"ADMINISTRACIÓN Y GESTIÓN DE LA RED DE ÁREA LOCAL DEL GADIP MUNICIPIO DE CAYAMBE, BASADO EN EL MODELO FUNCIONAL DE GESTIÓN DE RED ISO/OSI CON EL PROTOCOLO SNMP Y USO DE HERRAMIENTAS DE SOFTWARE LIBRE" (DICIEMBRE 2015)

Sandra K. Narváez, Cyntia M. Inuca.

***Resumen*—El presente proyecto, se ha desarrollado con el objetivo de ayudar a mejorar la disponibilidad de la red de área local, del GADIP Municipio de Cayambe, a través del modelo funcional de gestión de red ISO/OSI, y sus áreas de gestión; configuración, seguridad, fallos, rendimiento, y contabilidad, la cual permite administrar la red de forma organizada, e indica las funciones que se debe gestionar.**

Para la administración de la red se ocupan herramientas de software libre, como son Zentyal y Zenoss, que ayudan a monitorear las áreas de gestión del modelo antes mencionado, Zenoss actúa como estación gestora, el cual recopila información de los dispositivos que forma parte de la red, el rendimiento de sus recursos, inventarios, notificación de eventos y fallas producidas mediante correo electrónico, en cuanto a seguridad, Zentyal proporciona una plataforma de varios servicios en un solo sistema operativo, se aplica funciones de firewall, IDS/IPS, control de usuarios mediante OPEN LDAP junto a un portal cautivo. En este proyecto se utiliza el concepto del protocolo de administración de red simple, SNMP versión 2, el cual se habilitan a todos los dispositivos gestionados, para que puedan enviar al gestor la información del funcionamiento de sus recursos, y así el administrador pueda controlar las actividades de la red.

Todo esto forma parte de un sistema de gestión de red, que funciona en un centro de monitoreo y administración de red ubicada en el departamento de TIC de la institución, la cual se rigüe mediante políticas y procedimientos establecidos para administrar la red. Se ha planteado también un diseño de segmentación de la red, como una alternativa para mejorar la administración de la red.

***Términos indexados*—LAN, ISO, OSI, SNMP, IETF, TCP/IP, ITU, SMI, MIB, OID.**

I. INTRODUCCIÓN

El Gobierno Autónomo Descentralizado Intercultural y Plurinacional (GADIP) del Municipio de Cayambe es un ente público que brinda servicios a la ciudadanía, junto al departamento de Tecnologías de la Información y Comunicación (TIC) trabajan para mejorar la prestación de servicios de comunicación dentro de la institución, a través de la mejora de la infraestructura de la red de datos, e implementación de recursos tecnológicos.

El departamento de las TIC debe estar pendiente de la disponibilidad de la red, pero su función se ha visto complicada, ante la numerosa cantidad de usuarios y equipos adicionales instalados de manera que ha crecido de una forma no planificada y no estructurada. La falta de monitoreo adecuada de la red, provoca que al existir un problema sea difícil identificar la causa, por lo que deben ir personalmente a verificar el funcionamiento de equipos, configuraciones, y la infraestructura de red para detectar el problema. Tampoco lleva un control de estado de los recursos de la red y tráfico que circula por ella, que permita tomar medidas preventivas que controlen y resuelvan cualquier eventualidad que perjudique al desempeño de la red. La red de área local (LAN) de la institución no cuenta con segmentación, que permita una correcta administración, todos los equipos y servidores se encuentran bajo un mismo esquema de direccionamiento IP, el incremento de nuevos usuarios de red y necesidad de servicios que demanda el municipio requieren escalabilidad.

Debido a estos inconvenientes el presente proyecto propone la administración y gestión adecuada de la LAN basándose en el Modelo Funcional de Gestión de Red ISO/OSI utilizando el protocolo SNMP y herramientas de software libre, que tengan características de monitoreo.

Esta investigación se la realizó como proyecto previo para obtener el título Ingeniera en Electrónica y Redes de Comunicación carrera de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.
S.K. Narvaez, Docente de la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electronica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador (e-mail: sknarvaez@utn.edu.ec). C.M.Inuca, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (e-mail: mab_c6@yahoo.es).

II. FUNDAMENTOS TEÓRICOS

A. *Conceptos Fundamentales.*

No es lo mismo, administrar que gestionar, pero son conceptos que se complementan para asegurar el correcto funcionamiento una red, así como algunos conceptos más.

1) *Administrar.*

Significa organizar, dirigir, y controlar los recursos de una entidad, ya sea humano, financiero, tecnológico, o de conocimiento, para garantizar un nivel de servicio y mantener operativa la red.

2) *Gestionar.*

Significa asignar acciones o actividades a cada recurso que dispone para cumplir un objetivo, tal como es el mejoramiento de la operatividad de la red, uso eficiente de la red y sus recursos, hacer que sea más segura y controlar los cambios que se produzcan.

Según Saydam en su artículo de la revista Journal of Network and Systems Management "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 y los elementos necesarios para satisfacer los requisitos de respuesta en tiempo real, de rendimiento operacional y de calidad de servicio a un precio razonable." [1]

3) *Planificación de red.*

La planificación de redes consiste en actividades que anticipen las necesidades de la red, se toma criterios de una nueva instalación de red o modificación de la red existente, de acuerdo a la situación que se presente.

4) *Control de red.*

El control de redes implica la vigilancia cotidiana de la red para asegurar que mantenga el nivel de operación deseado. El control de redes incluye procedimientos como la detección de fallos, aislamiento de fallos y la restauración de la red. [2]

5) *Monitoreo de red.*

Es la supervisión, observación y análisis del estado de los componentes de la red, orientado a obtener información de la red, tráfico que circula por ella, para la detección preventiva de problemas, agilizando el proceso de los esfuerzos para la resolución de los problemas futuros.

B. *¿Por qué gestionar la red?*

La necesidad de gestionar las redes surge por diferentes causas como:

- Crecimiento de las redes.
- Entornos de red heterogéneos.
- Aumento de tráfico de red.
- Difícil diagnóstico de problemas en entornos grandes.
- Necesidad de herramientas de gestión de redes.
- Necesidad de un conjunto de reglas estandarizadas que gobierne la identificación y suplan acciones automatizadas para las diversas situaciones comunes que se presentan en la red.
- Aumento de expectativas de usuarios de una red confiable, segura, rápida y operacional.

C. *Objetivos de Gestión.*

Los objetivos principales de la gestión de red consisten en mejorar:

- La disponibilidad
- El rendimiento de los elementos del sistema,
- e Incrementar su efectividad.

D. *Modelos de gestión de red.*

- **Gestión de internet** definido por la IETF[1], basado en SNMP[2] para redes TCP/IP[3].
- **Arquitectura TMN[4]** definido por la ITU[5] para gestión de redes de telecomunicaciones.
- **Gestión de red OSI[6]** definida por la ISO[7] como un modelo de referencia general para entornos de red OSI.

1) *Modelo funcional de gestión de red OSI.*

El modelo de gestión de red OSI, presenta su modelo funcional, más conocido como modelo FCAPS, este es un modelo bien estructurado que divide las funciones de administración de redes, en cinco áreas de gestión.

Gestión de configuración.

El objetivo de la gestión de configuración es obtener datos de la red y utilizarlos para incorporar, mantener y retirar los distintos componentes y recursos a integrar. Consiste en la realización de tres tareas fundamentales:

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

[1] IETF, Internet Engineering Task Force, es una organización internacional abierto de normalización.

[2] SNMP, Simple Network Management Protocol, es un protocolo para administración de redes.

[3] TCP/IP, Transmission Control Protocol/Internet Protocol, es un modelo de arquitectura de red, con una familia de protocolos.

[4] TMN, Telecommunication Management Networks, es un protocolo para administración de sistemas abiertos.

[5] ITU, International Telecommunication Union, encargada de regular las telecomunicaciones a nivel internacional.

[6] OSI Open System Interconnection, es un modelo de interconexión de sistemas abiertos, creado por la ISO para resolver problemas de compatibilidad de hardware y software, de forma que ayude a los diseñadores de red implementar redes que puedan comunicarse y trabajar en conjunto, compatibles e interoperables.

[7] ISO International Organization for Standardization, es el organismo internacional de estandarización.

Gestión de fallos.

La gestión de fallos comprende la detección, el aislamiento y la corrección de fallos, así como la corrección de la operación anormal. Incluye funciones para:

- Mantener y examinar registros de error (error logs);
- Aceptar notificaciones de detección de error y reaccionar a las mismas;
- Rastrear e identificar fallos;
- Efectuar secuencias de pruebas de diagnóstico; y
- Eliminar fallos.

Gestión de contabilidad.

La gestión de contabilidad tiene como misión la medida de parámetros de utilización de la red que permitan a su explotador preparar las correspondientes facturas a sus clientes. Entre las tareas que se deben realizar en esta área, están:

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

Gestión de rendimiento o prestaciones.

La gestión de rendimiento permite evaluar el comportamiento de recursos que conforman la red, su objetivo principal es mantener el nivel de servicio que la red ofrece a sus usuarios, asegurándose de que está operando de manera eficiente en todo momento. La gestión de prestaciones se basa en cuatro tareas:

- Recolección de información estadística, tales como el troughput de la red, los tiempos de respuesta o latencia, etc.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.
- Determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

Gestión de seguridad.

La gestión de seguridad tiene como finalidad establecer mecanismos y políticas de seguridad orientadas a proteger la red, contra ataques de intrusos. Entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Identificación de recursos sensibles en la red, tales como ficheros o dispositivos de comunicaciones.
- Determinación de las relaciones entre los recursos sensibles de la red y los grupos de usuarios.
- Monitorización de los puntos de acceso a los recursos sensibles de red.
- Almacenamiento de los intentos de acceso no autorizados a estos recursos, para su posterior análisis. [3] [4]

E. Sistema de gestión de red.

Un sistema de gestión de red es un conjunto de herramientas para supervisar y controlar la red, de forma integrada. Se compone de hardware y software adicionales implementados en los componentes de red existentes, diseñado para ver la red como una arquitectura unificada.

1) Elementos de un sistema de gestión de red.

Estación de gestión o gestor.

Es el equipo principal donde se monitoriza las actividades de la red y su comportamiento, permite la recopilación, procesamiento, análisis y/o visualización de la información de gestión de la red. El gestor envía mensajes o solicitudes para realizar determinadas acciones e interactúa con los dispositivos que forman la red.

Dispositivo gestionado.

Es el equipo que contesta a esos mensajes con información sobre su funcionamiento actual o indicando si la operación solicitada se ha completado satisfactoriamente. Ejemplo: Router, switch, hub, PC, impresoras, etc.

