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

Carlos A. Vásquez, Viviana E. Ayala

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

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

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

***Términos Indexados*—ISO, NMS, ITU-T, UDP, SNMP.**

I. INTRODUCCIÓN

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

Documento recibido en Junio del 2015. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.

C.A. Vásquez, Docente de la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador (teléfono 5936-2955-413; e-mail: cava_6@hotmail.com).

V.E. Ayala, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (teléfono 5939-2054-723; e-mail: ayala_yandun@hotmail.com).

Es una entidad que día a día se compromete con el uso masivo de las Tecnologías de la Información y la Comunicación (TIC), conformando una plataforma integrada con todas sus unidades para brindar conectividad de servicios, a través de herramientas hardware y software para satisfacer los requerimientos y exigencias de los usuarios del cantón.

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

II. FUNDAMENTOS DE GESTIÓN DE RED

A. Administración de red

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

Tiene la capacidad de garantizar que el uso de la red se realice de manera eficaz, mejorando la continuidad en la operación de la red mediante mecanismos de monitoreo que ayudan a resolver problemas y tener monitoreados los recursos. [1]

B. Gestión de red.

Según la ISO (*International Organization for Standardization)* afirma a la gestión de red como: El conjunto de actividades necesarias para el control y supervisión de los recursos que ayudan al intercambio de información que circula por la red de datos, aumentando su funcionalidad y rendimiento. [2]

C. Elementos de un sistema de gestión de red.

Según como se especifica en el RFC de Internet y otros documentos distribuidos, un sistema de gestión comprende los

siguientes elementos y en la Figura 1 se indica cada uno de ellos:

Dispositivos Gestionados.- Equipamientos que se comunican con la red, con el propósito de ser monitoreados, se denominan elementos de red o dispositivos gestionados, tales como routers, switches, servidores, computadoras, impresoras, etc.

Gestor.- Es la consola a través de la cual el administrador de red realiza funciones de gestión de red, genera operaciones de gestión (comandos, peticiones) y recibe (respuestas, notificaciones) de los agentes.

Agentes.- Son módulos software que recopilan y almacenan información local acerca de los dispositivos gestionados en el que reside y luego almacenan esta información en una base de datos de gestión, para proporcionarla a las entidades de gestión a través de un protocolo de gestión de red.

Estación de gestión de red ó Network Management Station (NMS).- Son dispositivos independientes que sirven como interfaz entre el administrador y la red.

*Protocolo de gestión de red.- S*e utiliza para transmitir información de gestión entre los agentes y las estaciones de gestión de red (NMS).

*Base de Información de Gestión (MIB).- S*e deriva del modelo de gestión la red OSI/ISO y es un tipo de base de datos utilizada para gestionar los dispositivos en una red de comunicaciones. Se compone de una colección de objetos en una base de datos (virtual).

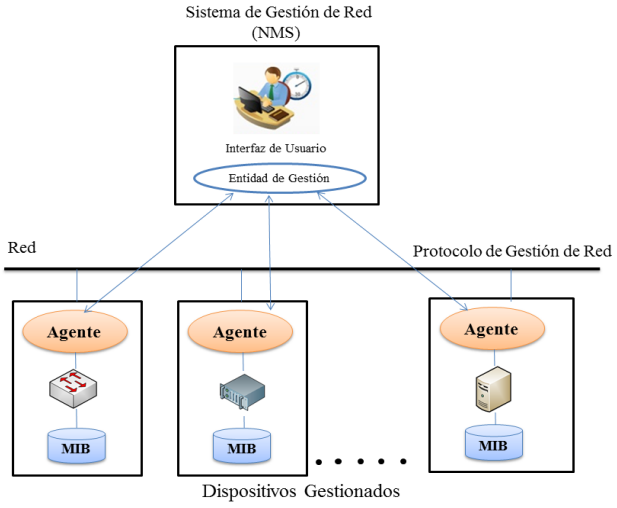


Figura 1. Elementos de un modelo de gestión de red
Fuente: (Ding, 2010)

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

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

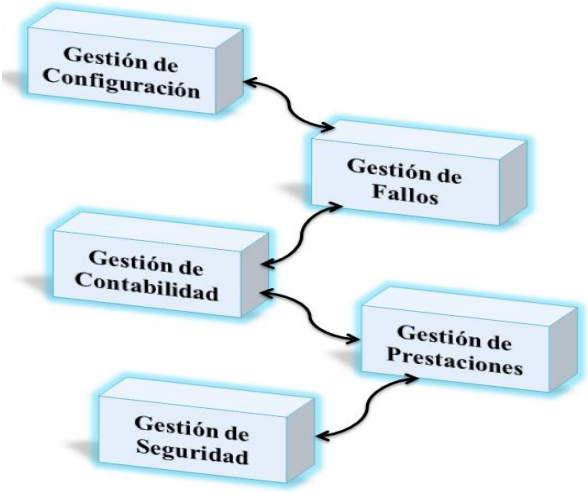


Figura 2. Áreas del Modelo Funcional
Fuente: (Jorquera, 2010)

Gestión de Configuración.
La gestión de configuración se refiere a mantener información relativa al diseño y configuración actual de la red. Esta área es quizás la más importante de la administración de la red porque una configuración incorrecta puede hacer que la red no funcione en absoluto. [3]

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

- *Gestión de configuración de hardware*

Su objetivo es mostrar lo que hace la infraestructura e ilustrar las ubicaciones físicas y vínculos entre cada elemento, que se conocen como elementos de configuración.

