Sistema de gestión de red basado en el modelo funcional SNMP de la IETF para monitorear los recursos de la red LAN en el edificio de EMAPA-I de la ciudad de Ibarra

Edgar A. Maya, Richard A. Mallamas

Resumen.- **El presente proyecto consiste en diseñar un sistema de monitorización basado en el modelo funcional SNMP utilizando herramientas Open Source en un servidor proporcionado por EMAPA-I con el propósito de obtener 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.- SNMP, CentOS, GLPI, OCS-INVENTORY, IP.

I. INTRODUCCIÓN

EMAPA-I es una empresa ibarreña que se esfuerza diariamente por mantener los altos índices de gestión en la dotación de servicios básicos eficientes, de calidad y con continuidad, logrando cada año incrementar el número de sus clientes, por lo que actualmente se encuentra fortaleciendo su infraestructura tecnológica paulatinamente con la finalidad de mejorar la prestación de los servicios en beneficio de la comunidad. Actualmente el departamento de sistemas se encuentra en la fase de inicio para la búsqueda de un software que le permita monitorear los recursos informáticos que se encuentran dentro de su red LAN, por tanto aún no se han establecido políticas y procesos que aseguren tanto la confiabilidad de la información como la disponibilidad en la red de comunicaciones, causando pérdidas económicas a la institución por la interrupción en la red.

Documento recibido en Marzo del 2016. 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.

E.A. Maya, 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 09-85198-101; e-mail: eamaya@utn.edu.ec).

R.A. Mallamas, egresado de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (teléfono 09-85155-075; e-mail: richard_mallamas@hotmail.com).

El incremento progresivo de los usuarios dificulta dar una solución pronta a los problemas que se dan por la saturación de la red, misma que es ocasionada por sobrepasar los umbrales de funcionamiento. Además no cuentan con herramientas que realicen tareas de envío, control y registro de notificaciones que alerten sobre el estado de los dispositivos de comunicación, por este motivo las fallas no se las pueda detectar a tiempo, provocando la molestia del personal que trabaja dentro de la institución.

Toda esta serie de inconvenientes han ido afectando gradualmente con la eficiencia de la red de datos, debido a que la entidad carece de procedimientos que permitan desplegar fallas en tiempo real o realizar el seguimiento continuo mediante estadísticas que permitan evaluar el funcionamiento de los recursos de comunicaciones. El crecimiento tecnológico de EMAPA-I debe garantizar la confiabilidad de la red de datos, por lo que la implementación de un sistema basado en un modelo de gestión permitirá establecer políticas de mantenimiento, destinadas a asegurar la disponibilidad de la red LAN de la institución.

II. DEFINICIONES Y CONCEPTOS BÁSICOS

A. Gestión de red

La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable.

B. Elementos de la gestión de red

En la gestión de red hay dos tipos de entidades: gestor y agente, entre las cuales se intercambian información para obtener un diagnóstico de la red.

Molero, L. (2010) menciona que un gestor es un servidor que ejecuta algún tipo de sistema de software que puede manejar las tareas de administración de una red, es responsable de la elección y recepción de capturas del tráfico de los agentes. El gestor es el que realiza una indagación en particular para conocer el estado específico

de uno o varios equipos dentro de la red con el fin de detectar irregularidades.

La segunda entidad, el agente, es un software dentro del dispositivo que se desea gestionar. Debido a la gran complejidad que presentan las redes actualmente, los fabricantes agregan agentes en sus equipos para dar flexibilidad a la gestión de red. Los agentes son los que perciben alguna inconsistencia dentro del dispositivo, y envía un aviso al gestor para alertarlo de su situación actual.

Hoy en día, la mayoría de los dispositivos IP vienen con algún tipo de agente SNMP incorporado, el hecho de los proveedores de dispositivos estén dispuestos a implementar agentes en muchos de sus productos ayuda en gran medida la administración del sistema.