Dentro de los dispositivos gestionados están:

- **Objetos gestionados:** Son elementos hardware como una tarjeta de interfaz de red, cada objeto gestionado tiene un identificador (OID), y este se identifican dentro de un árbol MIB.
- **Agente:** Es un software que reside en el dispositivo gestionado y que se comunica con el gestor, llevando a cabo acciones locales en el dispositivo gestionado bajo control de la estación de gestión.
- **Protocolo de gestión de red:** El protocolo se ejecuta entre la entidad gestora y los dispositivos gestionados, permite consultar el estado de los dispositivos gestionados y llevar a cabo acciones de manera indirecta en estos dispositivos a través de sus agentes. [5] [6]

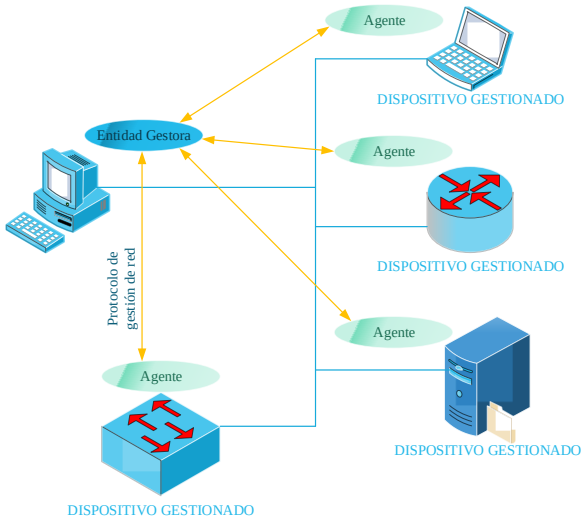

Fig. 1. Elementos de un sistema de gestión de red
Fuente: James Kurose. (2013).Redes de Computadoras. Editorial: PEARSON.

F. Protocolo de gestión de red simple (SNMP).

SNMP (Simple Network Management Protocol), es un protocolo de aplicación, que permite gestionar la red mediante intercambio de información de gestión de red, entre las entidades de gestión (gestor/agente), basado en solicitud/respuesta.

Junto al protocolo SNMP, también se definen la estructura de información de gestión (SMI) y la base de información de gestión (MIB).

1) Estructura de información de gestión (SMI).

Para obtener la información de gestión se usa el método de identificadores de objetos *(OID, Objetc Identifier)*, que permite alcanzar objetos siguiendo la secuencia de un árbol, obteniendo el tipo de dato que usa en la MIB.

La información de gestión es comunicada a través del protocolo SNMP, representada con el lenguaje ASN.1[8]

2) Base de información de gestión (MIB).

Es información virtual alojada en objetos gestionados, cuyos valores reflejan colectivamente el estado actual de la red.

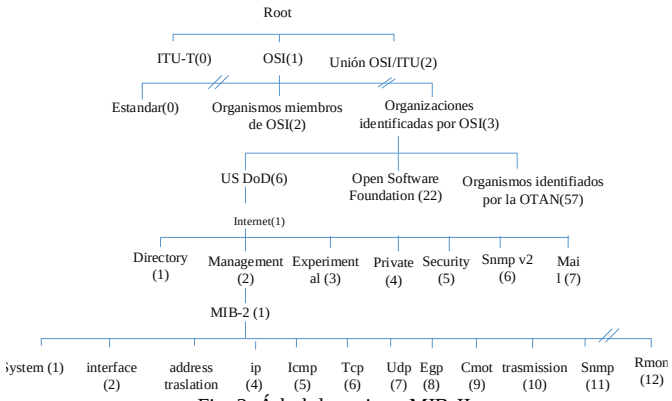

Fig. 2. Árbol de registro MIB-II.
Fuente: James Kurose. (2013).Redes de Computadoras. Editorial: PEARSON. Estados Unidos.

3) Funcionamiento de la arquitectura SNMP.

La estación de gestión de red ejecuta aplicaciones de administración, que monitoree y controle los elementos de red. Los elementos de red son dispositivos tales como: host, gateways, servidores, etc., donde tiene alojado el software agente encargado de desempeñar funciones de gestión solicitadas por la estación gestora. El Simple Network Management Protocol (SNMP) se utiliza para comunicar la información de gestión entre la estación de gestión de red y los agentes en los elementos de red.

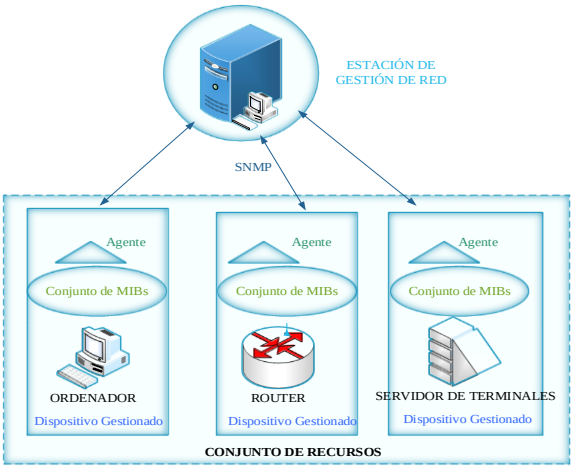

Fig. 3. Arquitectura de gestión SNMP.
Fuente: Antoni Barba. (1999). Gestión de red. Ediciones UPC. Barcelona.

Comunicación entre entidades de gestión.

La comunicación de información de gestión entre entidades de gestión se realiza a través de mensajes SNMP. Usa el protocolo de transporte UDP, los mensajes son enviados a través de un datagrama UDP. El gestor envía un mensaje por el puerto 161 UDP, y el agente recibe el mensaje por el puerto 162.

Operaciones SNMP.

La estación de gestión puede enviar los siguientes mensajes:

- **GetRequest:** Obtiene el valor de uno o más objetos MIB.
- **GetNextRequest:** Obtiene el valor de un objeto MIB puede moverse en una lista o tabla MIB.
- **GetBulk Request:** Obtiene el valor en un bloque grande de datos. El gestor obtiene una respuesta que sea tan grande como sea posible.
- **InformRequest:** un gestor proporcionar información de gestión (valores MIB) a otra entidad gestora.
- **SetRequest:** asigna o establece el valor de uno o más objetos MIB.

El agente puede enviar los siguientes mensajes:

- **GetResponse:** devuelve los valores solicitados por las operaciones anteriores.
- **Trap (notificación):** permite a un agente enviar a la estación de gestión notificaciones no solicitadas sobre eventos importantes.

Relaciones administrativas SNMP.

- **Comunidad SNMP:** se denomina comunidad a un conjunto de gestores y los dispositivos gestionados. A las comunidades se les asigna nombres, de tal forma que este nombre junto a cierta información adicional sirva para validar un mensaje SNMP y al emisor del mismo.

[8] ASN.1 es una notación formal utilizado para describir los datos transmitidos por protocolos de telecomunicaciones, independientemente de la implementación del lenguaje y la representación física de estos datos, cualquiera que sea la aplicación, ya sea compleja o muy simple.

- **Servicio de autenticación:** el agente puede limitar el acceso a las MIB a los gestores autorizados.
- **Políticas de acceso:** Es la asociación de la comunidad snmp, modo de acceso, y una vista MIB. El agente podría aplicar privilegios de acceso diferentes a diferentes gestores.
    - **Modo de acceso:** especifica cómo se accede a los dispositivos de la comunidad, los modos de acceso son: sólo lectura, lectura-escritura o sólo escritura.
    - **Una vista MIB:** define uno o más sub-árboles MIB a los cuales una comunidad SNMP específica puede tener acceso.
- **Servicios proxy:** un agente puede actuar como un proxy hacia otro agente.

4) Versiones de SNMP.

SNMP v1.

Es la primera versión estándar del protocolo SNMP, definido por la IETF, en el RFC 1157,1155, y1212. Define la arquitectura SNMP conformado por la estación de gestión y los elementos de gestión o dispositivos gestionados. Para la trasmisión de mensajes utiliza servicio no orientado a conexión por protocolo UDP, los mensajes son enviados en un datagrama UDP, usa las operaciones ***GetRequest, GetNextRequest, GetResponse, SetRequet y Trap***. Su funcionamiento se basa en comunidades como un método de seguridad. Su uso se expandió enormemente, y se empezó a notar algunas deficiencias, por lo que surge SNMP v2.

SNMP v2.

Es una versión mejorada que pule las deficiencias de la primera versión, se definen en los RFC 1905, 1906,1907. Su funcionamiento sigue basándose en comunidad, se realizan lagunas mejoras de operaciones de protocolo, respecto a la estructura de información de gestión SMIv2, que extiende el árbol de objetos añadiendo SNMPv2 al subárbol de internet, también tiene la capacidad de interacción gestor-gestor, en esta versión puede manejar siete tipos de operaciones SNMP PDU, GetRequest, GetBulkRequest, GetNextRequest, GetResponse, SetRequet InformRequest y Trap. Sin duda una de las mejoras más importantes en SNMP v2 es GetBulkRequest es minimizar el número de intercambios del protocolo requeridos para obtener gran cantidad de información de gestión, permite a un gestor SNMPv2 solicitar que la respuesta sea tan grande como sea posible, dadas las restricciones del tamaño del mensaje, e InformRequest transmite información no solicitada entre estaciones de gestoras.

SNMP v3.

SNMP v3, elimina el concepto de comunidad, tiene su enfoque principal en la seguridad, proporcionando tres servicios importantes: autenticación, privacidad y control de acceso, los cuales trabajan en una arquitectura modular. Los dos primeros forman parte del modelo de seguridad basada en el usuario (USM, User-Based Security), utiliza algoritmos como MD5 o SHA1 y DES, y el último se define en el modelo de control de acceso basado en vistas (VACM, View- Based Access Control Model), se encarga de controlar el acceso a los objetos MIB.

Mantiene su principio de arquitectura, con nuevas convenciones textuales, conceptos y terminologías.Los gestores y agentes se llaman entidades SNMP**,** cada entidad consiste de un motor SNMP y una o más aplicaciones SNMP. [7] [8]

5) Ventajas SNMP.

- Se puede tomar como una ventaja que SNMP es actualmente el protocolo de gestión de redes más usado convirtiéndose en un estándar de mercado.
- Actualmente los fabricantes de equipos de comunicación dan soporte para todas las versiones de SNMP.
- Posee un diseño simple, fácil de implementar y comprender para programadores.
- No consume muchos recursos.
- Tiene capacidades generales de monitorización y control.

6) Desventajas SNMP.

- Consumo de mayor ancho de banda en entornos extensos de red, lo cual no permite optimización de tráfico de red. (versión 1)
- La versión original no permite la transferencia de grandes cantidades de datos, lo cual se mejora en la versión 2, permitiendo mayor eficiencia de tráfico.
- Una de las principales desventajas de snmp es que tiene funcionalidades limitadas y el nivel de seguridad muy bajo en las versiones 1 y 2, lo que se ha corregido ya en la última versión SNMP v3, dando lugar a conceptos de: autenticación, privacidad y control de acceso, pero aumenta su complejidad de configuración.

G. Funciones del administrador en un entorno LAN.

Las labores de un administrador de red son muy importantes ya que de él depende el buen funcionamiento de la red, muchas veces el trabajo se divide entre un grupo de personas, sin embargo, es necesario la designación de un responsable, que conozca la red en su totalidad.

Las tareas que debe realizar el administrador de la red son:

- Planificación de la red.
- Preparación de red.
- Organización y configuración.
- Gestión de cambios.
- Gestión de problemas.
- Seguridad.
- Optimización.
- Mantenimiento de la documentación.
- Documentación de mantenimiento.
- Monitorización y control de tráfico.