- *Gestión de configuración de software*

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

- ✓ Identificación de la configuración.
- ✓ Control de cambios de configuración.
- ✓ Determinación del estado de configuración.
- ✓ Configuración de autenticación.

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

Dentro de las funciones de la gestión de fallos se encuentra las siguientes. [4]

Evitar el fallo antes de que suceda, aquí se encuentra la gestión proactiva y la gestión de pruebas preventivas.

Si el fallo ha sucedido, se conoce como gestión reactiva donde se encuentra los siguientes parámetros:

- Detección de fallos

Determina la causa de una avería, radica en el proceso de capturar indicaciones en forma de alarmas de (usuarios o de herramientas), acerca del desorden en las redes proporcionadas por los dispositivos que funcionan mal.

- Aislamiento de fallos

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

- Diagnosis de fallos

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

Gestión de Contabilidad.
La Gestión de Contabilidad se basa en el registro del uso de los recursos y servicios prestados por la red a los usuarios. Dentro de esta Gestión se menciona lo siguiente:

Funciones de la gestión de contabilidad.
A continuación se enumeran las principales tareas y funciones realizadas por la gestión de contabilidad:

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

Gestión de Prestaciones.
Se refiere a evaluar el comportamiento y asegurar el correcto funcionamiento de los dispositivos gestionados y la efectividad de determinadas actividades, además, recoge y procesa los datos medidos para generar los informes correspondientes.

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

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

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

E. Protocolo Simple de Gestión de Red (SNMP)

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

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

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

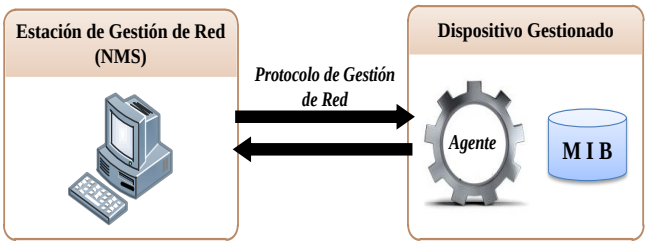


Figura 3. Componentes involucrados en SNMP
Fuente: (Guerrero Pantoja, 2011)

Estos componentes interaccionan con los operadores humanos y desencadenan las acciones necesarias para llevar a cabo las tareas por ellos invocadas o programadas

F. Servicios que ofrece GSM.

El estándar de telefonía móvil GSM facilita la existencia de una serie de servicios, sin necesidad de un módem externo a través de una tarjeta para conexión con el puerto serie del ordenador. Ofrece un servicio de mensajes alfanuméricos cortos (SMS) de hasta 160 caracteres y toda una completa gama de servicios suplementarios.

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

A. Topología física de la red local de datos.

En el diagrama que se muestra en la Figura 4 se detalla la estructura de la topología física de la red local de datos del GAD-Ibarra, donde se observa las conexiones de los enlaces LAN que se dirigen hacia los edificios de las dependencias internas y externas.

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

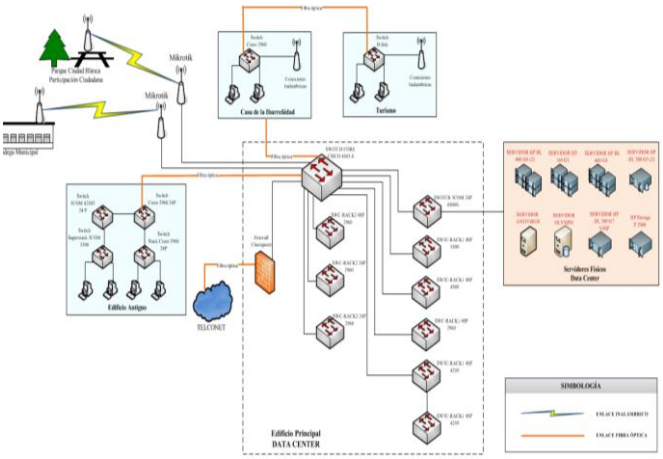


Figura 4. Topología física de la red de datos
Fuente: (Unidad de Hardware y Comunicaciones, 2013)

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

Después de haber obtenido los datos de la infraestructura física y lógica de la red local de datos del GAD-Ibarra se procede a realizar un análisis conjuntamente con el administrador de la red, en el cual se determina las áreas críticas y los equipos mayor prioridad los cuales van hacer objeto para la posterior implementación. [5]

Análisis para elección de switches.

