UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"ADMINISTRACIÓN Y GESTIÓN DE LA RED DE ÁREA LOCAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CAYAMBE, BASADO EN EL MODELO FUNCIONAL DE GESTIÓN DE RED ISO/OSI CON EL PROTOCOLO SNMP Y USO DE HERRAMIENTAS DE SOFTWARE LIBRE"

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: CYNTIA MARIBEL INUCA GONZA.

DIRECTOR: ING. SANDRA NARVÁEZ.

IBARRA-ECUADOR

2015

DECLARACIÓN

Yo, Cyntia Maribel Inuca Gonza, con cedula de identidad N° 1003243639, declaro bajo juramento que el trabajo aquí escrito es de mi autoría, que no ha sido previamente presentada para ningún grado o calificación profesional, y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por la Ley de propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Firma:

Nombre: Cyntia Maribel Inuca Gonza

C.I: 1003243639

Ibarra, Diciembre de 2015.

CERTIFICACIÓN

Certifico que la Srta. Cyntia Maribel Inuca Gonza portador de la cedula de identidad N° 1003243639 estudiante de la Facultad de Ingeniería en Ciencias Aplicadas-Carrera de Ingeniería en Electrónica y redes de comunicación ha desarrollado y terminado en su totalidad el trabajo de titulación **"ADMINISTRACIÓN Y GESTIÓN DE LA RED DE ÁREA LOCAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CAYAMBE, BASADO EN EL MODELO FUNCIONAL DE GESTIÓN DE RED ISO /OSI CON EL PROTOCOLO SNMP Y USO DE HERRAMIENTAS DE SOFTWARE LIBRE"** bajo mi supervisión por la cual firmo su constancia.

ING. SANDRA NARVAEZ

DIRECTORA DE TESIS

UNIVERSIDAD TÉCNICA DEL NORTE

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

Yo, Cyntia Maribel Inuca Gonza, con cédula de identidad Nro. 1003243639, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora de la obra o trabajo de grado denominado: **"ADMINISTRACIÓN Y GESTIÓN DE LA RED DE ÁREA LOCAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CAYAMBE, BASADO EN EL MODELO FUNCIONAL DE GESTIÓN DE RED ISO/OSI CON EL PROTOCOLO SNMP Y USO DE HERRAMIENTAS DE SOFTWARE LIBRE"**, que ha sido desarrollado para optar por el título de: Ingeniera en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, Diciembre del 2015.

Firma:

Nombre: Cyntia Maribel Inuca Gonza

C.I.: 1003243639

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

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

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100324363-9		
APELLIDOS Y NOMBRES:	Cyntia Maribel Inuca Gonza		
DIRECCIÓN:	Otavalo-Gonzales Suarez-Pijal Bajo		
EMAIL:	mab_c6@yahoo.es		
TELÉFONO FIJO:	062918-564	**TELÉFONO MÓVIL:**	0982616919

DATOS DE LA OBRA		
TÍTULO:	ADMINISTRACIÓN Y GESTIÓN DE LA RED DE ÁREA LOCAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CAYAMBE, BASADO EN EL MODELO FUNCIONAL DE GESTIÓN DE RED ISO /OSI CON EL PROTOCOLO SNMP Y USO DE HERRAMIENTAS DE SOFTWARE LIBRE	
AUTOR:	Cyntia Maribel Inuca Gonza	
FECHA:	Diciembre del 2015	
SOLO PARA TRABAJOS DE GRADO		
PROGRAMA:	■ PREGRADO	☐ POSGRADO
TITULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación	
ASESOR:	Ing. Sandra Narváez.	

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Cyntia Maribel Inuca Gonza, con cédula de identidad Nro. 1003243639, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, Diciembre del 2015.

EL AUTOR:

Firma: 

Nombre: Cyntia Maribel Inuca Gonza

CI.1003243639

AGRADECIMIENTO

Agradezco primero a Dios, por bendecirme cada día, cada hora, en mi etapa de estudiante, para poder alcanzar uno de mis objetivos, graduarme como Ingeniera en Electrónica y Redes de Comunicación.

Agradezco a mi familia por haber estado junto a mí y brindarme su apoyo incondicional hasta el final de mi carrera, su paciencia, trabajo y sacrificios por darme una buena formación han dado sus frutos.

Agradezco a la Universidad Técnica del Norte, a la Facultad de Ingeniería en Ciencias Aplicadas, y docentes de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, por haber compartido sus conocimientos, experiencias, e inculcar valores como, respeto, honestidad, compañerismo, puntualidad y ética, para crecer como buenos profesionales.

Agradezco a la Ing. Sandra Castro e Ing. Sandra Narváez, por guiarme y apoyarme con sus recomendaciones, para el desarrollo de mi tesis.

Agradezco también a la Dirección de TIC, del GADIP Municipio de Cayambe, por darme la oportunidad de desarrollar este trabajo.

DEDICATORIA

Este trabajo va dedicado especialmente a mis padres quienes son mí más preciado regalo, quienes me han brindado siempre su apoyo, me enseñaron buenos valores, y han impulsado en mí las ganas de superarme de forma personal y profesional. A mis tíos, Homero, Pedro, quienes me animaron a través de sus palabras de aliento en momentos difíciles, para no desmayar en el camino hacia mí objetivo, y a una persona especial Wili que ha estado junto a mí, motivándome y animándome a culminar esta etapa de mi vida.

Cyntia Inuca G.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN GENERAL

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, así como también el manejo 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 requerida de su funcionamiento, 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.

ABSTRACT

This project is developed for help improve the availability of local area network, the Municipality of Cayambe GADIP, through functional management model ISO / OSI network, and management areas; configuration, security, fault, performance, and accounting, which allows you to manage the network in an organized, and indicates the functions to be managed.

For network management concerned free software tools deals, as Zentyal and Zenoss, which help monitor the areas of management of the aforementioned model are, Zenoss acts as manager station, which collects information from devices that form part of the network, performance resources, inventories, also management e-mail event notification for the failure caused, for security Zentyal provides a platform for multiple services on a single operating system functions applies firewall, IDS / IPS, OPEN LDAP users control with a captive portal. In this project uses the concept of simple network management protocol, SNMP version 2, which for managed devices are enabled for send to manager the information required for its operation, so the administrator can control the activities used of the network.

All this is part of a network management system that runs on a central network monitoring and management located in the TIC department of the institution, which regulates for through policies and procedures established to manage the network.

It has also proposed a design of network segmentation as an alternative to improve network management.

PRESENTACIÓN

Este proyecto, trata sobre la administración y gestión de la red de área local del Gobierno Autónomo Descentralizado Intercultural y Plurinacional Municipio de Cayambe, basado en el modelo funcional de gestión de red ISO/OSI, con el protocolo SNMP, y el uso de herramientas de software libre, para mejorar la disponibilidad de la red.

Para la realización de este proyecto, se investiga conceptos relacionados a, administración y gestión de redes, el modelo funcional de gestión de red ISO/OSI y el protocolo SNMP, los cuales dan los lineamientos para desarrollar el proyecto.

Se realizó un análisis de la situación actual, recopilando información sobre el estado de su infraestructura, se monitoreó la red, y se aplicó encuestas para saber la satisfacción de los usuarios sobre la red y sus servicios. Mediante este proceso se reconocen los problemas existentes de la red, se determinan sus necesidades y requerimientos. Se establecen políticas y procedimientos a seguir para gestionar la red, y se plantea la creación de un centro de monitoreo de red, que opere funciones siguiendo el modelo funcional de gestión de red, que propone sus áreas de; configuración, seguridad, fallos, rendimiento, y contabilidad mediante un sistema de gestión de red. El sistema de gestión consta de dos servidores, Zentyal para gestión de seguridad, y Zenoss para la gestión de fallos, rendimiento, y contabilidad. La gestión de configuración es todo el proceso de instalación de los aplicativos para los servidores, además en esta área se plantea la segmentación de la red.

Además se realizó el análisis costo beneficio, en el que se ve el ahorro que representa el uso de software totalmente libre, finalmente se exponen conclusiones y recomendaciones,

anexos que consta de la investigación de las herramientas de software libre para monitoreo de la red, y elección de la mejor alternativa, manuales para uso del administrador de la red, y las fuentes bibliográficas, de las cuales se han tomado referencias para desarrollar el proyecto.

.

CAPÍTULO I

1 Antecedentes

Las instituciones públicas generalmente están inmersos en un ambiente de cambios constantes; incremento de personal, reubicación de estaciones de trabajo, renovación de equipos de computación, etc., el administrador de la red debe estar pendiente de estos cambios y adecuar/readecuar las infraestructura de la red, implementar nuevos equipos de comunicación, reconfigurar, etc., es inevitable el crecimiento de la red, siempre existirán necesidades que satisfacer para los usuarios. La complejidad de una red hace que sea difícil mantenerla en correcto funcionamiento.

Por eso es necesario que el municipio de Cayambe adopte un modelo que permita administrar la red de forma organizada, actualmente existen modelos de gestión de red, así también protocolos de gestión de red y aplicaciones de gestión que permiten monitorear la red.

1.1 Problema

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.

1.2 Objetivos

1.2.1 Objetivo General

Administrar y gestionar la LAN del GADIP Municipio de Cayambe, basado en el Modelo Funcional de Gestión de Red ISO/OSI con el protocolo SNMP y el uso de herramientas de software libre, para mejorar la disponibilidad de la red.

1.2.2 Objetivos Específicos.

- Investigar la información relacionada con la administración de red y monitoreo basado en Modelo Funcional de Gestión de Red ISO/OSI y el protocolo SNMP para aplicarla en la LAN del GADIP Municipal del cantón Cayambe.
- Analizar la situación actual de la LAN del GADIP Municipal de Cayambe, recopilando información del estado físico y lógico de la red, a fin de conocer necesidades y requerimientos de la misma.
- Determinar políticas de gestión que describan los requerimientos y necesidades del GADIP Municipal del cantón Cayambe, que permitan cubrir las áreas del modelo planteado.
- Configurar e instalar los elementos del sistema de gestión de red, mediante herramientas de software libre cubriendo las áreas del modelo funcional de gestión de red ISO/OSI para la administración y monitoreo de la LAN.
- Realizar un análisis de costo beneficio través del cual se conocerá la factibilidad del proyecto y los beneficios obtenidos.

1.3 Alcance

El presente proyecto tiene como finalidad administrar y gestionar la LAN del GADIP Municipal del Cantón Cayambe, monitoreando el uso de los recursos de la red.

Como fase inicial se investigará la información relacionada con la administración y gestión de red, protocolo SNMP, Modelo Funcional de Gestión de Red ISO/OSI destacando el papel que desempeña cada una de sus áreas.

Se analizará la situación actual de la LAN, recopilando información del estado físico y lógico de la red, a fin de conocer las necesidades y requerimientos de la misma, para lo cual se elaborará un diagrama topológico que indique la interconexión de los equipos de red, su ubicación, servidores, direccionamiento IP, la red pasiva, si emplean políticas de administración, para conocer el estado operacional de los equipos de la LAN se usará herramientas de software libre el cual se elegirá a través del estándar IEEE 29148, además para conocer datos de satisfacción de la red actual en los usuarios se realizarán encuestas.

Una vez que se estudie la situación actual, junto al administrador se determinarán las políticas de gestión con respecto a la administración de la red y procedimientos a seguir de forma que cubran los requerimientos y necesidades de la LAN, cumpliendo áreas funcionales del modelo de gestión de red de la ISO/OSI.

Se creará un centro de administración y monitoreo para la LAN, basado en el Modelo Funcional de Gestión de Red ISO/OSI que propone las siguientes áreas funcionales; área de configuración, fallas, rendimiento, contabilidad y seguridad, de forma que se administre la infraestructura física como lógica, detecte fallos o cambios en la red, prevenga la saturación

de los recursos de red, obtenga inventarios, provea seguridad de la información y control de usuarios de la red, para lo cual hay que configurar el sistema de gestión de la red como: gestores (servidores), protocolo SNMP (SNMP v2) y los agentes o dispositivos gestionados (equipos de red, servidores, host).

Para el control y monitoreo de la red tenemos las siguientes áreas funcionales:

La gestión de configuración, en el estudio de la situación actual se reunirá toda la información necesaria con respecto a la LAN, debido a que la red interna maneja su direccionamiento IP privado clase C, siendo este un solo dominio de broadcast en el que se encuentran conectados tanto servidores como usuarios, se plantea la segmentación de la red en VLANs, creando así pequeños segmentos según necesidades de la municipalidad, que dividan el tráfico de red, aumentando el rendimiento, además de facilitar la administración y seguridad, posteriormente se habilitará el protocolo SNMP v2 en todos los dispositivos a gestionar (agentes) ya que este protocolo presenta mecanismos de seguridad, mejoras en el intercambio de información de gestión y no es muy complejo, se realizará también la configuración del servidor (gestor) para el monitoreo y administración de la red, con herramientas de software libre elegidas con el estándar IEEE 29148 que cumplan con características como visualización de datos estadísticos, autodescubrimiento de la topología de red, soporte SNMP, que permita la configuración de alertas y notificación de eventos, seguridad, manejo de base de datos entre otras características, de forma que responda a las políticas y requerimientos de la entidad.

Para el control de acceso a los equipos de red se accederá únicamente por ssh, se va aplicar listas de acceso permitiendo conexión solo a un rango de direcciones IP que

pertenece a los administradores, estos serán asociados a una comunidad SNMP, que tendrá los permisos para acceder de forma remota a la información que se haya configurado en los equipos de red, para que el gestor reciba las notificaciones de los equipos gestionados estos deben estar bajo la misma comunidad, y todos los cambios que se realicen en la configuración de los equipos se lo almacenará en un servidor ftp, para que el administrador obtenga respaldos y haga uso de ello cuando sea necesario.

En esta área se establecerán políticas respecto a las configuraciones de equipos y el sistema de gestión de red, para que el administrador no tenga inconvenientes en el ingreso de nuevos equipos o usuarios de la red al sistemas de monitoreo.

En la gestión de seguridad, la institución municipal cuenta con un Firewall muy limitado por eso se configurará el servidor Zentyal que a través de sus funciones como Firewall/Proxy ayudará a proteger la red, permitirá el acceso a grupos de usuarios que pertenecen al Active Directory Open LDAP, y también se habilitará el Sistema de Detección de Intrusos (IDS/IPS) que integra el software Snort que detectará cualquier actividad sospechosa o maliciosa en la red.

Para asegurar y controlar los usuarios de la red local se va a configurar un servidor Active Directory basada en software libre Open LDAP, en el que se va a crear cuentas de usuarios por PC y grupos de usuarios dando acceso a los servicios de red, además de permitir tener una base de datos con información personal de ellos al que se le proporcionara una contraseña única, establecida en base a los requerimientos de la institución.

En esta área se establecerá políticas referentes a los privilegios de los grupos de usuarios y acceso de los servicios de la red.

En el área de gestión de fallos, el software estará monitoreando constantemente el comportamiento de la red para detectar fallos en la LAN, a través del protocolo SNMP los agentes y el gestor intercambian información mediante mensajes SNMP y traps, los cuales notificarán a la estación administradora sobre inconvenientes o cambios en el uso de la red, estos mensajes manejan una jerarquía de alarmas misma que el servidor podrá interpretar, de acuerdo al nivel de gravedad se enviará un correo electrónico a los administradores, utilizando un servidor de correo en este caso se instalará postfix y mailx para realizar las pruebas necesarias de forma que funcione junto al software de monitoreo.

En esta área se tendrán políticas para que el administrador pueda detectar fallas por medio de pruebas preventivas, si ya ocurre la falla aislarla, reparando el elemento de falla, si es el caso reconfigurando de modo que se resuelva el problema además de llevar la documentación respectiva en caso de que la falla persista.

En la gestión de rendimiento se recopilará datos estadísticos sobre uso de recursos, como la carga del procesador, carga de memoria, disco duro, interfaces de red activas, tráfico de la red, tiempos de respuestas, utilización de la red con el objetivo de analizar el comportamiento de la red para determinar niveles de rendimiento y evitar problemas de saturación, a fin de entregar al administrador información que le permita dar una pronta solución a problemas que se den en la red y que se administre de mejor manera los recursos.

Como política se establecerá niveles límite de uso de recursos gestionados (equipos de red, servidores, host) para que funcionen correctamente.

En la gestión de contabilidad se actualizará el inventario registrando la información de cada dispositivo de red que está siendo gestionado y a través de un software se obtendrá reportes de los dispositivos tales como: marca, sistema operativo, dirección IP, dirección MAC, vlan's, entre otros, y además también se tendrá un inventario sobre los usuarios quienes están haciendo uso de la red a través del servidor Open LDAP.

Una vez implementado el sistema de gestión se verificará el cumplimiento de las políticas y el correcto funcionamiento del sistema; se elaborará un manual de políticas y procedimientos basado en el modelo de gestión, la instalación y configuración de los software seleccionados, para uso del administrador.

Finalmente se realizará un análisis costo beneficio a través del cual se conocerá la factibilidad del proyecto, y si los beneficios obtenidos justifican su inversión.

1.4 Justificación

Cada día las instituciones públicas están prestas a dar sus servicios de una forma eficiente, en beneficio de los habitantes, sin embargo esto no es posible si no se cuenta con una infraestructura adecuada y servicios adicionales de Tecnologías de Información y Comunicación, por ello deben cumplir con proyectos que permitan explotar las TIC, para su desarrollo interno y funcional.

Hoy por hoy la administración y gestión las redes es importante ya que ayuda a mantener operativa la red, garantizando un nivel de servicio, e incrementando rendimiento, y eficiencia de la misma, permite además resolver cualquier acontecimiento que afecte su correcta función.

La LAN del GADIP Cayambe maneja un solo esquema de direccionamiento de red al que todos los usuarios existentes están conectados, en vista del crecimiento de usuarios esta se ve afectada ya que la red tiene un número limitado de usuarios, por ello se requiere dividir la red en segmentos (VLANs), haciendo que esta sea escalable, que permita una correcta administración y además se pueda incluir nuevos usuarios e implementar nuevos servicios que requiera el municipio.

Además el departamento de TIC no ha considerado llevar la administración de la red bajo un modelo de gestión, que permita la administración adecuada de la red, por lo que nace la necesidad de llevar control organizado de la red, invitando a plantear un proyecto que permita la administración y gestión adecuada de todos aquellos recursos que conforman la LAN (host, dispositivos de red, servidores, y aplicaciones), siguiendo el Modelo Funcional de Gestión de Red ISO/OSI con el protocolo SNMP y uso herramientas de Software Libre que monitoreará la red, de forma que el administrador tenga una interfaz gráfica amigable, y pueda conocer con detalle el funcionamiento de los recursos, flujo de tráfico, y permita detección de problemas y fallas en la red, llevar inventarios sobre los recursos existentes, dar seguridad a la información y configuraciones establecidas en los equipos de gestión, aportando al mejoramiento de la disponibilidad de la red, tal que los usuarios tengan la satisfacción de un servicio óptimo a través de la red de datos de su entidad.

CAPÍTULO II

2 Fundamentos Teóricos

En este capítulo se realiza la investigación de fundamentos teóricos, que explican los aspectos que conllevan la administración y gestión de una red.

2.1 Introducción a la administración y gestión de redes

Una red está conformada de muchos elementos de comunicación, tanto hardware como software interconectados entre sí, para trasmitir información y compartir recursos, debe ser capaz de soportar diferentes aplicaciones y servicios de comunicación, además de ser escalable y segura.

Actualmente las redes de comunicación son la base fundamental en el trabajo de una entidad o institución, haciéndose imprescindible y creciendo de una forma inmensurable, una falla en la red de datos puede representar la pérdida de mucho dinero, la gestión de red está encaminada prevenir y evitar cualquier inconveniente que afecte su correcto funcionamiento.

El administrador es quien se encarga de mantener operativa la red y siempre disponible para los usuarios, pero el manejo y funcionamiento de una red no solo depende del esfuerzo humano, si no que se ayuda también de herramientas de gestión, que ayude a monitorear y controlar red.

2.2 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.

2.2.1 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.

2.2.2 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.”,

2.2.3 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. Hay tres aspectos fundamentales:

- **Planificación de capacidad:** comprende análisis y planificación de uso del tráfico que opera en la red
- **Planificación de personal:** el número de personas y el nivel de conocimiento que requiere para manejar una red.
- **Vigilancia del desempeño:** análisis de tiempos de respuesta del tráfico de red.

2.2.4 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.

(McLeod, 2000).

2.2.5 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.

Se establecen cuatro fases para el monitoreo de una red:

- Definición de la información de gestión que se monitoriza.
    - Información estática: no cambia con la actividad de la red.
    - Información dinámica: evoluciona con la propia actividad de la red.
    - Información estadística: pos procesado de la información dinámica que proporciona un mayor significado de gestión.

- Acceso a la información de monitorización.
    - Monitoreo remoto de los recursos desde el centro de gestión.
    - Interactúan gestores y equipos gestionados.

- Diseño de mecanismos de monitorización.
    - Sondeo o polling.
    - Event reporting o notificación de eventos.

- Procesado de la información de monitorización.

  A través de las áreas funcionales de gestión de red OSI.
    - Gestión de configuración.
    - Gestión de fallos.
    - Gestión de rendimiento.
    - Gestión de contabilidad.
    - Gestión de seguridad. (Stacey, 2001)

2.3 ¿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.

  (Perpinan, 2004, pág. 204) (Romero)

2.4 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.

(Martí, 1999, pág. 15)

2.5 MODELOS DE GESTIÓN DE RED

En un principio las redes de comunicación eran pequeñas, era fácil identificar un problema en la red, simplemente a través de un ping se sabía dónde está la falla, pero hoy este método es ineficaz, en respuestas a esta situación se define lo que se denomina modelos de gestión de red, existen tres modelos:

- **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.

2.5.1 Gestión de red OSI.

La ISO define a la gestión de red como las facilidades para controlar, coordinar y monitorizar los recursos que permiten dar lugar a la comunicación en un entorno OSI. (Union, 1992)

La gestión de OSI, presenta varios modelos como se resumen en la Figura 1.

---

[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.

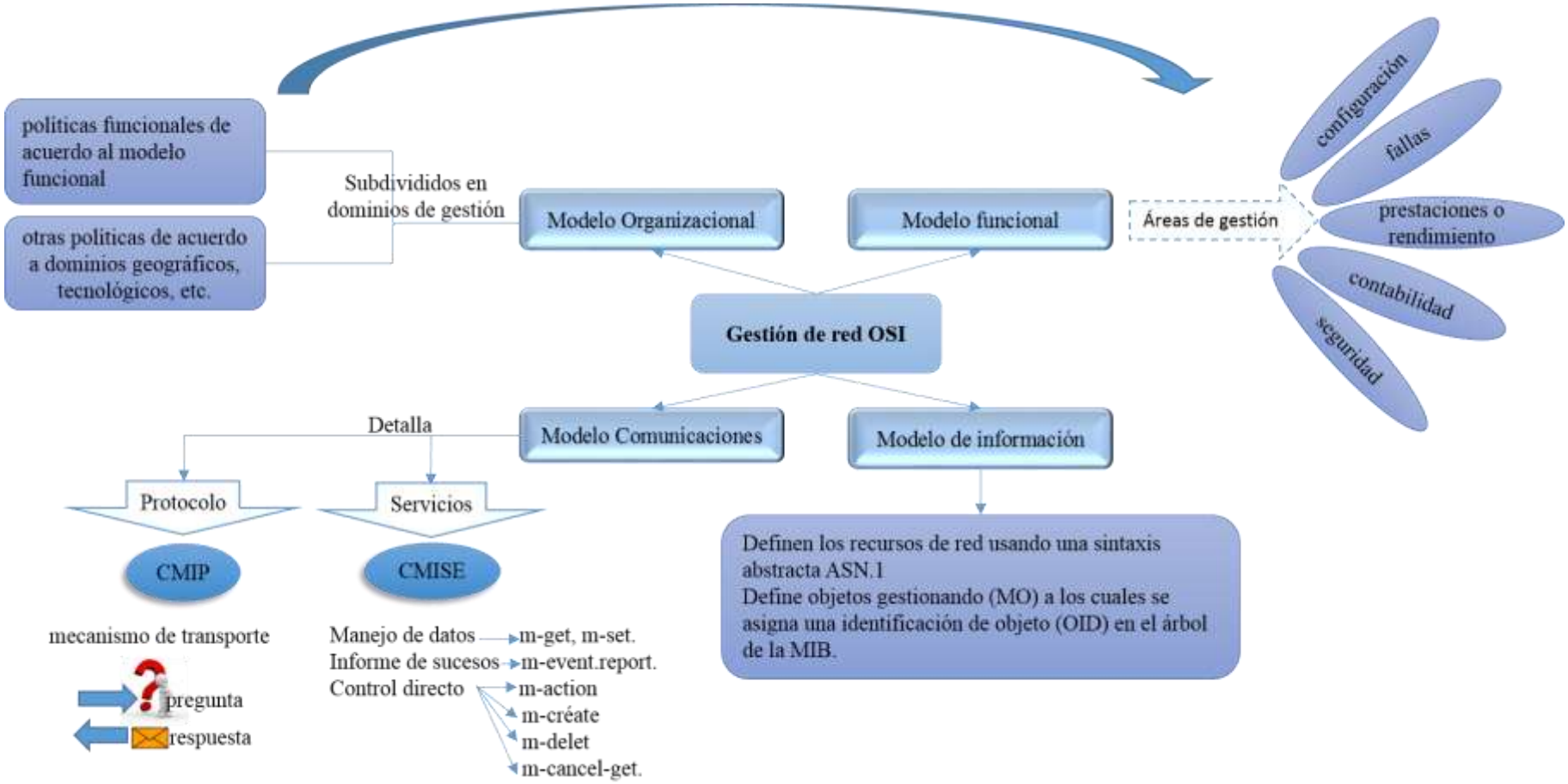


Figura 1. Modelo de gestión de red OSI.

Fuente: Antoni Barba Martí. (1999). Gestión de red. Editorial: UPC. Cataluña.

2.5.1.1 *Modelo funcional de gestión de red OSI.*

Más conocido como modelo FCAPS, este es un modelo bien estructurado que divide las funciones de administración de redes, en cinco áreas de gestión, la Figura 2, muestra las áreas comprendidas en este:

Figura 2. Áreas de gestión del modelo funcional de gestión de red ISO.
Fuente: (Millan Tejedor, Gestion de Red, 1999)Obtenido de http://www.ramonmillan.com /tutoriales/ gestionred.php#ISO

A continuación se detalla las funciones de cada área de gestión:

2.5.1.1.1 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.

2.5.1.1.2 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.

2.5.1.1.3 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.

2.5.1.1.4 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.

2.5.1.1.5 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.

(Union, 1992, págs. 3-4) (Millan Tejedor, Gestion de Red, 1999)

2.6 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, está diseñado para ver la red como una arquitectura unificada. (Stallings, Comunicaciones y Redes de Computadoras, 2004, pág. 795)

2.6.1 Elementos de un sistema de gestión de red.

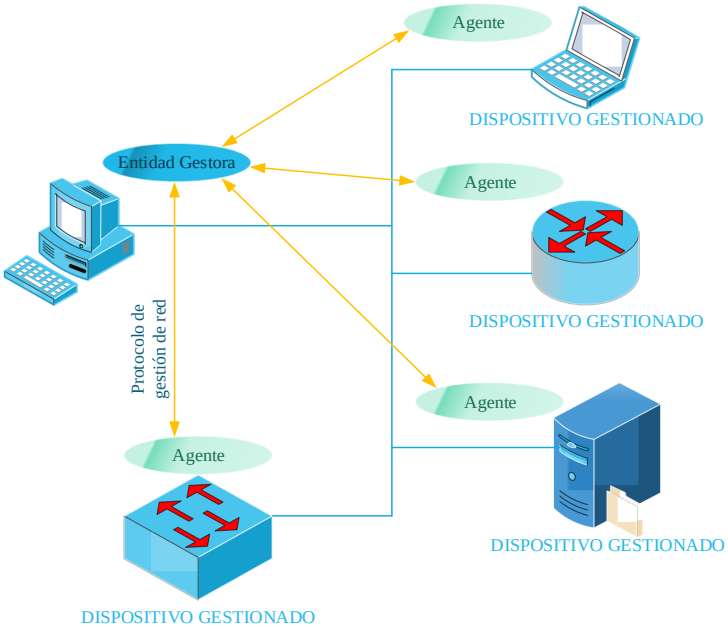


Figura 3. Elementos de un sistema de gestión de red

Fuente: James Kurose. (2013).Redes de Computadoras. Editorial: PEARSON. Estados Unidos.

2.6.1.1 *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.

2.6.1.2 *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:** Pueden ser 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.
- **Base de información de gestión (MIB):** Los objetos gestionados tienen asociados distintos elementos de información que se recopilan en una base de información de gestión (MIB).
- **Agente:** Es el 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.

(Kurose & Ross, págs. 6-7) (IETF, 1990)

2.7 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. Es un protocolo estándar de gestión para trabajar en entornos TCP/IP, además es compatible con la gestión de red OSI.

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

2.7.1 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] (*Abstract Syntax Notation One*), que es una notación independiente del hardware y el sistema de operación. Este leguaje es necesario para garantizar la sintaxis y la semántica de los datos de gestión de red, de forma que estén bien definidos y no exista ambigüedad. SNMP por simplicidad utiliza un solo subconjunto de las reglas de codificación básicas de ASN.1 que es el BER[9] (*Basic encoding rules*).

[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.

[9] BER son reglas de codificación básicas, para trasmitir información a través de la red.

2.7.2 Base de información de gestión (MIB).

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

Existen tipos de MIB, MIB-I es la primera MIB normalizada, formada con objetos de una torre de protocolos TCI/IP, MIB-II con algunas modificaciones de la primera versión de MIB. También existe las MIB Experimentales que están en desarrollo y MIB Privadas: corresponden a MIBs de productos específicos.

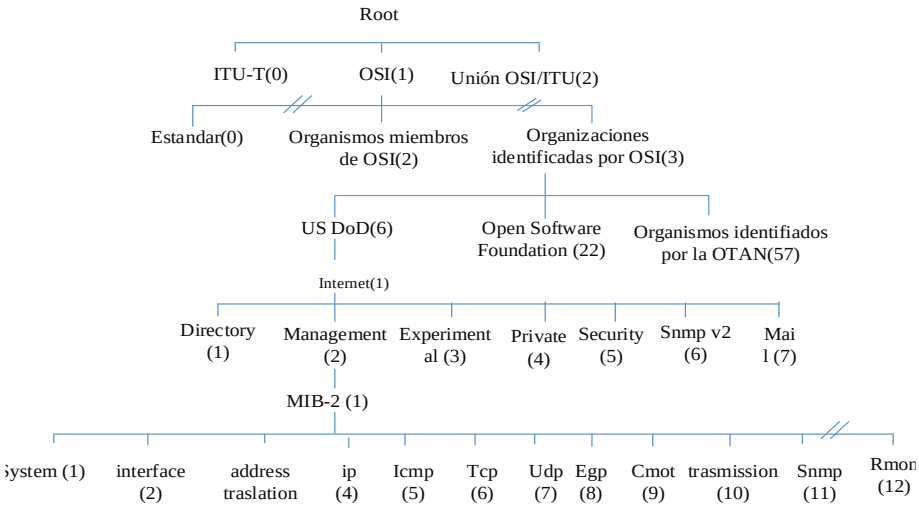


Figura 4. Árbol de registro MIB-II.

Fuente: James Kurose. (2013).Redes de Computadoras. Editorial: PEARSON. Estados Unidos.

2.7.3 Funcionamiento de la arquitectura SNMP.

El modelo de arquitectura SNMP es un conjunto de elementos de red y estaciones de gestión de red. 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.

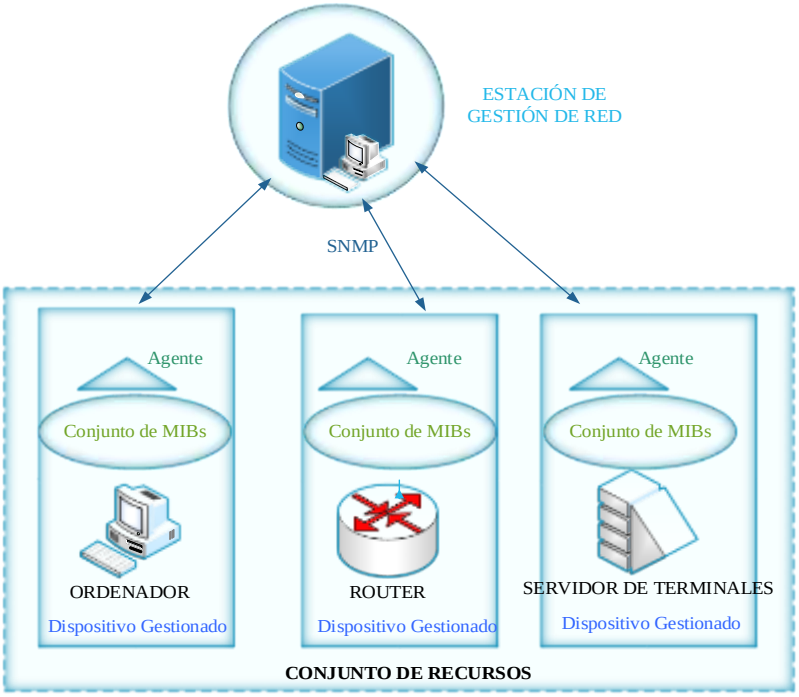


Figura 5. Arquitectura de gestión SNMP.
Fuente: Antoni Barba. (1999). Gestión de red. Ediciones UPC. Barcelona.

2.7.3.1 *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.

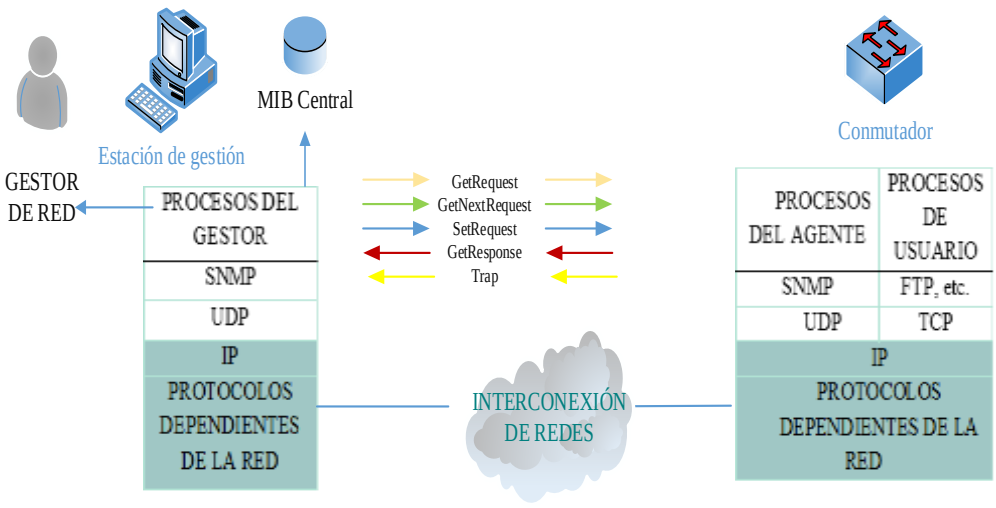


Figura 6. Comunicación entre entidades de gestión.

Fuente: William Stallings. (2004). Comunicación y redes de computadores. Editorial: PEARSON. Madrid.

2.7.3.2 *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.

2.7.3.3 *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 de mismo.

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.

2.7.4 Versiones de SNMP.

2.7.4.1 *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 lo que utiliza el 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 que establece una relación entre gestores y agentes, como un método de seguridad. Su uso se expandió enormemente, y se empezó a notar algunas deficiencias, como la imposibilidad de especificar de una forma sencilla la transferencia de grandes bloques de datos y ausencia de mecanismos de seguridad, por lo que surge SNMP v2.

2.7.4.2 *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 (SMI), ahora se usa 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.

2.7.4.3 *SNMP v3.*

SNMP v1 y v2 manejan un concepto de comunidad como método de seguridad, para permitir acceso a la información de gestión entre entidades gestor y agente, obviamente las entidades gestionadas de una red deben pertenecer a una comunidad para poder acceder, recuperar y proporcionar información de gestión.

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.

(Mauro & Schmidt, 2005) (Stallings, Comunicaciones y Redes de Computadoras, 2004, págs. 794-805)

2.7.5 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.

2.7.6 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.

2.7.7 Comparación SNMP y CMIP.

SNMP Y CMIP son los protocolos más importantes de gestión de red, en los últimos tiempos. SNMP es un protocolo de capa aplicación, usado en redes TCP/IP, y considerado el estándar de facto después del protocolo CMIP utilizado en grandes operadoras de telecomunicaciones. CMIP es un protocolo bien elaborado, desarrollado teniendo en cuenta errores y fallas de SNMP, de manera que sea más potente, pero su complejidad desestimo su uso. SNMP ha evolucionado, actualmente existe SNMP v1, v2, y v3, en las cuales se ha corregido sus deficiencias, incrementando su funcionalidad, con el tiempo este puede desplazar al protocolo CMIP.

Tabla 1. *Comparación CMIP y SNMP.*

CMIP	SNMP
Complejo para los programadores	Sencillo
Requiere 10 veces más recursos de red que SNMP	No requiere gran cantidad de recursos
Implementación de protocolos OSI en routers y plataformas resulta caro	SNMP opera sobre varios protocolos de transporte normalmente UDP, OSI, CNLS, AppleTalk, y Novel IPX
Muy pocas redes soportan CMIP en su totalidad	Soporte de varias plataformas comerciales de gestión de red multi-fabricantes.
Trabaja en modo conectado.	Trabaja con sondeo.
Ofrece mayor seguridad.	Vulnerable en seguridad en las primeras versiones, corregido en SNMP v3.

Fuente: (Millan Tejedor, Tendencias en gestión de red, 2004) Obtenido de http://www.ramonmillan.com/tutoriales/tedenciasgestionred.php

(Millan Tejedor, Tendencias en gestión de red, 2004)

2.8 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:** Comprende esta tarea la labor de instalación de una nueva red o modificación de la ya existente, para lo cual se debe determinar el material necesario, cableado, equipos de comunicación, etc.

- **Preparación de red:** terminada la fase de planificación, se debe proceder a la preparación de la red donde; se instalaran servidores y los servicios de red, impresoras, sistemas de Backup, etc., se preparan las estaciones de trabajo, incluyendo las tarjetas, el software de red, etc., y se prepara la documentación necesaria donde se refleja el mapa de red.

- **Organización y configuración:** Se organiza el espacio de almacenamiento de ficheros personales y compartidos. Se define también los grupos de trabajo, y derechos de cada uno de estos grupos y miembro particulares.

- **Gestión de cambios:** Esta es la que se podría decir diaria de los administradores de la red de la que deben dejar constancia, comprende los trabajos de instalación

de programas, altas y bajas de usuarios, cambios de grupos, cambios de los equipos, etc.

- **Gestión de problemas:** El control y la localización del origen de los problemas.

- **Seguridad:** Comprende dos aspectos fundamentales:
    - programar y mantener las copias de seguridad de los datos.
    - garantizar la integridad de los datos. (control de acceso, contraseñas, etc.)

- **Optimización:** El administrador de la red deberá distribuir los recursos de forma dinámica para que el rendimiento de la red sea siempre el más alto posible, observando su funcionamiento y haciendo los cambios oportunos con mucho tacto ya que los cambios que pueden beneficiar a algunas prestaciones pueden perjudicar a otras.

- **Mantenimiento de la documentación:** Todos los cambios que sufra la configuración de la red, así como la originaria de su instalación y configuración inicial, deben ser documentados, y será tarea del administrador de la red, el mantenimiento de dicha documentación. La documentación de la red suele estar estructurada de la siguiente forma:
    - **Documentación de la administración:** la tarea que realice el administrador.
    - **Mapas de cables:** donde se reflejara toda la información referente al cableado.

- **Información sobre vendedores:** Se debe guardar toda la información referente a los vendedores que han suministrado cada producto ya sea software o hardware, para posibles consultas. Se tendrán almacenadas facturas, garantías, manuales, etc.
- **Información y atención a los usuarios:** Debe dar ciertas instrucciones de cómo funciona la red, aplicaciones, y manejo de equipos terminales.
- **Planificación de backups:** Se debe tener bien documentado el calendario de realización de copias de seguridad.

- **Documentación de mantenimiento:** Las operaciones de mantenimiento que se realicen sobre cada máquina deberá ser documentado así como los fallos que hubieran producido en cada una de ellas y las soluciones acopladas.

- **Monitorización y control de tráfico:** la calidad del servicio de red que se está prestando no solo depende del buen funcionamiento de la misma, toma en parte otros factores entre los que destaca la detección y anticipación a los posibles errores que se puedan producir, para poder garantizarla; un punto fundamental a tener en cuenta es la monitorización o evaluación y administración del uso de los recursos de la red.

  En el control del tráfico de la red existen tres aspectos fundamentales a tener en cuenta: sesiones de usuario, recursos compartidos y recursos en uso.

(Comunidad Autonoma de Castilla y Leon, 2006, págs. 286-287)**.**

CAPÍTULO III

3 Análisis de la Situación Actual

Este capítulo 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), para lo cual se investigan las dependencias que se interconectan a la LAN, infraestructura física y lógica de la red, y se realizan encuestas a los usuarios, con el objetivo de conocer sus necesidades y requerimientos para mejorar la administración de la red.

3.1 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”.

3.1.1 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.

3.1.1.1 *Misión.*

Articular esfuerzos y recursos tecnológicos a efectos de que constituyan una herramienta de gestión para la conectividad social en el cantón, y para apoyo a cada proceso o subproceso de la institución, generando una cultura de servicio a la comunidad y acceso igualitario a nuevas tecnologías de la comunicación.

3.1.1.2 *Estructura.*

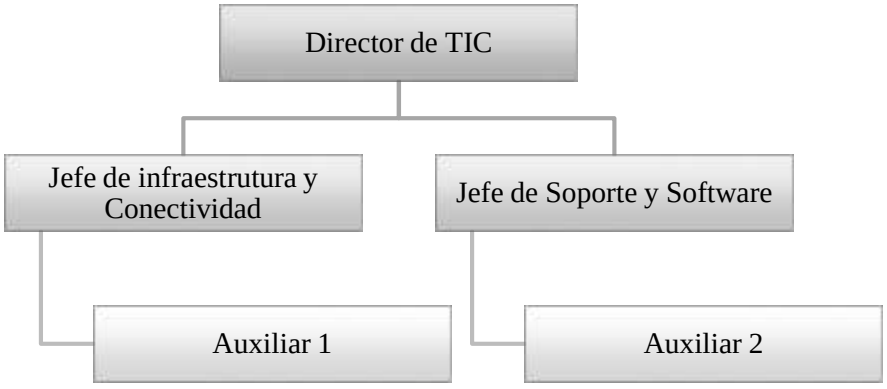


Figura 7. Estructura de la Dirección de TIC-GADIPMC
Fuente: Dirección de TIC del GADIPMC

3.1.1.3 *Funciones.*

El Director de TIC, es el máximo responsable de la Dirección de TIC, se encarga de gestionar, tramitar, autorizar, los proyectos que se ejecuten en esta dirección, implementación de servidores, recomendaciones y dotación de nuevos equipos tecnológicos

para mejorar la infraestructura de la red, brindar conectividad a la población, y la red interna (LAN) de la municipalidad, brindar seguridad tanto física como lógica, capacitación y manejo de software libre, automatización de procesos, manejo de la página web del municipio, etc.

La dirección de Tecnologías de la Información, cuenta con las siguientes jefaturas:

- Jefatura de Soporte y software.
- Jefatura de Infraestructura y Conectividad.

El **Jefe de Soporte y Software** es el encargado de diseño y programación de sistemas informáticos que ayuden a automatizar los procesos de la institución, instalación de paquetes de software a los distintos sistemas operativos, así como dar mantenimiento y soporte técnico de dichos sistemas.

El **Jefe de Infraestructura y Conectividad**, es encargado del correcto funcionamiento de la infraestructura y operaciones de red, tanto de la red local como la red inalámbrica de las instituciones. Responsable de planificar los requerimientos de la red como implementación de nuevos equipos y servicios, localización y resolución de problemas en la red, proveer seguridad física y lógica, y mantener operativa la red con un nivel de disponibilidad aceptable.

Los **Auxiliares**, ayudan a ejecutar proyectos correspondientes a su jefatura, atender los requerimientos de los usuarios, brindando soporte técnico y resolución de problemas existentes ya sea hardware o software.

3.2 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.

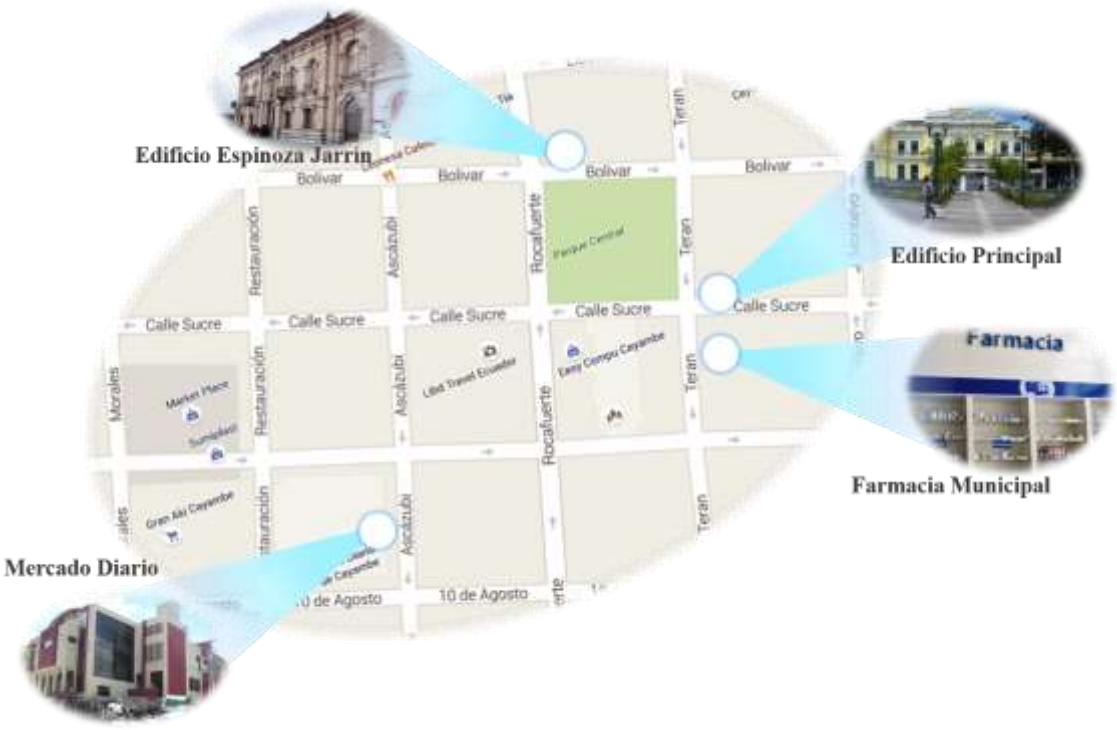


Figura 8. Ubicación de dependencias del GADIPMC.

