que se describen por la Base de Información de Gestión (MIB). Este protocolo se ha venido evolucionando a lo largo de la historia hasta alcanzar la versión tres en la actualidad.

##### **2.4.1. Funcionamiento del protocolo SNMP**

SNMP opera en la capa de aplicación, la capa 7 del modelo OSI, el agente SNMP recibe solicitudes, en el puerto UDP 161. El gestor puede enviar solicitudes desde cualquier puerto de origen disponible, entonces la respuesta del agente será enviada hacia el mismo puerto de origen en el gestor.

El administrador recibe notificaciones (Trampas e InformRequests) en el puerto 162, el agente puede generar notificaciones desde cualquier puerto disponible, si se utiliza Transport Layer Security (TLS), las solicitudes se reciben en el puerto 10161 y trampas se envían al puerto 10162. (Mejía, 2019, p.37)

#### 2.4.2. Versiones SNMP

La primera versión llamada SNMPv1, con una antigüedad de casi 30 años, realiza un sondeo básico con bajos recursos, su mayor desventaja es no poder implementar cifrado, por lo que ha ido perdiendo popularidad.

SNMPv2 surgió a partir de los años 90, incorporó características como la seguridad, además de agregar dos operaciones como GetBulk e Inform, la primera utilizada para la recuperación de bloques de datos grandes, y la segunda para enviar traps de información a un agente o gestor y permitir su respuesta.

SNMPv3, es la versión más reciente del protocolo, se enfoca en proporcionar seguridad para el acceso remoto a dispositivos conectados en red, con la incorporación de técnicas de autenticación y cifrado de los paquetes de información, en esta versión se utiliza HMAC, el Código de Autenticación de Mensaje Hash, una gran desventaja es que no es compatible con todos los equipos de red. (Terán, 2017, pp.19-20)

A continuación, se muestra una tabla comparativa con las funciones destacadas de cada versión de SNMP.

**Tabla 3-2:** Comparativa de las versiones SNMP.

<b>Característica</b>	<b>SNMPv1</b>	<b>SNMPv2</b>	<b>SNMPv3</b>
<b>Seguridad</b>	Sin seguridad para acceso a la red	Seguridad mínima	Seguridad mejorada
<b>Complejidad</b>	Limitaciones de rendimiento y seguridad	Tiene una mejor potencia pero aumenta complejidad	SE centra en mejorar el aspecto de seguridad.
<b>Operaciones de protocolo</b>	GetRequest GetNextRequest SetRequest Trap Respuesta	Se aumenta: Inform GetBulk	Se conjuga las especificaciones de SNMPv1 y v2
<b>MIB</b>	MIB limitado de fácil implementación de variables escalares y tablas bidimensionales.	Define el marco general con el que se define y construye la MIB	Puede configurar agentes para proporcionar un

			cantidad de niveles de acceso a MIB.
<b>Cadenas de texto sin formato</b>	Si	SI	No
<b>Tráfico cifrado, Detección de paquetes mal formados.</b>	No	Si	Si

Fuente: Shingote & Bagwe, 2018.

Realizado por: Terán, J, 2020, p.19.

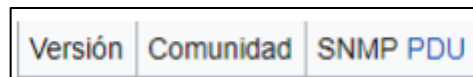
### 2.4.3. Mensaje SNMP

Como se ha mencionado, las diferentes operaciones que realiza el protocolo SNMP utiliza un servicio no orientado a conexión, es decir UDP, mediante el cual se puede enviar pequeños mensajes (PDU), entre el gestor y los agentes de los diferentes dispositivos. De esta forma se evita sobrecargar a la red con mecanismos de control y recuperación como se utiliza con los protocolos orientados a conexión como TCP. (Mejía, 2019, p.38).

Todas las PDUs de los mensajes SNMP se componen de la siguiente manera.

- Cabecera IP
- Encabezado UDP
- Tipo de UDP
- Petición-ID
- Error de estado
- Índice de errores.
- Enlaces de variables.

Los paquetes utilizados para realizar consultas y dar respuestas SNMP poseen el siguiente formato.



**Ilustración 13-2:** Formato de consultas y respuestas SNMP.

Fuente: Mejía, E., 2019, p.38

Donde los campos pueden tener los siguientes valores.

- Versión: se indica la versión del protocolo que se está utilizando, en donde es, 0 para SNMPv1, 1 para SNMPv2c, 2 para SNMPv2p y sNMPv2u, e para SNMPv3.

- Comunidad: Nombre o palabra clave que se usa para la autenticación.
- SNMP PDU: Se trata del contenido del mensaje y depende de la operación que se ejecute.

Los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la estructura en el campo SNMP PDU.



**Ilustración 14-2:** Estructura SNMP PDU.

**Fuente:** Mejía, E., 2019, p.39.

- Identificador: Se trata de un número utilizado por el NMS y el agente para enviar solicitudes y respuestas diferentes en forma simultánea.
- Estado e índice de error: Solo se usa en los mensajes GetResponse. El campo “índice de error” solo se usa cuando “estado error” es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema, este campo puede tener los siguientes valores:
  - 0: No hay error.
  - 1: Demasiado grande.
  - 2: No existe esa variable
  - 3: Valor incorrecto.
  - 4: El valor es de solo lectura.
  - 5: Error genérico.
- Enlazado de variables: Es una serie de nombre de variables con sus valores correspondientes.

#### **2.4.4. Comandos básicos**

Todos los dispositivos administrados, son supervisados y controlados usando cuatro comandos básicos, los mismos que son:

- Lectura: se utiliza principalmente en un NMS (Sistema de Administración de Red) en el cual se examina las diferentes variables que son mantenidas por los dispositivos gestionados.

- Escritura: se utiliza para controlar los elementos de red, el NMS puede cambiar los valores de las variables almacenadas en los dispositivos gestionados.
- Notificación: es usado por los dispositivos administrados para reportar eventos de forma asíncrona al NMS.
- Operaciones transversales: son usadas por los NMS para determinar que variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables. (Mejía, 2019, p.35)

#### 2.4.5. *GetRequest*

A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre, la respuesta que el agente envía una respuesta indicando el éxito o fracaso de la petición, en caso de ser correcta la petición, el mensaje resultante también contendrá el valor del objeto solicitado.

#### 2.4.6. *GetNextRequest*

Este mensaje es usado para recorrer una tabla de objetos, una vez utilizado el mensaje *GetRequest* para recoger le valor de un objeto, puede ser utilizado el mensaje *GetNextRequest* para repetir la operación con el siguiente objeto de la tabla.

#### 2.4.7. *SetRequest*

Se utiliza para solicitar a un agente modificar valores de objetos, para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

#### 2.4.8. *GetResponse*

Este mensaje es usado por el agente para responder un mensaje *GetRequest*, *GetNextRequest* o *SetRequest*. En el campo “Identificador de Request” lleva el mismo identificador que el “Request” al que está respondiendo.

#### 2.4.9. *Trap*

Es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato del SNMP PDU es el siguiente.



**Ilustración 15-2:** Estructura de un PDU en un Trap.

Fuente: Mejía, E., 2019, p.40.



Donde los campos se definen de la siguiente manera.

- Tipo del Trap:
  - Cold start (0): Indica que el agente ha sido inicializado o reinicializado.
  - Warm start (1): Indica que la configuración del agente ha cambiado.
  - Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (activa).
  - Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado.
  - EGP neighbor loss (5): Indica que en sistemas en los Routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio.
  - Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.
- Enterprise: Identificación del subsistema de gestión que ha emitido el trap.
- Dirección del agente: Dirección IP del agente que ha emitido el trap.
- Tipo específico de trap: Es usado para traps propietarios de los distintos fabricantes.
- Timestamp: Indica el tiempo que ha transcurrido entre la re-inicialización del agente y la generación del trap.
- Enlazado de variables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

#### **2.4.10. GetBulkRequest**

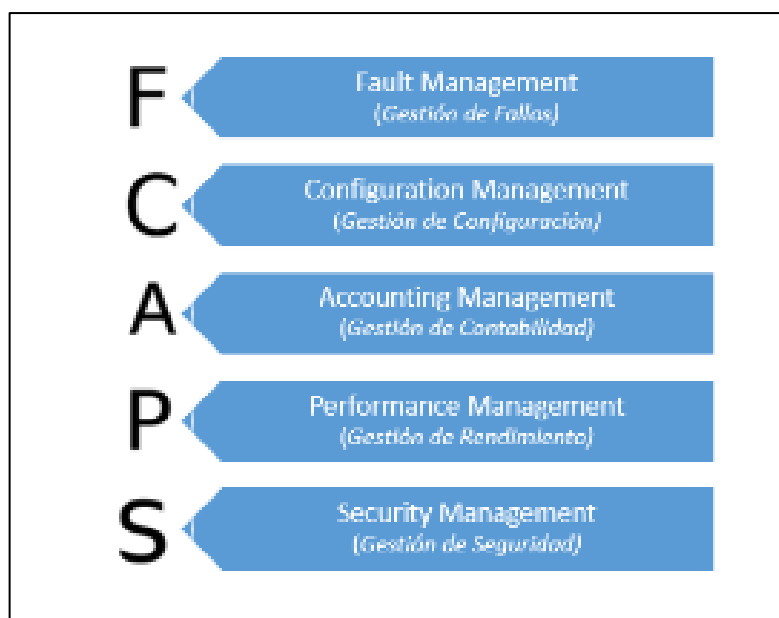
Es utilizado en el protocolo SNMP versión 2 o 3, generalmente cuando se requiere una larga transmisión de datos, su funcionamiento es parecido al mensaje GetNextRequest de la versión 1, sin embargo, GetBulkRequest es mucho más rápido y eficiente.

#### **2.4.11. InformRequest**

Se utiliza para transmitir un mensaje de este tipo entre dos NMS con igual características para notificar información sobre objetos administrados, utilizando el protocolo TCP, entonces se enviará un InformRequest hasta que tenga exista una confirmación de recibirlo. (Mejía, 2018, p.41).

### **2.5. Modelo de gestión ISO/FACPS**

Fue desarrollado por la Organización Internacional de Normalización (ISO), como un framework de administración para su aplicación en diferentes sistemas de gestión de infraestructuras de red. El modelo FCAPS es aplicable para los Sistemas de gestión de elementos (EMS), los Sistemas de gestión de redes (NMS) y los Sistemas de soporte de operaciones (OSS), convirtiéndose en un modelo universal ampliamente reconocido como un método simple, debido a que los usuarios pueden describir y clasificar características de las áreas del mismo modelo. (Terán, 2020, pp.19-20)



**Ilustración 16-2:** Modelo funcional FCAPS por la ISO para la gestión de redes.

**Fuente:** Terán, J., 2020, p.20

FCAPS se trata de un acrónimo de Fault, Configuration, Accounting, Performance, Security, según la Ilustración 16-2, se trata de las categorías en las cuales el modelo ISO define las tareas de gestión de redes, en algunos casos Accounting (Contabilidad) se reemplaza con Administración. (Mejía, 2019, p.27).

### **2.5.1. Gestión de Fallos / Fault**

Esta área tiene la función de detectar, aislar y solucionar inconvenientes que afectan el correcto funcionamiento y la disponibilidad de la red gestionada, además se realiza el mantenimiento, el registro de fallos, secuencias de pruebas de diagnóstico y presentación de informes o notificaciones de fallos.

También se incluye el establecimiento de alertas que son invocadas por umbrales establecidos previamente por el administrador de red, ya sea mediante el lanzamiento de un programa o el software de notificación para el envío de un correo electrónico, un mensaje SMS, entre otras acciones. (Ayala, 2015, p.19).

El modelo FCAPS recomienda varias recomendaciones para realizar la administración de fallas, las mismas que incluyen.

- Detección de falla.
- Corrección de falla.
- Aislamiento de la falla.
- Recuperación de la red.
- Manejo de alarmas.

- Filtrado de alarmas.
- Generación de alarmas.
- Pruebas de diagnóstico.
- Manejo de errores.
- Estadísticas de errores

Esta gestión se puede realizar de dos maneras, pasiva y activa.

#### *2.5.1.1. Gestión de fallos pasiva.*

Se realiza mediante la recopilación de alarmas de dispositivos a través de un protocolo de comunicación, de este modo el sistema de gestión solo sabe si el dispositivo gestionado es capaz de reportar una falla en sus puertos, sin embargo, si el dispositivo falla o se inhibe por completo, no se producirá ningún reporte al sistema de gestión y el problema no será detectado. (Ayala, 2015, p.20).

#### *2.5.1.2. Gestión de fallos activa*

Se realiza a través del monitoreo constante de los dispositivos gestionados a través de herramientas como el PING para determinar el estado del dispositivo, si este deja de responder, entonces el sistema generará una alarma correspondiente, lo que permite una respuesta proactiva para la resolución del problema.

#### **2.5.2. Gestión de Configuración / Configuration**

Con este aspecto se garantiza que todos los dispositivos contengan la configuración correcta según la política de la organización, también proporciona un mecanismo para la recuperación en caso de fallos de dispositivos, pues se establece el almacenamiento de la configuración de cada dispositivo en un repositorio de búsqueda independiente.

Dentro de las tareas de la gestión de configuración se encuentran las siguientes.

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

### **2.5.3. Gestión de Contabilidad / Administración**

Conocida también como administración de facturación, se enfoca principalmente en el registro de uso de los recursos y servicios facilitados por la red a los distintos abonados. Dentro de las funciones en esta área, se incluyen la recopilación de los datos sobre el manejo de los recursos, mantenimiento del registro de cuentas de usuario, sostenimiento de estadísticas de uso y la definición de procedimientos para tarificación.

Para el caso en que no se necesite gestionar redes tarifadas, la administración reemplaza a la contabilidad, donde el principal objetivo es gestionar el conjunto de usuarios autorizados estableciendo users contraseñas y permisos además de administrar las operaciones de los equipos como realizar backups de software. (Mejía, 2018, p.30).

### **2.5.4. Gestión de Rendimiento / Performance**

En esta área se encarga del monitoreo constante del correcto funcionamiento de los dispositivos gestionados y la efectividad de determinadas actividades, además de recolectar y procesar los datos medidos para la elaboración de informes, garantizando que la red gestionada funciones según lo esperado y que se usen de manera eficiente los recursos de la red.

Dentro de las tareas recomendadas por el modelo en esta área de gestión, se tiene.

- Capturar datos o variables indicadoras de rendimiento, tales como la tasa de datos efectiva de la red, tiempos de respuesta de los usuarios, utilización del CPU, memoria disponible, utilización de disco, puertos disponibles, entre otros.
- Analizar los datos para determinar los niveles normales de rendimiento
- Establecer indicadores de problemas en el rendimiento de la red.
- Determinar un sistema de procesamiento periódico de datos de desempeño acerca de los distintos equipos en la red para sus estudios permanente.
- Generar informes y estadísticas.

### **2.5.5. Gestión de Seguridad / Security**

Se encarga de cuidar la infraestructura de red contra los accesos no autorizados, se lo relaciona generalmente a la generación, distribución y almacenamiento de passwords, información de contraseñas, también de implementar protección a los equipos de comunicación, servidores y estaciones de trabajo de ataques provenientes de terceros que ayuda en la conservación de la integridad del sistema (Terán, 2020, p.22).

Para la seguridad de la infraestructura de red se debe proteger contra, hackers, usuarios no autorizados, además de daños físicos o electrónicos, de esta manera el personal adecuado puede vigilar lo que cada usuario autorizado puede o no puede hacer en el sistema. El modelo recomienda las siguientes tareas en esta área.

- Monitoreo de la red frente a ataques.
- Encriptado de la información
- Establecimiento de procedimientos de autenticación
- Implementación de medidas de seguridad.
- Mantenimiento de la información de seguridad
- Control de acceso a los recursos.
- Proteger la información confidencial mediante la configuración de directivas de cifrado
- Mantener reportes de intentos de intrusiones para su posterior análisis.

## **2.6. Servidor**

Un servidor es el encargado de proporcionar recursos, datos, servicios o programas a otras computadoras, las cuales se denominan clientes, en una red. Este equipo se trata de un dispositivo que puede ser software o hardware que responde a las distintas solicitudes realizadas a través de la red.

Estos servidores actualmente pueden ser solo software que se ejecuta en uno o más dispositivos físicos, éste a menudo se llama servidor virtual, inicialmente se utilizaron para aumentar la cantidad de funciones que podría realizar un solo servidor de hardware.

Actualmente, los servidores virtuales normales se ejecutan en la nube, lo que implica que se ejecuta en hardware que es propiedad de un tercero y se puede acceder a él a través de internet. (Maruri & Vargas, 2021, p.24).

### **2.6.1. Funcionamiento**

En el servidor se ejecutan aplicaciones que pueden responder a las solicitudes de los clientes, este dispositivo se encarga de escuchar todas las peticiones de los usuarios que se encuentran en el entorno de red, esta funcionalidad puede existir como parte del sistema operativo, es decir, como una aplicación o software instalado. Adicionalmente hay que tener en cuenta que una función o servicio instalado aumenta el número de tipos de solicitudes de cliente a las que el servidor puede responder.



**Ilustración 17-2:** Solicitud de Servicios.

Fuente: Maruri E., Vargas J., 2021, p.25.

## 2.6.2. Tipo de servidores

Dependiendo de las funcionalidades diferentes, en la mayoría de redes se puede encontrar al menos uno de los tipos de servidores más comunes.

### 2.6.2.1. Servidor de archivos

Almacenan y distribuyen archivos que pueden ser compartidos por varios clientes o usuarios, el almacenamiento de archivos centralizado permite la implementación de copias de seguridad o tolerancia a fallas más fácil que intentar garantizar la seguridad e integridad de archivos para todos los dispositivos de una organización. Este tipo de servidores posee un hardware optimizado para acelerar la lectura y escritura de archivos.

### 2.6.2.2. Servidor proxy

Actúa como un mediador entre el cliente y el servidor, suele utilizarse para aislar a un cliente o a el servidor como medida de protección, el servidor se encarga de reenviar la solicitud del cliente a otro servidor y viceversa, por lo que ni el cliente ni el servidor real están realmente conectados entre sí.

### 2.6.2.3. Servidor de base de datos

Todos los datos que utiliza la empresa, los usuarios, y otros servicios son almacenados en esta clase de equipos, en estos servidores se ejecutan aplicaciones de base de datos y responde a muchas solicitudes de clientes, los aplicativos más populares son, Oracle, Microsoft SQL Server, DB2 e Informix.

#### *2.6.2.4. Servidor web*

Este tipo se encarga del alojamiento web, en este se almacena programas y datos solicitados por los usuarios en internet, algunos de los servidores más conocidos incluyen, Apache Server, Microsoft Internet Information Services (IIS) y Nginx.

#### *2.6.2.5. Servidor DNS*

Este servidor es el encargado de traducir los nombres legibles por el humano a una dirección IP que pueda entender la máquina, cuando el cliente solicita una dirección del sistema, el servidor DNS recibe el nombre del recurso deseado para después responder con la dirección IP correspondiente en la tabla de nombres.

#### *2.6.2.6. Servidor de aplicaciones*

Se compone de contenedores los cuales contienen la lógica empresarial del sistema y brindan respuestas a las solicitudes de los distintos dispositivos que pueden acceder a él.

#### *2.6.2.7. Servidores de Supervisión y administración*

Actualmente existe muchos servidores que se utilizan para monitorear o administrar otros sistemas o clientes. Entre estos, existen del tipo que solo escucha a la red y recibe todas las solicitudes y respuestas de los clientes, mientras que los otros solicitan esta información a los clientes. Entre los principales servidores de monitoreo, se puede mencionar a Cacti, ACS, Zabbix, Nagios, entre otros.

### **2.6.3. Ubuntu Server LTS**

Este sistema operativo es una de las distribuciones Linux más utilizadas a la hora del levantamiento de servidores, pues dispone de gran rendimiento para las distintas funcionalidades de servidores y para la virtualización con dockers, entre otras características.

Por defecto este sistema operativo ofrece una interfaz de línea de comandos, mediante el cual se puede instalar los diferentes aplicativos para el desarrollo y administración de los distintos servidores que se requiera implementar. (Madrid, 2014, p.13).

Para su instalación el hardware del host debe poseer como mínimo las siguientes características:

- 2.5 GB de espacio libre en el disco
- 1 GB de memoria RAM
- Procesador a 1 GHz o superior
- Un dispositivo DVD o puerto USB para el soporte de instalación
- Conexión disponible a Internet.

## 2.7. Herramientas de monitoreo de red

Para poder realizar un adecuado monitoreo de una red de datos, en el mercado existe una gran variedad de programas de paga o libres que pueden llegar a cubrir las necesidades de monitoreo. En este apartado se hace mención de los principales softwares de código abierto de monitoreo de red y sus principales características. En la siguiente tabla comparativa se presenta varios de estos softwares, colocando un check en la casilla correspondiente a la característica que posee cada herramienta de monitoreo.

**Tabla 4-2:** Comparativa entre las diferentes herramientas de monitoreo de código abierto.

Característica	Nagios	Zabbix	Pandora FMS	PRTG Network Monitor	OpenNMS	OPSview	Zenoss
Monitoreo de red	✓	✓	✓	✓	✓	✓	✓
Monitoreo en la nube	✓	✓	✓	✓		✓	
Monitoreo de aplicaciones	✓	✓	✓	✓		✓	✓
Monitoreo de servidores	✓	✓	✓	✓	✓	✓	✓
Monitoreo web o remoto	✓	✓	✓	✓			
Dispositivos de almacenamiento	✓	✓	✓				
Monitoreo de máquina virtuales	✓	✓	✓	✓	✓	✓	✓
Aplicaciones java		✓			✓		
Monitoreo de base de datos	✓	✓	✓	✓	✓	✓	✓
KPI/SLA		✓	✓				
Telefonía	✓	✓	✓	✓	✓	✓	✓
Monitoreo de seguridad	✓	✓		✓	✓	✓	
Temperatura de un servidor	✓	✓	✓	✓	✓	✓	✓



Temperatura de un sistema	✓	✓	✓	✓	✓	✓	✓
Monitoreo de sistema operativo	✓	✓	✓	✓	✓	✓	✓
Servidor de respaldo				✓			
Monitoreo de rendimiento de un computador	✓					✓	
Monitoreo de correo electrónico	✓	✓	✓	✓	✓	✓	✓

Fuente: Intriago, M., 2019

Realizado por: Intriago, M, 2019, p.15.

Según el trabajo realizado por Intriago (2019, p.33) se determina que las herramientas que son más fáciles de implementar y configurar fueron Zabbix y PRTG, mientras que el proceso para la instalación y configuración para Nagios y Pandora FMS resultó más complejo además, en su evaluación de características, se determinó a Nagios como la herramienta de mayor nivel de cumplimiento con los parámetros presentados, aunque la herramienta PRTG cuenta con muy buenas especificaciones y administración sencilla, su uso se descarta debido a la necesidad de adquirir la licencia para utilizar todas sus funciones.

Los resultados obtenidos por Intriago (2019, p.33) evidencian el cumplimiento de las características mostradas en la Tabla 4-2 las mismas que abarcan las necesidades de monitoreo a ser cubiertas en la infraestructura de la empresa Intertec, por tal motivo se toma la decisión de optar por la implementación de la herramienta Nagios para el monitoreo de red en el sistema de gestión.

### 2.7.1. Nagios Core

Se trata de un sistema de monitorización de código abierto, con el cual los administradores de red pueden realizar un monitoreo completo de los equipos activos de una manera exhaustiva, lo que permite la identificación y control de problemas que puedan ocasionar un mal funcionamiento de una red antes de que los usuarios lo perciban, entre las principales características de monitorización de servicios de red, se incluyen SMTP, POP3, HTTP, SNMP, etc. Además de la vigilancia de los recursos del hardware como son, la carga del procesador, uso de los discos, memoria, estado de los puertos, etc.

Alguna de otras características que presenta este software de monitorización, son las siguientes.

- Diseño de plugins simple que permite a los usuarios desarrollar fácilmente sus propios chequeos de servicios.
- Chequeo de servicios paralizados.
- Habilidad para definir redes de host de forma jerárquica, mediante el atributo “*parents*”, permitiendo la detección y distinción entre hosts que están caídos y aquellos que son inalcanzables.
- Definición de contactos para notificar cuando ocurre problemas en un servicio o host a través de varios métodos como un e-mail.
- Habilidad para definir Event Handlers para que se activen durante eventos de hosts o servicios para lograr una resolución de problemas proactivos.
- Rotación automática de Archivos Log.
- Soporte para implementar hosts de monitoreo redundantes.
- Interfaz web para la visualización de status actual de la red, notificaciones, historial de problemas, archivos log, etc. (Nagios, 2022)



**Ilustración 18-2:** Logotipo de Nagios Core.

**Fuente:** Nagios Core, 2022.

La funcionabilidad de Nagios se basa en los distintos archivos de configuración en donde se puede especificar los componentes de red a ser monitoreados, con qué periodo y frecuencia se lo realiza, a quien y como se enviará los resultados de la monitorización.

Nagios Core, tiene el objetivo principal de procesar toda la información enviada por los *plugins*, además de ser el contenedor de todo el programa para la realización del monitoreo de los equipos y servicios de red. Estos *plugins* también son conocidos como *scripts*, son pequeños programas escritos en varios lenguajes de programación, como c, c++, php, Python, java, etc, cuya labor principal es la recolección de información de la monitorización predefinidos en los archivos de configuración. Además, utiliza una interfaz web que permite visualizar de forma gráfica los distintos equipos activos de red y obtener los resultados de monitorización. (Madril, 2014, p.31).

### *2.7.1.1. Requerimientos mínimos para la instalación de Nagios Core*

Nagios Core fue diseñado principalmente para correr sobre sistemas Linux, sin embargo, debería funcionar también en otros sistemas operativo, para la implementación es necesario tener acceso a internet y un compilador C instalado, además de los siguientes componentes.

- Sistema operativo Linux o variante UNIX
- Compilador C instalado
- Biblioteca de gráficos GD de Thomas Boutell, versión 1.6.3 o superior.
- Servidor Web Apache
- PHP y SNMP.

## CAPÍTULO III

### 3. MARCO METODOLÓGICO

#### 3.1. Situación actual de la empresa

La empresa Intertec es una empresa privada Proveedora de Servicios de Internet (ISP), que se encuentra ubicada en la ciudad de Riobamba provincia de Chimborazo, establecida en el año 2019, su giro de negocio principal es la de ofrecer el servicio de acceso a internet mediante radioenlaces y recientemente por fibra óptica, la misión de la empresa se resume en “proveer el acceso a las tecnologías de la información a las áreas urbanas y rurales de Chimborazo usando infraestructura de telecomunicaciones de última generación”.

En la actualidad la empresa Intertec cuenta con una cantidad considerable de abonados al servicio de acceso a internet, tanto en sector urbano como en rural, por lo cual el tráfico de datos ha ido en aumento, lo que da como resultado la incorporación de un mayor número de equipos en la infraestructura de red de la empresa, provocando que su gestión y mantenimiento manual se vuelve más compleja.

##### 3.1.1. Portafolio de servicios

Aunque el servicio principal de la empresa Intertec es el de ofrecer el acceso a Internet, también cuenta con otros servicios de valor agregado disponible para los clientes naturales y corporativos, los mismos que se indican en la siguiente Tabla 1-3.

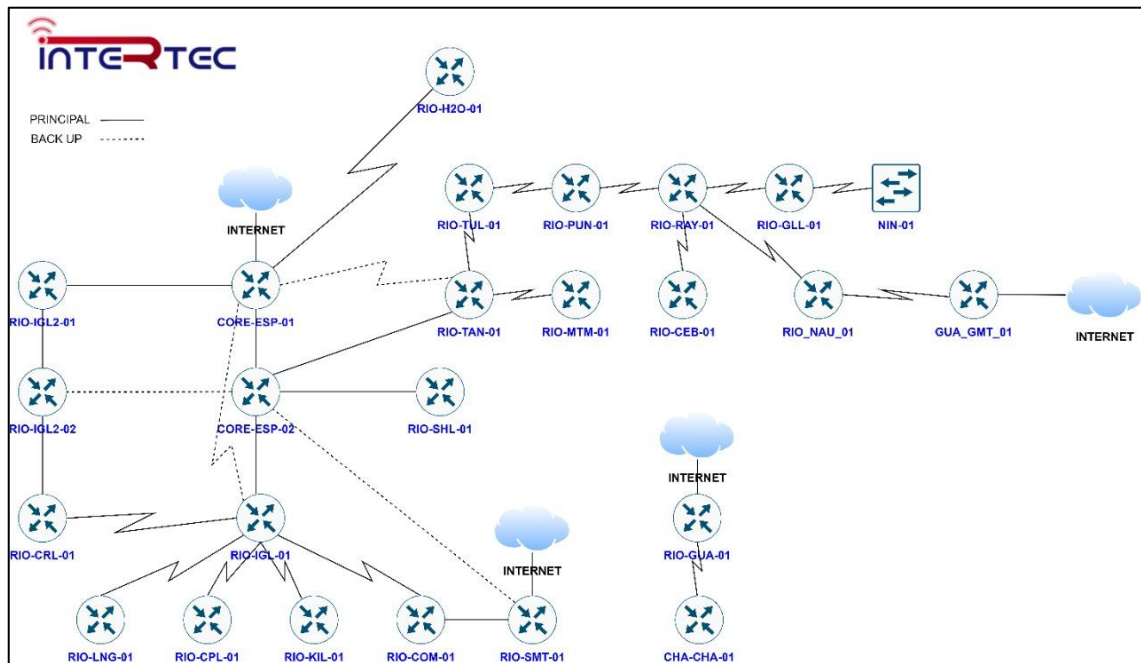
**Tabla 1-3:** Servicios que ofrece la empresa Intertec.

<b>Servicio</b>	<b>Descripción</b>
Consultoría Networking	Asesoría para el diseño, instalación, mantenimiento y soporte técnico de proyectos de redes y telecomunicaciones.
Diseño Web	Se enfoca en el diseño y hosting de páginas web.
Soluciones IoT	La empresa ofrece soluciones integrales IoT para cubrir las distintas necesidades del cliente.
Acceso a Internet	Se ofrece acceso a internet, por fibra óptica y radioenlace para clientes residenciales y corporativos, brindando una conexión rápida y eficiente.

**Fuente:** Intertec, 2022.

**Realizado por:** Sagnay, Mauro, 2022.

### 3.1.2. Topología de la red de Intertec.








**Ilustración 1-3:** Topología General de la red de la empresa Intertec.

Fuente: Intertec, 2022.

En la Ilustración 1-3 se aprecia la topología general de toda la red implementada por la empresa Intertec para brindar sus servicios, en la misma se puede apreciar los enlaces principales utilizados para la salida internacional a internet, además de la distribución de los distintos nodos que se ubican en locaciones geográficamente separadas con el fin de transportar los datos generado por los abonados. Se puede observar también que la tecnología utilizada para la interconexión entre los nodos corresponde a radioenlace y por fibra óptica. La topología que se observa utiliza la siguiente simbología.

**Tabla 2-3:** Simbología de red utilizada.

Simbología	Descripción	Simbología	Descripción
—————	Enlace principal de fibra óptica		Router para la interconexión de los nodos.
-----	Enlace backup o secundario de fibra óptica.		Switch de capa dos
~~~~~	Enlace principal radioeléctrico.		Red externa o salida a Internet.

	Equipo OLT para los enlaces de fibra óptica.		Servidores
-----------------------------------------------------------------------------------	----------------------------------------------	------------------------------------------------------------------------------------	------------

Fuente: Intertec, 2022.

Realizado por: Sagñay, Mauro, 2022

### 3.2. Requerimientos que debe cubrir el sistema de gestión de red.

La instalación del software de gestión de red se realiza en uno de los servidores que forman parte de la red local de servidores ubicados en la infraestructura de la empresa, cabe mencionar que dentro de la empresa se manejan tecnologías como Telefonía IP, computadores, routers, switches, cámara de seguridad, grabadores DVR y lector biométrico, los detalles de las marcas, modelos, configuración, diseño de red, entre otros aspectos no se incluyen en este trabajo por cuestiones de confidencialidad y seguridad de la empresa Intertec.

Como se mencionó anteriormente, el software de monitoreo de red elegido para la implementación del sistema de gestión es Nagios Core, el mismo que se instala sobre el sistema operativo de Ubuntu Server. De manera general, el servidor deberá tener acceso a internet para la descarga de los distintos paquetes de actualización del sistema operativo, el servidor debe ser exclusivo para albergar a Nagios Core debido a que su procesamiento va en aumento con el crecimiento de la red.

Los principales requerimientos que la empresa necesita cubrir se especifican en la siguiente tabla.

**Tabla 3-3:** Descripción de los requerimientos de monitoreo que necesita la empresa.

Requerimientos	Descripción
Monitoreo en Tiempo Real	El operador de red puede tener acceso a la información en tiempo real para determinar si la red está funcionando correctamente.
Detección de caídas de enlaces	El sistema deberá ser capaz de determinar cuándo un enlace inalámbrico está caído e informar al operador respectivo.
Monitoreo de equipos	El sistema deberá ser capaz de recopilar la información del estado del equipo para determinar y prevenir averías.
Gráficas de Tráfico	El sistema debe permitir la generación de graficas de los datos recopilados.
Topología de la red	El sistema debe incluir un apartado que dibuje la topología de red según los dispositivos monitoreados.

Integración de Notificaciones	El sistema deberá enviar las distintas notificaciones al correo electrónico o a un aplicativo de mensajería instantánea.
-------------------------------	--------------------------------------------------------------------------------------------------------------------------

Fuente: Intertec, 2022

Realizado por: Sagnay, Mauro, 2022.

### 3.3. Implementación de la herramienta de monitoreo Nagios Core

Previo a la implementación del sistema de gestión de red, conjuntamente con la gerencia de la empresa Intertec, se ha convenido el horario y acceso a los equipos y software necesarios ubicados en las instalaciones de la empresa, además, entre las partes se ha suscripto un Acuerdo de Confidencialidad y No Divulgación de la Información para la Empresa, en honor al cual, en el presente trabajo no se hace mención del direccionamiento IP, ubicación geográfica de los nodos, número de puertos, modelos y marcas de los equipos utilizados y otros datos que la empresa considere “información confidencial”.

#### 3.3.1. Instalación del software Nagios Core

Como se ha mencionado anteriormente, la instalación se lo realiza en un servidor de la empresa con el sistema operativo Ubuntu Server basado en Linux, por lo cual, la descarga de paquetes y la instalación se lo realizará por medio de la línea de comandos.

#### Instalación de prerequisites para Ubuntu Linux

```
sudo apt-get update

sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2
php libapache2-mod-php7.4 libgd-dev

sudo apt-get install openssl libssl-dev
```

#### Descargar la última versión de Nagios Core

```
cd /tmp

wget -O nagioscore.tar.gz
https://github.com/NagiosEnterprises/nagioscore/archive/nagios-
4.4.6.tar.gz

tar xzf nagioscore.tar.gz
```

#### Compilar

```
cd /tmp/nagioscore-nagios-4.4.6/

sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled

sudo make all
```

Creación de Usuario y Grupo de trabajo: como manera de ejemplo, se ha creado el usuario y grupo “nagios”, además se ha añadido el usuario www-data.