C. Modelo de gestión SNMP

IETF es un grupo de trabajo con una organización informal que contribuye a la ingeniería y evolución de las tecnologías de Internet, el cual tiene la responsabilidad de desarrollar los estándares de Internet; ha definido un modelo de gestión de red formado de cuatro áreas funcionales, las cuales se muestran en la figura 1.

Figura 1.- Modelo Funcional SNMP

A continuación se describe las funciones básicas que cumple cada una de estas áreas:

Función de Operación.- Comprende la ejecución diaria y continúa de la red, incluye actividades como la auditoría, descubrimiento y monitorización de la red para garantizar que todo se encuentra ejecutándose correctamente. (Alexander Clemm, 2007).

Función de Administración.- Incluye las funciones de soporte requeridas para administrar la red, incluye actividades tales como diseño de la red, seguimiento de su utilización, asignación de direcciones, planificación de actualizaciones en la red, recepción de órdenes de servicio asociadas con usuarios finales y clientes, seguimiento del inventario de red. (Alexander Clemm, 2007).

Función de Mantenimiento.- Incluye las funcionalidades que garantizan la operación de la red y de los servicios de comunicación conforme lo esperado. Comprende actividades tales como diagnóstico, resolución de problemas, y reparación de componentes que no trabajan de acuerdo a lo planificado, a fin de mantener la red en un estado en el que pueda ser utilizada continuamente y proporcionando el servicio apropiado. (Cátedra redes de información, 2010).

Función de Seguridad.- Incluye funciones como la de mantener y gestionar la información de control de acceso, detección de incidentes de seguridad, identificar los principales riesgos y amenazas que afecten a los servidores más críticos. (Cátedra redes de información, 2010).

D. Protocolo Simple de Gestión de Red (SNMP)

Según el RFC 1155, SNMP se basa en el paradigma gestor-agente, es un protocolo de capa aplicación basado en la arquitectura TCP/IP, el cual hace posible el intercambio de información de gestión entre dispositivos de red, su funcionamiento se describe en la figura 2, en donde se puede apreciar como interactuan sus componentes principales que son: agente, protocolo simple de gestión de red (SNMP) y la base de información de gestión (MIB).

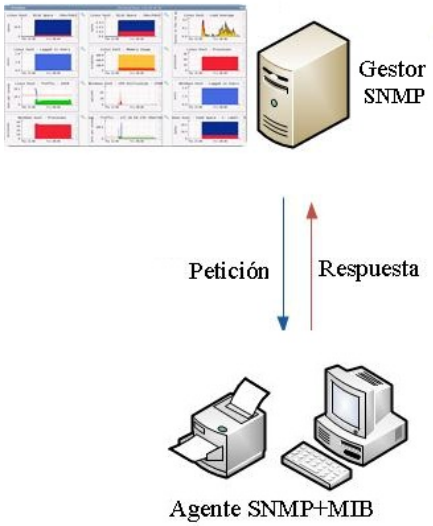

Figura 2.- Elementos de gestión SNMP

En la actualidad, existen tres versiones del protocolo SNMP definidas como: SNMPv1, SNMPv2 y SNMPv3.

SNMPv1 constituye la primera definición e implementación del protocolo SNMP, estando descrito en las RFC 1155, 1157 y 1212 del IETF (Internet Engineering Task Force), en la que cuenta con funciones básicas tanto de configuración como de seguridad. SNMPv2 ofrece varias operaciones de monitoreo, con configuración sencilla, las cuales son compatibles con la mayoria de dispositivos de red actuales. Sin embargo en la versión 3, se añade mejor seguridad, autentificación, y control de acceso.

III. SITUACIÓN ACTUAL DE LA RED LAN DE EMAPA-I

La infraestructura disponible en EMAPA se centraliza en la virtualización de servicios, actualmente está conformada por la siguiente infraestructura tecnológica:

A. Cuarto de Equipo

El cuarto de equipo se encuentra ubicado en la primera planta del edificio, aquí se encuentran los equipos de ruteo y conmutación así como también los servidores, los cuales se encuentran montados en racks estandares de diecinueve pulgadas. El cuarto de equipo es administrado por el departamento de tecnologías de la información y comunicación, que se encarga de realizar el mantenimiento y verificación del buen funcionamiento de la infraestructura tecnológica.