Fuente: Adaptado de Google Maps.

3.2.1 Edificio principal.

El edificio principal se encuentra ubicado en la ciudad de Cayambe, provincia de Pichincha, en las calles Terán S0-54 y Sucre.

Figura 9. Edificio principal del GADIPMC
Fuente: Fotografía tomada por Cyntia Inuca.

Es una infraestructura física de dos plantas, en la planta alta se encuentra el Data Center junto a la Dirección de Tecnologías de Información y Comunicación, es el área principal de la infraestructura de la red de datos.

A continuación se detalla los departamentos ubicados en el edificio principal y su número de usuarios. Debido a la expansión del edificio se lo divide en dos secciones. En la Tabla 2, se detalla la planta baja, y la Tabla 3, muestra los departamentos de la planta alta.

Tabla 2. *Departamentos de la planta baja del edificio principal.*

PLANTA BAJA		
	DEPARTAMENTOS	**N° USUARIOS**
SECCIÓN 1	Coactivas	2
	Contabilidad	3
	Rentas	3
	Tesorería	6
	Dirección de Avalúos y Catastros	2
	Jefatura de Avalúos y Catastros Urbano y Rural	6
	Dirección de Gestión Financiera	5
	Coordinación General	5
	Guarda Almacén	4
	Comisariato Municipal	2
SECCIÓN 2	Dirección de Desarrollo Territorial	5
	Administración Urbana y Rural	2
	Comisaria de Construcciones	1
	Recepción	2
	Centro de Mediación	3
	Dirección de Medio Ambiente	6
	Comisaria Municipal	2
	Total de usuarios	59

Fuente: Inventario de direcciones IP del GADIPMC.

Tabla 3. *Departamentos de la planta alta del edificio principal.*

PLANTA ALTA		
	DEPARTAMENTO	**N° USUARIO**
SECCIÓN 1	Alcaldía	2
	Secretaria alcaldía	2
	Dirección Asesoría Jurídica	6
	Dirección de TICS	4
	Concejales	6
	Vice alcaldía	2
	Recursos Hídricos y Topografía	5
	Compras Publicas	2
	Desarrollo Comunitario	3
	Dirección de Desarrollo Físico	6
	Fiscalización	4
SECCIÓN 2	Talento Humano	6
	Auditoria Interna	3
	Dirección de Gestión Administrativa	4
	Transporte Liviano	2
	Servicio Generales y Proveeduría	1
	Dirección de Transito	3
	Total de usuarios	61

Fuente: Inventario de direcciones IP del GADIPMC.

3.2.2 Edificio Espinoza Jarrín.

Este edificio se encuentra ubicado en Cayambe, provincia de Pichincha en las calles Ascázubi y Rocafuerte, es una infraestructura antigua remodelada de dos plantas.

Figura 10. Edificio Espinoza Jarrín del GADIPMC.

Fuente: Fotografía tomada por Cyntia Inuca.

En la segunda planta está instalado un Rack de equipos de comunicación, junto al Info-Centro, el mismo que se enlaza a través de fibra óptica desde el edificio principal. Aquí funcionan los siguientes departamentos:

Tabla 4. *Departamentos del GADIPMC en el edificio Espinoza Jarrín.*

EDIFICIO ESPINOZA JARRÍN

PLANTA	DEPARTAMENTOS	N° USUARIOS
BAJA	Dirección de Desarrollo Económico	5
ALTA	INFO-CENTRO	21
	Dirección de Comunicación	6
	Dirección de Cultura y Deportes	5
	Dirección de Educación	2
	Biblioteca Municipal	2
	Total de usuarios	36

Fuente: Inventario de direcciones IP del GADIPMC.

3.2.3 Dependencias que están ubicadas en otros sitios de la ciudad.

La Administración de Mercados es la única entidad que cumple funciones que competen al municipio, y está ubicada fuera de las instalaciones del municipio, se halla en el último piso del Mercado Diario, se conecta a la LAN a través de un enlace inalámbrico, y provee conexión a 3 usuarios.

3.2.4 Entidades independientes.

A continuación se detallan algunas entidades que pese a ser independientes trabajan en conjunto con el municipio y también se conectan a la LAN del GADIPMC, algunas de ellas están ubicadas en los edificios del municipio y otras se encuentra fuera.

Tabla 5. *Entidades independientes ubicadas en las instalaciones del GADIPMC.*

ENTIDAD	N° USUARIOS	UBICACIÓN
EMAPAAC	25	Planta baja del edificio principal GADIPMC, sección 2
SIGTIERRAS	3	Planta baja del edificio principal GADIPMC, sección 1.
SEGURIDAD CIUDADANA	4	Planta baja edificio Espinoza Jarrín GADIPMC
JUNTA DE LA NIÑEZ Y ADOLESCENCIA	2	Planta baja edificio Espinoza Jarrín GADIPMC
CONCEJO DE LA NIÑEZ Y ADOLESCENCIA	4	Planta baja edificio Espinoza Jarrín GADIPMC
UNIDAD EJECUTORA DE PROTECCION DE DERECHOS	38	Planta baja edificio Espinoza Jarrín GADIPMC
Total usuarios	66	

Fuente: Inventario de direcciones IP del GADIPMC.

Tabla 6. *Entidades independientes ubicadas fuera de las instalaciones del GADIPMC*

ENTIDAD	UBICACIÓN	OBSERVACIONES	N° USUARIOS
CONMUJER	Centro Comercial Popular	Pertenece a la red interna del municipio a través de un enlace de radio.	2
FARMACIA MUNICIPAL	Terán y Sucre frente al municipio	Tienen un enlace a través de cable UTP y pertenecen a la red interna del municipio	3
Total usuarios			5

Fuente: Inventario de direcciones IP del GADIPMC.

Aproximadamente se tiene como 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, como impresoras, y routers inalámbricos, ante los constantes cambios en la institución se ve el crecimiento de usuarios y por ende se instalan equipos adicionales como switch no administrables, routers inalámbricos, para abastecer al resto de usuarios que ingresan al municipio.

3.3 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.

3.3.1 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.

3.3.2 Enlaces de Backbone.

En el edificio principal actualmente existen 4 racks interconectados de la siguiente manera:

- El rack 1 y rack 2 se interconecta a través de fibra óptica.
- El rack 1 y rack 4 se interconecta a través de cable CAT 6A UTP.
- El rack 2 y rack 3 se interconecta a través de cable CAT 6A UTP.
- El rack 2 y rack 6 se interconectan a través de cable CAT 6A UTP.

Enlace hacia el info-centro:

- El rack 1 y rack 5 se interconecta a través de fibra óptica.

(Diego Borja, 2012)

3.3.2.1 *Ubicación de los Racks.*

Tabla 7. *Ubicación de Racks.*

N° DE RACKS	EDIFICIO	DEPARTAMENTO
RACK 1	Edificio Principal	Data Center- Departamento Tics
RACK 2	Edificio Principal	Departamento Concejalía-sección 2
RACK 3	Edificio Principal	Departamento de Gestión de Desarrollo Territorial
RACK 4	Edificio Principal	Avalúos y Catastros
RACK 5	Edificio Espinoza Jarrín	Info Centro
RACK 6	Edificio Principal	EMAPAAC

Fuente: Departamento de TIC del GADIPMC.

3.3.3 Data Center.

El Municipio de Cayambe, cuenta con un Data Center a través del cual funciona la red de datos, ubicado en el departamento de las TIC, fue construido bajo el estándar TIA 942, que tiene una serie de recomendaciones y directrices para instalación de infraestructura de un centro de datos, siendo su objetivo alcanzar un nivel de disponibilidad aceptable.

El Data Center alberga varios equipos de comunicación, sistemas informáticos, sistemas de climatización, energía y seguridad, allí se encuentran la conexión principal de proveedor de internet para luego distribuirlos a través de la red local a los usuarios finales.

Figura 11. Vista frontal e interior del Data Center.

Fuente: Fotografía tomada por Cyntia Inuca.

El Data Center cumple ciertos parámetros de los subsistemas que se debe tomar en cuenta para su diseño, en la Tabla 8**,** se detalla cuatro subsistemas; eléctrico, mecánico, arquitectónico, y de telecomunicaciones.

Tabla 8. *Parámetros que cumple el Data Center del GADIPMC.*

SUBSISTEMA	PARÁMETROS
Eléctrico	Tiene instalado un sistema de distribución de energía.
	Protección a través TVSS tipo B.
	Interconexión de un sistema de alimentación ininterrumpida (UPS).
	Cuentan con un generador eléctrico en casos de cortes de energía.
	Iluminación con lámparas empotrables de techo.
	No hay un control ni monitoreo ambiental y de potencia.
	No poseen un sistema de puesta a tierra.
Mecánico	Cuenta con aire acondicionado.
	No hay protección contra incendios.
Arquitectónico	Posee piso falso y techo falso.
	Dispone de control de acceso en la puerta.
	Es un cuarto totalmente cerrado.
Telecomunicaciones	Existe un solo proveedor de servicio de internet.
	Medios de trasmisión de backbone son fibra óptica y cable UTP Cat 6A.
	Para partir el sistema de cableado estructurado cuenta con patch panels Cat 6A.
	Existe documentación sobre proyecto de cableado estructurado y certificación de puntos en el edificio principal.
	No se maneja una red jerarquizada (no hay switch de Core)
	No hay redundancia de equipos de comunicación.
	No existe documentación sobre los servidores, ni equipos de comunicación.

Fuente: Departamento de TIC del GADIPMC.

3.3.3.1 *Elementos dentro del Data Center.*

Dentro del Data Center se encuentran alojados los equipos principales que permiten la comunicación de la red interna de la municipalidad, así como también equipos de comunicación que dan servicio de internet a la red inalámbrica de las instituciones educativas de cantón.

A continuación se detalla los siguientes:

Tabla 9.*Elementos de Data Center.*

CANT.	ELEMENTOS
6	Servidores físicos
1	Pantalla Samsung
2	Router Cisco System 800 S (Proveedor de Internet para red interna LAN, y red inalámbrica de las instituciones educativas respectivamente)
1	Router inalámbrico Cisco Small Business (Provee WI-FI, equipo conectado a la red inalámbrica)
1	Router Cisco Asa 5505 S (VPN SIGTIERRAS)
1	Firewall Netcyclon marca Supermicro
3	Switch Cisco SF 100-24 Switch Cisco 2960 S Switch HP v1910-24g
2	Patch panels marca Panduit Cat 6.
3	UPS marca Computer Power de 6KVA. UPS marca Tripp Lite de 2.2 KVA Smart UPS RT 1500 marca APC
1	Aire acondicionado marca Electrolux
4	Convertidores de fibra óptica
2	Regletas de energía

Fuente: Departamento de TIC del GADIPMC.

3.3.3.2 *Servidores.*

A través de la LAN del municipio se brinda varios servicios a los usuarios, estos se encuentran instalados en servidores físicos mismos que están ubicados en el Rack de servidores dentro del Data Center, a continuación se detallan sus características.

Tabla 10. *Servidores y sus características.*

SERVIDOR		CARACTERÍSTICAS	
Servidor de Base de Datos		**Marca**	HP Proliant DL 380 67
		Sistema Operativo	Windows server 2003
		Base de Datos	My SQL
		Software de Aplicación	Olympo (Sistema Contable Financiero)
			SIM (Sistema de Información Municipal)
		Función	Mantener una base de datos segura para usuarios que manejan los sistemas financieros del municipio
Servidor de Archivos		**Marca**	ALTEK
		Sistema Operativo	Ubuntu 12.04
		Paquete Instalado	Samba
		Software de Aplicación	Olympo (Sistema Contable Financiero)
			SIM (Sistema de Información Municipal)
		Función	Respaldar información relevante a través de un servidor de archivos en la red para los usuarios de los departamentos de la municipalidad
Servidor Proxy		**Marca**	HP Proliant ML 310 EGN 8
		Sistema Operativo	Centos 6
		Paquete Instalado	Apache
		Función	Restringir acceso a redes sociales y videos en línea para mejorar la productividad del trabajo de los usuarios de la red y evitar la saturación de la red.

Servidor Dataflow		**Marca**	HP Proliant ML 310 EGN 8
		Sistema Operativo	Windows 7
		Base de Datos	My SQL
		Función	Realizar un seguimiento de trámites de forma que se dé una respuesta rápida a las solicitudes ingresadas al municipio.
Servidor SIGTIERRAS		**Marca**	DELL
		Sistema Operativo	Centos6
		Software de Aplicación	Sistema Nacional de Administración de Tierras (SINAT)
		Función	El software de aplicación es un sistema de información para la gestión catastral de los predios rurales de todo el país y apoya el registro de la propiedad de cada uno de los municipios donde haya intervenido el Programa SIGTIERRAS.

Fuente: Departamento de TIC del GADIPMC.

3.3.3.3 *Firewall NETCYCLON.*

Sirve para dar seguridad a la red de área local del GADIPMC, el tráfico de la red pasa obligatoriamente por este sistema de seguridad, filtrando acceso a contenidos y páginas web, por http.

Figura 12. Firewall Netcyclon.

Fuente: Fotografía tomada por Cyntia Inuca.

3.3.3.4 *Switchs (Conmutadores).*

El Data Center tiene implementado switchs de varias marcas que actúan como switch de acceso, para la conexión de usuarios.

Tabla 11.*Switch ubicados en el Data Center.*

SWITCH	CARACTERÍSTICAS	FUNCIÓN
SWITCH CISCO SF 100-24 	Capa 2 No administrable 24 puertos	Constituye uno de los equipos principales para la red inalámbrica de las instituciones educativas y parques de la ciudad.
SWITCH CISCO 2960 S1 	Capa 2 Administrable 24 puertos	Es el switch principal para la interconexión de la red interna (LAN) del municipio. (enlaces de backbone)
SWITCH HP V1910 J600A 	Capa 3 Administrable 24 puertos	Es utilizado para la interconexión de los usuarios en la sección 1 de la planta alta del edificio principal.

Fuente: Departamento de TIC del GADIPMC.

3.3.3.5 *Convertidores de fibra óptica.*

Ya que el medio de trasmisión utilizado para la recepción del servicio de internet es fibra óptica, se cuenta con convertidores de fibra, para realizar la conversión de la señal óptica a señales eléctricas y distribuir el servicio a los usuarios a través de cable de cobre.

Tabla 12. *Convertidores de Fibra Óptica*.

TRANSEIVERS	VELOCIDADES	ENLACE
Since 1993	10/100 Base WDM	Proveedor de Internet CNT (LAN)
CTC Union Since 1993	10/100 Base WDM	Proveedor de Internet CNT (Red inalámbrica)

Fuente: Departamento de TIC del GADIPMC.

3.3.3.6 *Sistema de alimentación ininterrumpida (UPS).*

El sistema de alimentación ininterrumpida (UPS) proporciona energía eléctrica a los equipos que se encuentran en el Data Center durante un cierto tiempo cuando surge algún problema eléctrico, protegiéndolos y evitando que sufran daños irreparables.

Dentro del Data Center se encuentran instalados los UPS, mismos que están interconectados al tablero de distribución de energía.

Figura 13. Tablero de distribución de energía.
Fuente: Fotografía tomada por Cyntia Inuca.

3.3.3.6.1 UPS marca Computer Power de 6KVA.

Figura 14. UPS Computer Power.
Fuente: Obtenido de http:// www.firmesa.com/web/images/febrero2013/6a10.pdf

3.3.3.6.2 UPS marca Tripp Lite de 2.2 KVA.

Figura 15. UPS Tripp Lite.

Fuente: Obtenido de http://www.tripplite.com/on-line-double-conversion-ups-system-2.2kva-tower-110v-120v-nema-outlets~SU2200XLA/

3.3.3.6.3 Smart UPS RT 1500 VA marca APC.

Figura 16. Smart UPS

Fuente: Obtenido de http://www.apcguard.com/SURTA1500RMXL2U.asp

3.3.3.7 *Aire Acondicionado.*

La función del aire acondicionado es mantener a los equipos a una temperatura adecuada, de forma que no genere calor y mantenga su vida útil.

Figura 17. Aire Acondicionado.

Fuente: Fotografía tomada por Cyntia Inuca.

3.3.4 Racks Secundarios.

Los racks secundarios, alojan varios switchs que interconectan la red local y sus usuarios, debido a la expansión de las instalaciones del municipio, están ubicados en varias partes.

3.3.4.1 *Rack 2.*

Ubicado en el departamento de concejalía, este es un rack de piso, se interconecta al rack principal (Rack 1) a través de fibra óptica, aquí se aloja elementos que están en la Tabla 13.

Figura 18. Rack 2.
Fuente: Fotografía tomada por Cyntia Inuca.

Tabla 13.*Elementos del Rack 2.*

CANT.	ELEMENTOS	CARACTERISTICAS	FUNCIÓN
1	Convertidor de fibra óptica	Fiber Media Converter MMF	Convertir señales ópticas de la fibra óptica a señales eléctricas para el cable UTP CAT 6.
2	Switch HP v1910	24 puertos Administrable Capa 3	Permite la conexión de los usuarios a la red en la sección 2 la planta alta del edificio principal.
2	Patch panel	Panduit Cat 6 24 puertos	Distribuye el cableado estructurado.
1	Regleta de energía	-	Proveer energía a los equipos de comunicación.

Fuente: Departamento de TIC del GADIPMC.

3.3.4.2 *Rack 3.*

Ubicado en el departamento de Gestión de Desarrollo Territorial, interconectado al Rack 2 a través de cable UTP, este es un gabinete de pared, en el que se encuentran alojados los elementos que se detallan a continuación.

Figura 19. Rack 3.

Fuente: Fotografía tomada por Cyntia Inuca.

Tabla 14. *Elementos del Rack 3.*

CANT.	ELEMENTOS	CARACTERISTICAS	FUNCIÓN
1	Switch HP v1910	Administrable 24 puertos Capa 3	Permite la conexión de los usuarios a la red en la sección 2 de la planta baja del edificio principal.
1	Patch panel	Panduit Cat 6	Distribuye el cableado estructurado.
1	Regleta de energía	-	Proveer energía al switch

Fuente: Departamento de TIC del GADIPMC.

3.3.4.3 *Rack 4.*

Este es un gabinete de pared, ubicado en el departamento de Avalúos y Catastros, interconectado al Rack 1 del Data Center a través de cable UTP.

Figura 20. Rack 4.

Fuente: Fotografía tomada por Cyntia Inuca.

Tabla 15. *Elementos del Rack 4.*

CANT.	ELEMENTOS	CARACTERISTICAS	FUNCIÓN
1	Switch HP v1910	Administrable 24 puertos Capa 3	Permite la conexión de los usuarios a la red en la sección 1 la planta baja del edificio principal.
1	Switch TP-LINK TSFL 1024D	No administrable 24 Puertos Capa 2	Permite la conexión de los usuarios a la red en la sección 1 la planta baja del edificio principal.
2	Patch panel	Panduit Cat 6	Distribuye el cableado estructurado.
1	Regleta de energía	-	Distribuye energía a los switch ubicados en el rack 4.

Fuente: Departamento de TIC del GADIPMC.

3.3.4.4 *Rack 5.*

Ubicado en el Info-Centro, parte de la dirección de TIC, tiene una conexión través de fibra óptica desde el Data Center, este rack es de piso y aloja los siguientes componentes:

Figura 21. Rack 5.

Fuente: Fotografía tomada por Cyntia Inuca.

Tabla 16. *Elementos del Rack 5.*

CANT.	ELEMENTOS	CARACTERISTICAS	FUNCIÓN
1	Convertidor de fibra óptica	Fiber media converter DMC-300SC	Convertir señales ópticas de la fibra óptica a señales eléctricas para el cable UTP CAT 5e.
3	Switch DLINK DES 1024 R+	24 puertos No administrable Capa 2	Permite la conexión de los usuarios a la red en el edificio Espinoza Jarrín.
2	Patch panel	Panduit Cat 5e	Distribuye el cableado estructurado.
1	Regleta de energía		Distribuir energía a los equipos de comunicación en el Rack 5.
1	UPS	Marca CDP Output: 125 Vac/8A Input: 120 Vac	Provee energía durante un tiempo corto en caso de cortes de energía.

Fuente: Departamento de TIC del GADIPMC.

3.3.4.5 *Rack 6.*

Este es un rack de piso cerrado, de la Empresa Pública Municipal de Agua Potable y Alcantarillado del cantón Cayambe, EMAPAAC, el municipio de Cayambe brinda conectividad a internet a esta empresa a través de su red interna.

Los elementos que se encuentran en este rack son:

Tabla 17. *Elementos de Rack 6 EMAPAAC.*

CANT.	ELEMENTOS	CARACTERISTICAS	FUNCIÓN
1	Router inalámbrico D-LINK DES-600R	8 puertos Administrable	Proveer acceso a internet a los usuarios de EMAPAAC.
1	Switch D-link DES 1008A	8 PUERTOS Capa 2 No administrable	Permite conexión a la red entre el municipio y EMAPAAC.
1	Switch TP-LINK TL-SG 1024	24 puertos No administrable Capa 2	Permite la conexión de los usuarios que pertenecen a EMAPAAC a la red.
1	Patch Panel	Panduit Cat 5e	Distribuye el cableado estructurado.
1	Regleta de energía		Distribuir energía a los equipos de comunicación en el Rack 5.

Fuente: Departamento de TIC del GADIPMC.

3.3.5 Sistema Cableado Estructurado.

Para el buen funcionamiento de cualquier red de datos es importante que su infraestructura física se encuentre en buenas condiciones, el sistema de cableado estructurado debe contar con las normas respectivas.

3.3.5.1 *Edificio principal.*

El edificio principal cuenta con un sistema de cableado estructurado, donde el medio de trasmisión usado es cable de par trenzado UTP Cat 6A, cuenta con la certificación de 140 puntos de red (datos) y su respectiva etiqueta. (Diego Borja, 2012)

Figura 22. Punto de red certificado.
Fuente: Departamento de TIC del GADIPMC.

3.3.5.2 *Edificio Espinoza Jarrín.*

El medio de trasmisión usado en este edificio es cable de par trenzado Cat 5e, este edificio no cuenta con un buen diseño de sistema de cableado estructurado, que cumpla las correspondientes.

3.3.6 Equipos terminales de usuario.

Computadores de escritorio, portátiles, switch no administrables y routers inalámbricos, son usados por los usuarios de la LAN del GADIPMC. A continuación se detalla algunas características sobre los computadores de escritorio y portátiles que se usan en municipio.

3.3.6.1 *Computadores de escritorio.*

Tabla 18. *Detalle computadores personales.*

Marcas	ALTEK/ DELL/ DIKT/ URRICANE/ XTECH
Memoria RAM (GB)	2, 4, 8
Disco	200 GB/ 300 GB/ 500 GB / 1 TB
Procesador	AMD /INTEL CORE 2DUO, i3, i5, i7 / INTEL PENTIUM
Sistema operativo	WINDOWS 7
Software	Microsoft Office 2007/ Adobe Reader/ Mozilla /Thunderbird

Fuente: Departamento de TIC del GADIPMC.

3.3.6.2 *Computadores portátiles.*

Tabla 19. *Detalle de computadores portátiles.*

Marca	HP, Lenovo
Memoria RAM (GB)	4, 6,8
Disco	500 GB / 1 TB
Procesador	AMD /INTEL CORE i5/ INTEL CORE i7
Sistema operativo	Windows 7, Windows 8.
Software	Microsoft Office 2007, 2010 / Adobe Reader/ Mozilla /Thunderbird

Fuente: Departamento de TIC del GADIPMC.

3.4 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.

3.4.1 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.

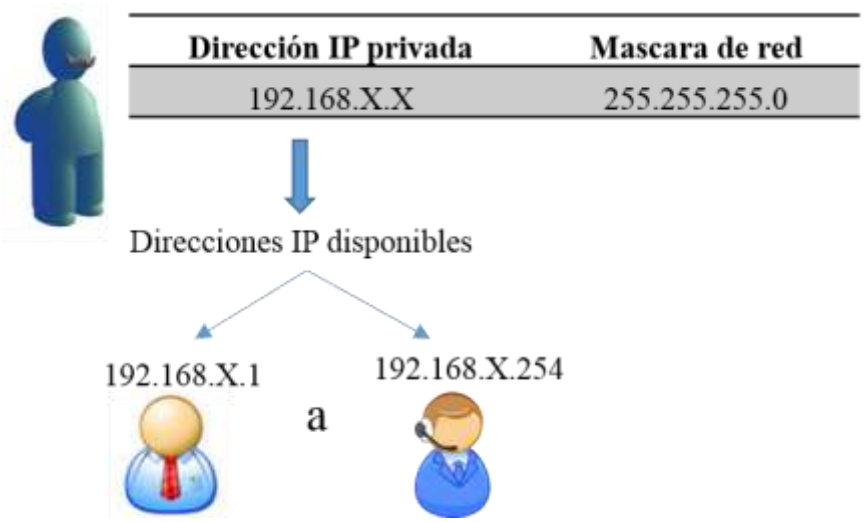


Figura 23. Direccionamiento IP.

Fuente: Obtenido de http://www.marbit.es/index_ip.html.

3.4.2 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.

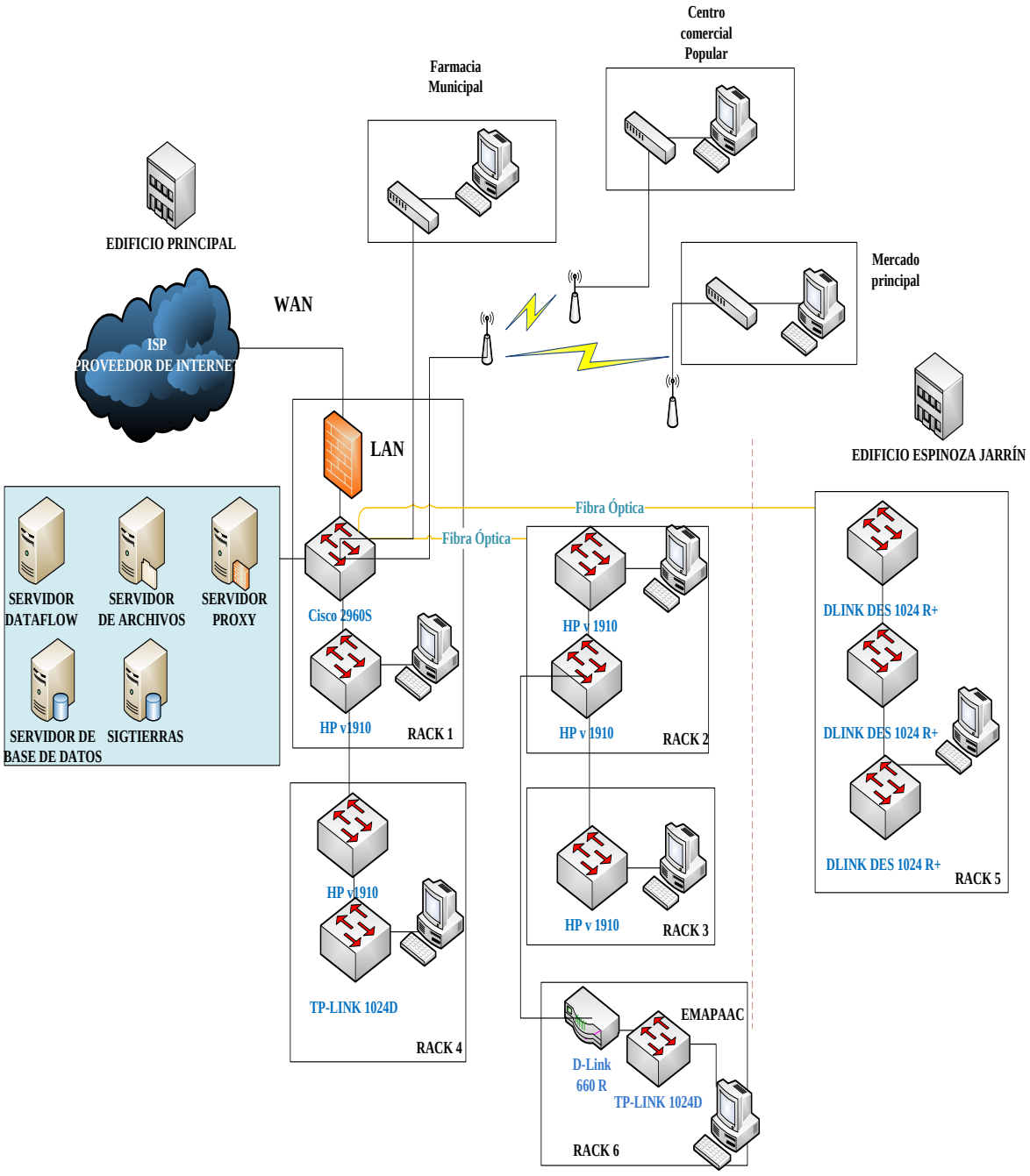


Figura 24. Topología Lógica de la LAN del GADIPMC.

Fuente: Departamento de TIC del GADIPMC.

3.4.3 Monitoreo de red

Para extraer información sobre el estado actual de la red se realiza la instalación de un software, que permita el monitoreo de la red, mismo que es elegido de acuerdo al estándar IEEE 29148, el cual es un estándar de requerimientos de ingeniería de software y sistemas, este proceso de selección se adjunta en el Anexo A, optando por Zenoss como herramienta de gestión para el monitoreo de la red actual. Véase el proceso de instalación en el Manual de Zenoss, Anexo D.

3.4.3.1 *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 ha realizado 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.

3.4.3.2 *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.

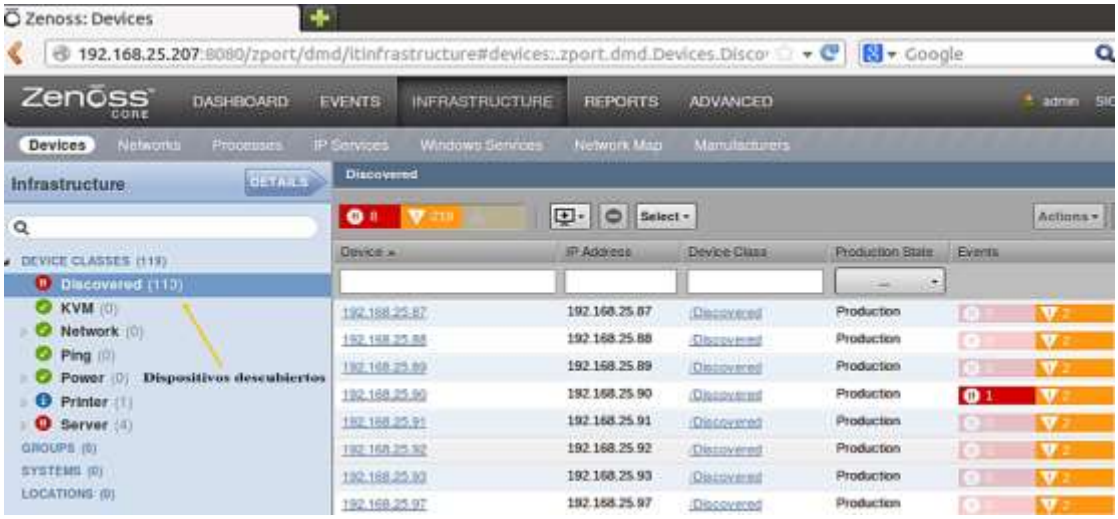


Figura 25. Autodescubrimiento de la LAN.

Fuente: Servidor Zenoss.

3.4.3.3 *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.

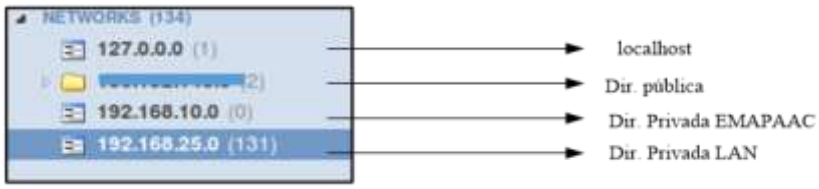


Figura 26. Redes descubiertas.

Fuente: Servidor Zenoss.

3.4.3.4 *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.

Figura 27. Estado del protocolo SNMP.

Fuente: Servidor Zenoss.

3.4.3.5 *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.

Figura 28. Topología LAN.

Fuente: Servidor Zenoss.

3.4.3.6 *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, como se ve en la Figura 29.

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.

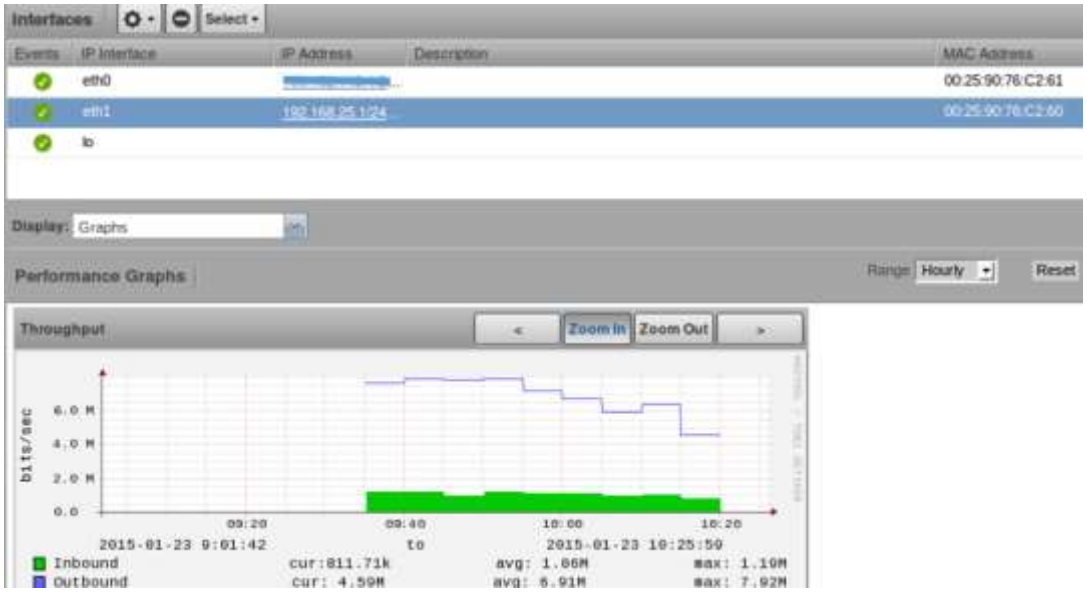


Figura 29. Estado de interfaces firewall.

Fuente: Servidor Zenoss.

3.5 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, ya que día a día los usuarios están haciendo uso de la red, y ellos son quienes califican el rendimiento de la red, y la calidad de los servicios ofrecidos por el departamento de las TIC, por eso 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, ya que 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.

3.5.1 Formato de las encuesta

Encuesta a los usuarios de la red interna (LAN) del GADIP Municipio de CAYAMBE			
Fecha:		**Direccion:**	
Objetivo: Conocer el nivel de satisfacción de los usuarios sobre la red interna (LAN) del GADIPMC.			
*Marque con una **X** las casillas que Ud. considere, evaluando el trabajo del departamento de TIC.*			
Gestión de fallos	**Atención a problemas**	**Detección del problemas**	**Resolución del problema**
	Siempre ☐	Rápido ☐	10 min ☐
	Casi siempre ☐	Se demora mucho ☐	30 min ☐
	A veces ☐	No lo identifican ☐	1 h ☐
	Rara vez ☐		Más de una hora ☐
	Nunca ☐		1 día ☐
			Más de un día ☐
Gestión de rendimiento	**Velocidad de internet**	**Servicios de red (e-mail,SIM,Olympo,Dataflow,Svr.Archivos)**	
	Muy rápida ☐	No funcionan ☐	
	Rápida ☐	Con problemas ☐	
	Normal ☐	No tengo inconvenientes ☐	
	Lenta ☐	Excelente ☐	
	Muy lenta ☐		
De acuerdo a los ítems anteriores ¿qué tan satisfecho esta Ud. con la labor que desempeña el departamento de TIC?		Muy satisfecho ☐	
		Satisfecho ☐	
		Poco satisfecho ☐	
		No satisfecho ☐	

3.5.2 Resultados y análisis.

A continuación se realizan las estadísticas correspondientes para analizar las respuestas de los usuarios.

3.5.2.1 *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. Analizando junto al administrador este inconveniente se da por falta de personal, ya que actualmente existe un solo técnico encargado de esta función.

Figura 30. Atención a problemas.

Fuente: Encuestas aplicadas a usuarios del GADIPMC.

3.5.2.2 *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 del problema, 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.

Figura 31. Detección de problemas

Fuente: Encuestas aplicadas a usuarios del GADIPMC.

Se debe dar pronta solución a problemas de los usuarios en el menor tiempo posible, por lo que sería bueno establecer procedimientos que ayuden a minimizar el tiempo de resolución de problemas, ayudando a identificar las posibles causas de los problemas en la red, dando solución a ellos de la manera más eficiente.

Figura 32. Resolución de problemas

Fuente: Encuestas aplicadas a usuarios del GADIPMC.

3.5.2.3 *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.

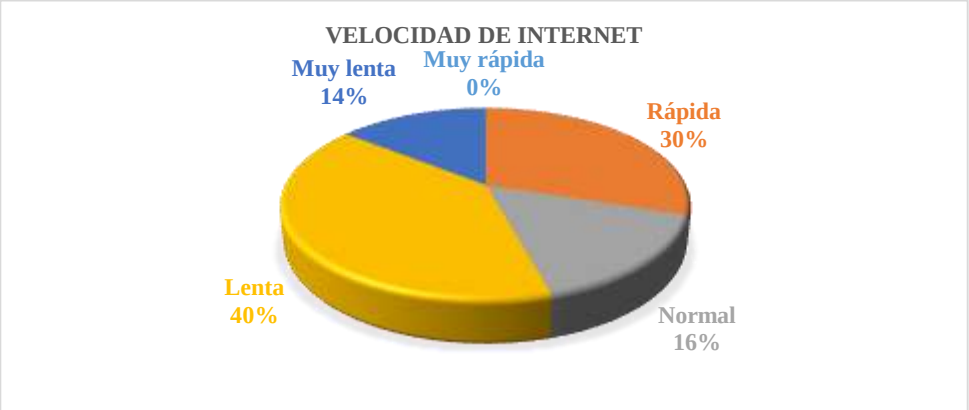


Figura 33. Velocidad de internet.

Fuente: Encuestas aplicadas a usuarios del GADIPMC.

Se deben tomar medidas que permitan preservar el ancho de banda de la red evitando el mal uso de la misma.

3.5.2.4 *Servicios de red*

Es importante que los servicios que se den a través de la red local, estén siempre disponibles, y no presente eventos que puedan afectar al trabajo de los usuarios, existe un 78% que manifiesta que no tienen ningún inconveniente, demostrando que están funcionando bien.

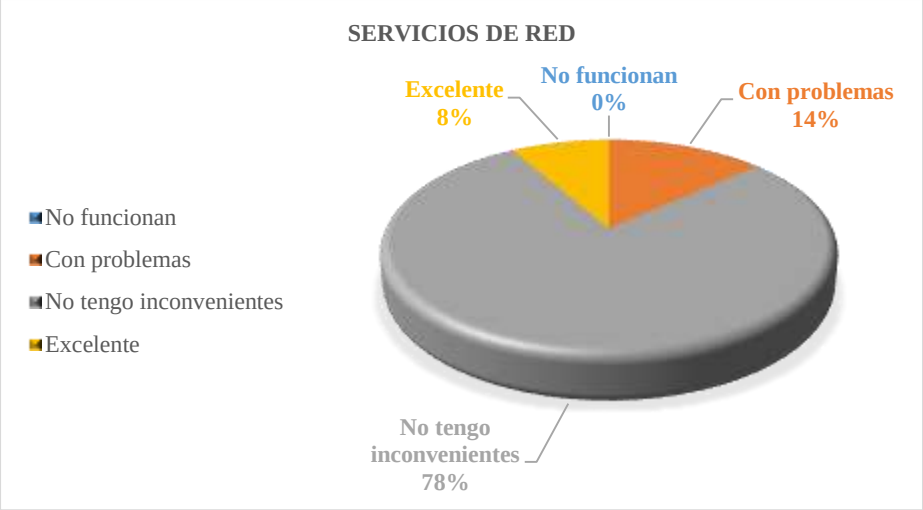


Figura 34. Servicios de red.

Fuente: Encuestas aplicadas a usuarios del GADIPMC.

3.5.2.5 *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.

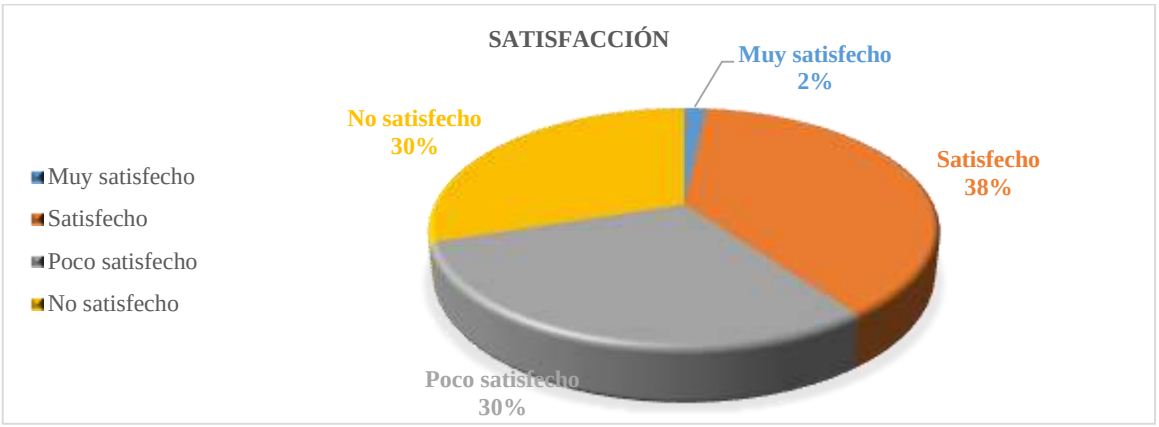


Figura 35. Satisfacción de los usuarios de la red.

Fuente: Encuestas aplicadas a usuarios del GADIPMC.

3.6 Necesidades y requerimientos de la LAN

Mediante la recopilación de información de la situación actual se han reconocido las necesidades y requerimientos de la LAN, las cuales se presentan en la siguiente tabla.

Tabla 20.*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, de todas las instalaciones 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, de manera que el administrador tenga el control total sobre sus configuraciones.	Servidor Zentyal.
	Proxy transparente	Restricción de páginas web https, (redes sociales, YouTube).	
La red se torna lenta, y en el monitoreo se puede ver que 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 que hacen los usuarios.	
Demasiado tiempo de resolución de problemas de los usuarios de la red.	Atender los requerimientos de los usuarios de la red, 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, que recopile información sobre el funcionamiento y uso de recursos de red.	
	Llevar documentación del funcionamiento 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.

CAPITULO IV

4 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.

4.1 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.

Figura 36. Centro de administración y monitoreo de red.

Fuente: Obtenido de: http://iteigo.net/archives/2109

4.1.1 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.

4.1.2 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.

Figura 37. Funciones del centro de administración y monitoreo de red.

Fuente: Adaptado por Cyntia Inuca.

4.1.2.1 *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.

4.1.2.2 *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.

4.1.2.3 *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.

4.1.2.4 *Documentación de red.*

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

4.1.2.5 *Brindar Seguridad*

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

4.2 Políticas de gestión de red

Las políticas de gestión son una guía que permitirá mejorar la administración y gestión de red de forma ordenada, que satisfagan las necesidades y requerimientos de la red, dichas políticas se establecen de acuerdo al Modelo Funcional de Gestión de Red ISO/OSI (FCAPS), que a través del Centro de Administración y Monitoreo de red, podrá cumplir las funciones de:

- Planificación de red.
- Monitoreo de red.
- Soporte técnico.
- Documentación de red, y;
- Brindar seguridad.

Para cada política se establecen procedimientos a seguir, a través de esto el administrador y personal encargado de la red local, podrá desempeñar mejor sus funciones.

4.2.1 Establecimiento de políticas para gestión de red local.

Gobierno Autónomo Descentralizado Intercultural y Plurinacional de Municipio De Cayambe		
	POLÍTICAS DE GESTIÓN DE RED	
Versión: 1.0	**Revisado por:** Tnlg. Rony Carvajal *Jefe de Infraestructura y Conectividad*	**Aprobado por:** Ing. Fabián Bautista *Director de TIC*

I. INTRODUCCIÓN

La base para que cualquier institución pueda trabajar a través de su red de datos, comienza con la definición de políticas y procedimientos adecuados, en el que actúan el administrador de red y los usuarios 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 realizar siguiendo un objetivo en común, la conformación de un manual sirve como un elemento de apoyo administrativo.

En este documento 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 lograra administrar la red por partes y mejorar el servicio brindado a la municipalidad, garantizando la disponibilidad de la red.

II. PROPÓSITO

Establecer directrices a través de políticas y procedimientos para gestionar la red local, y presentarlas a la dirección de TIC, para que sea de su conocimiento, uso y cumplimiento, de manera que puedan administrar la red de forma organizada, mantener y mejorar la disponibilidad de la red.

III. CONCEPTOS PRELIMINARES

- **Administración y gestión de red de área local**

  La administración y gestión de red local integra, el uso de herramientas gestión que permitan monitorear la red y obtener datos de la red, el uso de métodos que permitan el control de actividades entorno al funcionamiento de la red, para mediante estos garantizar la operatividad de la red y mejorar su disponibilidad.

- **Monitoreo de red**

  Es la supervisión, observación y análisis del estado de los recursos de 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.

- **Control de red**

  El control de la red implica la vigilancia cotidiana de la red, incluye procedimientos que permitan mantener la disponibilidad de red.

- **Políticas de gestión**

  Las políticas son guías que el permiten al administrador de red ejercer alguna acción ante un evento en la red, las políticas siempre irán acompañadas de una serie de procedimientos para cumplirlas, siempre teniendo un objetivo en común

IV. GENERALIDADES

a) Este documento maneja un lenguaje técnico, dirigido para la dirección de TIC quienes cumplen con conocimientos técnicos de redes.

b) Las políticas establecidas en este documento son recomendaciones para la buena administración de la red y no pretenden ser reglas absolutas y de uso obligatorio.

c) Para cumplir las políticas establecidas en este documento, interactuarán administrador de red, encargados de la red local, y los usuarios de la red.