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

Se determina los dispositivos de red de mayor prioridad de acuerdo al establecimiento de un modelo jerárquico en capas, con su respectivo diagrama unifilar de puertos, como se observa en la Figura 5. Se estructuró en tres capas que son: núcleo, distribución y acceso los cuales cumple funciones específicas que se detallan a continuación:

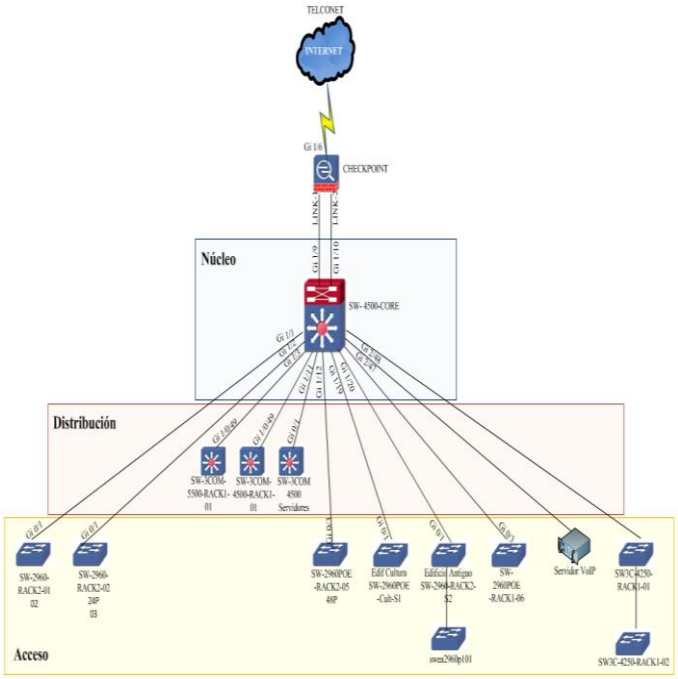


Figura 5. Modelo Jerárquico de la red del GAD-Ibarra
Fuente: (GAD-Ibarra, 2013)

Núcleo

Esta capa está constituida por un switch Cisco Catalyst 4503-E de alto rendimiento que es el Núcleo o Core. Este equipo se interconecta a través de la controladora uno hacia la capa de distribución, capa de acceso y conjuntamente con el equipo Firewall Check Point, el mismo que se conecta a su vez con la red Internet de Telconet. Y a través de la controladora dos se conecta con un switch de la capa de acceso y el servidor de VoIP.

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

Distribución

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

Acceso

Esta capa se encarga de establecer conectividad con los usuarios finales de la entidad integrando equipos de red como; impresoras de red, computadores, teléfonos IP, Access Point, entre otros. Los switches que conforman están capa poseen un

manejo de VLAN's que permiten segmentar los dominios de broadcast, y brindar mayor seguridad a los dispositivos del nodo final de la red, de tal manera que se ha establecido como área critica.

Se consideró gestionar el switch que se encuentra en el departamento de Cultura ya que este switch mantiene conectividad para el envío de información al edifico principal, es fundamental porque aquí se realizan actividades sociales y proyectos que deben ser supervisados por las autoridades de mayor orden.

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

Análisis para elección de servidores físicos.
Los servidores implican una gran relevancia para la entidad, de forma tal que la interrupción de sus prestaciones implicaría un alto valor de pérdidas es por eso que su correcto funcionamiento es fundamental. Entre los más críticos se encuentra los siguientes:

- Servidor POSTGRESQL.
- Servidor OLYMPO
- Servidor de antivirus.
- Servidores HP.

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

- Servidor de Correo.
- Servidor DNS y DHCP.
- Servidor documental Quipux.
- Servidor de repositorios.
- Servidor de aplicaciones web.
- Servidor SRI
- Servidor MAPSERVER.
- Servidor WEBSERVICE.
- Servidor de Base de datos POSTGIS.

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

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

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

Niveles Organizacionales

a) Director.- Autoridad de nivel superior. Bajo su administración está la aceptación de las políticas de gestión, en concordancia con el encargado de la Unidad de Hardware y Comunicaciones y la Unidad de Informática.
b) Encargado de la Unidad de Hardware y Comunicaciones.- Persona encargada del análisis previo del estado de la red de la entidad mediante evaluaciones de disponibilidad, mantenimiento y rendimiento. Mantiene informes de los procedimientos realizados conjuntamente en coordinación con la Unidad Informática.
c) Unidad Informática.- Departamento dentro de la entidad, que se encarga del funcionamiento del Data Center para la efectividad del procesamiento de datos e información con todo lo relacionado a la instalación de redes LAN y WLAN, utilización, mantenimiento y actualización de equipos informáticos.

Vigencia
La documentación presentada con sus respectivas políticas de gestión entrará en vigencia desde el momento en que sea aprobado como documento técnico de gestión de red por las autoridades correspondientes del departamento TIC del GAD-Ibarra.