[9]

III. Análisis de la Situación Actual

Se recopila información respecto a las condiciones actuales en la que se encuentra la red de área local (LAN) del Gobierno Autónomo Descentralizado Intercultural y Plurinacional del Municipio de Cayambe (GADIPMC), con el objetivo de conocer sus necesidades y requerimientos para mejorar la administración de la red.

A. Gobierno Autónomo Descentralizado Intercultural y Plurinacional del Municipio de Cayambe (GADIPMC).

El GADIPMC se encuentra ubicado en el cantón Cayambe, provincia de Pichincha, es una entidad pública que tiene como objetivo servir a la comunidad cayambeña, promoviendo el desarrollo equitativo, solidario y sustentable del territorio, la integración y participación ciudadana, así como el desarrollo social y económico de la población.

Maneja y administra fondos, bienes y recursos públicos, emprende, planifica, gestiona y ejecuta proyectos con el fin de mejorar la calidad de vida de los ciudadanos, cumpliendo su lema "Juntos por el buen vivir".

1) Dirección de Tecnologías de la Información y Comunicación.

La dirección de TIC del GADIPMC es la entidad encargada del desarrollo y crecimiento del área tecnológica de la institución.

Estructura.

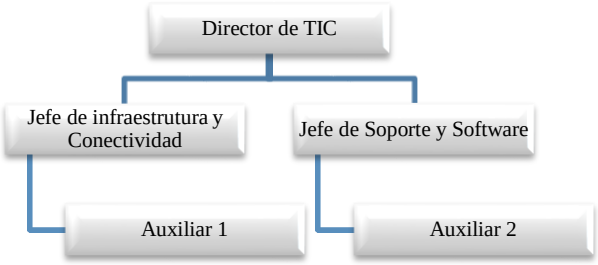

Fig. 3. Estructura de la Dirección de TIC-GADIPMC
Fuente: Dirección de TIC del GADIPMC

2) Dependencias municipales interconectadas a la LAN.

El Municipio de Cayambe cumple diversas funciones a través sus departamentos ubicados en los:

- Edificio principal;
- Edificio Espinoza Jarrín;
- Dependencias ubicadas en otros sitios de la ciudad.
- Entidades independientes.

Estas dependencias forman parte de la LAN, a través del cual los usuarios están interconectados, con acceso a servicios de red e internet, archivos compartidos, impresoras, etc.

Existen alrededor de 230 usuarios que pertenecen a la red interna del municipio, los cuales tienen asignado una dirección IP, sin considerar aun equipos que utilizan direccionamiento IP.

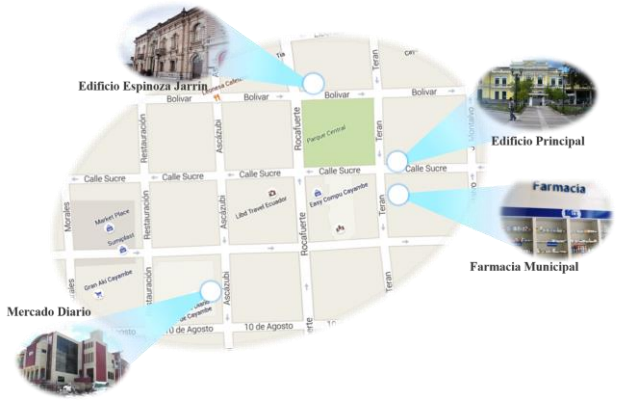

Fig. 4. Ubicación de dependencias del GADIPMC.
Fuente: Adaptado de Google Maps.

B. Infraestructura física de la LAN.

La infraestructura física de una red es la base sobre la que se constituyen todas las redes, conformado por diferentes medios de trasmisión, dispositivos de comunicación (enrutamiento/conmutación), equipos de usuarios final, etc.

1) Características Generales.

A continuación se describe los elementos físicos de la red local del GADIPMC.

- Cuenta con un Data Center donde se localizan los siguientes elementos:
  - Switchs.
  - Firewall.
  - Servidores.
  - Aire Acondicionado.
  - Tablero de distribución de energía.
  - UPSs.
- Varios racks albergan los equipos de conmutación.
- Maneja una topología estrella.
- Los medios de trasmisión usados son:
  - Cable de par trenzado UTP Cat 5e y Cat 6A.
  - Fibra óptica.
- El edificio principal cuenta con 140 puntos de red de datos certificados y respectivamente etiquetados.
- El edificio Espinoza Jarrín, y demás dependencias carece de un buen dimensionamiento de cableado estructurado.

C. Estado lógico de la red

Para la revisión del estado lógico de la red se detalla aspectos como direccionamiento IP, un diagrama sobre la topología de red, y se monitorea la red para conocer en qué estado se encuentra e identificar sus falencias.

1) Direccionamiento IP

Actualmente se usa un direccionamiento IPv4 privado clase C, que es distribuido a los usuarios de la LAN de forma estática, el personal de la Dirección de TIC son los encargados de esta labor y de mantener el control del rango de direcciones IP disponibles.

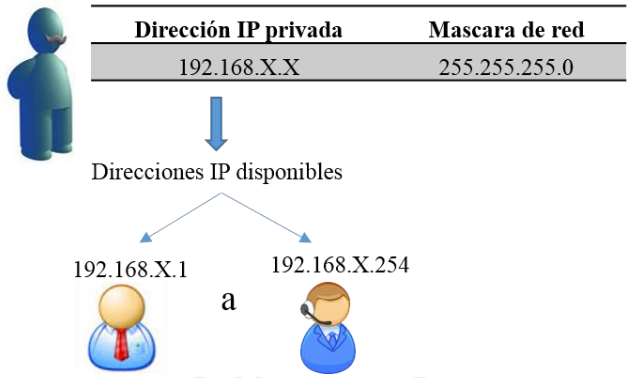

Fig. 5. Direccionamiento IP.
Fuente: Obtenido de http://www.marbit.es/index_ip.html.

2) Topología lógica de la LAN.

Se maneja una topología estrella, siendo el equipo central el firewall, a partir del cual se conforma la red local, con la conexión de varios equipos de conmutación para llegar a los usuarios finales.

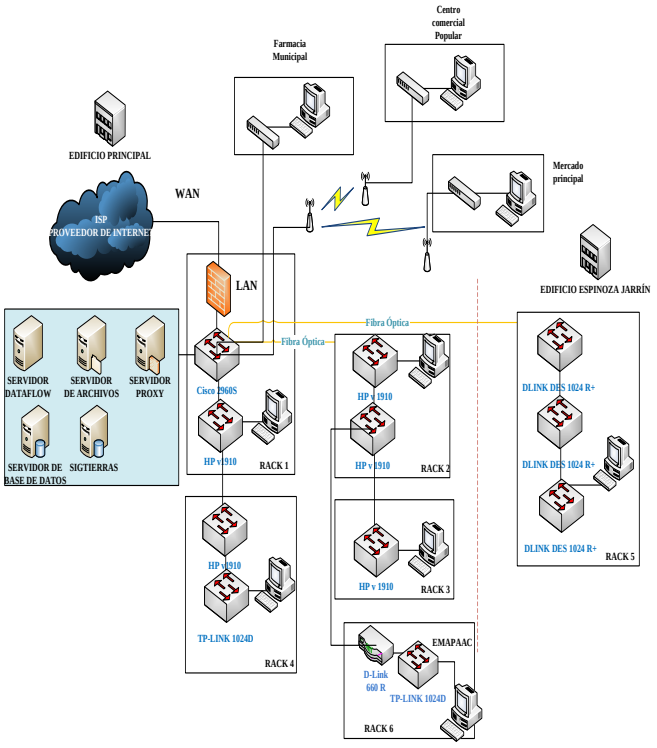

Fig. 6. Topología Lógica de la LAN del GADIPMC.
Fuente: Departamento de TIC del GADIPMC.

3) Monitoreo de red

Para extraer la información del estado actual de la red se monitorea la red a través de un software de gestión libre elegido por la IEEE 29148.

Zenoss.

Zenoss en un software que permite monitoreo de una infraestructura de red, sus funcionalidades son:

- Descubrimientos y configuración.
- Rendimiento y disponibilidad.
- Fallas y administración de eventos.
- Alertas y remediación.
- Reportes.

Para el monitoreo de la red actual no se realizó ningún tipo de configuración del protocolo SNMP, aprovechando la función de auto descubrimiento se ingresa el rango de direccionamiento IP de la red, a continuación se detallará que resultados se obtuvo, siguiendo las funcionalidades de Zenoss.

Dispositivos descubiertos.

Zenoss permite el auto descubrimiento de la red, ingresando el rango de direccionamiento IP de la red local se pudo conocer aproximadamente cuantos usuarios están conectados en tiempo real y el direccionamiento IP asignado a cada uno de ellos.

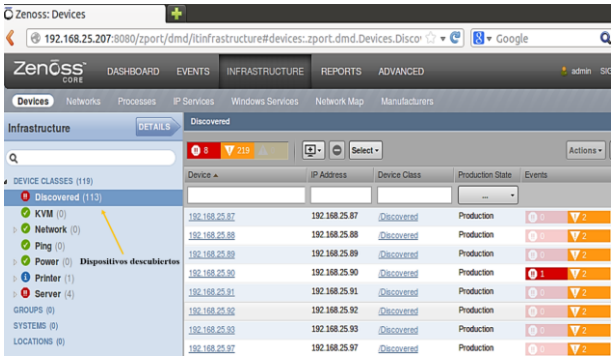

Fig. 7. Autodescubrimiento de la LAN.
Fuente: Servidor Zenoss.

Redes.

Se descubre la red y sus dispositivos, así como subredes interconectadas a la red local, se observa una sub red la cual se constató que pertenece a EMAPPAC, institución independiente a la cual el municipio provee de internet.

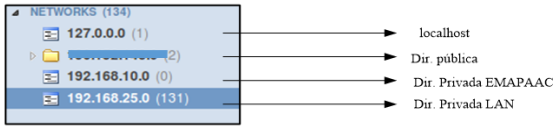

Fig. 8. Redes descubiertas.
Fuente: Servidor Zenoss.

Eventos y reportes.

En el área de eventos y reportes, el software nos indica que no está habilitado el protocolo SNMP en los equipos descubiertos, lo cual, para mejorar la administración de la LAN y poder obtener datos sobre los equipos gestionados hay que habilitar.

	192.168.25.19	snmp	/Status/Snmp	SNMP agent down
	192.168.25.16	snmp	/Status/Snmp	SNMP agent down
	192.168.25.17	snmp	/Status/Snmp	SNMP agent down
	192.168.25.13	snmp	/Status/Snmp	SNMP agent down
	192.168.25.11	snmp	/Status/Snmp	SNMP agent down
	192.168.25.18	snmp	/Status/Snmp	SNMP agent down
	192.168.25.51	snmp	/Status/Snmp	SNMP agent down

Fig. 9. Estado del protocolo SNMP.
Fuente: Servidor Zenoss.

Topología de red.

Automáticamente se obtiene una topología de los equipos que tenían activado el protocolo SNMP, con comunidad *public*, estas son algunas de las impresoras de red que se utilizan en las instalaciones del municipio.