```
sudo make install-groups-users
sudo usermod -a -G nagios www-data
```

Instalación de Binaries: se instalan los archivos binary, CGIs, y HTML.

```
sudo make install
```

Instalación del Servicio/Daemon: estos archivos se instalan y configuran para iniciar el software

```
sudo make install-daemoninit
```

Instalación de los Modos de Comando

```
sudo make install-commandmode
```

Instalación de los archivos de configuración: además de los archivos necesarios para Nagios, también se instalan archivos de ejemplo

```
sudo make install-config
```

Instalación de los archivos de Configuración Apache: se utiliza para configurar el Apache web server.

```
sudo make install-webconf
sudo a2enmod rewrite
sudo a2enmod cgi
```

Configuración de Firewall: se debe permitir el tráfico entrante en el Puerto 80, para poder ingresar a la interfaz web de Nagios Core.

```
sudo ufw allow Apache
sudo ufw reload
```

Para ingresar a la interfaz web, se necesita crear una cuenta de usuario en Apache, con fines didácticos se creará el usuario llamado “nagiosadmin”, luego se deberá proveer una contraseña adecuada.

```
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

A continuación, se procede a inicializar el servidor web Apache.

```
sudo systemctl restart apache2.service
```

Luego, se realiza la inicialización del servicio de Nagios.

```
sudo systemctl start nagios.service
```



Ahora, Nagios ya se encuentra operativo, pero todavía se debe instalar complementos llamados plugins, estos sets de paquetes son necesarios para que Nagios Core pueda operar apropiadamente.

De manera inicial se instalan los siguientes prerequisites

```
sudo apt-get update

sudo apt-get install -y autoconf gcc libc6 libmcrypto-dev make
libssl-dev wget bc gawk dc build-essential snmp libnet-snmp-perl
gettext
```

Luego se descarga la última versión del paquete de plugins

```
cd /tmp

wget --no-check-certificate -O nagios-plugins.tar.gz
https://github.com/nagios-plugins/nagios-plugins/archive/release-
2.4.0.tar.gz

tar xzf nagios-plugins.tar.gz
```

Por último, se compila y se instala.

```
cd /tmp/nagios-plugins-release-2.4.0/

sudo ./tools/setup

sudo ./configure

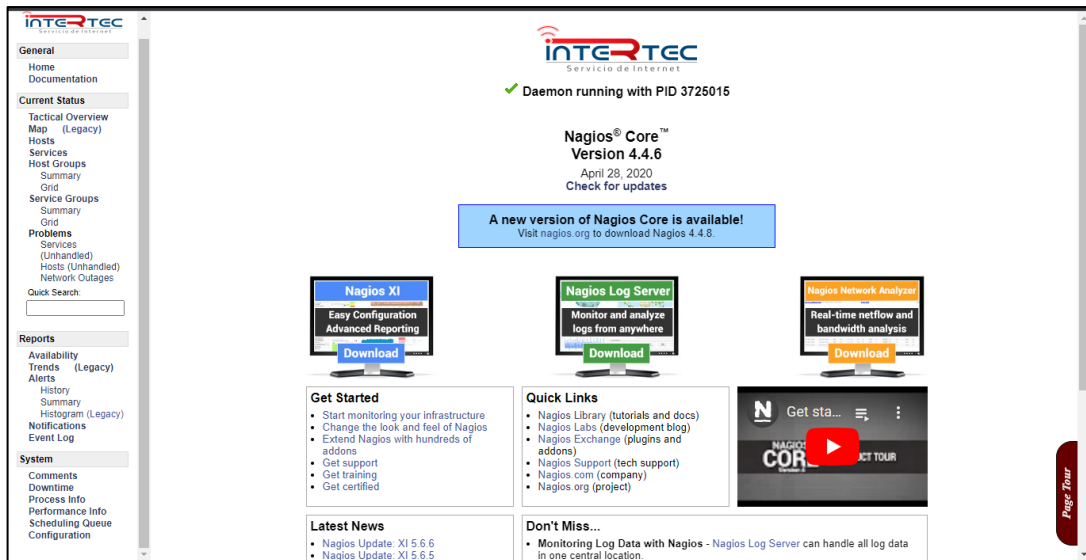
sudo make

sudo make install
```

Ahora, ya se puede ingresar a la interfaz web de Nagios utilizando un navegador web, ingresando la dirección IP del servidor, como se muestra un ejemplo ilustrativo a continuación,

```
http://10.25.5.143/nagios
```

Entonces se ingresa las credenciales antes creadas y obtenemos la siguiente pantalla.

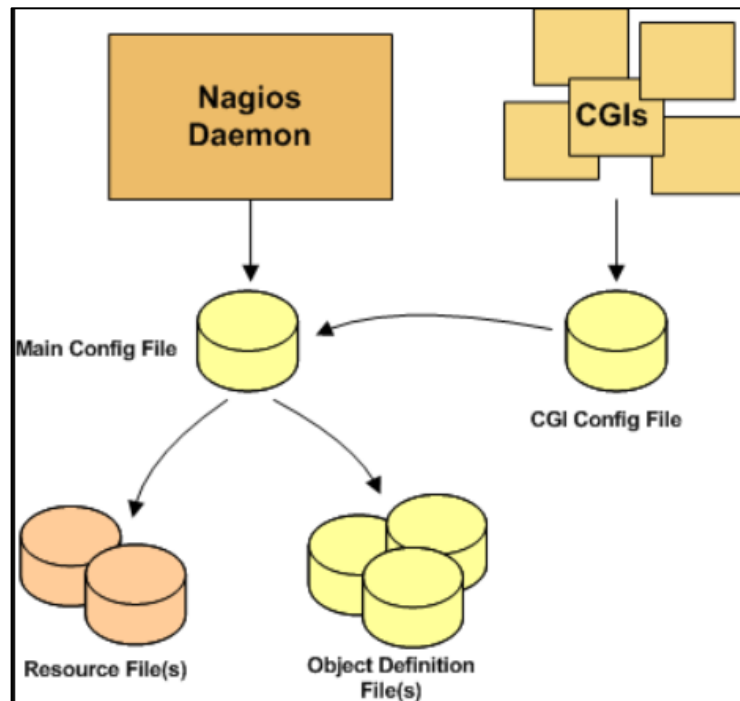


**Ilustración 2-3:** Página Inicial de la herramienta de monitoreo Nagios Core.

Realizado por: Sagnay, Mauro, 2022.

### 3.3.2. Configurando Nagios Core

Dentro los ficheros de Nagios se encuentran diferentes tipos de archivos de configuración los cuales son esenciales para monitorear cualquier equipo o dispositivo.



**Ilustración 3-3:** Funcionamiento de la herramienta Nagios Core.

Fuente: Nagios Core, 2022.

Estos se utilizan para adecuar la forma de monitoreo que se desea para cubrir las diferentes necesidades de la empresa, es decir, mediante la edición de estos archivos de configuración se

podrá variar el comportamiento general del software Nagios Core y obtener los resultados deseados.

#### *3.3.2.1. Archivo de Configuración Principal / Main Configuration File*

Se trata del archivo que contiene varias directivas que afectan cómo funciona el daemon de Nagios Core, como se observa en la Ilustración 3-3 este archivo es leído por ambos, el Nagios daemon y el CGI.

#### *3.3.2.2. Archivos de Recursos / Resource Files*

Es usada principalmente para guardar los macros definidos por el usuario, generalmente se utiliza para el almacenamiento de archivos sensibles, como información de configuración, sin que pueda ser leída por los CGIs.

#### *3.3.2.3. Archivos de Definición de Objetos / Object Definition Files*

Como su nombre lo indica, se trata de archivos que se utiliza para definir, hosts, servicios, grupos de hosts, contactos, comandos, entre otros.

En estos archivos es donde el usuario define todas las cosas que se desea monitorear y como se desea monitorearlos.

#### *3.3.2.4. Archivos de Configuración CGI / CGI Configuration File*

Estos archivos contienen varias directivas las cuales afectan como se visualiza la información para el usuario, como son, las pantallas de status de la red monitoreada, el mapa de hosts, la lista de problemas, la lista de eventos, entre otros.

### **3.3.3. Objetos en Nagios**

En el sistema Nagios, existe los objetos, que no son más que todos los elementos que están involucrado en el monitoreo y la lógica de notificaciones, dentro de los cuales se incluyen los siguientes tipos.

- Hosts.
- Servicios.
- Grupos de hosts y servicios.
- Contactos y grupo de contactos.
- Comandos.
- Periodo de tiempos.
- Notificaciones.
- Ejecución.

### 3.3.3.1. Definición de objetos

La definición de objetos en Nagios se lo realiza en ficheros con la extensión “.cfg”, los mismos que pueden ser creados en cualquier parte, pero su ubicación debe ser incluida en `/usr/local/nagios/etc/nagios.cfg` y el usuario de Nagios debe tener permisos para leerla.

Por defecto al momento de su instalación, Nagios ya trae unos cuantos ficheros de ejemplo para la definición de los objetos en la siguiente ubicación `/usr/local/nagios/etc/objects`, en ellos se encuentran archivos para monitorear máquinas Windows, Linux, Switches, Impresoras, entre otras.

### 3.3.3.2. Definición de un host.

Los hosts son los objetos centrales en la lógica de monitorización, y de manera general para monitorear cualquier equipo/host, se tiene el siguiente formato.

```
define host{
use          windows-server      ;
host_name    Windows 50         ;
alias        Equipo 50          ;
address      192.168.1.50       ;
hostgroups   equipos            ;
}
```

Detalles de los valores.

- Use: En este campo se indica una plantilla de la cual se hereda la configuración. En caso de conflicto porque una misma directiva se utilice tanto en la plantilla con la definición de un host, siempre tendrá prioridad el valor que se establece en la definición host.
- Host\_name: Nombre o descripción usada para identificar al host
- Address: Dirección IP del equipo a monitorear
- Hostgroups: Nombre del hostgroup al que pertenece.

Además de los atributos mencionados, en Nagios Core se permite la inclusión de más atributos que brindan mayores funciones, sin embargo, para efectos de este trabajo con los ya especificados son suficientes.

### 3.3.3.3. Definición de un servicio

Para la definición de servicios para cada host, se debe especificar el servicio a ser monitoreado, los mismo pueden ser diferentes dependiendo del host y la necesidad, para definir los servicios se utiliza el siguiente formato.

```
define service{
use                generic-service
host_name          Windows 50
service_description NSClient++ Version
check_command      check_nt!CLIENTVERSION
}
```

Detalle de los valores.

- Use: es igual al caso de la definición de hosts, es decir, se emplea para utilizar una plantilla.
- Host\_name: es el nombre del host al cual se le aplicará la monitorización de este servicio, también se le puede aplicar a un grupo de host, con la directiva hostgroup\_name en su lugar.
- Service\_description: Nombre descriptivo para el servicio.
- Check\_command: El comando que usará este servicio junto con su variable

Para que los cambios de configuración realizados tengan efecto, se deberá reiniciar y comprobar que la monitorización se ha realizado correctamente.

Para verificar que la configuración no tenga errores, se ingresa mediante consola el siguiente comando.

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

El reinicio se lo puede hacer de dos formas, desde un terminal o desde la interfaz web, para hacerlo desde el terminal se realiza el siguiente comando.

```
sudo systemctl restart nagios.service
```

Una vez realizado todo el proceso de configuración inicial, se procede con la instalación de los distintos complementos para cubrir las necesidades de monitoreo requeridos por la empresa.

### 3.3.4. Instalación de PNP4Nagios para la generación de gráficos

El complemento PNP4Nagios permite a Nagios Core la generación de gráficos del desempeño de la red que se está monitoreando. Este programa externo cumple la función de recopilar los datos recibidos por Nagios Core para luego procesarlos y graficar los mismos.

Dentro de sus funciones se encuentran las siguientes:

- Procesar y guardar los datos de desempeño recibidos en archivos Round Robin Database (RRD).
- Utiliza un GUI para mostrar los archivos RRD dentro de la interfaz gráfica de Nagios Core.

De manera inicial se procede con la instalación de los paquetes de prerequisites.

```
sudo apt-get update
sudo apt install rrdtool librrdp-perl php-gd php-xml
sudo apt install librrd-dev librrds-perl
```

Luego se descarga de la fuente, el módulo pnp4nagios.

```
cd /tmp
wget -O pnp4nagios.tar.gz
https://github.com/linge/pnp4nagios/archive/0.6.26.tar.gz
tar xzf pnp4nagios.tar.gz
```

Una vez descargado, se compila e instala.

```
cd pnp4nagios-0.6.26
sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
sudo make all
sudo make install
sudo make install-webconf
sudo make install-config
sudo make install-init
```

Por último, se configura y se inicia el Servicio/Daemon

```
sudo systemctl daemon-reload
sudo systemctl enable npcd.service
sudo systemctl start npcd.service
sudo systemctl restart apache2.service
```

De esta manera el módulo PNP4Nagios ya se encuentra corriendo como servicio npcd (Nagios-Perfdata-C-Daemon).

El siguiente paso es configurar Nagios Core para enviar los datos de desempeño a PNP4Nagios.

Esto se logra modificando el archivo de configuración ubicado en: /usr/local/nagios/etc/nagios.cfg quedando de la siguiente manera:

```
process_performance_data=1

host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata

host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::\$TIMET$\
tHOSTNAME::\$HOSTNAME$\tHOSTPERFDATA::\$HOSTPERFDATA$\tHOSTCHECKCOMMA
ND::\$HOSTCHECKCOMMAND$\tHOSTSTATE::\$HOSTSTATE$\tHOSTSTATETYPE::\$HOS
TSTATETYPE$

host_perfdata_file_mode=a

host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file-
```

```

bulk-npcd

service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata

service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$\tSERVICES-TATE::$SERVICESTATE$\tSERVICESTATETYPE::$SERVICESTATETYPE$

service_perfdata_file_mode=a

service_perfdata_file_processing_interval=15

service_perfdata_file_processing_command=process-service-perfdata-
file-bulk-npcd

```

Además, se deben definir 2 comandos para Nagios, los mismos que se deben colocar en el siguiente archivo `/usr/local/nagios/etc/objects/commands.cfg` quedando de la siguiente manera.

```

define command {
    command_name    process-service-perfdata-file-bulk-npcd
    command_line    /bin/mv /usr/local/pnp4nagios/var/service-
perfdata /usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$
}

define command {
    command_name    process-host-perfdata-file-bulk-npcd
    command_line    /bin/mv /usr/local/pnp4nagios/var/host-perfdata
/usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$
}

```

Para que los cambios tengan efecto, se debe reiniciar el servicio de Nagios Core.

```

sudo systemctl restart nagios.service

```

Ahora ya se podrá acceder a la interfaz web de PNP4Nagios a través de la dirección IP del servidor Nagios, como se aprecia a continuación.

```

http://ip_nagios_server/pnp4nagios/

```

Para poder ingresar rápidamente a las gráficas de cada parámetro que se necesite, lo que se hace es integrarlo a la interfaz web de Nagios Core. Esto se logra, añadiendo una plantilla o template en el siguiente archivo `/usr/local/nagios/etc/objects/templates.cfg` quedando de la siguiente forma.

```

define host {
    name            host-pnp
    action_url
/pnp4nagios/index.php/graph?host=$HOSTNAME&srv=_HOST_
    register       0
}

```

```

define service {
    name          service-pnp
    action_url
    /pnp4nagios/index.php/graph?host=$HOSTNAME&&srv=$SERVICEDESC$
    register      0
}

```

Para usar estos templates se necesita incluirlos en las directivas de los dispositivos y servicios, quedando de la siguiente manera.

```

define host{
    name          generic-host      ;
    use           host-pnp
}

define service{
    name          generic-service    ;
    use           service-pnp
}

```

Por último, para que los cambios tengan efecto, se debe reiniciar el servicio de Nagios Core

```
sudo systemctl restart nagios.service
```

Así entonces, alado de cada servicio de cada host, se observará un icono que al hacer clic se abrirá una gráfica del host o servicio en la interfaz web de PNP4Nagios.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	07-21-2022 16:08:01	15d 23h 1m 12s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	07-21-2022 16:08:39	15d 23h 1m 4s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	07-21-2022 16:09:14	15d 23h 0m 55s	1/4	HTTP OK: HTTP/1.1 200 OK - 11192 bytes in 0.026 second response time
	PING	OK	07-21-2022 16:09:50	15d 23h 0m 47s	1/4	PING OK - Packet loss = 0%, RTA = 0.06 ms
	Root Partition	OK	07-21-2022 16:10:28	15d 23h 0m 31s	1/4	DISK OK - free space: / 6563 MB (46 00% inode=87%)
	SSH	OK	07-21-2022 16:10:37	15d 23h 2m 10s	1/4	SSH OK - OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 (protocol 2.0)
	Swap Usage	OK	07-21-2022 16:11:11	15d 23h 1m 33s	1/4	SWAP OK - 100% free (3227 MB out of 3227 MB)
	Total Processes	OK	07-21-2022 16:11:12	15d 23h 0m 55s	1/4	PROCS OK: 109 processes with STATE = RSZDT

**Ilustración 4-3:** Integración de PNP4Nagios en la interfaz web de Nagios Core.

Realizado por: Sagñay, Mauro, 2022.





**Ilustración 5-3:** Interfaz web de PNP4Nagios.

Realizado por: Sagñay, Mauro, 2022.

### 3.3.5. Monitoreo de Equipos

El monitoreo de switches y routers es esencial para la infraestructura de un ISP, el software Nagios Core puede monitorear fácilmente estos equipos utilizando la herramienta PING a modo de un keep alive y para determinar la pérdida de paquetes, RTA, entre otras características.

Para una mejor gestión, se utiliza el protocolo SNMP para verificar el status de los diferentes parámetros del switch o router, esto se logra mediante la utilización del plugin check\_snmp, que se debe especificar en el apartado de servicios del software Nagios.

Para habilitar el monitoreo de equipos se sigue los siguientes pasos.

Si se va a monitorear por primera vez, se ingresa en el archivo de configuración de Nagios.

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

Y se remueve el símbolo #, para poder habilitar el archivo de configuración

```
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg
```

Ahora, para monitorear un equipo del tipo switch o router, se deberá crear un *object definition*, editando el archivo de configuración switch.cfg. Para lo cual los datos que se modifican, son el host\_name, alias, la dirección IP y el hostgroup, de esta manera con estos datos se deberá comunicar con el switch o router que se necesite monitorear, quedando de la siguiente manera.

```

define host {
use          generic-switch          ;
host_name    router_1                ;
alias        Router de Borde        ;
address      192.168.1.253          ;
hostgroups   allhosts, switches     ;
}

```

Para monitorear los diferentes parámetros de los equipos, se puede añadir un *service definition*, en el mismo archivo de configuración, como se indica a continuación.

### 3.3.5.1. Monitoreo de pérdida de paquetes y RTA

En el siguiente *service definition*, se monitorea la pérdida de paquetes y Round Trip Average entre el servidor Nagios Core y el equipo router\_1 con un periodo de 5 minutos bajo condiciones normales, mediante la herramienta PING.

```

define service {
use          generic-service          ;
host_name    router_1                ;
service_description    PING          ;
check_command    check_ping!200.0,20%!600.0,60% ;
normal_check_interval    5          ;
retry_check_interval    1          ;
}

```

### 3.3.5.2. Monitoreo de información de estatus mediante SNMP

Se puede monitorear una gran cantidad de parámetros mediante SNMP, usando el plugin `check_snmp`, de igual forma que el anterior, se debe crear un *service definition*. Como un ejemplo ilustrativo, se procede a monitorear el parámetro Uptime del equipo router\_1.

```

define service {
    use          generic-service          ;
    host_name    router_1                ;
    service_description    Uptime        ;
    check_command    check_snmp!-C public -o sysUpTime.0 ;
}

```

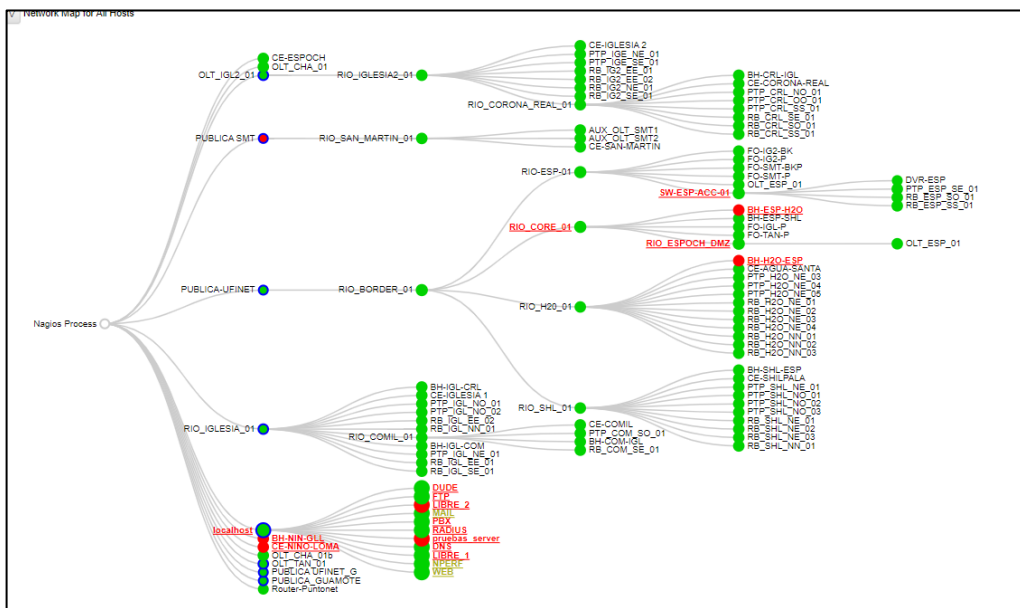
En el atributo `check_command` se indica la utilización del protocolo SNMP mediante `check_snmp` en el cual, “-C public” es la comunidad SNMP en la que forma parte el equipo `router_1`, para este ejemplo ilustrativo es “public” y el “-o sysUpTime.0” indica cual OID debería ser chequeado.

### 3.3.6. Gráficas de Tráfico

Para obtener las gráficas de tráfico se puede utilizar el servicio antes mencionado de SNMP, para realizarlo en un *service definition* en el cual se debe indicar el OID específico para el puerto o interfaz que se desea obtener la gráfica.

### 3.3.7. Topología de Red

El software Nagios Core viene integrado por defecto con un visualizador en el cual muestra todos los elementos que han sido agregados en el software, donde se forma un árbol con todos estos dispositivos donde la raíz es el motor de Nagios. En este visualizador además de los equipos gestionados, también se puede visualizar los distintos servidores que se está monitoreando.



**Ilustración 6-3:** Topología Lógica de la red de la empresa que se visualiza en el software Nagios.

Realizado por: Sagñay, Mauro, 2022.

### 3.3.8. Integración de Notificaciones

Una gran característica de Nagios, es la posibilidad de envía notificaciones a contactos específicos cuando ocurre algún imprevisto, ya sea que un equipo cambia de estado, tenga algún problema de algún tipo, un servicio no funciona, etc. Además de que este cambio se refleje en la interfaz gráfica de Nagios, se enviará también una notificación a un grupo de contactos específico. Las notificaciones puedes ser de diferente naturaleza, ya sea vía correo, SMS, sonoras o por alguna APP de mensajería.

### 3.3.8.1. Utilización de Telegram con Nagios Core.

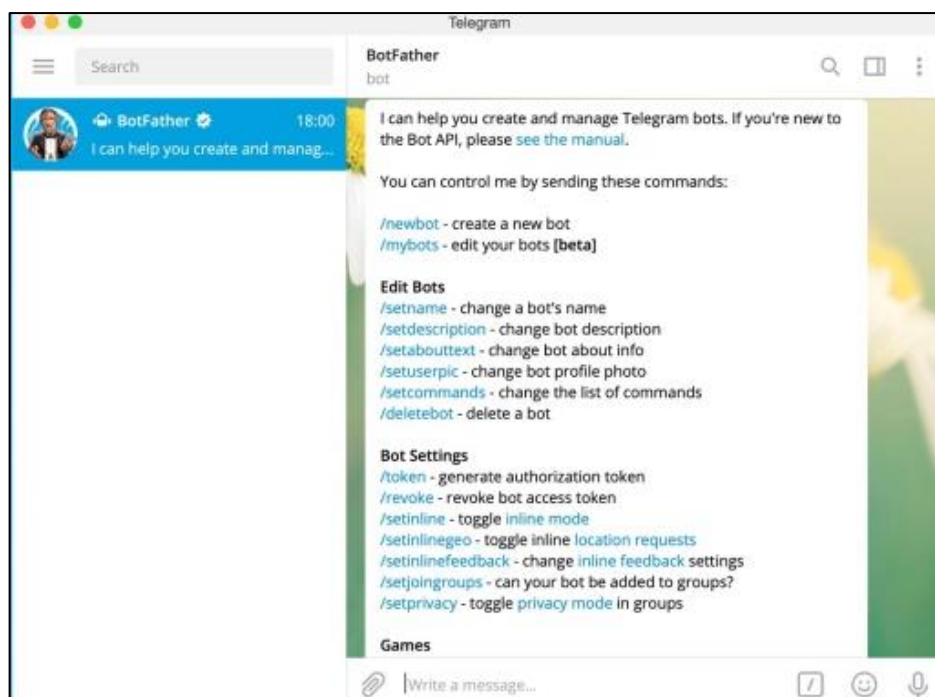
Telegram es un aplicativo de mensajería instantánea de código abierto, es de gran popularidad debido a las grandes funcionalidades que permiten desarrollar diferentes actividades de automatización, como IoT, por ejemplo, mediante la utilización de los denominados *bots*.

Los *bots* se tratan de pequeñas aplicaciones que corren directamente dentro de los servidores de Telegram, estos pequeños códigos pueden interactuar con los diferentes usuarios a través de interfaces flexibles que pueden soportar cualquier clase de servicio o tarea, dentro de las funciones que se puede realizar con los *bots*, se incluye la creación de herramientas personalizadas y la integración con otros servicios, en este caso con Nagios Core.

Esta comunicación entre los distintos usuarios y los *bots*, es completamente segura pues se utiliza a la API de Telegram como servidor intermediario entre ellos, utilizando así protocolos como HTTPS para garantizar la seguridad de los mensajes que se comparten.

### 3.3.8.2. Creación de un bot en Telegram.

Este proceso es relativamente sencillo, pues se utiliza a otro bot de Telegram para la creación de estos, se denomina BotFather. Sin importar la versión de Telegram que se tenga disponible, inicialmente se inicia una conversación con el bot, entonces se pulsa Start o Empezar.



**Ilustración 7-3:** Inicio de la conversación con BotFather para la creación de un bot.

**Fuente:** Telegram, 2022.

Como se muestra en la ilustración anterior, la respuesta que nos da es una lista de comandos disponibles, entre las cuales se utilizará la que indica “/nwebot” dándole un nombre del bot y un nombre de usuario, este último debe ser único.

Después Telegram devolverá un token de autorización para el bot creado, mediante este token se podrá tener acceso a la API de Telegram. Por último, este bot se debe incluir en un grupo o canal de Telegram, al cual también deberán estar agregados los distintos usuarios autorizados para leer las diferentes notificaciones que envíe Nagios Core.

### 3.3.8.3. Envío de notificaciones de Nagios con Telegram

Una vez realizado el proceso de creación del bot y de un grupo en Telegram se puede realizar la configuración para el envío de notificaciones de Nagios mediante Telegram. Para esto son necesarios los siguientes datos:

- CHAT-ID: del grupo de Telegram donde se enviarán todas las notificaciones.
- TOKEN: se trata del código alfanumérico que brinda acceso al API de Telegram.

A continuación, se realiza la modificación del siguiente archivo de configuración /usr/local/nagios/etc/commands.cfg se añade las siguientes líneas.

```
# 'notify-host-by-telegram' command definition

define command{
command_name      notify-host-by-telegram
command_line      /usr/bin/curl -X POST --data chat_id=#### --data text
="***** Nagios *****0A%0ANotification Type: $NOTIFICATIONTYPE$%0AHost
: $HOSTNAME$%0Astate: $HOSTSTATE$%0AAddress: $HOSTADDRESS$%0AInfo: $HO
STOUTPUT$%0A%0ADate/Time:
$LONGDATETIME$%0A" https://api.telegram.org/botTOKEN/sendMessage
}

# 'notify-service-by-telegram' command definition
define command {
command_name      notify-service-by-telegram

command_line      /usr/bin/curl -X POST --data chat_id=##### --data
text="***** Nagios *****0A%0ANotification Type:
$NOTIFICATIONTYPE$%0A%0AService: $SERVICEDESC$%0AHost:
$HOSTALIAS$%0AAddress: $HOSTADDRESS$%0Astate: $SERVICESTATE$%0A%0
ADate/Time: $LONGDATETIME$%0A%0AAdditional
```

```
Info:%0A%0A$SERVICEOUTPUT$%0A"  
https://api.telegram.org/botTOKEN/sendMessage
```

Además, se debe crear un nuevo contacto donde se incluyan los comandos antes creados, como se muestra a continuación.

```
define contact {  
contact_name telegram-contact  
alias Andreas Neumann  
service_notification_options w,u,c,r  
service_notification_period 24x7  
host_notification_period 24x7  
service_notification_commands notify-service-by-telegram  
host_notification_commands notify-host-by-telegram  
host_notification_options d,r  
}
```

Por último, para que los cambios tengan efecto se deberá reiniciar el servicio de Nagios.

### 3.3.9. WinSCP

Se trata de un software de código abierto del tipo cliente SFTP que posee una interfaz gráfica, su principal objetivo es la de facilitar la transferencia segura de archivos entre dos sistemas informáticos, el local y uno remoto que ofrezca servicios SSH (WinSCP, 2022).

Entre sus características que más benefician para este trabajo son las siguientes.

- Interfaz gráfica (GUI).
- Editor de texto integrado
- Soporte de autenticación mediante contraseñas SSH, método keyboard-interactive, clave pública o Kerberos (GSS)
- Interfaces similares al Explorador de Windows

WinSCP permite efectuar las operaciones básicas con archivos, tales como descargas y subidas, también es posible renombrar archivos y directorios, crear nuevos directorios, modificar las propiedades de archivos y carpetas, y crear enlaces simbólicos y accesos directos.

WinSCP permite conectarse a un servidor SSH (Secure Shell) empleando el protocolo SFTP (SSH File Transfer Protocol) o el servicio SCP (Secure Copy Protocol). SFTP es un estándar del paquete

SSH-2. SCP es un parte estándar del paquete SSH-1. Ambos protocolos pueden ser empleados en ambas versiones de SSH. WinSCP puede ser usado tanto con servidores SSH-1 como SSH-2. (WinSCP, 2022).

Esta herramienta permite editar los archivos de configuración en Nagios Core sin la necesidad de ingresar por consola, con esto solo es necesario las credenciales del servidor de acceso a Nagios.

### **3.4. Establecimiento de políticas de gestión de red**

#### ***3.4.1. Descripción de las políticas***

Se presenta entonces una propuesta de políticas de gestión de red, las mismas que cubren las necesidades de la empresa Intertec en concordancia con las recomendaciones del modelo de gestión de red FCAPS, mediante estas políticas se busca el monitoreo constante, supervisión y el control de la infraestructura de red que brinda los diferentes servicios a los abonados de la empresa.

Las políticas tienen como fin obtener una normativa para el adecuado funcionamiento del modelo de gestión, con estas, el personal encargado de la administración de la red podrá actuar ante una falla o evento imprevisto y evitar la degradación o interrupción de los servicios que ofrece la empresa.

Las políticas que se mencionan a continuación, no son estáticas, más bien son flexibles y modificables con el tiempo con el fin de orientarse a conseguir las metas definidas por la empresa en un lapso de tiempo determinado.

#### ***3.4.2. Desarrollo de las políticas de gestión de red***

Estas políticas deberán ser cumplidas por el operador de red y todo el personal autorizado para el acceso y manipulación de la infraestructura de red de la empresa Intertec, con el fin de tener una guía para el mantenimiento y administración de la red para poder disminuir al mínimo la degradación de los servicios de la empresa ocasionados por fallos o eventos inesperados en la red.

#### ***3.4.3. Generalidades***

- a) Estas políticas están enfocadas para ser usadas por un personal con conocimiento mínimo en redes y telecomunicaciones, puesto que se utiliza terminología técnica.
- b) Las políticas son de naturaleza flexible y están prestas a cambios y modificación total o parcial siempre y cuando cumplan con los objetivos y metas de la empresa.

- c) Todo el personal con acceso a la red deberá basarse en estas políticas para la ejecución de actividades y toma de decisiones que afecten al correcto funcionamiento de la red.

#### **3.4.4. Niveles Organizacionales**

Se trata de los niveles en la empresa que están involucrados y a quienes va dirigido estas políticas.

- a) **Gerencia técnica:** encargado de la gerencia para la aprobación de proyectos que afecten o se implementen en la infraestructura física o lógica de red de la empresa, se incluyen la creación y aprobación de las políticas.
  
- b) **Supervisor técnico:** se trata de la autoridad que puede tomar decisiones que afecten o se implementen en la infraestructura de red, además de la modificación de las políticas de gestión de red.
  
- c) **Operador de red:** se trata del personal encargado del mantenimiento de la infraestructura de la red, además de realizar evaluaciones de disponibilidad y rendimiento de los distintos elementos de red. También se encarga de la realización de informes de los procedimientos realizados conjuntamente en concordancia con el personal de soporte técnico.
  
- d) **Soporte técnico:** se trata del personal encargado de la parte de la ejecución de la planificación de actividades de red, como el cableado, instalación de antenas y tareas similares.

#### **3.4.5. Vigencia**

Estas políticas entrarán en vigencia a partir de la aprobación por parte de la gerencia técnica de la empresa, este documento podrá ser revisado, modificado o actualizado dependiendo de las necesidades y exigencias de la empresa o en su defecto cuando exista un cambio importante en la infraestructura de red.