V. NIVELES ORGANIZACIONALES

a) Director de TIC

Autoridad de nivel superior. Ente encargado de la aprobación de las políticas de gestión junto al Jefe de Infraestructura y Conectividad.

b) Jefe de Infaestructura y Conectividad

Autoridad a cargo de funcionamiento de la infraestructura tecnologica de red, a el se le atribuye las funciones de administrador de red, toma control sobre la manipulacion y configuraion de equipos que conforman la red local, toma decisiones entorno a su labor en caso de no estar la autoridad superior.

c) Soporte Tecnico

Encargado de brindar servicios de soporte tecnico referente a hardware y software a los usuarios, que pertenecen a la red local. Toma decisiones cuando no estan ninguna de las autoridades.

d) Usuarios

Son las personas que estan interconectadas a la red local para acceder a los servicos que brinda la direccion de TIC.

VI. VIGENCIA

Este documento no es de uso obligatorio, por lo cual entrará en vigencia cuando las autoridades competentes autoricen su uso, para ello deberán revisarlo, y de ser posible mejorarlo, para que cumpla los objetivos que persigue la dirección de TIC, referente a una buena administración y gestión de la red local.

VII. MARCO NORMATIVO

El presente documento se realizó en base Norma NTE INEN-ISO/IEC 27002:2009, que brinda soluciones de seguridad y están enfocadas a todo tipo de organizaciones, de cualquier tamaño y naturaleza.

De esta norma se acoge la estructura de documentos de políticas de seguridad y soluciones recomendadas, acoplándolas con el modelo funcional de gestión de red ISO/OSI.

VIII. ESTRUCTURA

Este documento se estructura políticas en base al modelo funcional de gestión de red ISO/OSI, para que funcione a través herramientas de software libre que permitan gestionar la red.

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 aplicacion 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.

IX. TÉRMINOS Y DEFINICIONES

Este documento hace uso de varios conceptos técnicos, los cuales se definen, para facilitar la comprensión y uso de este documento.

- **Red:** Es la interconexión de varios equipos de comunicación, a través de un medio de trasmisión, para intercambiar información, y acceder a varios servicios.
- **LAN:** Red de área local, son redes para un área geográfica pequeña con alcance a pocos km aproximadamente 100 km,, que puede alcanzar hasta 10Mbps de velocidad, y contener de 100 a 1000 usuarios, generalmente aplicadas en pequeñas empresas, compañía u organización.
- **Administración:** Significa organizar, dirigir, y controlar los recursos de una entidad.
- **Gestión:** Es la asignación de actividades de los recursos de red.
- **SNMP:** Es el protocolo de administración de red simple, trabaja en la capa aplicación, y sirve para el intercambio de información de gestión de red.
- **Sistema de gestión de red:** Un sistema de gestión de red, es un conjunto de elementos que permiten administrar la red, basado en el paradigma gestor-agente.
- **Sistema de seguridad:** es un conjunto de herramienta que permiten controlar el acceso de usuarios a la red, mejorar firewall, y proteger la red.
- **Gestor:** Es la estación principal donde se alojan aplicaciones de monitoreo el cual pide al agente información de los dispositivos gestionados.
- **Agente:** es un software que reside en el dispositivo gestionado y que se comunica con el gestor respondiendo a sus peticiones.
- **Monitoreo:** es la visualización de información de los recursos de red.
- **Recursos de red:** son aquellos elementos que están interconectados a la red como: switch, router, computadores y servidores, dentro de estos elementos se encuentran sus recursos como interfaces de red, disco duro, memoria, procesador, etc.
- **Servicios de red:** son aplicaciones que se ofrece a través de la red por medio de los servidores.

X. DESARROLLO DE POLÍTICAS

GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL
DEL MUNICIPIO DE CAYAMBE

1. Políticas de gestión de red local	**Código:**	POL-LAN-0001
1.1. Objetivos de políticas de gestión de red	**Art 1.** Establecer políticas y procedimientos de gestión de red, para administrar la red local cubriendo las necesidades y requerimientos de red, basándose en el modelo funcional de gestión de red ISO/OSI.	
1.2. Documento de políticas gestión de red	**Art 2.** La Dirección de TIC, elaborará un manual de políticas y procedimientos de gestión de red local, la cual debe será aprobada y publicada para conocimiento del administrador de red y los encargados de la red local, así como los usuarios finales.	
1.3. Revisión de políticas de gestión de red	**Art 3.** La dirección de TIC, deberá revisar el Manual de Políticas y procedimientos, en intervalos planificados para garantizar que es adecuada, eficaz, y suficiente. **Art 4.** Actualizar el manual, ante cambios significativos que se puedan dar en la institución.	

GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL
DEL MUNICIPIO DE CAYAMBE

2. Política para la gestión de configuración	**Código:**	POL-LAN-0002
2.1. Planificación de red	**Art 5.** Verificar constantemente el funcionamiento correcto de todos los recursos de red, y planificar proyecciones futuras para el avance tecnológico de la infraestructura de red de la institución. **Art 6.** Responder a las necesidades de los usuarios de la red, analizando sus requerimientos, y planificando la solución a estos. **Art 7.** Manejar información de red, y controlar cambios que se de en la infraestructura de red de manera que no afecte a su funcionamiento.	

2.2. Configuración de equipos	**Art 8.** Únicamente el administrador de red y sus autorizados podrán: a. Manipular los equipos de comunicación que este interconectados en la red local. b. Configurar, borra o modificar información del equipo. c. Integrar un equipo nuevo a la red local. **Art 9.** Todos los equipos que quieran ingresar a la red local deberán cumplir con la configuración básica que les permita beneficiarse de los servicios que provee la dirección de TIC a través de la red de la institución. **Art 10.** Los equipos y dispositivos de red que estén conectados a la red local, deberán tener habilitado el protocolo SNMPv2 (siempre y cuando lo soporten), e incluir un nombre de la comunidad SNMP para poder ser gestionados.
2.3. Ingreso de equipos	**Art 11.** La dirección de TIC, deberá tener su propio inventario de equipos activos en la red, al ingresar un nuevo equipo a la red se registrará las características más importantes, de forma que tenga un control sobre todos los elementos que conforman la red. **Art 12.** Los equipos que están conectados a la red local y soporten el protocolo SNMP, deben ser ingresados en la aplicación de gestión para monitorear sus recursos y conocer el estado actual de su funcionamiento.
2.4. Documentación de configuración	**Art 13.** El administrador de red, debe llevar la documentación correspondiente a configuraciones realizadas para que el sistema de gestión de red funcione. **Art 14.** Se mantendrán respaldos de las configuraciones realizadas en los equipos y servidores, para casos de eventos inesperados como perdida de información o des configuración del servidor. **Art 15.** Antes de realizar cambios en la configuraciones de equipos y servidores se respaldar la última configuración correcta del equipo.

GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL
DEL MUNICIPIO DE CAYAMBE

3. Políticas para la gestión de fallos	**CÓDIGO:**	POL-LAN-0003
3.1. Manejo de fallos	**Art 16.** El momento en que surja una falla en el entorno de la red local, el administrador es responsable de responder a dicho evento, pues él debe detectar, aislar, y resolver el fallo, ayudado de la aplicación de gestión y esfuerzo humano. Para conseguir una respuesta efectiva rápida y ordenada debe cumplir con el manual de procedimientos para la gestión de fallos. **Art 17.** Se debe tratar de dar solución al fallo en el menor tiempo posible, para evitar inconvenientes en el trabajo de los usuarios de la red.	
3.2. Notificación de fallos	**Art 18.** Comunicar los fallos ocurridos en la red lo más pronto posible, manejando canales apropiados que permitan actuar al administrador de red para que tome medidas correctivas oportunas.	
3.3. Documentación de fallos	**Art 19.** Se deberá documentar los fallos producidos y los procedimientos que se realizaron para solucionarlo, teniendo así un proceso a seguir en caso de que la falla se persista.	

GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL
DEL MUNICIPIO DE CAYAMBE

4. Políticas para la gestión de rendimiento	**CÓDIGO:**	POL-LAN-0004
4.1. Planificación y aceptación del sistema	**Art 20.** Planificar y garantizar la adecuada capacidad de un recurso para minimizar riesgos de fallos en los equipos que están interconectados a la red local y mantenerlos disponibles.	
4.2. Establecimiento umbrales	**Art 21.** Se garantizará que los equipos de red trabajen correctamente estableciendo umbrales de aceptación, para prevenir problemas en su funcionamiento.	

5. Políticas para la gestión de contabilidad	**CÓDIGO:**	POL-LAN-0005
5.1. Manejo de reportes	**Art 22.** El administrador de red podrá obtener reportes del uso de recursos de red monitoreados mediante una aplicación de gestión, de forma diaria, mensual y anual, en el momento que él lo requiera.	
5.2 Inventario de activos	**Art 23.** Se debe llevar un inventario de todos los activos de red, estos deben estar claramente identificados, en él se deben registrar los datos más importantes. **Art 24.** La dirección de TIC actualizará el inventario en un intervalo de tiempo de 6 meses.	

6. Políticas para la gestión de seguridad	**CÓDIGO:**	POL-LAN-0006
6.1. Control de acceso a equipos	**Art 25.** Restringir el acceso lógico a equipos de comunicación de la red local y su información de configuración únicamente a usuarios autorizados de la Dirección de TIC.	
6.2. Control de acceso a la aplicación de gestión de red.	**Art 26.** Se deberá restringir el acceso a la (s) aplicación (es) de gestión de red, únicamente el usuario administrador de red podrá acceder su configuración e información. **Art 27.** Deberá permitir el manejo de varios usuarios y permitir asignación de roles de usuarios.	
6.3. Control de acceso a servidor de seguridad	**Art 28.** Se deberá restringir el acceso al servidor de seguridad, únicamente el usuario administrador de red podrá acceder su configuración e información.	
6.4. Control de acceso a Internet	**Art 29.** El administrador de red deberá precautelar el ancho de banda por lo que el internet no debe ser mal utilizado, en actividades que demanden gran cantidad de consumo de red, como; descarga de videos, música, redes sociales, etc.	

6.5. Control de usuarios	**Art 30.** El administrador de red, definirá un procedimiento formal de registro de usuarios para otorgar acceso a los diferentes sistemas y servicios de la red. **Art 31.** Controlar la asignación de permisos privilegiados a los usuarios en caso de ser oportuno. **Art 32.** El administrador de la red podrá dar de alta o baja a un usuario. **Art 33.** El usuario será el único responsable del uso de su usuario y contraseña, asignada por el administrador.
6.6. Protección contra intrusos	**Art 34.** Mantener la integridad y disponibilidad de la red con herramientas que permita funciones de IDS/IPS que bloquee y registre cualquier actividad sospechosa y maliciosa que se detecte en la red.
6.7. Manejo de Backups	**Art 35.** Mantener respaldos de los servidores y guardarlo en un dispositivo de almacenamiento o servidor de archivos, para casos contraproducentes.

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

La administración y gestión la red local del Municipio de Cayambe, 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 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.

A través de la gestión de configuración y seguridad el administrador podrá controlar la red, mientras que las áreas de gestión de fallos, gestión de rendimiento y contabilidad, le permitirán monitorear la red, como se ve en la Figura 38.

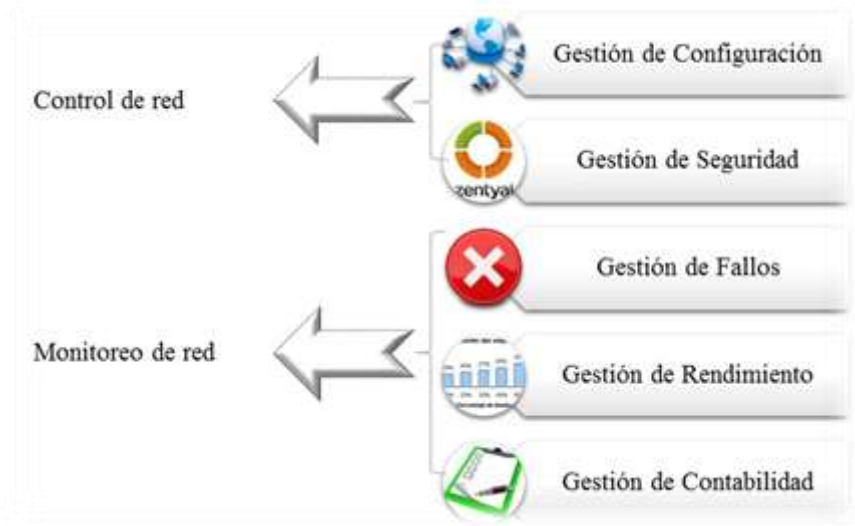


Figura 38. Áreas funcionales de gestión de red OSI.

Fuente: Adaptado por Cyntia Inuca.

4.3.1 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.

4.3.1.1 *Configuración del sistema de gestión de red.*

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

4.3.1.1.1 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.

En la actualidad existen una variedad de herramientas de gestión que permiten el monitoreo de la red obteniendo información de su funcionamiento, se puede optar por software privado así como libre, para elegir la mejor opción que se adapte a las necesidades de la LAN del GADIPMC, se aplica el estándar de requerimientos de Ingeniería de Software y Sistemas, IEEE 29148, mediante el cual se establecen los requisitos necesarios que debe cumplir el software, cubriendo las áreas del modelo funcional de gestión de red.

- **Estándar de Requerimientos de Ingeniería de Software y Ciclo de Vida de un Sistema IEEE 29148**

  Este estándar permite establecer acuerdos entre el proveedor y el comprador de un producto de software, de tal manera que el proveedor cumpla las necesidades requeridas por el comprador.

  Los aspectos que se deben tomar en cuenta para el establecimiento de acuerdos, son:

  - ✓ Funcionalidades del sistema.
  - ✓ Definición de restricciones necesarias.
  - ✓ Ciclo de vida del software.
  - ✓ Calidad del producto.
  - ✓ Identificación de vulnerabilidades

  El proveedor debe tomar en cuenta si los requerimientos son necesarios, en base a la realidad de la entidad, garantizar el correcto funcionamiento del software, seguridad, interacción entre el usuario y el sistema o software, definiendo el uso que se dará al mismo.

- **Requisitos de software de monitoreo.**

El software debe cumplir parámetros como:

- ✓ Ser de software libre, no comercial.
- ✓ Tener facilidad de manejo, para el administrador.
- ✓ No consumir muchos recursos de hardware.

Debe cumplir con las siguientes funcionalidades:

- Tener soporte SNMP v2.
- Permitir autodescubrimiento de la topología de red.
- Permitir obtener datos sobre características de dispositivos gestionados como, dirección IP, dirección MAC, Sistema Operativo, etc.
- Permitir el monitoreo de uso de: CPU, Memoria, Disco Duro, Interfaces de red, de los dispositivos gestionados.
- Manejo de una base de datos.
- Visualización de graficas de rendimiento.
- Obtención de reportes y datos estadísticos de los dispositivos gestionados.
- Permitir la configuración de alarmas y notificación de eventos, por correo electrónico.
- Seguridad.

- **Elección de software de monitoreo.**

En el Anexo A, se establece, como mejor alternativa el software Zenoss Core en su versión libre, que cumple los requisitos antes establecidos. A través del cual se puede realizar el monitoreo de la red.

Tabla 21. *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
	Graficas de rendimiento	✓	✓	✓	✓	✓
	Reportes	✓	✓	✓	✓	✓
	Base de datos	Oracle MySQL, PostgresSQ.	Programado en C MySQL PostgresSQL.	MySQL PostgreSQL.	MySQL	PostgreSQL
	Manejo de alarmas y notificación de eventos por correo electrónico	✓	✓	✓	✓	✓
Seguridad		✓	✓	✓	✓	✓

Fuente: Véase Anexo A.

- **Zenoss**

Zenoss en un software que permite monitoreo de una infraestructura de red, que incluye, redes, servidores, sistemas de aire acondicionado, y diferentes aplicaciones.

Integra programación que abarca varios proyectos de código abierto, usa:

- ✓ **Python:** como lenguaje de programación.
- ✓ **Zope:** es el conjunto de aplicaciones de servidor.
- ✓ **Net-SNMP:** protocolo de monitoreo de red para le recolección de información.
- ✓ **RRDtool:** reproduce gráficas y guarda registros temporales.
- ✓ **MySQL:** usada como base de datos.
- ✓ **Twisted:** es un controlador de eventos, basado en librerías de Python.

Entre las Funcionalidades de Zenoss, están:

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

Zenoss unifica todas estas funcionalidades, en un sistema simple y moderno, interactuando con el administrador de red mediante una interfaz web.

- ***Arquitectura y tecnologías.***

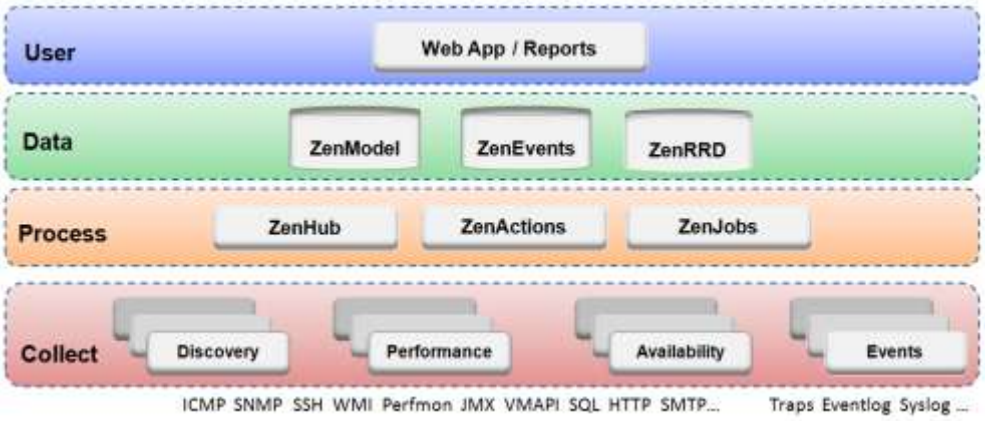


Figura 39. Capas de arquitectura de Zenoss.

Fuente:
http://www.zenoss.com/sites/default/files/documentation/Zenoss_Core_Administration_02-022014-4.2-v08.pdf

Zenoss se basa en un sistema de cuatro partes:

- ✓ **Capa usuario:** se muestra como interfaz web, a través de la cual puede: ver el estado de los equipos que conforma la red de una empresa, integrar dispositivos de red y sistemas, monitorear y responder a eventos, administrar usuarios, crear y ejecutar informes.
  - Esta capa interactúa con la capa de datos del mismo que traduce la información y se muestra al usuario.

- ✓ **Capa de datos:** almacena información de configuración e información recolectada.

  Se basa en tres bases de datos: ZenRRD, ZenModel, ZenEvents.

- **ZenRRD:** utiliza RRDtool, almacena los datos de rendimiento.
- **ZenModel:** sirve como el modelo de configuración básica, comprende dispositivos y sus componentes, grupos y localidades. ZODB, mantiene estos datos en una base de datos MySQL.
- **ZenEvents:** almacena los eventos en la base de datos de MySQL.

✓ **Capa de procesamiento:** Gestiona la comunicación entre la capa de recolección y datos. También ejecuta trabajos indicados por el usuario, con Zen Action y Zen Jobs.

✓ **Capa de recolección:** comprende servicios de recolección de datos, y alimentación a la capa de datos, estos servicios son proporcionados por numerosos demonios, que realizan funciones de modelado, seguimientos y gestión de eventos.

- El ***sistema de modelado***, utiliza SNMP, SSH, y WMI, para recopilar información de las maquina remotas. Así como plugins, que normalizan los datos en un solo formato.
- Los ***demonios de monitoreo***, hace un seguimiento de disponibilidad y rendimiento de la infraestructura tecnológica, usando múltiples protocolos. La información de rendimiento se aloja en los ficheros RRD, y la información de disponibilidad, tales como fallos de ping, infracciones de umbrales, son dirigidos al sistema de eventos ZenHub.

Enfoque de monitoreo: Zenoss utiliza un enfoque basado en modelos para el monitoreo. El monitoreo basado en modelos comienza con el descubrimiento, para continuar con una configuración definida, en el cual elige un formato de recolección de información, y empieza el monitoreo de forma automática, reduciendo gastos de mantenimiento del sistema, y asegura que los nuevos dispositivos y aplicaciones sean monitoreadas.

(Zenoss Community, 2005-2015)

- **Monitoreo con Zenoss**

Zenoss permitirá el monitoreo de la red local, para lo cual el administrador debe integrar los dispositivos a gestionar al software de gestión, en el que se descubre datos sobre uso de sus recursos, además de manejar las áreas de gestión de fallos, gestión de rendimiento y gestión de contabilidad.

- ✓ **Ingreso de equipos a gestionar de forma manual**

Para agregar un nuevo dispositivo a monitorear hay que tomar en cuenta el direccionamiento IP de dispositivo, asignarle una plantilla de acuerdo al tipo de dispositivo, la comunidad y el puerto por el que trasmite la información de gestión de red, como se ve en la Figura 40.

Figura 40. Parámetros de configuración un nuevo dispositivo.

Fuente: Aplicación Zenoss.

Al descubrir el dispositivo integrado se muestra información del dispositivo, permitiendo ver el nombre de equipo, localización, contacto, información de hardware, software, la comunidad SNMP y la versión usada.

Figura 41. Descubrimiento de dispositivos.

Fuente: Aplicación Zenoss.

Figura 42. Información Básica del dispositivo.

Fuente: Aplicación Zenoss.

Ya que Zenoss integra nmap descubre los puertos abiertos de cada equipo que este siendo monitoreado, así como también puede mostrar los programas instalados en los mismos.

Figura 43. Revisión puertos abiertos de un equipo gestionado.

Fuente: Servidor Zenoss.

Figura 44. Revision de programas instalados en el dispositivo gestionado.

Fuente: Servidor Zenoss.

- ✓ **Configuración de Zenoss para gestión de fallos.**

La gestión de fallas en Zenoss permite la configuración de alertas, y eventos, de manera que informa a través del software el estado de los dispositivos gestionados, la consola de eventos muestra las fallas de acuerdo al nivel de gravedad, y también se aplica la notificación por correo electrónico del evento ocurrido dirigido al administrador de la red.

- ➢ **Configuración de Alarmas.**

  Se establece una alarma para la recopilación de todos los eventos que produzcan cualquier error que sea crítico en el funcionamiento del equipo gestionado.

  La alarma creada se asigna al usuario administrador para que este pueda verificar los fallos generados, Zenoss permite crear alarmas y asignar a varios usuarios el manejo de ellas.

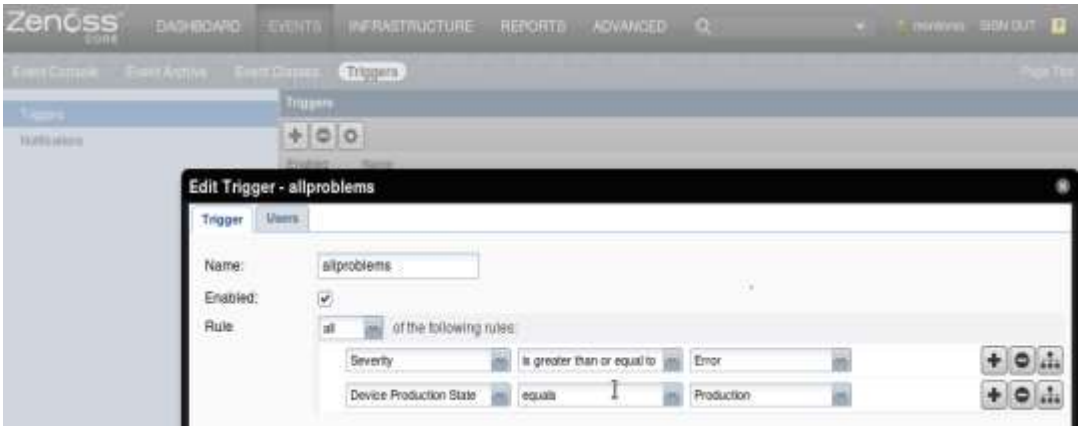


Figura 45. Configuración de alarmas.

Fuente: Aplicación Zenoss.

Figura 46. Configuración de usuario para el manejo de alarma.

Fuente: Aplicación Zenoss.

- **Configuración para notificación por correo electrónico.**

  Zenoss tiene integrado la funcionalidad de emitir notificaciones de fallos producidos en la red mediante correo electrónico de Gmail. Para recibir notificaciones por correo electrónico se requiere que el usuario administrador tenga configurado una cuenta de correo electrónico, verificar que tenga habilitado el puerto 25 del protocolo SMTP. A través de un test se puede verificar que la aplicación puede emitir una notificación de prueba.

  Al configurar la notificación se asigna el tipo de alarma que se emitirá, el contenido de la información del fallo producido, y el destinatario es decir el usuario administrador de red.

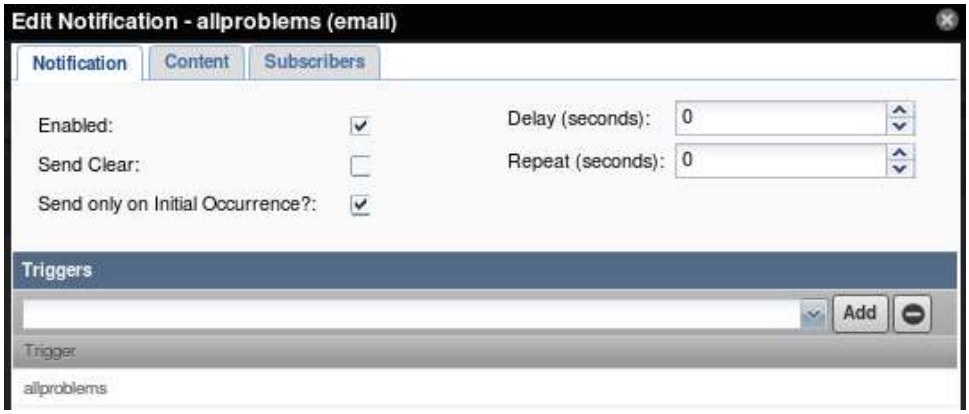


Figura 47. Configuración de notificaciones.

Fuente: Aplicación Zenoss.

Nota: Revise 4.3.3 Gestión de fallos para verificar el manejo de fallos, y el proceso de ciclo de vida de incidencia de un fallo.

- ✓ **Configuración de Zenoss para gestión de rendimiento.**

  Zenoss recoge datos a través del protocolo SNMP, a cada dispositivo se aplica una plantilla para la recopilación de la información, mediante un demonio ZenPerfSNMP, este puede monitorear el rendimiento de los recursos del dispositivo gestionado, depende mucho de la plantilla usada para que pueda ver datos de rendimiento.

  Establecimiento de umbrales.

  Antes de monitorear los recursos como uso de CPU, memoria, disco duro, hay verificar que la plantilla aplicada recopile esta información, para lo cual el administrador debe revisar la fuente de datos con la que trabaja la plantilla, en el que se registra las OID, para esto debe seguir el siguiente procesos.

  - Advance.
  - Monitoring templates.
  - Device.

- Elija la plantilla.
- Data Source.
- Revise la fuente de datos.
- Haga doble clic y revise la OID del recurso a monitorear.

En caso de que no se recopile la información debe averiguar la OID de los recursos que quiere monitorear e ingresarlos.

Figura 48. Configuración de recursos a monitorear.
Fuente: Aplicación Zenoss.

A través de un test dirigido al dispositivo a gestionar se puede verificar si este responde a la petición de información.

- Luego haga clic en Threshold, para establecer el umbral
- Ingrese el nivel de gravedad y el valor máximo del umbral.

Este permitirá que se genere un evento de fallo en caso de sobrepasar el umbral permitido.

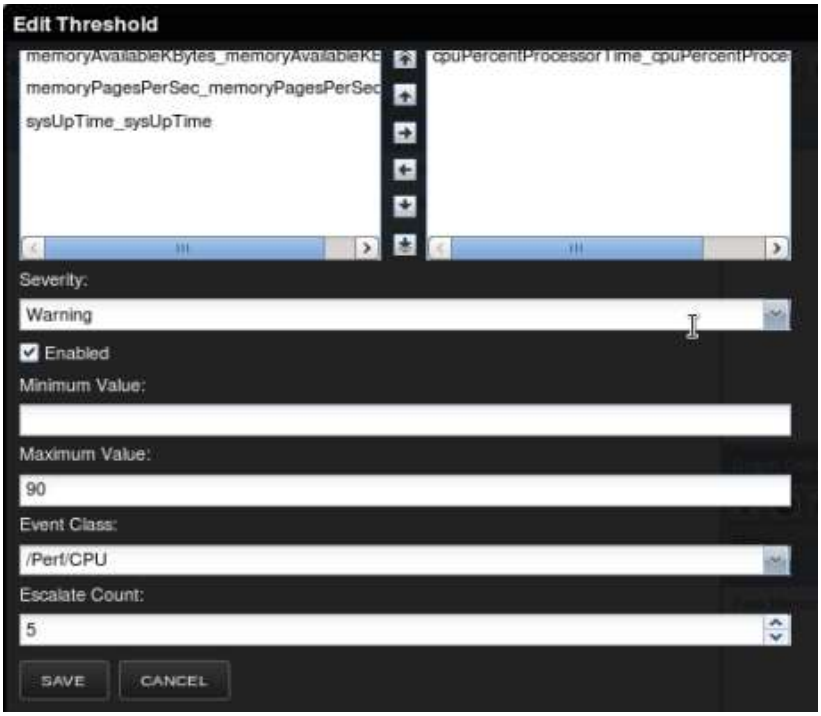


Figura 49. Establecimiento de umbral máximo.

Fuente: Aplicación Zenoss.

Para la revisión de datos de rendimiento el administrador puede definir la gráfica en Edit Graph, crearla definiendo un nombre que identifique al tipo de recurso monitoreado, y especificar la unidad en que se mide el rendimiento del recurso.

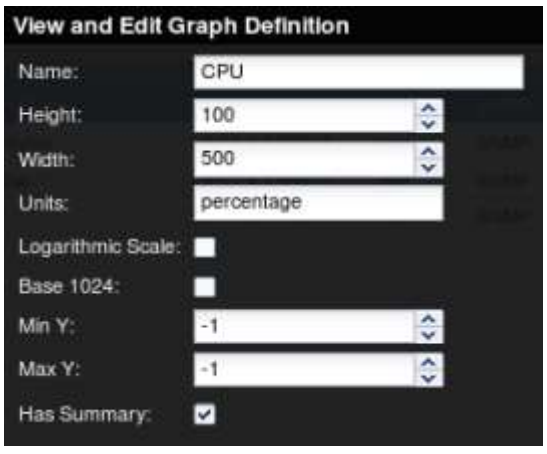


Figura 50. Definición de gráfica.

Fuente: Aplicación Zenoss.

Nota: Revise 4.3.4 Gestión de rendimiento. Donde verificará las gráficas de los recursos monitoreados.

4.3.1.1.2 Dispositivos gestionados.

El requerimiento para que el dispositivo de red sea gestionado es soportar el protocolo SNMP. Se gestiona servidores y equipos de computación de los usuarios, principalmente el área financiera, avalúos y catastros. El sistema operativo utilizado por los usuarios es Windows 7, y los servidores utilizan distribuciones de software libre, entre ellos Centos y Ubuntu.

4.3.1.1.3 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, para el intercambio de información de gestión, las dos partes deben pertenecer a la misma comunidad.
- **Permisos:** A través de permisos de solo lectura podremos monitorear la los recursos de red y observar la información de su funcionamiento.

- **SNMP en Windows.**

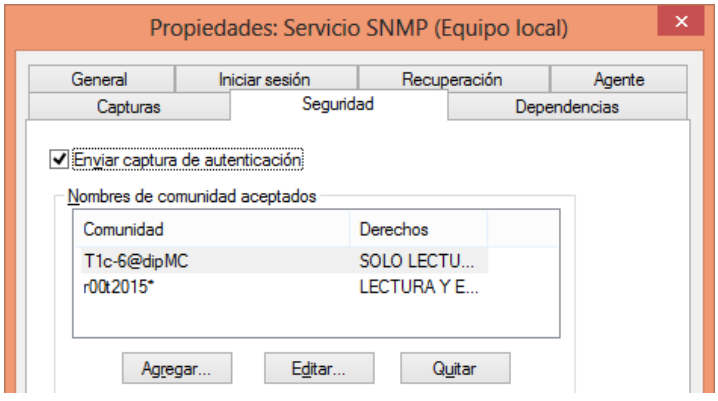


Figura 51. Habilitando protocolo SNMP.

Fuente: Sistema Operativo Windows 7.

- **SNMP en *Centos*.**

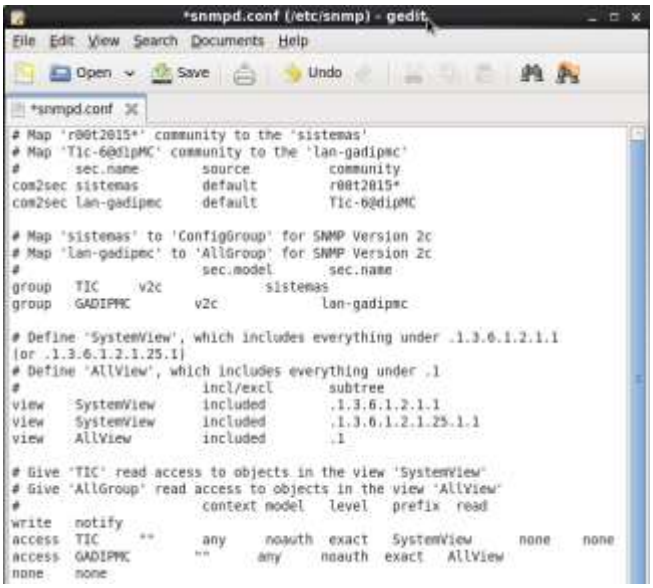


Figura 52. Configuración SNMP en Centos.

Fuente: Sistema Operativo Centos.

4.3.1.2 *Configuración del sistema de seguridad.*

Para brindar seguridad a la red local del Municipio de Cayambe se implementa una plataforma que integra varios servicios con 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.

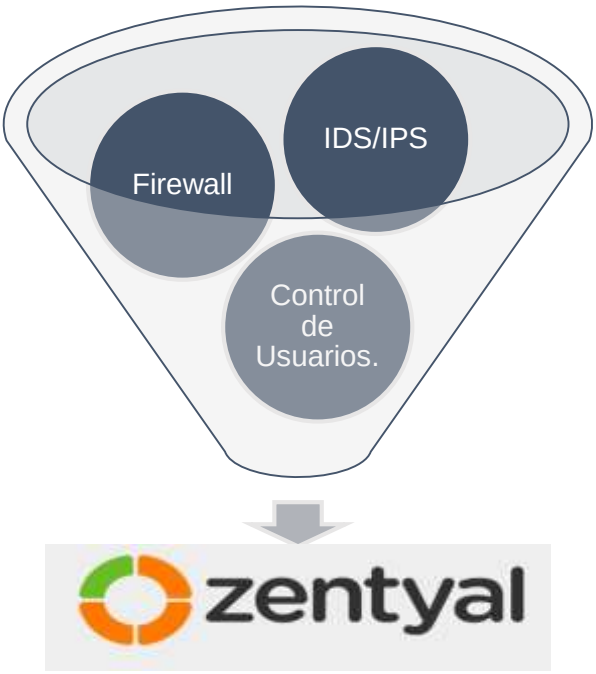


Figura 53. Zentyal plataforma multiservicios.
Fuente: https://wiki.zentyal.org/wiki/Es/3.2/Presentacion.

4.3.1.2.1 Zentyal 3.2.

Zentyal es una solución para la administración de redes de pequeñas y medianas empresas, a través de una plataforma única, actúa como: gateway, administrador de infraestructura, servicios de oficina, y comunicaciones. Este servidor está basado en una distribución de Linux, con el sistema operativo Ubuntu 12.04 LTS, existen varias versiones de este software, Zentyal 3.2 es una solución estable, que reúne las mejores características

que requiere un administrador de red, a través de una interfaz intuitiva, y amigable con el usuario administrador.

Zentyal permite instalar paquetes de software de acuerdo al rol de servidor que el administrador requiera, para este proyecto se utilizan varios módulos de Zentyal, como:

- ***Zentyal Infraestructure.***

  Gestiona la infraestructura de la red local, con servicios básicos como DHCP, DNS, NTP, etc.

  - ✓ **DHCP**, para la autoconfiguración de la red.
  - ✓ **DNS** para acceder a las máquinas y servicios usando nombres en lugar de direcciones IP.
  - ✓ **NTP** para sincronización del reloj.

- ***Zentyal Gateway (Cortafuegos).***

  Zentyal actúa como la puerta de enlace de la red local ofreciendo un acceso a Internet seguro y controlado, protege la red local contra ataques externos, intrusiones, amenazas a la seguridad interna y posibilita la interconexión segura entre redes locales a través de Internet u otra red externa.

  Integra las siguientes funciones:

  - ✓ **Proxy HTTP**, Zentyal utiliza squid, para la configuración del proxy http, junto a Dansguardian, para el control de contenidos.
  - ✓ **Cortafuegos**, utiliza para su módulo de cortafuegos el subsistema del kernel de Linux llamado Netfilter, que proporciona funcionalidades de filtrado, marcado de tráfico y redirección de conexiones.

- ✓ **IDS/IPS**, integra Snort, uno de los IDS más populares, compatible tanto con sistemas Windows como Linux y Suricata como la solución IPS.
- ✓ **Portal cautivo**, permite limitar acceso a la red desde la interfaz interna de la red, además permite también controlar el ancho de banda consumido por el usuario.

- ***Zentyal Office (Usuarios y Equipos).***

  A través de este módulo tiene la capacidad de gestionar los usuarios de la red de una forma centralizada, compartir ficheros e impresoras, tener aplicaciones web y por ultimo un sistema copias de seguridad backups.

  - ✓ **Usuarios y Equipos**, Integra Samba como servicio de directorio, con funcionalidad de controlador de dominio como Windows, el dominio se basa en una serie de servicios como Open LDAP, y DNS.

- **Requerimientos de hardware para la instalación de Zentyal.**

Tabla 22. *Requerimientos de hardware para Zentyal.*

Perfil de Zentyal	Usuarios	CPU	Memoria	Disco	Tarjetas de red
Puerta de acceso	<50	P4 o superior	2 GB	80 GB	2 o mas
	50 o mas	Xeon Dual core o superior	4GB	160 GB	2 o mas
Infraestructura	<50	P4 o superior	1 GB	80 GB	1
	50 o mas	P4 o superior	2 GB	160 GB	1
Oficina	<50	P4 o superior	1 GB	250 GB	1
	50 o mas	Xeon Dual core o superior	2 GB	500 GB	1

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

(Zentyal Community, s.f.)

- **Roles de Zentyal para administrar la red local del GADIPMC.**

Tabla 23. *Paquetes de instalación requeridos para Zentyal.*

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

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

Al instalar los paquetes de acuerdo al rol, en el DASHBOARD se puede ver una interfaz amigable, en el que estos paquetes están listos para ser configurados. .

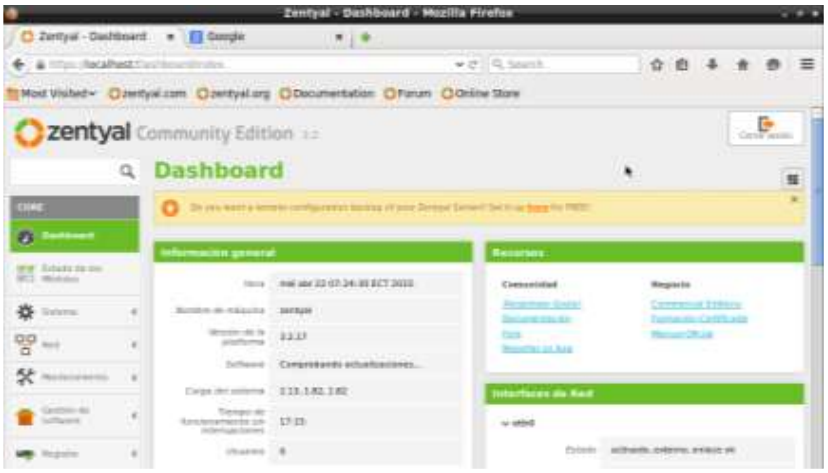


Figura 54. Dashboard de Zentyal.

Fuente: Servidor Zentyal.

A continuación se detalla el proceso que se realiza para satisfacer los requerimientos con la configuración de cada rol.

4.3.1.2.2 Configuración de Zentyal Infrastructure.

1. **Servicio DNS**

Esta configuración de nombre de dominio de red, sirve para que los usuarios de la red trabajen bajo un mismo dominio y así el administrador pueda controlar el uso de la red que ellos realizan.

Figura 55. Configuración de dominio de red.

Fuente: Servidor Zentyal.

2. **Servicio DHCP**

Se activa el servicio DHCP, a través del cual se asigna automáticamente el direccionamiento IP, para los usuarios de la red.

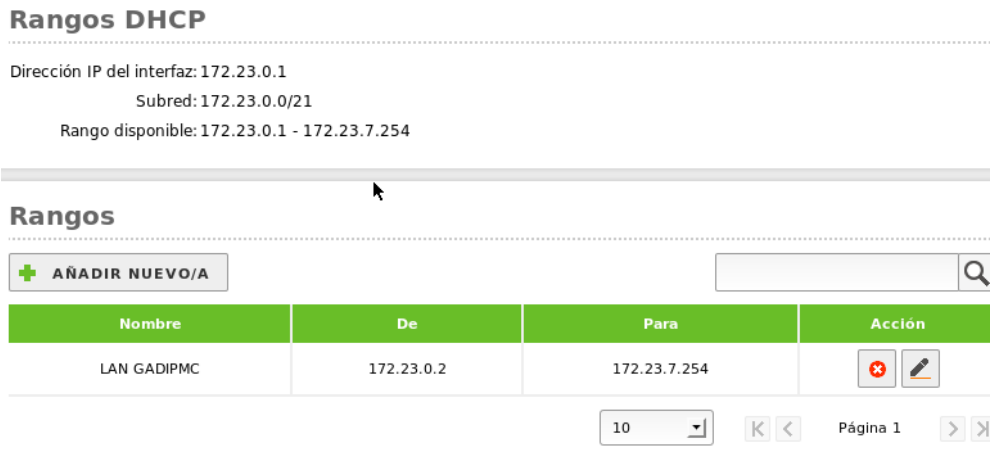


Figura 56. Activación DHCP.

Fuente: Servidor Zentyal.

4.3.1.2.3 Configuración de Zentyal Office.

1. **Servicio User and Computers**

Este servicio permite crear usuarios y grupos de usuarios bajo un dominio de red, el mismo que se vincula al servidor Open LDAP, para formar una base de datos de los usuarios.

Figura 57. Configuración LDAP.

Fuente: Servidor Zentyal.

- **Creación de grupos:**

Cree grupos de acuerdo a las direcciones existentes en el municipio de Cayambe.

Figura 58. Creación de Grupos.

Fuente: Servidor Zentyal.

- **Creación de usuarios:**

Para cada grupo cree los usuarios, ingresando la información correspondiente, como: nombre de, descripción, contraseña, y el grupo al que pertenece.

Figura 59. Creación de Usuarios.

Fuente: Servidor Zentyal.

2. Backup o Copias de seguridad.

Zentyal permite obtener respaldos de la información configurada en el servidor, por lo que es necesario que el modulo correspondiente, este activado. El administrador podrá obtener respaldos de las configuraciones realizadas en el servidor, y de la misma manera podrá restaurarlas.

Figura 60. Módulo copias de seguridad habilitado.

Fuente: Servidor Zentyal.

4.3.1.2.4 Configuración de Zentyal Gateway.

En este módulo se configura servicios como Proxy HTTP, Cortafuegos, el sistema de detección contra intrusos y portal cautivo.

1. **Servicio Firewall/Proxy**

Permite filtrar y negar acceso a páginas web http de forma transparente. Zentyal trabaja mediante ***perfiles de filtrado***, en el que se establece un umbral, mismo que usa un método heurístico y puede equivocarse en bloquear una página, por ello se hace uso de las listas por categorías, donde se sube un archivo que contiene una lista negra, el cual se aplica al perfil de filtrado, bloqueando las paginas requeridas.

Figura 61. Lista negra para el perfil restricciones.

Fuente: Servidor Zentyal.

Entre las páginas web para denegar el acceso se encuentran las redes sociales, páginas web de videos, música, contenidos obscenos, ya que estas son las que más recursos de red consumen.

Figura 62. Añadiendo dominio al perfil de filtrado.

Fuente: Servidor Zentyal.

Figura 63. Acceso denegado a YouTube.

Fuente: Navegador Mozilla.

2. Servicio Cortafuegos.

A través de este se complementa la denegación de páginas web https, para ello se configuran ***objetos y servicios***, los cuales no son más que pequeños archivos que ayudan a facilitar la creación de reglas de filtrado al final.

Para cada objeto se ingresa las direcciones IP de las páginas web o usuarios al que se le deniega o permite el acceso.

El servicio en este caso es https, mismo que tiene registrado su puerto, y se aplicará para denegar al acceso a redes sociales como Facebook, y YouTube.

Figura 64. Direcciones IP de Facebook

Fuente: Servidor Zentyal.

Figura 65. Configuración de servicio https.

Fuente: Servidor Zentyal.

Ya que es una entidad pública y manejan redes sociales y edición de material multimedia existen usuarios privilegiados a los cuales se les permite el acceso a todo a través del internet, esta es la dirección de Comunicación, Directores y Jefes Departamentales.

Figura 66. Reglas de acceso para la red interna.

Fuente: Servidor Zentyal.

3. 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 en la que se elige la acción a realizarse y la generación de una alarma en caso de detección de un intruso.

Figura 67. Habilitando IDS/IPS en la interfaces de red.

Fuente: Servidor Zentyal.

Figura 68. Establecimiento de reglas para el IDS/IPS.

Fuente: Servidor Zentyal.

4. Portal cautivo

Esta configuración se la realiza para el control de acceso de los usuarios a la red, y uso de internet. Se activa como interfaz cautiva a la interfaz que pertenece a la red local (LAN), éste se aplica a todos los usuarios.

Figura 69. Configuración de Portal Cautivo.

Fuente: Servidor Zentyal.

Nota: Para más detalle revise el manual de Zentyal 3.2 en el Anexo C.

4.3.2 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.