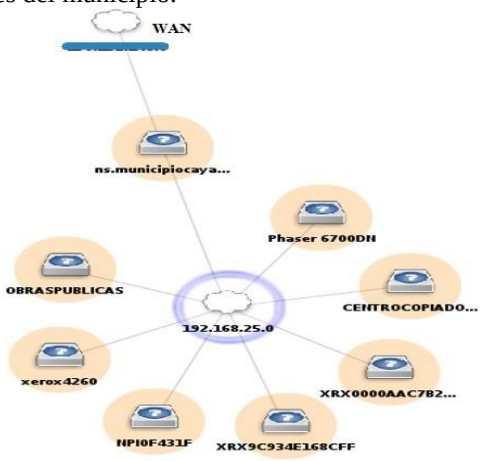

Fig. 10. Topología LAN.
Fuente: Servidor Zenoss.

Rendimiento.

El Firewall tiene habilitado por defecto el protocolo SNMP con la comunidad *public*, en el que se pudo hacer una importante observación, se visualizó el estado de las interfaces del firewall, la interfaz asignada a la LAN del GADIPMC, dispone de 7.92 MB como máximo de ancho de banda el cual se distribuye a los usuarios para conexión a internet, pero se puede observar que no se ocupa toda su capacidad, comprobando que no supera los 2 MB.

La dirección de TIC no está al tanto de configuraciones que limiten el ancho de banda por lo cual es preocupante saber la causa de este resultado.

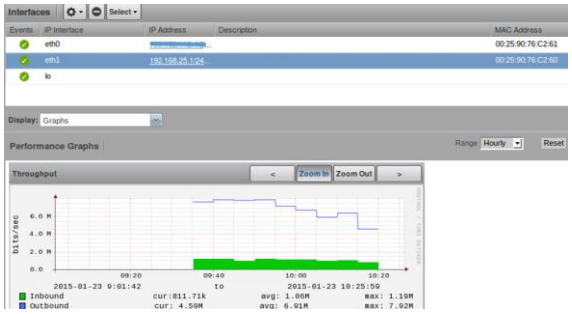

Fig. 11. Estado de interfaces firewall.
Fuente: Servidor Zenoss.

D. Análisis de las encuestas realizadas a los usuarios

Para conocer el nivel de satisfacción de los usuarios de la red se aplicó encuestas a un grupo de personas, funcionarias de la municipalidad, se aplica preguntas entorno a las áreas de:

Gestión de fallos, pues el departamento de TIC brinda soporte técnico a los usuarios, los cuales comunican cualquier problema relacionado a conexión a internet, aplicaciones de los servidores, problemas en los equipos, etc. Las preguntas se las realiza entorno a:

- La atención al problema reportado.
- Detección del problema.
- Resolución del problema

Gestión de rendimiento, los usuarios son quienes más evalúan la velocidad de conexión a internet, y la funcionalidad de las diversas aplicaciones que se provee a través de la red. Las preguntas se las realiza entorno a:

- Velocidad de conexión a internet; y
- aplicaciones de servidores de red.

1) Resultados y análisis.

A continuación se hace un breve resumen de los resultados estadísticos y un análisis de las respuestas que dieron los usuarios.

Atención a problemas.

En este ítem se ve necesidad de mejorar la atención a los problemas que tiene los usuarios, ya que existe un porcentaje mayoritario 47% que manifiesta que es a veces que el departamento de TIC atiende sus requerimientos.

Detección y resolución de problemas.

El personal encargado de resolver el problema debe realizar un diagnóstico del problema y detectar la causa, varias veces depende del tipo de problema que se suscite.

Si los problemas son fáciles se los resolverá rápidamente, un 49% manifiesta que si se realiza la detección rápida, cuando los problemas suscitados son complejos, toma tiempo resolverlos correspondiente al 34% que manifiestan que se demora mucho, y si no es posible identificarlos pues tomaran el tiempo necesario para resolver el problema.

Velocidad de internet.

Se requiere mejorar la velocidad de conexión a internet, el 40% manifiesta que es lenta por lo que hay que tomar medidas para controlar el ancho de banda, y mejorar su velocidad.

Servicios de red.

Es importante que los servicios que se den a través de la red local, estén siempre disponibles, existe un 78% que manifiesta que no tienen ningún inconveniente, demostrando que están funcionando bien.

Satisfacción de los usuarios.

Varios usuarios encuestados están satisfechos con la labor que desempeñan el departamento de TIC, pero también existen usuarios que indican estar poco satisfechos (30%) y no satisfechos (30%), el departamento de TIC, debe verificar que todos tengan los servicios de red necesarios de acuerdo a la labor del funcionario, proveer internet y mantenerlo disponible constantemente, de manera que ese porcentaje se reduzca.

E. Necesidades y requerimientos de la LAN

Tabla 1.Necesidades y requerimientos LAN GADIPMC.

Problema	Necesidades	Requerimientos	Solución
Incremento del número de usuarios.	Mayor número de puntos de red.	Reestructuración del sistema de cableado estructurado del municipio de Cayambe.	Segmentación de la red.
Saturación del rango de direcciones IP disponibles.	Incrementar el rango de direccionamiento IP.	Dimensionar el direccionamiento IP, con escalabilidad.	
Firewall limitado.	Tener el control sobre las configuraciones del firewall.	Mejorar el firewall, que el administrador tenga el control total sobre sus configuraciones.	Servidor Zentyal.
	Proxy transparente	Restricción de páginas web https.	
La red se torna lenta, y el ancho de banda esta sub ocupado.	Evitar el mal uso del internet y controlar el ancho de banda de la red.	Mejorar la velocidad de conexión a internet y controlar el uso de ancho de banda.	
Demasiado tiempo de resolución de problemas.	Atender los requerimientos de los usuarios en el menor tiempo posible.	Prevenir y detectar fallos en la red.	Servidor de monitoreo de red.
Ausencia de información sobre funcionamiento de la red.	Recopilación de información referente al uso de recursos de red.	Monitoreo de la red, mediante un software de gestion,	
	Llevar documentación del de la red y su infraestructura.	Manuales sobre configuración y uso de equipos y servidores. Llevar inventarios.	Manuales de configuración y uso de servidores. (Zentyal y Monitoreo)

Fuente: Elaborado por Cyntia Inuca.

IV. ADMINISTRACIÓN Y GESTIÓN DE LA RED DE ÁREA LOCAL DEL GADIP MUNICIPIO DE CAYAMBE

En este capítulo se muestra el desarrollo del proyecto, después del análisis de la situación actual de la red local se define políticas y procedimientos de gestión de red local, basado en el modelo funcional de gestión de red ISO/OSI, para que funcione mediante un sistema de gestión de red, en un centro de administración y monitoreo de red. Finalmente se plantea un diseño de segmentación de red, para mejorar la administración de la red.

A. Centro de administración y monitoreo de red

Es un espacio físico, ubicado en el departamento de TIC, donde intervienen recurso humano, software y hardware para permitir el control y visualización de datos de los recursos de red, mediante aplicaciones de monitoreo, mostrando al administrador de red una interfaz gráfica amigable.

Fig. 12. Centro de administración y monitoreo de red.
Fuente: Obtenido de: http://iteigo.net/archives/2109

Objetivos.

- Anticipar necesidades y requerimientos de la red.
- Monitorear y controlar las operaciones de los recursos de red.
- Brindar soporte técnico a los usuarios de red.
- Mantener información de la red.
- Controlar el buen uso del internet por parte de los usuarios, y;
- Brindar seguridad a través de la red.

Funciones.

Las funciones a desempeñarse en el centro de administración y monitoreo de red se establecen de acuerdo a cada área del Modelo Funcional de Gestión de red ISO/OSI.

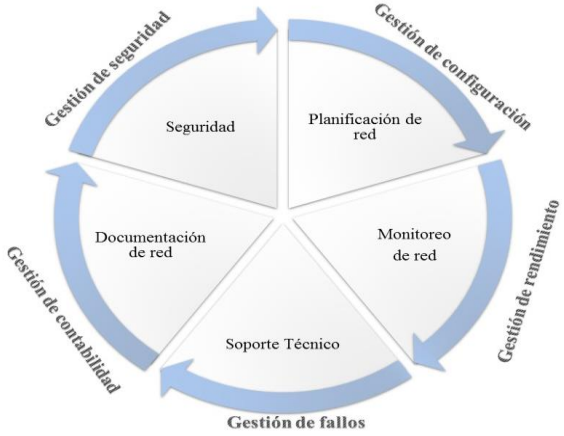

Fig. 13. Funciones del centro de administración y monitoreo de red.
Fuente: Adaptado por Cyntia Inuca.

(1) Planificación de red.

- Anticipar necesidades de la red, como:
  - Crecimiento de usuarios.
  - Crecimiento de equipos tecnológicos.
  - Actualización e implementación de nuevas tecnologías y servicios de red
- Planificar cambios de infraestructura en la red local.
  - Movilidad de personal y estaciones de trabajo.
  - Cambios de configuraciones en los equipos de red.
  - Reubicación, renovación o cambios de equipos de red.
- Revisar constantemente que la infraestructura de red y enlaces de backbone funcionen correctamente.

(2) Monitoreo de red.

- Visualización de los equipos activos que están conectados a la red local.
- Verificar continuamente el estado operacional de recursos de red.
  - Uso de memoria RAM.
  - Uso de disco duro.
  - Uso interfaces de red.
  - Uso de CPU (procesador)
- Detección de fallos.
- Controlar usuarios.

(3) Soporte técnico

- Atender, detectar, y resolver fallos.
- Brindar soporte técnico a necesidades de los usuarios.
  - Soporte de hardware.
    - Mantenimiento de equipos de comunicación.
    - Mantenimiento de computadores.
    -
  - Soporte de software.
    - Instalación de sistemas operativos, programas, y aplicaciones.
    - Actualización de sistemas operativos, programas, y aplicaciones.
    - Manejo y funciones de sistemas, programas y aplicaciones.

(4) Documentación de red.

- Inventarios de direcciones IP.
- Inventario de elementos de infraestructura de red.
  - Switch.
  - Routers.
  - Servidores, etc.
- Inventario de equipos terminales de usuario.

(5) Brindar Seguridad

- Ante ataques externos e internos de red.
- Controlar acceso de usuarios a la red y sus recursos.

B. Políticas y procedimientos de gestión de red.

La administración y gestión de redes es un campo amplio en el que intervienen elementos; humanos, hardware y software, para evaluar el funcionamiento de los recursos de red, al basarse en políticas y procedimientos se establece el desarrollo de funciones y los procesos a seguir, describiendo una secuencia lógica a las actividades a realizarse, con un objetivo en común.

Se estructuran políticas basadas en el modelo funcional de gestión de red ISO/OSI (FCAPS), el cual comprende cinco áreas funcionales:

- Gestión de configuración
- Gestión de fallas
- Gestión de rendimiento
- Gestión de contabilidad, y;
- Gestión de seguridad.

A través de estas se logrará administrar la red por partes y mejorar el servicio brindado a la municipalidad, garantizando la disponibilidad de la red.

1) Establecimiento de políticas.

1. Políticas para la gestión de red local.

1.1. Objetivos de políticas de gestión de red.
1.2. Documento de política de gestión de red.
1.3. Revisión de políticas de gestión de red.