#### **3.4.6. Referencia**

Las políticas de gestión se presentarán en documentos con un formato que cumplan con la normativa de la empresa Intertec. Debido a que no existe un precedente de este tipo de políticas en la empresa, estas se realizan en base al modelo de gestión de red FCAPS.



### **3.4.7. Políticas de gestión de red para la empresa Intertec.**

A continuación, se detallan el establecimiento de las políticas de gestión de red de la empresa Intertec en base al modelo FCAPS, además se incluye las diferentes actividades que se desarrolla en cada política y sus respectivos responsables.

#### **Política de gestión de red**

- Objetivos de la política de gestión
- Compromiso de las autoridades

#### **Política de gestión de fallos**

- Manejo de Fallas
- Manejo de Alarmas
- Pruebas de Diagnostico
- Manejo de Errores
- Envío de notificaciones

#### **Política de gestión de configuración**

- Supervisar y hacer cumplir las normas de ingreso y salida de equipos
- Conservar los datos de configuración y mantenimiento de un inventario actualizado de los componentes de red.
- Configuración remota

#### **Política de gestión de contabilidad / administración**

- Manejo del uso de recursos de la red

#### **Políticas de gestión de performance / desempeño**

- Captura de datos o variables indicadoras de rendimiento
- Análisis de los datos para determinar los niveles normales de rendimiento
- Generar informes y estadísticas

#### **Políticas de gestión de Seguridad**

- Monitoreo de la red frente a ataques
- Encriptado de la información
- Establecimiento de procedimientos de autenticación
- Control de acceso a los recursos

### **3.4.8. Términos y definiciones**

**Elementos de red:** se trata de los componentes que forman parte de la red y que permiten la interconexión y procesamiento y transmisión de datos de los diferentes nodos.

**Disponibilidad:** en el contexto tecnológico, se refiere a la capacidad de un sistema para procesar y responder a las diferentes solicitudes de recursos o servicios.

**FCAPS:** se trata de un modelo de gestión de red desarrollado por la ISO la cual utiliza cinco categorías funcionales para realizar el monitoreo de una infraestructura de red.

**SNMP:** (Simple Network Management Protocol) trabaja en la capa de aplicación y permite supervisar, analizar y comunicar información entre un agente y un gestor. Es compatible con una gran variedad de dispositivos en el mercado.

**Reportes:** se trata de un informe que contiene información de cada un elemento de red, dispositivo o servicio gestionado.

### **3.5. Desarrollo de políticas de gestión de red para la empresa Intertec**

A continuación, se presenta el desarrollo de políticas para la gestión de la red de la empresa, en las mismas se establecen su correspondiente procedimiento así también con los responsables de su ejecución y/o supervisión.

#### **3.5.1. Política de gestión de red**

##### **Política 1. Información del sistema de gestión de red**

El manual para la utilización del sistema de gestión deberá ser compartido y socializado con todo el personal que interactúe y manipule la infraestructura de red u otros dispositivos que necesiten ser monitoreados.

**Responsable:** Supervisión técnica

##### **Política 2. Creación y modificación de las políticas de gestión**

La creación, modificación, implementación y aprobación de las políticas de gestión estará a cargo de la autoridad de mayor jerarquía de la empresa en el ámbito técnico o de aquella entidad que esta delegue.

**Responsable:** Gerencia técnica, Supervisión técnica

### 3.5.2. *Política de gestión de fallos*

#### **Manejo de Fallas**

##### **Política 3. Reconocimiento de fallas**

Al ocurrir una falla en la infraestructura de red se deberá consultar la interfaz web del software de monitoreo además del aplicativo Telegram para la identificación del elemento de red que sufrió el fallo, para posteriormente aislarlo, diagnosticarlo y corregirlo.

**Responsable:** Operador de red.

##### **Política 4. Tiempo de atención a fallos**

Después de aislar y diagnosticar un fallo se deberá implementar medidas o procedimientos para recuperarse del fallo en el menor tiempo posible según el nivel de prioridad del mismo.

**Responsable:** Operador de red, soporte técnico.

Los niveles de prioridad se asignan según el estado del equipo o servicio que haya sufrido el fallo y la asignación automática es dada por el sistema de gestión.

- **Prioridad Alta (crítico):** El equipo está fuera de servicio o con interrupciones repetitivas durante breves periodos de tiempo, la acción inmediata busca el restablecimiento del equipo o servicio a la brevedad posible, considerando entre otras cosas, la ubicación del equipo afectado y el número de abonados.
- **Prioridad Media (advertencia):** El equipo presenta degradación en la calidad de su funcionamiento, pero sin cortes o interrupciones continuas. La acción a realizar es el diagnóstico de la afectación a través del sistema de gestión u otras herramientas disponibles, el tiempo para arreglar este inconveniente puede ser planificada según las necesidades de la empresa, como planes de expansión o actualización de hardware o software.
- **Prioridad Baja (notificación, información):** Se refiere a los avisos o notificaciones, generalmente de los servicios de los equipos monitoreados, su atención puede ser omitida o postergada sin que esto conlleve una afectación o impacto negativo en el funcionamiento de los equipos o servicios de la empresa.

**Política 5.** Se deberá hacer uso del software de monitoreo de red u otras herramientas disponibles para documentar de la manera más detallada posible la falla ocurrida y su procedimiento para dar solución en un tiempo determinado.

**Responsable:** Operador de red.

### **Pruebas de Diagnóstico**

#### **Política 6. Desarrollo de pruebas de diagnóstico**

Para determinar el buen funcionamiento de un equipo se deberá establecer en el software de monitoreo pruebas de conectividad mediante el protocolo ICMP con la herramienta Ping, además de la utilización del protocolo SNMP para la obtención de información más específica de cada equipo.

**Responsable:** Operador de red.

### **Manejo de Errores**

**Política 7.** Se deberá realizar un rollback a la configuración tanto física como lógica de los equipos del core y los diferentes nodos que forman parte de la red si estos llegaran a fallar después una actualización de firmware o un mantenimiento, para evitar la falta de servicio.

**Responsable:** Operador de red, servicio técnico.

#### **3.5.3. Políticas de gestión de configuración**

**Supervisar y hacer cumplir las normas de entrada y salida de equipos.**

#### **Política 8. Entrada de equipo al sistema de gestión**

En una ampliación de red o cuando se realice un cambio de equipo, la información básica de identificación de este como el nombre, alias, dirección IP y grupo de trabajo será ingresada en el sistema de gestión para poder ser monitoreado.

**Responsable:** Operador de red.

#### **Política 9. Identificación de los equipos**

Se usará la nomenclatura establecida por la gerencia técnica para identificar a un equipo que forme parte de la red y que pueda ser monitoreado, se usará este nombre o su equivalente en todos los sistemas de almacenamiento, inventario u otros, con el fin de que se pueda localizar con mayor facilidad.

**Responsable:** Gerencia técnica, Supervisor técnico.

#### **Política 10. Configuración SNMP**

Se deberá establecer una comunidad SNMP que será la misma para todos los equipos de la red que serán monitoreado, además de colocar la dirección IP del Sistema de gestión al cual se enviará los mensajes para el monitoreo de los equipos.

**Responsable:** Supervisor técnico, Operador de red

#### **Conservar los datos de configuración y mantenimiento en un inventario actualizado**

#### **Política 11. Backup de los archivos de configuración**

Se deberá realizar un respaldo de la configuración de los diferentes equipos que forman parte de la infraestructura de red, de manera diaria como mínimo; y almacenarlos de manera segura para su recuperación en caso de ser necesario.

**Responsable:** Operador red, soporte técnico.

#### **Configuración remota**

**Política 12.** Para el acceso remoto a los diferentes recursos de la empresa, se deberá establecer túneles VPN L2TP para poder realizar las diferentes configuraciones, también se podrá utilizar software de terceros.

**Responsable:** Supervisor técnico, Operador de red.

#### **3.5.4. Política de gestión de contabilidad / administración**

#### **Administración del uso de recursos de la red**

**Política 13.** Se deberá identificar correctamente al personal que tenga acceso al sistema de gestión y otras herramientas que se utilicen para el monitoreo y administración de la red mediante la creación de perfiles de usuario con sus credenciales respectivas para poder acceder a los recursos.

**Responsable:** Supervisor técnico.

**Política 14.** Las diferentes tareas y actividades que se ejecutan deberán tener un seguimiento a través de informes donde se evidencie el trabajo realizado.

**Responsable:** Supervisor técnico.

### **3.5.5. Políticas de gestión de desempeño / performance**

#### **Captura de datos o variables indicadoras de rendimiento**

**Política 15.** Determinar los distintos de parámetros de rendimiento de los equipos de red que serán recopilados mediante el software de monitoreo para su posterior procesamiento y visualización.

**Responsable:** Gerencia técnica, Supervisor técnico.

**Política 16.** Se deberá configurar todos los equipos de red de tal forma que utilicen el protocolo SNMP para la transmisión de las diferentes métricas hacia el sistema de gestión.

**Responsable:** Supervisor técnico, Operador de red.

#### **Análisis de los datos para determinar los niveles deseados de rendimiento**

**Política 17.** El establecimiento de los umbrales de las diferentes métricas de los equipos, se deberá basarse en las especificaciones técnicas de cada uno, así también como la generación de alertas en caso de anomalías.

**Responsable:** Supervisor técnico.

#### **Generar informes y estadísticas**

**Política 18.** Se deberá generar gráficos estadísticos de manera diaria, semanal y mensual u en otro periodo que se considere de interés, donde se aprecie el comportamiento de los parámetros de rendimiento recopilados por el sistema de gestión.

**Responsable:** Gerencia técnica, Supervisor técnico.

### **3.5.6. Políticas de gestión de seguridad**

#### **Encriptado de la información**

**Política 19.** Para el transmisión y almacenamiento de datos sensibles como datos personales de trabajadores, proveedores, clientes, contratos u otros que considere la empresa, se deberá utilizar protocolos seguros como SFTP o FTPS con una encriptación suficientemente segura como AES o superior.

**Responsable:** Supervisor técnico, Operador de red.

**Política 20.** Para la comunicación oficial de la empresa con personal interno o con entidades externas se deberá utilizar un servidor de email que haga uso de certificados SSL/TLS para cifrar los correos entrantes y salientes.

**Responsable:** Supervisor técnico, Operador de red.

### **Establecimiento de procedimientos de autenticación**

**Política 21.** Para la conexión con los diferentes servidores de la empresa se deberá utilizar el protocolo SSH para garantizar el acceso seguro a los recursos del servidor.

**Responsable:** Supervisor técnico, Operador de red.

**Política 22.** Se utilizará un servidor RADIUS para la autenticación del personal que manipule o tenga acceso a la infraestructura de red de la empresa.

**Responsable:** Supervisor técnico, Operador de red.

### **Control de acceso a los recursos**

**Política 23.** Se deberá limitar el acceso al sistema de gestión de red y otras herramientas utilizadas para el monitoreo, a los usuarios no autorizados o aquellos que no tengan los privilegios suficientes mediante la creación de diferentes perfiles de acceso.

**Responsable:** Supervisor técnico, Operador de red

**Política 24.** Las notificaciones de cualquier evento reportadas por el sistema de gestión deberán ser enviadas a través del aplicativo Telegram y solo al personal autorizado.

**Responsable:** Supervisor técnico, Operador de red.

### **Monitoreo de la red frente a ataques**

**Política 25.** Se deberá realizar un escaneo de vulnerabilidades de manera periódica para determinar las fallas potenciales de seguridad en la infraestructura de red de esta manera se podrá aislarlas y corregirlas.

**Responsable:** Operador de red.

## CAPÍTULO IV

### 4. RESULTADOS

#### 4.1. Cumplimiento de parámetros FCAPS

Para validar el sistema de gestión de red que se ha desarrollado en el presente trabajo, se debe satisfacer los parámetros del modelo FCAPS, los cuales ya se han estudiado en secciones previas, a continuación, se presenta una tabla donde se aprecia el cumplimiento de estos parámetros.

#### 4.2. Implementación en Gestión de Fallas

En este apartado se presenta la solución que busca cubrir con las necesidades de la empresa con respecto a la gestión de fallas por parte del software Nagios.

##### 4.2.1. Manejo de Fallas

###### 4.2.1.1. Detección de Fallas

Mediante el software Nagios se puede determinar cuándo un equipo llega a presentar algún inconveniente, ya sea cuando ha dejado de responder al keepalive, o cuando uno de sus servicios no funciona de manera adecuada.

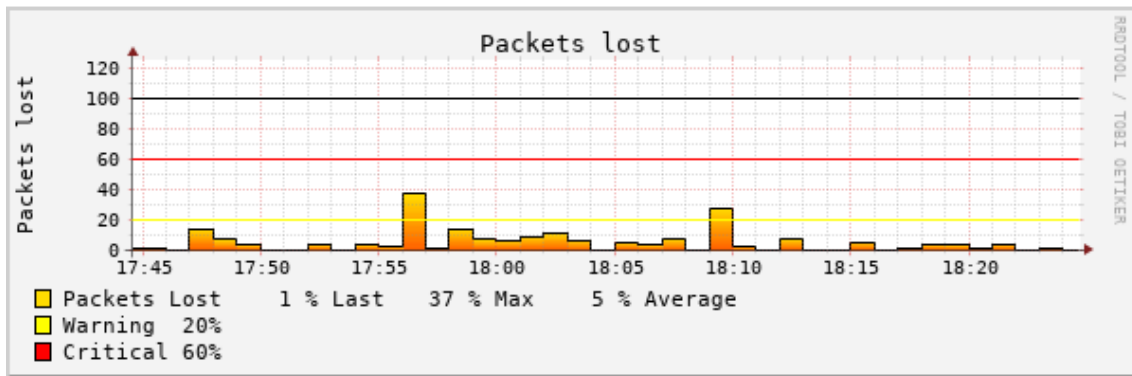
Host	Service	Status	Last Check	Duration	Attempt	Status Information
PTP_GLL_SE_01	PING	WARNING	12-18-2022 18:30:03	0d 0h 1m 8s	1/3	PING WARNING - Packet loss = 37%, RTA = 31.69 ms

**Ilustración 1-4:** Detección de falla en el keepalive de PING en el host PTP\_GLL\_SE\_01.

**Fuente:** Nagios, 2022.

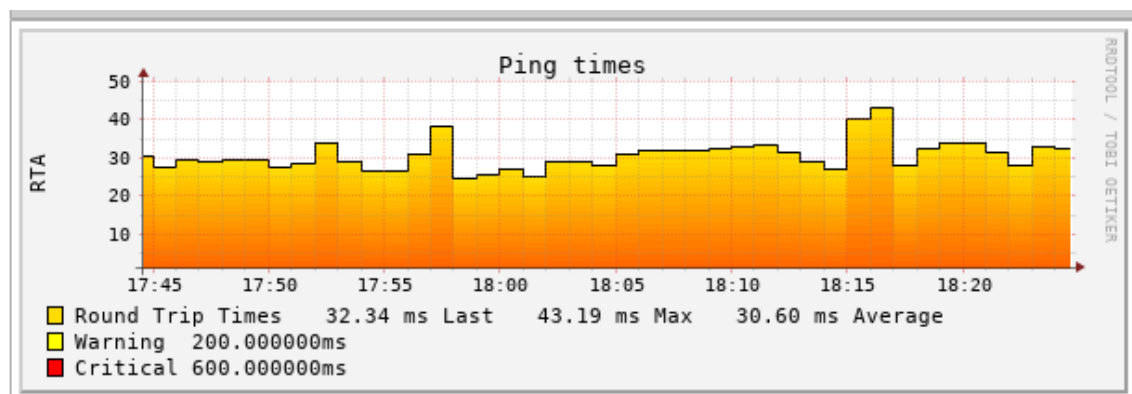
En la ilustración anterior se aprecia que el host PTP\_GLL\_SE\_01, en este caso una antena, ha presentado un inconveniente en el servicio PING, el software Nagios lo detecta, pintándolo de amarillo, que identifica un fallo del tipo WARNING (advertencia). Además de esto, también se puede obtener información como el último check y los intentos de chequeo (Attempt), en el estado del servicio, se obtiene métricas como el packet loss (pérdida de paquetes) y el RTA (tiempo de ping). De manera gráfica la detección de la falla se puede observar en la siguiente ilustración.





**Ilustración 2-4:** Registro de la pérdida de paquetes en el equipo PTP\_GLL\_SE\_01.

Fuente: Nagios, 2022.

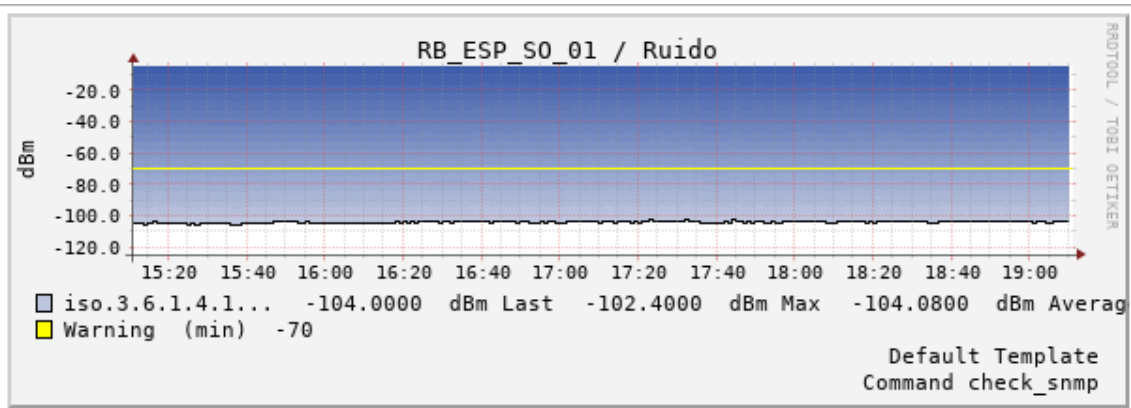


**Ilustración 3-4:** Registro del RTA en el equipo PTP\_GLL\_SE\_01.

Fuente: Nagios, 2022.

Como se observa, aunque el RTA (tiempo de Ping) no ha alcanzado los valores para lanzar una notificación de fallo, la pérdida de paquetes llega al 37 %, lo que sobrepasa el umbral de advertencia que es de un 20%, lo que podría implicar que el canal de comunicación presenta interferencias.

Otro caso se puede apreciar en la siguiente ilustración, en el equipo RB\_ESP\_SO\_0, en este caso una antena sectorial, se puede observar el nivel de ruido presente en el equipo, donde se aprecia que el ruido en todo el lapso de tiempo de la gráfica presenta un valor promedio de -104 dBm, lo que no sobrepasa el umbral de -70 dBm establecido.

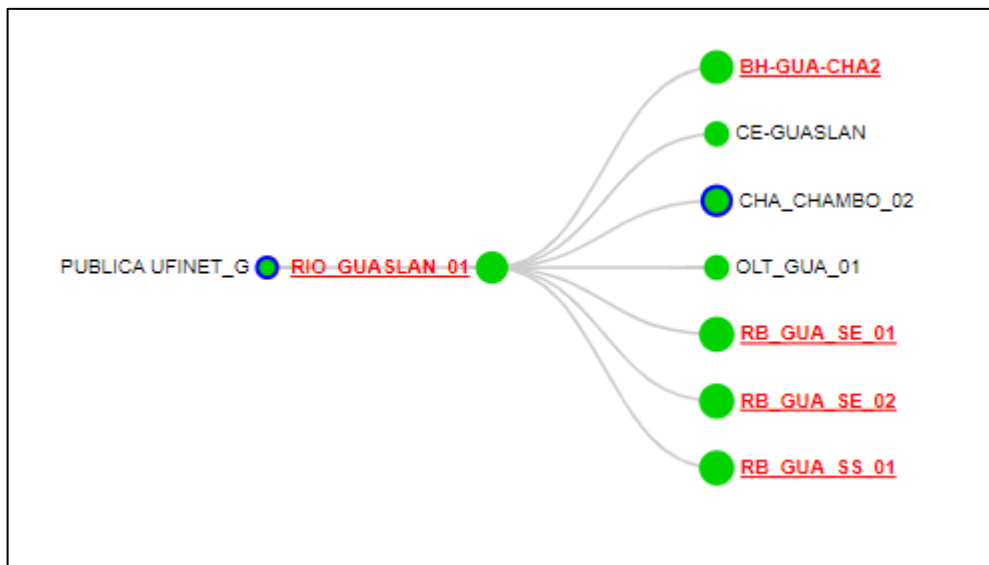


**Ilustración 4-4:** Ruido presente en el equipo RB\_ESP\_SO\_01 en un lapso de 4 horas.

Fuente: Nagios, 2022.

#### 4.2.1.2. Aislamiento de Fallas

Nagios puede aislar la falla mediante su topología dinámica, donde el host que presenta problemas se pinta de un tono rojo, mientras los demás permanecen en verde, como se observa en la siguiente ilustración.


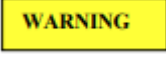


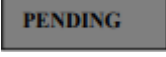


**Ilustración 5-4:** Topología dinámica usada en Nagios para aislar una falla.

Fuente: Nagios, 2022.

Otra forma de aislar una falla es que se puede etiquetar dependiendo de su criticidad/nivel de prioridad, la misma que puede clasificarse según el estado del servicio monitoreado, como se menciona en la siguiente tabla.

**Tabla 1-4:** Jerarquía de alertas dependiendo de su criticidad/nivel de prioridad en Nagios.

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

Fuente: Nagios, 2022.

Realizado por: Sagnay, Mauro, 2022.

#### 4.2.1.3. Corrección de Fallas

Una vez identificada la falla, Nagios puede detallar una lista de diferentes atributos de la misma para que el operador de red o el personal encargado pueda tener un mejor conocimiento del inconveniente ocurrido y así poder implementar medidas o procedimientos en el menor tiempo posible.

Como se observa en la siguiente ilustración, en este equipo, en este caso un servidor, se dio una falla del servicio HTTP, en el cual el puerto TCP 80 está bloqueado y por ende no se puede monitorear, Nagios detalla toda la información de la falla, como el tipo de falla, la información de estado de la falla, fecha del ultimo chequeo así también como sus últimos chequeos, entre otros.

**Service State Information**

**Current Status:** CRITICAL (for 114d 4h 1m 27s)

**Status Information:** connect to address 172.24.10.6 and port 80: Connection refused  
HTTP CRITICAL - Unable to open TCP socket

**Performance Data:**

**Current Attempt:** 4/4 (HARD state)

**Last Check Time:** 12-18-2022 21:11:23

**Check Type:** ACTIVE

**Check Latency / Duration:** 0,000 / 0,000 seconds

**Next Scheduled Check:** 12-18-2022 21:16:23

**Last State Change:** 08-26-2022 17:13:55

**Last Notification:** N/A (notification 0)

**Is This Service Flapping?** NO (0,00% state change)

**In Scheduled Downtime?** NO

**Last Update:** 12-18-2022 21:15:20 ( 0d 0h 0m 2s ago)

---

**Active Checks:** ENABLED

**Passive Checks:** ENABLED

**Obsessing:** ENABLED

**Notifications:** DISABLED

**Event Handler:** ENABLED

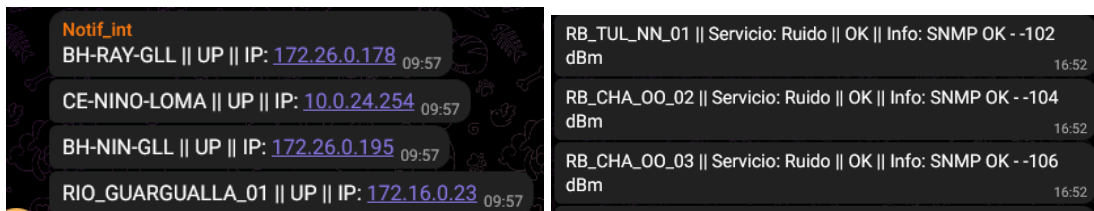
**Flap Detection:** ENABLED

**Ilustración 6-4:** Estado del servicio monitoreado cuando se da un error.

Fuente: Nagios, 2022.

- Recuperación de la red

Una vez que la falla sea solventada, Nagios notifica que el equipo o servicio ha vuelto a estar operativo, en este caso por la aplicación de mensajería Telegram.



**Ilustración 7-4:** Mensajes recibidos en la app de Telegram sobre la recuperación de los equipos después de una caída de conexión (izquierda) y del nivel de ruido en un equipo (derecha).

Fuente: Telegram, 2022.

También la recuperación de los equipos se puede apreciar en el apartado del Log de Nagios en la interfaz web.

Host	Service	Type	Time	Contact	Notification Command	Information
RIO_GUARGUALLA_01	N/A	HOST UP	12-18-2022 09:57:46	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 0%, RTA = 25.43 ms
BH-NIN-GLL	N/A	HOST UP	12-18-2022 09:57:46	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 0%, RTA = 31.74 ms
CE-NINO-LOMA	N/A	HOST UP	12-18-2022 09:57:38	telegram-contact	notify-host-by-telegram	PING WARNING - Packet loss = 83%, RTA = 37.31 ms
BH-RAY-GLL	N/A	HOST UP	12-18-2022 09:57:27	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 0%, RTA = 35.02 ms

**Ilustración 8-4:** Recuperación de Hosts registrada en el Log de Nagios.

Fuente: Nagios, 2022.

#### 4.2.1.4. Envío de notificaciones de alerta

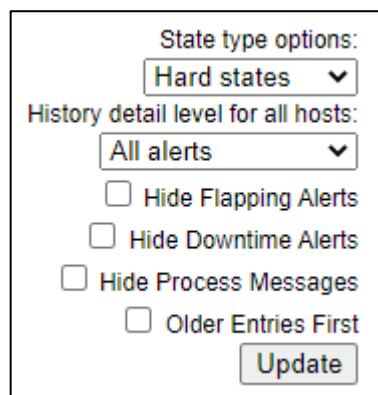
Al ocurrir una falla una alarma es activada, el tipo de alarma varía dependiendo de la criticidad de la falla ocurrida, así mismo se notifica al contacto respectivo, como se observa en la ilustración anterior, para este caso el contacto de referencia que se ha establecido en los archivos de Nagios es “Telegram-contact”.

```
define contact {  
  
    contact_name                telegram-contact  
    alias                       Alertas Intertec  
    service_notification_options w,c,r  
    service_notification_period 24x7  
    host_notification_period    24x7  
    service_notification_commands notify-service-by-telegram  
    host_notification_commands  notify-host-by-telegram  
    host_notification_options   d,r,u  
  
}
```

En las partes resaltadas se indica que las notificaciones serán enviadas cuando un host este caído (d = down) cuando esté recuperado de una falla (r=recovery) o cuando sea inalcanzable (u=unreachable) y en el caso de los servicios cuando esté en advertencia (w=warning), crítico (c=critic) y cuando se haya recuperado (r=recovery).

#### 4.2.1.5. Filtrado de alertas

Todas las alertas que se hayan presentado en los diferentes equipos pueden ser consultadas en el software Nagios, pues éste a través de un log almacena de forma cronológica todas las alertas ocurridas en cada host. Para obtener un resultado más preciso se puede hacer uso de un menú para filtrar los resultados, como se aprecia en la siguiente ilustración.

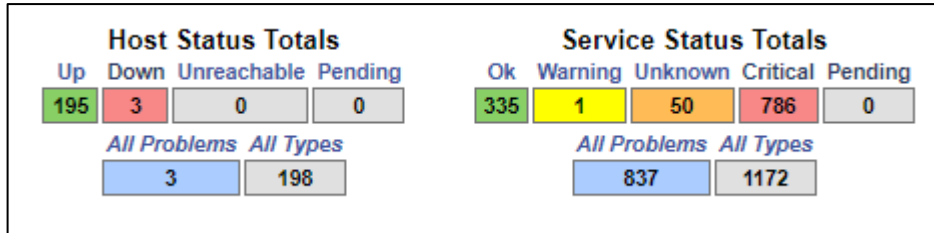


**Ilustración 9-4:** Menú para filtrar las alertas por el tipo y por host.

Fuente: Nagios, 2022.

También se puede obtener una vista general de todos inconvenientes generados como se puede apreciar a continuación. Se presenta dos graficas donde se clasifica el estado de los hosts y de los servicios, identificándolo además por un color.

Se puede filtrar las alertas de una forma más gráfica como se observa a continuación.



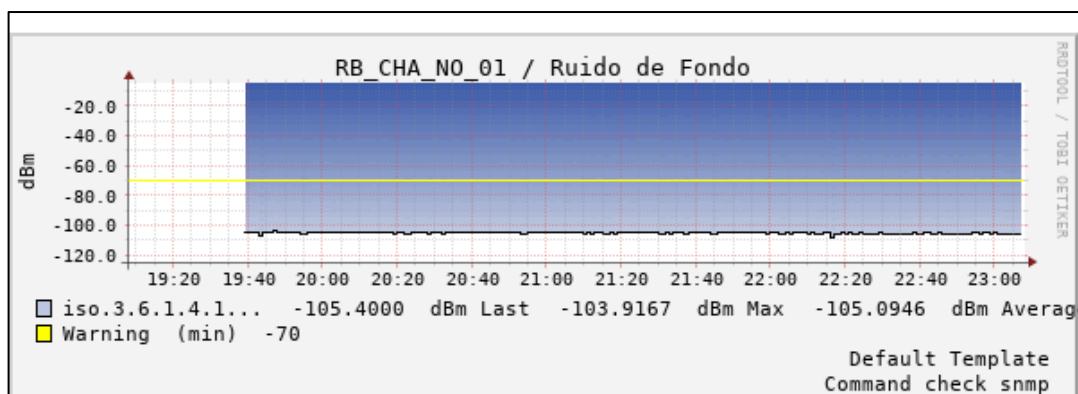
**Ilustración 10-4:** Filtrado de las alertas de host y de servicio de acuerdo a su criticidad.

Fuente: Nagios, 2022.

#### 4.2.1.6. Generación de Alertas

En Nagios se puede modificar el los diferentes umbrales o valores normales de las variables que se está monitoreado, esto se logra mediante la edición del archivo de configuración donde se establece estos valores.

Una vez establecido los niveles de umbral, estos se verán reflejados en las gráficas de monitoreo mediante una línea amarilla en este caso, ubicada en el valor correspondiente de umbral, como se aprecia en la siguiente ilustración.



**Ilustración 11-4:** Medición del parámetro del ruido en el equipo RB\_CHA\_NO\_01.

Fuente: Nagios, 2022.

Como se puede apreciar en la ilustración, en la antena RB\_CHA\_NO\_01 se está monitoreando el nivel de ruido (Noise Floor) presente. El umbral mínimo tolerado se ha establecido en -70 dBm, en la gráfica este umbral se reconoce como una línea amarilla, según el caso cuando se sobrepase o caiga de este valor, se producirá una alarma.

#### 4.2.2. Pruebas de Diagnóstico

Automáticamente Nagios envía mensajes ICMP del tipo PING para determinar el estatus del equipo o servicio, además de la utilización del protocolo SNMP para dar un diagnóstico más preciso.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
GUA_GMT_01	Carga CPU	OK	12-18-2022 23:16:51	0d 2h 19m 27s	1/3	SNMP OK - 1 %
	Memoria Total	OK	12-18-2022 23:16:52	0d 5h 35m 49s	1/3	SNMP OK - 950272
	Memoria Usada	OK	12-18-2022 23:16:49	0d 5h 35m 44s	1/3	SNMP OK - 333248
	PING	OK	12-18-2022 23:16:54	11d 4h 53m 40s	1/3	PING OK - Packet loss = 0%, RTA = 1.30 ms
	Uptime	OK	12-18-2022 23:16:57	0d 6h 7m 49s	1/3	SNMP OK - Timeticks: (722895300) 83 days, 16:02:33.00

**Ilustración 12-4:** Servicios monitoreados en el equipo GUA\_GMT\_01.

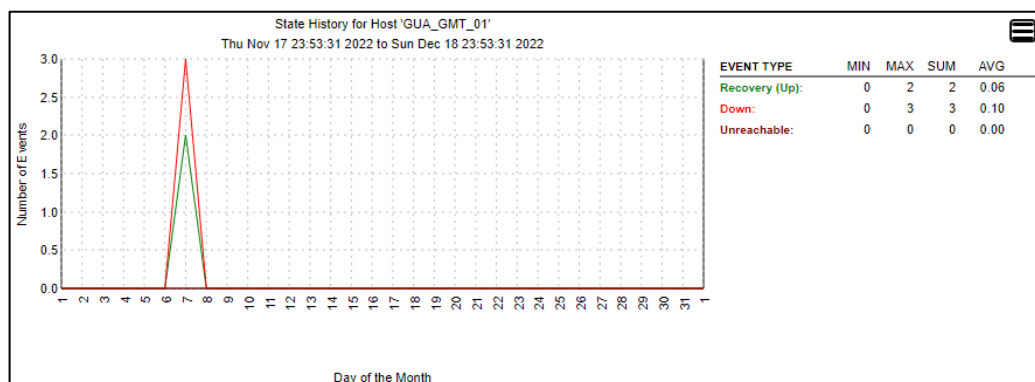
Fuente: Nagios, 2022

En la ilustración anterior, para el equipo GUA\_GMT\_01, en este caso un router, se ha establecido diferentes servicios para ser monitoreados por Nagios, dentro de las diferentes pruebas de diagnóstico se aprecia las de tipo PING, y otros servicios que se obtienen mediante consultas SNMP.

#### 4.2.3. Manejo de Errores

##### 4.2.3.1. Estadísticas de errores

En Nagios se puede obtener gráficos estadísticos donde se observe los eventos ocurridos de un host específico en un tiempo determinado, de esta manera se puede obtener una visión más general del funcionamiento del equipo monitoreado.



**Ilustración 13-4:** Histograma de alertas ocurridas en el equipo GUA\_GMT\_01 desde el 17 de Nov hasta el 18 de Dic de 2022.

Fuente: Nagios, 2022

En la ilustración anterior se observa la estadística de alertas suscitadas en el equipo GUA\_GMT\_01, en el periodo de 31 días ocurrieron 5 eventos, 2 de recuperación y 3 de caídas del host.

### 4.3. Implementación en Gestión de Configuración

La herramienta Nagios Core se utiliza principalmente para el monitoreo de los diferentes equipos y servicios de la infraestructura de red, por lo cual, su principal función en el apartado de Gestión de Configuración se enfoca en poner a disposición del respectivo operador de red y usuarios autorizados, las diferentes métricas y reportes que brindan una retroalimentación sobre el estado de la red, de esta manera el personal respectivo sería el encargado de determinar la actualización, modificación o la implementación de una nueva configuración.