Figura 70. Seguridad Lógica.

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

La gestión de seguridad se encarga de controlar el acceso al sistema de gestión de red, sistema de seguridad, y equipos de red local, así como también el control de acceso de usuarios, y protección de la red a través de un IDS/IPS.

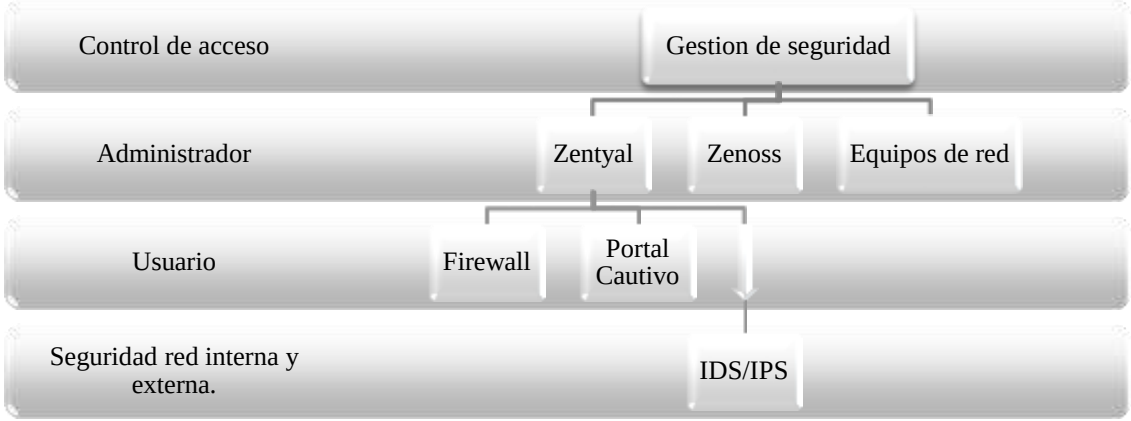


Figura 71. Manejo de gestión de seguridad.

Fuente: Elaborado por Cyntia Inuca.

4.3.2.1 *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.

- **Usuario administrador.**

  Para el control de la herramienta de gestión Zenoss se tiene dos usuarios:

  - ✓ Usuario ***admin.***
  - ✓ Usuario ***monitoreo***.

Los cuales tiene los mismos roles de administradores de la aplicación de gestión Zenoss.

Figura 72. Gestión de usuarios Zenoss.
Fuente: Aplicación Zenoss.

Figura 73. Ingreso a la aplicación Zenoss.
Fuente: Aplicación Zenoss.

4.3.2.2 *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.

Figura 74. 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.

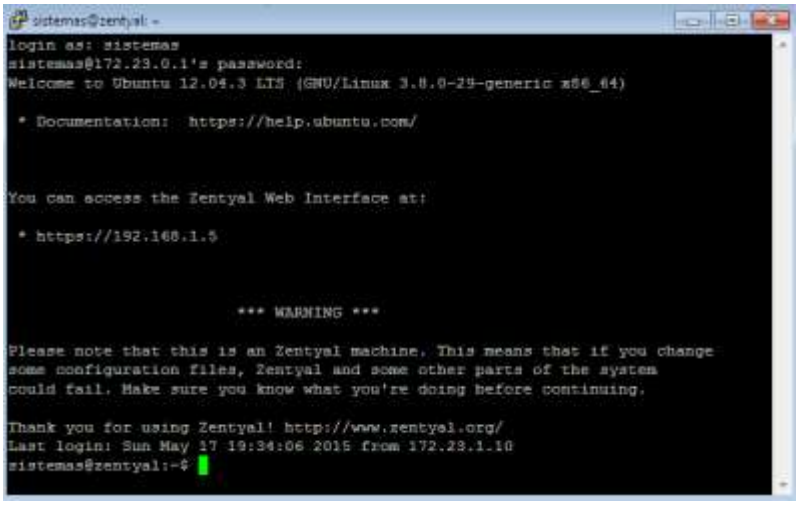


Figura 75. Ingreso de usuario administrador a través de ssh.

Fuente: Aplicación Putty.

4.3.2.3 *Control de acceso a equipos.*

Los equipos de red que conforman la red del municipio no cuentan con ningún tipo de configuración, la dirección de TIC no tiene un registro que especifique como acceder a estos equipos. La manera en que se accedió a estos equipos es a través de cable de consola, a través de ello se verificó la dirección IP de fábrica asignada al equipo, esta se usó para acceder mediante interfaz web y verificar si tiene soporte ssh, pero ya que los equipos de conmutación de la red actúan únicamente en modo acceso carecen de configuración alguna por ahora no se activa este servicio.

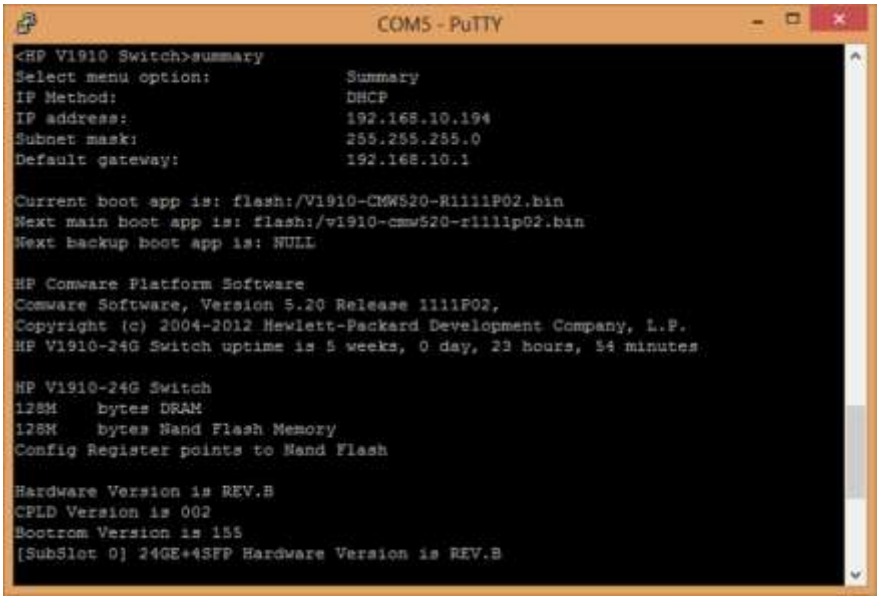


Figura 76. Acceso al switch HP-1910 por consola.
Fuente: Aplicación Putty.

Nota: No se puede acceder de ninguna manera a los equipos de red, ya que no cuentan con configuraciones de enrutamiento, para acceder al equipo por interfaz web debe configurar al equipo (PC) que quiera acceder entorno a la red de dirección IP de fábrica del equipo (switch).

4.3.2.4 *Control de usuarios de red.*

Cada funcionario tendrán asignado un usuario y contraseña para acceder a la red local del municipio mediante un portal cautivo, cada uno es responsable del que se le dé.

El administrador tiene la potestad de dar de alta o baja a un usuario, así como la asignación de privilegios.

Para preservar el ancho de banda se controla el acceso al internet limitando acceso a páginas web como redes sociales, páginas de videos y descargas ya que estas ocupan mucho recurso de la red, pudiendo de esta manera mantener un nivel de disponibilidad estable del servicio.

Figura 77. Acceso de usuarios por portal cautivo.

Fuente: Navegador Mozilla.

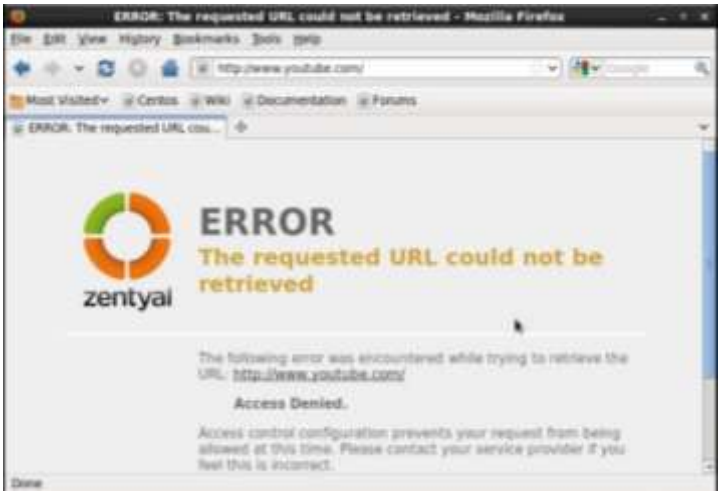


Figura 78. Acceso denegado a YouTube.

Fuente: Servidor Zentyal.

4.3.3 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.

Figura 79. 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.

4.3.3.1 *Detección de fallos*

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.

4.3.3.1.1 Gestión proactiva

La gestión proactiva anticipa que suceda un fallo, a través de herramientas básicas de diagnóstico, que permiten probar la conectividad, verificar si un dispositivo es alcanzable o está disponible. Zenoss tiene integradas herramientas esenciales como:

- **Ping:** La herramienta básica más conocida en administración de redes, través de la cual se envían paquetes ICMP, esperando una respuesta, para verificar si una maquina está respondiendo y por ende saber si es accesible a través de la red.

  Pasos para ejecutar el ping.

  - ✓ Infrastructure.
  - ✓ Selecciones el dispositivo.
  - ✓ Devices.
  - ✓ Commands.
  - ✓ Ping

Figura 80. Ventana Commands ping.

Fuente: Aplicación Zenoss.

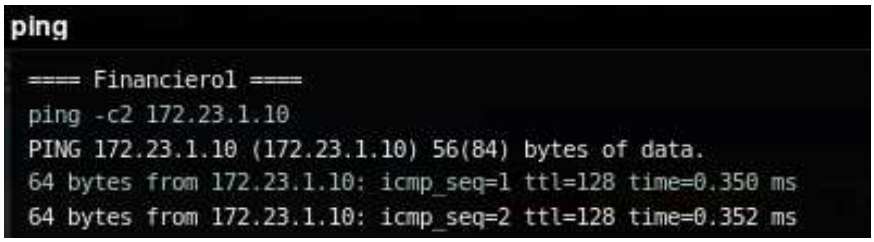


Figura 81. Respuesta de comando ping.

Fuente: Aplicación Zenoss.

- **Traceroute:** Esta herramienta ayuda a rastrear las rutas que tiene que atravesar los paquetes desde el servidor hasta el host destino.

  Pasos para ejecutar el comando traceroute.

  - ✓ Infastructure.
  - ✓ Selecciones el dispositivo.
  - ✓ Devices.
  - ✓ Commands.
  - ✓ Traceroute.

Figura 82. Ventana Commands Traceroute.

Fuente: Aplicación Zenoss.

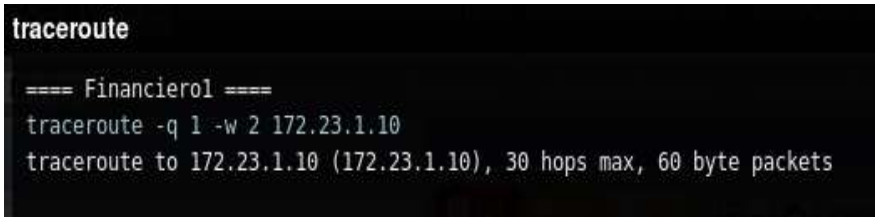


Figura 83. Respuesta de comando Traceroute.

Fuente: Aplicación Zenoss.

En caso de que el host destino no responda con un ping ésta es una herramienta ayuda a aislar la falla, a través de esta se puede detectar el punto hasta donde alcanza a llegar el paquete trasmitido, y diagnosticar el elemento de fallo.

- **Snmpwalk:** esta herramienta es útil para verificar la funcionalidad del protocolo SNMP, emite una serie de mensajes getnext al dispositivo gestionado pidiendo información de las OID´s del dispositivo gestionado.

Pasos para ejecutar el comando snmpwalk.

- ✓ Infastructure.
- ✓ Selecciones el dispositivo.
- ✓ Devices.
- ✓ Commands.
- ✓ Traceroute.

Figura 84. Ventana Commands snmpwalk.

Fuente: Aplicación Zenoss.

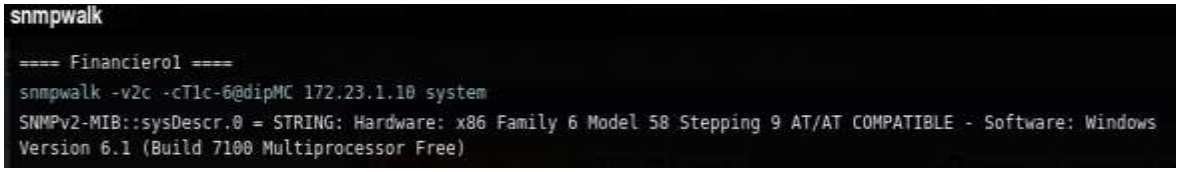


Figura 85. Respuesta de comando snmpwalk.

Fuente: Aplicación Zenoss.

4.3.3.1.2 Gestión reactiva.

Esta gestión actúa cuando el fallo ya ha sucedido, mediante el monitoreo con Zenoss se detectan las fallas producidas en la red, las cuales se pueden ver a través de la aplicación en la consola de eventos y mediante notificaciones por correo electrónico.

- **Consola Events**

Figura 86. Detección de fallos de Zenoss.

Fuente: Aplicación Zenoss.

- **Notificación por correo electrónico.**

Figura 87. Notificación de falla por correo electrónico.

Fuente: Correo electrónico gmail.

En las dos formas de verificar el fallo, el software proporciona información para continuar con el ciclo de vida de incidencias de fallos, estos son el aislamiento y diagnóstico de fallos.

Figura 88. Información de detección de fallos.

Fuente: Adaptado por Cyntia Inuca.

4.3.3.2 *Aislamiento del fallo.*

Al detectar una falla se procede a aislarla, localizando el elemento de falla e identificando el estado en el que se encuentra. Zenoss maneja una jerarquía de alarmas basada en colores, que representan el nivel de gravedad del fallo y a la vez identifica el dispositivo afectado, al cual se le identifica por su dirección IP o el nombre de equipo

Tabla 24. *Niveles de gravedad para fallos.*

Color	Estado	N° de prioridad
Rojo	Critical	5
Naranja	Error	4
Amarillo	Warning	3
Azul	Info	2
Gris	Debug	1
Verde	Cleared	0

Fuente: Curry, Jane.Event Management for Zenoss Core 4.

4.3.3.1 *Diagnóstico de fallos.*

Para el diagnóstico de fallos, se identifica la clase de evento ocurrido, y revisa el resumen de los eventos a través de Zenoss.

- ✓ **Clases de eventos.**
  - ✓ /Status: usado para eventos que afecten a la disponibilidad.
    - /Status/Ping: evento ping arriba/abajo.
    - /Status/Snmp: evento SNMP arriba/abajo.
    - /Status/Web: evento de sitio web o página arriba/abajo.
  - ✓ /Perf: Se utiliza para eventos de umbral de rendimiento.
    - /Perf/CPU: eventos utilización de CPU
    - /Perf/Memory: eventos de utilización de la memoria o de paginación.
    - /Perf/Interface: eventos de utilización de Interfaz de red.
    - /Perf/Filesystem: evento de uso del sistema de archivos.
  - ✓ /App: eventos relacionados con aplicaciones. .
  - ✓ /Change: eventos creados cuando el sistema encuentra cambios en su entorno.

4.3.3.2 *Solución de fallos.*

Después de haber diagnosticado la falla, se procede a la solución del fallo donde interviene mucho la experiencia del elemento humano pues la dirección de TIC brinda soporte técnico a los usuarios de la red constantemente.

Este proceso se detalla en el manual de procedimientos para la gestión de fallos, en este mismo documento.

4.3.4 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.

4.3.4.1 *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.

- ✓ **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.

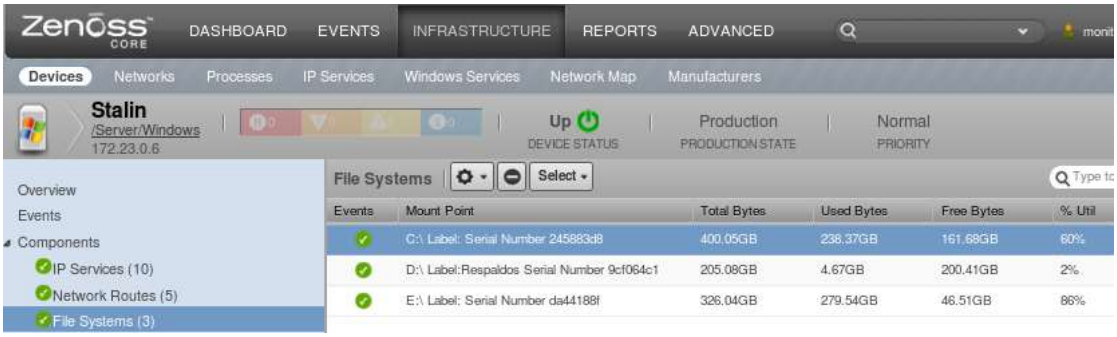


Figura 89. Monitoreo de uso de Disco Duro.

Fuente: Aplicación Zenoss.

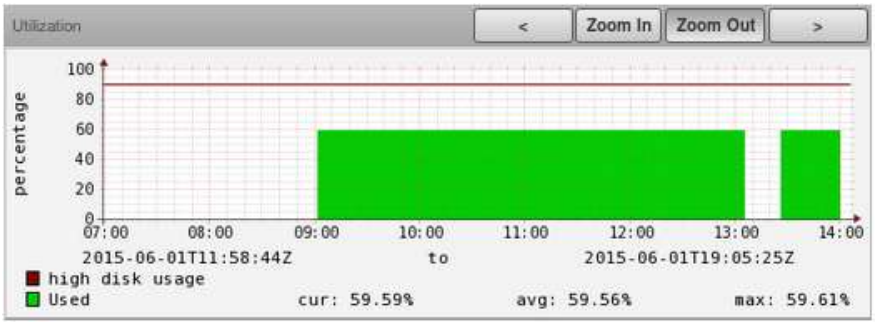


Figura 90. Grafica de uso de disco duro.

Fuente: Aplicación Zenoss.

- ✓ **Monitoreo de interfaces de red.**

Se descubren todas las interfaces del dispositivo gestionado, entre ellas se puede ver la interface 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.

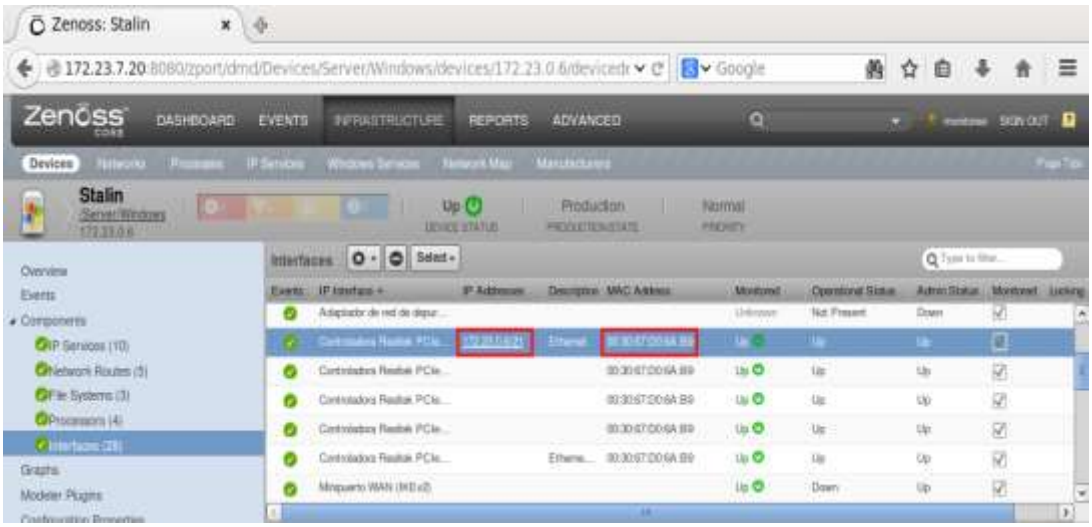


Figura 91. Monitoreo de Interfaces.

Fuente: Aplicación Zenoss.

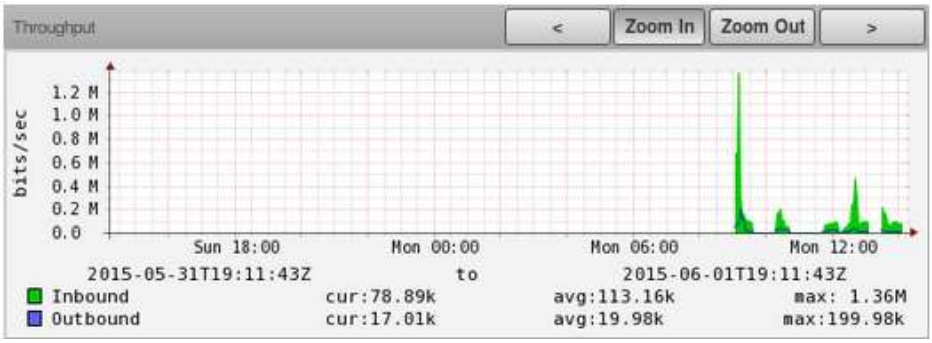


Figura 92. Grafica de rendimiento de interfaz de red.

Fuente: Aplicación Zenoss.

- ✓ **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.

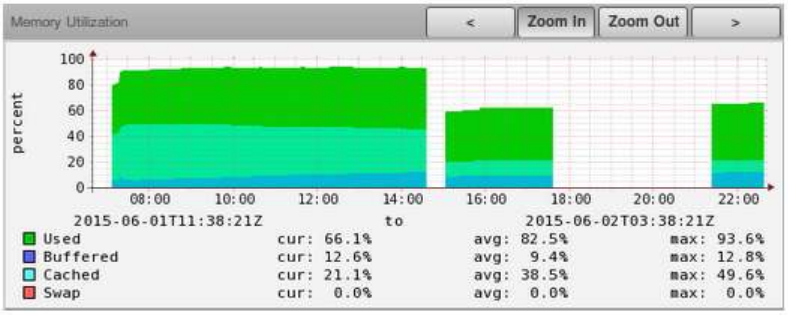


Figura 93. Monitoreo de uso de memoria.

Fuente: Aplicación Zenoss.

- ✓ **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.

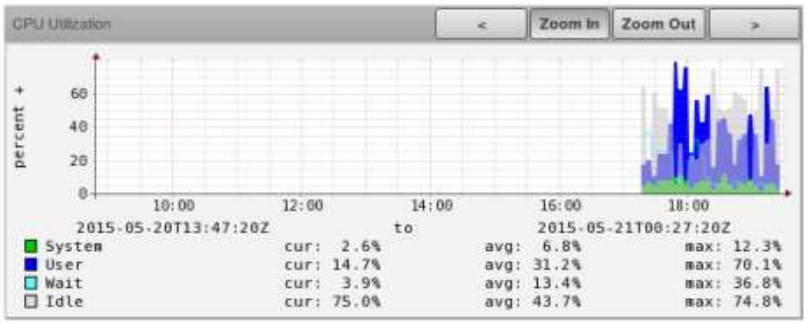


Figura 94. Monitoreo de uso de CPU.

Fuente: Aplicación Zenoss.

4.3.4.2 *Zentyal.*

Zentyal muestra información del uso de sus recursos, de manera que el administrador de red puede revisar cómo está funcionando.

- ✓ **Uso de CPU (Procesador).**

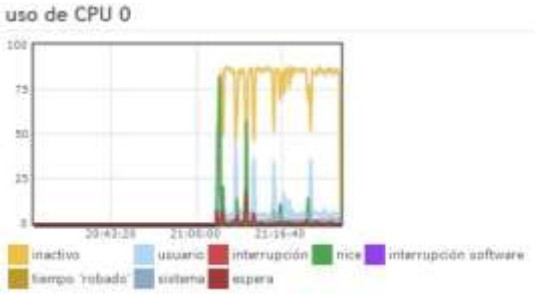


Figura 95. Uso de CPU de Zentyal.

Fuente: Servidor Zentyal.

- ✓ **Memoria RAM.**

Figura 96. Uso de memoria RAM.

Fuente: Servidor Zentyal.

- ✓ **Disco Duro.**

Figura 97. Uso de disco duro de Zentyal.

Fuente: Servidor Zentyal.

- ✓ **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.

Figura 98. Monitoreo de ancho de banda.
Fuente: Servidor Zentyal

4.3.5 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 manejar 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.

Figura 99. Gestión de contabilidad.

Fuente: Adaptado por Cyntia Inuca.

- **Inventario administrador**

El administrador de red lleva un inventario mediante Excel, en el que se registran las características más importantes de los dispositivos que están conectados a la red.

Inventario de Equipos de la Red Local GADIPMC

DEPARTAMENTO	NOMBRE USUARIO	NOMBRE RED	GRUPO TRABAJO	DIRECCIÓN IP	MACADRESS	PROCESADOR
COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	DANIEL CHICAIZA	SOFTECNICO	WORKGRUOP	172.23.0.4	E0-69-95-46-3F-97	INTEL CORE
COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	RONNY CARVAJAL	SISTEMASLTPS-PC	WORKGRUOP	172.23.0.5	00-27-0E-01-4F-58	INTEL CORE
COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	GERSON MALDONADO	ANALISTA-PC	GADMCAYAMBE	172.23.0.6	00-27-0E-03-5A-26	INTEL CORE
INFOCENTRO	MARTHA VALLADARES	PC8	WORKGROUP	172.23.1.223	E0-69-95-4F-90-0A	INTEL CORE
INFOCENTRO	MARTHA VALLADARES	PC9	WORKGROUP	172.23.1.224	F0-4D-A2-0C-B2-A2	INTEL CORE
INFOCENTRO	MARTHA VALLADARES	PC10	WORKGROUP	172.23.1.225	F0-4D-A2-0C-B2-96	INTEL CORE
INFOCENTRO	MARTHA VALLADARES	PC11	WORKGROUP	172.23.1.226	E0-69-95-50-1F-50	INTEL CORE

Figura 100. Inventario de equipos GADIPMC.

Fuente: Dirección de TIC GADIPMC.

- **Reportes en Zenoss.**

Para ingresar a ver los reportes en Zenoss ubíquese en la pestaña Reports, donde puede generar reportes de los dispositivos gestionados, y exportarlos.

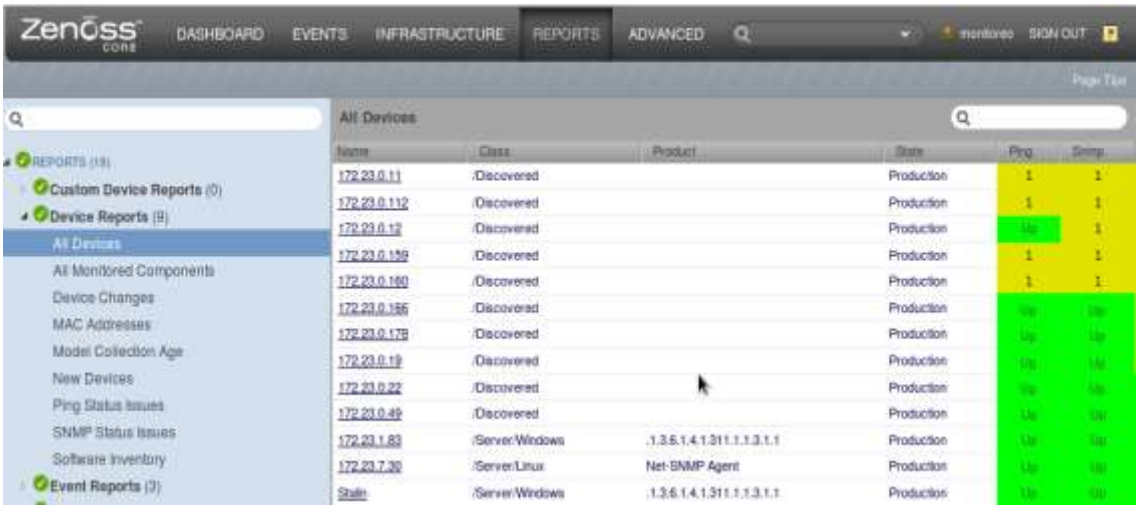


Figura 101. Reportes de todos los dispositivos que se monitorean.

Fuente: Aplicación Zenoss.

Figura 102. Reporte de los componentes de los dispositivos monitoreados.

Fuente: Aplicación Zenoss.

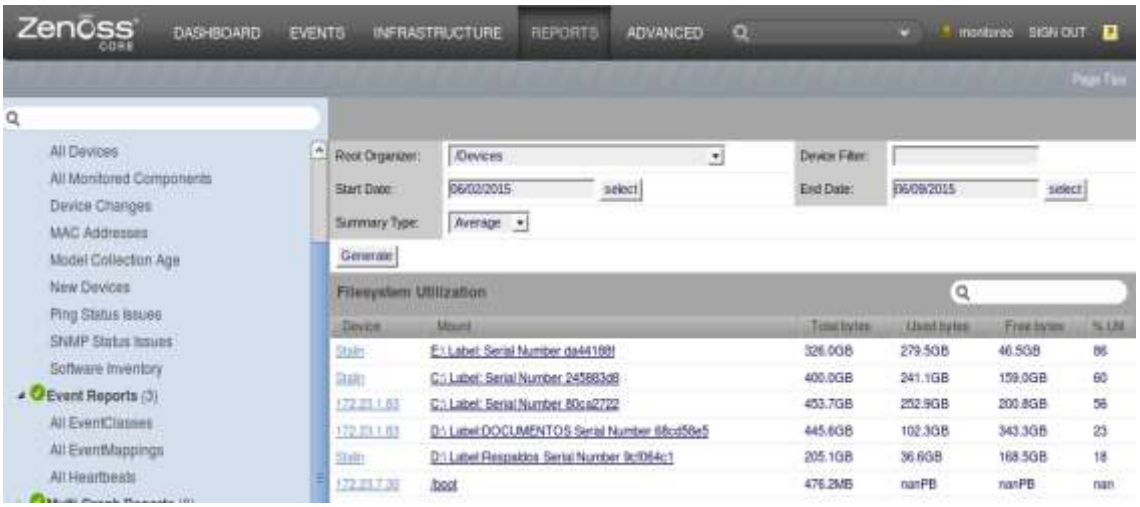
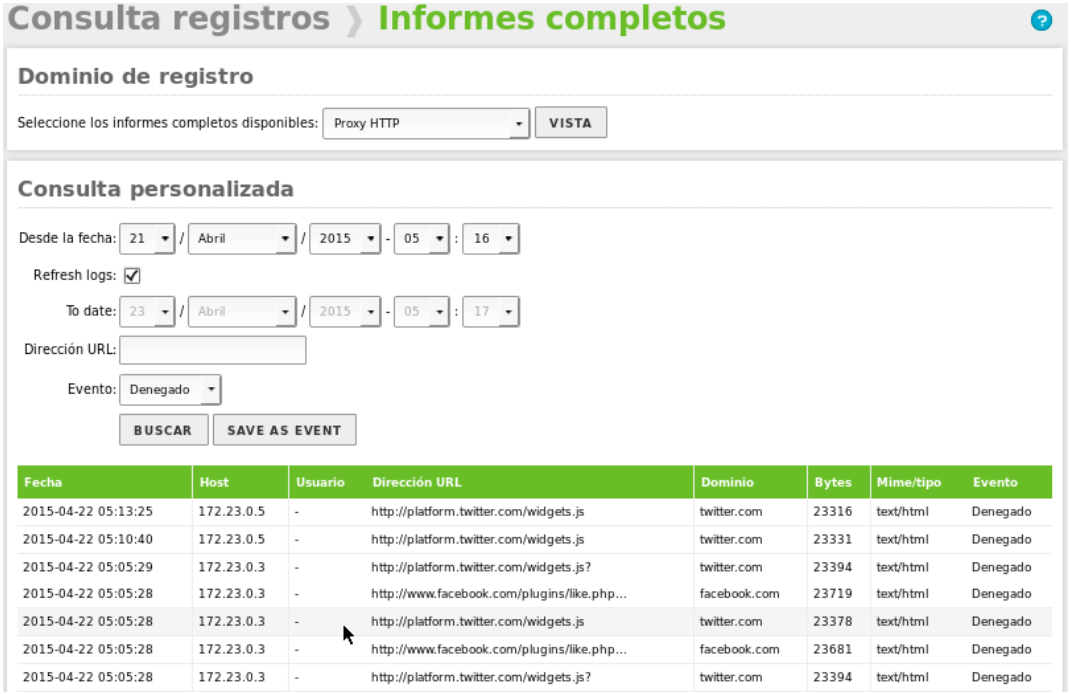


Figura 103. Reporte de rendimiento de Disco Duro.

Fuente: Aplicación Zenoss.

- **Registros en Zentyal.**

Zentyal proporciona registros de Proxy HTTP, donde el administrador puede verificar el uso que le dan al internet los usuarios, en este se identifica la dirección IP del dispositivo, la URL al que accedió, si se permitió o se denegó el acceso.



Fecha	Host	Usuario	Dirección URL	Dominio	Bytes	Mime/tipo	Evento
2015-04-22 05:13:25	172.23.0.5	-	http://platform.twitter.com/widgets.js	twitter.com	23316	text/html	Denegado
2015-04-22 05:10:40	172.23.0.5	-	http://platform.twitter.com/widgets.js	twitter.com	23331	text/html	Denegado
2015-04-22 05:05:29	172.23.0.3	-	http://platform.twitter.com/widgets.js?	twitter.com	23394	text/html	Denegado
2015-04-22 05:05:28	172.23.0.3	-	http://www.facebook.com/plugins/like.php...	facebook.com	23719	text/html	Denegado
2015-04-22 05:05:28	172.23.0.3	-	http://platform.twitter.com/widgets.js	twitter.com	23378	text/html	Denegado
2015-04-22 05:05:28	172.23.0.3	-	http://www.facebook.com/plugins/like.php...	facebook.com	23681	text/html	Denegado
2015-04-22 05:05:28	172.23.0.3	-	http://platform.twitter.com/widgets.js?	twitter.com	23394	text/html	Denegado

Figura 104. Registros de Proxy HTTP de acceso a páginas web denegadas.

Fuente: Servidor Zentyal.

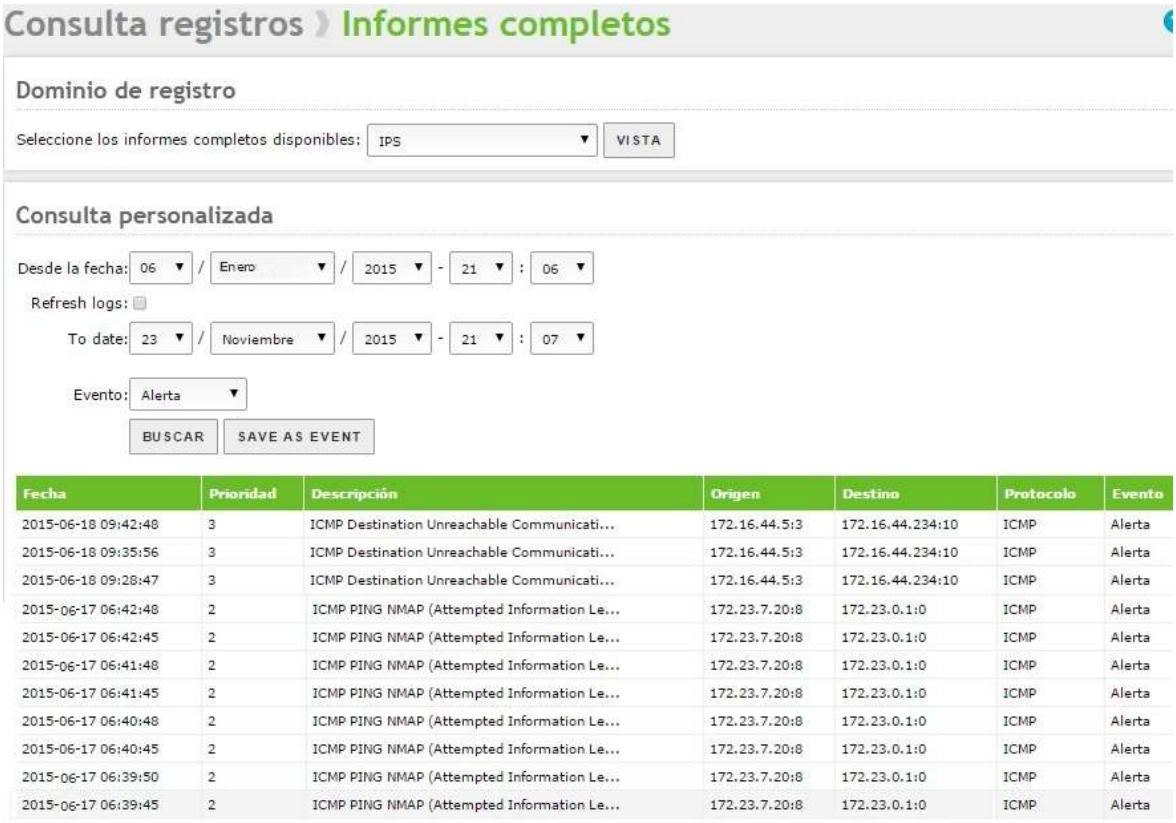
Si el administrador verifica que un dispositivo está intentando acceder frecuentemente a un cierto dominio, el podrá identificar al usuario ya que puede realizarse el seguimiento a través de la dirección IP y portal cautivo.

Usuario	Dirección IP	Uso de ancho de banda en el último mes (MB)	Acción
soportegadip	172.23.0.5	4	
cyntia.inuca	172.23.0.3	14	

Figura 105. Control de usuarios a través del portal cautivo.

Fuente: Servidor Zentyal.

Zentyal permite revisar registros IDS, a través de una alerta se identifican actividades que sean sospechosas en la red.



Fecha	Prioridad	Descripción	Origen	Destino	Protocolo	Evento
2015-06-18 09:42:48	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-18 09:35:56	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-18 09:28:47	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-17 06:42:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:42:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:41:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:41:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:40:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:40:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:39:50	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:39:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta

Figura 106. Registros IDS.

Fuente: Servidor Zentyal.

4.3.6 Topología nueva de la red local GADIPMC.

La Figura 107, integra el sistema de gestión de red y el sistema de seguridad formando la red por completo, y permitiendo al administrador el control total de la misma.

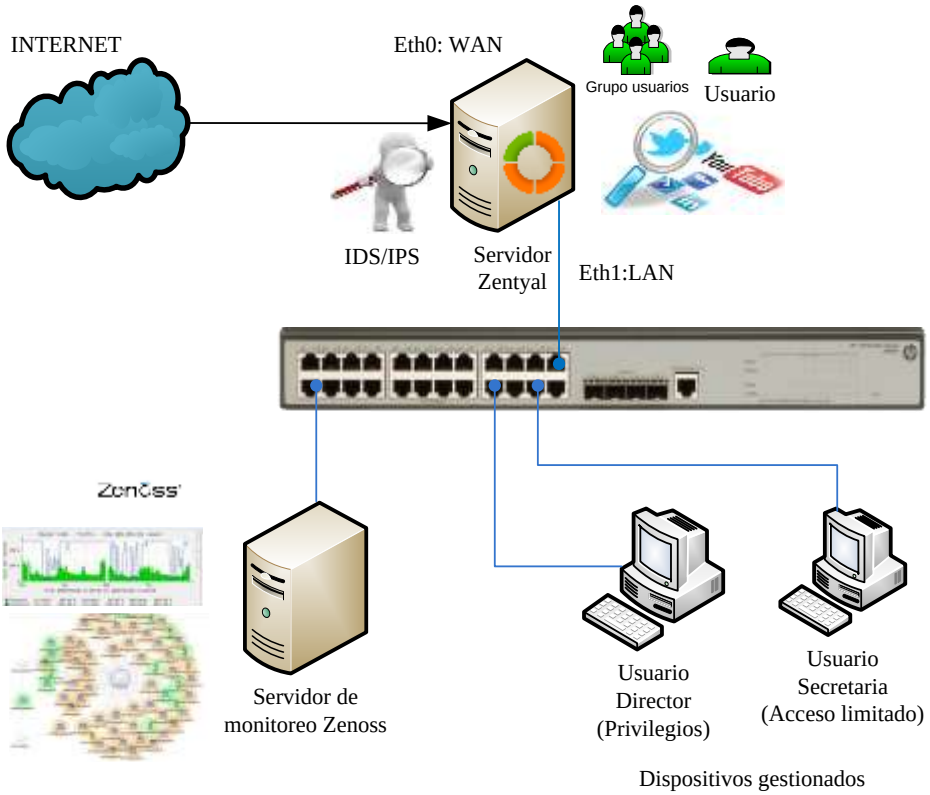


Figura 107. Topología nueva de la LAN GADIPMC.

Fuente: Elaborado por Cyntia Inuca.

4.3.7 Diseño de segmentación de la red de área local.

Debido al incremento del número de usuarios, así como la demanda del mayor número de puntos de red adicionales a su infraestructura, 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.

4.3.7.1 *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.

4.3.7.2 *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 25. *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.

Nota: El rango de direcciones IP, se distribuyen de acuerdo a las solicitudes del administrador

4.3.7.3 *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.

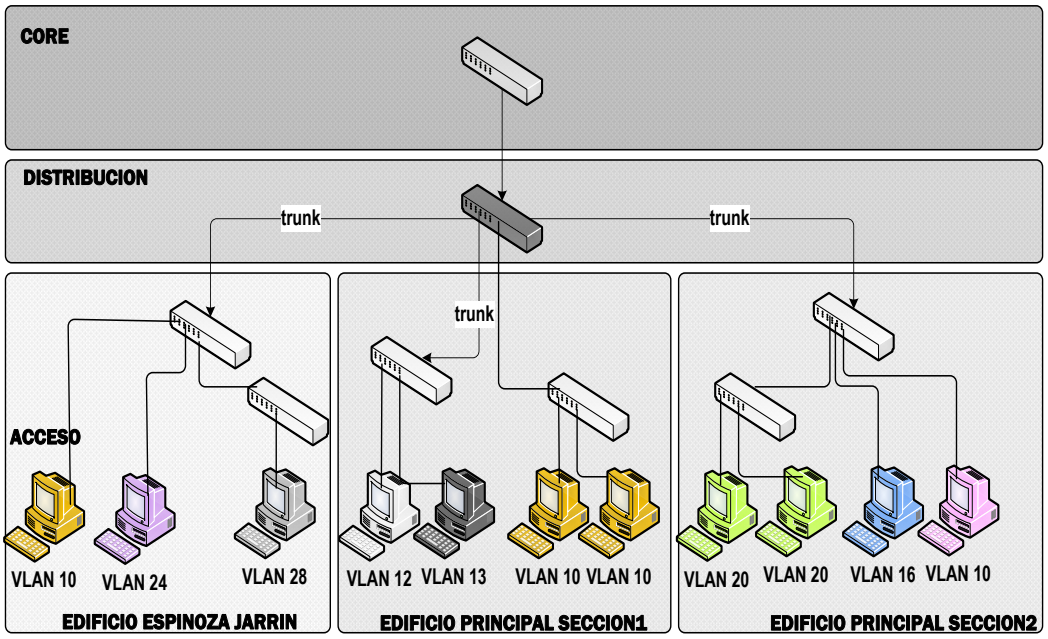


Figura 108. Segmentación de la red bajo un modelo jerarquizado.

Fuente: http://sistemasumma.com/2012/02/19/redes-jerarquicas/

4.3.7.4 *Simulación.*

Se realizó una simulación para demostrar el funcionamiento de la segmentación de la red, de acuerdo al direccionamiento IP asignado a cada dirección del municipio.

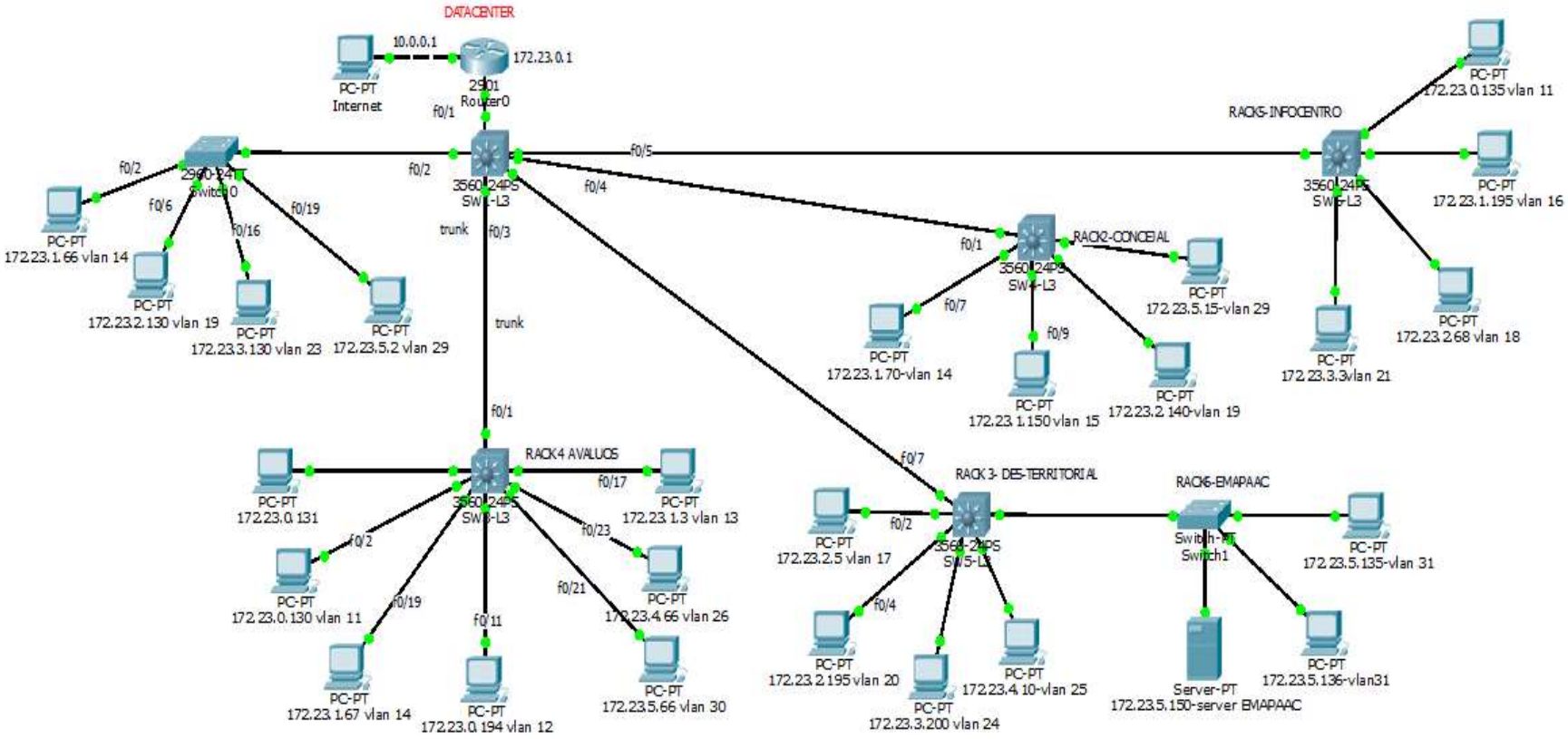


Figura 109. Simulación de segmentación de la red.