2. **Política para la gestión de configuración.**
   - 2.1. Planificación de red
   - 2.2. Configuración de equipos.
   - 2.3. Ingreso de equipos.
   - 2.4. Documentación de configuración.
3. **Política para la gestión de fallos.**
   - 3.1. Manejo de fallos.
   - 3.2. Notificación de fallos.
   - 3.3. Documentación de fallos.
4. **Política para gestión de rendimiento.**
   - 4.1. Planificación y aceptación del sistema
   - 4.2. Establecimiento de umbrales.
5. **Política para gestión de contabilidad**
   - 5.1. Manejo de Reportes.
   - 5.2. Manejo de Inventarios.
6. **Política para gestión de seguridad**
   - 6.1. Controles de acceso a equipos.
   - 6.2. Control de acceso a la aplicación de gestión.
   - 6.3. Control de acceso a servidor de seguridad.
   - 6.4. Control de acceso a Internet.
   - 6.5. Control de usuarios.
   - 6.6. Protección contra intrusos.
   - 6.7. Manejo de Backups.

C. Implementación del modelo funcional de gestión de red ISO/OSI en la red local

La administración y gestión de la red local del GADIPMC se basa en el modelo funcional de gestión de red ISO/OSI, misma que presenta sus cinco áreas funcionales, gestión de configuración, gestión de seguridad, gestión de fallos, gestión de rendimiento y gestión de contabilidad.

Para el cumplimento de estas áreas se implementa un sistema de gestión de red basado en el paradigma gestor-agente que permite el monitoreo de los recursos que pertenecen a la red, así como también se implementa un sistema de seguridad que tiene funciones de firewall, IDS/IPS, y permite el control de usuarios. Finalmente se plantea un diseño de segmentación de red para mejorar la administración y gestión de red.

1) Gestión de configuración.

Esta área trata todo lo referente a configuraciones, que permite controlar la red, identificar los dispositivos conectados a la LAN y obtener información de su funcionamiento. Para ello se configura un sistema de gestión de red, así como también un sistema de seguridad.

Configuración del sistema de gestión de red.

El sistema de gestión de red está conformado por: un gestor, dispositivos a gestionar y el protocolo de gestión de red.

(1) Gestor.

El gestor o estación gestora no es más que el servidor que permite el monitoreo de los recursos de la red, a través de herramientas de gestión de red.

Esta herramienta es elegida por el estándar IEEE 29148, donde se establecen requisitos que debe cumplir el software de monitoreo, entre el comprador y el vendedor de la aplicación.

Se realizó un análisis de las herramientas de gestión más conocidas siendo Zenoss la mejor alternativa, como se ve en la Tabla 2.

Zenoss permite el monitoreo de la red local, unifica varias funcionalidades, que permiten gestionar las áreas funcionales de gestión de fallos, rendimiento y contabilidad, en un sistema simple y moderno, interactuando con el administrador de red mediante una interfaz web.

Tabla 2. Elección de una herramienta de monitoreo de red.

Características		Zabbix	Nagios	Zenoss	Pandora FMS	Open NMS
Software libre	Libre	✓	✓	✓	✓	✓
	Comercial	x	✓	✓	✓	✓
Manejo de software		Dificultad baja	Dificultad alta	Dinámica	Dificultad media	Dificultad media
Recursos de hardware		Bajo	Alto	Medio	Medio	Medio
Funciones	SNMP v2	✓	✓	✓	✓	✓
	Auto-descubrimiento de red	x	x	✓	x	x
	Auto-descubrimiento de topología	x	✓	✓	x	x
	Gráficas de rendimiento	✓	✓	✓	✓	✓
	Reportes	✓	✓	✓	✓	✓
	Base de datos	Oracle MySQL, PostgresSQ.	Programado en C MySQL Postgres SQL.	MySQL Postgre SQL.	MySQL	Postgre SQL
	Manejo de alarmas y notificación de eventos por correo electrónico	✓	✓	✓	✓	✓
Seguridad		✓	✓	✓	✓	✓

Fuente: Paginas web oficiales de cada software.

El administrador puede autodescubrir la red o ingresar cada dispositivo a gestionar de forma manual, para luego poder obtener información de su funcionamiento.

Fig. 14. Descubrimiento de dispositivos.
Fuente: Aplicación Zenoss.

Pero es importante antes de iniciar a monitorear los dispositivos habilitar el protocolo SNMP.

(2) Dispositivos Gestionados.

Para que el dispositivo de red sea gestionado se debe verificar que tenga soporte SNMP. Se gestiona servidores y equipos de computación de los usuarios de la red del GADIPMC.

(a) Protocolo SNMP.

Para habilitar el protocolo SNMP se toma en cuenta tres aspectos:

- **Versión:** Se usa la versión SNMP v2c, basada en comunidad.
- **Comunidad:** Este actúa como una contraseña, usado para la autenticación entre la estación gestora y el dispositivo gestionado.
- **Permisos:** A través de permisos de solo lectura podremos monitorear la los recursos de red y observar la información de su funcionamiento.

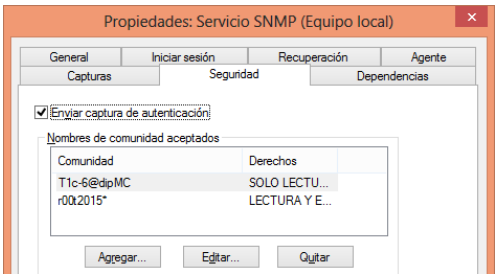

Fig. 15. Habilitando protocolo SNMP.
Fuente: Sistema Operativo Windows 7.

Configuración del sistema de seguridad.

Para brindar seguridad a la red local del Municipio de Cayambe se implementa una plataforma que integra varios servicios, Zentyal es un Sistema operative basado en Ubuntu, proporciona funciones de firewall, IDS/IPS, y control de usuarios mediante Open LDAP, el administrador podrá tener control total de la red a través de las configuraciones de dichas funciones.

(1) Roles de Zentyal para administrar la red local del GADIPMC.

Tabla 3. Paquetes de instalación requeridos para Zentyal.

ROL	PAQUETE	REQUERIMIENTO
GATEWAY 	Proxy HTTP Cortafuegos IDS/IPS Portal Cautivo	Limitar acceso a páginas web Proteger la red de intrusos Controlar acceso de usuarios
INFRASTRUCTURE 	DNS DHCP	Dar un nombre de dominio de red. Acceso a la red automáticamente.
OFFICE 	User and Computers Backup	Controlar acceso de usuarios a la red Respaldar información de configuración del servidor.

Fuente: Obtenido de https://wiki.zentyal.org

Servicio DNS: Permite dar un nombre de dominio a el servidor Zentyal.

Servicio DHCP: Asigna automáticamente el direccionamiento ip a los usuarios de la red.

Fig. 16. Servicio DHCP de Zentyal.
Fuente: Servidor Zentyal.

Servicio User and Computers: este servicio permite crear usuarios y grupos de usuarios los cuales estan dentro de un dominio, este servicio se complementa con el **Portal Cautivo** aplicado a la interfaz de red de la LAN, los usuarios deberán ingresar usuario y contarseña para acceder a los servicios que proporciona la red. El administrador puede verificar cuantos usuarios estan conectados en tiempor real, además también puede establecer usuarios exentos de ingresar por el portal cautivo.

Fig. 17. Creación de grupos de usuarios.
Fuente: Servidor Zentyal.

Backup: Permite obtener una copia de seguridad de las configuraciones realizadas en el servidor Zentyal, como respaldo para uso emergente.

Fig. 18. Backup de Zentyal.
Fuente: Servidor Zentyal.

Servicio de firewall/proxy: A tráves de este servicio se realiza el filtrado de páginas web de forma transparente, se aplican un lista negra de contenido de dominios y se establecen reglas que permitan denegar el acceso a páginas web de contenidos obscenos, videos, descargas, música, que conseemen muchos recursos de red.

Fig. 19. Configuración proxy transparente.
Fuente: Servidor Zentyal.

Para páginas web https, permite la creación de servicios, y objetos que son pequeños archivos que permiten la creación de reglas de filtrado que permitan o denieguen el acceso de un objeto a un servicio especifico.

Fig. 20. Dominios de denegar.
Fuente: Servidor Zentyal.

Servicio IDS/IPS: Se activa este servicio para proteger a la red contra ataques de intrusos, se habilitan las interfaces a modo escucha y se aplican reglas que permitan bloquear y registrar el acceso de un intruso en la red.

Fig. 21. Intefaces cautivas.
Fuente: Servidor Zentyal.

Fig. 22. Reglas para IDS/IPS
Fuente: Servidor Zentyal.

2) Gestión de seguridad.

La gestión de seguridad se encarga de proteger la red y sus componentes, para ello se basa en la seguridad lógica, aplicando mecanismos de control de acceso, firewall, y detección de intrusos, y cumplimiento de políticas.

Fig. 23. Seguridad Lógica.
Fuente: Santos. J. (2011).Seguridad y alta disponibilidad. Editorial: RA-MA

Control de acceso al sistema de gestión de red.

Zenoss permite la configuración de usuarios para administrar la red, el usuario administrador tiene acceso a todo tipo de configuraciones e información monitoreada, y podrá asignar a otro usuario para que también pueda monitorear la red, y asignarle permisos iguales o limitados al acceso de información de la red.

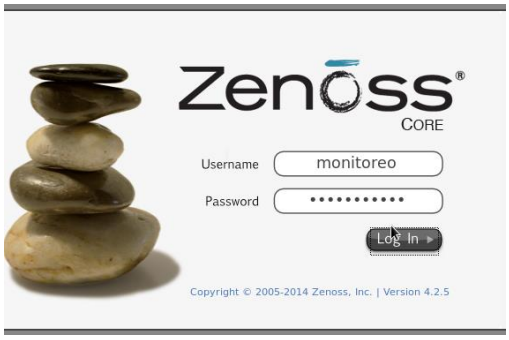

Fig. 24. Ingreso a la aplicación Zenoss.
Fuente: Aplicación Zenoss.

Control de acceso al sistema de seguridad.

El acceso al sistema de seguridad Zentyal será únicamente a través del usuario administrador.

Al acceder como usuario administrador, este podrá ingresar a través de la interfaz web del servidor, o mediante ssh.

Fig. 25. Ingreso de usuario administrador a Zentyal.
Fuente: Servidor Zentyal.

Para el acceso mediante ssh, es necesario que acceda a través de un equipo que pertenezca a la Dirección de TIC, ya que se establece como regla el acceso a través de uno de ellos.

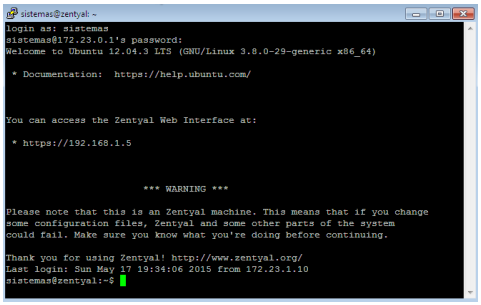

Fig. 26. Ingreso de usuario administrador a través de ssh.
Fuente: Aplicación Putty.