#### 4.3.1. Supervisar y hacer cumplir las normas de entrada y salida de equipos.

##### 4.3.1.1. Entrada de equipos al sistema de gestión

El ingreso de equipos o host al sistema de gestión se ha realizado mediante la edición de los archivos de configuración de Nagios Core, como se muestra a continuación.

```
define host {
use          generic-switch          ;
host_name    router_1                ;
alias        Router de Borde         ;
address      172.24.x.x              ;
hostgroups   RouterCore              ;
}
```

La información básica que se ingresa es, el nombre, el alias, la dirección IP y el hostgroup. Este proceso se repite para todos los equipos sin importar su tipo, además también se deberá establecer los servicios a ser monitoreados en este host, como se muestra a continuación.

```
define service {
use          generic-service          ;
host_name    router_1                ;
service_description    PING          ;
check_command    check_ping!200.0,20%!600.0,60% ;
normal_check_interval    5          ;
retry_check_interval    1          ;
}
```



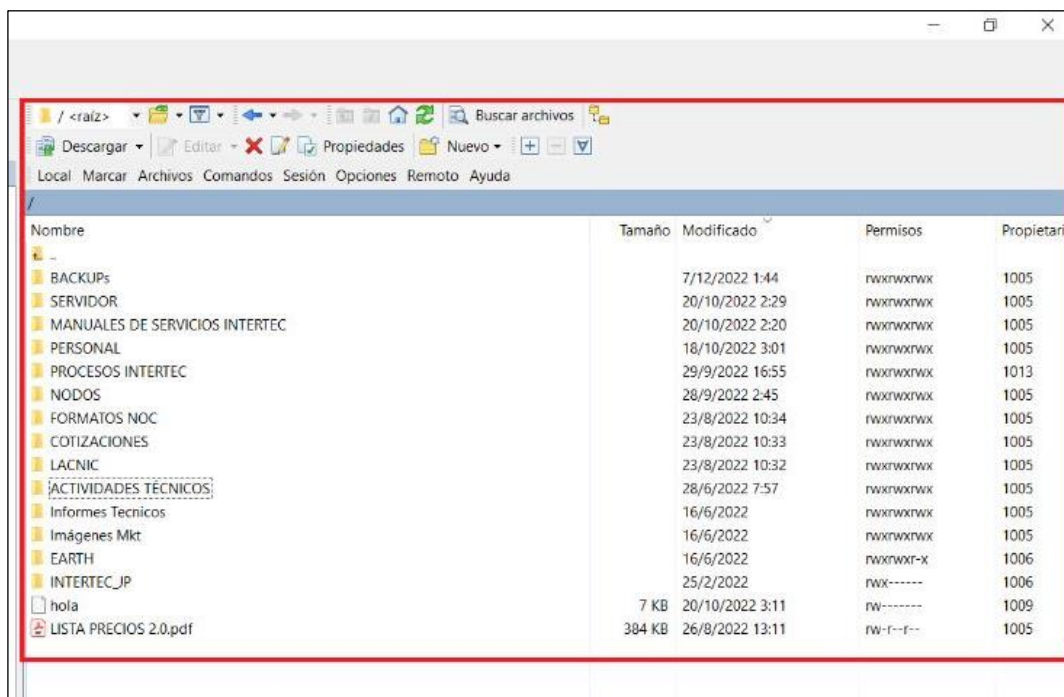
#### 4.3.1.2. Configuración SNMP

Para establecer la comunicación entre los equipos monitoreados y el software Nagios Core, se utiliza el protocolo SNMP para la transmisión de las diferentes métricas que serán recopiladas por el software Nagios y su posterior visualización en gráficas.

Para este caso se utiliza el protocolo SNMP versión 2, y los puertos 161, 162 UDP; además para todos los equipos de red se establece la dirección IP del sistema de gestión de red y una comunidad que será única para toda la gestión de la red.

#### 4.3.2. Conservar los datos de configuración y mantenimiento en un inventario actualizado de todos los componentes de la red.

Dentro de los procedimientos de la empresa, se almacena los archivos de configuración de los diferentes routers, antenas, switches y demás información sensible en un servidor FTP.



Nombre	Tamaño	Modificado	Permisos	Propietari
-				
BACKUPs		7/12/2022 1:44	rw-rw-rw-	1005
SERVIDOR		20/10/2022 2:29	rw-rw-rw-	1005
MANUALES DE SERVICIOS INTERTEC		20/10/2022 2:20	rw-rw-rw-	1005
PERSONAL		18/10/2022 3:01	rw-rw-rw-	1005
PROCESOS INTERTEC		29/9/2022 16:55	rw-rw-rw-	1013
NODOS		28/9/2022 2:45	rw-rw-rw-	1005
FORMATOS NOC		23/8/2022 10:34	rw-rw-rw-	1005
COTIZACIONES		23/8/2022 10:33	rw-rw-rw-	1005
LACNIC		23/8/2022 10:32	rw-rw-rw-	1005
ACTIVIDADES TÉCNICOS		28/6/2022 7:57	rw-rw-rw-	1005
Informes Tecnicos		16/6/2022	rw-rw-rw-	1005
Imágenes Mkt		16/6/2022	rw-rw-rw-	1005
EARTH		16/6/2022	rw-rw-r-x	1006
INTERTEC_JP		25/2/2022	rw-r-----	1006
hola	7 KB	20/10/2022 3:11	rw-r-----	1009
LISTA PRECIOS 2.0.pdf	384 KB	26/8/2022 13:11	rw-r--r--	1005

**Ilustración 14-4:** Archivos de configuración alojados en el servidor FTP.

**Fuente:** Servidor vsftpd, 2022.

Como se muestra en la ilustración anterior, se aprecia los archivos de configuración, backups, imágenes entre otra documentación que la empresa considera esencial y debe mantenerse segura. Se utiliza la herramienta Vsftpd, que se trata de un servidor FTP basado en Linux bastante completo y potente.

#### 4.3.2.1. Backup de seguridad de configuración de red.

En cada equipo de red, en medida de lo posible, se establece un script compatible con el servidor FTP en el cual tiene como objetivo, guardar la configuración de cada equipo y enviarlo al servidor FTP de forma automática, como se muestra en el siguiente script.

```
# ftp server
:local ftphost "172.28.x.x"
:local ftpuser "XXXXX"
:local ftppassword "XXXXX"
:local ftppath "/home/XXXX/"

#GetDate
:local GDate [/system clock get date]
:local GDay [ :pick $GDate 4 6 ]
:local GMonth [ :pick $GDate 0 3 ]
:local GYear [ :pick $GDate 7 11 ]
:local GResult "$GDay $GMonth $GYear"

# file name for config export
:local ExportConf ([/system identity get name]".rsc")
:log info $ExportConf

# backup the data
/export compact file=$ExportConf
:log info message="Config export finished."

# upload the config export
:log info message="Uploading config export."
/tool fetch address="$ftphost" src-path=$ExportConf user="$ftpuser" mode=ftp password="$ftppassword" dst-path="$ftppath/$GResult-$ExportConf" upload=yes
:log info message="Configuration backup finished.";

/file remove "$ExportConf"
:log info "Remove backup...";
```

Una vez que el script sea cargado en el equipo de red, se podrá configurar el período que se deba realizar las copias de seguridad, este periodo lo determina el operador de red generalmente y dependiendo de la función que realiza el equipo.

Como se observa en la siguiente ilustración, los archivos de backups son almacenados en el servidor Vsftpd (FTP), además se muestran su tamaño y su fecha de guardado.

**Índice de /backups/**

[directorio principal]

Nombre	Tamaño	Fecha de modificación
ACAN_ANGEL.rsc	2.7 kB	29/6/22 12:04:00
CHA_CHAMBO_01.rsc	8.9 kB	29/6/22 11:08:00
CHA_CHAMBO_02.rsc	30.4 kB	29/6/22 12:51:00
CHA_TULABUG_01.rsc	17.6 kB	29/6/22 12:26:00
CORE_ESP_01.rsc	10.9 kB	29/6/22 7:34:00
CPE-ESP-SE-01.rsc	2.8 kB	29/6/22 8:03:00
CPE_COM_SE_01.rsc	2.5 kB	29/6/22 12:02:00
CPE_SHL_NO_01.rsc	2.3 kB	29/6/22 10:55:00
PTP_CRL_OO_01.rsc	2.2 kB	29/6/22 11:53:00
PTP_ESP_SE_01.rsc	2.2 kB	29/6/22 7:58:00
RB-CHA_EE_01.rsc	2.3 kB	29/6/22 12:48:00
RB-CHA_NO_01.rsc	2.2 kB	29/6/22 12:50:00
RB-CHA_OO_01.rsc	2.4 kB	29/6/22 12:40:00
RB-CHA_OO_02.rsc	2.5 kB	29/6/22 12:45:00
RB-CHA_OO_03.rsc	2.5 kB	29/6/22 12:42:00
RB-CHA_OO_04.rsc	2.4 kB	29/6/22 12:43:00
RB-CHA_OO_05.rsc	2.4 kB	29/6/22 12:44:00
RB-CHA_SO_01.rsc	2.3 kB	29/6/22 12:47:00
RB-CHA_SO_02.rsc	2.3 kB	29/6/22 12:48:00
RB-GUA_SE_01.rsc	2.5 kB	29/6/22 12:11:00
RB-GUA_SE_02.rsc	2.4 kB	29/6/22 12:14:00
RB-GUA_SS_01.rsc	2.3 kB	29/6/22 12:09:00
RB-H2O-NE-04.rsc	2.6 kB	29/6/22 10:11:00
RB-IGL-SE-01.rsc	2.3 kB	29/6/22 8:19:00
RB-MOD-SE-01.rsc	2.4 kB	29/6/22 12:24:00
RB-SHL_NE_02.rsc	2.2 kB	29/6/22 10:25:00
RB-SHL_NE_03.rsc	2.2 kB	29/6/22 10:30:00
RB-SHL_NN_01.rsc	2.3 kB	29/6/22 10:33:00
RB-TAN-OO-01.rsc	2.3 kB	29/6/22 11:16:00
RB-TAN-SS-01.rsc	2.3 kB	29/6/22 11:17:00

**Ilustración 15-4:** Verificación en el servidor FTP de los archivos backups de los equipos concentradores.

**Fuente:** Servidor Vsftpd, 2022.

#### 4.3.2.2. Registro e informe de cambios en las configuraciones.

En la empresa se maneja un proceso denominado como registro de mantenimiento, en el cual se especifica las diferentes modificaciones físicas y lógicas realizadas a los diferentes equipos, entre estas modificaciones también se incluyen las configuraciones hechas y sus responsables, esta documentación también se almacena en el servidor Vsftpd.

#### 4.3.3. Configuración remota.

La empresa utiliza diferentes métodos para el trabajo remoto, que incluye también la configuración remota de equipos, ya sea con software de terceros o mediante la implementación de diferentes protocolos.

**Tabla 2-4:** Métodos de configuración remota que utiliza la empresa.

Acceso Remoto	Descripción
Túnel VPN	Se utiliza el protocolo L2TP .
Mediante software de terceros	Se utiliza programas como Anydesk o Teamviewer..

Fuente: Intertec, 2022

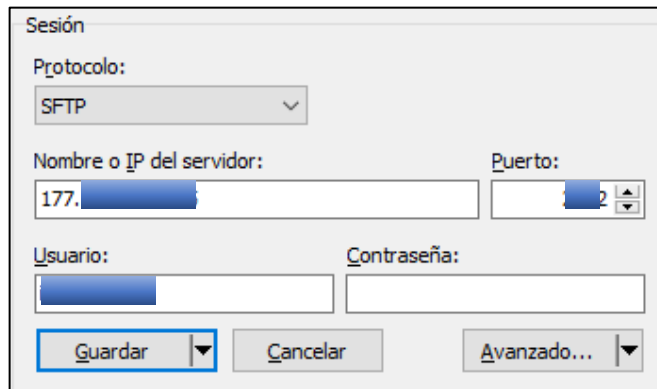
Realizado por: Sagñay, Mauro, 2022.

#### 4.4. Implementación en Gestión de Contabilidad / Administración

##### 4.4.1. Administración del uso de recursos de red

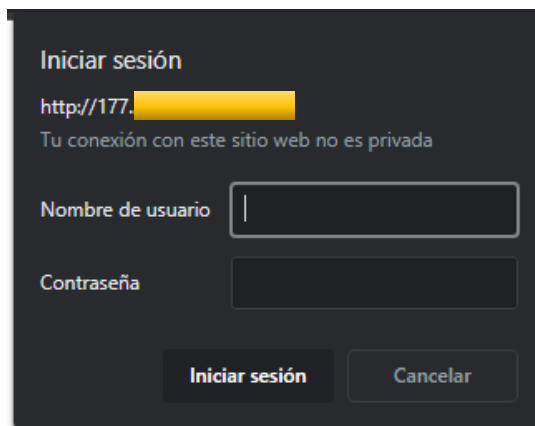
###### 4.4.1.1. Establecimiento de usuarios autorizados.

Así como en el servidor FTP y la herramienta Nagios Core, para su acceso hacen uso de un usuario y contraseña, además desde el aplicativo WinSCP que utiliza el protocolo SSH para la conexión con los servidores.



**Ilustración 16-4:** Acceso a WinSCP mediante SSH.

Fuente: WinSCP, 2022.



**Ilustración 17-4:** Inicio de sesión en la Nagios Core.

Fuente: Nagios, 2022.

#### 4.4.1.2. Establecimiento de cronograma de ventanas de mantenimiento para los distintos equipos

En la empresa se utiliza informes de actividades donde se evidencia las tareas realizadas ya sea en un evento emergente o planificado, en el mismo se evidencias las tareas realizadas además de sus respectivos responsables.

### 4.5. Implementación en Gestión de Rendimiento

Mediante el monitoreo y las métricas obtenidas por el software Nagios se puede verificar y dar seguimiento al correcto desempeño de la infraestructura de red de la empresa, así entonces se puede dar cumplimiento con el modelo FCAPS.

#### 4.5.1. Captura de datos o variables indicadoras de rendimiento

##### 4.5.1.1. Establecimiento de los parámetros de rendimiento

En la Tabla 3-4 se detalla los parámetros que se están monitoreando mediante el sistema de gestión.

**Tabla 3-4:** Definición de parámetros de rendimiento.

<b>Equipos gestionados</b>	<b>Métricas</b>	<b>Funcionalidad</b>	<b>Notificaciones</b>
<b>Core</b>	Carga del CPU	Medida de ocupación actual del procesador.	Telegram
	Memoria Total	Cantidad de memoria total del equipo	
	Memoria Usada	Cantidad de memoria utilizada	
	Uptime	Tiempo de funcionamiento del equipo.	
	PING	Si existe conectividad IP	
<b>Concentradores</b>	Carga de CPU	Medida de ocupación actual del procesador.	Telegram
	Memoria Total	Cantidad de memoria total del equipo	
	Memoria Usada	Cantidad de memoria utilizada	
	Uptime	Tiempo de funcionamiento del equipo.	
	PING	Si existe conectividad IP	

<b>Punto a Punto (PTP)</b>	Intensidad de Señal	Nivel de la intensidad de señal, en dBm	Telegram
	Ruido de Fondo	Suma de todas las señales de ruido y no deseadas, en dBm	
	SNR	La proporción entre la potencia de señal que se transmite y la del ruido, en dB	
	Tx Rate	Tasa de transmisión de datos en bps.	
	Rx Rate	Tasa de recepción de datos en bps.	
<b>Radio Bases (RB)</b>	Carga del CPU	Medidas de ocupación actual del procesador.	Telegram
	Memoria Total	Cantidad de memoria total del equipo	
	Memoria Usada	Cantidad de memoria utilizada	
	Ruido de Fondo	Suma de todas las señales de ruido y no deseadas, en dBm	
	SNR_RB	La proporción entre la potencia de señal que se transmite y la del ruido, en dB.	
	Intensidad de Señal	Nivel de la intensidad de señal, en dBm.	
	Clientes Registrados	Número de clientes que se conectan a la antena.	
PING	Medida para determinar si el equipo de red está activo o no, además de obtener la latencia entre dos equipos		

**Fuente:** Sagñay, Mauro, 2022.

**Realizado por:** Sagñay, Mauro, 2022.

Dependiendo del equipo monitoreado y su ubicación en la red se establecen métricas que son supervisadas periódicamente para determinar valores normales, como se aprecia en la siguiente sección.

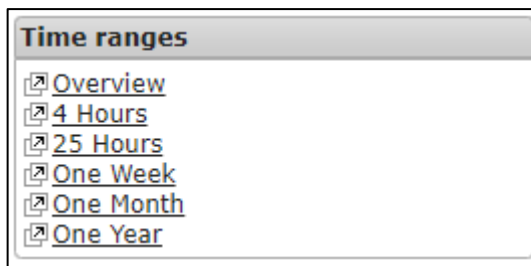
#### **4.5.2. Análisis de los datos para determinar los niveles deseados de rendimiento**

Debido a que no existe un estándar o normativa que defina valores de umbrales para estos parámetros, se usó las especificaciones técnicas de cada equipo como criterio para determinar los

valores adecuados para su funcionamiento. Se utiliza el protocolo SNMP para realizar las consultas de los diferentes parámetros a los equipos monitoreados. Una vez ingresado los equipos y establecido los servicios a monitorear, estos se pueden observar en la interfaz gráfica de Nagios Core.

En las siguientes ilustraciones se muestran el rendimiento de un equipo representativo de los tipos de equipos que posee la infraestructura de red de la empresa. Para todos los casos en el software Nagios, se aprecia el nombre del host o equipo monitoreado, servicio, Status y su información, además de los tiempos de chequeo.

Cabe recalcar que las siguientes capturas de métricas se llevaron a cabo en un período de 4 horas y en diferentes días, sin embargo, esto es irrelevante para determinar el correcto funcionamiento del sistema de gestión de red. También el software Nagios Core a través de su generación de gráficos de desempeño de la red mediante el plugin PNP4Nagios, brinda un bloque para determinar el período de muestra de los datos, como se aprecia en la siguiente ilustración.



**Ilustración 18-4:** Rangos de tiempo para visualizar los gráficos de desempeño de red.

Fuente: Nagios, 2022.

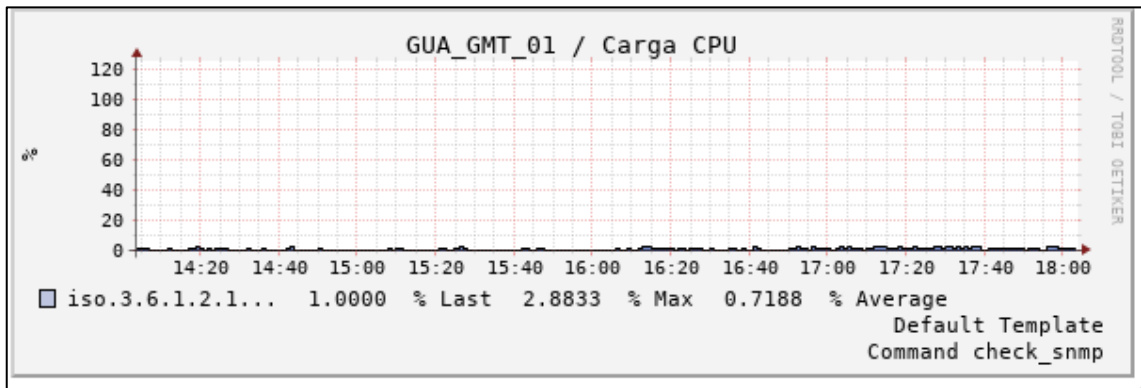
#### 4.5.2.1. Parámetros medidos en equipos del Core

Host	Service	Status	Last Check	Duration	Attempt	Status Information
GUA_GMT_01	Carga CPU	OK	01-29-2023 18:01:39	20d 21h 1m 2s	1/3	SNMP OK - 1 %
	Memoria Total	OK	01-29-2023 18:01:35	20d 22h 21m 59s	1/3	SNMP OK - 950272
	Memoria Usada	OK	01-29-2023 18:01:32	20d 22h 16m 1s	1/3	SNMP OK - 334976
	PING	OK	01-29-2023 18:01:36	20d 20h 10m 43s	1/3	PING OK - Packet loss = 0%, RTA = 1.95 ms
	Uptime	OK	01-29-2023 18:01:34	20d 22h 22m 1s	1/3	SNMP OK - Timeticks: (1083883000) 125 days, 10:47:10.00

**Ilustración 19-4:** Parámetros medidos en el host GAU\_GMT\_01 ubicado en el Core.

Fuente: Nagios, 2022.

- **Consumo del CPU**



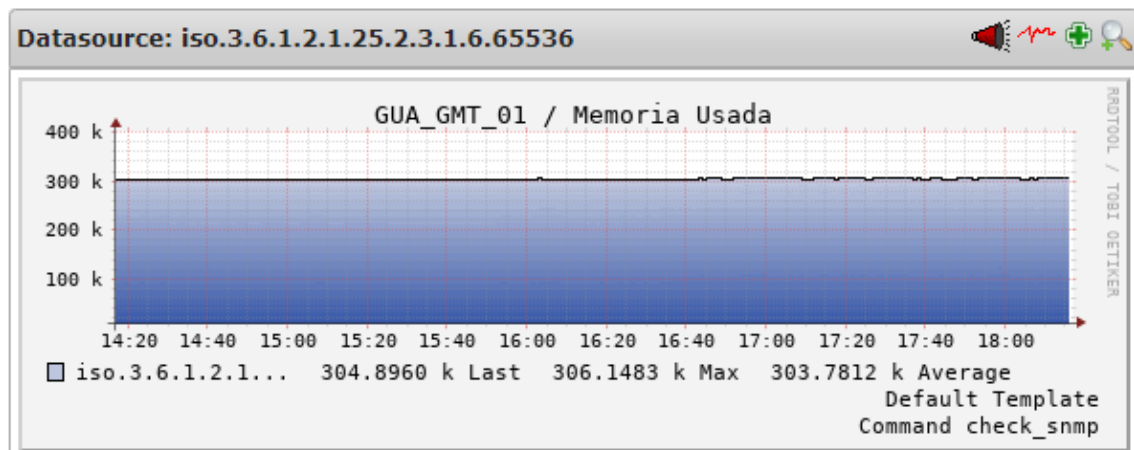
**Ilustración 20-4:** Carga del CPU en el GUA\_GMT\_01 ubicado en el Core.

Fuente: Nagios, 2023.

En la ilustración se aprecia el desempeño del procesador del equipo GUA\_GMT\_01, el cual está ubicado en el core, en las últimas 4 horas, desde las 14h07 hasta las 18h07, obteniéndose valores relativamente bajos del trabajo del procesador, alcanzando un pico de 2.88 % y promedio de uso de 0.718 % en el periodo analizado.

- **Consumo de la Memoria**

**4 Hours** 13.02.23 14:16 - 13.02.23 18:16

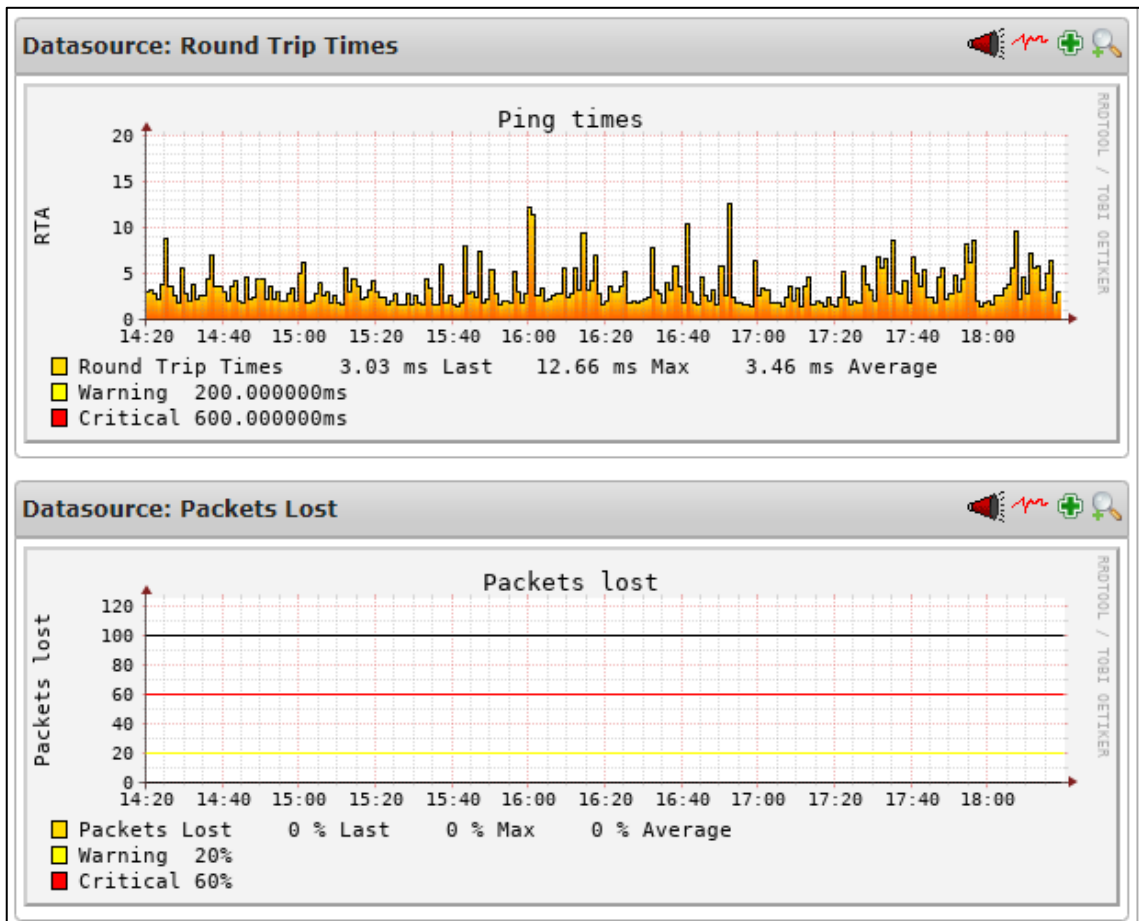


**Ilustración 21-4:** Memoria del equipo Usada.

Fuente: Nagios, 2023.



- PING



**Ilustración 22-4:** Captura de los tiempos de PING y de las pérdidas de paquetes en el equipo.

Fuente: Nagios, 2023.

Como se observa en la ilustración, al estar ubicado el equipo en el core de la infraestructura es esencial que no exista interrupciones de servicio, obteniéndose una pérdida de paquetes nula y tiempos de PING muy bajos alcanzando un pico máximo de 12.66 ms en las 4 horas que se ha realizado el monitoreo.

#### 4.5.2.2. Parámetros medidos en equipos Concentradores

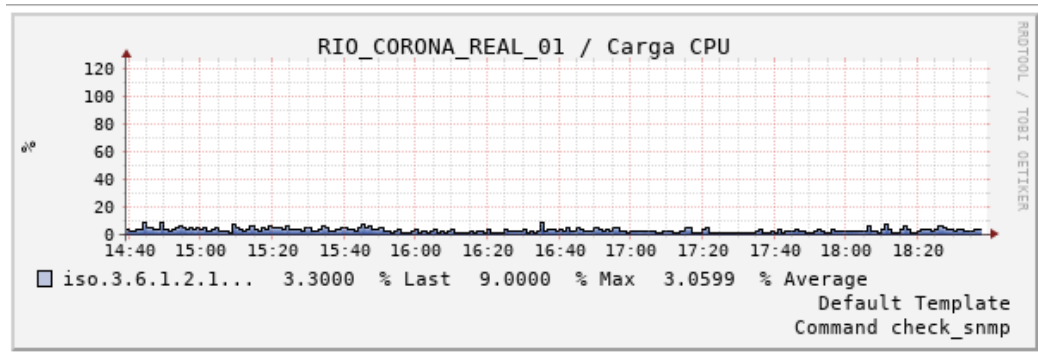
RIO_CORONA_REAL_01	Carga CPU	OK	01-29-2023 18:06:22	25d 12h 39m 40s	1/3	SNMP OK - 3 %
	Memoria Total	OK	01-29-2023 18:06:21	25d 12h 39m 46s	1/3	SNMP OK - 262144
	Memoria Usada	OK	01-29-2023 18:06:20	25d 12h 39m 40s	1/3	SNMP OK - 61688
	PING	OK	01-29-2023 18:06:25	20d 6h 37m 34s	1/3	PING OK - Packet loss = 0%, RTA = 2.52 ms
	Uptime	OK	01-29-2023 18:06:20	25d 12h 39m 39s	1/3	SNMP OK - Timeticks: (596770300) 69 days, 1:41:43.00

**Ilustración 23-4:** Medición de parámetros en el equipo Concentrador RIO\_CORONA\_REAL\_01.

Fuente: Nagios, 2022.

- **Carga del CPU**

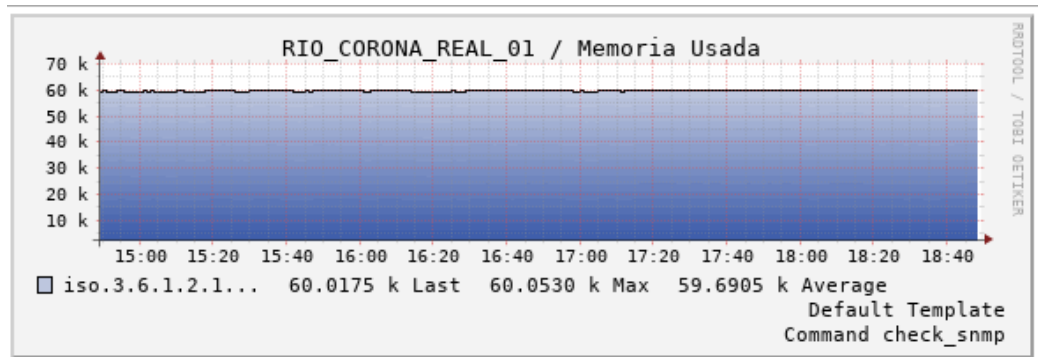
A diferencia del equipo del core de la sección anterior, en este apartado el equipo concentrador presenta una mayor carga de CPU, alcanzando un pico de 9% en el periodo monitoreado.



**Ilustración 24-4:** Carga del CPU en el equipo RIO\_CORONA\_REAL\_01.

Fuente: Nagios, 2023.

- **Memoria Usada**

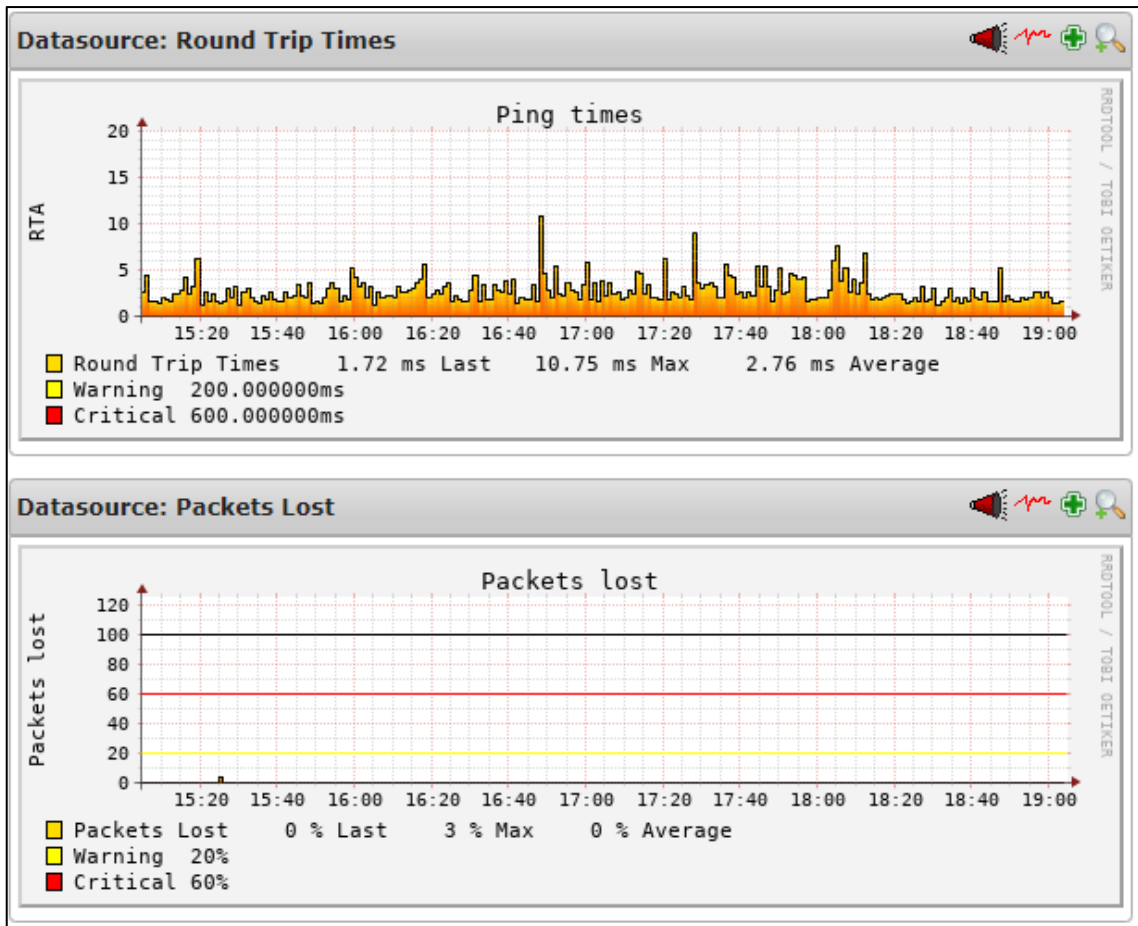


**Ilustración 25-4:** Memoria usada en el equipo RIO\_CORONA\_REAL\_01.

Fuente: Nagios, 2023.

- **PING**

En la ilustración se muestra el tiempo de Ping (RTA) y el porcentaje de paquetes ICMP perdidos, donde se aprecia que en el tiempo de monitoreo no se excede los valores normales.



**Ilustración 26-4:** Tiempo de Ping y pérdida de paquetes en el equipo RIO\_CORONA\_REAL\_01

Fuente: Nagios, 2023.