Referencia
El presente documento es realizado tomando como referencia el formato que la institución ya tiene de un proyecto anterior. [6]

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

- Políticas de Gestión de la red de área local de datos.
  - ✓ Objetivo de la Política de Gestión.
  - ✓ Compromiso de las Autoridades.
- Gestión de Configuración.
  - ✓ Ingreso de dispositivos de red al software de gestión.
  - ✓ Configuración de dispositivos de red.
- Gestión de Fallos.
  - ✓ Manejo de fallos.
  - ✓ Manejo de umbrales.
- Gestión de Contabilidad.
  - ✓ Parámetros de monitoreo.
- Gestión de Prestación.
  - ✓ Colección de datos estadísticos del rendimiento de la red.
  - ✓ Reportes.
- Gestión de Seguridad.
  - ✓ Acceso al Software de Gestión.
  - ✓ Acceso a los dispositivos de red gestionados.

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

Implementación dentro de la Gestión de Configuración.

Esta área de gestión comprende en realizar el análisis de la situación actual de la red de datos del GAD-Ibarra para conocer el estado físico y lógico en el que se encuentra.

Requerimientos para elección del software de gestión.

Dentro de esta área de gestión es necesario realizar un previo análisis comparativo de las funcionalidades y mejores características de software de gestión, se ha seleccionado Pandora FMS, Zabbix, Cacti y Nagios. El software de gestión fue elegido en base al estándar IEEE Std. 830-1998, tomando como referencia el cumplimiento del modelo de gestión FCAPS y las necesidades de la entidad.

Se eligió Nagios porque cumple con aspectos como; presentar una interfaz de gestión centralizada, soportar el monitoreo remoto de varios sistemas operativos, establecimiento de umbrales que generan alertas cuando llegan a su límite máximo de funcionamiento y envían notificaciones de correo electrónico o SMS al administrador de la red, proporciona distintas opciones para la generación de informes, datos estadísticos, basándose en la información recolectada y además soporta su instalación en un entorno virtualizado característica fundamental para el desarrollo de la implementación. [7]

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

Una vez determinado el software de gestión a utilizar y los requerimientos hardware que necesita para su funcionamiento se procedió a realizar el diseño del sistema de gestión como se indica en la Figura 6. Donde se explica que el servidor de administración Nagios se encuentra instalado en un servidor físico HP BL 460 G6 mediante un entorno virtualizado, fue instalado en el sistema operativo Debian 6.0.1 debido a que los servidores actualmente se encuentran dentro de un entorno de virtualización y utilizando esta versión de software libre.

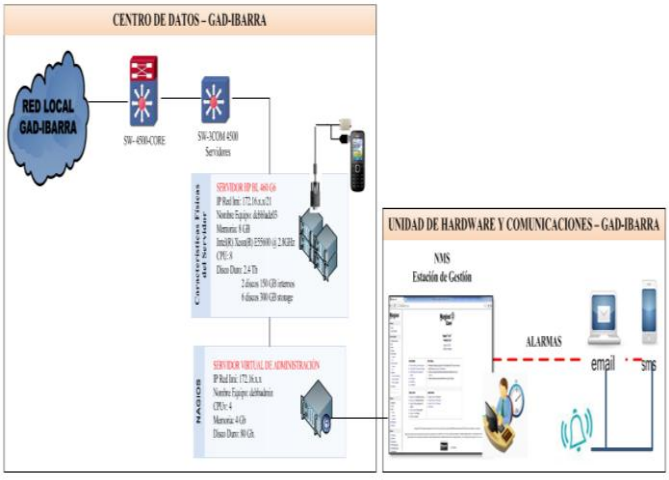


Figura 6. Diseño del Sistema de Gestión implementado
Fuente: Basada en inventario de TIC del GAD-Ibarra

Configuración del Gestor.

Dentro de este complemento de la gestión de configuración se incluye la secuencia de pasos de instalación que necesita el software de gestión Nagios para entrar en funcionamiento y en la Figura 7 se ilustra la misma:

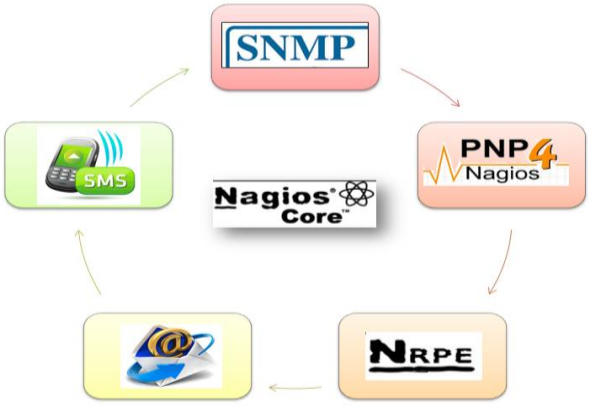


Figura 7. Representación del orden de Instalación
Fuente: Basada en software de gestión Nagios

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

Implementación dentro de la Gestión de Fallos.