Fuente: Packet Tracer.

4.3.7.5 *Pruebas de conectividad.*

Es necesario que todas las vlans se comuniquen entre ellas, ya que se comparte información entre ellas, además de usar los servicios de la red.

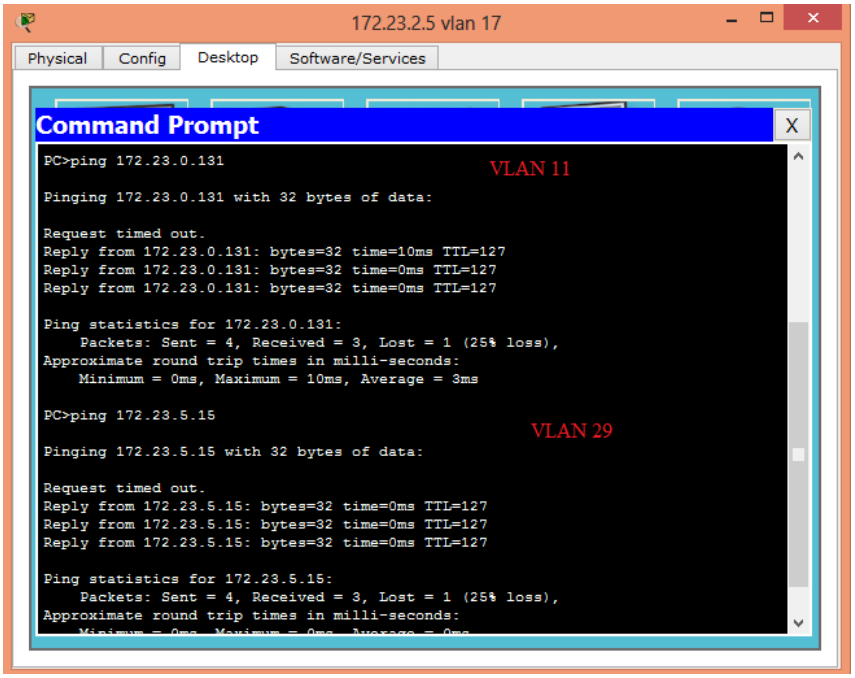


Figura 110. Respuestas de conectividad de las vlans.

Fuente: Packet Tracer.

4.4 Procedimientos para la gestión de red

El establecimiento de procedimientos es de vital importancia para la administración y gestión de la red, brindando al administrador una secuencia de procesos para mantener la red disponible, brinda soluciones rápidas para actuar ante un evento inesperado.

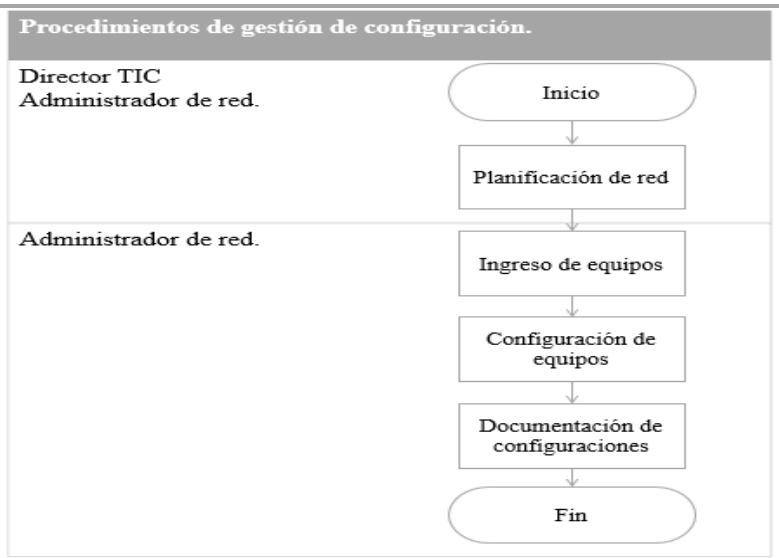
Los procedimientos a establecer cubren el modelo funcional de gestión de red ISO/OSI, para cada área se definen procedimientos seguir, integrando las herramientas de software libre, Zenoss y Zentyal, así como recurso humano.

<table>
<tr><td colspan="4">Gobierno Autónomo Descentralizado Intercultural y Plurinacional de Municipio de Cayambe</td></tr>
<tr><td></td><td colspan="2">PROCEDIMIENTOS PARA LA GESTIÓN DE RED</td><td></td></tr>
<tr><td>Versión: 1.0</td><td colspan="2">Revisado por:
Tnlg. Rony Carvajal
Jefe de Infraestructura y Conectividad</td><td>Aprobado por:
Ing. Fabián Bautista
Director de TIC</td></tr>
<tr><td colspan="4">DESARROLLO DE PROCEDIMIENTOS PARA LA GESTIÓN DE RED LOCAL</td></tr>
<tr><td colspan="4">GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE</td></tr>
<tr><td colspan="3">1. Procedimientos para la gestión de configuración.</td><td>Código: PRO-LAN-0001</td></tr>
<tr><td>N°</td><td>Actividad</td><td>Descripción</td><td>Responsable</td></tr>
<tr><td>1</td><td>Panificación de red</td><td>El administrador debe estar atento a:
– Cambios en la infraestructura de red.
– Requerimientos de nuevas tendencias tecnológicas, que mejoren el funcionamiento de la red.
– Responder a las solicitudes de los usuarios.</td><td>Director de TIC y administrador de red.</td></tr>
</table>

N°	Actividad	Descripción	Responsable
1	Panificación de red	El usuario debe notificar al administrador cuando: – Vaya a realizar algún cambio en las oficinas que afecten a la infraestructura de la red. – Cuando se roten los puestos de trabajo. – Cuando requiera acceso a algún servicio a través de la red. Cuando requiera la compra de un equipo tecnológico que se vaya a integrar a la red.	Director de TIC y administrador de red.
2	Ingreso de equipos.	Al comprar y adquirir un equipo de red, que vaya a ingresar la red, el administrador debe: – Verificar su funcionamiento, que no haya fallas de fábrica. – Registrarlo en su inventario. – y prepararlo para integrarlo a la red.	Administrador de red.
3	Configuración de equipos.	Para todo equipo de red que requieran integrarse a la red, debe: – Tener la configuración básica que le permita conectarse a la red local y sus servicios. o Configuración de direccionamiento ip estático o dhcp. Habilitar el protocolo SNMP, siempre y cuando lo soporte. o Habilite el protocolo SNMP. o Configure comunidad SNMP y asigne permisos. o Agregue información de contacto y ubicación.	Administrador de red.

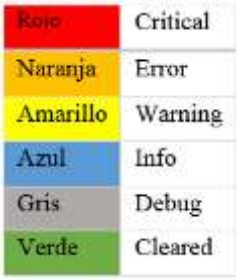
N°	Actividad	Descripción	Responsable
1	Configuración de equipos.	Para integrar un equipo al sistema de gestión de red Zenoss: – Vaya a Device, – Haga clic en + (añadir) – Ingrese la dirección ip del equipo, la clase de dispositivo, habilite snmp e ingrese la comunidad y el puerto 161. El direccionamiento ip del dispositivo a gestionar debe estar configurado de forma estática.	Administrador de red.
4	Documentación de configuración.	1. Obtener respaldos de configuraciones estables realizadas en: – Servidores (Zentyal y Zenoss). – Configuraciones que se realicen en los dispositivos a gestionar, ej. switch administrables. 2. Almacenar los respaldos en el servidor de archivos FTP de la institución. 3. En caso de haber algún tipo de des configuración, copiar el respaldo y cargarlo nuevamente al servidor o equipo.	Administrador de red.

Flujograma:



GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

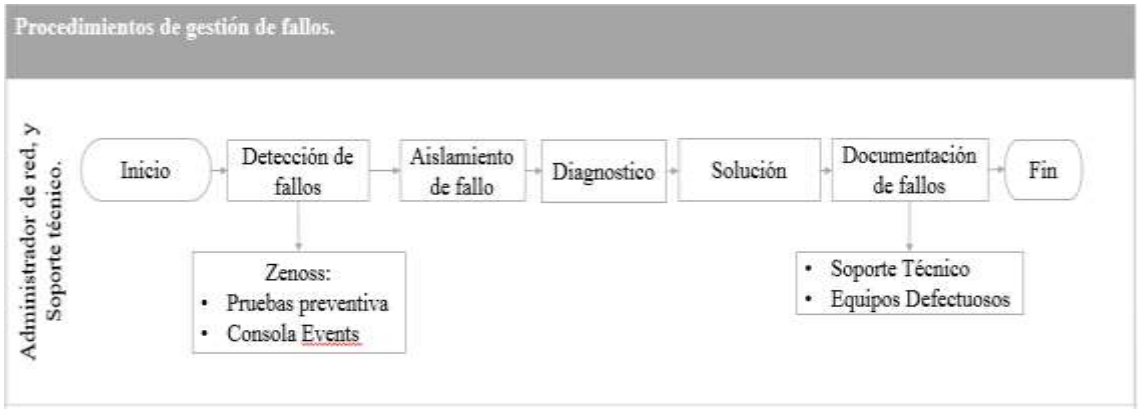
2. Procedimientos para la gestión de fallos.			**Código:**	PRO-LAN-0002
N°	**Actividad**	**Descripción**		**Responsable**
1	Detección de fallos.	La detección de fallos se lo realiza a través de la aplicación de gestión Zenoss: **Pruebas preventivas:** A través del software de monitoreo se puede ejecutar comandos como: – Ping, Para verificar conectividad. – Traceroute, Puede actuar como aislador para detectar hasta qué punto de la red llega el paquete emitido. – Snmpwalk, Para verificar si hay comunicación entre estación gestora y dispositivo gestionado. **Gestión reactiva:** El administrador de red puede revisar los fallos producidos en: 1. Consola EVENTS de Zenoss. 2. Correo electrónico. 3. Llamada por el usuario. En el que el administrador debe analizar los eventos, y actuar ante estos.		Administrador de red.
2	Aislamiento de fallos.	El software de monitoreo Zenoss, permite aislar la falla, detecta que dispositivo es, y emite alarmas por colores, los cuales definen el estado en que se encuentra el dispositivo.		Administrador de red.

N°	Actividad	Descripción	Responsable
2	Aislamiento de fallos.	 El administrador sabrá dar prioridad a los fallos de acuerdo a estas alarmas. Y procederá con el diagnostico.	Administrador de red.
3	Diagnóstico de fallos.	Zenoss, proporciona información de diagnóstico, en el que muestra la clase de eventos ocurrido, mediante esta información el administrador procede a verificar el fallo y buscar las posibles soluciones junto al técnico encargado. – **CMD is down:** problemas en la interfaz de red. – **SNMP is down**: protocolo snpm no está habilitado. – **Perf/CPU:** problemas en el rendimiento de CPU. – **Perf/disk:** problemas de saturación de disco.	Administrador de red y Personal de Soporte técnico
4	Solución de fallos.	**Procedimientos para resolver problemas de conexión a internet.** – Revisar la conexión de cable de red, desde el punto de red hacia el equipo terminal del usuario. – Revisar si detecta conexión, a través de la tarjeta de red. – Si no detecta revisar del direccionamiento y asignación IP. – Realizar pruebas de testeo, como ping, al gateway de la red. – Realiza un ping o traza a una página de internet. Si el procedimiento anterior no funciona: – Revisar la tarjeta de red y el punto de conexión de red. – Cambio de cable de red.	Soporte técnico.

N°	Actividad	Descripción	Responsable
4	Solución de fallos.	– Reiniciar el equipo (computador, o routers inalámbricos). – Reconfigurar los equipos. **Procedimiento para resolver problemas de acceso denegado a sistemas y servicios de la red.** – Los accesos a sistemas y servicios de red, generalmente manejan usuario y contraseña, revisar si está ingresando correctamente el usuario y contraseña asignado, de lo contrario el administrador deberá revisar este acceso a través del sistema y generan una nueva contraseña. – Otra causa posible es la desconexión del servidor, el administrador debe revisar el software de monitoreo el estado del servidor, si emite alguna alerta o no, el administrador y técnico encargado deben estar pendientes de que el servidor no presente problemas. – En compartición de archivos la posibilidad de que no pueda acceder a la información compartida es que el equipo del usuarios que comparte esta apagada, o se limitó el número de accesos. **Procedimientos para resolver problemas de compartición de impresoras.** – Los usuarios que deseen imprimir deben tener instalado el driver o controlador de la impresora. – Si la impresora esta compartida, el equipo terminal del usuario que desea imprimir debe vincular su conexión al equipo que tiene instalado la impresora. Si el equipo donde está instalado la impresora no está encendido, no puede imprimir debido a que no hay conexión.	Soporte técnico

N°	Actividad	Descripción	Responsable
4	Solución de fallos.	**Procedimientos para resolver problemas de SNMP** 1. Verificar si el equipo gestionado tiene SOPORTE SNMP. 2. Configurar comunidad SNMP. 3. Asignar permisos. 4. Para probar la funcionalidad SNMP verificar a través de un snmpwalk. **Procedimiento para solucionar problemas de rendimiento de recursos de los equipos gestionado** 1. Verificar como está trabajando cada recurso gestionado mediante Zenoss. 2. Analizar capacidades. 3. Verificar los procedimientos para gestión de rendimiento. PRO-LAN-0003.	Soporte técnico
5	Documentación de fallos	1. Al solucionar un problema el técnico registrara el proceso de realizado en una hoja de control en el que se detalle: a. Fecha. b. Departamento. c. Usuario. d. Descripción del daño. e. Solución ejecutada. f. Si se solucionó o no, o está pendiente la solución. g. Y para constancia de brindad soporte técnico tendrá que firmar el usuario que pidió el soporte así como el técnico que atendió el requerimiento. 2. Se llevará un registro de aquellos equipos que presentan defectos que están provocando problemas constantes. a. Registrará los datos del equipo. b. La frecuencia de fallos. c. El historia de problemas y soluciones dadas.	Soporte técnico.

Flujograma:



Anexos:

HOJA DE SOPORTE TÉCNICO			
Fecha:		Departamento:	
Usuario:			
Descripción del daño:			
Solución ejecutada:			
Cumplido:	Si: ☐ No: ☐ Pendiente: ☐	Nombre del técnico:	
Firma del usuario:		Firma del técnico:	

REGISTROS DE EQUIPOS DEFECTUOSOS.			
Equipo:	**Dirección IP:**	**Frecuencia de fallos**	
Marca:	**Dirección MAC:**	**Semana**	**Día**
Persona Encargada:	**Serie:**	1	1
Departamento:		2	2
		3	3
		4	4
		5	5
		más=	más =

historial problemas	Solución:
Fecha:	
Fecha:	
Fecha:	
Fecha:	

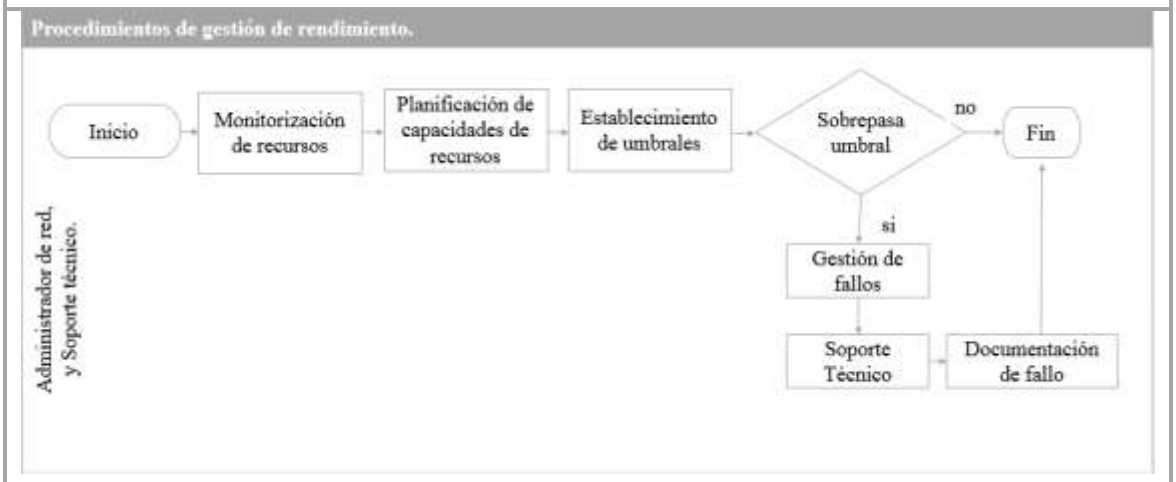
GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

3. Procedimientos para gestión de rendimiento.			**Código:**	PRO-LAN-0003
N°	**Actividad**	**Descripción**		**Responsable**
1	Planificación y aceptación del sistema	1. Monitorear el uso de los recursos a través de Zenoss, el administrador verificará las capacidades de cada recurso, y través de esto se analiza el uso que se está dando a dichos recursos. 2. Proyectar requisitos de la capacidad adecuada para asegura que los recursos de los equipos funcionen adecuadamente.		Administrador de red
2	Establecimiento de umbrales	Al monitorear los recursos, el administrador podrá ver que ciertos dispositivos están sobresaturando el uso de sus recursos, por lo que se determina umbrales para garantizar que los recursos trabajen correctamente. Recurso / Umbral Disco Duro / 80% Memoria RAM / 80% Carga de procesador (CPU) / 80% Si sobrepasan los umbrales establecidos, el software de monitoreo emitirá un evento, indicando que se sobrepasó el umbral establecido de uso ya sea de disco duro, memoria RAM, CPU. – Si el uso del disco duro de un servidor, o computador, supera el 80% de su capacidad máxima, se debe respaldar la información en unidades de almacenamiento, como discos duros, o un servidor de archivos que tenga la capacidad suficiente de mantener dicha información.		Administrador de red

N°	Actividad	Descripción	Responsable
2	Establecimiento de umbrales	– El uso de la memoria RAM depende del trabajo que realice un servidor o computador, por eso se establece como un valor máximo de trabajo el 80%, previniendo que este provoque que los procesos que se realicen se tornen lentos. El administrador de red, decidirá qué es lo mejor para los usuarios, y servidores de acuerdo a las funciones que se desempeñe, poniendo alternativas como: Uso de sistemas operativos de software libre, que tienen requerimientos de RAM, bajos. Incremento de la capacidad de memoria RAM, si el equipo lo soporta, en el caso de servidores permitirá el manejo de mayor número de usuarios que pueden realizar petición de procesos al servidor. (Hoy, 2012) – La carga de procesador es importante ya que es el núcleo de funcionamiento de un equipo, al establecer el umbral máximo es de 80% de su capacidad, se previene que se produzcan cuellos de botella de los procesos que se ejecutan. La carga de procesador viene de la mano junto a la memoria RAM, y el disco duro, de forma que se coordina el trabajo de manera eficiente. (Magazine, 2008) En caso de que se sobrepase el umbral, el administrador de red deberá tomar medidas, como: Revisión de procesos y eliminación de aquellos que no se solicitaron, ya que muchas veces se ejecutan proceso por defecto que no se usan.	Administrador de red.

N°	Actividad	Descripción	Responsable
2	Establecimiento de umbrales	Cambio de procesador, de acuerdo al trabajo que desempeñe, existen procesadores de uso básico (athom, celeron, Pentium, AMD E2 o E4) intermedio (core i 3, i5, AMD A3,A8) o avanzado (core i7, AMD A10 o FX). A la vez elegir la memoria RAM adecuada, de 2, 4GB en memoria RAM es suficiente para el uso normal que se les da a las computadoras, y para procesos más avanzados se eligen ente 8 a 16GB, el disco duro dependerá de la cantidad de información que maneje. (Organización de Consumidores y Usuarios, 2015)	Administrador de red.

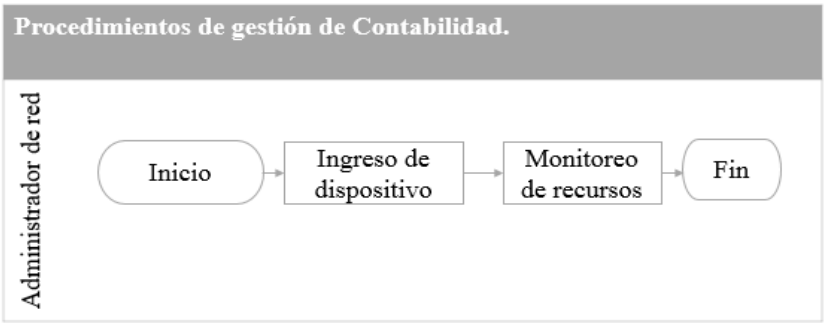
Flujogramas.



4. Procedimientos para gestión de contabilidad.	Código:	PRO-LAN-0004

N°	Actividad	Descripción	Responsable
1	Manejo de reporte.	La **aplicación de Zenoss** permite manejo de reportes. 1. Diríjase a la pestaña ***Reports***, donde puede ver reportes de los dispositivos gestionados de la red.	Administrador de red.

<table>
<tr><th>N°</th><th>Actividad</th><th>Descripción</th><th>Responsable</th></tr>
<tr><td>1</td><td>Manejo de reporte.</td><td>2. El administrador puede generar los reportes y exportarlos en un formato cvs, en caso de ser necesario.

Zentyal permite obtener registros uso de internet, Proxy HTTP, IDS/IPS, y también ver los usuarios que hacen uso de la red.
– Haga clic en Mantenimiento
– Registros
– Y seleccione el tipo de registro que desea ver, (Proxy HTTP, IDS/IPS).
Para ver los usuarios de la red.
– Haga clic en portal cautivo.
– Usuarios actuales.</td><td>Administrador de red.</td></tr>
<tr><td>2</td><td>Manejo de inventarios.</td><td>1. Registrar los equipos de comunicación interconectados a la red en un inventario basado en Excel, donde se registre.
a. Equipo
b. Modelo
c. Serial
d. Características físicas del equipo
e. Direccionamiento IP estática si es el caso.</td><td>Administrador de red.</td></tr>
<tr><td colspan="4">Flujograma:</td></tr>
<tr><td colspan="4"> 
</td></tr>
</table>

GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

5. Procedimientos para la gestión de seguridad.		**Código:**	PRO-LAN-0005
N°	**Actividad**	**Descripción**	**Responsable**
1	Control de accesos	**1. Equipos de comunicación (servidores, PC, routers inalámbricos, switch administrables, etc):** a. Establecer un usuario y contraseña para administrar el equipo de comunicación que este interconectado en la red local. **2. Equipos de conmutación:** a. Ingresar por cable de consola. b. Averiguar su dirección ip por default, para luego acceder por interfaz web. c. Verificar si tiene soporte ssh, para en un futuro habilitarlo. **3. Acceso a sistema de gestión de red, Zenoss:** Se establece un usuario administrador que tenga el control de todos los campos de gestión de red a través del software. El usuario administrador puede crear otros usuarios que también puedan acceder a la aplicación pero con acceso limitado a la información y visualización de los recursos monitoreados. Para acceder al sistema de gestión de red, se lo realiza en el navegador donde ingresa la IP del servidor y accede mediante su usuario y contraseña.	Administrador de red.

N°	Actividad	Descripción	Responsable
1	Control de accesos	**4. Acceso a sistema de seguridad, Zentyal:** a. ***Interfaz web.*** Únicamente el usuario administrador puede ingresar a la plataforma de Zentyal, a través del navegador debe ingresar la IP o dominio del servidor, e ingresar su usuario y contraseña. b. ***Ssh.*** El administrador puede realizar configuraciones para que se acceda a Zentyal a través de ssh, esta configuración se la realiza en: – Cortafuegos. – Redes internas y redes externas. – Cree la regla. – Permitir el servicio ssh, al rango de direcciones IP que pertenecen a departamento de TIC, para que se acceda únicamente desde cualquiera de esos equipos. Para acceder mediante ssh hágalo a través de la aplicación putty. a. Habilite ssh puerto 22. b. E ingrese la dirección ip del servidor	Administrador de red.

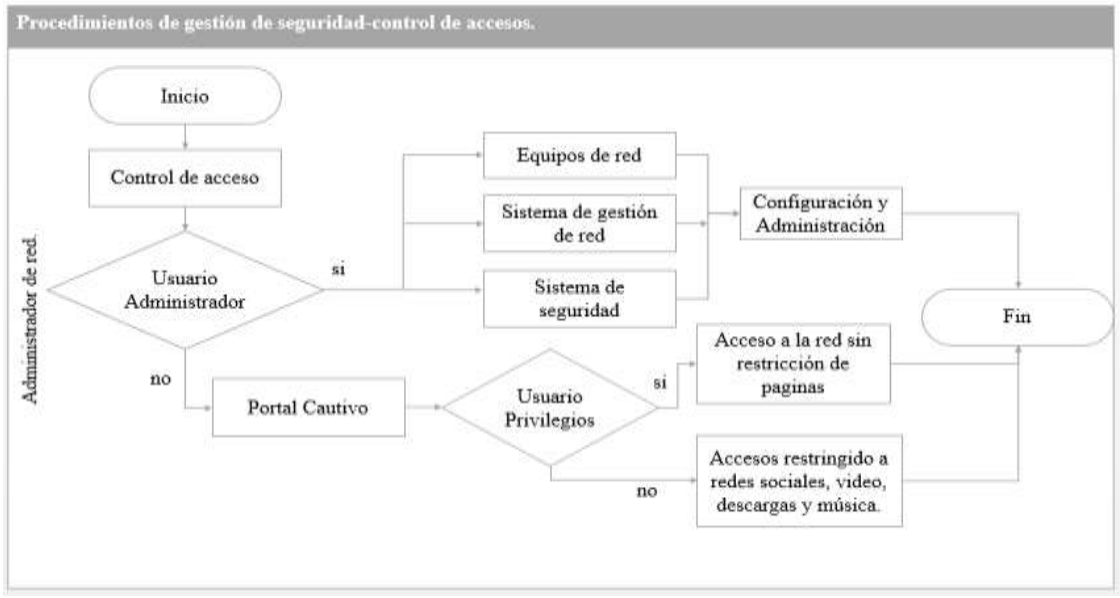
N°	Actividad	Descripción	Responsable
1	Control de accesos	**5. Gestión de usuarios de la red:** **a. Proceso de solicitud:** Al contratar un nuevo funcionario a la municipalidad la dirección de talento humano debe dirigir una solicitud a la dirección de TIC pidiendo que se le registre y asigne un usuario y contraseña para tener los servicios de red brindados a través de la red local. ***b. Administrador.*** Para el manejo y control de acceso de usuarios a los servicios de la red el administrador gestiona usuarios y grupos de usuarios a través de Zentyal mediante Open LDAP. 1. El usuario se crea en base al primer nombre y primer apellido. 2. Y la contraseña aplicada se basa en la combinación de números y letras y símbolos. Creación de grupos y usuarios: – Office. – Usuarios y Computadores. – Gestionar – Cree los grupos de acuerdo a las direcciones del municipio. – Cree usuarios para cada dirección. – Asigne el usuario y contraseña.	Administrador de red y usuarios.

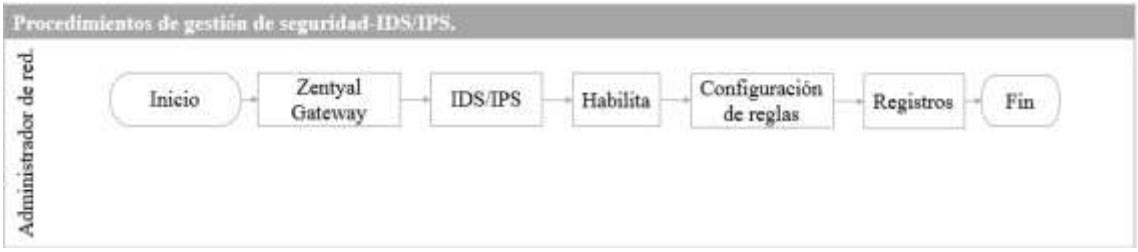
N°	Actividad	Descripción	Responsable
1	Control de accesos	Para que estos ingresen haciendo uso del usuario y contraseña asignada por el administrador se debe activar el portal cautivo, estableciendo a la interfaz de la LAN como interfaz cautiva. – Gateway. – Portal Cautivo. – Habilite la interfaz de la LAN. El administrador puede verificar que usuarios están haciendo uso de la red en: – portal cautivo, – usuarios actuales. ***c. Usuarios.*** Los usuarios deberán abrir su navegador registrar su usuario y contraseña para acceder al internet y servicios brindados por la dirección de TIC a través de la red local. **6. Internet y servicios de red local.** a. ***Usuarios limitados.*** Se restringe el acceso a páginas web, como redes sociales, descargas, videos, música. ***b. Usuarios privilegiados.*** Son directores y jefes, los mismos que pueden acceder libremente a páginas de redes sociales, videos, etc. Los usuarios que requieran ser usuarios privilegiados y no sean directores ni jefes deberán emitir un oficio al departamento de TIC, justificando el uso que hacen del internet, y la autorización de su jefe inmediato.	Administrador de red y usuarios.

N°	Actividad	Descripción	Responsable
1	Control de accesos	Para que los usuarios privilegiados tengan acceso libre el administrador debe registrarlos**.** 1. Ingresar a Zentyal. 2. Objetos. 3. Usuarios privilegiados. 4. Ingrese la dirección ip de usuario.	Administrador de red y usuarios.
2	Protección contra intrusos	Se habilita el IDS/IPS en Zentyal, aplicado a las dos interfaces, para que permita detección de intrusos, que fisgoneen en la red. – Gateway. – IDS/IPS. – Habilite las interfaces LAN y WAN. Para verificar la detección de actividades sospechosas vaya a: – Mantenimiento – Consulta de registros – Seleccione IPS y puede ver los eventos que se haya detectado.	Administrador de red.
3	Manejo de Backups	***Zentyal.*** Vaya a: – Sistema – Importar/exportar configuración. – Obtenga su respaldo haciendo clic en copia de seguridad. – Descargue el respaldo y guárdelo en el servidor de archivos.	Administrador de red.

N°	Actividad	Descripción	Responsable
3	Manejo de Backups	***Zenoss*** Vaya a: – Advance. – Backup Y genere un respaldo.	Administrador de red.

Flujograma:





Capítulo V

5 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.

5.1 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 con pago de licencias que incluyen soporte, mantenimiento y capacitación. 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.

Para saber la inversión que se realizaría utilizando software licenciado se presenta una comparativa de costos, generalmente las licencias son anuales, y de acuerdo al número de usuarios que la empresa disponga, la siguiente tabla, estima valores para alrededor de 100 a 300 usuarios.

Tabla 26. *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.

5.2 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 27. *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

Un requerimiento importante es el procesador, en ambos casos, Xeon Dual Core para Zentyal y un procesador de cuatro núcleos para Zenoss, cabe recalcar que el procesador Xeon Dual Core trabaja en cuatro núcleos, así como los procesadores Core 2 Quad, i3, i5, e i7, los cuales son compatibles, de manera que podemos utilizar cualquiera de estos procesadores.

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 28. *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. Ver Anexo B.

Tabla 29. *Costo de equipos de hardware para servidores.*

Servidores	Zentyal	Zenoss
Características	Procesador: Intel Xeon. Memoria: 8GB Disco Duro:500GB Tarjetas de red: 2.	Procesador: Intel Core i5. Memoria: 8GB. Disco Duro: 1TB. Tarjeta de red: 1.
Costo para adquisición de hardware	$ 3377,70	$ 956,48
Costo total	$ 4.334,19 *(este valor puede ser destinado a otros fines del municipio.)*	

Fuente: Proforma TECNIT.

5.3 Beneficios obtenidos

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.

- **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.

- **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.

Capítulo VI

6 Conclusiones y Recomendaciones

6.1 Conclusiones

Para la administración y gestión de red local del municipio de Cayambe basado en el modelo funcional de gestión de red ISO/OSI, junto al protocolo SNMP y herramientas de software libre, se implementó un sistema de gestión de red, y un sistema de seguridad, que cubren las áreas de gestión del modelo, para mejorar la disponibilidad de la red.

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 gestión 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.

6.2 Recomendaciones

Para la realización del proyecto se toma como base el modelo funcional de gestión de red ISO/OSI, y el protocolo snmp; se recomienda mantener la administración y gestión de red local sobre estos principios, ya que estas brindan las pautas esenciales para gestionar la red.

Las políticas de gestión se establecieron de acuerdo a las necesidades y requerimientos obtenidos en el análisis de la situación actual, no son de uso obligatorio, pero para administrar la red de forma organizada se recomienda seguirlas, el administrador puede actualizarlas de acuerdo a los cambios que puedan producirse en la infraestructura de la red local.

Se recomienda la implementación de la segmentación de la red, con equipos que tengan la función apropiada para formar una red jerarquizada, que permita mejorar la administración de la red, seguridad y escalabilidad. Los equipos que interconectan la red local pueden ser usados como switchs de acceso.

Adecuar la infraestructura de la red, para el incremento de puntos de red para los usuarios, ejecutando un proyecto de restructuración tomando en cuenta la escalabilidad y el crecimiento de la red a futuro.

Todo equipo que requiera integrarse a la red local debe tener la configuración básica que le permita beneficiarse de los servicios que esta brinda, y para integrarlos a sistema de gestión verificar si soporta el protocolo snmp, de lo contrario el administrador no podrá monitorear el equipo.

Zenoss cuenta con varias plantillas que permiten el monitoreo de los recursos de un dispositivo gestionado, se recomienda investigar plantillas o buscar las OIDs que permitan obtener información de CPU y memoria para Windows, ya que la plantilla que integra Zenoss no extrae esta información.

Revisar las nuevas versiones que se publiquen de las herramientas de gestión de software libre usadas para este proyecto, analizando las nuevas funcionalidades que presente e investigar si estas pueden aportar a mejorar la administración y gestión de la red local.

Es importante que el elemento humano aplique su experiencia para la administración y gestión de la red; se recomienda asignar la función de soporte técnico a una o dos personas que puedan cumplir únicamente estas funciones, para mejorar el servicio al usuario, y llevar la documentación de fallos.

Se recomienda que el administrador lleve un inventario que registre datos de los equipos interconectados a la red, para controlar el número de equipos que conforman la red, ya que el software de monitoreo no recopila información de características físicas de un equipo.

Zentyal puede obtener sus respaldos de todas las configuraciones, menos el directorio activo, por lo que se recomienda tener un listado con la información de los usuarios, nombre de usuario y contraseña asignada, para reingresarlos en caso de que suceda un inconveniente en el que se pierda esta información.

Los usuarios de la red serán los responsables del uso del usuario y contraseña que el administrador les asigne para que puedan acceder a los servicios de red local del municipio, por lo que se recomienda hacer buen uso de ella.

Al ser una institución pública la municipalidad debe fomentar el uso de software libre en los usuarios de la red, migrando de Windows a Linux, el administrador debe buscar una distribución adecuada y capacitar a los usuarios para que no tengan inconvenientes en su uso. A través de esto también se mitiga la contaminación de los terminales de usuarios por virus y pérdidas de información.

Respaldar todo tipo de información de los servidores en un servidor de archivos o en la nube, así como también información que maneja el área de avalúos y catastros como el área financiera.

BIBLIOGRAFÍA

Artica Soluciones Tecnologicas. (2006-2012). *The monitoring wiki PANDORA FMS Enetrprice*. Obtenido de http://wiki.pandorafms.com/index.php

Comunidad Autonoma de Castilla y Leon. (2006). Tecnicos de Soporte Informatico. En J. Desongles, E. A. Ponce, M. L. Garzon, M. d. Sampalo de la Torre, & I. Rocha, *Tenicos de Soporte Informatico* (págs. 286-287). Sevilla: MAD, S.L.

Comunidad Autonoma de Castilla y Leon. (2006). *Tecnicos de Soporte Informatico.* Sevilla: MAD, S.L.

Curry, J. (Enero de 2013). *Gestión de Eventos para Zenoss Core 4*. Obtenido de http://www.skills-1st.co.uk/papers/jane/zenoss4-events/zenoss_Core4_event_management_paper.pdf

Diego Borja. (2012). *PROYECTO DE CABLEADO ESTRUCTURADO DEL GAD MUNICIPAL DEL CANTON CAYAMBE.*

Gil, P., Pomares, J., & Candela, F. (2010). Redes y Trasmision de Datos. En P. Gil, J. Pomares, & F. Candela, *Redes y Trasmision de Datos.*

Hoy, I. (2012). *Como optimizar la memoria RAM*. Obtenido de http://www.informatica-hoy.com.ar/

IETF. (05 de 1990). *Simple Network Management Protocol (SNMP).* Obtenido de Simple Network Management Protocol (SNMP): https://www.ietf.org/rfc/rfc1157.txt

Kurose, J., & Ross, K. (s.f.). *Computer Network.* PEARSON.

Lázaro Laporta, J., & Miralles Aguiñiga, M. (2005). *Fundamentos de Telemática.* Universidad Politecnica de Valencia.

Magazine, T. (2008). *Optimización del rendimiento de la CPU de SQL Serve*. Obtenido de https://technet.microsoft.com/es-es/magazine/2007.10.sqlcpu.aspx

Martí, A. B. (1999). *Gestión de Red.* Barcelona: Universidad Politecnica de Cataluña.

Mauro, D., & Schmidt, K. (2005). *Essential SNMP*. Estados Unidos : O'Reilly Media, Inc.

McLeod, R. (2000). Sistemas de información gerencial. En R. McLeod, *Sistemas de información gerencial* (pág. 298). Mexico: Pearson Educación .

Millan Tejedor, R. J. (1999). Gestion de Red. *Windows NT/2000*.

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

Organización de Consumidores y Usuarios, O. (2015). *Guía de compra de ordenadores*. Obtenido de http://www.ocu.org/tecnologia/ordenador/informe/guia-de-compra-de-ordenadores-2014

Perpinan, A. (2004). *Administración de redes GNU/LINUX*. Santo Domingo: GAMMA.

QUASAR SOFTWARE . (2014). *QUASAR SOFTWARE* . Obtenido de http://www.quasarbi.com/ZABBIX.html

R, L. (s.f.). *IP Reference*. Obtenido de https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

Robles, F. J. (2010). *Planificacion y Administacion de Redes.* Madrid-España: RA-MA.

Romero, M. d. (s.f.). *Sistemas Avanzados de Comunicaciones - Gestion de Redes.* Obtenido de Sistemas Avanzados de Comunicaciones - Gestion de Redes: http://www.dte.us.es/personal/mcromero/docs/sac/sac-gestionderedes.pdf

Saydam, T. (1996). From Networks and Network Management Into Service and Service Management. *Journal of Network and Systems Management*.

Stacey, D. C. (2001). *Gestion de red.* Obtenido de ftp://ftp.puce.edu.ec/Facultades/Ingenieria/Sistemas/Network%20news/Gestion%20de%20Redes/GESTION%20DE%20RED.ppt

Stallings, W. (2004). *Comunicaciones y Redes de Computadoras.* Madrid: PEARSOON EDUCACIÓN.

Stallings, W. (2004). *Fundamentos de seguridad en redes, Aplicaciones y estandares.* Madrid: PEARSON.

Union, I. T. (1992). *International Telecomunication Union.* Obtenido de X.700 : Management framework for Open Systems Interconnection (OSI) for CCITT applications: http://www.itu.int/rec/T-REC-X.700-199209-I/en

Untiveros, S. (JULIO de 2004). *METODOLOGIAS PARA ADMINISTRAR REDES.* Obtenido de http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

ZABBIX. (2001-2015). *ZABBIX*. Obtenido de La Solución de Monitoreo de clase empresarial para Todos.: http://www.zabbix.com/features.php

Zenoss Community. (2005-2015). *Zenoss Documentation*. Obtenido de http://www.zenoss.com/sites/default/files/documentation/Zenoss_Core_Administration_02-022014-4.2-v08.pdf

Zenoss Community. (s.f.). *Zenoss Core*. Obtenido de http://es.wikipedia.org/wiki/Zenoss

Zenoss Own IT. (2005-2015). *¿Por que Zenoss?* Obtenido de http://www.zenoss.com/solution/why-zenoss

Zentyal Community. (s.f.). *Documentacion oficial de Zentyal.* Obtenido de Zentyal Wiki: https://wiki.zentyal.org/wiki/Es/3.2/Zentyal_3.2_Documentacion_Oficial

ANEXOS

ANEXOS A

ELECCIÓN DE HERRAMIENTAS DE SOFTWARE LIBRE

Elección de herramientas de software libre para la administración y gestión de la LAN del GADIPMC

La red de área local del GADIPMC, requiere herramientas de monitoreo, que permitan obtener información de la red, auto descubrimiento de la red y su topología, que ayude a detectar fallos, maneje eventos, notificación por correo electrónico, visualización de gráficas, obtención de reportes, que permita el monitoreo de uso de recursos de los dispositivos gestionados.

Análisis de herramientas de software libre

Para elegir la herramienta más adecuada se revisarán las características, ventajas y desventajas, de los siguientes software; Zabbix, Nagios, Zenoss, Pandora FMS y Open NMS, que son herramientas de software libre más conocidas en monitoreo de la red.

- ***Zabbix***

Fig-SM 1. Logo de Zabbix.

Es el último software a nivel empresarial diseñado para monitorizar disponibilidad y rendimiento de los componentes de una infraestructura de red. Este software es totalmente de código libre bajo licencia GPL v2, y no tiene ningún costo. Se lanza en el 2001. A través de su interfaz gráfica se puede monitorear, servidores, aplicaciones web, bases de datos, y equipos de red, en varios plataformas, a través de su propio agente Zabbix, o puede aplicar

el protocolo SNMP, JMX, IPMI, para la recopilación de información de los dispositivos que desea gestionar, además cuenta con plantillas prediseñadas, que facilitan el manejo del software, permite configurar alarmas y notificar eventos mediante correo electrónico, jabber, y SMS. Utiliza una base de datos basada en Oracle, MySQL, Postgres, o SQLite. Se puede configurar usuarios para la administración de la red mediante Zabbix, con diferentes permisos.

(ZABBIX, 2001-2015) (QUASAR SOFTWARE , 2014)

Tabla-SM 1.*Ventajas y desventajas de Zabbix.*

Ventajas	Desventajas
Fácil instalación. Agente propio. Plantillas prediseñadas	Todas las configuraciones hay que hacerlas de forma manual. Resulta difícil recordad todas las configuraciones que se realizan debido a la su interfaz gráfica tiene muchas características, lo cual puede resultar un poco complejo. No auto descubre la red, si se quiere tener una topología hay que dibujarla en el software.

Fuente: http://www.quasarbi.com/ZABBIX.html

- ***Nagios***

Nagios es un potente sistema de monitoreo que permite a las organizaciones identificar y resolver los problemas de infraestructura de TI antes de que afecten los procesos críticos de negocio.

Fig-SM 2. Logo Nagios.

Nagios permite monitorear los componentes de una infraestructura de red, como servidores, aplicaciones, servicios (SMTP, POP3, HTTP, HTTPS, NTP, ICMP, SNMP, FTP, DNS, etc.), sistemas operativos, protosol de red, y métricas de los sistemas, recursos de hardware (Carga de procesador, uso de disco, procesos del sistema), puede entregar mediante un mensaje de correo electrónico, o un SMS, alertas al personal de TIC, proporciona registros históricos de los cortes, notificaciones, y la respuesta a las alertas para su posteríos análisis. La comunidad mantiene un constante desarrollo de plugins, que el administrador puede añadir para su funcionamiento.

Tabla-SM 2. *Ventajas y desventajas de Nagios.*

Ventajas	Desventajas
De código abierto, libre la versión de Core. Variedad de plugins y se mantienen en constante desarrollo. Escalable y robusto, pues soporta decenas de miles de nodos, y tiene la capacidad de especificar una jerarquía topológica y eliminar notificaciones innecesarias.	Se comercializa, lo cual limita funciones, y para tener soporte hay que pagar. Número de opciones y parámetros tiende a ser frustrante al principio Configuraciones basadas en plantillas o plugins, lo cual en el mantenimiento de múltiples nodos lo hace pesado.

Fuente: https://ws.edu.isoc.org/data/2004/12233513244826d2f8d0eb/Ejercicio_Nagios.pdf

- ***Zenoss***

Es una aplicación de código abierto para la gestión de la red y servidores, basada en aplicaciones Zope, liberado bajo Licencia Publica General de GNU (GPL) v2.

Fig-SM 3. Logo de Zenoss.

Inicia su desarrollo en el 2002 y en el 2005 se funda Zenoss.Inc promoviendo su versión empresarial, patrocina el desarrollo de Zenoss Core, y vende su versión empresarial Zenoss Service Dynamics basada en la versión de Core ¿Que monitorea Zenoss?, infraestructuras convergentes, bases de datos y aplicaciones redes, sistemas operativos, sistemas de almacenamiento, virtualización y Cloud. Para el monitoreo aplica ZenPack, que son plugins a través de los cuales controla todo, el administrador puede adaptarlo de acuerdo a lo que requiere monitorear. No utiliza agentes adicionales, realiza el monitoreo de los dispositivos de red a mediante SNMP, WMI y SSH. (Zenoss Own IT, 2005-2015)

La versión de Core tiene las siguientes funcionalidades:

- Monitoreo de servicios de red (HTTP,POP3,NNTP,SNMP,FTP)
- Monitoreo de recursos de máquinas anfitrionas (Microprocesador, utilización de disco) en la mayoría de los sistemas operativos de red.
- Monitoreo de rendimiento de dispositivos a través de series temporales de datos.
- Herramientas de gestión de eventos para anotar las alertas de un sistema.

- Detecta automáticamente recursos en una red y cambios en su configuración.
- Sistema de alertas que provee notificaciones basadas en un conjunto de reglas y calendarios.
- Integra funciones de Nagios (plugins de Nagios) y Cacti (graficas).

(Zenoss Community, s.f.)

Tabla-SM 3.*Ventajas y desventajas de Zenoss.*

Ventajas	Desventajas
Interfaz amigable al usuario. Se puede aplicar la instalación de forma automática o pasó a paso. Pude descubrir en parte los parámetros de los sistemas de forma automática. Funciona bien con el protocolo SNMP. Integra nmap, con el que se pude auto descubrir la red.	El software termina comercializándose. Algunos zenpack son de pago y otros aportados por la comunidad. Ocupan más recursos que los anteriores softwares. Al principio puede resultar complejo entender cómo funciona Zenoss.