Control de acceso a equipos.

Se accedió a los equipos de conmutación a graves de consola para averiguar su tienen algun tipo de configuracion, se verifica la direccion ip por defecto a traves del cual se peude accede por interfza web.

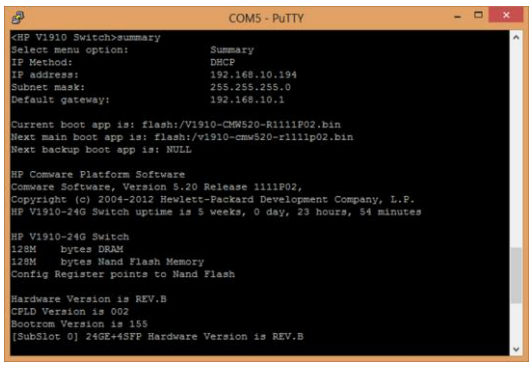

Fig. 27. Acceso al switch HP-1910 por consola.
Fuente: Aplicación Putty.

Control de usuarios de red.

Los usuarios de la red del GADIPMC, deberan ingresar un usuario y contraseña para aceder a los servicios que brinda la red del GADIPMC, el es el unico responsible del uso que se le de a este, el administrador tiene la potestad de dar de alta o baja de un usuario, puede tambien manejar usuarios con privilegos y sin privilegios permitiendo o denegando acceso a ciertos servicios.

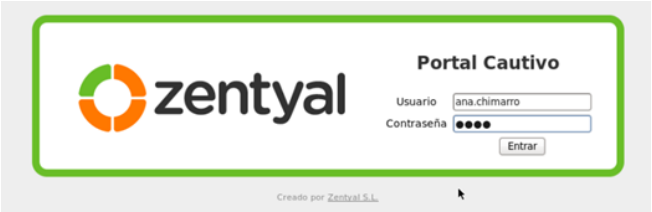

Fig. 28. Acceso de usuarios por portal cautivo.
Fuente: Navegador Mozilla.

3) Gestión de fallos.

La gestión de fallos, permite monitorear constante de la red a fin de identificar fallas en la misma, la gestión de fallos no solo se limita al monitoreo si no que cumple con un proceso de ciclo de vida de incidencias de fallo, lo que facilita realizar un seguimiento de la falla, hasta resolverla.

Fig. 29. Ciclo de vida de incidencias de fallos.
Fuente: Adaptado por Cyntia Inuca.

Zenoss permite seguir el proceso de ciclo de vida de incidencias de un fallo en la red, detectando, aislando y diagnosticando los fallos, a través del cual el administrador podrá determinar la solución al fallo ocurrido.

Para detectar fallos en la red se lo hace de manera proactiva y reactiva, actuando antes que suceda el fallo y después de que suceda un fallo inesperado.

Zenoss tiene integradas herramientas esenciales como:

- Ping .
- Traceroute.
- Snmpwalk.

Las cuales son herramientas esenciales para realizar pruebas preventivas de conectividad y verificar si se alcanza un destino.

Zenoss permite la detectar, aislar, y diagnosticar fallos en la red, proporcionando al administrador infromacion que le permitan brindar una solución al problema. El administrador de red puede verificar el estado del fallo en la consola events y

también puede recibir notificaciones mediante correo electrónico.

Zenoss maneja un código de colores para mostrar el estado o gravedad del fallo, y por ende su prioridad, e identifica el dispositivo por su dirección IP y resume el tipo de fallo.

Para la solución de los fallos interviene mucho la experiencia del elemento humano tecnico, mismo que seguirá un proceso para resolver el problema.

Fig. 30. Detección de fallos de Zenoss.
Fuente: Aplicación Zenoss.

4) Gestión de rendimiento.

La gestión de rendimiento permite monitorear la información del funcionamiento de los recursos de la red, y visualizarla a través de gráficas y datos estadísticos.

Zenoss.

Mediante el software Zenoss se verifica disponibilidad, se visualiza datos y graficas de rendimiento de uso de Disco Duro, interfaces de red, memoria RAM, y CPU.

(1) Uso de disco duro

Se puede revisar la capacidad del disco, y sus particiones, el tamaño asignado a cada partición, cuanto de esa capacidad se está usando y cuanto está libre, así como su utilidad en porcentaje.

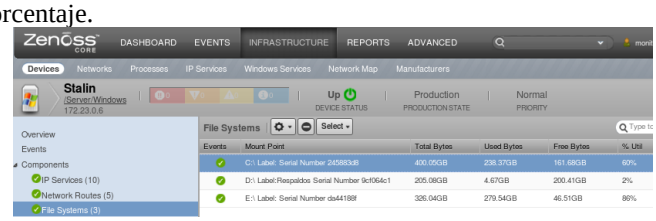

Fig. 31. Monitoreo de uso de Disco Duro.
Fuente: Aplicación Zenoss.

(2) Monitoreo de interfaces de red.

Se descubren todas las interfaces del dispositivo gestionado, entre ellas se puede ver la interfaz de red, con la dirección IP asignada, y su MAC, e informa si esta activa o no, muestra también una gráfica sobre su rendimiento con la cantidad de tráfico que está haciendo uso.

Fig. 32. Monitoreo de Interfaces.
Fuente: Aplicación Zenoss.

(3) Monitoreo de uso de memoria.

Es importante el monitoreo de este recurso, ya que es un componente clave para que un computador se desempeñe de forma eficiente, y aplicaciones que haga uso el usuario fluyan rápidamente, Zenoss permite la visualización de graficas de uso de memoria, donde el administrador puede evaluar, el uso que se esté dando a este recurso, a través del monitoreo puede hacer sugerencias de cambio o incremento de memoria al equipo del usuario.

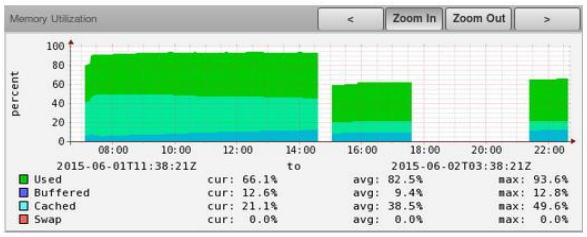

Fig. 33. Monitoreo de uso de memoria.
Fuente: Aplicación Zenoss.

(4) Monitoreo de uso de CPU (Procesador).

Este recurso es el núcleo de funcionamiento de un ordenador, el cual ejecuta instrucciones, Zenoss muestra el tipo de procesador que usa el equipo y una gráfica sobre el uso que se está haciendo de este recurso.

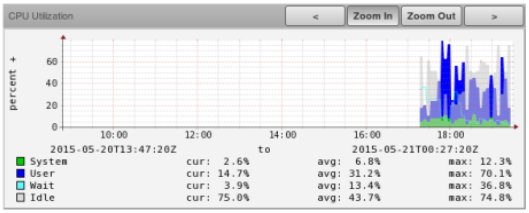

Fig. 34. Monitoreo de uso de CPU.
Fuente: Aplicación Zenoss.

Zentyal.

Zentyal muestra información del uso de sus recursos; disco duro, memoria RAM, CPU, de manera que el administrador de red puede revisar cómo está funcionando. Ademas permite tambien monitorear el uso de ancho de banda.

(1) Uso de CPU (Procesador).

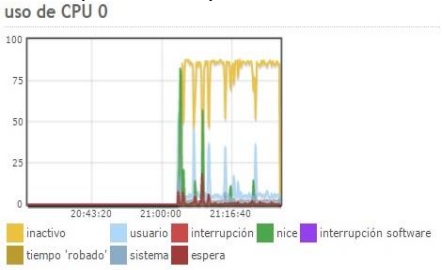

Fig. 35. Uso de CPU de Zentyal.
Fuente: Servidor Zentyal.

(2) Memoria RAM.

Fig. 36. Uso de memoria RAM.
Fuente: Servidor Zentyal.

(3) Disco Duro.

Fig. 37. Uso de disco duro de Zentyal.
Fuente: Servidor Zentyal.

(4) Ancho de banda.

A través de Zentyal se puede ver el uso de ancho de banda que hace cada usuario de la red, a través del cual el administrador puede identificar al usuario que este excediendo de este recurso.

Fig. 38. Monitoreo de ancho de banda.
Fuente: Servidor Zentyal

5) Gestión de contabilidad.

La gestión de contabilidad permite llevar el control de la información de la red, mediante inventarios, registros y reportes.

El administrador debe llevar inventarios del dispositivo que pertenecen a la red local, y complementar esa información con la aplicación de gestión de red Zenoss, que le proporciona al administrador reportes de funcionamiento de los dispositivos monitoreados.

Zentyal también proporciona registros de Proxy HTTP, IDS, y además se puede verificar los usuarios que están conectados a la red.

Fig. 39. Gestión de contabilidad.
Fuente: Adaptado por Cyntia Inuca.

Reports de Zenoss

Zenoss proporciona varios reportes ubíquese en la pestaña Reports, y se mostrarán reportes de todos los dispositivos gestionados, información como direccionamiento IP, MAC, reportes de eventos, reporte de rendimiento, etc.

Fig. 40. Reportes de todos los dispositivos que se monitorean.
Fuente: Aplicación Zenoss.

Registros de Zentyal

Zentyal proporciona registros de:

- **Proxy HTTP,** registra accesos realizados a páginas web, donde el administrador puede verificar el uso que los usuarios dan al internet.
  El administrador puede identificar si un usuario estan intentando accede varias veces a un dominio denegado y hacer un seguimiento mediante la direccion IP.
- **IDS:** contiene registros de cualquier actividad sospechosa en la red como extraccion de informacion de red, mismos que se registran con una alerta.

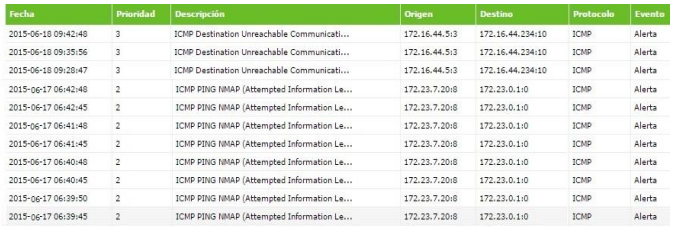

Fig. 41. Registros IDS.
Fuente: Servidor Zentyal.

6) Diseño de segmentación de la red de área local.

Se plantea un diseño para la segmentación de red en vlans, bajo un modelo jerarquizado, con escalabilidad, para el mejoramiento de la administración y seguridad de la misma.

Jerarquización de la red.

Una red jerarquizada se basa en tres capas, núcleo (core), distribución, y acceso, cada capa tiene su función.

Capa núcleo: será el enlace de backbone, que permita la conectividad de internet, y agregue tráfico a la capa de distribución, esta capa requiere de un switch de Core, que siempre esté disponible y realice una rápida convergencia, para los diferentes servicios que se puedan implementar en la red.

Capa de distribución: en esta capa es donde se puede realizar las configuraciones de enrutamiento entre vlans, se requiere un switch capa 3, el tráfico fluirá por los switch de distribución y será entregado a la capa núcleo.