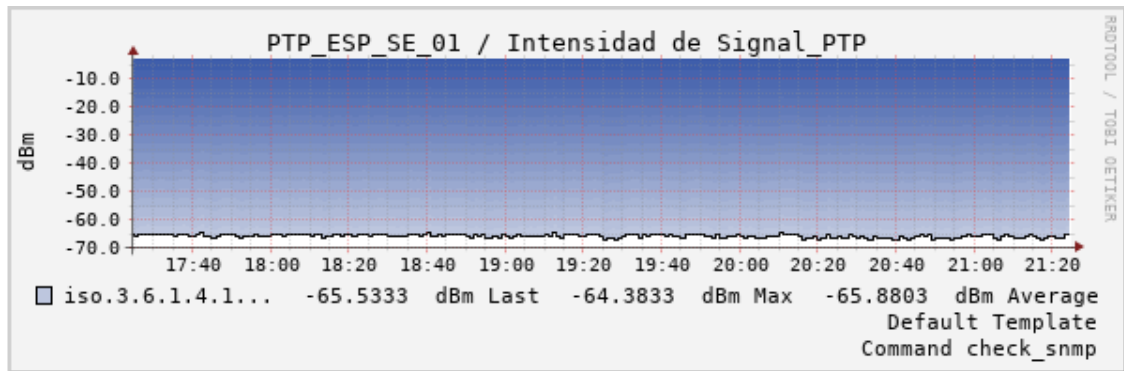
#### 4.5.2.3. Parámetros medidos en los equipos Punto a Punto (PTP)

PTP_ESP_SE_01	Intensidad de Signal_PTP	OK	01-29-2023 18:10:55	1d 4h 15m 34s	1/3	SNMP OK - -67 dBm
	PING	OK	01-29-2023 18:10:53	1d 4h 15m 35s	1/3	PING OK - Packet loss = 0%, RTA = 0.98 ms
	Ruido de Fondo	OK	01-29-2023 18:10:59	25d 12h 44m 9s	1/3	SNMP OK - -111 dBm
	Rx Rate	OK	01-29-2023 18:10:55	1d 4h 15m 33s	1/3	SNMP OK - 57700000 bps
	SNR_PTP	OK	01-29-2023 18:10:59	1d 4h 15m 34s	1/3	SNMP OK - 44 dB
	Tx Rate	OK	01-29-2023 18:10:49	1d 4h 15m 33s	1/3	SNMP OK - 78000000 bps
	Uptime_PTP	OK	01-29-2023 18:10:58	1d 4h 15m 34s	1/3	SNMP OK - Timeticks: (10175800) 1 day, 4:15:58.00

**Ilustración 27-4:** Parámetros medidos en el equipo Punto a Punto PTP\_ESP\_SE\_01

Fuente: Nagios, 2022.

- **Intensidad de señal**

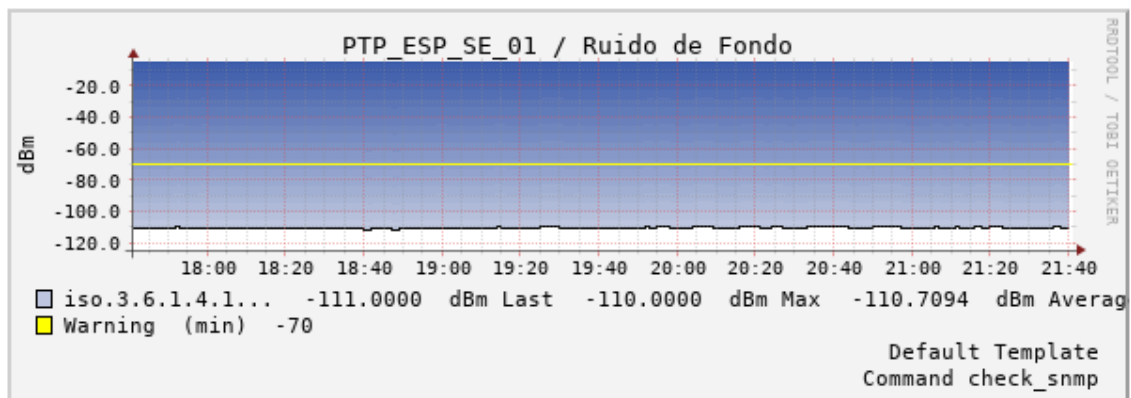


**Ilustración 28-4:** Intensidad de señal del equipo PTP\_ESP\_SE\_01.

Fuente: Nagios, 2023

Como se observa en la ilustración, la intensidad de señal que transmite la antena no ha tenido variaciones bruscas o caídas, lo que favorece a mantener operativo el radioenlace para el transporte de datos. El valor relativo constante alcanza -65.88 dBm, que superara los -75 dBm mínimos necesarios para un correcto funcionamiento.

- **Ruido de fondo (Noise Floor)**



**Ilustración 29-4:** Ruido de fondo captado en el equipo PTP\_ESP\_SE\_01.

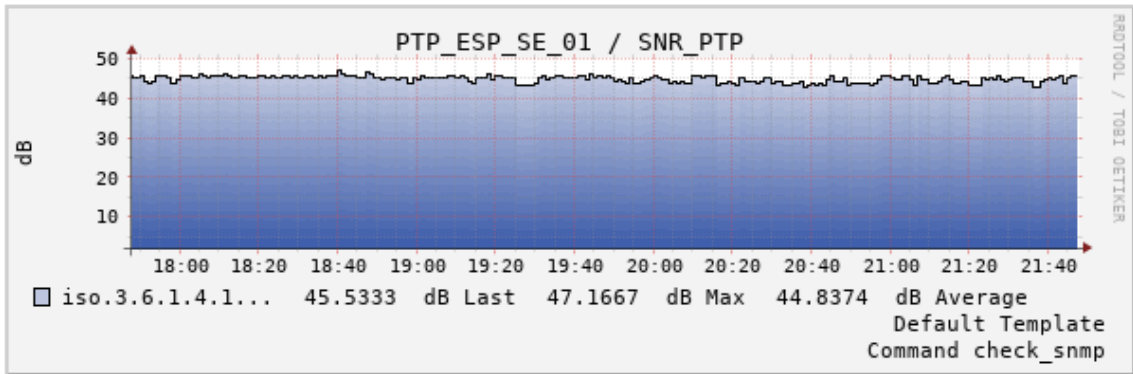
Fuente: Nagios, 2023.

Por definición, el ruido de fondo es la sumatoria del ruido del entorno y todas las señales no deseadas alrededor de la antena. Este valor debe estar por encima de la sensibilidad mínima del equipo que son -75 dBm, como se observa en la ilustración el ruido de fondo no sobrepasa los -110 dBm de potencia, este valor no llega a interferir en la recepción normal de los datos.

- **Nivel de SNR**

El Nivel de señal a ruido SNR, define la relación entre la potencia de la señal sobre la potencia del ruido, por lo que un valor alto garantiza una buena transmisión / recepción de los datos, como

se aprecia en la siguiente ilustración el valor permanece constante en todo el tiempo de monitoreo, entonces de igual manera el enlace no se verá afectado.

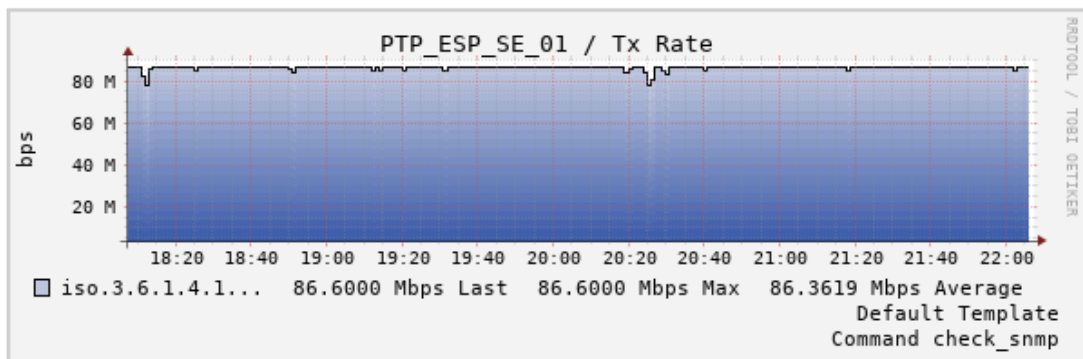


**Ilustración 30-4:** Nivel de Señal a Ruido SNR del equipo PTP\_ESP\_SE\_01

Fuente: Nagios, 2023.

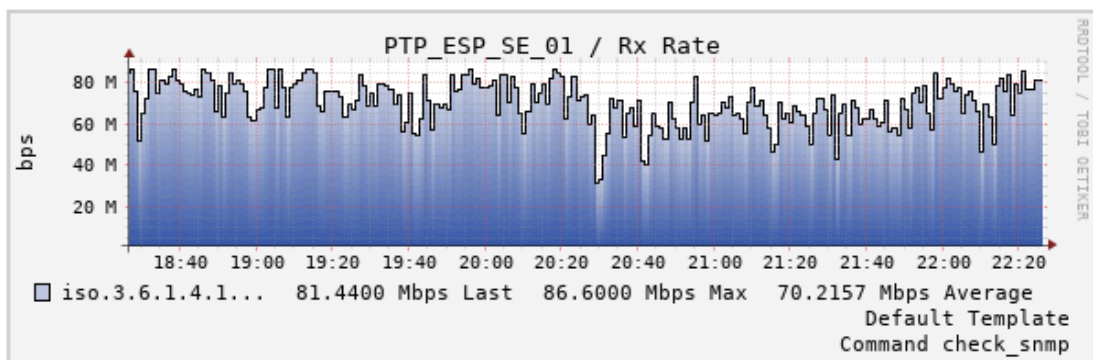
- **Tasa de Tx y Rx**

En las siguientes ilustraciones se aprecian las tasas de transmisión y recepción del equipo PTP\_ESP\_SE\_01, obteniendo los siguientes valores.



**Ilustración 31-4:** Tasa de transmisión del equipo PTP\_ESP\_SE\_01.

Fuente: Nagios, 2023



**Ilustración 32-4:** Tasa de recepción del equipo PTP\_ESP\_SE\_01.

Fuente: Nagios, 2023

Como se puede apreciar, las tasas de datos tanto en transmisión como en recepción son graficadas brindando información del consumo de los clientes y la ocupación del ancho de banda del radioenlace, en este caso se observa que la tasa de transmisión permanece relativamente constante, mientras que la tasa de recepción sus valores varían.

El valor promedio ronda los 86.6 Mbps, sin sobrepasar los 100 Mbps que este equipo soporta.

#### 4.5.2.4. Parámetros medidos en los equipos Radio Base (RB)

Host	Service	Status	Last Check	Duration	Attempt	Status Information
RB_GLL_SE_01	Carga CPU	OK	01-29-2023 18:14:31	1d 22h 50m 45s	1/3	SNMP OK - 12 %
	Cientes Registrados	OK	01-29-2023 18:14:37	1d 22h 50m 36s	1/3	SNMP OK - 6 Clients
	Intensidad de Signal_RB	OK	01-29-2023 18:14:36	1d 5h 23m 51s	1/3	SNMP OK - -62 dBm
	Memoria Total	OK	01-29-2023 18:14:29	1d 21h 43m 19s	1/3	SNMP OK - 131072
	Memoria Usada	OK	01-29-2023 18:14:30	1d 22h 50m 38s	1/3	SNMP OK - 45292
	PING	OK	01-29-2023 18:14:31	0d 20h 41m 57s	1/3	PING OK - Packet loss = 0%, RTA = 33.19 ms
	Ruido de Fondo	OK	01-29-2023 18:14:37	1d 22h 50m 39s	1/3	SNMP OK - -106 dBm
	SNR_RB	OK	01-29-2023 18:14:29	1d 5h 23m 52s	1/3	SNMP OK - 43 dB

**Ilustración 33-4:** Parámetros medidos en el equipo Radio Base RB\_GLL\_SE\_01.

Fuente: Nagios, 2022

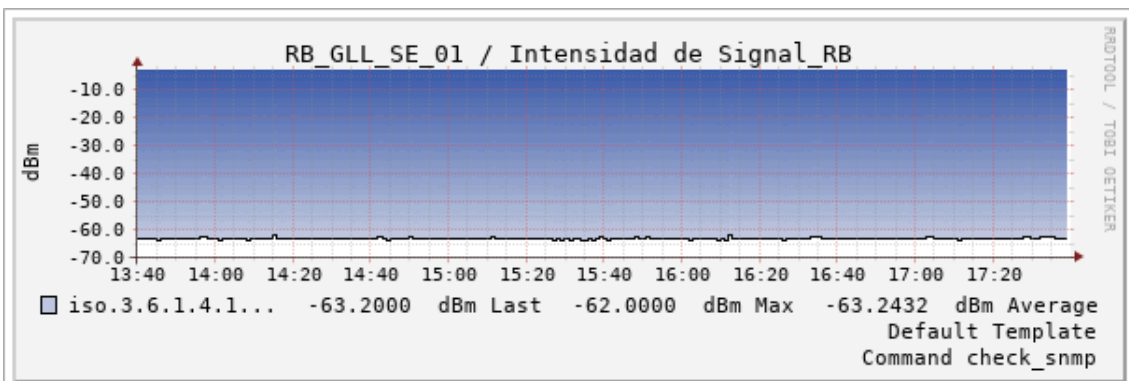
Como se observa en las ilustraciones anteriores, como herramientas para el monitoreo de los diferentes equipos se utilizó el protocolo ICMP a través de PING y el protocolo SNMP para la realización de consultas de parámetros a los diferentes equipos de la red.

- **Cientes Registrados**

También se capturo el número de clientes, esta métrica es necesario para tener un mejor control a la hora de definir una migración de abonados debido a la saturación de la antena o para el cambio de un equipo de mejores características. Como se aprecia en la ilustración anterior, en el momento de la toma de mediciones la Radio Base cuenta con 12 abonados.

Otras métricas que también se tomó en cuenta se presentan en las siguientes ilustraciones.

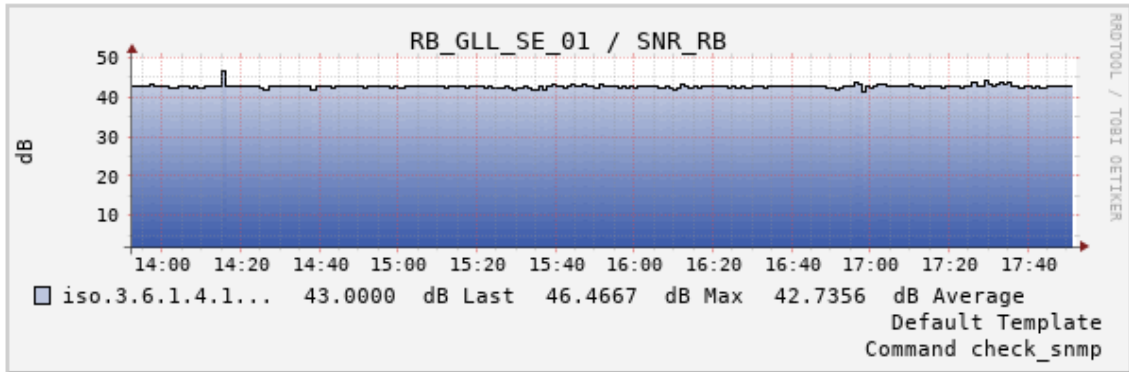
- **Intensidad de señal**



**Ilustración 34-4:** Intensidad de señal en el equipo RB\_GLL\_SE\_01.

Fuente: Nagios, 2023

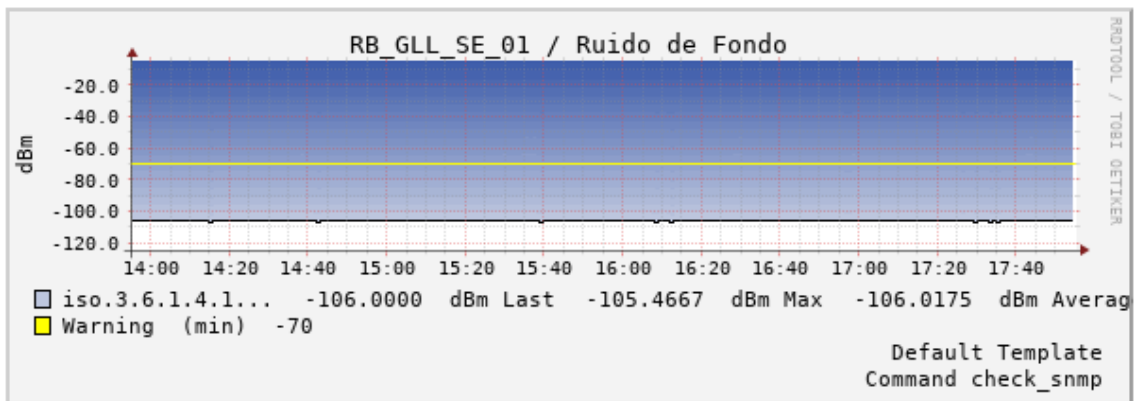
- **Nivel SNR**



**Ilustración 35-4:** Nivel de SNR en el equipo RB\_GLL\_SE\_01.

Fuente: Nagios, 2023

- **Ruido de Fondo (Noise Floor)**



**Ilustración 36-4:** Nivel de ruido captado en el equipo RB\_GLL\_SE\_01.

Fuente: Nagios, 2023

Como se observa, estos parámetros se encuentran relativamente invariables en todo el periodo que se ha monitoreado lo que se traduce en un enlace sin caídas mejorando así la disponibilidad del servicio entregado. Los valores obtenidos en la intensidad de señal alcanzan un punto máximo de -63 dBm, el nivel de SNR alcanza los 46.46 dB, mientras que el nivel de ruido percibido por el equipo no supera los -105 dBm que llega a causar algún tipo de interferencia en la señal.

#### 4.5.2.5. Medición de parámetros en servidores

Se aprecia los parámetros medidos en los servidores dentro de la infraestructura de la empresa,

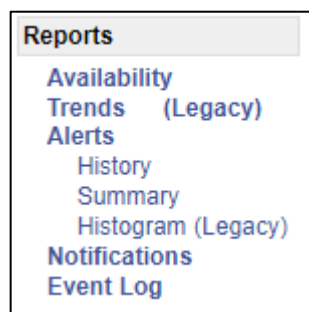
Host	Service	Status	Last Check	Current	Target	Units	Info
NPERF	Current Load	CRITICAL	02-14-2023 18:25:58	0d 11h 1m 53s	4/4		CRITICAL - load average: 5.03, 6.01, 6.49
	Current Users	OK	02-14-2023 18:26:17	172d 1h 22m 54s	1/4		USERS OK - 1 users currently logged in
	HTTP	OK	02-14-2023 18:26:25	104d 12h 39m 57s	1/4		HTTP OK: HTTP/1.1 200 OK - 306 bytes in 0,001 second response time
	PING	OK	02-14-2023 18:26:29	104d 12h 40m 49s	1/4		PING OK - Packet loss = 0%, RTA = 0.24 ms
	Root Partition	OK	02-14-2023 18:26:34	0d 9h 27m 17s	1/4		DISK OK - free space: / 2982 MiB (20,96% inode=53%):
	SSH	OK	02-14-2023 18:26:54	104d 12h 40m 49s	1/4		SSH OK - OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 (protocol 2.0)
	Swap Usage	OK	02-14-2023 18:26:10	172d 1h 17m 36s	1/4		SWAP OK - 100% free (3227 MB out of 3227 MB)

**Ilustración 37-4:** Medición de parámetros en el servidor NPERF.

Fuente: Nagios, 2023

#### 4.5.3. Generación de Reportes

De manera integrada en el software Nagios Core, se genera los reportes de los diferentes equipos que se está monitoreando, dentro de las opciones que se puede escoger se aprecia en la siguiente ilustración los tipos de reportes disponibles.



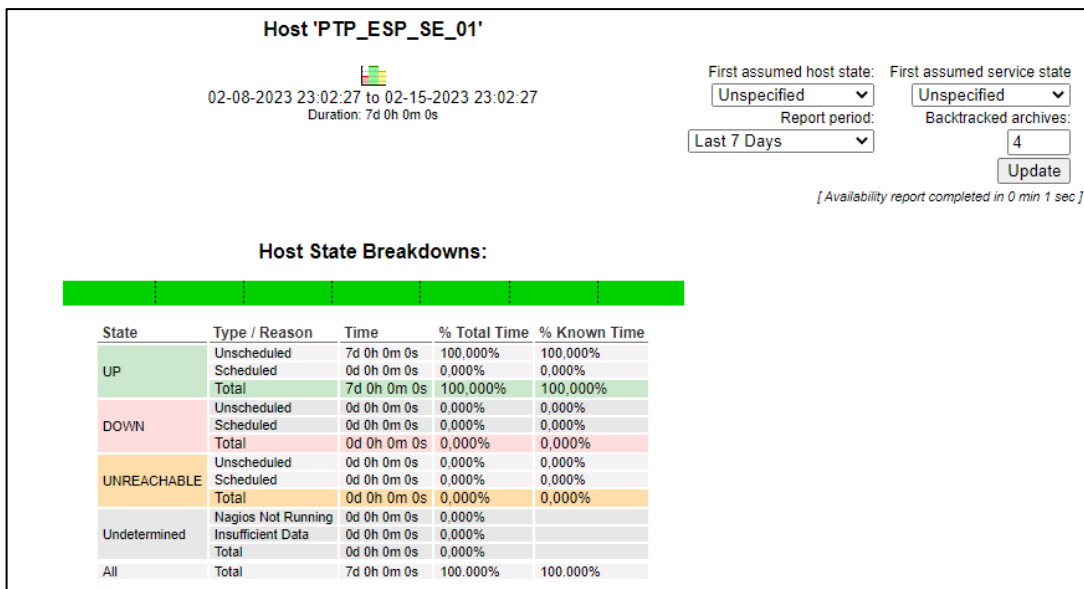
**Ilustración 38-4:** Tipos de reportes disponibles.

Fuente: Nagios, 2023.

##### 4.5.3.1. Reporte de disponibilidad

Mediante este reporte se logra obtener estadísticas sobre la disponibilidad del equipo, en este caso se muestra la variación del estado up, down, unreachable (inalcanzable), o undetermined (indeterminado), como se muestra en la siguiente ilustración, mediante Nagios Core se obtiene la disponibilidad de este equipo en los últimos 7 días.





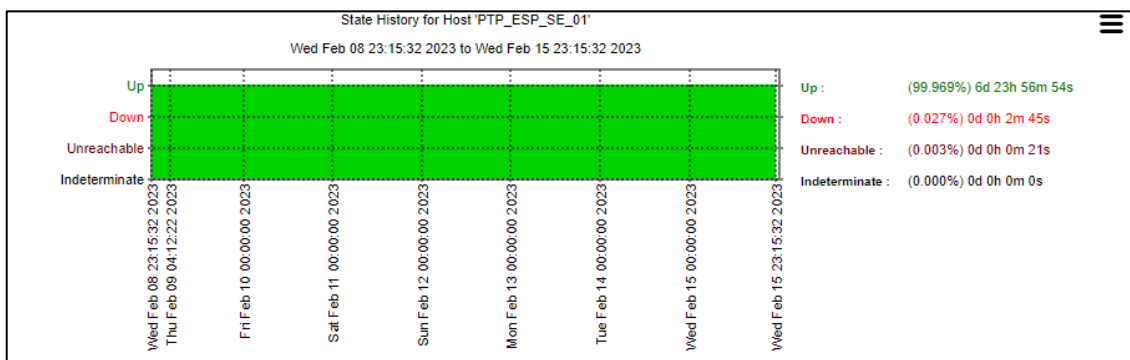
**Ilustración 39-4:** Reporte de disponibilidad del equipo PTP\_ESP\_SE\_01.

Fuente: Nagios, 2023.

Dentro de la información que entrega este reporte se incluye, el tipo o razón del cambio de estado, tiempo que el equipo permaneció en ese estado, y su representación porcentual.

#### 4.5.3.2. Reporte de Tendencia

Este reporte se encarga de realizar un desglose del estado del equipo o servicio monitoreado, como se observa en la siguiente ilustración se obtiene el período tanto en porcentaje como en día, horas, minutos y segundos, para este caso este equipo no tuvo ninguna caída en todo el período monitoreado.



**Ilustración 40-4:** Reporte de tendencia del equipo PTP\_ESP\_SE\_01.

Fuente: Nagios, 2023.

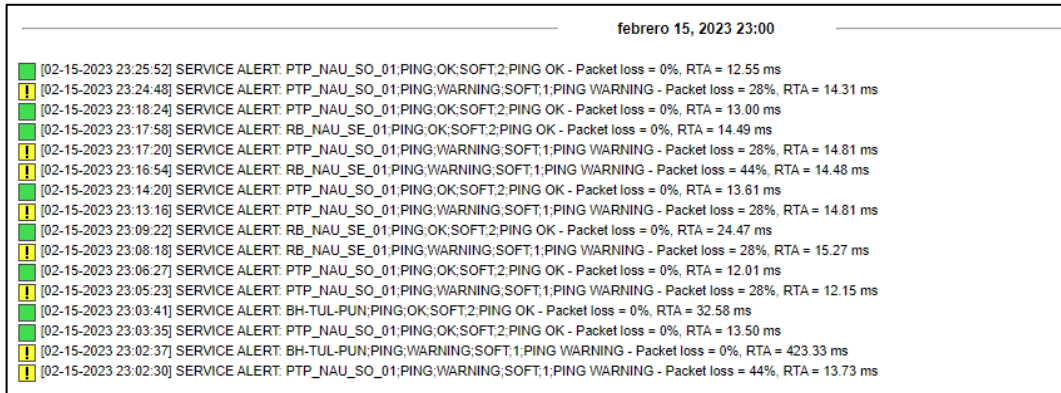
#### 4.5.3.3. Reporte de Alertas

Estos reportes engloban a todos los eventos ocurridos en los equipos monitoreados, dentro de este se puede obtener otros reportes como son el historial que muestra un listado ordenado cronológicamente de todas las alertas generadas, el summary o resumen donde se obtiene los

resultados en forma de tabla y el histograma donde se genera una gráfica que muestra la variación de los estados del equipo o servicio monitoreado. Esto se aprecia en las siguientes ilustraciones.

- **Historial de alertas**

En la siguiente ilustración se aprecia las últimas alertas ocurridas en el lapso de una hora en el sistema de gestión.



**Ilustración 41-4:** Historial de alertas generadas en Nagios Core, en el período de una hora.

Fuente: Nagios, 2023

- **Resumen de alertas**

Mediante esta opción se puede obtener una vista general de las diferentes alertas generadas como se observa en la siguiente ilustración, se generó una lista con los equipos que generan la mayor cantidad de alertas en el período de 7 días, siendo el principal el equipo RB\_NIN\_01 con 7 alertas.

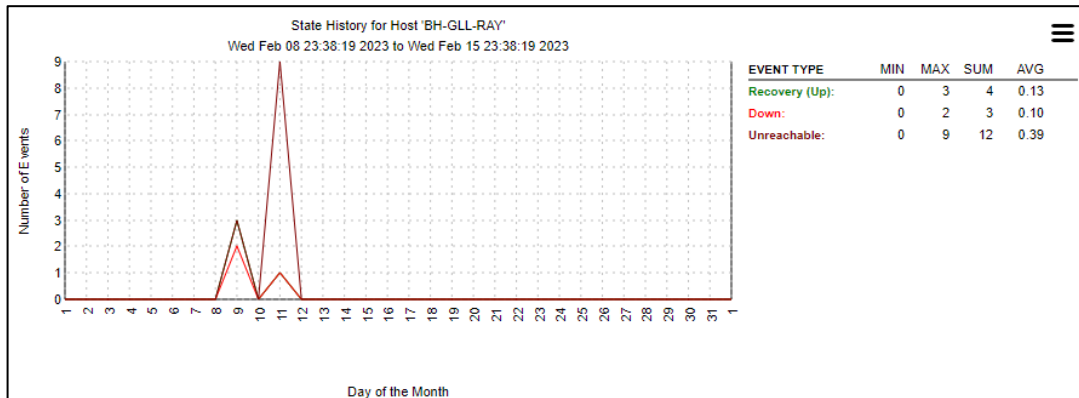
Rank	Producer Type	Host	Service	Total Alerts
#1	Host	RB_NIN_01	N/A	7
#2	Host	CE-NINO-LOMA	N/A	6
#3	Host	BH-NIN-GLL	N/A	6
#4	Host	CPE_NIN_01	N/A	6
#5	Host	RB_NIN_SO_01	N/A	6
#6	Host	PTP_H2O_NE_03	N/A	6
#7	Host	PTP_H2O_NE_04	N/A	6
#8	Host	CE-TANQUE	N/A	4
#9	Host	CE-CEBADAS	N/A	4
#10	Host	PTP_TUL_NO_01	N/A	4
#11	Host	CE-GUARGUALLA	N/A	3
#12	Host	GMT_GAL_01	N/A	2
#13	Host	CE-GALTE	N/A	2
#14	Host	RB_GAL_SE_01	N/A	2
#15	Host	CE-CALPI	N/A	2
#16	Host	PTP_GAL_EE_01	N/A	2
#17	Host	RB_GAL_NE_01	N/A	2
#18	Host	BH-GAL_CEB	N/A	2
#19	Host	RB_GLL_EE_01	N/A	2
#20	Host	PTP_GLL_SE_01	N/A	2
#21	Host	RIO_GUARGUALLA_01	N/A	2
#22	Host	RB_GLL_SE_01	N/A	2
#23	Host	BH-GLL-NIN	N/A	2
#24	Host	BH-GLL-RAY	N/A	2
#25	Host	CE-ESPOCH	N/A	2

**Ilustración 42-4:** Resumen de los equipos que más alertas han generado en los últimos 7 días.

Fuente: Nagios, 2023.

- **Histograma de Alertas**

Esta opción permite el desglose de una gráfica donde se observa la variación de los estados que ha sufrido un equipo monitoreado en un lapso de tiempo, para este caso en la siguiente ilustración se aprecia que el equipo BH\_GLL\_RAY ha tenido 2 caídas el 9 de febrero además de que se ha recuperado en 3 ocasiones el mismo día, además de que ha estado inalcanzable 9.



**Ilustración 43-4:** Histograma de la variación de estados ocurridos en equipo BH\_GLL\_RAY en el período de 7 días.

Fuente: Nagios, 2023.

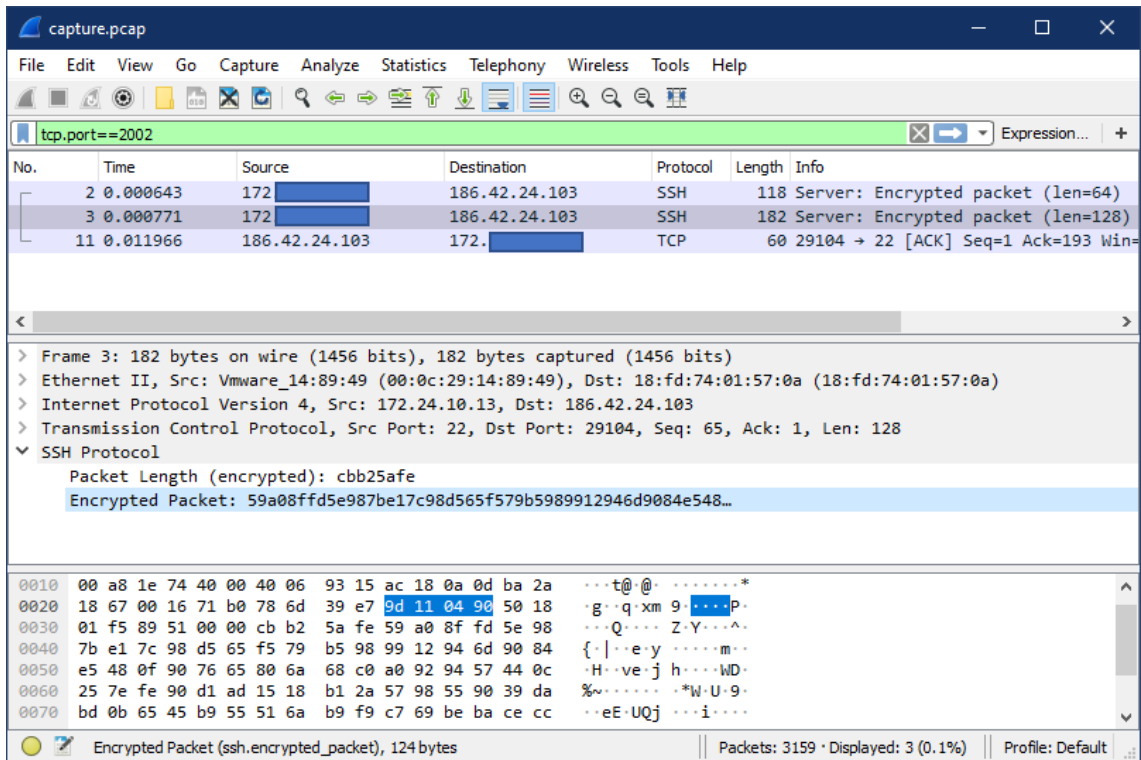
#### 4.6. Implementación en Gestión de Seguridad

El software Nagios Core maneja un control de acceso con credenciales y diferentes niveles de usuario, ayudando a evitar un acceso a personal no adecuado y que se comprometa la información confidencial de los equipos y servidores monitoreados, además de que sirve como un gran apoyo para cumplir con los aspectos de seguridad en el modelo FCAPS.

##### 4.6.1. Encriptado de la información

Para la transferencia y almacenamiento de archivos sensibles se utiliza un servidor Linux vsftpd, en el cual se utiliza el Protocolo Seguro de Transferencia de Archivos (SFTP), este protocolo se utiliza con Secure Shell (SSH) para brindar seguridad a los datos.

Como se observa en la siguiente ilustración, se verifica a través de una captura de tráfico, mediante Wireshark, que se da la conexión segura mediante SSH para el acceso al software de monitoreo Nagios Core.



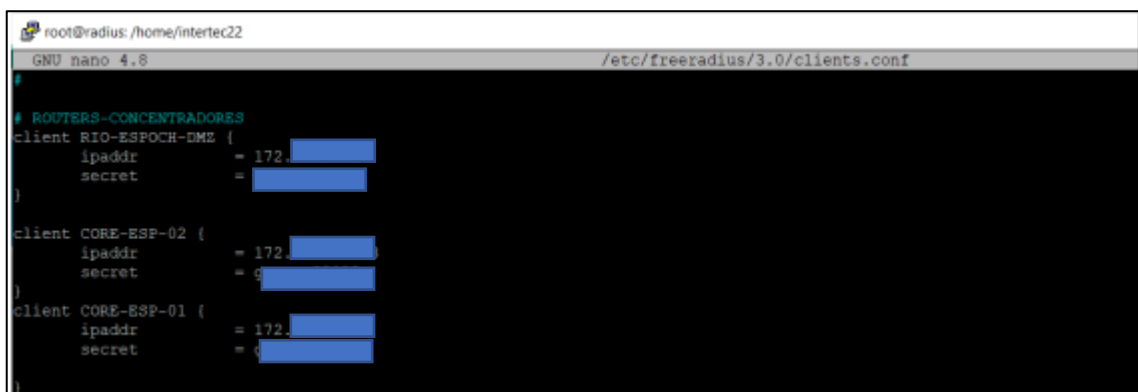
**Ilustración 44-4:** Verificación de acceso a Nagios mediante SSH para una conexión segura.