Fuente: http://www.zenoss.com/

- ***Pandora FMS***

Fig-SM 4. Logo Pandora FMS.

Es una de las herramientas más flexibles y completas del mercado, basado en software libre con licencia GPL v2, inició en el 2004, permite el monitoreo de redes, servidores, aplicaciones, entornos virtuales, cualquier servicio TCP/IP, monitoreo de recursos de equipos como routers, switch, balanceadores de carga, impresoras, a cada dispositivo gestionado se aplican módulos, que especifican el valor de la información que quiere monitorear, este puede ser uso de CPU, memoria, disco duro, interfaces de red, etc., mediante el protocolo SNMP, y WMI.

Esta herramienta ayuda a detectar problemas antes de que se conviertan en un mal mayor, con la gestión de alertas, estableciendo umbrales, notificación por correo electrónico y SMS. Tiene la facilidad de auto descubrir la topología de red.

Pandora FMS Open Source ha sobrepasado las 600.000 descargas en todo el mundo y constituye una solución completamente eficaz para pequeñas empresas o grupos de usuarios que deseen monitorizar sus máquinas de manera independiente, también ofrece su versión comercial, para entornos empresariales, que tiene funcionalidades más específicas. (Artica Soluciones Tecnologicas, 2006-2012)

Tabla-SM 4.*Ventajas y desventajas de Pandora FMS.*

Ventajas	Desventajas
Escalabilidad. Pandora FMS da la posibilidad de descubrir módulos SNMP para aplicarse a los equipos a gestionar. Para el manejo del software integra ayuda en ítems donde el administrador tiene dudas de configuración.	Ocupa considerablemente recursos de hardware. Descubre información con el wizard SNMP, muestra la MIB descubiertas, pero la información no se muestra, en concreto como en Zenoss. Las gráficas muy sencillas.

Fuente: pandorafms.com/downloads/Pandora_Tecnica_ES_Abril2012.pdf

- ***Open NMS***

Fig-SM 5.*Logo Open NMS.*

Es una plataforma de aplicaciones de gestión de red, con una larga trayectoria y largo historial de proporcionar soluciones para empresas y operadoras, permite automatización de descubrimiento de red, y sus servicios, proporciona funcionalidades como gestión de eventos, y notificación por correo electrónico o SMS.

Ofrece garantía de servicio, ya que cumple con los Acuerdos de niveles de servicio (SLA). Fue desarrollado desde un inicio, para ser una solución empresarial capaz de monitorear un número ilimitado de dispositivos. Tiene soporte SNMP, WMI,JMX, permite la configuración de umbrales no solo en estados alto o bajo, sino de un valor relativo, donde puede configurar un evento y notificación. Los datos de rendimiento pueden ser graficados, y la generación de informes puede ser útil para la identificación de áreas problemáticas dentro de la red.

Tabla-SM 5. *Ventajas y desventajas de Open NMS.*

Ventajas	Desventajas
Tiene mucha trayectoria. Cumple los acuerdos de niveles de servicio. Aplica una plataforma basada en el modelo FCAPS.	Su instalación es aparentemente sencilla, pero para un usuario no familiarizado con la base de datos postgres le resulta difícil el acople de este, con java. El no lograr el acople no permite arrancar el servicio de openNMS.

Fuente: http://www.opennms.org/

Elección del software de monitoreo

Luego de haber revisado las características de las diferentes herramientas de monitoreo, sus ventajas y desventajas, de Zabbix, Nagios, Zenoss, Pandora, y Open NMS, se determina como mejor alternativa el software de monitoreo de red Zenoss en su versión Core.

Tabla-SM 6.Calificación del cumplimiento de características de los software.

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
	Graficas de rendimiento	✓	✓	✓	✓	✓
	Reportes	✓	✓	✓	✓	✓
	Base de datos	Oracle MySQL, PostgresSQ.	Programado en C MySQL PostgresSQL.	MySQL PostgreSQL.	MySQL	PostgreSQL
	Manejo de alarmas y notificación de eventos por correo electrónico	✓	✓	✓	✓	✓
Seguridad		✓	✓	✓	✓	✓

Nota: Se revisó el cumplimiento de las características de cada software en sus páginas oficiales.

Este software se aplica para la recopilación de la información del estado actual de la red y para el desarrollo del resto del proyecto.

ANEXO B

PROFORMA

PROFORMA DE SERVIDORES

TECNIT

Teresa de Cepada N35-12 y Av. República
Telf. 332 0 332 / 332 0 177 / 332 0 178
RUC: 1792179742001

PROPUESTA ECONOMICA

Cliente:	GADIP MUNICIPIO DE CAYAMBE	**Fecha:**	Quito, 2015 / 05/ 25
Dirección:	TERÁN SO-54 Y SUCRE	**No. Cotización**	**763**
Teléfono:	2360052	**EJECUTIVO**	VA
Ciudad:	Cayambe		
RUC:	1760003680001		
Atención:	ING. FABIAN BAUTISTA		

ITEM	CANT	MARCA	MODELO	DESCRIPCION	P. UNIT. USD	P. TOTAL USD	OBSERVACIONES
Opcion 1:							
1	1	Computador de escritorio DELL	Inspiron 3647	Procesador Intel Core i5-4460S, Quad Core , 6Mb Cache, 2,40 GHz; 8Gb RAM DDR 3 1600MHz; Disco duro Sata 1TB 7200RPM; Unidad de 16x con Bandeja de carga automática CD/DVD, Gigabit Ethernet, tarjeta de video, gráficos integrados HD; Controladora de audio Integrated 5.1; 4 USB 2.0, 2 USB 3.0, HDMI, VGA, Sistema operativo MS Windows 7 Home Premium 64 Bit.	$ 854,00	$ 854,00	NUEVO
2	1	Servidor	HP DL-180 GEN9	Procesador Intel® Xeon® E5-2609 v3 (6 núcleos, 1,9 GHz, 15 MB, 85 W), 8Gb RAM, DDR 4, 2 adaptadores Ethernet de 1 Gb, unidades de disco duro incluidas 8 (LFF).	$ 2718,00	$ 2718,00	NUEVO
3	1	Disco Duro	HP	DISCO DURO HP 500GB 6G SATA 7.2K LFF 3.5in.	$ 297,81	$ 297,81	NUEVO

SUBTOTAL	$ 3.869,81
12% (IVA)	$ 464,38
TOTAL	$ 4.334,19

SON: OCHO MIL NOVECIENTOS CON 64/100

CONDICIONES GENERALES

VALIDEZ DE LA OFERTA:	15 DIAS O HASTA AGOTAR STOCK
FORMA DE PAGO:	100% CONTRA ENTREGA
TIEMPO DE ENTREGA:	INMEDITA PREVIA CONFIRMACION DE STOCK
GARANTÍA:	DE FABRICA
IMPUESTO A APLICAR	APLICA IVA 12%

IMPORTANTE

Equipos entregados localmente
Disponemos de servicios de instalación, mantenimiento y soporte técnico a pedido del cliente Precio exclusivo y confidencial para el cliente
Los precios que se presentan responden únicamente a los precios que aparecen en la cotización Este número de oferta reemplaza a cualquier oferta emitida anteriormente

GADIP MUNICIPIO DE CAYAMBE
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TECNIT	**Aprobado por:**	**Cliente**	**Firma Cliente**
Vinicio Arcos		GADIP MUNICIPIO DE CAYAMBE	

Fecha:

ANEXO C

MANUAL DE ZENTYAL

UNIVERSIDAD TÉCNICA DEL NORTE

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL MUNICIPIO DE CAYAMBE

MANUAL

ZENTYAL 3.2

Autor: Cyntia Inuca

Mail: mab_c6@yahoo.es

INSTALACION DE ZENTYAL 3.2

1. Para la instalación de Zentyal buscamos en el portal web de Zentyal el CD de instalación, http://download.zentyal.com/, elegimos va versión requerida y descargamos.

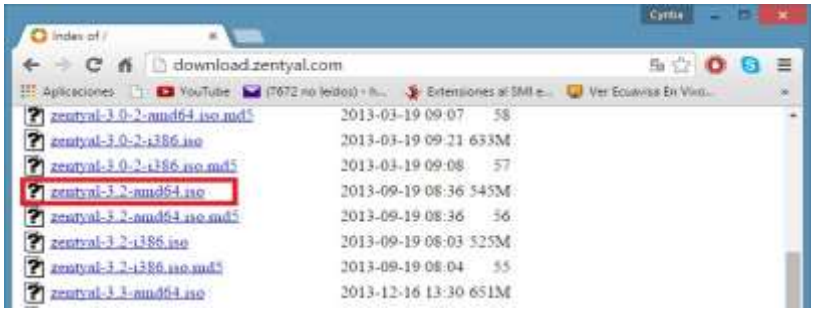


Fig-Zentyal 1. Download Zentyal.

2. Una vez descargado el CD de instalación, se procede a la instalación del sistema operativo Zentyal 3.5 64 bits.

Fig-Zentyal 2. Instalación Zentyal 3.2.

3. Seleccione la ubicación del país, Ecuador.

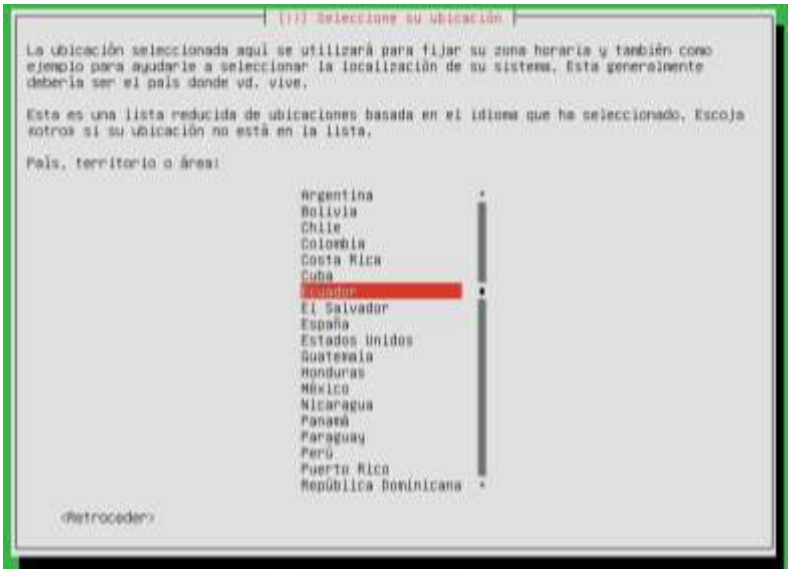


Fig-Zentyal 3.Ubicación Ecuador.

4. Configure el teclado.

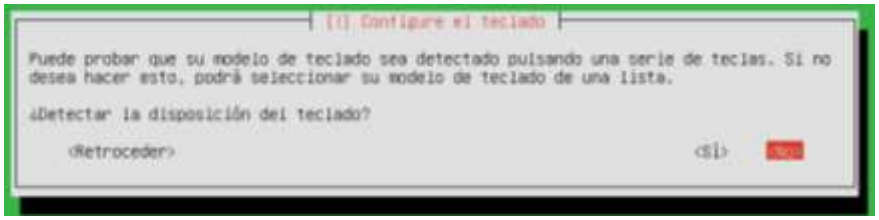


Fig-Zentyal 4. Configuración de teclado.

5. Elija el idioma para el teclado, Español Latinoamericano.

6. Elija la interfaz de red primaria.

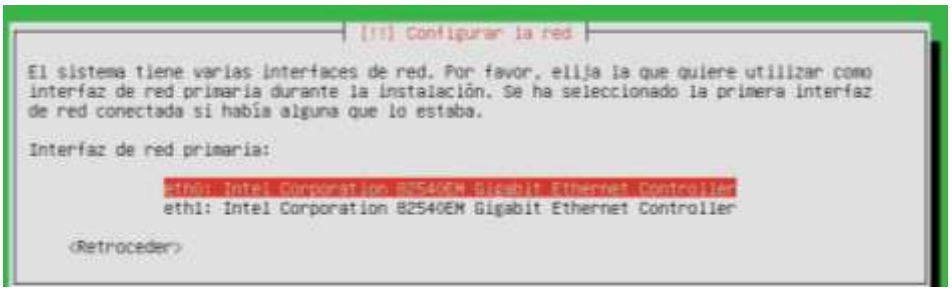


Fig-Zentyal 5. Interfaz de red primaria.

7. Configure el nombre de la máquina; el usuario ingresará el nombre como le convenga.

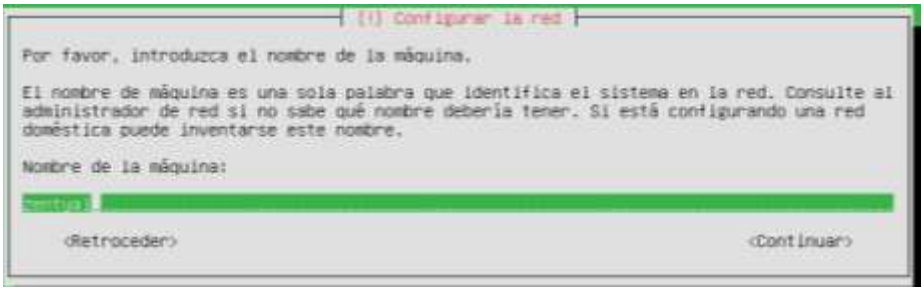


Fig-Zentyal 6. Nombre de máquina.

8. Configure el usuario que administrará este servidor, en este caso es ***sistemas***.

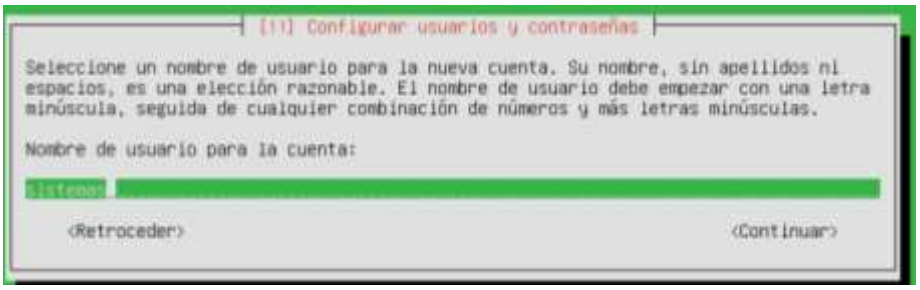


Fig-Zentyal 7. Configuración de usuario.

9. Introduzca una contraseña segura para el usuario.

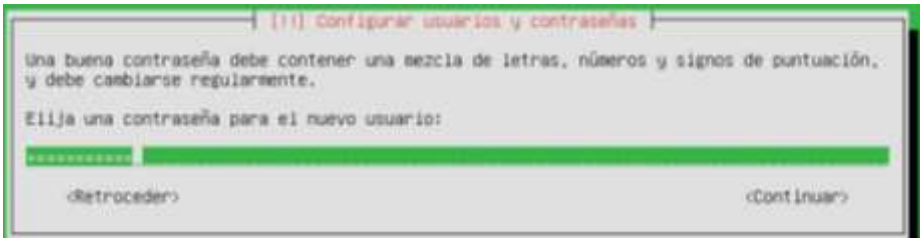


Fig-Zentyal 8. Configuración de contraseña.

10. Configure el reloj y confirme si la zona horaria es la correcta.

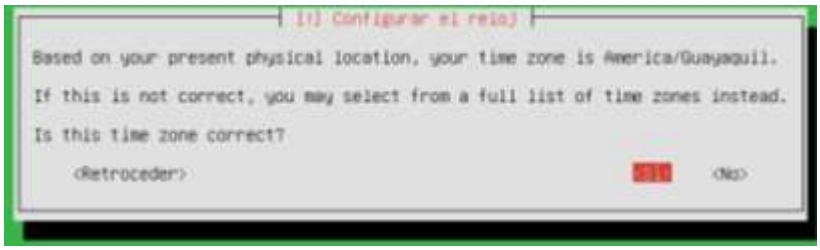


Fig-Zentyal 9. Configuración del reloj.

11. Una vez terminada las configuraciones espere hasta que termine la instalación del sistema operativo.

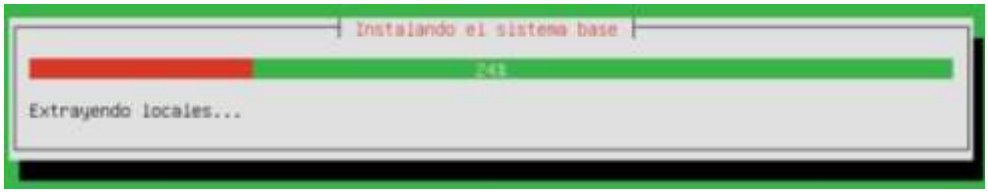


Fig-Zentyal 10. Instalando el sistema.

12. El sistema se reinicia automáticamente, presentando su interfaz gráfica donde debe ingresar el usuario y contraseñas correspondientes.

Fig-Zentyal 11. Acceso a Zentyal.

13. Al ingresar seleccione los paquetes que requiere instalar de acuerdo a los roles que vaya a desempeñar el servidor, e instale.

Fig-Zentyal 12. Paquetes de Zentyal.

14. Ahora elija la interfaz que corresponderá a la WAN (externa), ya la interfaz que corresponda a la LAN (interna).

Fig-Zentyal 13. Configuración de interfaces de red.

15. Finalizando la configuración anterior vamos al DASHBOARD, y podemos ver una interfaz amigable donde se muestran los paquetes instalados, listo para configurarlos, para que realiza la función que disponga el administrador.

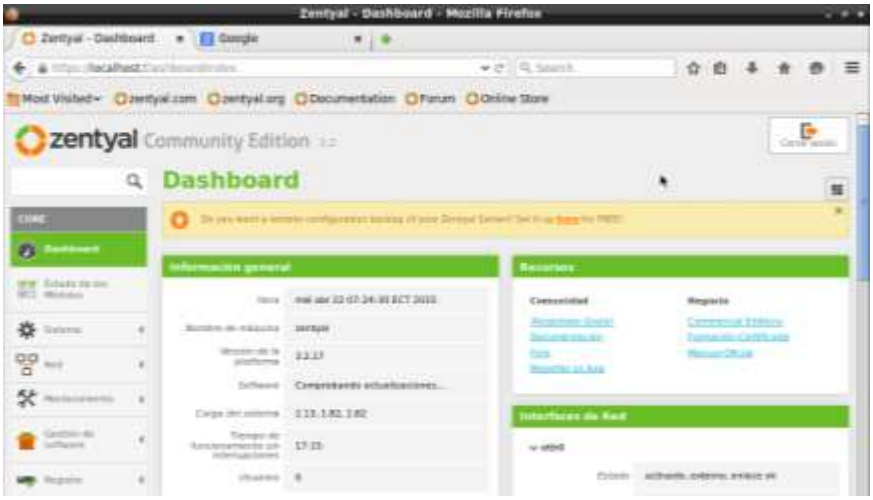


Fig-Zentyal 14. Dashboard Zentyal.

CONFIGURACIÓN DE SERVICIOS DE ZENTYAL

1. Antes de iniciar la configuración de los servicios de Zentyal, previamente debemos habilitar los paquetes necesarios.

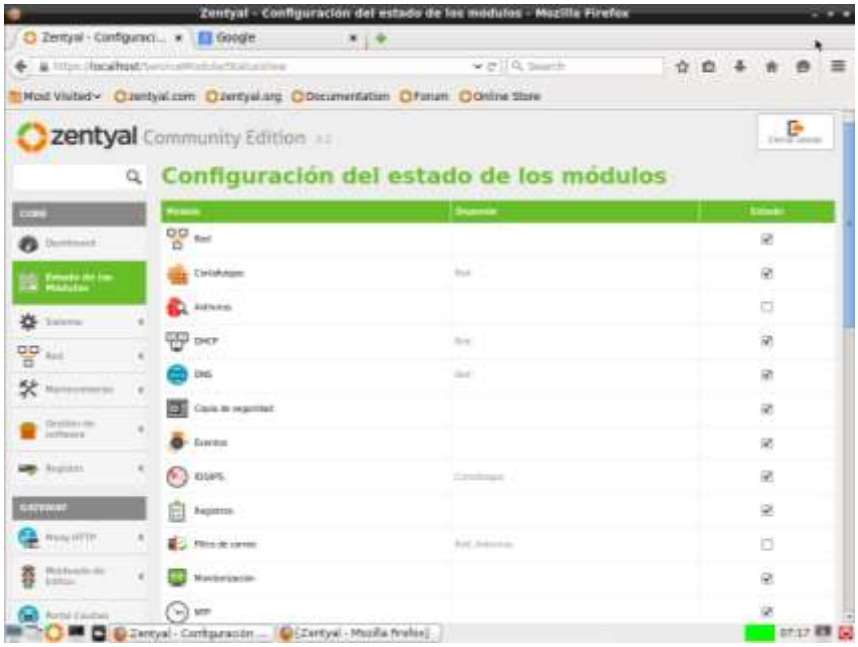


Fig-Zentyal 15. Estado de módulos.

2. Configuración de interfaces de red para la WAN y LAN.

   - Ubíquese en la pestaña ***Red***.

     a. *Interfaces.*

        - ***Eth0:*** asígnese a la WAN.
        - ***Eth1:*** asígnese a la LAN.

Fig-Zentyal 16. Interfaz de red WAN.

Fig-Zentyal 17. Interfaz de red LAN.

CONFIGURACIÓN DE SERVICIO FIREWALL /PROXY

1. PROXY HTTP

Este servicio ayudará a filtrar y denegar páginas web por http, a través de la URL o nombre de dominio.

1.1 Ubíquese en la pestaña ***Proxy HTTP.***

- ***Configuración General.***
  - Habilite, proxy trasparente.
  - Habilite, bloqueo de anuncios.

Fig-Zentyal 18. Configuración general de Proxy HTTP.

- ***Perfiles de filtrado.***
  - Haga clic en Añadir nuevo.

Fig-Zentyal 19. Creación de un nuevo perfil.

- Proceda a la configuración del perfil creado. 
- En la pestaña configuración, elija el nivel de umbral para su perfil.

Fig-Zentyal 20. Establecimiento de umbral.

- Haga clic en la pestaña Reglas de filtrado, e ingrese a las páginas web que desea denegar.

Fig-Zentyal 21. Configuración de reglas de dominio y URL.

- ***Listas por categoría.***
  - Haga clic en la pestaña listas por categoría y suba un archivo que contenga un listado de varios dominios para luego aplicar una regla.

Fig-Zentyal 22. Archivo contenedor de dominios.

  - Diríjase a perfiles de filtrado y aplique la regla bloquear a aquellos contenidos obscenos, violentos, descargas, tv, música, dominios que consumen muchos recursos de red.
  - Luego aplique una regla de filtrado.

- ***Reglas de acceso***

Se modifica la regla que viene por defecto para aplicar una nueva regla con el perfil de filtrado que se creó anteriormente; ***restricciones***.

Fig-Zentyal 23. Regla por defecto.

- Haga clic en **Añadir nuevo**; para crear una nueva regla.
- En **origen**: seleccione ***cualquiera***, para aplicar las reglas a todos los usuarios de la red.
- En **decisión**: aplique el ***perfil de filtrado*** "restricciones".

Fig-Zentyal 24. Regla aplicando el perfil.

A través de esta regla todos los usuarios que pertenecen a la LAN del GADIPMC no tendrán acceso a las páginas web como Facebook. YouTube, Twitter, y contenidos filtrados de acuerdo a la categoría de dominios que se bloqueo.

- Verifique si la configuración Proxy HTTP es correcta, accediendo a las páginas web a las que se aplica la regla.

Fig-Zentyal 25. Acceso negado a YouTube.

Nota: La configuración de Proxy HTTP únicamente filtra páginas web por http, para negar definitivamente el acceso por https a Facebook, YouTube y Twitter, existen dos opciones de configuración a través de los servicios en Zentyal.

- ***DNS***
- ***Cortafuegos.***

2. CONFIGURE DNS

La configuración en el DNS nos ayudara a re direccionar la página solicitada por el usuario hacia una dirección IP cualquiera, haciendo imposible que se resuelva la página deseada.

2.1 Ubíquese en la pestaña del ***DNS*** de servicios de Gateway.

En Dominio, haga clic en Anadir nuevo, e ingrese el nombre de dominio.

Fig-Zentyal 26. Ingresando el dominio.

Una vez creado el dominio, haga clic en configurar ***direcciones ip del dominio,*** e ingrese la dirección ip cualquiera.

Figura 25. Creación de un nuevo dominio.

Fig-Zentyal 27. Configuración de ip para el dominio.

Verifique si la configuración es correcta.

Fig-Zentyal 28. Acceso denegado a Facebook por https.

Nota: Esta configuración es opcional, para la denegación definitiva de los dominios que se configuraron en el DNS. No permite opciones de acceso a ciertos usuarios, para resolver esto podemos configurar los cortafuegos.

3. CONFIGURE CORTAFUEGOS.

3.1 Ubíquese en la pestaña ***Red***.

1. Haga clic en ***Objetos***, cree varios objetos con los siguientes nombre:

- YouTube: ingrese las direcciones ip correspondientes a YouTube.
- Facebook: ingrese las direcciones ip de Facebook.
- Usuarios_privilegiados: ingrese direcciones ip de usuarios quienes solicitan acceso total al internet.

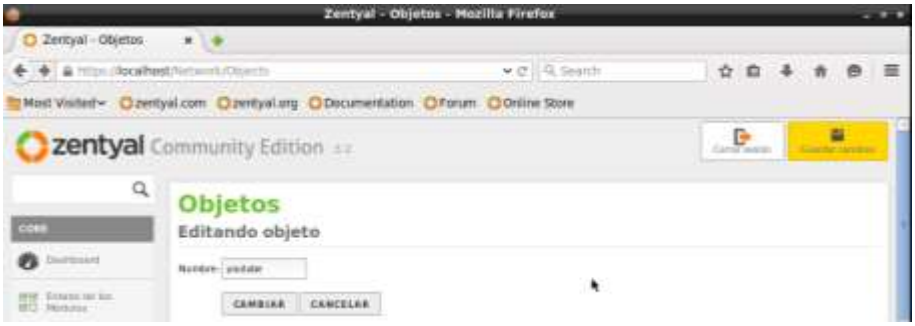


Fig-Zentyal 29. Creación de objeto nuevo YouTube.

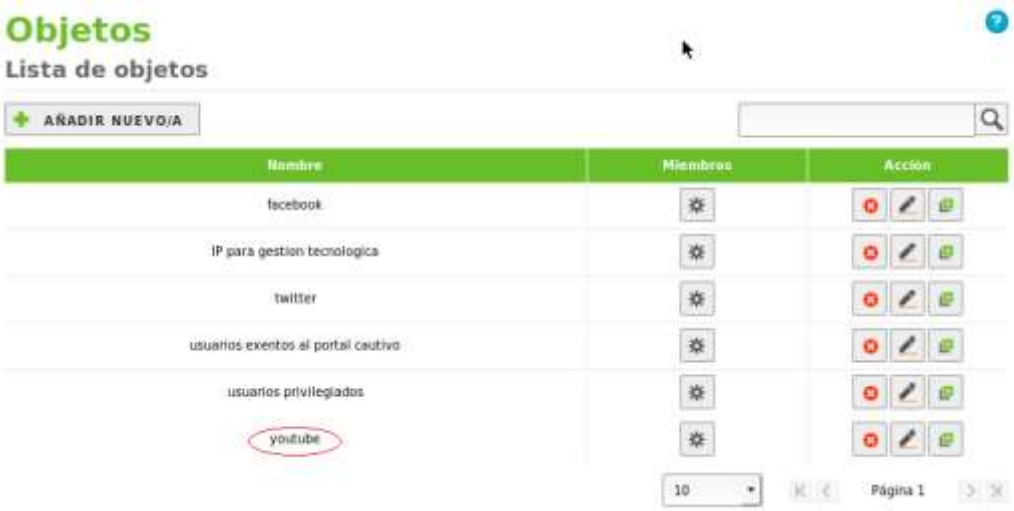


Fig-Zentyal 30. Objeto creado.

Fig-Zentyal 31. Configuración de miembros del objeto.

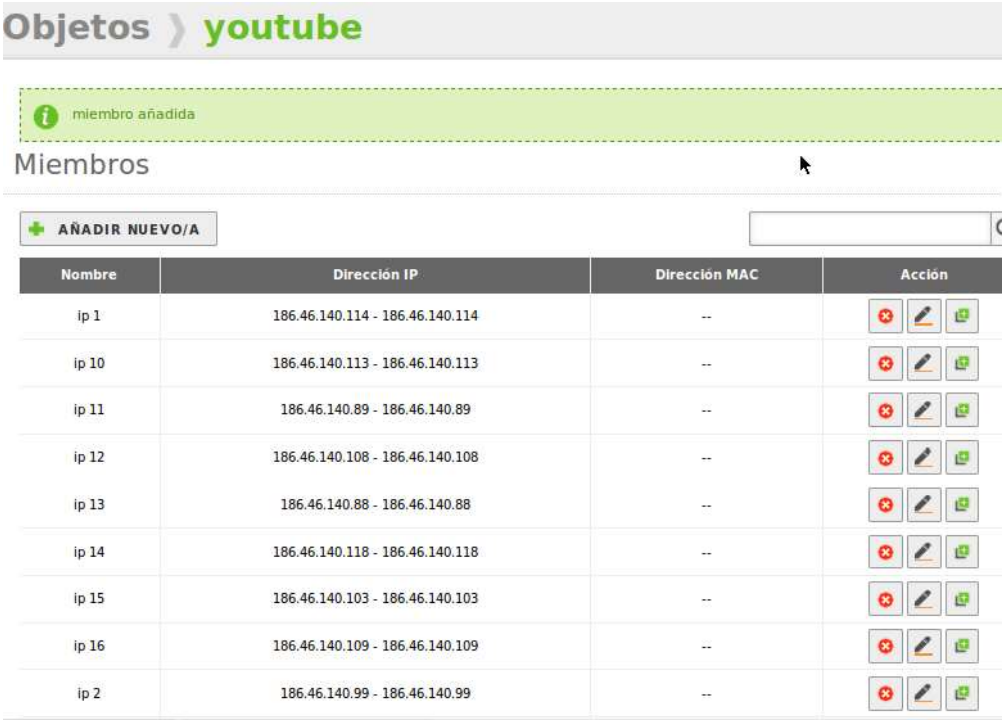


Fig-Zentyal 32. Miembros de objeto YouTube.

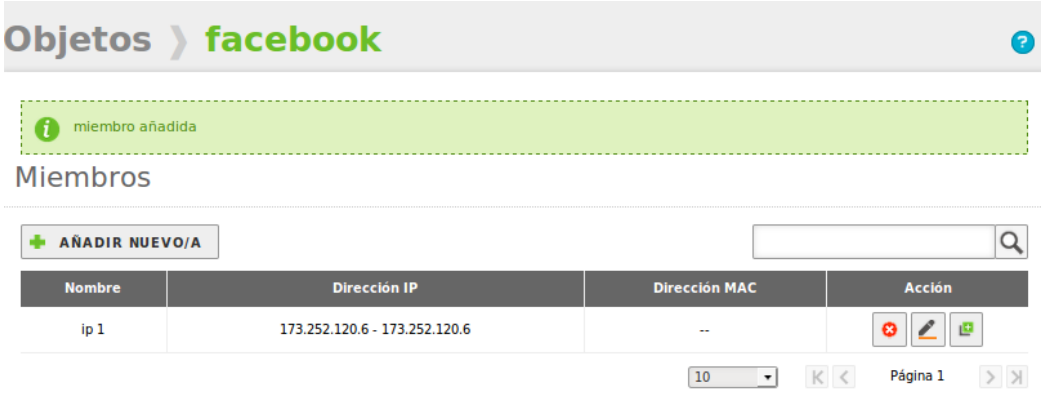


Fig-Zentyal 33. Configuración de miembro objeto Facebook.

Fig-Zentyal 34. Configuración de miembros objeto usuarios_ privilegiados.

Fig-Zentyal 35. Lista de objetos creados.

2. Finalizado la creación de objetos haga clic en ***servicios.***

   - Cree un nuevo servicio https; haga clic en Añadir nuevo.

Fig-Zentyal 36. Creación de nuevo servicio.

Fig-Zentyal 37. Configure servicio https.

1.2 En la pestaña ***cortafuegos,*** haga clic en ***Reglas de filtrado para las redes internas.***

Fig-Zentyal 38. Filtrado de paquetes.

- Por defecto aparece una regla que permite acceso a todo.

Fig-Zentyal 39. Regla por defecto.

- Haga clic en añadir nuevo y proceda a configurar.

  Deniegue acceso a cualquier usuario a Facebook por https.

Fig-Zentyal 40. Creación de regla para negar Facebook.

- Guarde los cambios y verifique si la configuración realizada es correcta.

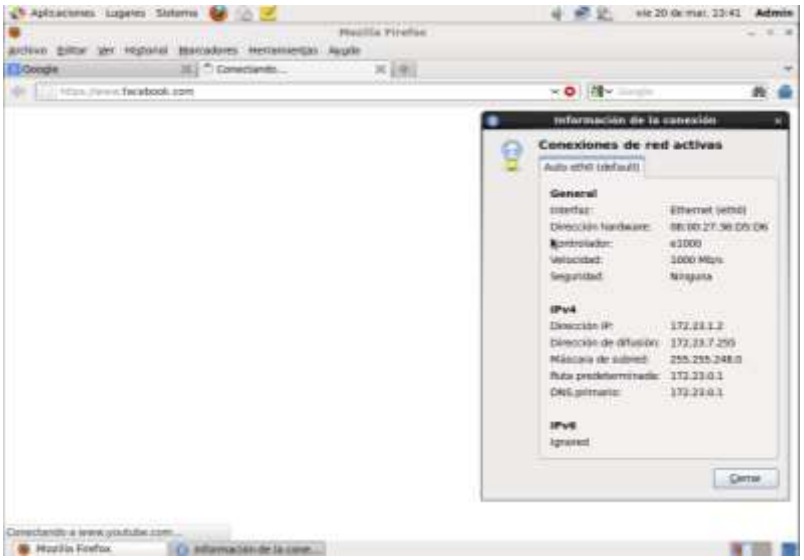


Fig-Zentyal 41. Acceso denegado a Facebook.

- Ahora para dar acceso a Facebook a cierto usuario se realiza la siguiente configuración.

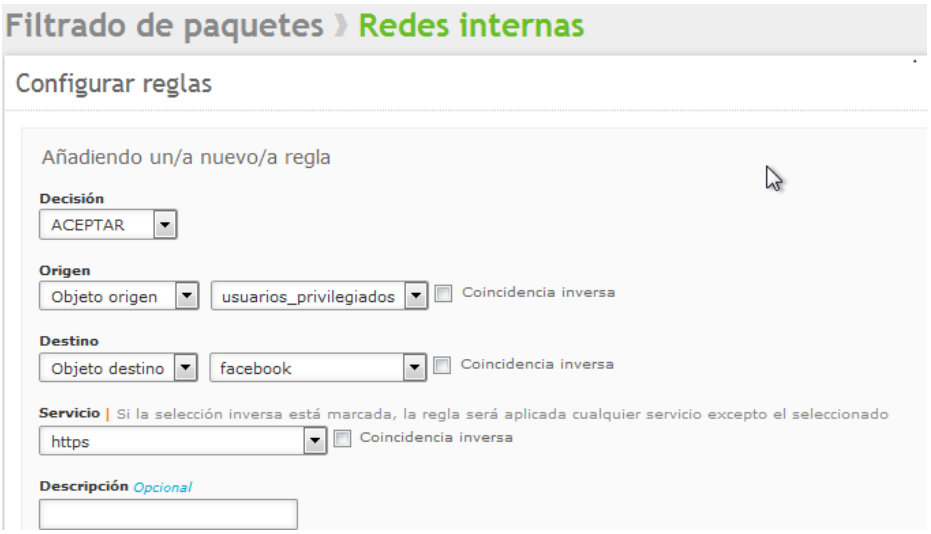


Fig-Zentyal 42. Creación de regla para usuarios privilegiados.

- Realice el mismo proceso para permitir acceso a YouTube a los usuarios privilegiados.
- Las reglas quedan de esta manera.

Fig-Zentyal 43. Reglas de filtrado de redes internas.

Nota: Si un usuario está en la lista de miembros del objeto usuarios_privilegiados tendrá acceso a Facebook, YouTube, twitter.

- Verificación de reglas configuradas.

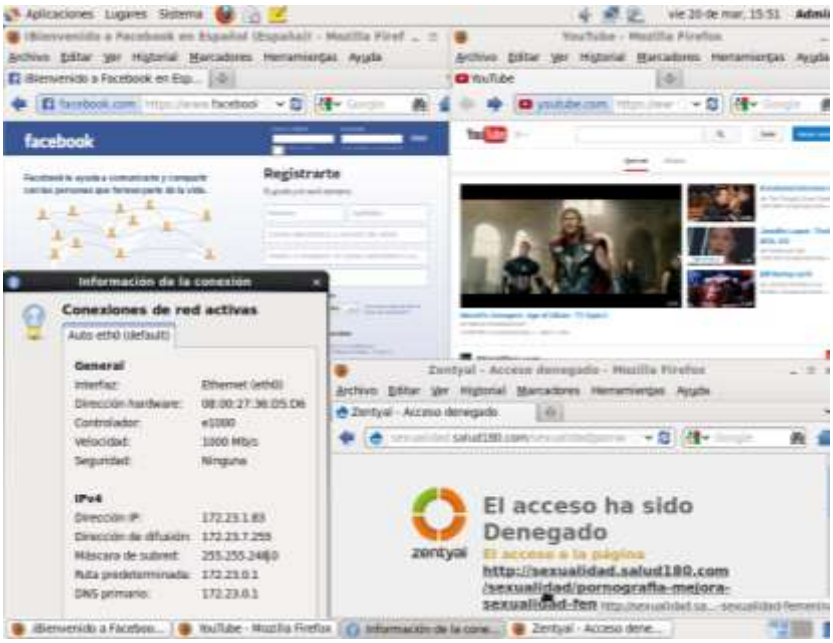


Fig-Zentyal 44. Verificación de reglas en usuario con privilegios.

- Pestaña ***Mantenimiento***.

  Ubíquese en ***Registros***, y haga clic en Proxy HTTP. Al hacer clic en informe completo, podrá ver las páginas web peticionadas por los usuarios de la LAN.

Fecha	Host	Usuario	Dirección URL	Dominio	Bytes	Mime/tipo	Evento
2015-03-20 16:06:26	172.23.4.2	-	http://static.ak.facebook.com/connect/xd...	facebook.com	23584	text/html	Denegado
2015-03-20 16:01:12	172.23.4.2	-	http://www.facebook.com/plugins/like_box...	facebook.com	24076	text/html	Denegado
2015-03-20 16:01:12	172.23.4.2	-	http://static.ak.facebook.com/connect/xd...	facebook.com	23525	text/html	Denegado
2015-03-20 16:00:46	172.23.4.2	-	http://static.ak.facebook.com/connect/xd...	facebook.com	23525	text/html	Denegado
2015-03-20 16:00:46	172.23.4.2	-	http://www.facebook.com/plugins/like_box...	facebook.com	24076	text/html	Denegado
2015-03-20 15:57:25	172.23.4.2	-	http://www.facebook.com/plugins/activity...	facebook.com	23614	text/html	Denegado
2015-03-20 15:54:44	172.23.4.2	-	http://www.youtube.com/	youtube.com	23364	text/html	Denegado
2015-03-20 15:54:27	172.23.4.2	-	http://www.youtube.com/favicon.ico	youtube.com	23338	text/html	Denegado
2015-03-20 15:54:27	172.23.4.2	-	http://www.youtube.com/favicon.ico	youtube.com	23338	text/html	Denegado
2015-03-20 15:54:27	172.23.4.2	-	http://www.youtube.com/	youtube.com	23305	text/html	Denegado

Fig-Zentyal 45.Páginas web negadas.

DIRECTORIO ACTIVO CON OPEN LDAP EN ZENTYAL

Para el control de usuarios de la LAN del GADIPMC se aplica el servicio de Directorio Activo de Zentyal que contiene el paquete OPEN LDAP.

Para la configuración de este servicio ubíquese en el área de **Office,** se puede ver la pestaña **Dominio, Usuarios y Equipos** que es lo que se requiere configurar.

1. CONFIGURACIÓN DE DOMINIO.

Todos los usuarios pertenecientes a la LAN va estar controlados bajo un dominio llamado ***gadipmc***.

Haga clic en Dominio, y registre el nombre del dominio ***gadipmc.***

Fig-Zentyal 46. Configuración de dominio.

2. Creación de grupos:

Haga clic en la pestaña **Usuario y Equipos**, y seleccione **Gestionar**.

Cree los grupos de acuerdo a las direcciones del GADIPMC.

Fig-Zentyal 47. Creación de Grupos.

Una vez que culmine la creación de grupos, para cada uno de ellos cree los usuarios correspondientes, e ingrese a información solicitada.

3. Creación de usuarios.

Para cada grupo cree los usuarios, ingresando la información correspondiente, como: nombre de, descripción, contraseña, y el grupo al que pertenece.

Fig-Zentyal 48. Creación de Usuarios.

CONFIGURACIÓN DE PORTAL CAUTIVO

Este servicio ayudara al mejor control de los usuarios de la LAN, permitiendo saber en tiempo real, los usuarios que están conectados al internet a través de la LAN del municipio.

Ya que anteriormente se crean los grupos y usuarios pertenecientes al dominio ***gadipmc***, en vez de ligarlos por equipos, se aplicara el portal cautivo donde el usuario tendrá obligatoriamente que acceder por su nombre de usuario y contraseña establecida por el administrador.

1. Ubíquese en el área de **GATEWAY**, y haga clic en **Portal Cautivo**.
2. Configure para que todos los usuarios inicien sesión por el portal cautivo.

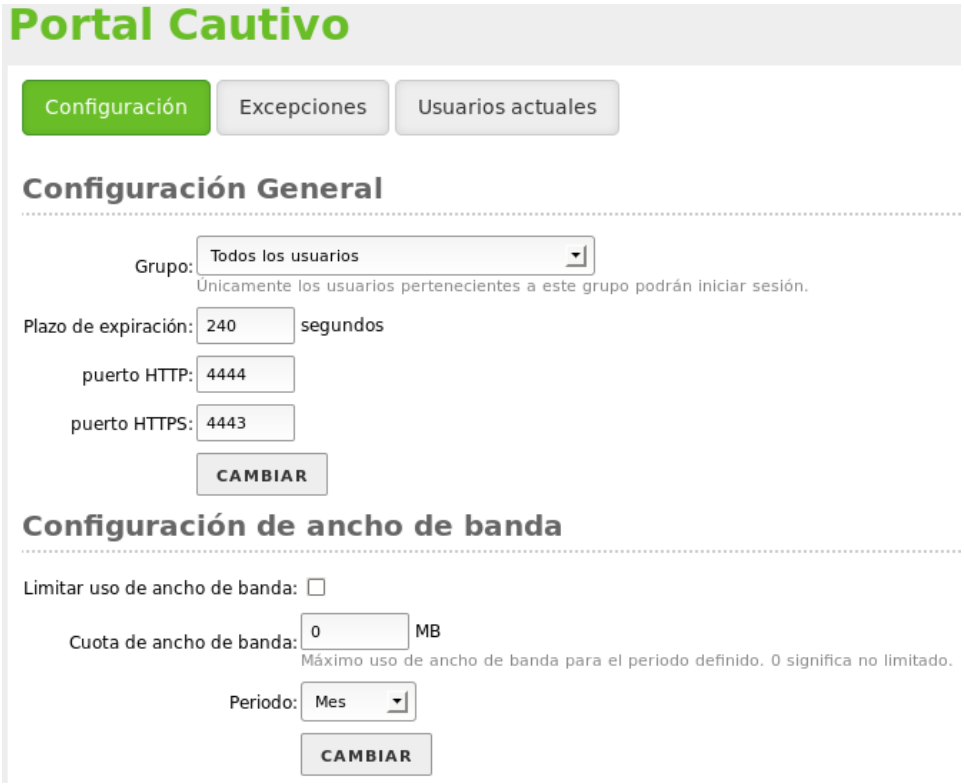


Fig-Zentyal 49. Portal Cautivo.

3. Si el administrador considera limitar el ancho de banda lo puede hacer, actualmente está en 0, sin limitarse.
4. Aplique el portal cautivo a la interface de la LAN.

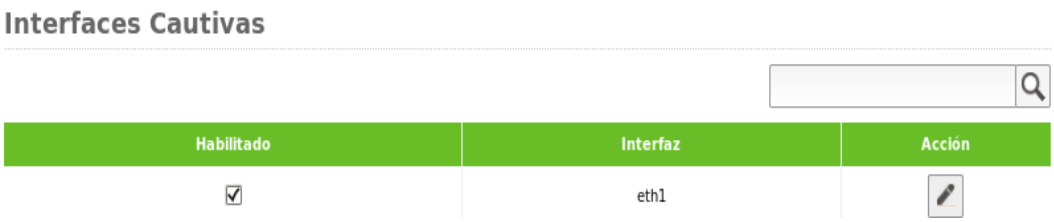


Fig-Zentyal 50. Habilitando Interfaces cautivas.

5. **Excepciones del portal cautivo**.

Para configurar excepción del portal cautivo se requiere crear un objeto, entonces vaya al área de **CORE**, la pestaña **Red**, y seleccione **Objeto**.

- Cree un objeto, llamado ***usuarios exentos del portal cautivo.***
- Al crearse el objeto, haga clic en **Añadir nuevo miembro**.

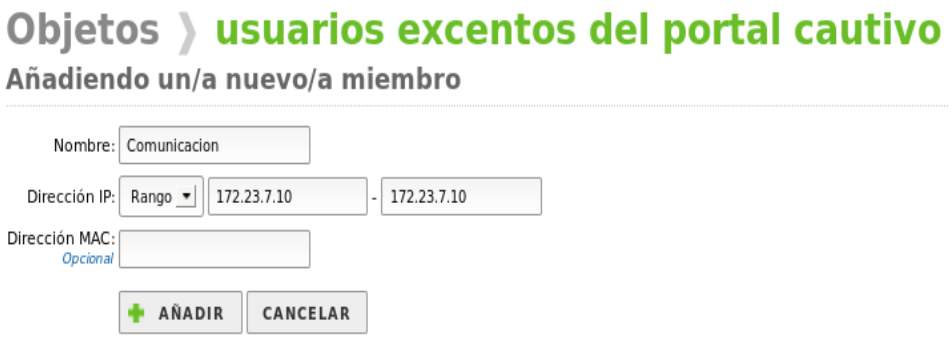


Fig-Zentyal 51. Ingresando usuarios exentos del portal cautivo.