B. Servidores

Los servidores son de vital importancia para el buen funcionamiento de la institución, del banco de servidores, algunos cuentan son soporte externo, mientras que los siguientes estan a cargo del departamento de informática:

Tabla I.
Servidores que cuentan con el mantenimiento del departamento de informática

Marca	Servidor	Importancia
HP PROLIANT		Alta
Virtualizado	Active Directory-Antivirus-DNS	Alta
Virtualizado	Correo	Alta
RouterBoad Mikrotik 1100AHx2	Router-Firewall-DHCP	Alta

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.

C. Topología de Red

La red se encuentra en topología en estrella, en donde cuenta con conmutadores como distribuidores centrales y un firewall. El edificio de EMAPA-I tiene 4 pisos los cuales cuentan con cableado UTP para la conexión entre los departamentos con los que cuenta cada piso. El cableado horizontal de la institución es de tipo UTP categoría 6 y 5e, los cuales están instalados en el cuarto de equipos, los servidores, y en los departamentos de la institución respectivamente.

D. Esquema de Red

El esquema de red con el que cuenta la empresa incorpora un dispositivo cortafuego, además de un conmutador Cisco que enlaza las redes virtuales con el firewall, así como se muestra en la siguiente figura:

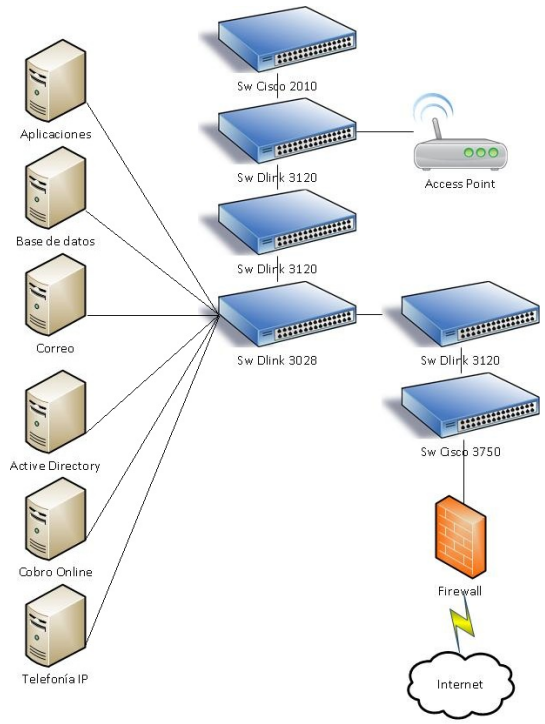

Figura 3.- Esquema de red EMAPA

IV. GESTIÓN DE LA RED LAN DE EMAPA-I

A. Establecimiento de políticas de gestión de los recursos informáticos en EMAPA-I

A continuación se detalla las políticas de gestión de red evaluadas a partir del sistema de gestión SNMP, una auditoría sistemática al departamento de recursos informáticos y las normas de control internas para las tecnologías de información las cuales tienen la finalidad de ampliar el nivel de seguridad y cumplir de mejor forma los objetivos del departamento de informática.

Niveles organizacionales

a) Jefe de Infraestructura Tecnológica.- Asegurar el mantenimiento de una alta disponibilidad y correcto funcionamiento de las plataformas informáticas que soportan las actividades de EMAPA-I para los usuarios.

b) Analista informático 1.- Ejecutar y coordinar actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones

c) Analista informático 2.- Ejecutar y coordinar actividades de soporte técnico y de mantenimiento de equipos

informáticos, tecnologías de la información y comunicaciones

Vigencia

El documento descrito con las políticas sobre la gestión de red entrará en vigencia en el momento en que éste sea aprobado como documento técnico por las autoridades correspondientes de EMAPA-I. Esta normativa deberá ser revisada y actualizada de acuerdo a los cambios en la infraestructura que pueda presentarse en la institución.

Al no existir un estándar específico para la administración de red, las políticas de gestión están realizadas en base al modelo de gestión SNMP, establecido por la IETF:

1. Política de Gestión de la red de datos
   1.1 Objetivo de la Política de Gestión.
   1.2 Compromiso de las Autoridades.
2. Gestión de Operación.
   2.1 Inventario de la red
   2.2 Configuración de equipos.
3. Gestión de Administración.
   3.1. Mantenimiento del inventario e ingreso.
   3.2. Mesa de ayuda.
4. Gestión de Mantenimiento.
   4.1. Parámetros de monitoreo
   4.2. Manejo de Fallos.
   4.3. Reportes
5. Gestión de Seguridad.
   5.1. Acceso al Software de Gestión.
   5.2. Acceso a los dispositivos de red.

B. Implementación de herramientas de gestión en la red LAN de EMAPA-I

Esta área de gestión comprende en realizar el análisis de la situación actual de la red de datos de EMAPA-I 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 Zennos, Zabbix, Cacti y Nagios. El software de gestión fue elegido en base al estándar IEEE 29148, tomando como referencia el cumplimiento del modelo de gestión SNMP y las necesidades de la entidad

Se escogió la herramienta Zabbix por las características que se evaluaron, una de las necesidades principales que justificaron su uso fue que el departamento de informática solicito una plataforma que sea configurable en su totalidad por medio de una interfaz gráfica. Además los equipos a monitorizar se encuentran en su totalidad con sistema operativo Windows, y Zabbix da muchas opciones para obtener datos de este S.O., tambien brinda establecimiento de umbrales que generan alertas cuando llegan a su límite máximo de funcionamiento y envían notificaciones de correo electrónico.

Función de operación del modelo SNMP

La entidad no contaba con un registro de inventario de equipos y configuraciones de red por lo que si se producía falla en algún dispositivo se perdía la información, y volver a configurar sin un respaldo disminuia la disponibilidad de la red.

Por lo tanto en la función de operación se realizó el inventario y descubrimiento de los equipos, nos ayudamos de la herramienta: Open Computer and Software Inventory Next Generation (OCS-NG) que es un software libre que permite a los usuarios de soporte administrar el inventario de los activos de la red, basada en un modelo cliente-servidor entre las cuales se intercambian información para obtener un diagnóstico, recopilando la información del software y el hardware instalado en los equipos de nuestra red en un sistema centralizado.

Función de administración del modelo SNMP

El personal técnico cumple con actividades dentro y fuera de la institución, por lo que si un equipo de red fallaba y los técnicos no se encontraban, la disponibilidad de red dependía de que los técnicos regresen a dar solución a dicha incidencia y de igual forma los problemas de los funcionarios no eran atendidos con prontitud.

Es por este motivo que las funciones de administración que se abarcaron están enfocadas a la implementación de un sistema de incidencias. Se escogió la herramienta GLPI el cual funciona de la siguiente manera: el funcionario ingresa a la plataforma web y emite la incidencia que puede estar relacionada con: problemas de ingreso al internet o al sistema integrado, problemas de impresión, daños con el mouse, el teclado, el teléfono, monitor, y daños relacionados con los recursos informáticos en general, por su parte el equipo de soporte, recibirá la incidencia tanto por la plataforma web como por el correo, y de acuerdo a la urgencia del problema se tomaran las debidas consideraciones para resolver la incidencia, la cual se almacenará en una base de datos tanto para obtener reportes de las acciones realizadas como para hacer un seguimiento a la incidencia producida.

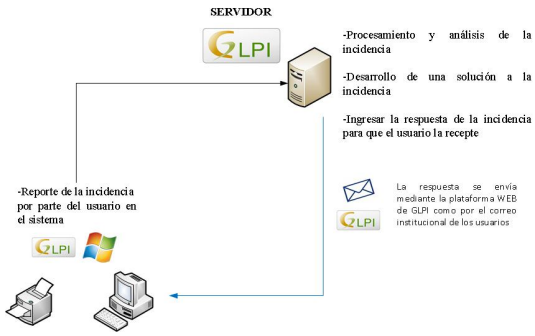

Figura 4.- Funcionamiento GLPI en EMAPA-I

Función de mantenimiento del modelo SNMP

Al no tener un control de las capacidades tanto del disco duro, ancho de banda, memoria ram, o interfaces de los servidores, si estas características se sobrecargaban, causaba retraso en la disponibilidad y confiabilidad de la red de datos hasta volverles funcionales nuevamente, y si tocaba reemplazar algún componente se producía un gasto no planificado

De tal forma que se realizó la monitorización de los equipos de encaminamiento y servidores descritos anteriormente con el fin de determinar el comportamiento de la red, a continuación se presenta la estructura de corrección de fallas que seguimos en la institución.

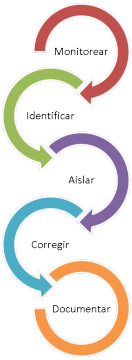

Figura 5.- Proceso de detección de fallas en EMAPA-I

Monitoreo de alarmas.- Al monitorear la red con la plataforma Zabbix, podemos identificar cual es equipo que tiene algún inconveniente y posteriormente configurar alarmas que nos indiquen que característica del equipo es la que requiere más atención, se debe considerar que configurar las alarmas para que solo nos indiquen un estado crítico, no es muy conveniente, pues el tiempo de respuesta para dar solución no siempre es inmediata, por este motivo se tiene que prever un nivel de alarmas que notifiquen al administrador mucho antes de que ocurra un incidente, o evaluar fallas menores constantes para impedir problemas más graves a futuro. (Alexander Clemm, 2007).

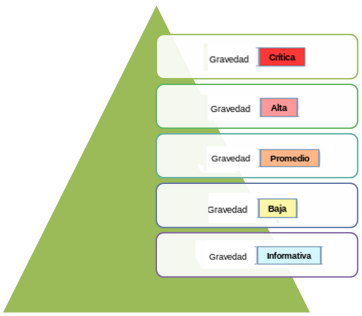

Figura 6.- Niveles de gravedad en la plataforma Zabbix

Identificación de la falla.- Al momento que se encuentra una incidencia en los equipos de red, se procederá a buscar la causa del origen del problema, los iniciadores de alamas que nos muestre la plataforma Zabbix, nos ayudará a encontrar el equipo que generó la incidencia, pero para resolverla se necesita de pruebas adicionales las cuales dependerán de conocimiento de red del administrador para que pueda proponer posibles soluciones, los equipos monitoreados presentaron las siguientes caracteristicas.

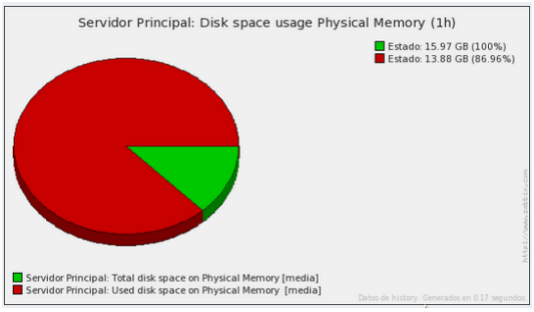

Figura 7.- Espacio de memoria RAM en el servidor Active Directory

Se puede destacar a varios equipos con nivel de gravedad critica, los cuales se revisaron y se verificó que tenían un consumo alto tanto en la memoria RAM como en el disco duro, capacidades que generaron una notificación al correo electrónico del administrador de red.

De igual forma se realizó el análisis del ancho de banda de tráfico de la red LAN, donde se constato que hay índices de uso de ancho de banda de subida más que de bajada, y esto se da, ya que la mayoria de usuarios usa la red de datos para subir archivos a los diferentes sistemas de la EMAPA-I.

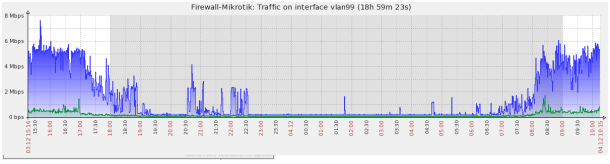

Figura 8.- Tráfico de red en la VLAN de datos

Aislamiento.- Se debe tomar en cuenta que los equipos que presentan algún inconveniente critico afectan drásticamente al funcionamiento de red, por este motivo se debería tener un documento basado en las configuraciones de los equipos o adquirir un dispositivo que sirva de respaldo para ayudar a solventar el problema por un cierto tiempo, de tal forma que se disminuya el impacto de la falla en la red de datos. (Dolores Gómez, 2014).

Corrección de la Falla.- Para dar una corrección a la falla se debe tener en cuenta la gravedad de la misma y la disponibilidad de recursos que se tenga en la empresa, entre las acciones más comunes se puede presentar las siguientes:

- Remplazo de recursos, ya sea solo la parte afectada o en su totalidad.
- Instalar actualizaciones relacionadas al incidente presentado
- Reinicio o configuración de uno o varios parámetros en específico en los equipos de red

Documentación.- Los datos que genera Zabbix se almacenan continuamente en una base de datos, y esta información puede ayudar al administrador de red para documentarla ya sea en el sistema de incidencias de GLPI, o en alguna otra plataforma que decida, ya que esta actividad dependerá principalmente del departamento de informática.

Función de seguridad del modelo SNMP

En la función de seguridad se oriento a disminuir la posibilidad de que existan incidentes, por lo tanto, en las herramientas que fueron instaladas se tomaron en cuenta las siguientes observaciones, mientras que para los demás equipos que se encuentran en la red de datos se dejó como recomendación a seguir.

- Asignación de privilegios de acceso solo aquellas personas que necesitan un constante ingreso ya sea para obtener reportes o ingresar nuevos equipos al sistema de monitoreo.
- Ingresar una contraseña robusta que integre letras, números y símbolos, para que sean más difícil de vulnerar.
- Realizar un cambio de contraseña de forma robusta a los equipos que se encuentren a su cargo cada 6 meses
- Tener un punto de restauración de los equipos en caso de alguna falla para tener un respaldo de los datos obtenidos

A. Monitoreo mediante el protocolo snmpv3

En la versión 3 de snmp se emplean campos que permiten tanto la autenticación como la encriptación de las contraseñas, para realizar el monitoreo. A diferencia de las versiones anteriores de snmp ya no se utiliza el concepto de comunidad, el cual fue cambiado por el campo de usuarios. Además cuenta con la característica de encriptación del paquete que se envía para ser procesado con el gestor, haciendo más difícil que un intruso quiera infiltrar datos con un software que despliegue el tráfico de red, como se comprobó en las pruebas realizadas.

B. Restricción de páginas web

Una vez que se tiene documentada la red de datos, se procede a denegar ciertas páginas web acorde a las políticas descritas; las cuales se establecieron mediante el estudio de la situación actual; en vista que disminuyen el rendimiento de la red y es muy común que se realice instalación de virus involuntaria mediante estas plataformas.

La configuración de estas reglas permitió controlar el tráfico de datos que circula diariamente a través de la red. También de esta manera se indicó las ventajas de aprovechar todas las funciones con lo que cuentan los equipos que se encuentran dentro de la institución.

V. MANUALES DE PROCEDIMIENTOS

Introducción

El departamento de recursos informáticos tiene por objetivo contribuir en el mantenimiento y mejoramiento de la infraestructura tecnológica, que son el apoyo fundamental para el buen manejo, funcionamiento, estructura y organización de la institución. En la actualidad existe una gran variedad de métodos en los cuales basarnos para presentar un manual de procedimientos, pero debido a la importancia que presentan tanto las entidades públicas como privadas se debe cumplir con estándares que garanticen la uniformidad tanto en el contenido, como su forma de presentación, es por este motivo que el presente manual está basado en la norma ISO.

Manual de procedimientos para la función Operación

- Objetivo.- Proporcionar la información que permita supervisar la configuración de los equipos de red y de los servidores que van a ser monitoreados
- Alcance.- Se indicará los procesos que permitan la configuración de los equipos y servidores de red para agregarlos al sistema de gestión, además se presentará los procesos que permitan agregar los computadores de usuario final al sistema de inventario.

Manual de procedimientos para la función Administración

- Objetivo.- Dar información acerca del seguimiento al inventario inicial y el reporte de incidencias de parte del usuario final mediante helpdesk
- Alcance.- Esta función se relaciona conjuntamente tanto con la gestión de operación como la gestión de mantenimiento, por lo tanto aquí se determina el seguimiento de los componentes de los dispositivos ya inventariados, y también se explicará la forma en que se procederá a recibir las incidencias que reporten los usuarios finales.

Manual de procedimientos para la función Mantenimiento

- Objetivo.- Establecer procesos que permitan la revisión de los umbrales que generan notificaciones específicas, las cuales son una base para analizar, e identificar las fallas que sucedan en los equipos monitoreados.
- Alcance.- Se establecen los umbrales que los equipos a gestionar deben mantener, y si son sobrepasados los técnicos encargados busquen una solución oportunamente permitiendo ofrecer un nivel de continuidad alto en la red.

Manual de procedimientos para la función Seguridad

- Objetivo.- Ofrecer seguridad al sistema de gestión mediante la autenticación e ingresos intransferibles a los usuarios del departamento de recursos informáticos para garantizar la integridad de la información
- Alcance.- Supervisar y vigilar los cambios del sistema de gestión revisando las amenazas o modificaciones no documentadas, previniendo los accesos no autorizados a la información.

VI. CONCLUSIONES

Al analizar los requerimientos institucionales mediante las áreas funcionales del modelo SNMP se pudieron encontrar falencias como: no contar con un inventario actualizado, no tener el control de las capacidades técnicas de sus dispositivos, ni tampoco documentación de políticas que aseguren la confiabilidad de la información de sus recursos informáticos; se puede destacar que este modelo entrega una serie de pasos bien organizados para que el personal técnico pueda identificar con exactitud los aspectos que disminuyen el rendimiento de la red con el fin de que sean solucionados a tiempo.

El monitoreo de los equipos en la red de Emapa-I se lo realizó mediante el protocolo snmpv2, ya que fue de fácil implementación tanto para los equipos de red como los servidores de la entidad; también se configuró un sistema de alarmas para indicar al departamento técnico que los umbrales establecidos en las capacidades tanto de consumo de ancho de banda, memoria RAM y disco duro se están sobrepasando, disminuyendo considerablemente el tiempo de respuesta en dar una solución.

Las herramientas que intervienen en este proyecto son orientadas a entornos libres, se tomó en cuenta los requerimientos institucionales analizados en base a la especificación del estándar IEEE 29148, la cual permitió tener una perspectiva amplia en aspectos como la detección de errores, documentación y mantenimiento de las plataformas instaladas, características fundamentales para cumplir con los objetivos planteados.

Se realizaron pruebas de funcionamiento de las plataformas instaladas las cuales ayudaron a elaborar y mantener un inventario actualizado, llevar el control de las capacidades técnicas de los dispositivos, y establecer políticas de seguridad, que son la base para cumplir los objetivos institucionales que incluyen actividades como: elaboración de informes técnicos, realizar planificaciones y organizar su infraestructura tecnológica, tomando en cuenta estándares que contribuyan a asegurar la disponibilidad de los recursos dentro de la institución

Se configuró una herramienta que permita llevar un control de incidencias, ya que no se mantenía una coordinación y documentación de las soluciones que los funcionarios solicitaban al departamento de informática, permitiendo entregar informes más detallados de las actividades realizadas por este departamento, además de agilitar los procesos de soporte a los usuarios dando un margen aproximado de 10 minutos en dar una solución a las incidencias.

Se realizaron pruebas de simulación de sobrecarga de umbrales establecidos en las capacidades tanto de consumo de ancho de banda, memoria RAM y disco duro, también se revisó el formato de envío y recepción de incidencias para verificar que tanto el sistema de alarmas al correo electrónico como las configuraciones estén en correcto funcionamiento.

Se recopiló información acerca de las características de seguridad del protocolo snmpv3 la cual se verificó mediante un análisis de protocolos con la plataforma Wireshark, en donde se demostró la encriptación y la autenticación de paquetes monitorizados; indicando a la institución los beneficios de que los ataques externos e internos puedan ser evitados oportunamente.

Para reforzar el estudio realizado del protocolo snmpv3 se ejecutaron pruebas de funcionamiento en el departamento financiero de la institución, en donde se establecieron umbrales que indiquen cuando las capacidades tanto de disco duro, o memoria RAM estén sobrecargadas; además para verificar la encriptación se utilizó la herramienta Wireshark con la que se demostró que las configuraciones de encriptación y autenticación en los dispositivos están en correcto funcionamiento.

Mediante la implementación de las plataformas destinadas al sistema de inventario, el sistema de incidencias, y el sistema de monitorización se logró elaborar los manuales de procedimiento en base a las áreas del modelo de gestión SNMP, las cuales son un conjunto de instrucciones que sirven de guía al personal técnico para mantener la red de datos de la entidad actualizada y en constante monitorización, asegurando de esta manera la disponibilidad de funcionamiento de sus recursos informáticos.

De acuerdo a los resultados obtenidos en la situación actual donde se destacan falencias como: no contar con un inventario actualizado y no tener el control de las capacidades técnicas de sus dispositivos; se establecieron políticas que cubran las funciones del modelo de gestión SNMP el cual cuenta con ciertas directrices que permiten al administrador de red manejar los recursos informáticos de la institución de forma eficiente, generando cambios significativos, ya que por medio de estas políticas y procedimientos se mostrará como una entidad que oferta servicios con continuidad y calidad a la comunidad.

REFERENCIAS

Subramanian, A & Timothy A. (2010). Network Management. 2da edición. Sitio de Publicación: Pearson Education India

Douglas, M. & Schmidt K. (2009). Essential SNMP. 2da. Edición. Sitio de publicación: O'Reilly Media.

Molero, L. & Villaruel M. (2010). Planificación y gestión de red. Recuperado el 14 de febrero del 2015 de: http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-I.pdf

Orozco P. (2010). Gestión y organización de sistemas y redes de comunicaciones en el departamento de T.I. Recuperado el 15 de febrero del 2015 de: http://www.slideshare.net/pakus/gestion-de-red

RFC 1901. (1996). Introduction to Community-based SNMPv2. Recuperado el 10 de marzo del 2015 de: https://www.ietf.org/rfc/rfc1901.txt

RFC 2578. (1999). Structure of Management Information Version 2 (SMIv2). Recuperado el 10 de marzo del 2015 de: https://www.ietf.org/rfc/rfc2578.txt

RFC 2570. (1999). Introduction to Version 3 of the Internet-standard Network Management Framework. Recuperado el 5 de abril del 2015 de: https://www.ietf.org/rfc/rfc2570.txt

RFC 3411. (2002). An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Recuperado el 10 de abril del 2015 de: https://www.ietf.org/rfc/rfc3411.txt

Nació en Ibarra provincia de Imbabura el 22 de abril de 1980. Ingeniero en Sistemas Computacionales, Universidad Técnica del Norte – Ecuador en 2006. Actualmente es docente en la carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra – Ecuador, obtuvo la Maestría en Redes de Comunicación en la Pontificia Universidad Católica del Ecuador, Quito – Ecuador.

Nació en Atuntaqui el 21 de Septiembre de 1987, sus estudios secundarios lo realizó en el Colegio Nacional Técnico Mariano Suarez Veintimilla, donde obtuvo el título de Bachiller en Comercio y Administración especialidad aplicaciones informáticas. En 2006 ingresó a la Universidad Técnica del Norte en la que realiza sus estudios en la carrera de Electrónica y Redes de Comunicación. Actualmente es egresado de la Universidad Técnica del Norte .