Capa acceso: a esta capa pertenecerán los equipos de usuario final, que se conectarán a través de un switch de acceso, este puede ser un switch de capa 2, no administrable, los switch de acceso estarán conectados al switch de distribución.

Al jerarquizar una red se obtiene beneficios tales como, facilidad de expansión de la red, ya que es más escalable y se puede incluir mayor número de usuarios a la red en cualquier momento, incremento de rendimiento, facilidad de identificación de problemas y rapidez en dar una solución, mejora la administración y seguridad de la red.

Planteamiento para la segmentación de red.

Se plantea la segmentación de red en vlans, que permitirá tener varias redes lógicas dentro de una misma red física, cada dirección que se desempaña dentro de la municipalidad, pertenecerá a una vlan, cada vlan tendrá asignado un rango de direccionamiento IP, suficiente para abarcar el número de usuarios de su dependencia, de acuerdo a estas observaciones se plantea la segmentación de la red, de la siguiente manera:

Tabla 4. Planteamiento de segmentación de red.

VLAN	DIRECCIONES	RANGO HOSTS	SUB-MASCARA
10	GESTION DE TIC	172.23.0.1 - 172.23.0.126	255.255.255.128
11	FINANCIERO	172.23.0.129 - 172.23.0.190	255.255.255.192
12	AVALUOS Y CATASTROS	172.23.0.193 - 172.23.0.254	255.255.255.192
13	ALCALDIA	172.23.1.1 - 172.23.1.62	255.255.255.192
14	ADMINISTRATIVO	172.23.1.65 - 172.23.1.126	255.255.255.192
15	CONCEJO MUNICIPAL	172.23.1.129 - 172.23.1.190	255.255.255.192
16	CONCEJO DE LA NIÑEZ	172.23.1.193 - 172.23.1.254	255.255.255.192
17	DESARROLLO AMBIENTAL	172.23.2.1 - 172.23.2.62	255.255.255.192
18	DESARROLLO ECONOMICO	172.23.2.65 - 172.23.2.126	255.255.255.192
19	DESARROLLO FISICO	172.23.2.129 - 172.23.2.190	255.255.255.192
20	DESARROLLO INTEGRAL DEL TERRITORIO	172.23.2.193 - 172.23.2.254	255.255.255.192
21	DESARROLLO SOCIAL	172.23.3.1 - 172.23.3.62	255.255.255.192
22	COMUNICACIÓN	172.23.3.65 - 172.23.3.126	255.255.255.192
23	PARTICIPACION CIUDADANA	172.23.3.129 - 172.23.3.190	255.255.255.192
24	PLANIFICACION URBANA Y RURAL	172.23.3.193 - 172.23.3.254	255.255.255.192
25	PROCURADURÍA SÍNDICA	172.23.4.1 - 172.23.4.62	255.255.255.192
26	PROTECCION DE DERECHOS	172.23.4.65 - 172.23.4.126	255.255.255.192
27	SEGURIDAD, RIESGOS	172.23.4.129 - 172.23.4.190	255.255.255.192
28	TALENTO HUMANO	172.23.4.193 - 172.23.4.254	255.255.255.192
29	TRANSITO, TRANSPORTE	172.23.5.1 - 172.23.5.62	255.255.255.192
30	GESTION DE PROYECTOS	172.23.5.65 - 172.23.5.126	255.255.255.192
31	EMAPAAC	172.23.5.129 - 172.23.5.190	255.255.255.192

Fuente: Elaborado por Cyntia Inuca.

Diagrama de segmentación de la red.

Al distribuir la red por segmentos de vlans, el administrador mantendrá una estructura ordenada de la red, el switch de distribución tendrá configurado las vlans y a través de enlaces troncales puede replicar todas las vlans, hacía los otros switch, para que desde las diferentes ubicaciones de las instalaciones del municipio los usuarios accedan a través del segmento al que pertenecen.

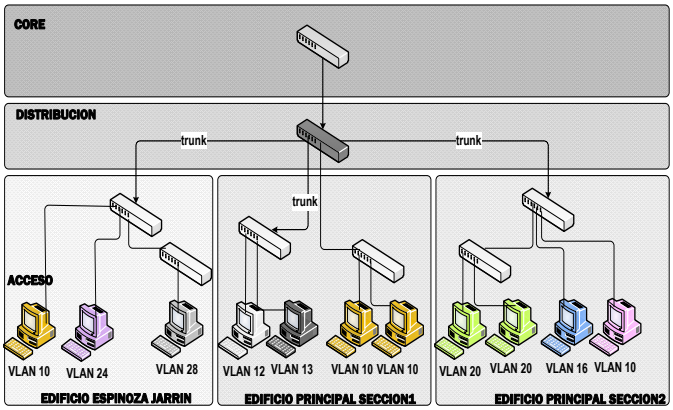

Fig. 42. Segmentación de la red bajo un modelo jerarquizado.
Fuente: http://sistemasumma.com/2012/02/19/redes-jerarquicas/

V. Análisis Costo Beneficio

Este capítulo se lo desarrolla con el fin de conocer los gastos que conllevan la realización del proyecto y los beneficios que se obtienen. Para este capítulo se analizan dos aspectos, primero en relación al software y segundo el hardware.

A. *Software*

El proyecto plantea herramientas de software libre, mismas que se eligieron para cubrir las necesidades de la red de área local del GADIPMC, dichas herramientas no representan ningún costo referente a licencias.

Actualmente se dispone de herramientas de software libre en varias versiones, la versión de Core que es gratuita y versión empresarial. Para este proyecto se hace uso de las versiones Core, ya que las versiones empresariales se basan en las funcionalidades que tiene la versión de Core.

Tabla 5. Comparativa de costos de herramientas de software libre.

Software	Costo anual	
Versión	Core	Profesional/Enterprise
Zentyal	$ 0	$ 1280,00
Zenoss	$ 0	$32.500,00
Total	$ 0	$34.495,00

Fuentes: Correo electrónico personal y https://store.zentyal.com/so3137.html?_store=euro_es&_from_store=global.

Análisis de Costo: El pago de licencias anuales resulta ser una inversión elevada, al usar las versiones Core, la institución ahorra dinero, que puede invertirse en obras para la ciudadanía.

Análisis de beneficios al usar software totalmente libre: las funcionalidades que presentan las versiones Core son la base para las versiones Enterprise, al usar las versiones de Core, se aprovecha la funcionalidades de estas, y se puede adaptar a las nuestras necesidades.

Las versiones de Core son aportes de la comunidad, gratuitas, y también se actualizan.

En cuanto a soporte, las comunidades tienen foros donde se puede obtener información, preguntar, y aportar.

B. *Hardware*

La ventaja de usar software libre es que pueden funcionar en equipos que de bajos requerimientos de hardware, la municipalidad disponía de computadores que cumplen características aceptables para su correcto funcionamiento, por lo cual no fue necesario la adquisición de servidores.

A continuación se revisan las características de hardware requerido para la instalación de los softwares, características de los computadores disponibles, y características de los equipos en caso de que se realizara la adquisición.

Tabla 6. Características requeridas por los software.

Servidor Características	Zentyal 3.2.	Zenoss Core.
Procesador:	Xeon Dual Core	4 Core
Memoria:	4 GB	8 GB
Disco Duro:	160 GB	300 GB
Tarjetas de red.	2 o más	1

Fuente: https://wiki.zentyal.org/wiki/File:Es-3.2-images-intro-zentyal-install-tabla-installation-ES.png

Los computadores disponibles en el área de TIC, cumple las características adecuadas para el correcto funcionamiento de los software, para el sistema de gestión, aprovechando estas características se hizo el uso de ellos.

Tabla 7. Características de hardware utilizados.

Servidores	Zentyal	Zenoss
Características	Procesador: i7. Memoria: 4 GB Disco Duro:500GB Tarjetas de red: 2.	Procesador: Intel Core i3. Memoria: 4 GB. Disco Duro: 300 GB. Tarjeta de red: 1.
Costo:	$ 0	$ 0

Fuente: Computadores disponibles en el área de TIC.

Para estimar el costo que conllevaría la compra de servidores, que cumplan las características de los software, se tiene la siguiente tabla, donde muestra el valor para su adquisición, las características que se acoplan a los requerimientos, estos valores se basan en una proforma propuesta.

Tabla 8. Costo de equipos de hardware para servidores.

Servidores	Zentyal	Zenoss
Procesador: **Memoria:** **Disco:** **Tarjeta de red**	Intel Xeon. 8GB 500GB 2.	Intel Core i5. 8GB. 1TB. 1.
Costo para adquisición de hardware	$ 3377,70	$ 956,48
Costo total	$ 4.334,19	

Fuente: Proforma TECNIT.
(Este valor puede ser destinado a otros fines del municipio.)

C. *Beneficios.*

El uso de software libre y la disponibilidad de equipos con características para el correcto funcionamiento de los software, no representó gastos, pero si se obtuvo beneficios tanto para el administrador de la red como para el usuario.

1) *Beneficios del administrador:*

- ✓ Mejoramiento de la seguridad de la red, contra ataques.
- ✓ Tiene el control de usuarios de la red.
- ✓ Puede revisar cualquier fallo en la red y atender rápidamente a los requerimientos de los usuarios.
- ✓ Dispone de mayor número de direcciones IP, para asignar a los usuarios.
- ✓ Obtiene reportes sobre los equipos que están conectados a la red, y su funcionamiento.
- ✓ Puede llevar inventarios de manera más fácil ya que puede identificarse el usuario, la IP, características del equipo, y;
- ✓ Monitorear el uso que está haciendo de los recursos del equipo y la red.

2) *Beneficios del usuario:*

- ✓ Atención eficiente a los problemas del usuario.
- ✓ Tiene una red más segura y estable, con conexión a internet mediante un usuario y una contraseña,
- ✓ El administrador puede sugerir al usuario, mejoras para el buen desempeño de su equipo de computación, sin que el usuario lo solicite, como expansión de disco duro, memoria, cambio de tarjetas de red, obtención de respaldos, etc.

VI. CONCLUSIONES

El modelo funcional de gestión de red ISO/OSI y el protocolo SNMP, son las bases en la que se fundamenta este proyecto, ya que plantean directrices para la administración y gestión de una red de forma organizada, permitiendo tener el control total de la red.

La utilización de herramientas de software libre para la gestión de red cumple un papel importante para el administrador ya que se presenta a él como una interfaz gráfica amigable que le permite visualizar los datos requeridos de funcionamiento de los recursos que están conectados en la red.

Existen una variedad amplia de herramientas de monitoreo de red, cada una tiene sus funcionalidades, unas complejas y otras sencillas. Al buscar una herramienta para que realice la gestión de la red local, el administrador busca facilidad de manejo del software, claro que hay herramientas muy buenas pero que tiene su nivel de complejidad, mientras más funciones quieres que realice más compleja es, la elección de herramientas de software libre para la gestión de red se la realizó a través del estándar IEEE 29148, mismo que permite establecer acuerdos entre el proveedor y el comprador de la funcionalidades o características que este debe cumplir el software, una de las características importantes a cumplir fue el autodescubrimiento de la red.

En el análisis de la situación actual se revisó los equipos que dispone la infraestructura de la LAN de GADIPMC, siendo estos switch capa tres y capa dos, que se usan únicamente en modo acceso para la interconexión de los usuarios a la red. Para la segmentación de la red estos deben tener la capacidad suficiente para manejo de varias vlans y permitir el enrutamiento entre ellas, para actuar como un switch de distribución, pero estos permiten enrutamiento máximo de 8 vlans, por lo que no son aptos para la creación de vlans por direcciones.

Los equipos que funcionan en modo acceso no tienen ningún tipo de configuración que incluya un direccionamiento ip, por lo cual no se habilita el acceso por ssh, el administrador puede ingresar únicamente por consola en caso de que se realice algún tipo de configuración.

Al monitorear la situación actual de la red, se detecta información de los dispositivos que tenían activado snmp con comunidad public, entre ellos el firewall, esto muestra el riesgo de que cualquier otro usuario puede ver la información de gestión, por eso luego se realiza el monitoreo de la red a través de una comunidad al que pertenezcan todos los equipos, la comunidad actúa como una contraseña para el intercambio de información de gestión entre el dispositivo gestionado y el gestor, esta comunidad se define tal cual se establece una contraseña.

El firewall es el equipo más importantes dentro de la red de cualquier institución, el administrador de la red debe tener control total sobre este, caso que no se cumplía en la municipalidad, pues este era muy limitado a realizar funciones específicas, por ello se plantea un sistema de seguridad que mejore este firewall, mismo que permite manejar varios servicios y funciones en una sola plataforma, Zentyal, agregando funciones de firewall, IDS//IPS, además de permitir el control de usuarios.

Todo el proceso de análisis de la situación actual permite la recopilación de necesidades y requerimientos de la red local, para lo cual se definen políticas de gestión como una guía para mejorar la administración de la red, siendo una herramienta de apoyo administrativo para el encargado de la red, en este se definen reglas a cumplirse, que solvente dichas necesidades y requerimientos.

La conformación de un sistema de gestión de red, con herramientas que permitan monitorear y visualizar datos de sus recursos gestionados, basado en un modelo, regido por políticas, permite al administrador tomar decisiones y actuar ante un evento inesperado en la red, para mantener el nivel de disponibilidad de la red en una forma estable.

Al administrar la red no solo intervienen el protocolo snmp, y el modelo de gestion en el que se basa para realizar la gestión de red, sino que también es importante el papel que desempeña el recurso humano para que el modelo se cumpla así como el correcto funcionamiento del sistema de gestión.

Zenoss monitorea de la red, y maneja las áreas de gestión de fallos, rendimiento y contabilidad, al detectar un fallo permite el envío de notificaciones por correo electrónico, a través del uso de un servidor postfix así como Gmail, para el proyecto inicialmente se planteaba realizar pruebas mediante un servidor postfix, pero en vista de la funcionalidad de notificaciones a través de Gmail se aprovecha este medio, ya que Gmail está disponible a todas horas y en cualquier lugar que tenga conectividad a internet, a comparación del servidor postfix que era un medio local para realizar las pruebas pertinentes.

La realización de este proyecto ha facilitado al administrador, tener un control sobre la información de la red y su funcionamiento, ya no es necesario realizar un inventario manual en el que se registraba direcciones IP utilizadas, las características del equipo, y el nombre del usuario, ya que la información del equipo la obtiene a través del monitoreo, y puede ver los usuarios que hacen uso de la red a través del portal cautivo.

El trabajo del administrador de la red o el técnico encargado del área de TIC, es atender los requerimientos de los usuarios, en el caso de resolución de problemas, debe ir a verificar el problema que se dio, buscar las posibles causas, y ver alternativas de solución, pero ahora existen las herramientas que le permiten diagnosticar los problemas, y a través de este dar soluciones más rápidas.

Existen varias versiones de Zentyal, con varias funcionalidades, que ayudan a mejorar la administración de una red, con un todo en uno, el administrador de red debe definir muy bien las funcionalidades que requiere su red, para ponerlas en ejecución. Zentyal genera reglas por defecto, por ello es importante saber las configuraciones que se va a realizar en el

servidor de seguridad (Zentyal), uno de los aspectos importantes son los puertos que necesariamente deben estar abiertos.

Al segmentar la red local bajo un modelo jerárquico se obtendrá beneficios tales como, facilidad de expansión de la red, ya que se vuelve más escalable, incremento de rendimiento, facilidad de identificación de problemas y rapidez en dar una solución, ya que este se maneja por capas, permitiendo el mejoramiento de la administración y seguridad de la red.

Al realizar el análisis de costo beneficio del proyecto, en cuanto a software, se establecen las diferencias que tiene un software libre con licencia (empresarial) y el software libre sin licencia (core), siendo la versión de core la mejor solución, ya que la versión licenciada se basa en la versión de core, y se diferencian por añadir unas mejoras, brindar soporte técnico, consultas y mantenimiento, lo cual en la versión de core podemos obtenerla a través de foros de comunidades de software libre así como las mejoras que se le den a la versión de core.

Lo beneficios del proyecto se reflejan en el administrador de red y los usuarios, ya que el administrador tiene el control sobre el funcionamiento de la red y los usuarios tienen una red más estable, segura y disponible.

El uso de herramientas de software libre, es beneficioso ya que evita altos gastos en licencias, y se obtiene los mismos beneficios que provee un software pagado.

VII. REFERENCIAS

[1] T. Saydam, «From Networks and Network Management Into Service and Service Management,» *Journal of Network and Systems Management*, 1996.

[2] R. McLeod, «Sistemas de información gerencial,» Mexico, Pearson Educación, 2000, p. 289.

[3] I. T. Union, «International Telecomunication Union,» 1992. [En línea]. Available: http://www.itu.int/rec/T-REC-X.700-199209-I/en.

[4] R. J. Millan Tejedor, «Gestion de Red,» *Windows NT/2000*, 1999.

[5] J. Kurose y K. Ross, Computer Network, PEARSON.

[6] IETF, «Simple Network Management Protocol (SNMP),» 05 1990. [En línea]. Available: https://www.ietf.org/rfc/rfc1157.txt.

[7] D. Mauro y K. Schmidt, Essential SNMP, Estados Unidos : O'Reilly Media, Inc., 2005.

[8] W. Stallings, Fundamentos de seguridad en redes, Aplicaciones y estandares., Madrid: PEARSON, 2004.

[9] Comunidad Autonoma de Castilla y Leon, Tecnicos de Soporte Informatico, Sevilla: MAD, S.L, 2006, p. 285.

[10] S. Untiveros, «METODOLOGIAS PARA ADMINISTRAR REDES,» JULIO 2004. [En línea]. Available: http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf.

[11] W. Stallings, Comunicaciones y Redes de Computadoras, Madrid: PEARSOON EDUCACIÓN, 2004.

[12] M. d. C. Romero, «Sistemas Avanzados de Comunicaciones - Gestion de Redes,» [En línea]. Available: http://www.dte.us.es/personal/mcromero/docs/sac/sac-gestionderedes.pdf.

[13] F. J. M. Robles, «Planificacion y Administacion de Redes,» Madrid-España, RA-MA, 2010, p. 605.

[14] L. R, «IP Reference,» [En línea]. Available: https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/.

[15] A. Perpinan, «ADMINISTRACION DE REDES GNU/LINUX,» de *ADMINISTRACION DE REDES GNU/LINUX*, Santo Domingo-República Dominicana, GAMMA, 2004, p. 9.

[16] R. J. Millan Tejedor, «Tendencias en gestión de red,» *Comunicaciones World*, pp. 54-56, 2004.

[17] R. McLeod, «Sistemas de información gerencial,» de *Sistemas de información gerencial*, Mexico, Pearson Educación , 2000, p. 298.

[18] A. B. Martí, Gestión de Red, Barcelona: Universidad Politecnica de Cataluña, 1999.

[19] T. Magazine, «Optimización del rendimiento de la CPU de SQL Serve,» 2008. [En línea]. Available: https://technet.microsoft.com/es-es/magazine/2007.10.sqlcpu.aspx.

[20] J. Lázaro Laporta y M. Miralles Aguiñiga, Fundamentos de Telemática, Universidad Politecnica de Valencia, 2005.

[21] I. Hoy, «Como optimizar la memoria RAM,» 2012. [En línea]. Available: http://www.informatica-hoy.com.ar/.

[22] P. Gil, J. Pomares y F. Candela, «Redes y Trasmision de Datos,» de *Redes y Trasmision de Datos*, 2010.

[23] J. Curry, «Gestión de Eventos para Zenoss Core 4,» Enero 2013. [En línea]. Available: http://www.skills-1st.co.uk/papers/jane/zenoss4-events/zenoss_Core4_event_management_paper.pdf.

[24] Zenoss Community, «Zenoss Documentation,» 2005-2015. [En línea]. Available: http://www.zenoss.com/sites/default/files/documentation/Zenoss_Core_Administration_02-022014-4.2-v08.pdf.

[25] ZABBIX, «ZABBIX,» 2001-2015. [En línea]. Available: http://www.zabbix.com/features.php.

[26] Artica Soluciones Tecnologicas, «The monitoring wiki PANDORA FMS Enetrprice,» 2006-2012. [En línea]. Available: http://wiki.pandorafms.com/index.php.

[27] Comunidad Autonoma de Castilla y Leon, «Tecnicos de Soporte Informatico,» de *Tenicos de Soporte Informatico*, Sevilla, MAD, S.L, 2006, pp. 286-287.

[28] Diego Borja, «PROYECTO DE CABLEADO ESTRUCTURADO DEL GAD MUNICIPAL DEL CANTON CAYAMBE,» 2012.

[29] Zentyal Community, «Documentacion oficial de Zentyal.,» [En línea]. Available: https://wiki.zentyal.org/wiki/Es/3.2/Zentyal_3.2_Documentacion_Oficial.

[30] Zenoss Own IT, «¿Por que Zenoss?,» 2005-2015. [En línea]. Available: http://www.zenoss.com/solution/why-zenoss.

BIOGRAFÍA

Cyntia M. Inuca G. Nace un 8 de abril de 1990 en Gonzales Suarez – Otavalo – Ecuador. Realizó sus estudios primarios en la Escuela de Práctica Docente "Juan Montalvo", sus estudios secundarios los termina en el Instituto Tecnológico "Otavalo" en el 2007 en en la especialidad de Físico Matemático, actualmente se encuentra culminando sus estudios superiores en la Universidad Técnica del Norte de la ciudad de Ibarra, para obtener el título de ingeniera en Electrónica y Redes de Comunicación.

Realizó sus prácticas preprofesionales en el Municipio de Cayambe en el departamento de Tecnologías de la Información y Comunicación, donde desempeño tareas de soporte técnico entorno a la infraestructura de la red de datos interna de la municipalidad; instalación de nuevos puntos de red, configuraciones de equipos de comunicación, inventarios de equipos interconectados a la red y direccionamiento IP, diseño de cableado estructurado para el edificio Espinoza Jarrín, el municipio también tiene a su cargo la red inalámbrica de las instituciones educativas de cantón Cayambe, donde se dotó de servicio de internet a varias escuelas, realizando actividades de instalación, mantenimiento y configuración de antenas, routers inalámbricos, para la conformación de la red de las instituciones.