Una vez configurado el objeto, ubíquese en el área de **GATEWAY, Portal Cautivo, Excepciones** y configure.

Fig-Zentyal 52. Creación de objeto para usuarios exentos del portal cautivo.

- Haga clic en añadir nuevo.
- Asegúrese de habilitar.
- En excepciones: seleccione; **objeto exento,** y luego elija el objeto que creo anteriormente (***usuarios exentos del portal cautivo***).

Para que aplicar el objeto exento, configure la regla en el **Cortafuegos, Reglas para redes internas a Zentyal.**

- Haga clic en **Añadir Nuevo.**
- Configure la regla que permita, cualquier servicio, a los usuarios exentos.

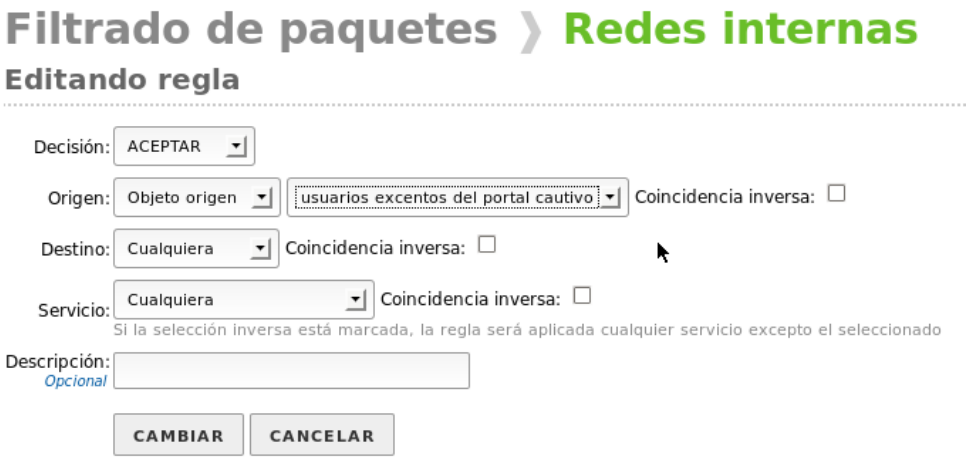


Fig-Zentyal 53. Configuración de reglas para usuarios exentos del portal cautivo.

6. Acceso por el portal cautivo

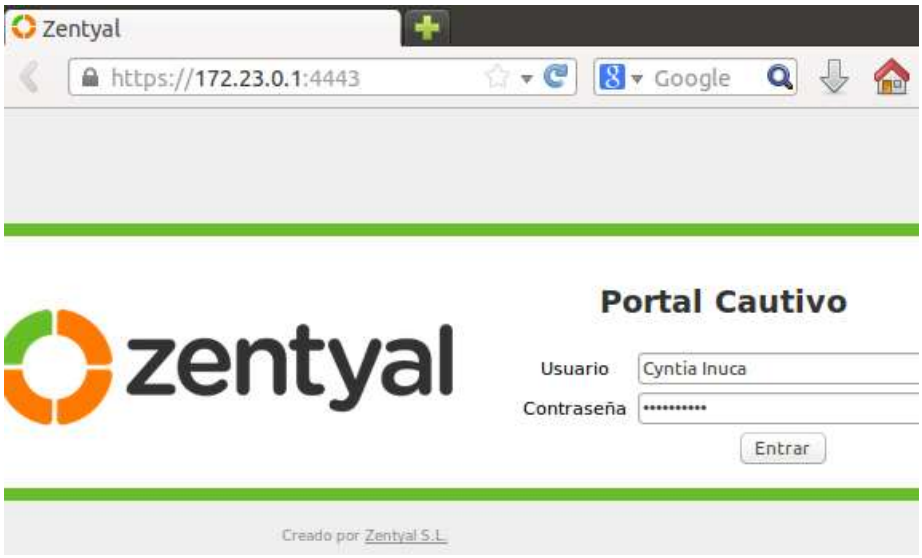


Fig-Zentyal 54. Acceso al portal cautivo.

7. Usuarios actuales

En el portal cautivo existe una pestaña llamada **Usuarios Actuales**, donde se puede ver los usuarios que están conectados en ese momento.

Fig-Zentyal 55. Usuarios actuales del portal cautivo.

IDS/IPS SISTEMA DE DETECCION Y PROTECCION CONTRA INTRUSOS.

1. Habilite el IDS/IPS en Zentyal, en el área de Gateway.

Fig-Zentyal 56. Interfaces de red activas.

2. Elija las reglas y la acción a ejecutarse en caso de detección de un evento.

Fig-Zentyal 57. Reglas para IDS/IPS.

3. En la pestaña mantenimiento puede revisar si se tiene registros sobre infiltraciones en la red, en un informe completo o resumido.

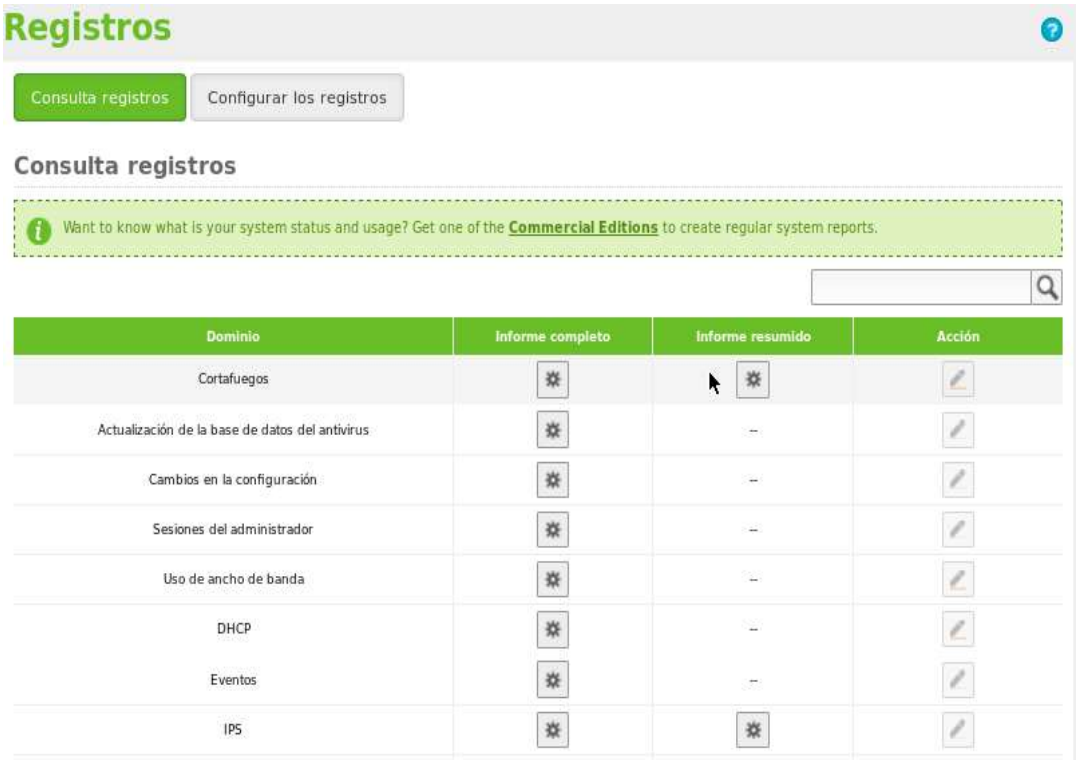
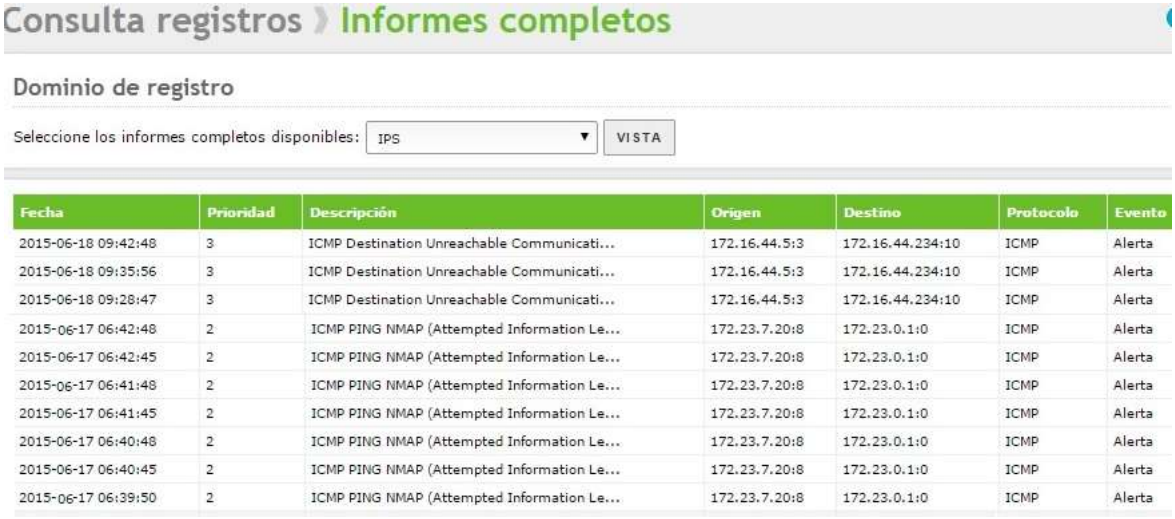


Fig-Zentyal 58. Registros.



Fecha	Prioridad	Descripción	Origen	Destino	Protocolo	Evento
2015-06-18 09:42:48	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-18 09:35:56	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-18 09:28:47	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-17 06:42:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:42:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:41:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:41:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:40:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:40:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:39:50	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta

Fig-Zentyal 59. Registros IPS.

ANEXO D

MANUAL DE ZENOSS

UNIVERSIDAD TÉCNICA DEL NORTE

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL MUNICIPIO DE CAYAMBE

MANUAL

MONITOREO CON ZENOSS CORE

Autor: Cyntia Inuca

Mail: mab_c6@yahoo.es

INSTALACION DE ZENOSS CORE

- **Instalación de Zenoss Core**

1. Zenoss puede instalarse de forma manual o de forma automática, acceda a la página web http://wiki.zenoss.org/Install_Zenoss, y busque el proceso de descarga e instalación de Zenoss para el sistema operativo Centos.
2. Abra el terminal y ejecute los siguientes comando:

```
# wget https://github.com/zenoss/core-autodeploy/tarball/4.2.5 -O auto.tar.gz

# tar xvf auto.tar.gz

# cd zenoss-core-autodeploy-*

# ./core-autodeploy.sh
```

3. Espere que termine la instalación, los ZenPack se instalan de forma predeterminada.

Fig-Zenoss 1. Instalación de Zenoss.

4. Después que finalice la instalación inicie el servicio de Zenoss.

```
# service zenoss start
```

5. Ingrese la dirección IP del servidor en su navegador, para ver la pantalla de configuración inicial de Zenoss.

   a. Haga clic en Get Started.

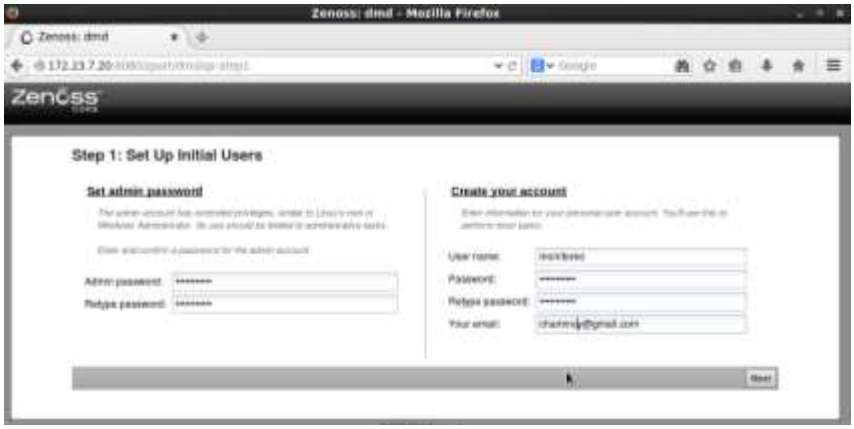


Fig-Zenoss 2. Pantalla de inicio de Zenoss.

6. Configure la contraseña para el usuario administrador por defecto (*admin*) y un usuario adicional para que también acceda como administrador a la consola de monitoreo de Zenoss, ingrese la contraseña y el correo electrónico.

   El correo electrónico es necesario para que el administrador pueda recibir las notificaciones de eventos o fallos.

7. En la siguiente pantalla podrá enviar a descubrir la red, de forma automática o agregar dispositivos de red de forma manual.

   Nota: si tiene activado el protocolo SNMP en los dispositivos a gestionar puede enviar a auto descubrir la red de lo contrario siga el proceso manual de ingreso.

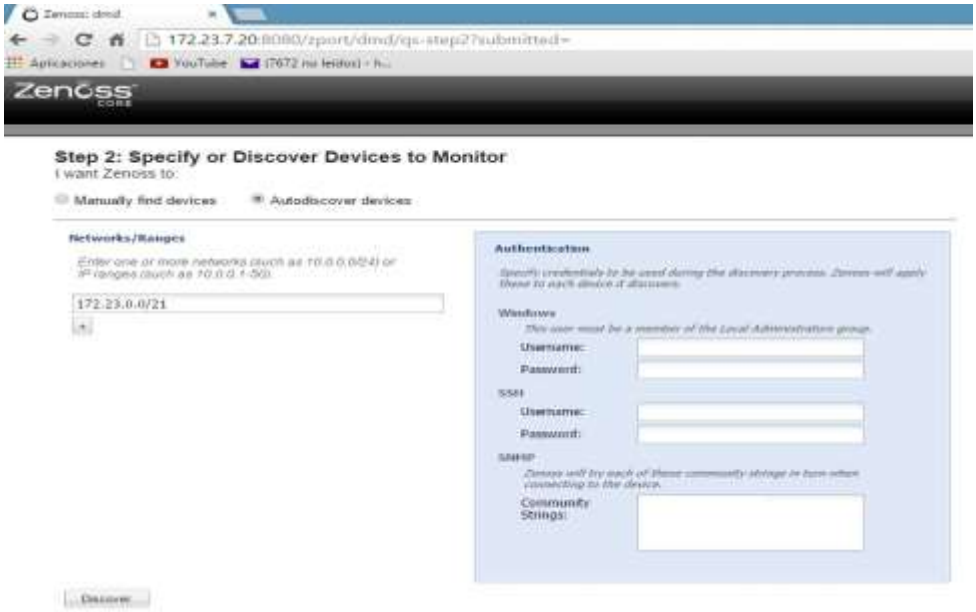


Fig-Zenoss 3. Ingreso de equipos al software de gestión Zenoss**.**

8. Por ahora salte este procedimiento.
9. Para continuar el procedimiento manual de ingreso de equipos a gestionar debe primero habilitarse el protocolo SNMP en los dispositivos.

ACTIVACION DEL PROTOCOLO SNMP

1. Habilite el protocolo SNMP con un nombre de comunidad, en los dispositivos que desee monitorear, de lo contrario no obtendrá información sobre los dispositivos.

    a. Activando SNMP en Windows.

        - Ingrese a ***servicios locales*** de Windows y busque ***Servicio SNMP.***
        - Habilite el servicio, y configure el nombre de la comunidad.

Fig-Zenoss 4.SNMP en Windows.

    b. Activando SNMP en Centos.

        - Mediante el terminal descargue el paquete snmp.
        - Ingrese a /etc/snmp, donde estará el archivo de configuración de snmp.
        - Edite el archivo y configure el nombre comunidad, y la version de SNMP v2.

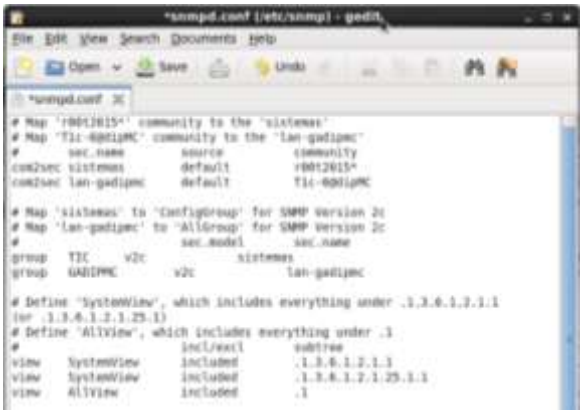


Fig-Zenoss 5.SNMP en Centos.

USANDO ZENOSS

Zenoss presenta una interfaz amigable para el usuario administrador, presenta varias pestañas que ayudan al administrador a gestionar la red.

Pestañas de Zenoss:

- **Dashboard:** es la pantalla inicial de Zenoss, que muestra un mapa, y la vista de eventos.
- **Events:** permite tener un reporte de todos los eventos de cada dispositivo.
- **Infraestruture:** es el núcleo de este software, aquí se agregan los dispositivos que requiere monitorearse, y recopila toda la información referente al dispositivo y permite ver con detalle el uso de sus recursos.
- **Reports:** muestra reportes completos sobre todos los componentes de los dispositivos que son monitoreados.
- **Advance:** disponible solo para el usuario administrador que tenga permisos de administración de Zenoss.

1. Infraestructure.

Esta pestaña es la que permite el ingreso de nuevos dispositivos, redes, procesos y servicios, para el monitoreo.

Fig-Zenoss 6 Pestaña Infraestruture.

Esta pestaña tiene subpestañas.

a. Devices: permite,

- Ingresar un dispositivo de forma manual, si es una red completa se puede auto descubrirla. 
- Eliminar un dispositivo. 
- Seleccionar un dispositivo o un grupo de dispositivos. 

Ingresando un dispositivo.

1. Haga clic en añadir  .
2. Ingrese el dispositivo, con la dirección IP del equipo, la clase de dispositivo, la comunidad snmp, y el puerto.

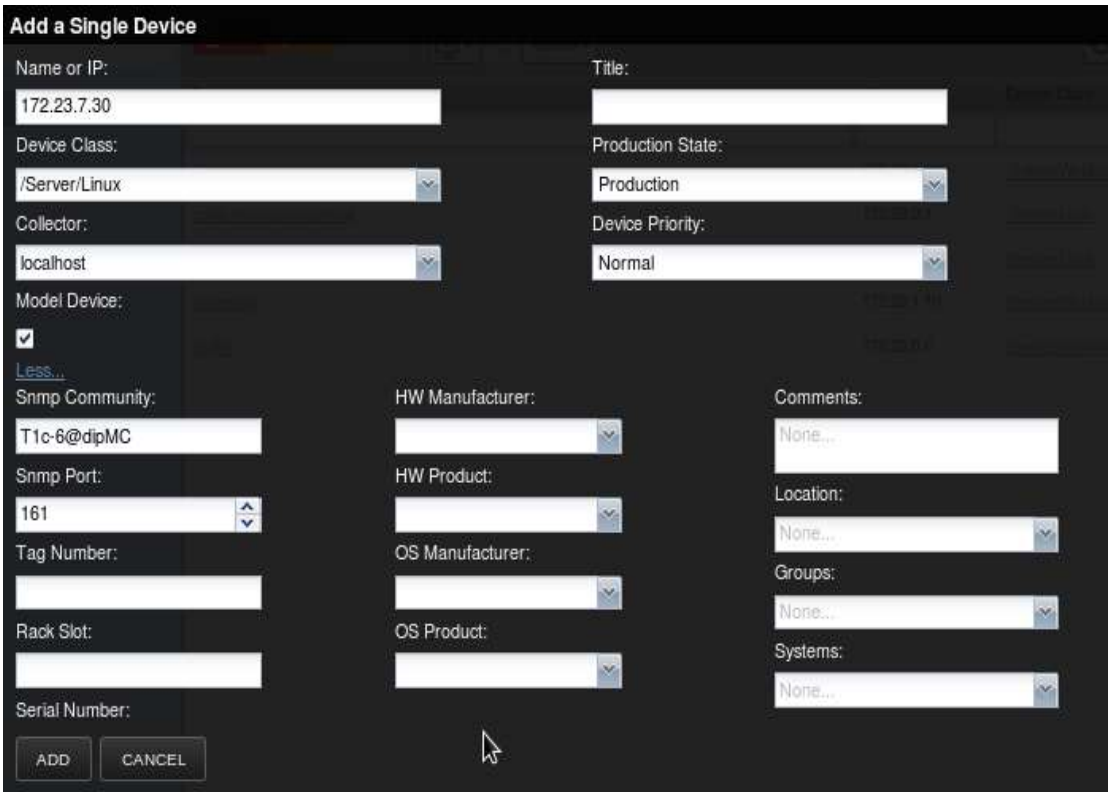


Fig-Zenoss 7. Ingresando dispositivo de forma manual.

Al añadir el dispositivo, gracias a la plantillas de Zenoss se descubre información del equipo, e inicia el monitoreo de sus recursos.

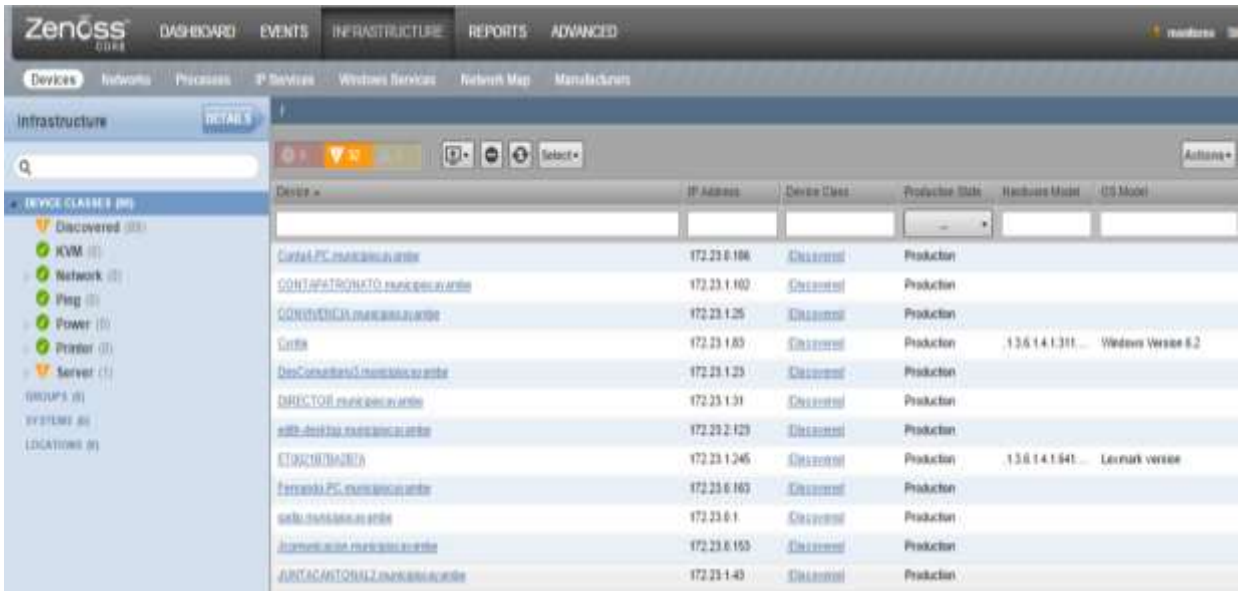


Fig-Zenoss 8. Dispositivos ingresados.

Revisión de información de dispositivo.

Haga clic en uno de los dispositivos, se muestra información sobre el equipo gestionado.

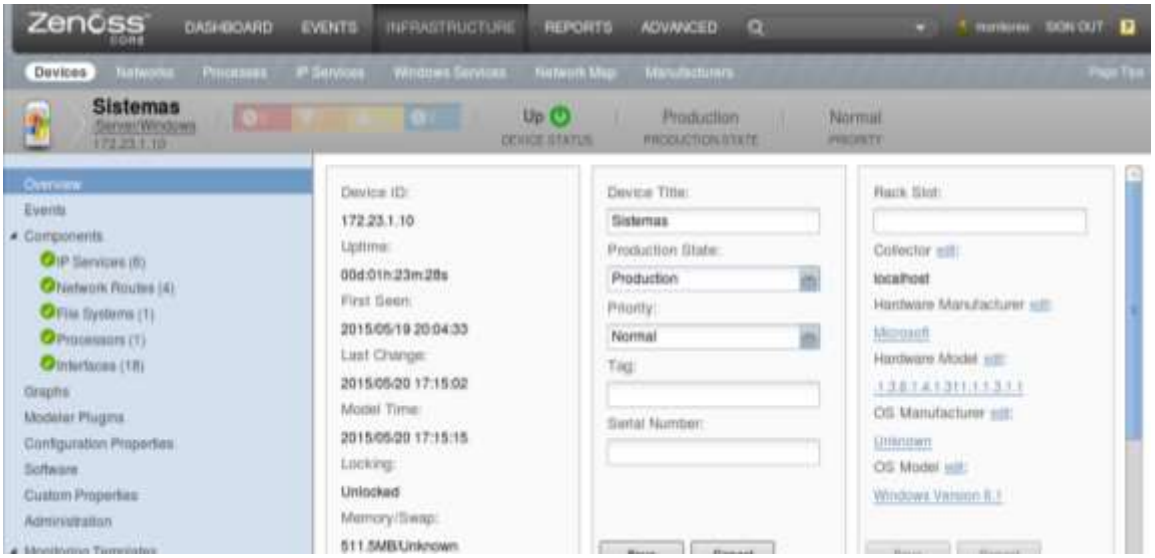
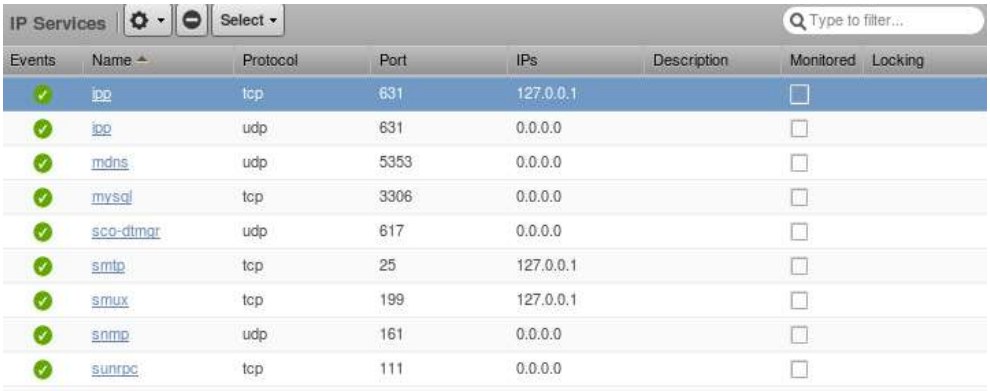


Fig-Zenoss 9. Información del equipo gestionado.

Al abrir la información de los dispositivos, usted podrá ver los componentes que se están monitoreando, entre ellos:

- **Ipservice.**

  Muestra los servicios ip activos en el dispositivo, y sus puertos.



Events	Name	Protocol	Port	IPs	Description	Monitored	Locking
	ipp	tcp	631	127.0.0.1			
	ipp	udp	631	0.0.0.0			
	mdns	udp	5353	0.0.0.0			
	mysql	tcp	3306	0.0.0.0			
	sco-dtmgr	udp	617	0.0.0.0			
	smtp	tcp	25	127.0.0.1			
	smux	tcp	199	127.0.0.1			
	snmp	udp	161	0.0.0.0			
	sunrpc	tcp	111	0.0.0.0			

Fig-Zenoss 10. Servicios ip y puertos abiertos del dispositivo.

- **Interfaces de red.**

  Muestra las interfaces de red del dispositivo, con su dirección IP, dirección MAC, si esta activa, y muestra a la vez una gráfica en el que el administrador puede analizar el tráfico que está saliendo de esta interfaz.

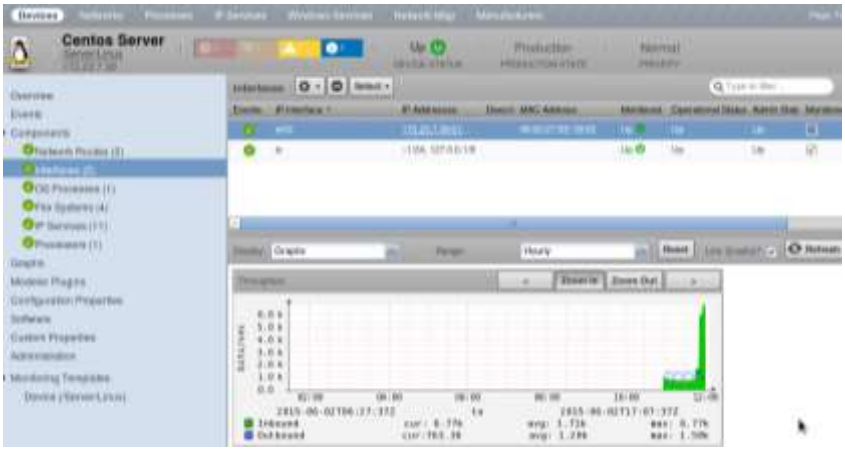


Fig-Zenoss 11. Interfaz de red y gráfica.

- **Networks Routes.**

  Muestra la red a la que pertenece el equipo, y si maneja alguna otra red adicional.

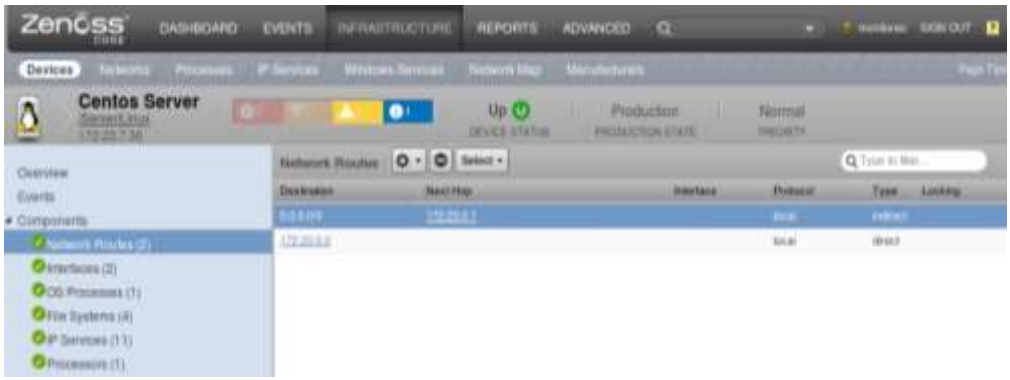


Fig-Zenoss 12. Red a la que pertenece el equipo.

- **File System.**

  Detalla el uso de disco duro, como esta particionado, el espacio libre disponibles, y en porcentaje se muestra el uso que se hace de este recurso.

Fig-Zenoss 13. Detalle del sistema de archivos del dispositivo.

- **Processor.**

  Indica el procesador que está usando el dispositivo.

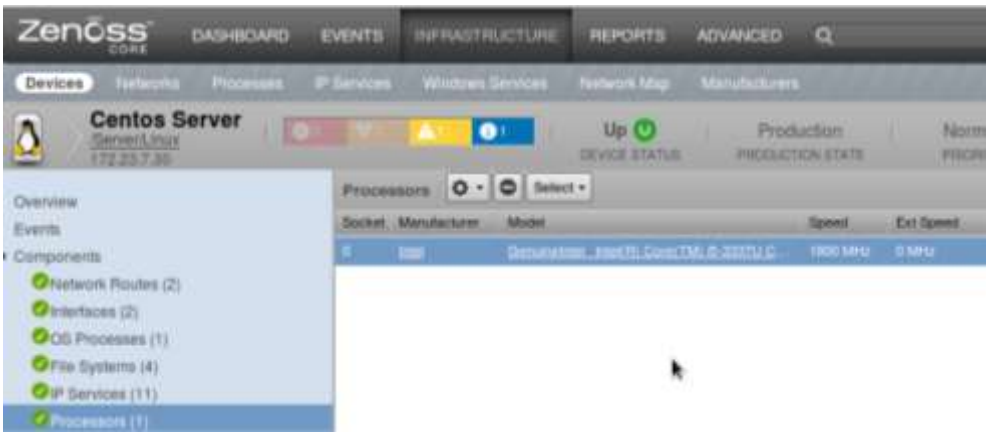


Fig-Zenoss 14. Vista del procesador usado.

- **Graphs.**

Presenta gráficas de disponibilidad del dispositivo, uso de memoria, CPU.

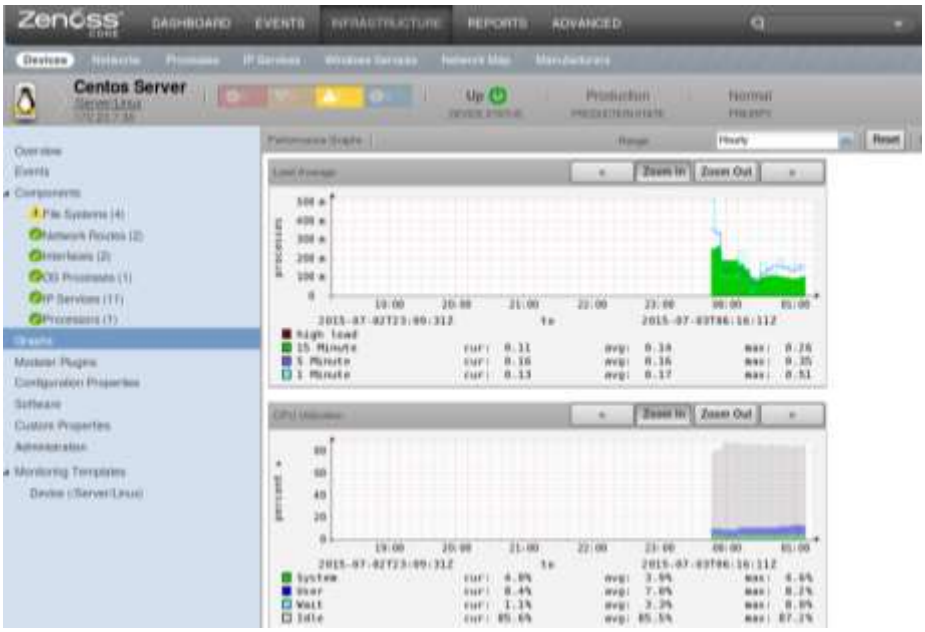


Fig-Zenoss 15. Vista de gráficas.

b. Network:

Usted puede ver las redes que el software está monitoreando, y todo el rango de direcciones IP.

1. Haga clic en la pestaña Netwoks.
2. Revise la el rango de direcciones ip, nombre del dispositivo, el nombre de la interfaz, el direccionamiento MAC, etc.

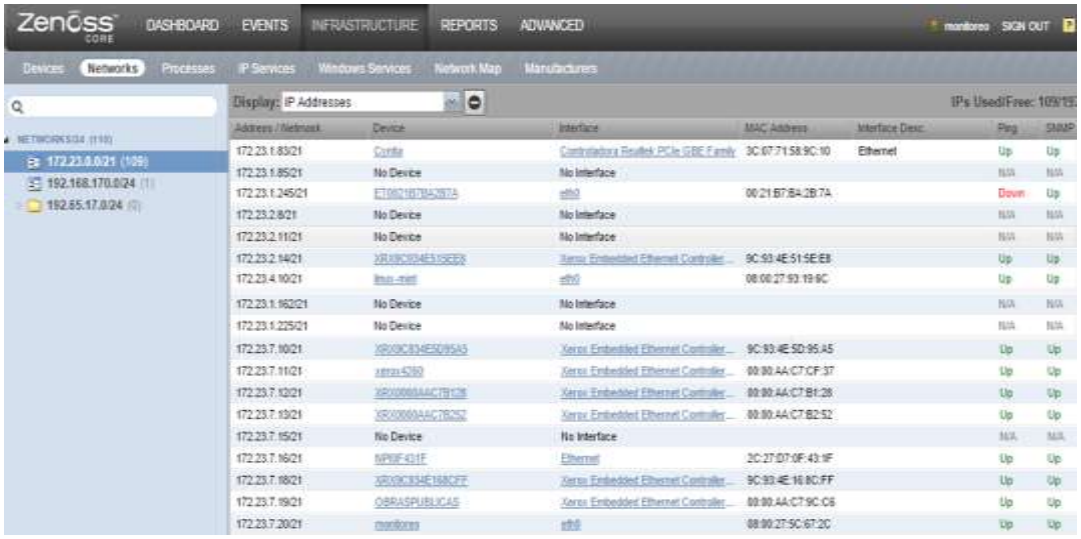


Fig-Zenoss 16. Redes descubiertas.

2. Events

Permite ver todos los eventos de falla que se presenten en los dispositivos, se puede identificar el nivel de gravedad de acuerdo a los colores.

Además esta pestaña permite la configuración de alarmas, notificaciones de los mismos.

a. Creando una alarma

Pasos de configuración:

- Events
- Triggers (alarmas)
- Clic en ✚, e ingresa el nombre para la alarma.
- Seleccione la alarma que creo y haga clic en ⚙.
- En trigger, habilite la alarma; y,
- Configure las reglas.

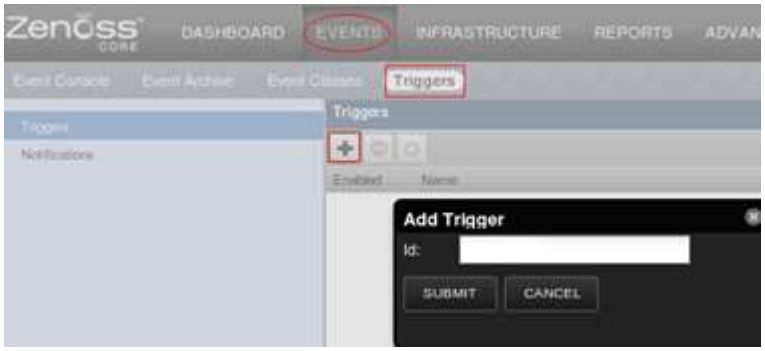


Fig-Zenoss 17. Creación de alarmas.

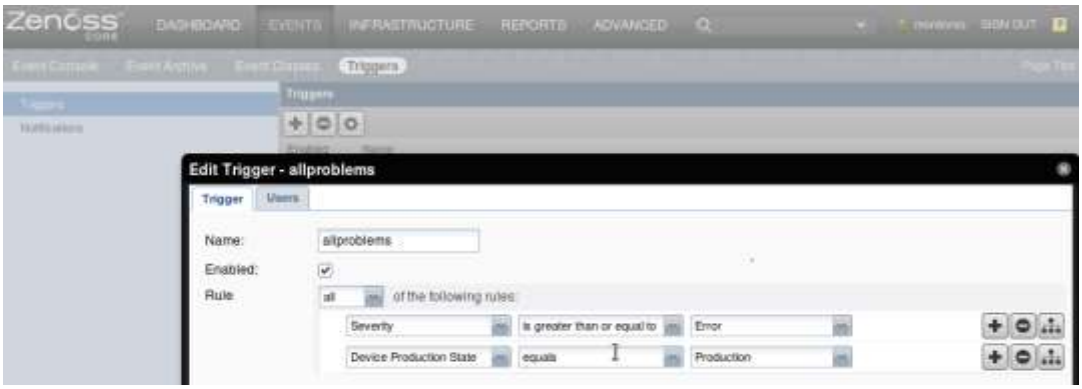


Fig-Zenoss 18. Configuración de alarmas.

- Clic en User,
- Asigne permiso al usuario que verificará esta alarma.(Manage Users)
- Elija el usuario administrador y haga clic en Add.

Fig-Zenoss 19. Asignación de alarma a un usuario administrador**.**

b. Creando una notificación por correo electrónico.

- Events
- Triggers (alarmas).
- Notifications.
- Clic en , e ingresa el nombre de la notificación y el medio de notificación (mail).
- Seleccione la notificación que creó anteriormente y haga clic en .
- Añada la alarma a notificar.
- Haga clic en Content.
- Verifique la estructura del mensaje que se enviará al correo del administrador cuando ocurra un evento.
- Haga clic en Subscribers.
- Añada el usuario administrador que puede enviarle el mensaje.

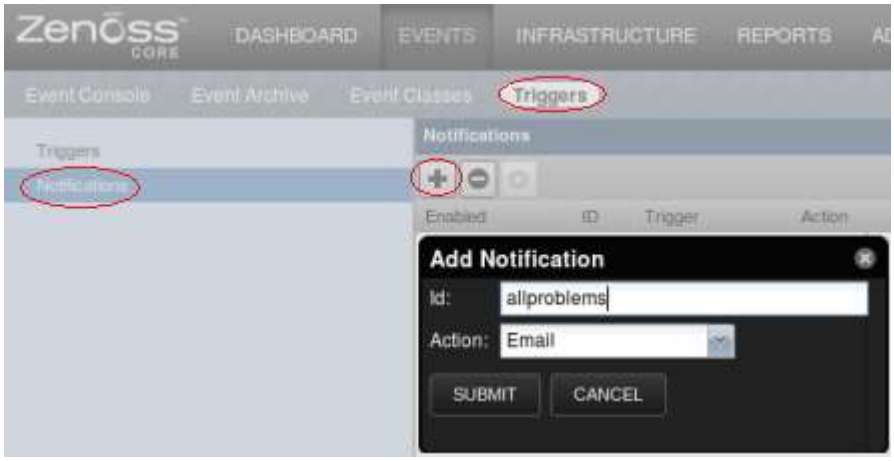


Fig-Zenoss 20. Creación de notificaciones.

c. Visualización de notificaciones en la consola eventos.

Haga clic en *event console*, y verifique para los eventos producidos en cada elemento gestionado.

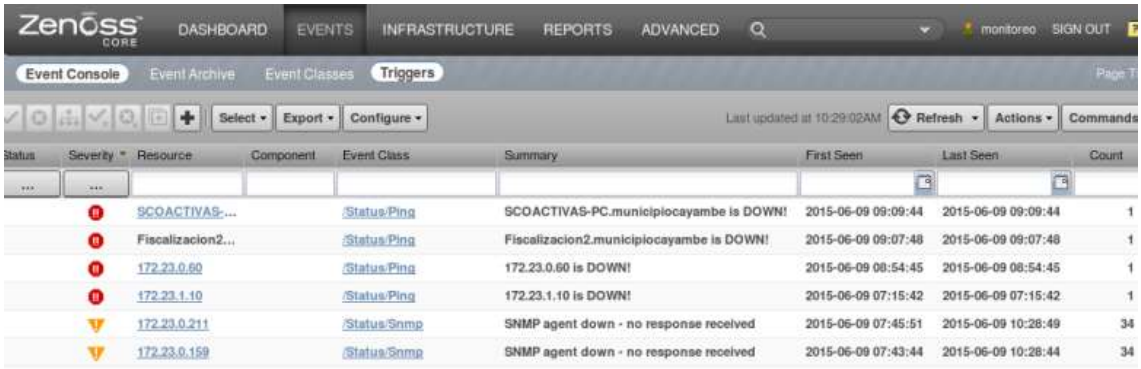


Fig-Zenoss 21. Revisando consola de eventos.

d. Visualización de notificaciones por correo electronico.

A continuación se observa como es el recibido el mensaje por correo electrónico para el administrador de red.

Fig-Zenoss 22. Notificación por correo electrónico.

3. Reports.

Zenoss permite la obtención de reportes de todos los dispositivos gestionados y sus componentes, así como reportes de los eventos, graficas, y reportes de rendimiento.

1. Haga clic en Reports.
2. Elija el reporte que necesita ver.
3. Haga clic en generar y Zenoss le mostrara información con todo detalle.

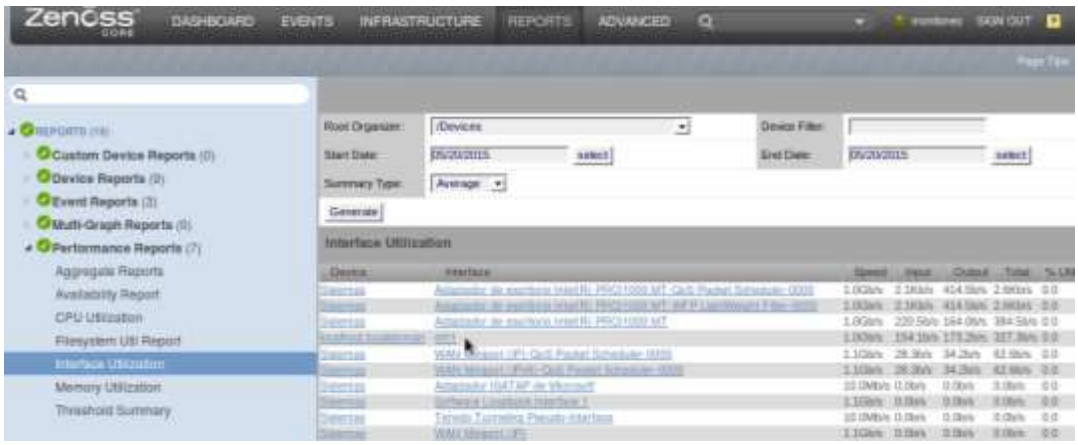


Fig-Zenoss 23. Reporte de uso de interfaces de red.

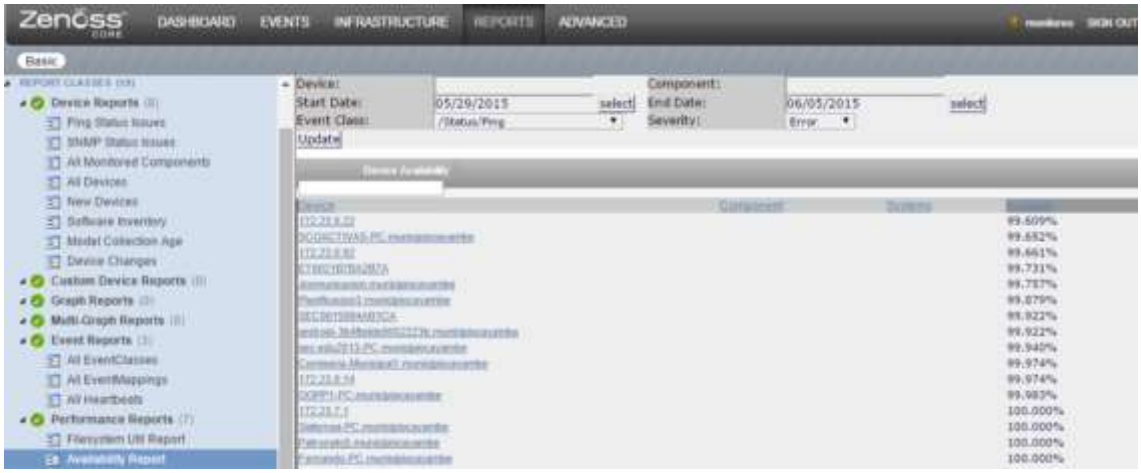


Fig-Zenoss 24. Reporte de disponibilidad.