Dentro de esta gestión de fallos se presenta dos situaciones a considerar:

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

Gestión Proactiva.

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

Definición de umbrales.

Los umbrales que se establecen a continuación en la Tabla 1 se encuentran en función de las características propias del dispositivo gestionado, por tal razón se establece un margen o porcentaje referencial.

Tabla 1. Umbrales para el Monitoreo

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

Fuente: Basada en umbrales de monitoreo

Se establece los umbrales de advertencia para que el administrador pueda dar una solución rápida antes que el dispositivo gestionado llegue a un estado crítico y de esta forma optimizar sus recursos. [8]

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

- *Pruebas de conectividad física.*

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

- *Pruebas de conectividad lógica.*

Este tipo de pruebas se realizan ingresando mediante el programa PuTTY a través del puerto 22 y 23 correspondiente a SSH y Telnet para comprobar conectividad punto a punto mediante el comando "ping" y mediante "traceroute" comprobar conectividad salto por salto.

Gestión Reactiva.
Este tipo de gestión se ejecuta cuando el fallo ha sucedido y se realiza el proceso de detectar, aislar, diagnosticar, corregir y documentar como se observa en la secuencia de la Figura 8:

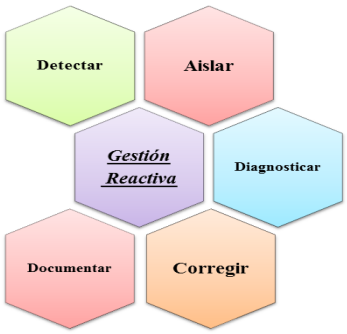


Figura 8. Proceso de Gestión Reactiva
Fuente: Basada en la Gestión Reactiva

Detectar.
Nagios permite detectar en la primera señal que emita el fallo mediante la visualización de cambio de colores en el mapa de la interfaz web de acuerdo a los (parents) es decir que dispositivo es el que está afectado, un switch de la capa de acceso que está conectado al switch core o un servidor que está conectado en un switch de la capa de distribución. En la Figura 9 se observa como Nagios permite al administrador que detecte fácilmente un fallo.

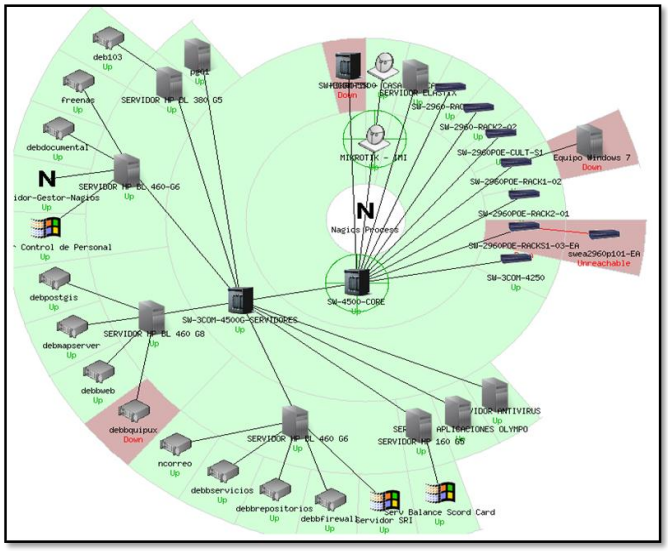


Figura 9. Detección de fallos en el mapa de la interfaz web
Fuente: Extraída del gestor Nagios

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

En las Figuras 10 y 11 se indica una notificación enviada desde Nagios a la cuenta de correo electrónico Gmail donde informa que existe un problema, el servicio número 17 donde se encuentra configurada la interfaz GigabitEthernet 1/20 Enlace de Fibra Óptica que se conecta con el Edificio Antiguo del Switch_CORE con la dirección IP 172.x.x.x presenta un estado crítico porque la interfaz esta down (abajo).

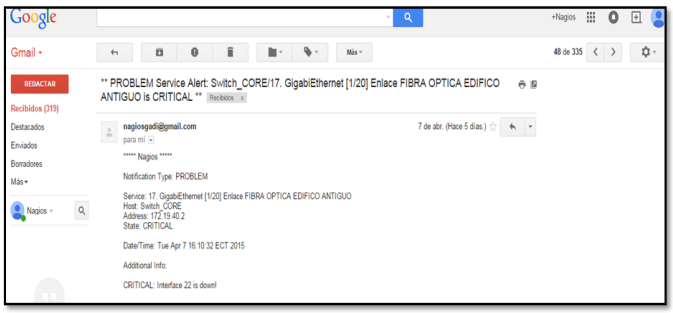


Figura 10. Envío de correo electrónico desde Nagios
Fuente: Extraída de cuenta de correo Gmail, creada específicamente para la entidad

Figura 11. Envío de mensaje de texto desde Nagios
Fuente: Extraída desde teléfono móvil del administrador de la red

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

Jerarquía de alertas
En la Tabla 2 se indica cómo se puede aislar un fallo dependiendo del color que generan los dispositivos gestionados de acuerdo a la jerarquía de alertas, mediante cinco tipos de estados, tratando así de que otros equipos no se vean afectados a causa del mismo problema y poder encontrar la mejor solución.

Tabla 1. Jerarquía de alertas que genera Nagios

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

Fuente: Datos obtenidos del software de gestión Nagios

Diagnosticar.
Una vez que se ha detectado y aislado el origen del fallo sea en equipos o servicios que se vieron afectados. Se procede a establecer un diagnóstico mediante Nagios de las posibles causas que han provocado un fallo:

- El dispositivo gestionado perdió conectividad lógica, no existe tiempos de respuesta en ambos sentidos de la comunicación.
- El dispositivo gestionado perdió conectividad física, cables de red rotos, tarjetas de red dañadas.
- Los dispositivos gestionados no responden a peticiones de SNMP.
- Tan solo con dar click en el dispositivo que se ha detectado y aislado Nagios diagnostica un fallo crítico cuando existe un elevado consumo de niveles de umbrales normales de funcionamiento.
- Fallos que se relacionan con el tráfico de la red y con la falta de disponibilidad de los servicios.

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

- Remplazo de recursos dañados, hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente. En la infraestructura de la red local de datos del GAD-Ibarra los equipos más susceptibles a fallos y con más criticidad en la red se encuentran los switch Cisco Catalyst de la serie 2960 los cuales forman parte de la capa de acceso.
- Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento. En este punto, el diseño de la red de la entidad cuenta con la existencia un enlace redundante activo para el chasis de servidores, garantizando de esta manera el funcionamiento normal de los servicios utilizados por los diferentes equipos de la capa de distribución y la capa core.
- Los dispositivos de red recuperan conectividad y se estabilizan si son reiniciados.

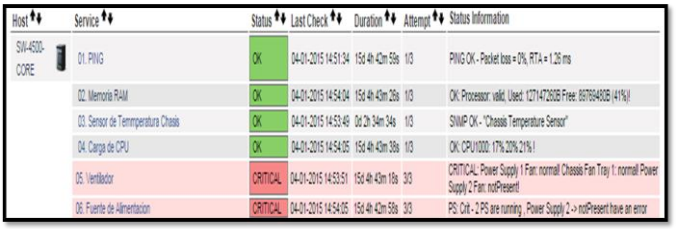
Documentar.
La documentación será registrada en una base de datos para su respectivo manejo y seguimiento. Además cabe recalcar que esta área de gestión es de competencia solamente de la entidad.

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

- Parámetros de monitoreo.
- Parámetros de estado.
- Parámetros de chequeo.

Implementación dentro de la Gestión de Prestaciones.
Esta área de gestión consiste en mantener monitoreado constantemente el estado de los dispositivos gestionados y salvaguardar su rendimiento para determinar su comportamiento sea este en un en un intervalo de tiempo o en tiempo real.

Rendimiento en la Capa Núcleo.
Nagios permite al administrador visualizar en su interfaz web el nombre del dispositivo gestionado, servicio que está monitoreando, estado, tiempo de chequeo, duración y la información del servicio en tiempo real. Enseguida se describe los parámetros que indica la interfaz web en la Figura 12.



Host	Service	Status	Last Check	Duration	Attempt	Status Information
SW-4500-CORE	01. PING	OK	04-01-2015 14:51:34	15d 4h 42m 59s	1/3	PING OK - Packet loss = 0%, RTA = 1.26 ms
	02. Memoria RAM	OK	04-01-2015 14:54:04	15d 4h 43m 29s	1/3	OK: Processor: valid; Used: 127147265B Free: 897894908 (41%)!
	03. Sensor de Temmperatura Chasis	OK	04-01-2015 14:53:49	0d 2h 34m 34s	1/3	SNMP OK - "Chassis Temperature Sensor"
	04. Carga de CPU	OK	04-01-2015 14:54:05	15d 4h 43m 39s	1/3	OK: CPU1000: 17% 20% 21%!
	05. Ventilador	CRITICAL	04-01-2015 14:53:51	15d 4h 43m 16s	3/3	CRITICAL: Power Supply 1 Fan: normal Chassis Fan Tray 1: normal Power Supply 2 Fan: notPresent
	06. Fuente de Alimentacion	CRITICAL	04-01-2015 14:54:05	15d 4h 43m 59s	3/3	PS Crit - 2 PS are running , Power Supply 2 -> notPresent have an error

Figura 12. Rendimiento de servicios del Switch Core
Fuente: Captura propia extraída de software de gestión Nagios

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

En la Figura 13 se muestra el rendimiento capturado por Nagios en su interfaz web de cada una de las interfaces Gigabit Ethernet y VLAN configuradas del switch core y que se conectan a los diferentes switches de distribución y acceso de la entidad.

07. GigabitEthernet [1/1] Hacia SW-2960-RACK2-01	OK	03-22-2015 11:35:56	4d 23h 44m 43s	1/3	OK - Average IN: 184.29Kbps 0.18% Average OUT: 222.33Kbps 0.22%
08. GigabitEthernet [1/2] Hacia SW-2960-RACK2-02	OK	03-22-2015 11:36:06	2d 0h 43m 45s	1/3	OK - Average IN: 42.98Kbps 0.04% Average OUT: 185.08Kbps 0.19%
09. GigabitEthernet [1/3] Hacia SW-3COM-5500-RACK1-01	OK	03-22-2015 11:36:31	2d 2h 46m 44s	1/3	OK - Average IN: 12.34Kbps 0.01% Average OUT: 44.00Kbps 0.04%
10. GigabitEthernet [1/7]	OK	03-22-2015 11:36:46	2d 2h 46m 42s	1/3	OK - Average IN: 1.24Kbps 0.00% Average OUT: 18.52Kbps 0.02%
11. GigabitEthernet [1/9] Hacia LINK-1-CHECKPOINT	OK	03-22-2015 11:36:21	2d 2h 46m 43s	1/3	OK - Average IN: 4.31Mbps 4.31% Average OUT: 157.50Kbps 0.16%
12. GigabitEthernet [1/10] Hacia LINK-2-CHECKPOINT	CRITICAL	03-22-2015 11:36:16	5d 1h 27m 29s	3/3	CRITICAL: Interface 12 is down!
13. GigabitEthernet [1/11] Hacia SW-3COM-SERVIDORES	OK	03-22-2015 11:36:15	2d 0h 15m 43s	1/3	OK for 13 - Average IN: 77.49Kbps 0.01% Average OUT: 455.74Kbps 0.05%
14. GigabitEthernet [1/12] Hacia SW-2960POE-RACK2-05	OK	03-22-2015 11:35:51	2d 2h 46m 6s	1/3	OK - Average IN: 406.27Kbps 0.41% Average OUT: 2.50Mbps 2.50%
15. GigabitEthernet [1/18] Hacia CUARTEL	CRITICAL	03-22-2015 11:36:11	4d 23h 36m 14s	3/3	CRITICAL: Interface 20 is down!
16. GigabitEthernet [1/19] Enlace FIBRA OPTICA CULTURA	OK	03-22-2015 11:36:31	2d 2h 46m 6s	1/3	OK - Average IN: 11.84Kbps 0.01% Average OUT: 36.42Kbps 0.04%
17. GigabitEthernet [1/20] Enlace FIBRA OPTICA EDIFICO ANTIGUO	CRITICAL	03-22-2015 11:35:56	4d 23h 36m 13s	3/3	CRITICAL: Interface 22 is down!
18. GigabitEthernet [2/47] Hacia SW-2960POE-RACK1-06	OK	03-22-2015 11:35:56	2d 2h 46m 6s	1/3	OK - Average IN: 11.19Kbps 0.01% Average OUT: 27.46Kbps 0.03%
19. GigabitEthernet [2/48] Hacia Servidor VoIP	OK	03-22-2015 11:36:45	2d 2h 46m 11s	1/3	OK - Average IN: 16.59Kbps 0.02% Average OUT: 36.79Kbps 0.03%
20. VLAN 1	OK	03-22-2015 11:36:25	2d 2h 46m 41s	1/3	OK - Average IN: 134.13Kbps 0.13% Average OUT: 4.55Mbps 4.55%
21. VLAN 2	OK	03-22-2015 11:36:11	2d 2h 46m 6s	1/3	OK - Average IN: 1.70Kbps 0.00% Average OUT: 967.73bps 0.00%
22. VLAN 3 VoIP	CRITICAL	03-22-2015 11:35:51	1d 18h 29m 13s	3/3	CRITICAL Traffic IN for 80 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 80
23. VLAN 7	OK	03-22-2015 11:36:11	4d 23h 36m 50s	1/3	OK - Average IN: 166.55Kbps 0.17% Average OUT: 224.33Kbps 0.22%

Figura 13. Rendimiento de servicios del Switch Core
Fuente: Captura propia extraída de software de gestión Nagios

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

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

V. MANUALES DE PROCEDIMIENTOS

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

A. Introducción.

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

Por consiguiente se realiza la estructuración de estos manuales con sus respectivas directrices que ayuden a los encargados de la red a diagnosticar y corregir problemas en la red local de datos en el menor tiempo posible, mediante las cinco áreas de gestión las cuales se relacionan entre sí para obtener un mayor rendimiento de sus recursos gestionados. Se presenta el proceso de ingreso y configuración de equipos, localización de fallos, corrección de fallos, visualización de reportes e informes, envió de notificaciones entre otras. [9]

Manual de procedimientos para la Gestión de Configuración.

- Objetivo.- Indicar a los administradores de la red el proceso de configuración de nuevos dispositivos a gestionar.
- Alcance.- Aplica este manual al ingreso de dispositivos al software de gestión, los cuales cumplan con los requerimientos de red, su nomenclatura y especificaciones técnicas, además se presenta el procedimiento para switches y servidores.

Manual de procedimientos para la Gestión de Fallos.

- Objetivo.- Encontrar la mejor solución frente a un problema que se presente en la red local de datos, antes de que sea percibido por los usuarios.
- Alcance.- Aplica el establecimiento de umbrales para los recursos que se van a gestionar, logrando tener mayor disponibilidad de funcionamiento en le red local de datos. Restaurar el servicio tan pronto sea posible e identificar y analizar la causa de los incidentes con el fin de evitar su recurrencia.

Manual de procedimientos para la Gestión de Contabilidad.

- Objetivo.- Indicar los parámetros que se utilizarán para el monitoreo y configuración de los dispositivos de red que se van a gestionar en la red local de datos.
- Alcance.- Se presenta el procedimiento para agregar dispositivos de red y servicios al software de gestión Nagios los mismos que deben cumplir con las características establecidas para que puedan ser monitoreados y se obtenga la información pertinente de la utilización de cada recurso.

Manual de procedimientos para la Gestión de Prestaciones.

- Objetivo.- Recopilar y analizar información acerca del rendimiento de los recursos de los dispositivos gestionados.
- Alcance.- Esta gestión se relaciona conjuntamente con la gestión de fallos, por lo tanto aquí se determina el comportamiento en diversos aspectos, ya sea en un intervalo de tiempo en particular o en tiempo real. Esto permitirá tomar las decisiones respectivas de acuerdo a los resultados que generen el comportamiento de los dispositivos gestionados.

Manual de procedimientos para la Gestión de Seguridad.

- Objetivo.- Brindar seguridad al sistema de gestión el cual requiere la habilidad para autentificar usuarios y aplicaciones de gestión, con el fin de garantizar la confidencialidad e integridad de intercambios de operaciones de gestión y prevenir accesos no autorizados.
- Alcance.- La información del GAD-Ibarra posee un valor muy importante porque vincula el sistema financiero y el servicio a los usuarios de la ciudadanía por ese motivo es fundamental mantener protegidos los recursos que hacen posible la conectividad y comunicación con entidades externas.

VI. Conclusiones

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

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

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

Mediante la descripción de políticas de gestión de las cinco áreas funcionales del modelo de gestión, se determinó los lineamientos que ayudan a mejorar el funcionamiento y disponibilidad de los dispositivos que forman parte de la red de la entidad.

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

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

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

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

REFERENCIAS

[1] Alarcón Ávila, R. (2007). Gestión y Administración de Redes como Eje Temático de Investigación. Bogotá: Universida Libre.

[2] ISO / IEC . (1989, 11 15). ISO / IEC 7498-4:1989. Retrieved from ISO / IEC 7498-4:1989: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=14258

[3] Ding, J. (2010). Advances in Network Management. United States of America: Auerbach Publications Taylor & Francis Group.

[4] Orozco, P. (2010). Gestión de Red del boli al SNMP. CASTELLDEFELS: UPCnet.

[5] GAD-Ibarra. (2013). Inventario de depencias. Ibarra: Gobierno Autónomo Descentralizado de San Miguel de Ibarra.

[6] Cevallos Michilena, M. A. (2013). Metodología de seguridad informática con base en la norma iso 27002 y en herramientas de prevención de intrusos para la red administrativa del Gobierno Autónomo Descentralizado de San Miguel de Ibarra. Ibarra: Universidad Técnica del Norte.

[7] Nagios Enterprises. (2014, Marzo 05). Nagios Core Documentación. Retrieved from http://www.nagios.org/

[8] Microsoft. (2005, Octubre 25). Microsoft TechNet. Retrieved from http://technet.microsoft.com/es-es/library/bb124583(v=exchg.65).aspx

[9] Rea Lozada, R. A. (2012). "NORMAS DE CONTROL INTERNO EMITIDAS POR LA CONTRALORÍA GENERAL DEL ESTADO, APLICADAS A LA DIRECCIÓN DE TECNOLOGÍAS. Ibarra: Universidad Técnica del Norte.

Carlos A. Vásquez A.

Nació en Quito - Ecuador el 19 de Septiembre de 1981. Ingeniero en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional en 2008. Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador, y es egresado de la Maestría en Redes de Comunicación, Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

Viviana E. Ayala Y.

Nació en Carchi - Ecuador el 17 de Agosto de 1989. Realizó sus estudios primarios en la Escuela "María Angélica Idrobo". En el año 2006 obtuvo su título de Bachiller en ciencias especialización físico matemáticas en el colegio "Nacional Ibarra". Actualmente, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.