Fuente: Wireshark, 2022

#### 4.6.2. Establecimiento de procesos de autenticación

Para cumplir con este apartado se utiliza un servidor RADIUS, a través del software FreeRadius, el mismo que es gratuito y proporciona gran rendimiento para la autenticación y autorización de los diferentes usuarios.

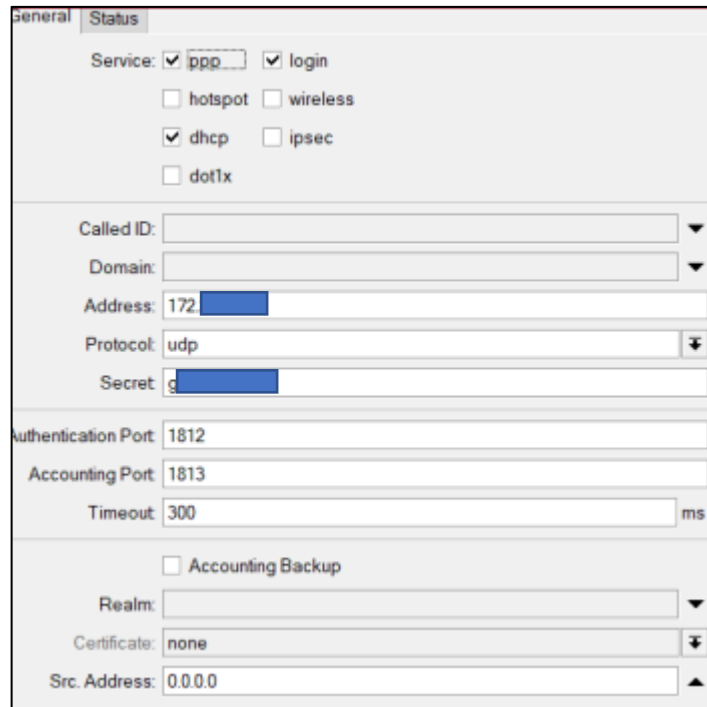
Para agregar equipos en el servidor RADIUS se logra modificando el archivo *clients.conf* como se muestra en la siguiente ilustración.



**Ilustración 45-4:** Creación de credenciales para los diferentes equipos de la red.

Fuente: Freeradius, 2022

En el archivo se deberá incluir la dirección IP del equipo y en el apartado de secret, se deberá establecer la contraseña de acceso. Como se observa en la ilustración anterior, se ha creado las credenciales para los equipos concentradores, este proceso es similar para los demás equipos. Luego se crea los diferentes usuarios que tendrán acceso a los equipos ingresados en el servidor, luego se deberá establecer la configuración del apartado RADIUS en cada equipo, donde se establece la dirección IP del servidor y la contraseña, para de esta manera lograr la gestión de credenciales mediante el servidor FreeRadius.



**Ilustración 46-4:** Configuración de RADIUS en equipos Mikrotik.

Fuente: Mikrotik, 2022

#### 4.6.3. Control de acceso a los recursos

El acceso y uso del software de monitoreo se realiza mediante la creación de perfiles de usuarios con diferentes permisos o privilegios, esto se logra mediante la edición del siguiente archivo de configuración.

```
htpasswd /usr/local/nagios/etc/htpasswd.users nuevo_user
```

Al ingresar ese comando pedirá una contraseña, luego se ingresa y se pulsa Enter.

Para poder establecer los privilegios del nuevo usuario creado, se deberá modificar el archivo de configuración *cgi.cfg*. Para este caso se ha establecido dos tipos de usuarios de software de monitoreo.

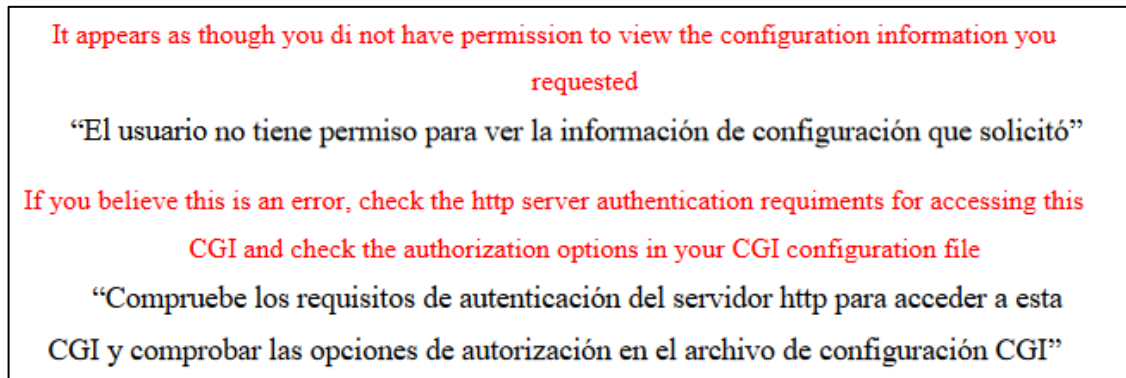
**Tabla 4-4:** Generación de usuarios y sus respectivos privilegios.

Tipo de Usuario	Descripción de permisos
Gerente Técnico	Agregación, cambio, eliminación y configuración de equipos y servicios.
Operador de red	Solo se permite el acceso a la interfaz web para solo lectura de los diferentes estados de equipos y servicios.

Fuente: Nagios, 2022.

Realizado por: Sagñay Mauro, 2022.

El usuario de solo lectura, no podrá visualizar las pestañas de Información de Procesamiento, Scheduling queue, al intentar ingresar a esa sección se obtendrá un mensaje de error de la siguiente forma.



**Ilustración 47-4:** Mensaje de error obtenido cuando se intenta el acceso a secciones no autorizadas.

Fuente: Nagios, 2022.

#### 4.7. Cumplimiento de las políticas de gestión de red.

En la siguiente tabla se presenta el nivel de cumplimiento, expresado en porcentajes, a las políticas de gestión de red por parte del software de monitoreo Nagios Core y las demás herramientas de gestión presentadas en este trabajo.

**Tabla 5-4:** Nivel de cumplimiento en porcentaje a las políticas de gestión de red.

Políticas	Porcentaje de cumplimiento	Descripción
1. Información del sistema de gestión de red	75%	El manual para la utilización del sistema de gestión ha sido entregado a la gerencia de la empresa, mas no se ha verificado si esta documentación fue socializada.

2. Creación y modificación de las políticas de gestión.	100%	Las políticas de gestión de red fueron desarrolladas y aprobadas por la autoridad respectiva.
3. Reconocimiento de fallas	100%	Mediante el software de monitoreo Nagios se logra determinar cuando un equipo o servicio ha cometido una falla y visualizarlo en su interfaz gráfica.
4. Tiempo de atención a fallos	75%	Mediante Nagios se puede aislar la falla de un equipo o servicio y asignar niveles de prioridad mediante colores, sin embargo los tiempos de atención son determinados según el criterio del Operador de red o la autoridad de mayor jerarquía.
5. Documentación de fallas	75%	El sistema de gestión de red se encarga principalmente de generar y presentar gráficas o métricas que sirva como insumos para el desarrollo de informes u otra documentación sobre el estado de la red, la documentación es desarrollada por el Operador de red o el personal respectivo.
6. Desarrollo de pruebas de diagnóstico	100%	Mediante el software Nagios Core se establecen diferentes chequeos mediante el protocolo ICMP o SNMP que ayudan diagnosticar el estado de equipos y servicios de la red.
7. Manejo de errores	75%	Mediante el almacenamiento de los archivos de configuración de cada equipo monitoreado, se puede restablecer su configuración en caso de errores graves de funcionamiento, sin embargo, este proceso se lo realiza de forma manual por el Operador de red u otro personal designado.
8. Entrada de equipos al sistema de gestión.	100%	Para ser monitoreados, todos los equipos se ingresaron en el sistema de gestión de manera correcta.

9. Identificación de equipos	100%	En el software de monitoreo se establecen los nombres para identificar cada equipo, es totalmente personalizable.
10. Configuración SNMP	100%	En todos los equipos a ser monitoreados se estableció la configuración respectiva para establecer una comunicación mediante SNMP funcional.
11. Backup de archivos de configuración	100%	Se estableció un script para la descarga y transmisión de los archivos de configuración de los equipos y su posterior almacenamiento seguro en un servidor.
12. Configuración remota	50%	Los métodos para realizar una configuración remota, los realiza enteramente los Operadores de red o autoridades de jerarquías mayores que tengan la potestad de brindar acceso a la red.
13. Uso de recursos de la red	100%	Para este trabajo se ha considerado la creación de dos usuarios con todos los privilegios y otro de solo lectura.
14. Seguimiento a actividades	50%	Esta tarea es llevada a cabo enteramente por el personal técnico que realiza las actividades ya sea programadas o emergentes.
15. Determinar los parámetros de rendimiento	100%	Los parámetros a medir dependen de cada tipo de equipo, así mismo de su ubicación en la red.
16. Utilización del protocolo SNMP	100%	Tanto los equipos de red como el sistema de gestión se han configurado para utilizar el protocolo SNMP para la transmisión de las distintas métricas de rendimiento.
17. Establecimiento de umbrales	100%	Estos valores se asignaron según las especificaciones técnicas de cada equipo o según el criterio del Operador de red u otro autoridad de mayor jerarquía.
18. Generación de Informes	75%	El software de monitoreo Nagios Core permite la generación de gráficas donde se



		aprecia el comportamiento del equipo o los servicios monitoreados, estos son usados como respaldo al personal respectivo al momento de realizar los informes.
19. Encriptación en la transmisión de información	75%	Para la transmisión y almacenamiento de información sensible como datos personales de clientes y trabajadores se utiliza un servidor vsftpd, sin embargo no se implementan algoritmos para el cifrado de la información guardada.
20. Encriptación en servidor de correo	0%	No se ha establecido aspectos de seguridad en el servidor de correo de la empresa.
21. Autenticación en servidores	100%	Para el acceso y operación de los servidores de la empresa se utiliza un protocolo seguro como SSH para la autenticación de usuarios.
22. Autenticación en equipos de red	100%	Se estableció el servidor RADIUS para la administración de usuarios y que estos logren tener acceso a los equipos de la red.
23. Control de acceso a los recursos	100%	En Nagios Core se puede establecer usuarios con diferentes privilegios de esta manera se puede controlar la información que puede visualizar un usuario del sistema de gestión.
24. Envío de notificaciones	100%	Las notificaciones se envían mediante el aplicativo Telegram y solo a los usuarios autorizados que pertenecen a un grupo de chat previamente creado.
25. Monitoreo frente a ataques.	50%	Mediante el sistema de gestión se puede determinar un comportamiento inusual en los equipos de la red, mas no se puede determinar si la causa es un ataque exterior o una falla propia del equipo.

**Fuente:** Sagnay Mauro, 2022.

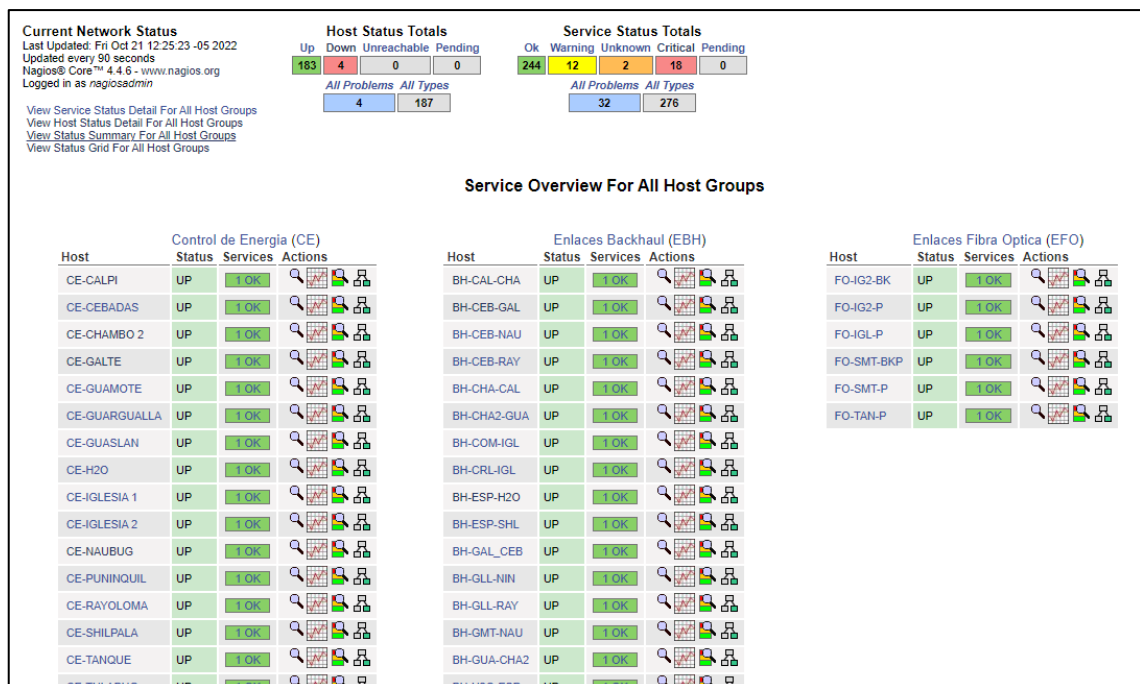
**Realizado por:** Sagnay Mauro, 2022.

#### 4.8. Implementación final del sistema de gestión de red.

A continuación, se muestran el resultado final de la implementación del sistema de gestión de red basado en FCAPS para monitorear el servicio de acceso a internet de la empresa Intertec.

##### 4.8.1. Establecimiento de grupos de host

En las capturas siguientes se muestran los grupos de hosts creados, los cuales hacen referencia a los distintos niveles y categoría de la infraestructura de red de la empresa, de esta manera es más fácil y cómodo para el personal encargado, encontrar el dispositivo que está generando problemas o que se necesita realizar algún tipo de mantenimiento.



**Ilustración 48-4:** Lista Hostgroup 1 generada en la infraestructura de red.

**Realizado por:** Sagñay, Mauro, 2022

OLT Fibra (OLT)				Enlaces Punto a Punto (PTP)				Radio Bases (RB)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
OLT_CHA_01	UP	1 OK		CPE_NIN_01	DOWN	1 CRITICAL		RB_CEB_NO_01	UP	1 OK	
OLT_CHA_01b	UP	1 OK		PTP_COM_SE_01	UP	1 OK		RB_CEB_SO_01	UP	1 OK	
OLT_ESP_01	UP	1 OK		PTP_COM_SO_01	UP	1 OK		RB_CHA_NO_01	UP	1 OK	
OLT_GMT_01	UP	1 OK		PTP_CRL_NO_01	UP	1 OK		RB_CHA_NO_02	UP	1 OK	
OLT_GUA_01	UP	1 OK		PTP_CRL_OO_01	UP	1 OK		RB_CHA_OO_01	UP	1 OK	
OLT_IGL2_01	UP	1 OK		PTP_CRL_SS_01	UP	1 OK		RB_CHA_OO_02	UP	1 OK	
OLT_SMT1	UP	1 OK		PTP_ESP_SE_01	UP	1 OK		RB_CHA_OO_03	UP	1 OK	
OLT_SMT2	UP	1 OK		PTP_GAL_EE_01	UP	1 OK		RB_CHA_OO_04	UP	1 OK	
OLT_TAN1	UP	1 OK		PTP_GLL_SE_01	UP	1 OK		RB_CHA_OO_05	UP	1 OK	
				PTP_H2O_NE_03	UP	1 OK		RB_CHA_SE_01	UP	1 OK	
				PTP_H2O_NE_04	UP	1 OK		RB_CHA_SO_01	UP	1 OK	
				PTP_H2O_NE_05	UP	1 OK		RB_CHA_SO_02	UP	1 OK	
				PTP_IGE_NE_01	UP	1 OK		RB_COM_SE_01	UP	1 OK	
				PTP_IGE_SE_01	UP	1 OK		RB_COM_SO_02	UP	1 OK	
				PTP_IGL_NO_01	UP	1 OK		RB_CRL_SE_01	UP	1 OK	
				PTP_IGL_NO_02	UP	1 OK		RB_CRL_SO_01	UP	1 OK	
				PTP_PUN_NE_01	UP	1 OK		RB_CRL_SS_01	UP	1 OK	
				PTP_RAY_SE_01	UP	1 OK		RB_ESP_SO_01	UP	1 OK	
				PTP_SHL_NE_01	UP	1 OK		RB_ESP_SS_01	UP	1 OK	
				PTP_SHL_NO_01	UP	1 OK		RB_GAL_NE_01	UP	1 OK	
				PTP_SHL_NO_02	UP	1 OK		RB_GAL_SE_01	UP	1 OK	
				PTP_SHL_NO_03	UP	1 OK		RB_GLL_EE_01	UP	1 OK	
				PTP_TAN_OO_01	UP	1 OK		RB_GLL_SE_01	UP	1 OK	

**Ilustración 49-4:** Lista Hostgroup 2 generada en la infraestructura de red.

Realizado por: Sagnay, Mauro, 2022.

OLT Fibra (OLT)				Enlaces Punto a Punto (PTP)				Radio Bases (RB)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
OLT_CHA_01	UP	1 OK		CPE_NIN_01	DOWN	1 CRITICAL		RB_CEB_NO_01	UP	1 OK	
OLT_CHA_01b	UP	1 OK		PTP_COM_SE_01	UP	1 OK		RB_CEB_SO_01	UP	1 OK	
OLT_ESP_01	UP	1 OK		PTP_COM_SO_01	UP	1 OK		RB_CHA_NO_01	UP	1 OK	
OLT_GMT_01	UP	1 OK		PTP_CRL_NO_01	UP	1 OK		RB_CHA_NO_02	UP	1 OK	
OLT_GUA_01	UP	1 OK		PTP_CRL_OO_01	UP	1 OK		RB_CHA_OO_01	UP	1 OK	
OLT_IGL2_01	UP	1 OK		PTP_CRL_SS_01	UP	1 OK		RB_CHA_OO_02	UP	1 OK	
OLT_SMT1	UP	1 OK		PTP_ESP_SE_01	UP	1 OK		RB_CHA_OO_03	UP	1 OK	
OLT_SMT2	UP	1 OK		PTP_GAL_EE_01	UP	1 OK		RB_CHA_OO_04	UP	1 OK	
OLT_TAN1	UP	1 OK		PTP_GLL_SE_01	UP	1 OK		RB_CHA_OO_05	UP	1 OK	
				PTP_H2O_NE_03	UP	1 OK		RB_CHA_SE_01	UP	1 OK	
				PTP_H2O_NE_04	UP	1 OK		RB_CHA_SO_01	UP	1 OK	
				PTP_H2O_NE_05	UP	1 OK		RB_CHA_SO_02	UP	1 OK	
				PTP_IGE_NE_01	UP	1 OK		RB_COM_SE_01	UP	1 OK	
				PTP_IGE_SE_01	UP	1 OK		RB_COM_SO_02	UP	1 OK	
				PTP_IGL_NO_01	UP	1 OK		RB_CRL_SE_01	UP	1 OK	
				PTP_IGL_NO_02	UP	1 OK		RB_CRL_SO_01	UP	1 OK	
				PTP_PUN_NE_01	UP	1 OK		RB_CRL_SS_01	UP	1 OK	
				PTP_RAY_SE_01	UP	1 OK		RB_ESP_SO_01	UP	1 OK	
				PTP_SHL_NE_01	UP	1 OK		RB_ESP_SS_01	UP	1 OK	
				PTP_SHL_NO_01	UP	1 OK		RB_GAL_NE_01	UP	1 OK	
				PTP_SHL_NO_02	UP	1 OK		RB_GAL_SE_01	UP	1 OK	
				PTP_SHL_NO_03	UP	1 OK		RB_GLL_EE_01	UP	1 OK	
				PTP_TAN_OO_01	UP	1 OK		RB_GLL_SE_01	UP	1 OK	

**Ilustración 50-4:** Lista Hostgroup 3 generada en la infraestructura de red.

Realizada por: Sagnay, Mauro, 2022

Host	Status	Services	Actions
PBX	UP	6 OK 1 WARNING 1 CRITICAL	
RADIUS	UP	6 OK 1 WARNING 1 CRITICAL	
WEB	UP	7 OK 1 WARNING	
pruebas_server	DOWN	4 OK 1 WARNING 3 CRITICAL	

Routers Core (routerC)				Routers Salida Internacional (routerINT)				Routers Concentradores (routerT)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
AUX-OLT-ESPOCH	UP	1 OK 1 UNKNOWN		PUBLICA-UFINET	UP	No matching services		CHA_CHAMBO_02	UP	1 OK	
GUA_GMT_01	UP	2 OK		Router-Puntonet	UP	No matching services		GMT_GAL_01	UP	1 OK	
RIO-ESP-01	UP	2 OK						RIO_CEBADAS_01	UP	1 OK	
RIO_BORDER_01	UP	2 OK						RIO_COMIL_01	UP	1 OK	
RIO_CORE_01	UP	1 OK 1 UNKNOWN						RIO_CORONA_01	UP	1 OK	
RIO_DMZ_01	UP	1 OK 1 CRITICAL						RIO_GUARGUALLA_01	UP	1 OK	
RIO_GUASLAN_01	UP	1 OK 1 CRITICAL						RIO_H20_01	UP	1 OK	
SW-ESP-02-TRONGAL	UP	1 OK 1 CRITICAL						RIO_IGLESIA2_01	UP	1 OK	
								RIO_IGLESIA_01	UP	1 OK	
								RIO_NAUBUG_01	UP	1 OK	
								RIO_PUÑINQUIL_01	UP	1 OK	
								RIO_RAYOLOMA_01	UP	1 OK	
								RIO_SHL_01	UP	1 OK	
								RIO_TANQUE_01	UP	1 OK	
								RIO_TULABUG_01	UP	1 OK	
								SAN MARTIN_01	UP	1 OK	

**Ilustración 51-4:** Lista Hostgroup 4 generada en la infraestructura de red.

**Realizada por:** Sagnay, Mauro, 2022.

También brinda la posibilidad de obtener una lista completa de todos los hosts dados de alta en Nagios, en donde nos brinda un resumen rápido del estado del equipo, como se aprecia a continuación.

Current Network Status		Host Status Totals				Service Status Totals				
Last Updated: Fri Oct 21 12:24:32 -05 2022 Updated every 90 seconds Nagios® Core™ 4.4.6 - www.nagios.org Logged in as nagiosadmin		Up	Down	Unreachable	Pending	OK	Warning	Unknown	Critical	Pending
		183	4	0	0	243	12	2	19	0
		All Problems		All Types		All Problems		All Types		
		4		187		33		276		
<b>Host Status Details For All Host Groups</b>										
Limit Results: <input type="text" value="100"/>		Results 0 - 100 of 187 Matching Hosts								
Host	Status	Last Check	Duration	Status Information						
AUX-OLT-ESPOCH	UP	10-21-2022 12:23:07	14d 8h 13m 24s	PING OK - Packet loss = 0%, RTA = 0.44 ms						
BH-CAL-CHA	UP	10-21-2022 12:24:04	6d 19h 10m 52s	PING OK - Packet loss = 0%, RTA = 25.99 ms						
BH-CEB-GAL	UP	10-21-2022 12:23:51	0d 4h 24m 41s	PING OK - Packet loss = 0%, RTA = 26.06 ms						
BH-CEB-NAU	UP	10-21-2022 12:23:17	0d 4h 25m 15s	PING OK - Packet loss = 0%, RTA = 19.70 ms						
BH-CEB-RAY	UP	10-21-2022 12:23:16	0d 4h 25m 16s	PING OK - Packet loss = 16%, RTA = 21.76 ms						
BH-CHA-CAL	UP	10-21-2022 12:24:00	6d 19h 10m 52s	PING OK - Packet loss = 0%, RTA = 22.31 ms						
BH-CHA2-GUA	UP	10-21-2022 12:24:01	6d 19h 10m 52s	PING OK - Packet loss = 0%, RTA = 23.19 ms						
BH-COM-IGL	UP	10-21-2022 12:22:33	13d 0h 16m 27s	PING OK - Packet loss = 0%, RTA = 2.98 ms						
BH-CRL-IGL	UP	10-21-2022 12:23:04	13d 0h 16m 27s	PING OK - Packet loss = 0%, RTA = 4.91 ms						
BH-ESP-H2O	UP	10-21-2022 12:22:56	7d 2h 55m 36s	PING OK - Packet loss = 0%, RTA = 0.83 ms						
BH-ESP-SHL	UP	10-21-2022 12:23:07	7d 20h 4m 24s	PING OK - Packet loss = 0%, RTA = 0.47 ms						
BH-GAL_CEB	UP	10-21-2022 12:23:41	0d 4h 24m 51s	PING OK - Packet loss = 0%, RTA = 26.52 ms						
BH-GLL-NIN	UP	10-21-2022 12:21:36	1d 1h 25m 47s	PING OK - Packet loss = 0%, RTA = 26.06 ms						
BH-GLL-RAY	UP	10-21-2022 12:21:35	1d 1h 25m 51s	PING OK - Packet loss = 0%, RTA = 19.61 ms						
BH-GMT-NAU	UP	10-21-2022 12:23:52	14d 8h 13m 37s	PING OK - Packet loss = 0%, RTA = 1.64 ms						
BH-GUA-CHA2	UP	10-21-2022 12:24:00	6d 19h 10m 56s	PING OK - Packet loss = 0%, RTA = 31.45 ms						
BH-H2O-ESP	UP	10-21-2022 12:23:34	6d 2h 49m 5s	PING OK - Packet loss = 0%, RTA = 6.36 ms						
BH-IGL-COM	UP	10-21-2022 12:23:08	13d 0h 16m 27s	PING OK - Packet loss = 0%, RTA = 0.65 ms						
BH-IGL-CRL	UP	10-21-2022 12:23:09	13d 0h 16m 26s	PING OK - Packet loss = 0%, RTA = 0.59 ms						

**Ilustración 52-4:** Lista de Hosts dados de Alta.

**Realizado por:** Sagnay, Mauro, 2022

También se puede apreciar en detalle el estatus de todos los servicios de los hosts correspondientes.

**Current Network Status**  
 Last Updated: Fri Oct 21 12:25:05 -05 2022  
 Updated every 30 seconds  
 Nagios® Core™ 4.4.6 - www.nagios.org  
 Logged in as nagiosadmin

View History For all hosts  
 View Notifications For All Hosts  
 View Host Status Detail For All Hosts

Host Status Totals				Service Status Totals				
Up	Down	Unreachable	Pending	Ok	Warning	Unknown	Critical	Pending
183	4	0	0	244	12	2	18	0
All Problems: 4, All Types: 187				All Problems: 32, All Types: 276				

**Service Status Details For All Hosts**

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
AUX-OLT-ESPOCH	Memoria Usada	UNKNOWN	10-21-2022 12:24:57	14d 8h 14m 9s	3/3	External command error: Error in packet
	PING	OK	10-21-2022 12:24:56	14d 8h 14m 1s	1/3	PING OK - Packet loss = 0%, RTA = 0.40 ms
BH-CAL-CHA	PING	OK	10-21-2022 12:24:56	0d 1h 27m 1s	1/3	PING OK - Packet loss = 0%, RTA = 29.31 ms
BH-CEB-GAL	PING	OK	10-21-2022 12:24:52	0d 4h 25m 18s	1/3	PING OK - Packet loss = 0%, RTA = 24.64 ms
BH-CEB-NAU	PING	OK	10-21-2022 12:24:54	0d 4h 25m 52s	1/3	PING OK - Packet loss = 0%, RTA = 19.97 ms
BH-CEB-RAY	PING	OK	10-21-2022 12:24:52	0d 4h 25m 53s	1/3	PING OK - Packet loss = 0%, RTA = 24.02 ms
BH-CHA-CAL	PING	OK	10-21-2022 12:24:52	0d 1h 27m 5s	1/3	PING OK - Packet loss = 0%, RTA = 20.07 ms
BH-CHA2-GUA	PING	OK	10-21-2022 12:24:53	0d 1h 27m 4s	1/3	PING OK - Packet loss = 0%, RTA = 22.20 ms
BH-COM-IGL	PING	OK	10-21-2022 12:24:52	4d 15h 28m 29s	1/3	PING OK - Packet loss = 0%, RTA = 5.13 ms
BH-CRL-IGL	PING	OK	10-21-2022 12:24:55	13d 0h 17m 0s	1/3	PING OK - Packet loss = 0%, RTA = 4.82 ms
BH-ESP-H2O	PING	OK	10-21-2022 12:24:52	7d 2h 55m 58s	1/3	PING OK - Packet loss = 0%, RTA = 0.98 ms
BH-ESP-SHL	PING	OK	10-21-2022 12:24:56	7d 20h 4m 37s	1/3	PING OK - Packet loss = 0%, RTA = 0.49 ms
BH-GAL_CEB	PING	OK	10-21-2022 12:24:56	0d 4h 25m 19s	1/3	PING OK - Packet loss = 0%, RTA = 34.12 ms
BH-GLL-NIN	PING	OK	10-21-2022 12:24:57	0d 6h 35m 29s	1/3	PING OK - Packet loss = 0%, RTA = 25.69 ms
BH-GLL-RAY	PING	OK	10-21-2022 12:24:55	0d 6h 35m 30s	1/3	PING OK - Packet loss = 0%, RTA = 24.23 ms
BH-GMT-NAU	PING	OK	10-21-2022 12:24:55	1d 1h 57m 13s	1/3	PING OK - Packet loss = 0%, RTA = 1.72 ms
BH-GUA-CHA2	PING	OK	10-21-2022 12:24:56	0d 1h 27m 5s	1/3	PING OK - Packet loss = 0%, RTA = 30.25 ms

**Ilustración 53-4:** Lista de todos los servicios del host respectivo.

Realizado por: Sagnay, Mauro, 2022.

De una manera más resumida también se puede obtener una vista del estatus de todos los grupos de hosts.

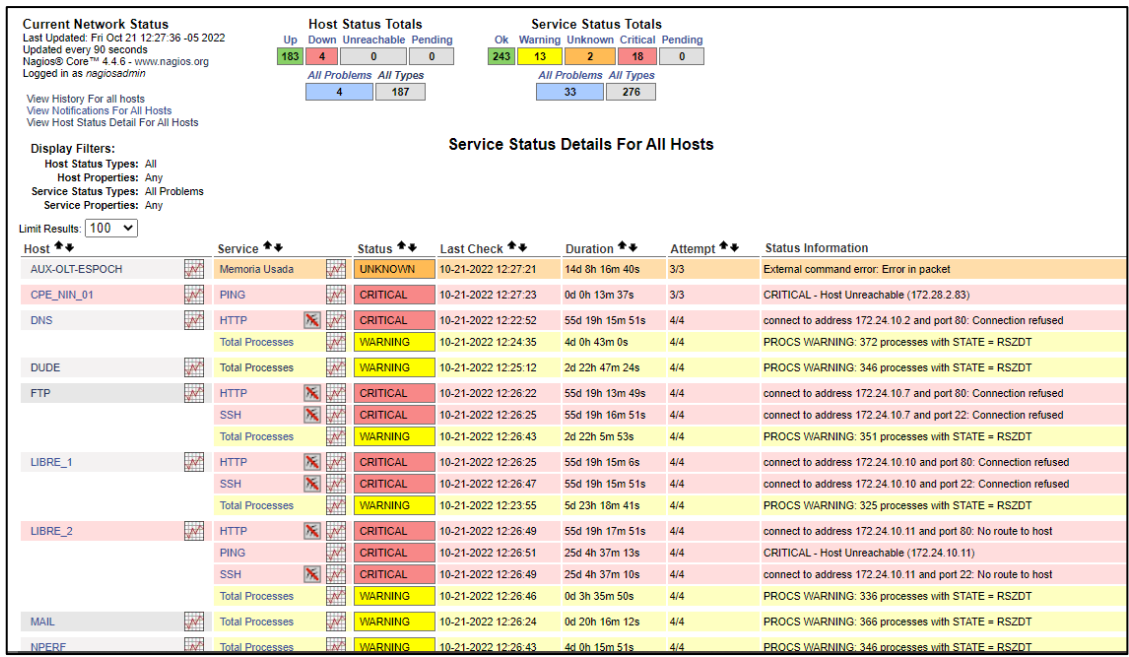
**Status Summary For All Host Groups**

Host Group	Host Status Summary	Service Status Summary
Control de Energia (CE)	16 UP	16 OK
Enlaces Backhaul (EBH)	32 UP	32 OK
Enlaces Fibra Optica (EFO)	6 UP	6 OK
OLT Fibra (OLT)	9 UP	9 OK
Enlaces Punto a Punto (PTP)	26 UP 1 DOWN : 1 Unhandled	26 OK 1 CRITICAL : 1 on Problem Hosts
Radio Bases (RB)	57 UP 1 DOWN : 1 Unhandled	56 OK 2 CRITICAL : 1 Unhandled 1 on Problem Hosts
Switches (SW)	1 UP	1 OK 1 CRITICAL : 1 Unhandled
Servidores Core (ServerC)	9 UP 2 DOWN : 2 Unhandled	84 OK 11 WARNING : 9 Unhandled 2 on Problem Hosts 13 CRITICAL : 7 Unhandled 6 on Problem Hosts
Servidor NAGIOS (linux-servers)	1 UP	7 OK 1 WARNING : 1 Unhandled
Routers Core (routerC)	8 UP	11 OK 2 UNKNOWN : 2 Unhandled 3 CRITICAL : 3 Unhandled
Routers Salida Internacional (routerINT)	2 UP	No matching services
Routers Concentradores (routerT)	16 UP	16 OK

**Ilustración 54-4:** Vista resumida del estatus de todos los hostgrups

Realizado por: Sagnay, Mauro, 2022.

También se muestra un resumen de los servicios de todos los hosts.

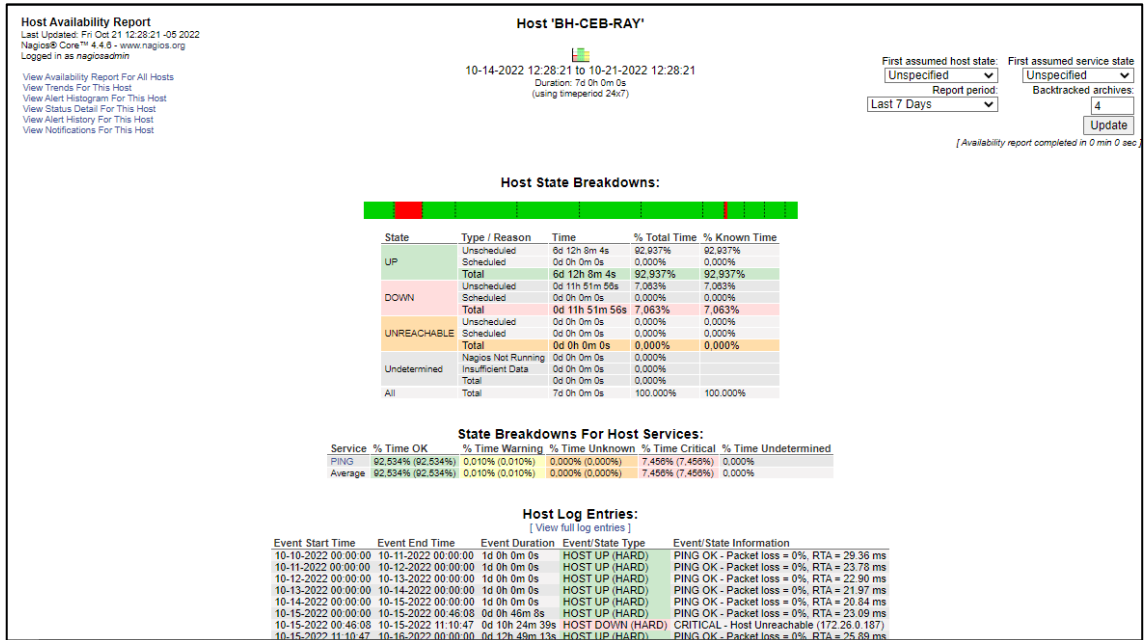


**Ilustración 55-4:** Resumen del estatus de los servicios de todos.

Realizado por: Sagñay, Mauro, 2022.

**4.8.2. Obtención de Reportes**

El software Nagios Core, también tiene la capacidad de general reportes de disponibilidad, como se aprecia en las siguientes capturas.

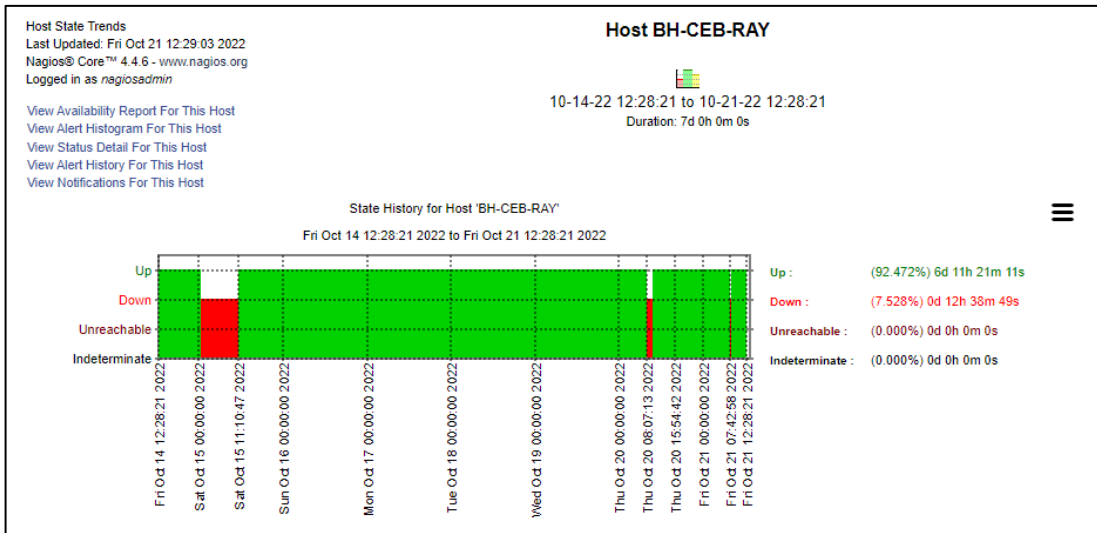


**Ilustración 56-4:** Reporte de disponibilidad del host BH-CEB-RAY por 7 días.

Realizado por: Sagñay, Mauro, 2022.

Para fines de muestra de funcionamiento, se ha escogido al azar a un host para extraer el reporte de disponibilidad por 7 días, del 14 al 21 de octubre de 2022, el resultado se muestra en la captura

anterior. En el resultado se aprecia una gráfica, el detalle del status del equipo a lo largo de tiempo de muestra, además de la afectación de los servicios de este host y, por último, el log de ese equipo en el periodo establecido.



**Ilustración 57-4:** Tendencia del status del host en el periodo de 7 días.

**Realizado por:** Sagñay, Mauro, 2022.

También se muestra la tendencia del estado que ha tenido el host en el periodo establecido, como se muestra en la ilustración, se detalla muy bien el tiempo que el host se ha mantenido en un estado específico.

#### 4.8.3. Generación de Alertas

Nagios Core almacena todas las alertas generadas ya sea por un host o por un servicio, de esta manera el operador puede consultar todos los problemas que hayan ocurrido y ubicarlos de manera cronológica como se muestra a continuación.

**Alert History**  
 Last Updated: Fri Oct 21 12:30:20 -05 2022  
 Nagios® Core™ 4.4.6 - www.nagios.org  
 Logged in as nagiosadmin

View Status Detail For All Hosts  
 View Notifications For All Hosts

**All Hosts and Services**

Latest Archive ← Log File Navigation  
 Fri Oct 21 00:00:00 -05 2022  
 to Present.

File: /usr/local/nagios/var/nagios.log

State type options:  
 ▾

History detail level for all hosts:  
 ▾

Hide Flapping Alerts  
 Hide Downtime Alerts  
 Hide Process Messages  
 Older Entries First

---

octubre 21, 2022 12:00

110-21-2022 12:30:01] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:SOFT:2:PING WARNING - Packet loss = 0%, RTA = 577.06 ms
110-21-2022 12:28:57] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:SOFT:1:PING WARNING - Packet loss = 0%, RTA = 289.33 ms
110-21-2022 12:28:41] SERVICE ALERT RB_ESP_SO_01:PING:OK:HARD:3:PING OK - Packet loss = 0%, RTA = 133.37 ms
110-21-2022 12:28:13] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:HARD:3:PING WARNING - Packet loss = 0%, RTA = 504.40 ms
110-21-2022 12:27:09] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:SOFT:2:PING WARNING - Packet loss = 0%, RTA = 247.51 ms
110-21-2022 12:26:05] SERVICE ALERT RB_ESP_SO_01:PING:CRITICAL:SOFT:1:PING CRITICAL - Packet loss = 0%, RTA = 740.98 ms
110-21-2022 12:24:54] SERVICE ALERT RB_ESP_SO_01:PING:OK:SOFT:2:PING OK - Packet loss = 0%, RTA = 121.29 ms
110-21-2022 12:23:50] SERVICE ALERT RB_ESP_SO_01:PING:CRITICAL:SOFT:1:PING CRITICAL - Packet loss = 0%, RTA = 777.02 ms
110-21-2022 12:23:39] SERVICE ALERT RB_ESP_SO_01:PING:OK:HARD:3:PING OK - Packet loss = 0%, RTA = 139.12 ms
110-21-2022 12:23:29] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:HARD:3:PING WARNING - Packet loss = 0%, RTA = 324.71 ms
110-21-2022 12:22:49] HOST ALERT CPE_NIN_01:DOWN:HARD:10:CRITICAL - Host Unreachable (172.28.2.83)
110-21-2022 12:22:36] HOST ALERT RB_NIN_01:DOWN:HARD:10:CRITICAL - Host Unreachable (172.28.2.84)
110-21-2022 12:22:25] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:SOFT:2:PING WARNING - Packet loss = 0%, RTA = 332.42 ms
110-21-2022 12:22:10] SERVICE ALERT RB_SHL_NE_03:PING:OK:SOFT:2:PING OK - Packet loss = 0%, RTA = 150.49 ms
110-21-2022 12:21:46] HOST ALERT CPE_NIN_01:DOWN:SOFT:9:CRITICAL - Host Unreachable (172.28.2.83)
110-21-2022 12:21:36] HOST ALERT RB_NIN_01:DOWN:SOFT:9:CRITICAL - Host Unreachable (172.28.2.84)
110-21-2022 12:21:21] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:SOFT:1:PING WARNING - Packet loss = 0%, RTA = 390.24 ms
110-21-2022 12:21:06] SERVICE ALERT RB_SHL_NE_03:PING:WARNING:SOFT:1:PING WARNING - Packet loss = 0%, RTA = 202.43 ms
110-21-2022 12:20:46] HOST ALERT CPE_NIN_01:DOWN:SOFT:8:CRITICAL - Host Unreachable (172.28.2.83)
110-21-2022 12:20:33] HOST ALERT RB_NIN_01:DOWN:SOFT:8:CRITICAL - Host Unreachable (172.28.2.84)
110-21-2022 12:20:17] SERVICE ALERT RB_ESP_SO_01:PING:OK:SOFT:3:PING OK - Packet loss = 0%, RTA = 2.15 ms
110-21-2022 12:19:43] HOST ALERT CPE_NIN_01:DOWN:SOFT:7:CRITICAL - Host Unreachable (172.28.2.83)
110-21-2022 12:19:31] HOST ALERT RB_NIN_01:DOWN:SOFT:7:CRITICAL - Host Unreachable (172.28.2.84)
110-21-2022 12:19:13] SERVICE ALERT RB_ESP_SO_01:PING:WARNING:SOFT:2:PING WARNING - Packet loss = 0%, RTA = 501.67 ms
110-21-2022 12:18:40] HOST ALERT CPE_NIN_01:DOWN:SOFT:6:CRITICAL - Host Unreachable (172.28.2.83)

**Ilustración 58-4:** Generación y almacenamiento de todas las alertas ocurridas en el host y servicios.

Realizado por: Sagñay, Mauro, 2022.

Para ubicar más rápido una alerta ocurrida, se procede a filtrarlas utilizando el siguiente menú que proporciona Nagios Core.

**Alert Summary Report**  
 Last Updated: Fri Oct 21 12:30:57 -05 2022  
 Nagios® Core™ 4.4.6 - www.nagios.org  
 Logged in as nagiosadmin

**Standard Reports:**

Report Type:  ▾

**Custom Report Options:**

Report Type:  ▾

Report Period:  ▾

If Custom Report Period..

Start Date (Inclusive):  ▾

End Date (Inclusive):  ▾

Limit To Hostgroup:  ▾

Limit To Servicegroup:  ▾

Limit To Host:  ▾

Alert Types:  ▾

State Types:  ▾

Host States:  ▾

Service States:  ▾

Max List Items:

**Ilustración 59-4:** Lista de opciones para obtener un reporte de las Alertas ocurridas.

Realizado por: Sagñay, Mauro, 2022.

De igual manera se procede a la obtención de un reporte de alertas por un periodo de 7 días, del 14 al 21 de octubre de 2022.



Alert Summary Report		Most Recent Alerts				Report Options Summary:	
Last Updated: Fri Oct 21 12:31:27 -05 2022		10-21-2022 12:31:27 to 10-21-2022 12:31:27				Alert Types: Host & Service Alerts	
Nagios® Core™ 4.4.6 - www.nagios.org		Duration: 7d 0h 0m 0s				State Types: Hard States	
Logged in as nagiosadmin						Host States: Up, Down, Unreachable	
						Service States: Ok, Warning, Unknown, Critical	
						<a href="#">Generate New Report</a>	
Displaying most recent 25 of 1471 total matching alerts							
Time	Alert Type	Host	Service	State	State Type	Information	
10-21-2022 12:31:23	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 472.12 ms	
10-21-2022 12:31:06	Service Alert	RB_ESP_SO_01	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 0%, RTA = 737.86 ms	
10-21-2022 12:28:41	Service Alert	RB_ESP_SO_01	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 133.37 ms	
10-21-2022 12:28:13	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 504.40 ms	
10-21-2022 12:23:39	Service Alert	RB_ESP_SO_01	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 139.12 ms	
10-21-2022 12:23:29	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 324.71 ms	
10-21-2022 12:22:49	Host Alert	CPE_NIN_01	N/A	DOWN	HARD	CRITICAL - Host Unreachable (172.28.2.83)	
10-21-2022 12:22:36	Host Alert	RB_NIN_01	N/A	DOWN	HARD	CRITICAL - Host Unreachable (172.28.2.84)	
10-21-2022 12:15:13	Service Alert	RB_ESP_SO_01	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 8.73 ms	
10-21-2022 12:15:03	Service Alert	RB_ESP_SO_01	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 16%, RTA = 619.87 ms	
10-21-2022 12:14:46	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 452.77 ms	
10-21-2022 12:14:02	Service Alert	CPE_NIN_01	PING	CRITICAL	HARD	CRITICAL - Host Unreachable (172.28.2.83)	
10-21-2022 12:14:00	Service Alert	RB_NIN_01	PING	CRITICAL	HARD	CRITICAL - Host Unreachable (172.28.2.84)	
10-21-2022 12:12:26	Service Alert	RB_ESP_SO_01	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 132.85 ms	
10-21-2022 12:12:16	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 281.10 ms	
10-21-2022 12:12:05	Service Alert	RB_ESP_SO_01	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 0%, RTA = 689.16 ms	
10-21-2022 12:09:45	Service Alert	RB_ESP_SO_01	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 123.06 ms	
10-21-2022 12:09:29	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 378.19 ms	
10-21-2022 12:07:11	Service Alert	RB_ESP_SO_01	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 110.85 ms	
10-21-2022 12:07:01	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 209.61 ms	
10-21-2022 12:06:44	Service Alert	RB_ESP_SO_01	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 0%, RTA = 683.25 ms	
10-21-2022 12:06:09	Service Alert	RB_ESP_SO_01	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 327.24 ms	
10-21-2022 12:05:59	Service Alert	RB_ESP_SO_01	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 0%, RTA = 635.23 ms	
10-21-2022 11:58:18	Service Alert	RB_ESP_SO_01	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 80.11 ms	
10-21-2022 11:58:02	Service Alert	RB_ESP_SO_01	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 0%, RTA = 645.94 ms	

**Ilustración 60-4:** Reporte de la Alertas generadas en el periodo de 7 días.

Realizado por: Sagnay, Mauro, 2022.

#### 4.8.4. Generación de Notificaciones

Cuando una alerta es generada, ya sea por un problema en un host o servicio o por algún otro evento, se debe notificar de este a los contactos respectivos, Nagios Core también incluye un reporte de las notificaciones enviadas, como se muestra en la siguiente ilustración.

Contact Notifications		All Contacts				Notification detail level for all contacts:	
Last Updated: Fri Oct 21 12:32:32 -05 2022		Log File Navigation				All notifications	
Nagios® Core™ 4.4.6 - www.nagios.org		Fri Oct 21 00:00:00 -05 2022				Older Entries First	
Logged in as nagiosadmin		to Present.				<input type="checkbox"/> <a href="#">Update</a>	
		File: /usr/local/nagios/var/nagios.log					
Host	Service	Type	Time	Contact	Notification Command	Information	
RIO_GUASLAN_01	Memoria Usada	CRITICAL	10-21-2022 12:30:53	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
CPE_NIN_01	N/A	HOST DOWN	10-21-2022 12:22:49	telegram-contact	notify-host-by-telegram	CRITICAL - Host Unreachable (172.28.2.83)	
RB_NIN_01	N/A	HOST DOWN	10-21-2022 12:22:36	telegram-contact	notify-host-by-telegram	CRITICAL - Host Unreachable (172.28.2.84)	
RIO_DMZ_01	Memoria Usada	CRITICAL	10-21-2022 11:48:19	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
SVW-ESP-02-TRONCAL	Memoria Usada	CRITICAL	10-21-2022 11:39:53	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
RIO_GUASLAN_01	Memoria Usada	CRITICAL	10-21-2022 11:01:46	telegram-contact	notify-host-by-telegram	CRITICAL - Host Unreachable (172.24.10.11)	
LIBRE_2	N/A	HOST DOWN	10-21-2022 11:01:25	telegram-contact	notify-host-by-telegram	CRITICAL - Host Unreachable (172.24.10.11)	
pruebas_server	N/A	HOST DOWN	10-21-2022 11:01:25	telegram-contact	notify-host-by-telegram	CRITICAL - Host Unreachable (172.24.10.4)	
RIO_DMZ_01	Memoria Usada	CRITICAL	10-21-2022 10:48:19	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
SVW-ESP-02-TRONCAL	Memoria Usada	CRITICAL	10-21-2022 10:48:18	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
RB_ESP_SO_01	PING	CRITICAL	10-21-2022 10:43:45	telegram-contact	notify-service-by-telegram	PING CRITICAL - Packet loss = 0%, RTA = 646.96 ms	
RIO_GUASLAN_01	Memoria Usada	CRITICAL	10-21-2022 10:30:53	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
RB_ESP_SO_01	PING	CRITICAL	10-21-2022 09:52:07	telegram-contact	notify-service-by-telegram	PING CRITICAL - Packet loss = 0%, RTA = 795.29 ms	
RIO_DMZ_01	Memoria Usada	CRITICAL	10-21-2022 09:48:19	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
SVW-ESP-02-TRONCAL	Memoria Usada	CRITICAL	10-21-2022 09:48:18	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
RIO_GUASLAN_01	Memoria Usada	CRITICAL	10-21-2022 09:30:53	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
LIBRE_2	N/A	HOST DOWN	10-21-2022 09:01:46	telegram-contact	notify-host-by-telegram	CRITICAL - Host Unreachable (172.24.10.11)	
pruebas_server	N/A	HOST DOWN	10-21-2022 09:01:25	telegram-contact	notify-host-by-telegram	CRITICAL - Host Unreachable (172.24.10.4)	
RIO_DMZ_01	Memoria Usada	CRITICAL	10-21-2022 08:48:19	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
SVW-ESP-02-TRONCAL	Memoria Usada	CRITICAL	10-21-2022 08:48:18	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
RIO_GUASLAN_01	Memoria Usada	CRITICAL	10-21-2022 08:30:53	telegram-contact	notify-service-by-telegram	CRITICAL - Plugin timed out while executing system call	
BH-CEB-GAL	N/A	HOST UP	10-21-2022 07:59:55	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 0%, RTA = 18.92 ms	
CE-CALPI	N/A	HOST UP	10-21-2022 07:59:51	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 54%, RTA = 25.45 ms	
GMT_GAL_01	N/A	HOST UP	10-21-2022 07:59:51	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 37%, RTA = 21.77 ms	
RB_GAL_SE_01	N/A	HOST UP	10-21-2022 07:59:51	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 37%, RTA = 27.80 ms	
RB_GAL_NE_01	N/A	HOST UP	10-21-2022 07:59:51	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 54%, RTA = 27.91 ms	
FTP_GAL_EE_01	N/A	HOST UP	10-21-2022 07:59:51	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 54%, RTA = 23.79 ms	
CE-GALTE	N/A	HOST UP	10-21-2022 07:59:51	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 28%, RTA = 27.40 ms	
CE-CEBADAS	N/A	HOST UP	10-21-2022 07:59:48	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 0%, RTA = 22.72 ms	
RIO_CEBADAS_01	N/A	HOST UP	10-21-2022 07:59:48	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 0%, RTA = 23.53 ms	
BH-GAL_CEB	N/A	HOST UP	10-21-2022 07:59:47	telegram-contact	notify-host-by-telegram	PING OK - Packet loss = 28%, RTA = 25.24 ms	

**Ilustración 61-4:** Reporte de las notificaciones enviadas.

Realizado por: Sagnay, Mauro, 2022.

Como se muestra en la ilustración, se aprecian detalles como como el nombre del host, el tiempo, el contacto, y el tipo de notificación, en este caso se realiza por mensaje a Telegram.

#### 4.8.5. Visualización de configuración de host

En la interfaz web de Nagios también se puede obtener una lista con la configuración con la que se ha dado de alta en el sistema a cada host, donde se aprecia los distintos atributos que se ha establecido para cada host.

**Configuration**  
 Last Updated: Fri Oct 21 12:34:57 -05 2022  
 Nagios® Core™ 4.4.6 - www.nagios.org  
 Logged in as nagiosadmin

Object Type:  
  
 Show Only:

Hosts															
Host Name	Alias/Description	Address	Importance (Host)	Importance (Host + Services)	Parent Hosts	Max. Check Attempts	Check Interval	Retry Interval	Host Check Command	Check Period	Obsess Over	Enable Active Checks	Enable Passive Checks	Check Freshness	Freshness Threshold
AUX-OLT-ESPOCH	AUX-OLT-ESPOCH	172.28.1.66	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-CAL-CHA	BH-CAL-GHA	172.28.0.131	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-CEB-GAL	BH-CEB-GAL	172.28.0.58	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-CEB-NAU	BH-CEB-NAU	172.28.0.115	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-CEB-RAY	BH-CEB-RAY	172.28.0.187	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-CHA-CAL	BH-GHA-CAL	172.28.0.130	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-CHA2-GUA	BH-CHA2-GUA	172.28.0.98	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-COM-IGL	BH-COM-IGL	172.28.0.11	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
BH-CRL-IGL	BH-CRL-IGL	172.28.0.83	0	0		10	0h 3m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value

**Ilustración 62-4:** Visualización de la configuración de todos los hosts.

Realizado por: Sagnay, Mauro, 2022.

## CONCLUSIONES

En este trabajo se implementó un sistema de gestión de red basado en el modelo FCAPS en la infraestructura de red de la empresa Intertec, mediante la utilización de la herramienta de monitoreo Nagios Core para obtener un control y evaluación del funcionamiento de la red.

Mediante el análisis desarrollado del modelo FCAPS, se pudo determinar las necesidades de gestión que presenta la infraestructura de red de la empresa, además de determinar diferentes parámetros de monitoreo para mejorar la calidad y disponibilidad del servicio de acceso a Internet entregado.

La selección del software de monitoreo Nagios Core se basó en un análisis de sus características frente a otras herramientas similares, donde mediante una tabla comparativa se evidenció un alto cumplimiento a los parámetros de monitoreo evaluados, además de ser una herramienta de software libre, lo que reduce los costos de implementación.

El servicio de acceso a Internet es monitoreado mediante las pruebas de diagnóstico realizadas a los equipos que conforman los nodos de la red, utilizando los protocolos ICMP y SNMP, de esta forma es posible detectar fallas que puedan disminuir la calidad o disponibilidad del servicio.

Para cubrir con las 5 áreas funcionales del modelo FCAPS, se establecieron un conjunto de políticas de gestión de red, las cuales se utilizaron como una guía para la configuración, monitoreo, acceso y la manipulación segura de los equipos que conforman la red.

Las pruebas de funcionamiento del sistema de gestión de red se realizaron en cada área funcional del modelo FCAPS mediante la utilización de Nagios Core y otras herramientas para cumplir con las tareas de gestión que se establecieron en las políticas, de esta manera se pudo monitorear adecuadamente el servicio de acceso a Internet, detectando fallas o averías en los equipos de red.

Para evaluar el rendimiento del sistema de gestión de red que se ha implementado, se determinó el porcentaje de cumplimiento de las diferentes tareas de gestión descritas en las políticas, en donde 21 de 25 políticas se encuentran en el rango de 75 a 100% de cumplimiento, mientras que la única política con 0% que corresponde a la de Encriptación en Servidor de Correo, no se considera como un factor de riesgo para el monitoreo del servicio de acceso a Internet, pues el servidor de correo es utilizado solamente por el personal de la empresa, mas no por clientes.

## **RECOMENDACIONES**

Para ayudar a cubrir las necesidades de la empresa en cuanto a seguridad se recomienda implementar un IPS o herramientas con funciones similares para evitar la interrupción del servicio debido a posibles ataques.

El software Nagios Core presenta limitación en cuanto a la falta de autodescubrimiento de equipos que se conecten a la red, esto puede cambiar debido a el desarrollo de complementos realizados por la comunidad, por lo que se recomienda al personal encarga prestar atención a las actualizaciones más recientes de este aspecto.

Para establecer un nivel de protección a los datos sensibles almacenados en los servidores de la empresa, es necesario implementar encriptación a través de algoritmos AES o más robustos para evitar comprometer la información sensible de la empresa en caso de un ataque.

## BIBLIOGRAFÍA

- AGUAIZA TENELEMA, D.G.** Propuesta de rediseño de la infraestructura de red de la Universidad Laica “Eloy Alfaro” de Manabí, para ofrecer un modelo de servicios con Calidad de Servicio (QoS). [En línea] (Trabajo de Titulación) (Maestría) Pontificia Universidad Católica del Ecuador, Facultad de Ingeniería. Quito – Ecuador, 2016. pp. 19 – 38. [Consulta: 8 de mayo 2022]. Disponible en: [http://repositorio.puce.edu.ec/bitstream/handle/22000/12638/TESIS\\_DANNY\\_AGUAIZA.pdf?sequence=1&isAllowed=y](http://repositorio.puce.edu.ec/bitstream/handle/22000/12638/TESIS_DANNY_AGUAIZA.pdf?sequence=1&isAllowed=y)
- AYALA YANDÚN, V.E.** Modelo de gestión de red funcional en la red local de datos del Gobierno Autónomo Descentralizado de San Miguel de Ibarra basado en el estándar ISO. [En línea] (Trabajo de Titulación) (Tesis de Grado) Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas. Ibarra – Ecuador, 2015. pp. 16 – 26. [Consulta: 16 de mayo de 2022]. Disponible en: <http://repositorio.utn.edu.ec/bitstream/123456789/4512/1/04%20RED%20060%20TESIS.pdf>
- BARRAGÁN PIÑA, A.J.** *Topologías* [blog]. [Consulta: 08 de mayo 2022]. Disponible en: <http://uhu.es/antonio.barragan/content/5topologias>
- GARRIDO AGUILAR, G.** Gestión de Desempeño de una Red ATM en Internet 2 utilizando la especificación MPLS. [En línea] (Trabajo de Titulación) (Maestría) Instituto Politécnico Nacional, Centro de Investigación y Desarrollo de Tecnología Digital. Tijuana – México, 2003. p: 24. [Consulta: 8 de mayo 2022]. Disponible en: [https://tesis.ipn.mx/bitstream/handle/123456789/638/247\\_2005\\_CITEDI\\_MAESTRIA\\_gerardo\\_garrido.pdf?sequence=1&isAllowed=y](https://tesis.ipn.mx/bitstream/handle/123456789/638/247_2005_CITEDI_MAESTRIA_gerardo_garrido.pdf?sequence=1&isAllowed=y)
- GUZMAN LÓPEZ, A.,** *Introducción a la Gestión de Redes* [blog]. [Consulta: 15 de mayo 2022]. Disponible en: <https://docplayer.es/9434597-1-introduccion-a-la-gestion-de-redes.html>
- INTRIAGO CEDEÑO, M.L.** Comparativa entre herramientas de monitoreo de red de computadoras aplicadas a la empresa Puerto Atún. [En línea] (Trabajo de Titulación) (Maestría) Escuela Superior Politécnica Agrícola de Manabí Manuel Félix López, Dirección de Posgrado y Formación Continua, Calceta – Ecuador. 2019. pp: 22-34. [Consulta: 12 de junio de 2022]. Disponible en: <https://repositorio.espam.edu.ec/bitstream/42000/1083/1/TTMTI13.pdf>
- LASSO, J., & PAUCAR, L.** Diseño de un ISP sobre ADSL para presentar el servicio de internet y servicios agregados de voz (VOIP) y datos, y estudio de factibilidad de implementación del ISP para la ciudad de Puerto Ayora en la Isla Santa Cruz (Galápagos) [En línea]. (Trabajo de Titulación) (Tesis de Grado) Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Quito – Ecuador. 2010. p: 38. [Consulta: 12 de mayo 2022]. Disponible en:

[https://www.researchgate.net/figure/Figura-31-Arquitectura-Final-del-ISP\\_fig3\\_45179269/download](https://www.researchgate.net/figure/Figura-31-Arquitectura-Final-del-ISP_fig3_45179269/download)

**LINARES, Álvaro M.; SANCHEZ, Parrales L.;& MARCILLO Parrales K.** " Implementación de los sistemas de gestión de la red en dos universidades americanas". *Revista Científica Sinapsis* [en línea], 2018, (Ecuador) 2(11), pp. 6-7- [Consulta: 04 diciembre 2022]. ISSN 1390 – 9770. Disponible en: <https://www.itsup.edu.ec/myjournal/index.php/sinapsis/article/view/125>

**MADRIL ACURIO, P.V.** Diseño e Implementación de un sistema de monitoreo de red y mensajes de alerta basado en la plataforma Nagios. [en línea]. (Trabajo de Titulación) (Tesis de Grado) Universidad de las Américas, Facultad de Ingeniería y Ciencias Agropecuarias, Quito – Ecuador, 2014. pp: 13 - 32. [Consulta: 6 de junio de 2022]. Disponible en: <https://dspace.udla.edu.ec/bitstream/33000/2659/8/UDLA-EC-TIRT-2014-10.pdf>

**MARTÍN MONTES, A.; & LEÓN DE MORA, C.** Arquitecturas inteligentes para la gestión de redes de comunicaciones [En línea]. Sevilla - España: Universidad de Sevilla, 2014 [Consulta: 4 mayo 2022]. Disponible en: <https://editorial.us.es/es/detalle-libro/719487/arquitecturas-inteligentes-para-la-gestion-de-redes-de-comunicaciones>.

**MARURI URÍÑA, E.S.; & VARGAS MAQUILON, J.A.** Implementación de un servidor de autoconfiguración y monitoreo para un ISP ubicado en el cantón Balzar. [En línea]. (Trabajo de Titulación) (Tesis de Grado). Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Físicas. Guayaquil - Ecuador, 2021. pp. 15 - 25. [Consulta: 04 mayo 2022] Disponible en: <http://repositorio.ug.edu.ec/bitstream/redug/56515/1/B-CINT-PTG-N.693%20Vargas%20Maquil%20Jonathan%20Aldahir%20.%20%20Maruri%20Uri%20Erick%20%20Steven%20.pdf>

**MEJÍA PÉREZ, E.D.** Implementación de una Herramienta de Monitoreo de la Red de Fibra Óptica Universitaria. [En línea] (Trabajo de Titulación) (Tesis de grado) Universidad Autónoma del Estado de Hidalgo, Instituto de Ciencias Básica e Ingeniería, Área Académica de Computación y Electrónica. Hidalgo - México, 2019. pp. 31 – 40. [Consulta: 5 de octubre de 2022]. Disponible en:

<http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/bitstream/handle/231104/2180/Implementaci%C3%B3n%20de%20una%20Herramienta%20de%20Monitoreo%20de%20la%20Red%20Universitaria..pdf?sequence=1&isAllowed=y>

**NAGIOS CORE** [blog]. [Consulta: 13 junio de 2022]. Disponible en: <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/config.html>

**PACHAR FIGUEROA, F.,** Diseño de la red para un Wireless internet service provider (WISP) para el cantón Yantzaza. [En línea] (Trabajo de Titulación) (Maestría) Universidad de Cuenca, Facultad de Ingeniería., Cuenca – Ecuador. 2010. pp. 17 -29. [Consulta: 12 de mayo 2022]. Disponible en: <https://dspace.ucuenca.edu.ec/bitstream/123456789/2534/1/tm4399.pdf>

**PADILLA BENÍTEZ, R.D.** Propuesta de modelo de gestión de infraestructura de red, basado en las mejores prácticas de gestión de TI y los modelos estándar de gestión de red – caso de estudio EP Petroecuador. [En línea] (Trabajo de Titulación) (Maestría) Escuela Politécnica Nacional, Facultad de Ingeniería de Sistemas. Quito-Ecuador, 2015. pp: 4-19. [Consulta: 8 de mayo de 2022]. Disponible en: <https://bibdigital.epn.edu.ec/bitstream/15000/15092/1/CD-6904.pdf>

**PRIETO ZAPARDIEL, J.** Diseño de una red de Acceso mediante Fibra Óptica. [En línea]. (Proyecto de Fin de Carrera) Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, Madrid – España. 2014. pp: 7 - 59. [Consulta: 13 de mayo 2022]. Disponible en: [https://oa.upm.es/33869/1/PFC\\_jaime\\_prieto\\_zapardiel.pdf](https://oa.upm.es/33869/1/PFC_jaime_prieto_zapardiel.pdf)

**SÁENZ DE VIGUERA, A.P. de L.** Infraestructura de un ISP. *Universidad Politécnica de Madrid* [En línea]. 2002. [Consulta: 6 mayo 2022]. Disponible en: <http://www.dit.upm.es/~david/tar/trabajos2002/10-Infraestructura-ISP-Andoni-Perez-res.pdf>.

**SILVA BRACERO, L.M.** Estudio y Análisis del estado actual de la implantación de IPv6 de los proveedores de servicios de internet a nivel nacional. [En línea] (Trabajo de Titulación) (Tesis de Grado) Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Quito – Ecuador, 2012. pp. 2 – 18 [Consulta: 07 de mayo 2022]. Disponible en: <http://bibdigital.epn.edu.ec/handle/15000/4549>

**SOLÍS ÁLVAREZ, C.J.** Implementación de NOC para el monitoreo de Servicios e Infraestructura de Redes para el Banco de Loja, Basado en Software Libre. [en línea]. (Trabajo de Titulación) (Tesis de Grado) Universidad Técnica Particular de Loja, Loja-Ecuador, 2014. p: 199 [Consulta: 06 de mayo 2022]. Disponible en: <https://dspace.utpl.edu.ec/handle/123456789/9187>.

**TERÁN ESCANTE, J.G.** Sistema de gestión de configuración para la infraestructura de networking de la empresa pública YACHAY E.P [en línea]. (Trabajo de Titulación) (Tesis de Grado) Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas, Ibarra – Ecuador, 2020. p: 11 - 20. [Consulta: 7 de mayo de 2022]. Disponible en: <http://repositorio.utn.edu.ec/bitstream/123456789/10294/2/04%20RED%20246%20TRABAJO%20GRADO.pdf>

**TERÁN MOREANO, R.E.** Implementación de un sistema de gestión de red de datos para la toma de decisiones de la empresa Clicknet S.A. [en línea]. (Trabajo de Titulación) (Maestría) Pontificia Universidad Católica del Ecuador, Oficina de Investigación y Postgrados, Ambato – Ecuador, 2017. pp: 16 - 20 [Consulta: 29 de abril 2022]. Disponible en: <https://repositorio.pucesa.edu.ec/bitstream/123456789/1979/1/76489.pdf>.

**WINS CP** [blog]. [Consulta 15 junio de 2022]. Disponible en: <https://winscp.net/eng/docs/lang:es>

**YACELGA CUSÍN, J.G.** Estudio de Factibilidad y diseño de una red inalámbrica ISP para proveer servicio de Internet en las comunidades de la cuenca del Lago San Pablo. [En línea]

(Trabajo de Titulación) (Maestría) Pontificia Universidad Católica del Ecuador, Facultad de Ingeniería, Quito – Ecuador. 2017. pp. 23 – 50. [Consulta: 11 de mayo 2022]. Disponible en: <http://repositorio.puce.edu.ec/bitstream/handle/22000/13691/TESIS%20DE%20INVESTIGACION%20DE%20UN%20ISP%20INALAMBRICO.pdf?sequence=1&isAllowed=y>

**ZAYAS, L., & SAO ÁVILES, A.** “Elementos conceptuales básicos útiles para comprender las redes de telecomunicación”. ACIMED [En línea], 2002, (Cuba), 10(6), pp. 5-6. [Consulta: 08 de mayo 2022]. ISSN 1024-9435. Disponible en: [http://scielo.sld.cu/scielo.php?script=sci\\_abstract&pid=S1024-94352002000600003](http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S1024-94352002000600003)



## ANEXOS

### ANEXO A:

Formato para el control y mantenimiento de actividades.

<b>DATOS GENERALES DEL MANTENIMIENTO</b>	
SOLICITANTE:	NOC
TITULO:	INSTALACIÓN DE UNA TORRE PARA LA REUBICACIÓN DE LAS ANTENAS Y EQUIPOS EN EL NODO TULABUG.
ANTECEDENTES:	
IMPACTO O DISTURBIOS:	Ninguna
NOMBRE DEL SITIO/ NODO:	TULABUG
FECHA y HORA DE INICIO DE LA ACTIVIDAD:	30 de septiembre de 2021, 11H00
FECHA y HORA DE FIN DE LA ACTIVIDAD:	30 de septiembre de 2021, 18H00
ABORTAR ACTIVIDAD:	Problemas Eléctricos, Defecto en Equipos, Falta de acceso, Falta de personal.
DATOS DEL SISTEMA:	Se trabajará con las siguientes bases RB_TUL_NN_01, RB_TUL_NN_02, el BH_TUL_CHA, BH_TUL_PUN y un punto a punto CPE_TUL_NN_01.
SINTESIS DE LA ACTIVIDAD:	<ul style="list-style-type: none"><li>- Preparación del terreno donde se instalará la torre.</li><li>- Ensamblado e instalación de la torre y soportes.</li><li>- Preparación del cableado para la reubicación de antenas y equipos.</li></ul>
REFERENCIAS:	
VALIDACIONES:	
REQUISITOS:	

### CONTACTOS Y ESCALAMIENTO

#### INFORMACION DEL PERSONAL DEL PROVEEDOR

Nombre	Puesto	Proveedor	Teléfono Celular	Correo Electrónico

#### INFORMACION DEL PERSONAL DE INTERTEC DE OPERACIÓN

Nombre	Puesto	Teléfono Celular	Correo Electrónico
Trabajador 1	Operador NOC	XXXXXX	XXX@XXX
Trabajador 2	Técnico	XXXXXX	XXXX@XXX

**INFORMACION DEL PERSONAL DE INTERTEC (INGENIERÍA-NETWORKING)**

<b>Nombre</b>	<b>Puesto</b>	<b>Teléfono Celular</b>	<b>Correo Electrónico</b>

**CONTACTOS ADICIONALES**

<b>Nombre</b>	<b>Puesto</b>	<b>Teléfono Celular</b>	<b>Correo Electrónico</b>

**AUTORIZACIONES**

<b>Elaboró / Modificó:</b>	<b>Revisó:</b>	<b>Autorizó:</b>

## ANEXO B:

### Manual de utilización de Nagios Core

#### Definición de un host para monitoreo dentro de Nagios Core

1. Se ingresa al servidor donde se encuentra alojado Nagios Core, y se ingresa las credenciales correspondientes para el usuario, el mismo que deberá tener permisos para editar estos archivos.
2. Se crea un nuevo archivo para ingresar el equipo y sus servicios a monitorear, en este caso, se crea el archivo de configuración *switch*, utilizando los siguientes comandos.

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

#nano /usr/local/nagios/etc/nagios.cfg
Se incluye la siguiente línea
Cfg_file = /usr/local/nagios/etc/objects/switch.cfg
```

3. Se configura la definición del host

```
define host {
use          generic-switch          ;
host_name   router_1                ;
alias       Router de Borde         ;
address     192.168.x.x              ;
hostgroups   allhosts,switches,xxx   ;
}
```

4. Definición de hostgroup

```
define hostgroup {
hostgroup_name      switches          ;
alias              Switches del Core ;
}
```

5. Definición de los servicios para el host

```
define service {

    use          generic-service          ;
    hostgroup_name      swithes          ;
    service_description  PING             ;
    check_command       check_ping!200.0,20%!600.0,60% ;
    check_interval      0.1              ;
    retry_interval      1                ;
}
```

**Nota:** Este proceso se repite para todos los dispositivos de la red que se desee monitorear mediante Nagios Core.

## Configuración de Contactos

1. Definición de contactos, se deberá editar el archivo `/usr/local/nagios/etc/objects/contacts.cfg`

```
define contact {  
  
    contact_name                XXX  
    alias                       XXX  
    service_notification_options w,c,r  
    service_notification_period 24x7  
    host_notification_period     24x7  
    service_notification_commands notify-service-by-telegram  
    host_notification_commands  notify-host-by-telegram  
    host_notification_options    d,r,u  
  
}
```

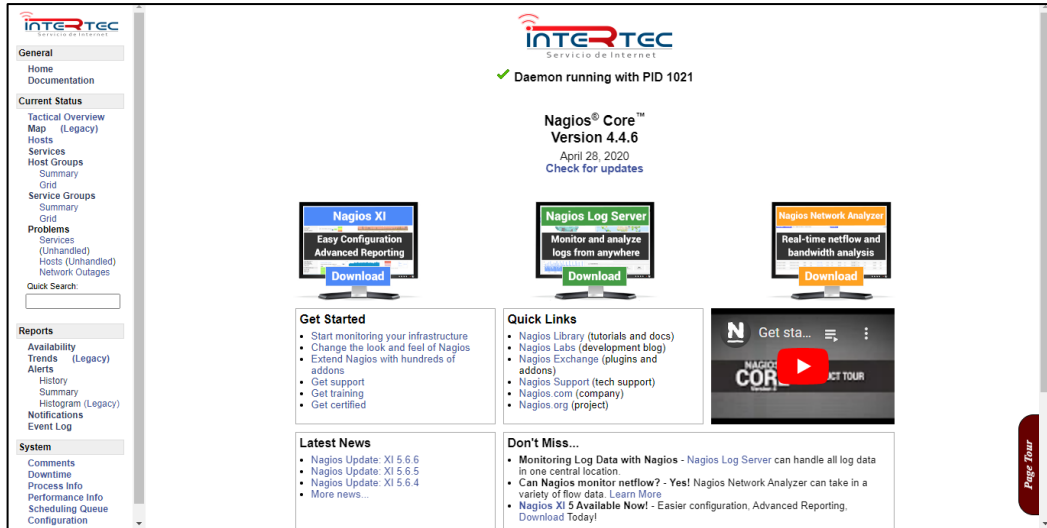
2. Se deberá establecer los comandos para el envío de notificaciones mediante Telegram, editando el archivo de comandos de la siguiente manera

```
# 'notify-host-by-telegram' command definition  
  
define command{  
    command_name    notify-host-by-telegram  
  
    command_line    /usr/bin/curl -X POST --data chat_id=#### --data text  
="***** Nagios *****%0A%0ANotification Type: $NOTIFICATIONTYPE$%0AHost  
: $HOSTNAME$%0AState: $HOSTSTATE$%0AAddress: $HOSTADDRESS$%0AInfo: $HO  
STOUTPUT$%0A%0ADate/Time:  
$LONGDATETIME$%0A" https://api.telegram.org/botTOKEN/sendMessage  
  
}  
  
# 'notify-service-by-telegram' command definition  
  
define command{  
    command_name    notify-service-by-telegram  
  
    command_line    /usr/bin/curl -X POST --data chat_id=##### --data tex  
t="***** Nagios *****%0A%0ANotification Type: $NOTIFICATIONTYPE$%0A%0A  
Service: $SERVICEDESC$%0AHost: $HOSTALIAS$%0AAddress: $HOSTADDRESS$%0A  
State: $SERVICESTATE$%0A%0ADate/Time: $LONGDATETIME$%0A%0AAdditional  
Info:%0A%0A$SERVICEOUTPUT$%0A" https://api.telegram.org/botTOKEN/sendM  
essage
```

TOKEN y ChatID se deben obtener del grupo de chat de Telegram creado previamente.

### Uso de la interfaz gráfica de Nagios Core.

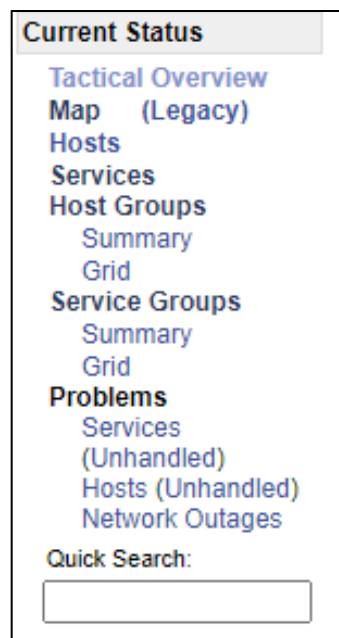
1. En la barra de dirección de un navegador, se ingresa la dirección IP del servidor seguido de `/nagios`, al dar enter se solicita las credenciales de acceso, se ingresan las mismas y se pulsa enter.



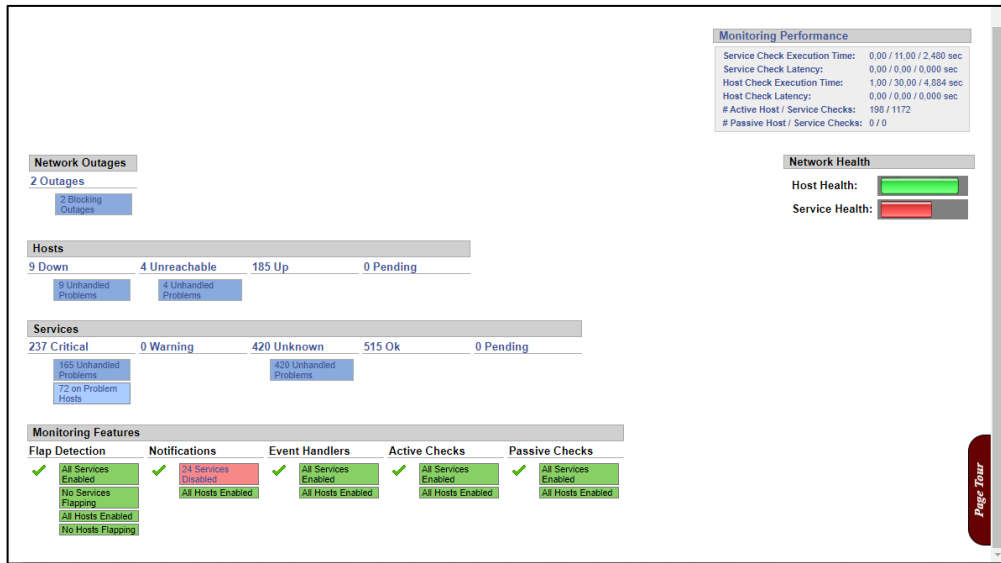
El obtener la pantalla de inicio de Nagios Core confirma el acceso correcto.

## 2. Visualizar los equipos y servicios monitoreados

Se debe hacer clic en cada una de las secciones que se desea visualizar.



1. **Tactical Overview:** se observa un resumen del monitoreo.



2. **Map:** presenta la topología de red de todos los dispositivos que se están monitoreado, también se puede visualizar los dispositivos activos e inactivos.

3. **Host:** se presenta una lista de todos los dispositivos / host monitoreados

Host Status Details For All Host Groups					
Host	Status	Last Check	Duration	Status Information	
AUX_OLT_SMT1	UP	02-22-2023 22:00:41	13d 17h 48m 22s	PING OK - Packet loss = 0%; RTA = 0.91 ms	
AUX_OLT_SMT2	UP	02-22-2023 22:00:21	13d 17h 48m 38s	PING OK - Packet loss = 0%; RTA = 0.61 ms	
BH-CAL-CHA	UP	02-22-2023 21:59:03	0d 4h 16m 57s	PING OK - Packet loss = 0%; RTA = 30.80 ms	
BH-CEB-GAL	UP	02-22-2023 22:00:32	3d 14h 26m 4s	PING OK - Packet loss = 0%; RTA = 38.79 ms	
BH-CEB-NAU	UP	02-22-2023 21:58:18	3d 14h 24m 58s	PING OK - Packet loss = 0%; RTA = 16.99 ms	
BH-CEB-RAY	UP	02-22-2023 22:00:32	3d 14h 26m 26s	PING OK - Packet loss = 0%; RTA = 32.04 ms	
BH-CHA-CAL	UP	02-22-2023 21:59:13	13d 17h 47m 56s	PING OK - Packet loss = 0%; RTA = 26.45 ms	
BH-CHA2-GUA	UP	02-22-2023 21:58:10	13d 17h 47m 56s	PING OK - Packet loss = 0%; RTA = 25.83 ms	
BH-COM-IGL	UNREACHABLE	02-22-2023 21:59:46	42d 3h 40m 39s	(Host check timed out after 30.33 seconds)	
BH-CRL-IGL	UP	02-22-2023 22:00:38	0d 7h 27m 22s	PING OK - Packet loss = 0%; RTA = 4.11 ms	
BH-ESP-H2O	UP	02-22-2023 22:00:21	13d 17h 48m 39s	PING OK - Packet loss = 0%; RTA = 1.08 ms	
BH-ESP-SHL	UP	02-22-2023 22:00:23	13d 17h 48m 39s	PING OK - Packet loss = 0%; RTA = 0.70 ms	
BH-GAL-CEB	UP	02-22-2023 22:00:30	3d 14h 25m 46s	PING OK - Packet loss = 0%; RTA = 36.70 ms	
BH-GLL-NIN	UP	02-22-2023 22:00:35	3d 14h 24m 16s	PING OK - Packet loss = 0%; RTA = 24.18 ms	
BH-GLL-RAY	UP	02-22-2023 21:58:23	11d 7h 7m 39s	PING OK - Packet loss = 0%; RTA = 21.17 ms	
BH-GMT-NAU	UP	02-22-2023 22:00:38	13d 17h 48m 21s	PING OK - Packet loss = 0%; RTA = 2.25 ms	
BH-GUA-CHA2	UP	02-22-2023 21:58:08	13d 17h 47m 56s	PING OK - Packet loss = 0%; RTA = 33.26 ms	
BH-H2O-ESP	UP	02-22-2023 22:00:03	13d 17h 48m 36s	PING OK - Packet loss = 0%; RTA = 9.31 ms	
BH-IGL-COM	DOWN	02-22-2023 21:57:23	13d 17h 54m 16s	(Host check timed out after 30.01 seconds)	
BH-IGL-CRL	UP	02-22-2023 21:59:15	0d 7h 28m 45s	PING OK - Packet loss = 0%; RTA = 0.78 ms	
BH-NAU-CEB	UP	02-22-2023 21:58:31	3d 14h 25m 45s	PING OK - Packet loss = 0%; RTA = 9.54 ms	

4. **Services:** se presenta una lista de todos los servicios monitoreados.

Display Filters:  
 Host Status Types: All  
 Host Properties: Any  
 Service Status Types: Ok  
 Service Properties: Any

Limit Results: 100

Results 0 - 100 of 514 Matching Services

Host	Service	Status	Last Check	Duration	Attempt	Status Information
AUX_OLT_SMT1	PING	OK	02-22-2023 22:03:03	13d 17h 50m 19s	1/3	PING OK - Packet loss = 0%, RTA = 1.09 ms
AUX_OLT_SMT2	PING	OK	02-22-2023 22:03:05	13d 17h 50m 22s	1/3	PING OK - Packet loss = 0%, RTA = 0.80 ms
BH-CAL-CHA	PING	OK	02-22-2023 22:03:02	0d 4h 19m 14s	1/3	PING OK - Packet loss = 0%, RTA = 26.01 ms
BH-CEB-GAL	PING	OK	02-22-2023 22:03:06	0d 0h 19m 41s	1/3	PING OK - Packet loss = 0%, RTA = 26.15 ms
	Ruido de Fondo	OK	02-22-2023 22:03:01	1d 10h 36m 4s	1/3	SNMP OK - -107 dBm
BH-CEB-NAU	PING	OK	02-22-2023 22:03:06	3d 1h 51m 55s	1/3	PING OK - Packet loss = 0%, RTA = 20.12 ms
BH-CEB-RAY	PING	OK	02-22-2023 22:03:05	0d 0h 19m 41s	1/3	PING OK - Packet loss = 0%, RTA = 22.81 ms
BH-CHA-CAL	PING	OK	02-22-2023 22:03:06	0d 23h 29m 59s	1/3	PING OK - Packet loss = 0%, RTA = 26.87 ms
BH-CHA2-GUA	PING	OK	02-22-2023 22:03:05	1d 3h 19m 2s	1/3	PING OK - Packet loss = 0%, RTA = 35.84 ms
BH-CRL-IGL	PING	OK	02-22-2023 22:03:07	0d 7h 29m 39s	1/3	PING OK - Packet loss = 0%, RTA = 5.86 ms
BH-FSP-H2O	PING	OK	02-22-2023 22:03:04	13d 17h 50m 21s	1/3	PING OK - Packet loss = 0%, RTA = 1.40 ms

5. **Hostgroup:** Se indica a todos los dispositivos agrupados

**Service Overview For All Host Groups**

Control de Energia (CE)				Enlaces Backhaul (EBH)			
Host	Status	Services	Actions	Host	Status	Services	Actions
CE-AGUA-SANTA	UP	1 OK		BH-CAL-CHA	UP	1 OK 6 UNKNOWN	
CE-CALPI	UP	1 OK		BH-CEB-GAL	UP	2 OK 5 UNKNOWN	
CE-CEBADAS	UP	1 OK		BH-CEB-NAU	UP	1 OK 6 UNKNOWN	
CE-CHAMBO 2	UP	1 OK		BH-CEB-RAY	UP	1 OK 6 UNKNOWN	
CE-COMIL	UNREACHABLE	1 CRITICAL		BH-CHA-CAL	UP	1 OK 6 UNKNOWN	
CE-CORONA-REAL	UP	1 OK		BH-CHA2-GUA	UP	1 OK 6 UNKNOWN	
				BH-COM-IGL	UNREACHABLE	7 CRITICAL	
				BH-CRL-IGL	UP	1 OK 6 UNKNOWN	

6. **Problems:** muestra una lista de equipos que se encuentran en estado crítico o de advertencia y una descripción del servicio que causa.

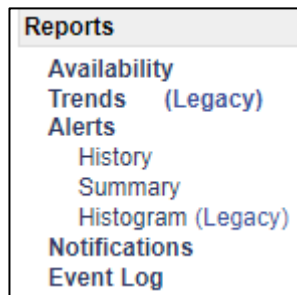
Display Filters:  
 Host Status Types: All problems  
 Host Properties: Any  
 Service Status Types: All  
 Service Properties: Any

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
BH-COM-IGL	UNREACHABLE	02-22-2023 22:11:46	42d 3h 52m 8s	(Host check timed out after 30.01 seconds)
BH-IGL-COM	DOWN	02-22-2023 22:09:23	13d 18h 5m 45s	(Host check timed out after 30.01 seconds)
CE-COMIL	UNREACHABLE	02-22-2023 22:11:13	23d 6h 32m 17s	(Host check timed out after 30.03 seconds)
LIBRE_1	DOWN	02-22-2023 22:11:55	20d 5h 35m 52s	CRITICAL - Host Unreachable (172.24.10.1)
LIBRE_2	DOWN	02-22-2023 22:11:54	149d 14h 25m 17s	CRITICAL - Host Unreachable (172.24.10.1)
PTP_COM_SO_01	UNREACHABLE	02-22-2023 22:09:07	42d 3h 48m 50s	(Host check timed out after 30.01 seconds)
PTP_H2O_NE_03	DOWN	02-22-2023 22:11:46	13d 17h 36m 49s	CRITICAL - Host Unreachable (172.28.0.15)
PTP_H2O_NE_04	DOWN	02-22-2023 22:11:45	13d 17h 36m 49s	CRITICAL - Host Unreachable (172.28.0.15)
PTP_TUL_NN_01	DOWN	02-22-2023 22:09:44	13d 17h 59m 47s	CRITICAL - Host Unreachable (172.28.0.24)
PUBLICA SMT	DOWN	02-22-2023 22:11:17	4d 20h 24m 10s	(Host check timed out after 30.03 seconds)
RB_COM_SE_01	UNREACHABLE	02-22-2023 22:11:44	42d 3h 51m 44s	(Host check timed out after 30.06 seconds)
RIO_COMIL_01	DOWN	02-22-2023 22:09:16	13d 18h 5m 45s	(Host check timed out after 30.01 seconds)
pruebas_server	DOWN	02-22-2023 22:11:54	149d 14h 23m 8s	CRITICAL - Host Unreachable (172.24.10.4)

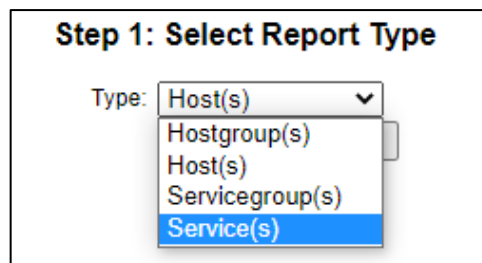
## 7. Reportes

Se utiliza el mismo método, se presenta una sección, donde se debe hacer clic en cada opción disponible.



Al seleccionar una opción, entonces se debe completar la siguiente plantilla.

- a) **Availability:** Se deberá selección el tipo de reporte.



Después se establecer al host o grupo de host que se desea generar el reporte de disponibilidad.



### Step 2: Select Hostgroup

Hostgroup(s): **\*\* ALL HOSTGROUPS \*\*** ▼

- \*\* ALL HOSTGROUPS \*\***
- CE
- EBH
- EFO
- OLT
- PTP
- RB
- SW
- ServerC
- linux-servers
- routerC
- routerINT
- routerT

Luego, se deberá seleccionar varias opciones para poder filtrar el periodo de tiempo que se desea obtener.

### Step 3: Select Report Options

Report Period: Last 7 Days ▼

If Custom Report Period...

Start Date (Inclusive): February ▼ 1 2023

End Date (Inclusive): February ▼ 22 2023

Report time Period: None ▼

Assume Initial States: Yes ▼

Assume State Retention: Yes ▼

Assume States During Program Downtime: Yes ▼

Include Soft States: No ▼

First Assumed Host State: Unspecified ▼

First Assumed Service State: Unspecified ▼

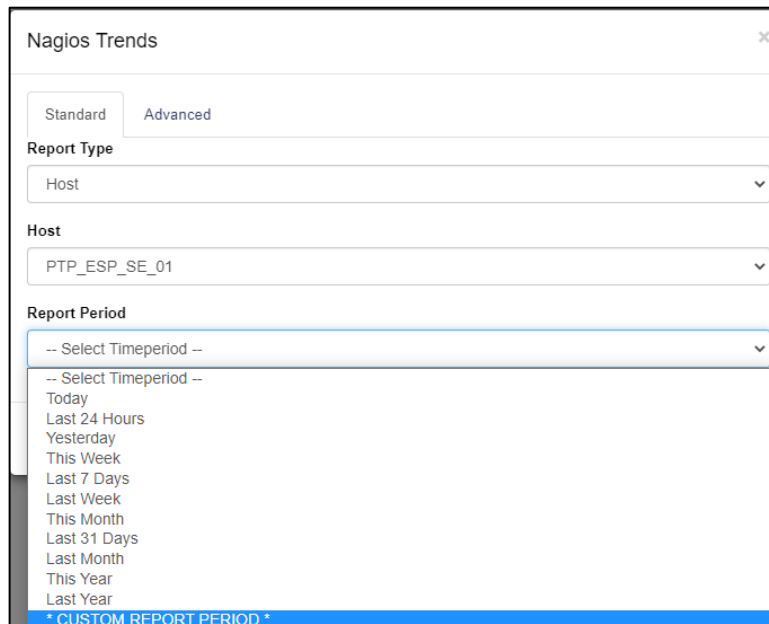
Backtracked Archives (To Scan For Initial States): 4

Output in CSV Format:

**Create Availability Report!**

Se da clic en el botón de “ Create Availability Report! “

b) **Trends:** Se establecen las tendencias que ha tenido los estados de un equipo monitoreado.

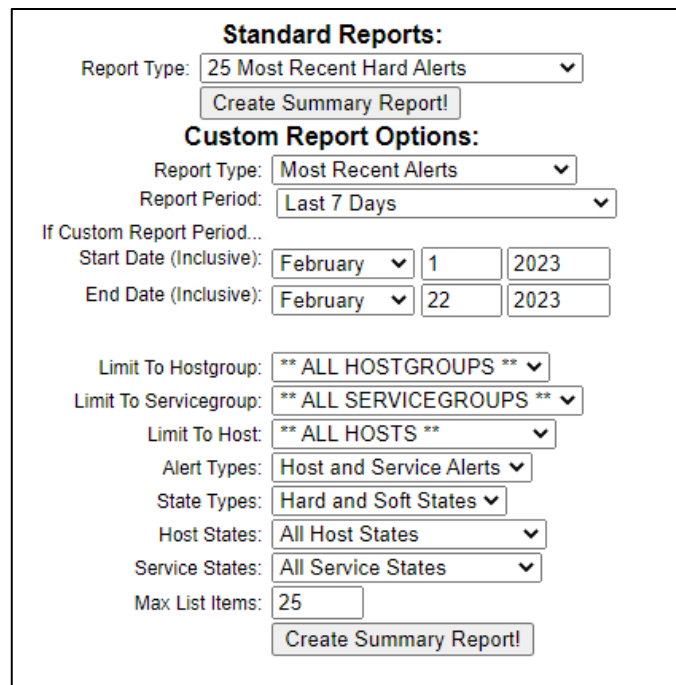


The screenshot shows the 'Nagios Trends' window with the following configuration:

- Standard (selected) / Advanced
- Report Type: Host
- Host: PTP\_ESP\_SE\_01
- Report Period: -- Select Timeperiod -- (dropdown menu is open showing options: Today, Last 24 Hours, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last 31 Days, Last Month, This Year, Last Year, \*CUSTOM REPORT PERIOD\*)

c) **Alertas:** También se presenta una plantilla para filtrar de mejor manera las subsecciones de Summary e Histogram.

○ Summary



The screenshot shows the 'Standard Reports:' configuration form with the following settings:

- Report Type: 25 Most Recent Hard Alerts
- Button: Create Summary Report!
- Custom Report Options:**
- Report Type: Most Recent Alerts
- Report Period: Last 7 Days
- If Custom Report Period...
  - Start Date (Inclusive): February 1 2023
  - End Date (Inclusive): February 22 2023
- Limit To Hostgroup: \*\* ALL HOSTGROUPS \*\*
- Limit To Servicegroup: \*\* ALL SERVICEGROUPS \*\*
- Limit To Host: \*\* ALL HOSTS \*\*
- Alert Types: Host and Service Alerts
- State Types: Hard and Soft States
- Host States: All Host States
- Service States: All Service States
- Max List Items: 25
- Button: Create Summary Report!

○ Histograma: es muy parecido al del apartado de Trends.

## ANEXO C:

### Propuesta para instalación del servidor Nagios Core



Dir.: Ave. 11 de noviembre 613 y Juan Salinas – Riobamba.  
Teléfonos: 0984552160 – 0987628653  
www.intertec.ec

#### PROPUESTA PARA IMPLEMENTACION DE SERVIDOR NAGIOS CORE

**REALIZADA POR:** Sebastián Sagñay León

#### RECURSOS NECESARIOS

##### Requerimientos recomendados para la instalación del software Nagios Core

- Sistema Operativo Linux o variante Unix, puede ser virtualizado.
- CPU de 2 núcleos a 2.66 GHz o superior
- RAM 4 GB o superior
- Unidad de disco duro de 20 GB o más.
- Conexión a internet para la actualización de paquetes.

##### Sistema Operativo.

- Centos 7 u 8.
- Debian 7 o superior
- Ubuntu 20.04 LTS "Fossa Focal" 64 bits (recomendado)

Nagios Core puede necesitar mayores recursos con el aumento de dispositivos a monitorear, por lo que se recomienda un servidor exclusivo.

##### Puertos Necesarios

Se requiere que el firewall permita las siguientes conexiones ENTRANTES desde CUALQUIER LUGAR:

Puertos	Uso	Protocolo
5666 / TCP	Nagios NRPE	Privado
161-162/ UDP	Nagios SNMP	SNMP v1,v2
25 / TCP	Notificaciones Nagios	SMTP
110 / TCP	Notificaciones Nagios	POP3
995 / TCP	Notificaciones Nagios	POP3
143 / TCP	Notificaciones Nagios	IMAP
993 / TCP	Notificaciones Nagios	IMAP

Se requiere que el firewall permita las siguientes conexiones SALIENTES a CUALQUIER LUGAR:

Puertos	Uso	Protocolo
5666 / TCP	Nagios NRPE	Privado
161-162/ UDP	Nagios SNMP	SNMP v1,v2
25 / TCP	Notificaciones Nagios	SMTP
110 / TCP	Notificaciones Nagios	POP3
995 / TCP	Notificaciones Nagios	POP3
143 / TCP	Notificaciones Nagios	IMAP
993 / TCP	Notificaciones Nagios	IMAP

## ANEXO D:

### Acuerdo de confidencialidad



Dir.: Av. 11 de noviembre 613 y  
Juan Salinas – Riobamba.

Teléfonos: 0984552160 -  
0987628653

www.intertec.ec

#### **ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN PARA LA EMPRESA RIOBIT CÍA. LTDA.**

Intervienen en la celebración del presente "ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN", por una parte, **Carlos Andrés Hervas Parra** con cédula de ciudadanía Nro. 0604153262, en mi calidad de GERENTE GENERAL de la empresa RIOBIT CÍA. LTDA., y por otro lado **Mauro Sebastián Sagnay León** con cédula de ciudadanía Nro. 0605151018 en mi calidad ESTUDIANTE de la CARRERA DE TELECOMUNICACIONES de la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, ambas partes reconocen recíprocamente su capacidad para obligarse, por lo que suscriben libre y voluntariamente el presente "ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN" con base a las siguientes cláusulas.

##### **PRIMERA.- ANTECEDENTES**

Para efectos del presente acuerdo, la "INFORMACIÓN CONFIDENCIAL" comprende toda la información divulgada por parte de la empresa RIOBIT CÍA. LTDA., ya sea de manera oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como tal al ser entregada a la parte receptora. La parte receptora se obliga a mantener de manera confidencial toda la información generada durante la vigencia de su contrato en relación de dependencia con la empresa RIOBIT CÍA. LTDA.

##### **SEGUNDA.- CONVENIO DE CONFIDENCIALIDAD**

- El estudiante se obliga en forma irrevocable ante la empresa RIOBIT CÍA. LTDA., a no revelar, divulgar o facilitar la "INFORMACIÓN CONFIDENCIAL" de la empresa RIOBIT CÍA. LTDA., bajo cualquier forma a persona alguna sea natural o jurídica, pública o privada, o de cualquier otra naturaleza, y a no utilizar dicha información para su propio beneficio o para beneficio de un tercero.
- El estudiante no podrá reproducir, modificar, hacer pública, divulgar o utilizar de cualquier forma conocida o por conocerse a terceros o para su propio beneficio o para beneficio de cualquier otra persona natural o jurídica la "INFORMACIÓN CONFIDENCIAL" del presente acuerdo sin previa autorización escrita y expresa por parte de la empresa RIOBIT CÍA. LTDA.
- En caso de que la información resulte revelada, divulgada o utilizada por un trabajador de cualquier forma distinta al objeto de este acuerdo, ya sea de forma dolosa o por mera negligencia, será sancionado de acuerdo con las leyes vigentes para el efecto.

##### **TERCERA.- PROPIEDAD INTELECTUAL**

- Toda la información, productos y servicios creados, modificados o generados por el estudiante durante la vigencia de su trabajo de tesis en relación de dependencia con la empresa serán de propiedad de RIOBIT CÍA. LTDA.
- Los derechos de propiedad intelectual de la información que pertenecen a la empresa RIOBIT Cía. Ltda., no podrán ser revelados por el estudiante para su producción parcial o total; así como su comunicación pública y distribución.

#### **CUARTA.- DIVERGENCIAS Y CONTROVERSIAS**

En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente ACUERDO, las partes se someten expresamente a las instancias Administrativas, a los Juzgados y Tribunales del País, con renuncia a su fuero propio, aplicándose a la legislación ecuatoriana vigente.

#### **QUINTA.- ACEPTACIÓN**

Para constancia de que el contenido del presente Acuerdo de Confidencialidad ha sido comunicado, conocido y entendido a cabalidad por parte del trabajador, quién en consecuencia acepta su contenido y se compromete a su fiel cumplimiento, por lo cual lo suscribe dos ejemplares de igual tenor y valor.

En la ciudad de Riobamba, a los 09 días del mes de junio de 2022.

**Firman:**

  
CARLOS ANDRÉS HERVAS PARRA  
0604153262  
GERENTE GENERAL  
RIOBIT CÍA. LTDA.

  
MAURO SEBASTIÁN SAGÑAY LEÓN  
0605151018  
ESTADIANTE




ESCUELA SUPERIOR POLITÉCNICA DE  
CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL  
APRENDIZAJE



UNIDAD DE PROCESOS TÉCNICOS  
REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 10/04/2023

<b>INFORMACIÓN DE LOS AUTORES</b>	
<b>Nombres – Apellidos:</b>	Mauro Sebastián Sagñay León
<b>INFORMACIÓN INSTITUCIONAL</b>	
<b>Facultad:</b>	Informática y Electrónica
<b>Carrera:</b>	Telecomunicaciones
<b>Título a optar:</b>	Ingeniero en Electrónica, Telecomunicaciones y Redes
<b>f. Analista de Biblioteca responsable:</b>	 Ing. Fernanda Arévalo M.