4. Advance.

Esta pestaña permite administración de usuarios para el sistema de gestión de red, así como también plantillas para el monitoreo de los dispositivos gestionados.

Plantillas:

Si accede como administrador de red, podrá revisar e instalar plugins o ZenPack para uso de Zenoss.

Fig-Zenoss 25. Paquetes instalados para el funcionamiento de Zenoss.

Las plantillas o zenpack, pueden ser configurados para que cuando monitoree los recursos de la red, este presente gráficas y notifique cuando se sobrepase umbrales de rendimiento permitidos.

Pasos para establecimiento de umbrales.

- Advance.
- Monitoring templates.
- Device.
- Elija la plantilla.

- Data Source.
- Revise una fuente de datos que va a monitorear o haga clic en  para añadir una nueva fuente de datos.
- Haga doble click sobre la fuente de datos y revise si la OID responde a la solicitud de información mediante un test.
- Finalmente Submit.

Fig-Zenoss 26. Configuración de recursos a monitorear.

- Luego haga clic en Threshold.
- Ingrese el nivel de gravedad y el valor máximo del umbral, y guarde.

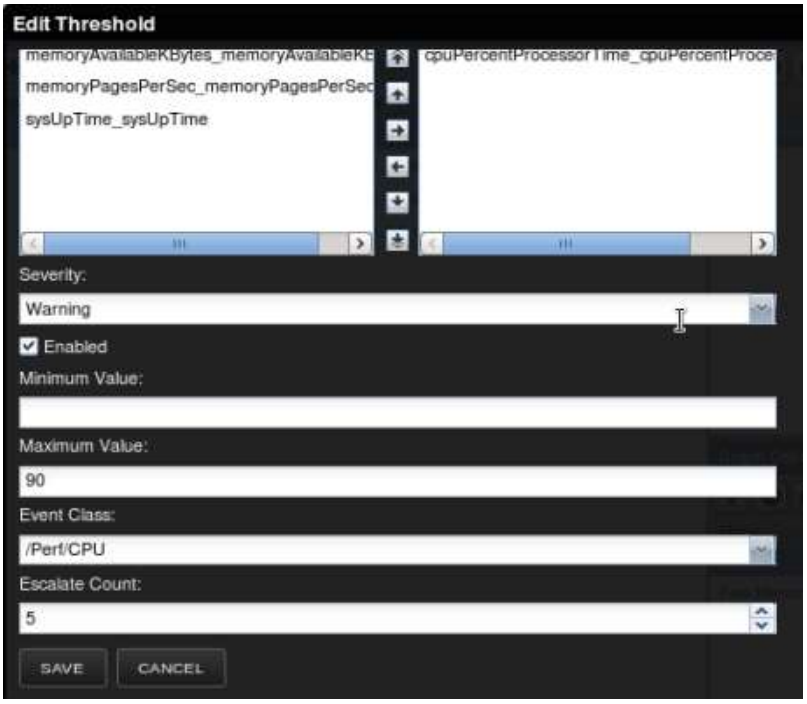


Fig-Zenoss 27. Establecimiento de umbral máximo.

- Defina el gráfico para ver el rendimiento del recurso en Edit Graph.
- Defina la unidad en que se mide el rendimiento del recurso.

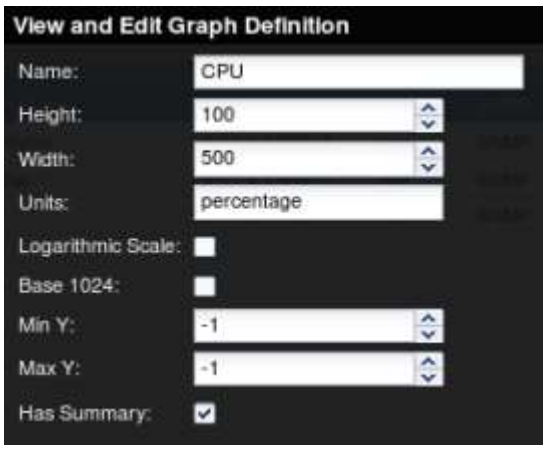
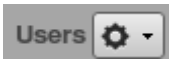


Fig-Zenoss 28. Definición de gráfica.

Usuarios:

Pasos creación de usuarios.

- Advance.
- Users.

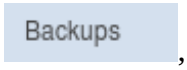
- Para agregar un usuario haga clic en 

- Asigne el rol que va a cumplir.
- Registre un correo electrónico si va a manejar notificaciones de fallas producidas en la red.

Fig-Zenoss 29. Usuarios administradores de Zenoss.

Nota: La cuenta de correo electrónico es de Gmail, ya que este software al instalarlo por defecto también se instala y configura la función de emitir mensajes de correo electrónico a Gmail automáticamente, el administrador debe cerciorarse que para el cumplimiento de esta función este habilitado el protocolo 25 SMTP.

Respaldos:

En esta misma pestaña permite la obtención de respaldos de información haga clic en 

, y cree un respaldo de Zenoss.

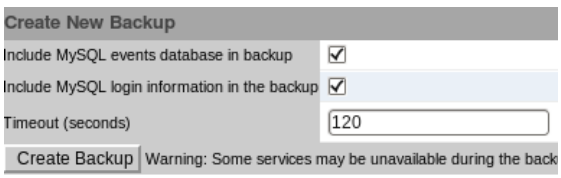


Fig-Zenoss 30. Creaccion de un Backup.

Fig-Zenoss 31. Respaldo de Zenoss.

ANEXO E

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

MANUAL DE POLÍTICAS

Y PROCEDIMIENTOS

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

Autor: Cyntia Inuca

Mail: mab_c6@yahoo.es

Gobierno Autónomo Descentralizado Intercultural y Plurinacional de Municipio De Cayambe		
	MANUAL DE POLÍTICAS Y PROCEDIMIENTOS PARA LA GESTIÓN DE RED LOCAL GADIPMC	
Versión: 1.0	**Revisado por:** Tnlg. Rony Carvajal *Jefe de Infraestructura y Conectividad*	**Aprobado por:** Ing. Fabián Bautista *Director de TIC*

I. INTRODUCCIÓN

La base para que cualquier institución pueda trabajar a través de su red de datos, comienza con la definición de políticas y procedimientos adecuados, en el que actúan el administrador de red y los usuarios 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 realizar siguiendo un objetivo en común, la conformación de un manual sirve como un elemento de apoyo administrativo.

En este documento 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 lograra administrar la red por partes y mejorar el servicio brindado a la municipalidad, garantizando la disponibilidad de la red.

II. PROPÓSITO

Establecer directrices a través de políticas y procedimientos para gestionar la red local, y presentarlas a la dirección de TIC, para que sea de su conocimiento, uso y cumplimiento, de manera que puedan administrar la red de forma organizada, mantener y mejorar la disponibilidad de la red.

III. CONCEPTOS PRELIMINARES

- **Administración y gestión de red de área local**

  La administración y gestión de red local integra, el uso de herramientas gestión que permitan monitorear la red y obtener datos de la red, el uso de métodos que permitan el control de actividades entorno al funcionamiento de la red, para mediante estos garantizar la operatividad de la red y mejorar su disponibilidad.

- **Monitoreo de red**

  Es la supervisión, observación y análisis del estado de los recursos de 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.

- **Control de red**

  El control de la red implica la vigilancia cotidiana de la red, incluye procedimientos que permitan mantener la disponibilidad de red.

- **Políticas de gestión**

  Las políticas son guías que el permiten al administrador de red ejercer alguna acción ante un evento en la red, las políticas siempre irán acompañadas de una serie de procedimientos para cumplirlas, siempre teniendo un objetivo en común

IV. GENERALIDADES

d) Este documento maneja un lenguaje técnico, dirigido para la dirección de TIC quienes cumplen con conocimientos técnicos de redes.

e) Las políticas establecidas en este documento son recomendaciones para la buena administración de la red y no pretenden ser reglas absolutas y de uso obligatorio.

f) Para cumplir las políticas establecidas en este documento, interactuarán administrador de red, encargados de la red local, y los usuarios de la red.

V. NIVELES ORGANIZACIONALES

e) Director de TIC

Autoridad de nivel superior. Ente encargado de la aprobación de las políticas de gestión junto al Jefe de Infraestructura y Conectividad.

f) Jefe de Infaestructura y Conectividad

Autoridad a cargo de funcionamiento de la infraestructura tecnologica de red, a el se le atribuye las funciones de administrador de red, toma control sobre la manipulacion y configuraion de equipos que conforman la red local, toma decisiones entorno a su labor en caso de no estar la autoridad superior.

g) Soporte Tecnico

Encargado de brindar servicios de soporte tecnico referente a hardware y software a los usuarios, que pertenecen a la red local. Toma decisiones cuando no estan ninguna de las autoridades.

h) Usuarios

Son las personas que estan interconectadas a la red local para acceder a los servicos que brinda la direccion de TIC.

VI. VIGENCIA

Este documento no es de uso obligatorio, por lo cual entrará en vigencia cuando las autoridades competentes autoricen su uso, para ello deberán revisarlo, y de ser posible mejorarlo, para que cumpla los objetivos que persigue la dirección de TIC, referente a una buena administración y gestión de la red local.

VII. MARCO NORMATIVO

El presente documento se realizó en base Norma NTE INEN-ISO/IEC 27002:2009, que brinda soluciones de seguridad y están enfocadas a todo tipo de organizaciones, de cualquier tamaño y naturaleza.

De esta norma se acoge la estructura de documentos de políticas de seguridad y soluciones recomendadas, acoplándolas con el modelo funcional de gestión de red ISO/OSI.

VIII. ESTRUCTURA

Este documento se estructura políticas en base al modelo funcional de gestión de red ISO/OSI, para que funcione a través herramientas de software libre que permitan gestionar la red.

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 aplicacion 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.

IX. TÉRMINOS Y DEFINICIONES

Este documento hace uso de varios conceptos técnicos, los cuales se definen, para facilitar la comprensión y uso de este documento.

- **Red:** Es la interconexión de varios equipos de comunicación, a través de un medio de trasmisión, para intercambiar información, y acceder a varios servicios.
- **LAN:** Red de área local, son redes para un área geográfica pequeña con alcance a pocos km aproximadamente 100 km,, que puede alcanzar hasta 10Mbps de velocidad, y contener de 100 a 1000 usuarios, generalmente aplicadas en pequeñas empresas, compañía u organización.
- **Administración:** Significa organizar, dirigir, y controlar los recursos de una entidad.
- **Gestión:** Es la asignación de actividades de los recursos de red.
- **SNMP:** Es el protocolo de administración de red simple, trabaja en la capa aplicación, y sirve para el intercambio de información de gestión de red.
- **Sistema de gestión de red:** Un sistema de gestión de red, es un conjunto de elementos que permiten administrar la red, basado en el paradigma gestor-agente.
- **Sistema de seguridad:** es un conjunto de herramienta que permiten controlar el acceso de usuarios a la red, mejorar firewall, y proteger la red.
- **Gestor:** Es la estación principal donde se alojan aplicaciones de monitoreo el cual pide al agente información de los dispositivos gestionados.
- **Agente:** es un software que reside en el dispositivo gestionado y que se comunica con el gestor respondiendo a sus peticiones.
- **Monitoreo:** es la visualización de información de los recursos de red.
- **Recursos de red:** son aquellos elementos que están interconectados a la red como: switch, router, computadores y servidores, dentro de estos elementos se encuentran sus recursos como interfaces de red, disco duro, memoria, procesador, etc.
- **Servicios de red:** son aplicaciones que se ofrece a través de la red por medio de los servidores.

X. DESARROLLO DE POLÍTICAS

1. Políticas de gestión de red local		**Código:**	POL-LAN-0001
1.1. Objetivos de políticas de gestión de red	**Art 1.** Establecer políticas y procedimientos de gestión de red, para administrar la red local cubriendo las necesidades y requerimientos de red, basándose en el modelo funcional de gestión de red ISO/OSI.		
1.2. Documento de políticas gestión de red	**Art 2.** La Dirección de TIC, elaborará un manual de políticas y procedimientos de gestión de red local, la cual debe será aprobada y publicada para conocimiento del administrador de red y los encargados de la red local, así como los usuarios finales.		
1.3. Revisión de políticas de gestión de red	**Art 3.** La dirección de TIC, deberá revisar el Manual de Políticas y procedimientos, en intervalos planificados para garantizar que es adecuada, eficaz, y suficiente. **Art 4.** Actualizar el manual, ante cambios significativos que se puedan dar en la institución.		

2. Política para la gestión de configuración		**Código:**	POL-LAN-0002
2.1. Planificación de red	**Art 5.** Verificar constantemente el funcionamiento correcto de todos los recursos de red, y planificar proyecciones futuras para el avance tecnológico de la infraestructura de red de la institución. **Art 6.** Responder a las necesidades de los usuarios de la red, analizando sus requerimientos, y planificando la solución a estos. **Art 7.** Manejar información de red, y controlar cambios que se de en la infraestructura de red de manera que no afecte a su funcionamiento.		

2.2. Configuración de equipos	**Art 8.** Únicamente el administrador de red y sus autorizados podrán: a. Manipular los equipos de comunicación que este interconectados en la red local. b. Configurar, borra o modificar información del equipo. c. Integrar un equipo nuevo a la red local. **Art 9.** Todos los equipos que quieran ingresar a la red local deberán cumplir con la configuración básica que les permita beneficiarse de los servicios que provee la dirección de TIC a través de la red de la institución. **Art 10.** Los equipos y dispositivos de red que estén conectados a la red local, deberán tener habilitado el protocolo SNMPv2 (siempre y cuando lo soporten), e incluir un nombre de la comunidad SNMP para poder ser gestionados.
2.3. Ingreso de equipos	**Art 11.** La dirección de TIC, deberá tener su propio inventario de equipos activos en la red, al ingresar un nuevo equipo a la red se registrará las características más importantes, de forma que tenga un control sobre todos los elementos que conforman la red. **Art 12.** Los equipos que están conectados a la red local y soporten el protocolo SNMP, deben ser ingresados en la aplicación de gestión para monitorear sus recursos y conocer el estado actual de su funcionamiento.
2.4. Documentación de configuración	**Art 13.** El administrador de red, debe llevar la documentación correspondiente a configuraciones realizadas para que el sistema de gestión de red funcione. **Art 14.** Se mantendrán respaldos de las configuraciones realizadas en los equipos y servidores, para casos de eventos inesperados como perdida de información o des configuración del servidor. **Art 15.** Antes de realizar cambios en la configuraciones de equipos y servidores se respaldar la última configuración correcta del equipo.

3. Políticas para la gestión de fallos	**CÓDIGO:**	POL-LAN-0003
3.1. Manejo de fallos	**Art 16.** El momento en que surja una falla en el entorno de la red local, el administrador es responsable de responder a dicho evento, pues él debe detectar, aislar, y resolver el fallo, ayudado de la aplicación de gestión y esfuerzo humano. Para conseguir una respuesta efectiva rápida y ordenada debe cumplir con el manual de procedimientos para la gestión de fallos. **Art 17.** Se debe tratar de dar solución al fallo en el menor tiempo posible, para evitar inconvenientes en el trabajo de los usuarios de la red.	
3.2. Notificación de fallos	**Art 18.** Comunicar los fallos ocurridos en la red lo más pronto posible, manejando canales apropiados que permitan actuar al administrador de red para que tome medidas correctivas oportunas.	
3.3. Documentación de fallos	**Art 19.** Se deberá documentar los fallos producidos y los procedimientos que se realizaron para solucionarlo, teniendo así un proceso a seguir en caso de que la falla se persista.	

4. Políticas para la gestión de rendimiento	**CÓDIGO:**	POL-LAN-0004
4.1. Planificación y aceptación del sistema	**Art 20.** Planificar y garantizar la adecuada capacidad de un recurso para minimizar riesgos de fallos en los equipos que están interconectados a la red local y mantenerlos disponibles.	
4.2. Establecimiento umbrales	**Art 21.** Se garantizará que los equipos de red trabajen correctamente estableciendo umbrales de aceptación, para prevenir problemas en su funcionamiento.	

5. Políticas para la gestión de contabilidad	**CÓDIGO:**	POL-LAN-0005
5.1. Manejo de reportes	**Art 22.** El administrador de red podrá obtener reportes del uso de recursos de red monitoreados mediante una aplicación de gestión, de forma diaria, mensual y anual, en el momento que él lo requiera.	
5.2 Inventario de activos	**Art 23.** Se debe llevar un inventario de todos los activos de red, estos deben estar claramente identificados, en él se deben registrar los datos más importantes. **Art 24.** La dirección de TIC actualizará el inventario en un intervalo de tiempo de 6 meses.	

6. Políticas para la gestión de seguridad	**CÓDIGO:**	POL-LAN-0006
6.1. Control de acceso a equipos	**Art 25.** Restringir el acceso lógico a equipos de comunicación de la red local y su información de configuración únicamente a usuarios autorizados de la Dirección de TIC.	
6.2. Control de acceso a la aplicación de gestión de red.	**Art 26.** Se deberá restringir el acceso a la (s) aplicación (es) de gestión de red, únicamente el usuario administrador de red podrá acceder su configuración e información. **Art 27.** Deberá permitir el manejo de varios usuarios y permitir asignación de roles de usuarios.	
6.3. Control de acceso a servidor de seguridad	**Art 28.** Se deberá restringir el acceso al servidor de seguridad, únicamente el usuario administrador de red podrá acceder su configuración e información.	
6.4. Control de acceso a Internet	**Art 29.** El administrador de red deberá precautelar el ancho de banda por lo que el internet no debe ser mal utilizado, en actividades que demanden gran cantidad de consumo de red, como; descarga de videos, música, redes sociales, etc.	

6.5. Control de usuarios	**Art 30.** El administrador de red, definirá un procedimiento formal de registro de usuarios para otorgar acceso a los diferentes sistemas y servicios de la red. **Art 31.** Controlar la asignación de permisos privilegiados a los usuarios en caso de ser oportuno. **Art 32.** El administrador de la red podrá dar de alta o baja a un usuario. **Art 33.** El usuario será el único responsable del uso de su usuario y contraseña, asignada por el administrador.
6.6. Protección contra intrusos	**Art 34.** Mantener la integridad y disponibilidad de la red con herramientas que permita funciones de IDS/IPS que bloquee y registre cualquier actividad sospechosa y maliciosa que se detecte en la red.
6.7. Manejo de Backups	**Art 35.** Mantener respaldos de los servidores y guardarlo en un dispositivo de almacenamiento o servidor de archivos, para casos contraproducentes.

I. DESARROLLO DE PROCEDIMIENTOS PARA LA GESTIÓN DE RED LOCAL

El establecimiento de procedimientos para la gestión y administración de la red local permite tener a la mano una guía para solucionar cualquier evento inesperado, ayudando al administrador a desempeñar mejor sus funciones. A través de control de administración y monitoreo con las herramientas de software libre se cubrirán todas las áreas del modelo funcional de gestión de red IS/OSI.

A continuación se detallan los procedimientos de acuerdo al modelo.

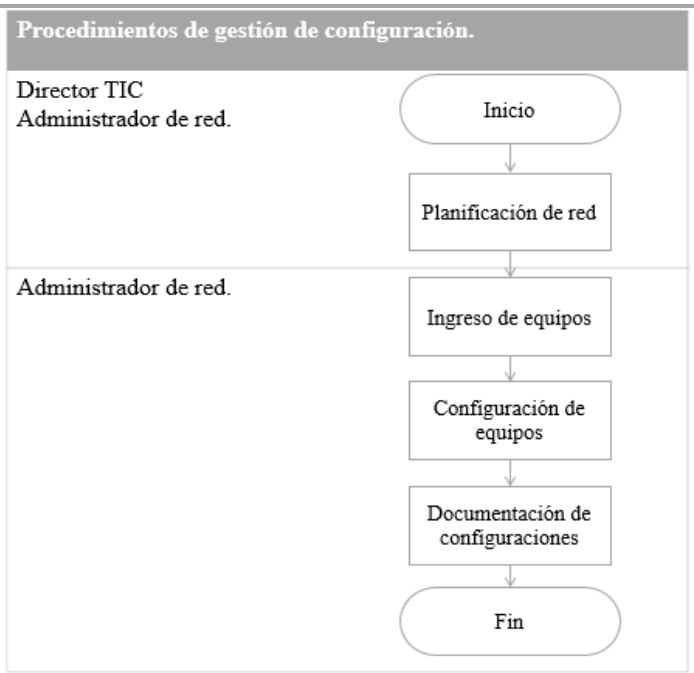
GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

1. Procedimientos para la gestión de configuración.		**Código:**	PRO-LAN-0001
N°	**Actividad**	**Descripción**	**Responsable**
1	Panificación de red	El administrador debe estar atento a: – Cambios en la infraestructura de red. – Requerimientos de nuevas tendencias tecnológicas, que mejoren el funcionamiento de la red. – Responder a las solicitudes de los usuarios. El usuario debe notificar al administrador cuando: – Vaya a realizar algún cambio en las oficinas que afecten a la infraestructura de la red. – Cuando se roten los puestos de trabajo. – Cuando requiera acceso a algún servicio a través de la red. Cuando requiera la compra de un equipo tecnológico que se vaya a integrar a la red.	Director de TIC y administrador de red.

N°	Actividad	Descripción	Responsable
2	Ingreso de equipos.	Al comprar y adquirir un equipo de red, que vaya a ingresar la red, el administrador debe: – Verificar su funcionamiento, que no haya fallas de fábrica. – Registrarlo en su inventario. – y prepararlo para integrarlo a la red.	Administrador de red.
3	Configuración de equipos.	Para todo equipo de red que requieran integrarse a la red, debe: – Tener la configuración básica que le permita conectarse a la red local y sus servicios. o Configuración de direccionamiento ip estático o dhcp. Habilitar el protocolo SNMP, siempre y cuando lo soporte. o Habilite el protocolo SNMP. o Configure comunidad SNMP y asigne permisos. o Agregue información de contacto y ubicación. Para integrar un equipo al sistema de gestión de red Zenoss: – Vaya a Device, – Haga clic en + (añadir) – Ingrese la dirección ip del equipo, la clase de dispositivo, habilite snmp e ingrese la comunidad y el puerto 161. El direccionamiento ip del dispositivo a gestionar debe estar configurado de forma estática.	Administrador de red.

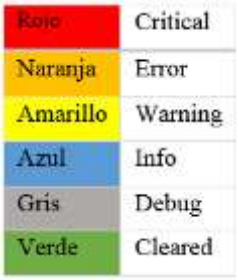
N°	Actividad	Descripción	Responsable
4	Documentación de configuración.	1. Obtener respaldos de configuraciones estables realizadas en: – Servidores (Zentyal y Zenoss). – Configuraciones que se realicen en los dispositivos a gestionar, ej. switch administrables. 2. Almacenar los respaldos en el servidor de archivos FTP de la institución. 3. En caso de haber algún tipo de des configuración, copiar el respaldo y cargarlo nuevamente al servidor o equipo.	Administrador de red.

Flujograma:



GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

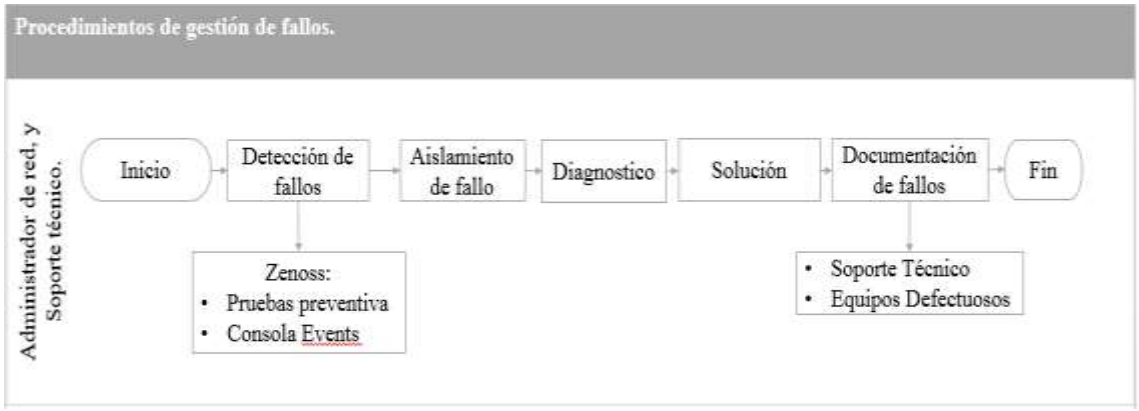
2. Procedimientos para la gestión de fallos.			**Código:**	PRO-LAN-0002
N°	**Actividad**	**Descripción**		**Responsable**
1	Detección de fallos.	La detección de fallos se lo realiza a través de la aplicación de gestión Zenoss: **Pruebas preventivas:** A través del software de monitoreo se puede ejecutar comandos como: – Ping, Para verificar conectividad. – Traceroute, Puede actuar como aislador para detectar hasta qué punto de la red llega el paquete emitido. – Snmpwalk, Para verificar si hay comunicación entre estación gestora y dispositivo gestionado. **Gestión reactiva:** El administrador de red puede revisar los fallos producidos en: 1. Consola EVENTS de Zenoss. 2. Correo electrónico. 3. Llamada por el usuario. En el que el administrador debe analizar los eventos, y actuar ante estos.		Administrador de red.
2	Aislamiento de fallos.	El software de monitoreo Zenoss, permite aislar la falla, detecta que dispositivo es, y emite alarmas por colores, los cuales definen el estado en que se encuentra el dispositivo.		Administrador de red.

N°	Actividad	Descripción	Responsable
2	Aislamiento de fallos.	 El administrador sabrá dar prioridad a los fallos de acuerdo a estas alarmas. Y procederá con el diagnostico.	Administrador de red.
3	Diagnóstico de fallos.	Zenoss, proporciona información de diagnóstico, en el que muestra la clase de eventos ocurrido, mediante esta información el administrador procede a verificar el fallo y buscar las posibles soluciones junto al técnico encargado. – **CMD is down:** problemas en la interfaz de red. – **SNMP is down**: protocolo snpm no está habilitado. – **Perf/CPU:** problemas en el rendimiento de CPU. – **Perf/disk:** problemas de saturación de disco.	Administrador de red y Personal de Soporte técnico
4	Solución de fallos.	**Procedimientos para resolver problemas de conexión a internet.** – Revisar la conexión de cable de red, desde el punto de red hacia el equipo terminal del usuario. – Revisar si detecta conexión, a través de la tarjeta de red. – Si no detecta revisar del direccionamiento y asignación IP. – Realizar pruebas de testeo, como ping, al gateway de la red. – Realiza un ping o traza a una página de internet. Si el procedimiento anterior no funciona: – Revisar la tarjeta de red y el punto de conexión de red. – Cambio de cable de red.	Soporte técnico.

N°	Actividad	Descripción	Responsable
4	Solución de fallos.	– Reiniciar el equipo (computador, o routers inalámbricos). – Reconfigurar los equipos. **Procedimiento para resolver problemas de acceso denegado a sistemas y servicios de la red.** – Los accesos a sistemas y servicios de red, generalmente manejan usuario y contraseña, revisar si está ingresando correctamente el usuario y contraseña asignado, de lo contrario el administrador deberá revisar este acceso a través del sistema y generan una nueva contraseña. – Otra causa posible es la desconexión del servidor, el administrador debe revisar el software de monitoreo el estado del servidor, si emite alguna alerta o no, el administrador y técnico encargado deben estar pendientes de que el servidor no presente problemas. – En compartición de archivos la posibilidad de que no pueda acceder a la información compartida es que el equipo del usuarios que comparte esta apagada, o se limitó el número de accesos. **Procedimientos para resolver problemas de compartición de impresoras.** – Los usuarios que deseen imprimir deben tener instalado el driver o controlador de la impresora. – Si la impresora esta compartida, el equipo terminal del usuario que desea imprimir debe vincular su conexión al equipo que tiene instalado la impresora. Si el equipo donde está instalado la impresora no está encendido, no puede imprimir debido a que no hay conexión.	Soporte técnico

N°	Actividad	Descripción	Responsable
4	Solución de fallos.	**Procedimientos para resolver problemas de SNMP** 1. Verificar si el equipo gestionado tiene SOPORTE SNMP. 2. Configurar comunidad SNMP. 3. Asignar permisos. 4. Para probar la funcionalidad SNMP verificar a través de un snmpwalk. **Procedimiento para solucionar problemas de rendimiento de recursos de los equipos gestionado** 1. Verificar como está trabajando cada recurso gestionado mediante Zenoss. 2. Analizar capacidades. 3. Verificar los procedimientos para gestión de rendimiento. PRO-LAN-0003.	Soporte técnico
5	Documentación de fallos	1. Al solucionar un problema el técnico registrara el proceso de realizado en una hoja de control en el que se detalle: a. Fecha. b. Departamento. c. Usuario. d. Descripción del daño. e. Solución ejecutada. f. Si se solucionó o no, o está pendiente la solución. g. Y para constancia de brindad soporte técnico tendrá que firmar el usuario que pidió el soporte así como el técnico que atendió el requerimiento. 2. Se llevará un registro de aquellos equipos que presentan defectos que están provocando problemas constantes. a. Registrará los datos del equipo. b. La frecuencia de fallos. c. El historia de problemas y soluciones dadas.	Soporte técnico.

Flujograma:



Anexos:

HOJA DE SOPORTE TÉCNICO			
Fecha:		Departamento:	
Usuario:			
Descripción del daño:			
Solución ejecutada:			
Cumplido:	Si: ☐ No: ☐ Pendiente: ☐	Nombre del técnico:	
Firma del usuario:		Firma del técnico:	

REGISTROS DE EQUIPOS DEFECTUOSOS.			
Equipo:	**Dirección IP:**	**Frecuencia de fallos**	
Marca:	**Dirección MAC:**	**Semana**	**Día**
Persona Encargada:	**Serie:**	1	1
Departamento:		2	2
		3	3
		4	4
		5	5
		más=	más =

historial problemas	Solución:
Fecha:	
Fecha:	
Fecha:	
Fecha:	

GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

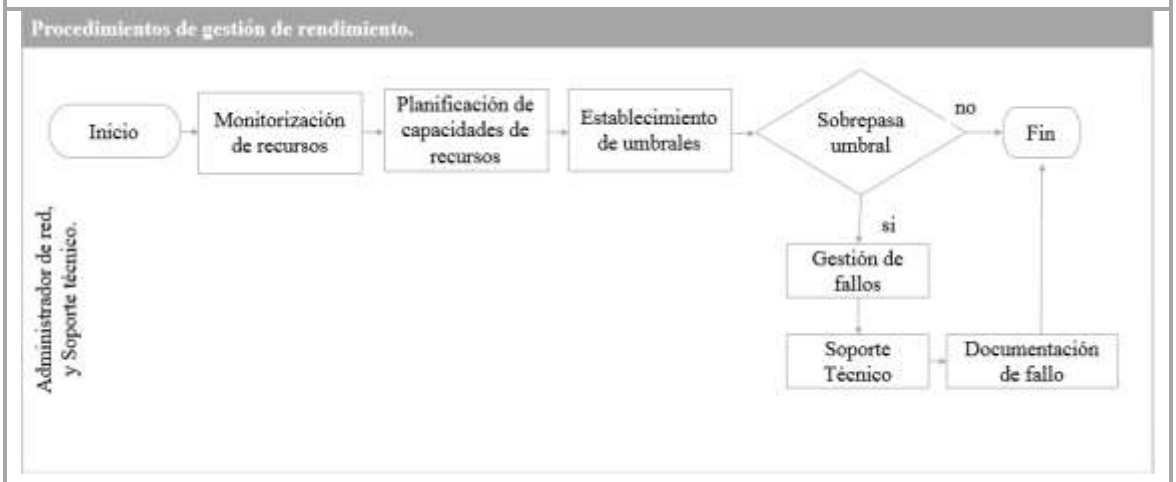
3. Procedimientos para gestión de rendimiento.			**Código:**	PRO-LAN-0003
N°	**Actividad**	**Descripción**		**Responsable**
1	Planificación y aceptación del sistema	1. Monitorear el uso de los recursos a través de Zenoss, el administrador verificará las capacidades de cada recurso, y través de esto se analiza el uso que se está dando a dichos recursos. 2. Proyectar requisitos de la capacidad adecuada para asegura que los recursos de los equipos funcionen adecuadamente.		Administrador de red
2	Establecimiento de umbrales	Al monitorear los recursos, el administrador podrá ver que ciertos dispositivos están sobresaturando el uso de sus recursos, por lo que se determina umbrales para garantizar que los recursos trabajen correctamente. Si sobrepasan los umbrales establecidos, el software de monitoreo emitirá un evento, indicando que se sobrepasó el umbral establecido de uso ya sea de disco duro, memoria RAM, CPU. – Si el uso del disco duro de un servidor, o computador, supera el 80% de su capacidad máxima, se debe respaldar la información en unidades de almacenamiento, como discos duros, o un servidor de archivos que tenga la capacidad suficiente de mantener dicha información.		Administrador de red

Recurso	Umbral
Disco Duro	80%
Memoria RAM	80%
Carga de procesador (CPU)	80%

N°	Actividad	Descripción	Responsable
2	Establecimiento de umbrales	– El uso de la memoria RAM depende del trabajo que realice un servidor o computador, por eso se establece como un valor máximo de trabajo el 80%, previniendo que este provoque que los procesos que se realicen se tornen lentos. El administrador de red, decidirá qué es lo mejor para los usuarios, y servidores de acuerdo a las funciones que se desempeñe, poniendo alternativas como: Uso de sistemas operativos de software libre, que tienen requerimientos de RAM, bajos. Incremento de la capacidad de memoria RAM, si el equipo lo soporta, en el caso de servidores permitirá el manejo de mayor número de usuarios que pueden realizar petición de procesos al servidor. (Hoy, 2012) – La carga de procesador es importante ya que es el núcleo de funcionamiento de un equipo, al establecer el umbral máximo es de 80% de su capacidad, se previene que se produzcan cuellos de botella de los procesos que se ejecutan. La carga de procesador viene de la mano junto a la memoria RAM, y el disco duro, de forma que se coordina el trabajo de manera eficiente. (Magazine, 2008) En caso de que se sobrepase el umbral, el administrador de red deberá tomar medidas, como: Revisión de procesos y eliminación de aquellos que no se solicitaron, ya que muchas veces se ejecutan proceso por defecto que no se usan.	Administrador de red.

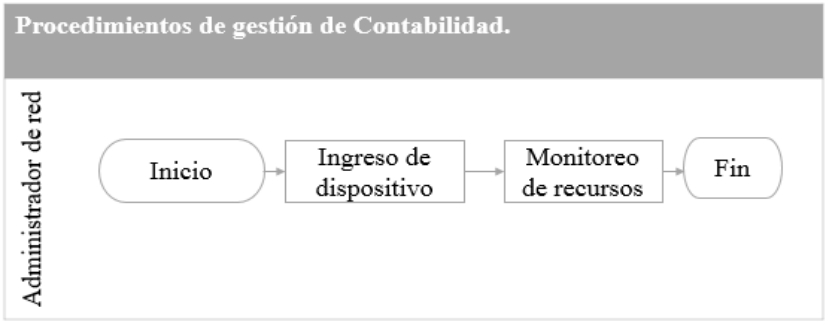
N°	Actividad	Descripción	Responsable
2	Establecimiento de umbrales	Cambio de procesador, de acuerdo al trabajo que desempeñe, existen procesadores de uso básico (athom, celeron, Pentium, AMD E2 o E4) intermedio (core i 3, i5, AMD A3,A8) o avanzado (core i7, AMD A10 o FX). A la vez elegir la memoria RAM adecuada, de 2, 4GB en memoria RAM es suficiente para el uso normal que se les da a las computadoras, y para procesos más avanzados se eligen ente 8 a 16GB, el disco duro dependerá de la cantidad de información que maneje. (Organización de Consumidores y Usuarios, 2015)	Administrador de red.

Flujogramas.



4. Procedimientos para gestión de contabilidad.	Código:	PRO-LAN-0004

N°	Actividad	Descripción	Responsable
1	Manejo de reporte.	La **aplicación de Zenoss** permite manejo de reportes. 1. Diríjase a la pestaña ***Reports***, donde puede ver reportes de los dispositivos gestionados de la red.	Administrador de red.

N°	Actividad	Descripción	Responsable
1	Manejo de reporte.	2. El administrador puede generar los reportes y exportarlos en un formato cvs, en caso de ser necesario. **Zentyal** permite obtener registros uso de internet, Proxy HTTP, IDS/IPS, y también ver los usuarios que hacen uso de la red. – Haga clic en Mantenimiento – Registros – Y seleccione el tipo de registro que desea ver, (Proxy HTTP, IDS/IPS). Para ver los usuarios de la red. – Haga clic en portal cautivo. – Usuarios actuales.	Administrador de red.
2	Manejo de inventarios.	Registrar los equipos de comunicación interconectados a la red en un inventario basado en Excel, donde se registre. a. Equipo b. Modelo c. Serial d. Características físicas del equipo e. Direccionamiento IP estática si es el caso.	Administrador de red.
Flujograma:			
			

GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

3. Procedimientos para la gestión de seguridad.			Código:	PRO-LAN-0005
N°	**Actividad**	**Descripción**		**Responsable**
1	Control de accesos	**1. Equipos de comunicación (servidores, PC, routers inalámbricos, switch administrables, etc):** a. Establecer un usuario y contraseña para administrar el equipo de comunicación que este interconectado en la red local. **2. Equipos de conmutación:** b. Ingresar por cable de consola. c. Averiguar su dirección ip por default, para luego acceder por interfaz web. d. Verificar si tiene soporte ssh, para en un futuro habilitarlo. **3. Acceso a sistema de gestión de red, Zenoss:** Se establece un usuario administrador que tenga el control de todos los campos de gestión de red a través del software. El usuario administrador puede crear otros usuarios que también puedan acceder a la aplicación pero con acceso limitado a la información y visualización de los recursos monitoreados. Para acceder al sistema de gestión de red, se lo realiza en el navegador donde ingresa la IP del servidor y accede mediante su usuario y contraseña.		Administrador de red.

N°	Actividad	Descripción	Responsable
1	Control de accesos	**4. Acceso a sistema de seguridad, Zentyal:** a. ***Interfaz web.*** Únicamente el usuario administrador puede ingresar a la plataforma de Zentyal, a través del navegador debe ingresar la IP o dominio del servidor, e ingresar su usuario y contraseña. b. ***Ssh.*** El administrador puede realizar configuraciones para que se acceda a Zentyal a través de ssh, esta configuración se la realiza en: – Cortafuegos. – Redes internas y redes externas. – Cree la regla. – Permitir el servicio ssh, al rango de direcciones IP que pertenecen a departamento de TIC, para que se acceda únicamente desde cualquiera de esos equipos. Para acceder mediante ssh hágalo a través de la aplicación putty. c. Habilite ssh puerto 22. d. E ingrese la dirección ip del servidor	Administrador de red.

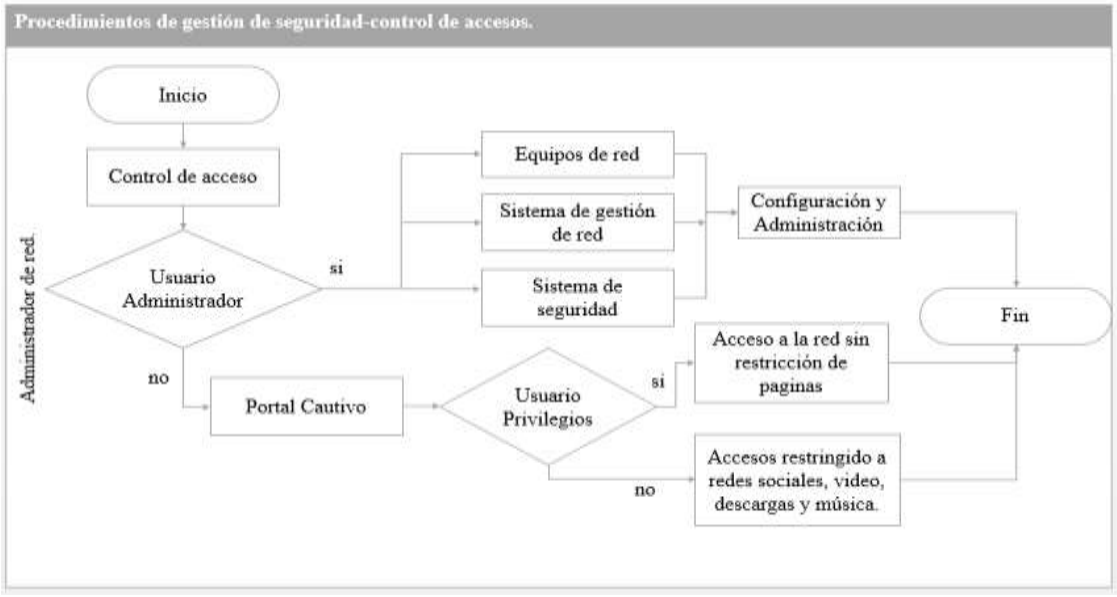
N°	Actividad	Descripción	Responsable
1	Control de accesos	**5. Gestión de usuarios de la red:** **a. Proceso de solicitud:** Al contratar un nuevo funcionario a la municipalidad la dirección de talento humano debe dirigir una solicitud a la dirección de TIC pidiendo que se le registre y asigne un usuario y contraseña para tener los servicios de red brindados a través de la red local. ***b. Administrador.*** Para el manejo y control de acceso de usuarios a los servicios de la red el administrador gestiona usuarios y grupos de usuarios a través de Zentyal mediante Open LDAP. 1. El usuario se crea en base al primer nombre y primer apellido. 2. Y la contraseña aplicada se basa en la combinación de números y letras y símbolos. Creación de grupos y usuarios: – Office. – Usuarios y Computadores. – Gestionar – Cree los grupos de acuerdo a las direcciones del municipio. – Cree usuarios para cada dirección. – Asigne el usuario y contraseña.	Administrador de red y usuarios.

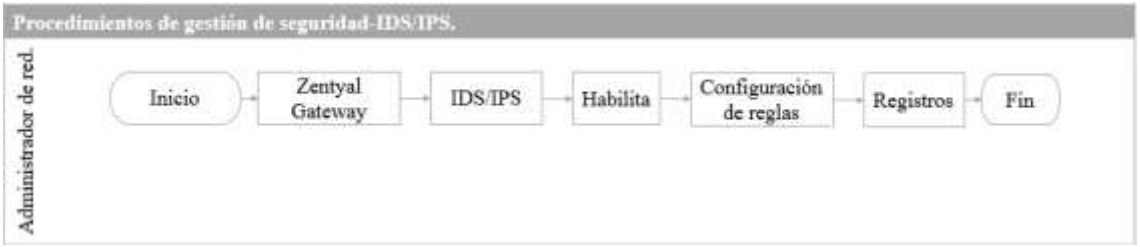
N°	Actividad	Descripción	Responsable
1	Control de accesos	Para que estos ingresen haciendo uso del usuario y contraseña asignada por el administrador se debe activar el portal cautivo, estableciendo a la interfaz de la LAN como interfaz cautiva. – Gateway. – Portal Cautivo. – Habilite la interfaz de la LAN. El administrador puede verificar que usuarios están haciendo uso de la red en: – portal cautivo, – usuarios actuales. ***c. Usuarios.*** Los usuarios deberán abrir su navegador registrar su usuario y contraseña para acceder al internet y servicios brindados por la dirección de TIC a través de la red local. **6. Internet y servicios de red local.** a. ***Usuarios limitados.*** Se restringe el acceso a páginas web, como redes sociales, descargas, videos, música. *b.* ***Usuarios privilegiados.*** Son directores y jefes, los mismos que pueden acceder libremente a páginas de redes sociales, videos, etc. Los usuarios que requieran ser usuarios privilegiados y no sean directores ni jefes deberán emitir un oficio al departamento de TIC, justificando el uso que hacen del internet, y la autorización de su jefe inmediato.	Administrador de red y usuarios.

N°	Actividad	Descripción	Responsable
1	Control de accesos	Para que los usuarios privilegiados tengan acceso libre el administrador debe registrarlos**.** 1. Ingresar a Zentyal. 2. Objetos. 3. Usuarios privilegiados. 4. Ingrese la dirección ip de usuario.	Administrador de red y usuarios.
2	Protección contra intrusos	Se habilita el IDS/IPS en Zentyal, aplicado a las dos interfaces, para que permita detección de intrusos, que fisgoneen en la red. – Gateway. – IDS/IPS. – Habilite las interfaces LAN y WAN. Para verificar la detección de actividades sospechosas vaya a: – Mantenimiento – Consulta de registros – Seleccione IPS y puede ver los eventos que se haya detectado.	Administrador de red.
3	Manejo de Backups	***Zentyal.*** Vaya a: – Sistema – Importar/exportar configuración. – Obtenga su respaldo haciendo clic en copia de seguridad. – Descargue el respaldo y guárdelo en el servidor de archivos.	Administrador de red.

N°	Actividad	Descripción	Responsable
3	Manejo de Backups	***Zenoss*** Vaya a: – Advance. – Backup Y genere un respaldo.	Administrador de red.

Flujograma:





GADIP Cayambe
Sumak Kawsaypak
Juntos por el buen vivir

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL
DEL MUNICIPIO DE CAYAMBE

Cayambe, 15 de julio del 2015

CERTIFICACIÓN

Señores:
UNIVERSIDAD TÉCNICA DEL NORTE
Presente.

De mis consideraciones.-

Me permito certificar por medio de la presente que la Srta. Inuca Gonza Cyntia Maribel con CI. 100324363-9, ha desarrollado su trabajo de tesis con el tema: **ADMINISTRACIÓN Y GESTIÓN DE LA RED DE ÁREA LOCAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CAYAMBE, BASADO EN EL MODELO FUNCIONAL DE GESTIÓN DE RED ISO/OSI CON EL PROTOCOLO SNMP Y USO DE HERRAMIENTAS DE SOFTWARE LIBRE"**, y me es grato informar que se han realizado las pruebas respectivas para probar sus funcionalidades, obteniendo resultados satisfactorios, en beneficio de nuestra institución.

Es todo cuanto puedo certificar, la interesada puede hacer uso de este documento para los fines que lo amerite.

Atentamente,

.....
Ing. Fabián Bautista
Director de Tecnologías de la Información.

GADIP MUNICIPIO DE CAYAMBE
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN