Gestión y monitoreo de la red interna del Gobierno Provincial de Imbabura mediante el modelo de gestión ISO y software libre

Edgar A. Maya, Sara C. Cuchala
Carrera de Ingeniería en Electrónica y Redes de Comunicación, Universidad Técnica del Norte
Ibarra, Ecuador
eamaya@utn.edu.ec
sccuchalav@utn.edu.ec

***Resumen*— El presente proyecto, se ha realizado con la finalidad de brindar un mejor servicio a la ciudadanía garantizando la disponibilidad de la red de la Prefectura de Imbabura, utilizando el modelo de gestión de redes OSI/ISO con sus cinco áreas funcionales: configuración, fallos, contabilidad, prestaciones y seguridad.**

Durante la elaboración de este proyecto, se analizó las definiciones de gestión de red, así como el protocolo SNMP y sus funcionalidades, se realizó una auditoría lógica y de comunicaciones para determinar el estado actual de la red, a continuación, se escogió el software para el monitoreo y se implementó la solución en los equipos del Gobierno Provincial de Imbabura.

***Terminos Indexados*—ISO, NMS, MIB, UDP, SNMP.**

I. INTRODUCCIÓN

La Prefectura de Imbabura es la institución encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial Participativo; fortaleciendo la productividad, la vialidad, el manejo adecuado de sus recursos naturales y promoviendo la participación ciudadana; a fin de mejorar la calidad de vida de sus habitantes.

Es necesario implementar un modelo de gestión y monitoreo de los sistemas de información para la red del Gobierno Provincial de Imbabura de tal manera que el administrador logre detectar las fallas que puedan aparecer en los distintos equipos y servicios de la red.

Mediante el uso de un sistema de gestión de red se conseguirá prestar un mejor servicio a los diferentes usuarios de la red del Gobierno Provincial de Imbabura y facilitar la gestión para el administrador de la red de datos de tal manera que exista mayor eficiencia en su trabajo, y por ende se brindará un mejor servicio a la ciudadanía.

II. FUNDAMENTOS DE GESTIÓN DE REDES

Desde el momento en que las redes se consideran cada vez más una parte esencial y estratégica de las empresas, industrias u otros tipos de instituciones y como resultado de las cada vez mayores dimensiones que están adoptando, resulta más importante su control y gestión con el fin de obtener la mejor calidad de servicio posible.

A. Arquitectura de Gestión de Red

Los sistemas de gestión que existen actualmente, utilizan una estructura básica, conocida como paradigma gestor-agente, cuyo esquema queda reflejado en la Figura 1. Los sistemas de apoyo a la gestión se componen, por lo general:

- Interfaz con el operador o el responsable de la red. Es la interfaz a la información de gestión, a través de la cual el operador puede invocar la realización de operaciones de control y vigilancia de los recursos que están bajo su responsabilidad, es una pieza fundamental en la consecución de un sistema de gestión que tenga éxito. Se puede componer de alarmas y alertas en tiempo real, análisis gráficos y reportes de actividad.
- Elementos hardware y software repartidos entre los diferentes componentes de la red.

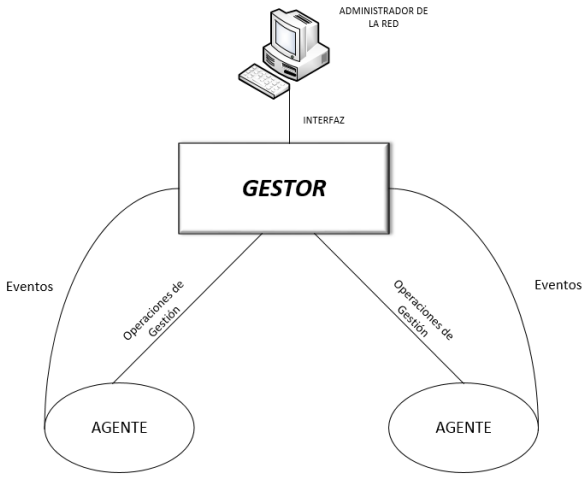

Fig. 1. Arquitectura de gestión de red

Documento recibido en Abril del 2016. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte. E.A. Maya, Docente de la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador. S.C. Cuchala, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (teléfono 5932-955-519; e-mail: sccuchalav@utn.edu.ec).

Los elementos del sistema de gestión de red, bajo el paradigma gestor-agente, se clasifican en dos grandes grupos:

- Los gestores son los elementos del sistema de gestión que interaccionan con los operadores humanos y desencadenan acciones necesarias para llevar a cabo las tareas por ellos invocadas.
- Los agentes, son los componentes del sistema de gestión invocados por el gestor o gestores de la red.

B. Modelo de Gestión FCAPS

Use one space after periods and colons. Hyphenate complex modifiers: "zero-field-cooled magnetization." Avoid dangling participles, such as, "Using (1), the potential was calculated." [It is not clear who or what used (1).] Write instead, "The potential was calculated by using (1)," or "Using (1), we calculated the potential."

La ISO clasifica las tareas de los sistemas de gestión en cinco áreas funcionales:

- Gestión de configuración.
- Gestión de prestaciones.
- Gestión de seguridad.
- Gestión de fallos.
- Gestión de contabilidad.

A continuación se especifican las características de cada una de estas áreas.

1) Gestión de configuración: Es el proceso de obtención de datos de la red y utilización de los mismos para incorporar, mantener y retirar los diferentes componentes y recursos que la integran. Consiste en la realización de tres tareas fundamentales:

- Recolección de datos sobre el estado de la red. Para ello generalmente se emplean dos tipos de herramientas que funcionan de forma automática: las herramientas de autodescubrimiento (auto-discovery) y las herramientas de auto-topología (auto-mapping).
- Cambio en la configuración de los recursos. Todas las configuraciones nuevas realizadas en los dispositivos deben ser documentadas de manera oportuna.
- Almacenamiento de los datos de configuración. Todos los datos obtenidos han de ser almacenados para obtener el inventario de red.

2) Gestión de prestaciones: Tiene como principal objetivo el mantenimiento del nivel de servicio de la red. La gestión de prestaciones basa sus tareas en la definición de unos indicadores de funcionamiento. Es decir, es necesario fijar una serie de criterios que permitan conocer cuál es el grado de utilización de un recurso. Los indicadores más utilizados se clasifican en dos grandes grupos:

- Parámetros de funcionamiento orientados al servicio. Miden el grado de satisfacción del usuario al acceder a los recursos. Los más importantes son la disponibilidad, el tiempo de respuesta y la tasa de error.
- Parámetros de funcionamiento orientados a la eficiencia. Miden el grado de utilización de los recursos. Básicamente son la productividad (throughput) y la utilización.

La gestión de prestaciones consiste en realizar cuatro tareas básicas:

- Recopilación de datos. Inventario de dispositivos y equipos que pertenecen a la red.
- Análisis de datos. Se analizan los datos obtenidos en el inventario.
- Establecimiento de umbrales. Cuando se supera un determinado grado de utilización de un recurso se dispara una alarma.
- Modelado de la red. Se crea un modelo teórico para simular el comportamiento de la red bajo determinadas circunstancias.

3) Gestión de fallos: Permite la localización y recuperación de los problemas de la red. Abarca dos tareas principales:

- Detección e identificación de los fallos. Al aparecer un fallo en la red este debe detectarse y ubicarse de manera eficaz.
- Corrección del problema. Luego de haber detectado el fallo el responsable de la red debe encontrar una solución para el problema de manera rápida, de esta manera se garantiza la disponibilidad de la red.

4) Gestión de seguridad: Ofrece mecanismos que faciliten el mantenimiento de políticas de seguridad. La gestión de seguridad se ocupa de los siguientes puntos:

- Identificación de la información a proteger y dónde se encuentra.
- Identificación de los puntos de acceso a la información.
- Protección de los puntos de acceso.
- Mantenimiento de los puntos de acceso protegidos.

5) Gestión de contabilidad: Tiene como misión la recolección de estadísticas que permitan generar informes de tarificación que reflejen la utilización de los recursos por parte de los usuarios. Requiere la realización de las siguientes tareas:

- Recolección de datos sobre la utilización de los recursos.
- Establecimiento de cuotas.
- Cobro a los usuarios por la utilización de los recursos.

C. Protocolo SNMP

Para monitorear las redes complejas, con todos sus nodos y dispositivos, y poder realizar diagnósticos precisos, se necesita reunir información proveniente de diferentes fuentes. Para facilitar la administración de la red a través del intercambio de información de gestión y el desarrollo de aplicaciones específicas para tal fin, existe el protocolo SNMP (Simple Network Management Protocol – Protocolo simple de administración de la red) utilizado en las redes TCP/IP.

SNMP tiene como objetivos posibilitar las siguientes tareas, las cuales son fundamentales para la administración y el monitoreo de las redes:

- Conseguir información sobre los dispositivos de red.
- Consultar el estado y la configuración de los dispositivos de red.
- Monitorear la actividad de los nodos que conforman la red.
- Analizar el tráfico en los diferentes segmentos de la red y a través de los distintos dispositivos de red.
- Detectar los cuellos de botella en la red y quiénes son los causantes.
- Analizar el rendimiento de la red.
- Generar informes sobre los dispositivos de la red.
- Monitorear variables críticas del funcionamiento de la red.

1) Componentes de SNMP: Una red administrada con SNMP consiste en tres elementos fundamentales: sistema administrador de red, dispositivos administrados y agentes.

- ***Sistema administrador de red (NMS – Network Management System):*** NMS ejecuta aplicaciones que monitorean y controlan los Managed Devices. Los NMS´s proporcionan la mayor parte de recursos de procesamiento y memoria requeridos para la gestión de la red. Uno o más NMS´s deben existir en cualquier red administrada.
- ***Dispositivos administrados (Managed Devices MD):*** Un dispositivo administrado, es un nodo de red que contiene un agente SNMP y que reside en una red administrada, los cuales colectan, almacenan y hacen que la información esté disponible al NMS´s utilizando SNMP. Los Managed Devices, también pueden ser llamados elementos de red, pueden ser routers, servidores de acceso, switch, bridges, hubs, computadoras anfitrionas o impresoras.
- ***Agente:*** Un agente es un módulo de gestión de red que se encuentra en un Manage Device, el cual tiene conocimiento local de la información (memoria, número de paquetes recibidos enviados, direcciones IP, rutas, etc.) y traduce esa información en un formato compatible con SNMP.

2) Versiones SNMP: SNMP determina versiones para satisfacer distintas necesidades que se presentan en el manejo de redes.

- ***SNMPv1:*** El protocolo simple de administración de red, fue diseñado a mediados de los años 80, principalmente fue desarrollado para la gestión de dispositivos (servidores, estaciones de trabajo, enrutadores, conmutadores) sobre una red IP. Se encuentra definido en los siguientes RFCs: RFC 1115[1], RFC 1157[2], RFC 1212[3] Y RFC 1213[4].
- ***SNMPv2:*** Es una evolución de SNMPv1, se encuentra documentado en el RFC 1901[5]. Agrega y mejora algunas operaciones del protocolo. La operación trap de SNMP v2, tiene la misma función que la utilizada en SNMPv1, pero emplea un formato de mensaje diferente y está diseñado para sustituir las trap de SNMPv1.
- ***SNMPv3:*** Es un protocolo de interoperabilidad basado en estándares para la gestión de red se encuentra documentado en el RFC 3410[6]. Proporciona acceso seguro a los dispositivos mediante una combinación de autenticación y encriptación de los paquetes a través de la red, entre sus principales características se tiene: seguridad del mensaje, autenticación y encriptado.

3) MIB (Management Information Base): La Base de Información para Gestión, es un tipo de base de datos que contiene información jerárquica de todos los dispositivos gestionados en una red, se encuentra estructura en forma de árbol. Es parte de la gestión de red definida en el modelo OSI, define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red.

Cada objeto manejado en una MIB tiene un identificador de objeto único e incluye el tipo, nivel de acceso, restricciones de tamaño y la información del rango del objeto.

Los objetos de la MIB se definen usando un subconjunto de ASN.1, las MIB tienen un formato común de modo que aun cuando los dispositivos sean de fabricantes distintos puedan ser administrados con un solo protocolo.

III. Situación Actual de la Red de la Prefectura de Imbabura

Para determinar las características de la Infraestructura de red de la Prefectura de Imbabura, se realizó una auditoría lógica y de comunicaciones, esta información permitirá conocer el estado actual de la red.

El proveedor de servicios mediante un router CISCO 881 se conecta a la red pasando por el Switch CISCO ASA 5520 el cual cumple las funciones de Firewall, a continuación se conecta el Switch principal el mismo que cumple las funciones de CORE, este equipo tiene características y funciones de Capa 3, y es el encargado de recibir todas los enlaces de Conexión de Fibra Óptica entre edificios y entre pisos como se muestra en la Figura 2.

Los switch de acceso, tienen características y funciones de capa 2, son administrables y permiten la interconexión de todos los usuarios a la red de la Prefectura de Imbabura. La Figura 7 muestra la topología física de la red.

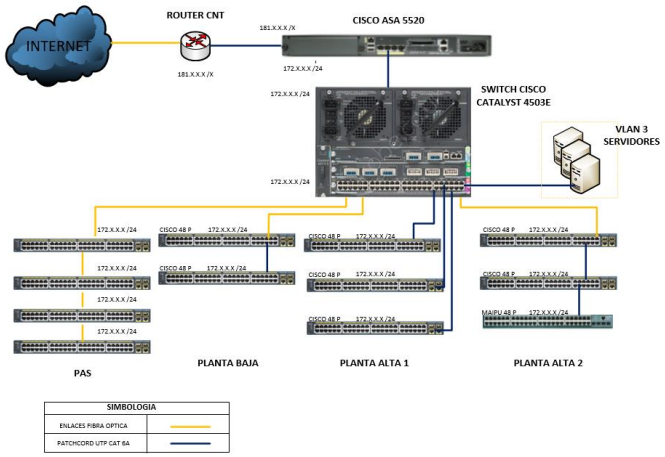

Fig. 2. Topología de la Red del Gobierno Provincial de Imbabura

[1] **RFC 1115:** Mejoramiento de Privacidad de Internet de correo electrónico: Parte III - Algoritmos , Modos y Identificadores

[2] **RFC 1157:** Protocolo Simple de Administración de Red (SNMP)

[3] **RFC 1212:** Definiciones concisas de MIB

[4] **RFC 1213:** Base de información de gestión para la administración de red basadas en TCP/IP

[5] **RFC 1901:** Introducción a comunidades basadas en SNMPv2

[6] **RFC 3410:** Introducción y aplicabilidad de reglas para el marco de gestión de internet.

A. *Cuarto de Comunicaciones*

En cuanto al cuarto de comunicaciones se encuentra ubicado en el primer piso del edificio dentro del Departamento de Tecnologías de la Información, desde este punto parten la interconexión de los enlaces de fibra óptica entre pisos y también el enlace con las oficina del Patronato de Acción Social, y a su vez todas las instalaciones de cableado horizontal. En la Figura 3 se muestra la distribución de equipos activos en el cuarto de comunicaciones de la Prefectura de Imbabura.

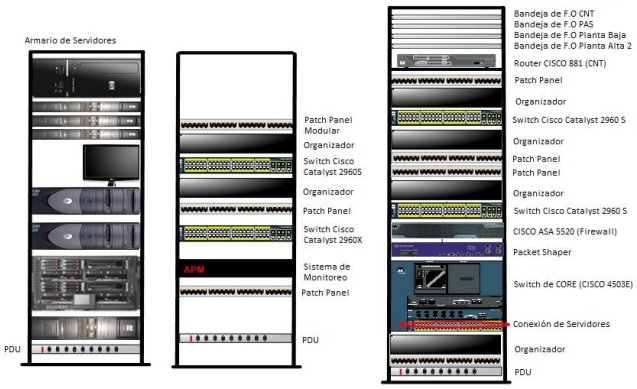

Fig. 3. Distribución de Equipos en el Cuarto de Comunicaciones

B. *Armario de Servidores*

Actualmente en el cuarto de comunicaciones se albergan lo siguientes servidores:

- Servidor de Archivos (Alfresco)
- Servidor Web (Joomla)
- Servidor de Desarrollo de Software (Mantis)
- Servidor de Obtención de Licencias (Arcgis)
- Servidor de Gestión Documental (Quipux)
- Servidor Cloud (OwnCloud)
- Servidor de Camaras
- Servidor de Relojes Biometricos
- Servidor Proxy (Squid)
- Servidor DNS (OpenDNS)
- Servidor Ambiente de Desarrollo
- Servidor Geolocalización
- Servidor Sistema Financiero Contable
- Servidor de Streaming de Video
- Servidor de Telefonía IP
- Servidor DNS (OpenDNS)

Estos servidores se encuentran alojados en distintos equipos, siendo el Chasis HP C3000 Blade System el que alberga a la mayoría de ellos. En la tabla 1 se muestran las características de este equipo.

C. *Definición de Equipos monitoreados*

Con el objetivo de analizar el rendimiento de la red de la Prefectura de Imbabura, se realizará un monitoreo de los diferentes equipos que posee la institución, tanto de la capa de acceso como de la capa de distribución, para esto se consideró los equipos que al tener un mal funcionamiento podrían ocasionar fallas en la red y consumo excesivo de recursos.

Para la capa de distribución se considera al Switch de CORE CISCO 4503-E como el principal elemento a ser monitoreado ya que este permite la conectividad a todos los dispositivos y host que se encuentran alojados en la red, las características de este equipo se muestran en la Tabla 12 y se puede observar su conexión en la red en la topología mostrada en la Figura 7.

Para conocer el estado de la capa de acceso se monitoreara los Switch CISCO 2960-S que permiten la conexión entre pisos del edificio, y realizan la propagación de VLAN's en la red interna de la Prefectura de Imbabura. Las características de estos equipos se muestran en la Tabla 13 y su conexión en la red en la Figura 7.

Los servidores se encuentran especificados en el apartado 2.3.2.6 de la situación actual, se realizará el monitoreo de los servicios descritos a continuación, los cuales fueron solicitados por la Dirección de TIC's.

- Servidor de Archivos (Alfresco)
- Servidor Web (Joomla)

El Servidor Alfresco fue solicitado para ser monitoreado debido a que este necesita constantemente un vaciado de memoria ya que maneja todos los archivos escaneados de obras y contratos que maneja la Prefectura de Imbabura.

En cuanto al Servidor Web, fue escogido ya que es necesario que la página del GPI este constantemente actualizada y en línea, por lo cual debe ser monitoreada, de tal manera que si existe algún problema este pueda ser identificado rápidamente por el administrador de la red.

Luego de haber realizado el análisis de la situación actual de la Prefectura de Imbabura, se procede a la implementación del modelo de gestión ISO en conjunto con la elección del software de monitoreo.

IV. IMPLEMENTACIÓN DEL MODELO DE GESTIÓN

Para la implementación del modelo de gestión propuesto por la ISO se aplican sus cinco áreas funcionales.

A. *Gestión de Configuración*

La gestión de configuración puede realizarse luego de haber analizado la situación actual de la red interna de la Prefectura de Imbabura, esta contiene, la elección del servidor a implementarse y la configuración del software de gestión, lo que permitirá documentar y registrar los cambios realizados en los elementos de la red.

1) Elección del software de monitoreo: Actualmente en el mercado existen varios tipos de software para la gestión y monitoreo muchos de ellos son gratuitos y otros tienen versiones de pago. Es necesario distinguir cuáles de ellos brindan las mejores prestaciones de acuerdo a los requerimientos que la empresa o institución necesite.

En la tabla I se muestran varios tipos de software de monitoreo identificando las prestaciones que estos brindan.

TABLA I
COMPARACIÓN DE SOFTWARE DE MONITOREO

NOMBRE	CACTI	ZENOSS	NMAP	OPMANAGER	PANDORA FMS	NAGIOS	PRTG NETWORK MONITOR
ESTADISTICAS	Si	No	No	Si	Si	Si	Si
GRAFICAS	Si	No	No	Si	Si	Si	Si
BASE DE DATOS	RRDtools MySQL	RRDtools MySQL	RRDtools MySQL	MySQL MSSL	MySQL	MySQL	MySQL MSSL
AGENTES	No	No	Si	Si	Si	Si	Si
SNMP	Si	Si	Si	Si	Si	Usando Plugins	Si
PLUGINS	Si	Si	No	Si	Si	Si	Si
ALERTAS	Si	Si	Si	Si	Si	Si	Si
APLICACIÓN WEB	Control Total	Control Total	Control Total	Control Total	Control Total	Solo Visualiza	Control Total
SEGURIDAD	No	No	No	No	Acceso Regulado	No	No

2) Estándar IEEE 29148: Define el estándar 29148 (Systems and software engineering -- Life cycle processes --Requirements engineering), como aquel que "permite manejar los procesos y dentro de éstos las actividades que se deben llevar a cabo para una buena obtención de requerimientos, que es precisamente una de las ventajas de utilizar la metodología.

Este estándar fue creado en el 2011 en sustitución al IEEE 830. Contiene provisiones para los procesos relacionados con la ingeniería de requerimientos para sistemas, productos de software y servicios.

Su objetivo principal es definir la construcción de requerimientos de un sistema, analizando sus atributos y características, con la finalidad de estudiar las aplicaciones recursivas de los requisitos a lo largo de un ciclo de vida.

Proporciona orientación adicional en la aplicación de procesos de ingeniería y gestión de requerimientos para las actividades relacionados con otras normas. Puede ser utilizado de forma independiente para analizar el software a instalarse.

- ***SRS (Software Requirements Specifications):*** En el caso particular de este proyecto se utilizó el SRS por su acrónimo en ingles (Software Requirements Specification), para identificar los requerimientos que la Prefectura de Imbabura necesita para la implementación de un software de gestión.

3) Software elegido: El monitoreo de una red es un proceso complejo y por parte de la institución se solicitó una herramienta que sea amigable con el usuario, que permita una instalación sin demasiadas complicaciones y que cuente con información suficiente para solucionar cualquier problema que se pueda presentar en el sistema.

Tomando en cuenta las características solicitadas por el administrador de la red de la Prefectura de Imbabura mostradas en el SRS, y la Tabla I, se realiza una comparación entre varios software de acceso gratuito que brinda el mercado.

Se escoge el software Pandora FMS, porque su instalación es sencilla en referencia a otros software, además posee una interfaz Web que no tan sólo permite visualizar los eventos de la red, sino tambien manejar y configurar de manera gráfica la mayoria de sucesos y alertas que puedan suceder.

También permite manejar de manera eficiente el protocolo SNMP, ya que posee un conjunto de herramientas para crear módulos de forma remota y reconoce automáticamente los dispositivos y equipos que tienen activado este protocolo.

Con este software el administrador será capaz de crear reportes y gráficos sobre el estado de la red, además podrá filtrar los tipos de notificaciones, para poder solucionar las más criticas de manera rápida.

4) Arquitectura de Pandora FMS: Pandora FMS tiene varios elementos, los servidores se encargan de recolectar y procesar los datos. Estos, introducen los datos recolectados y procesados en la base de datos. La consola es la parte encargada de mostrar los datos presentes en la base de datos y de interactuar con el usuario final.

Los agentes son aplicaciones que corren en los sistemas monitorizados (servidores o dispositivos de red), y recolectan la información para enviarla a los servidores de Pandora FMS.

Los servidores de Pandora FMS son los elementos encargados de realizar las cmprobaciones existentes. Ellos las verifican y cambian el estado de las mismas en función de los resultados obtenidos. También son los encargados de disparar alertas que se establezcan para controlar el estado de los datos.

Pueden existir servidores simultáneos, uno de ellos es el servidor principal y el resto de los servidores son servidores esclavos. Aunque exista un servidor esclavo y uno maestro, todos trabajan simultáneamente. La diferencia entre ambos es que cuando un servidor del mismo tipo se cae el servidor maestro se encarga de procesar todos los datos que tenía asociado el servidor que se ha caído.

Pandora FMS gestiona automáticamente el estado de cada servidor, su nivel de carga y otros parámetros. El usuario puede monitorizar el estado de cada servidor, a través de la sección de estado de servidores de la consola web.

La consola web de Pandora FMS es la interfaz de usuario de Pandora FMS. Esta consola de administración y operación permite a diferentes usuarios, con diferentes privilegios, controlar el estado de los agentes, ver información estadística, generar gráficas y tablas de datos así como gestionar incidencias con su sistema integrado. También es capaz de generar informes y definir de forma centralizada nuevos módulos, agentes, alertas y crear otros usuarios y perfiles.

Pandora FMS utiliza una base de datos MySQL. Mantiene una base de datos asíncrona con todos los datos recibidos, realizando una unión temporal de todo lo que recibe y normalizando todos los datos de las diversas fuentes de origen. Estos datos se gestionan automáticamente desde Pandora FMS, llevando a cabo un mantenimiento periódico y automático de la base de datos, esto permite que Pandora FMS no requiera ningún tipo de administración de base de datos ni proceso manual asistido por un operador o administrador.

En la Figura 4 se muestra el modelo de la arquitectura del software.

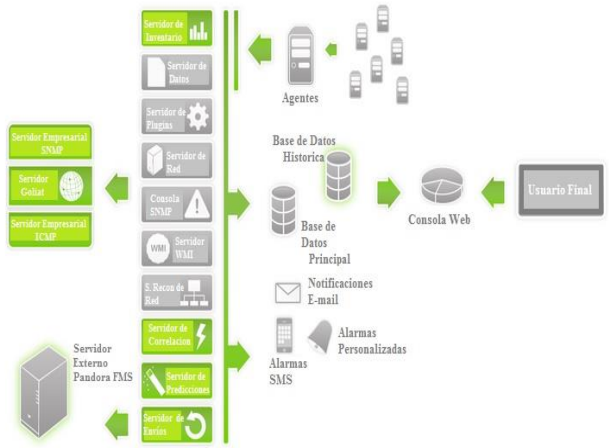

Fig. 4. Arquitectura de Pandora FMS

5) Instalación del software: Para la utilización de Pandora FMS en una red como la que posee la Prefectura de Imbabura es necesario que el equipo en el cual se instale el software tenga las siguientes características:

- 3GB de RAM
- CPU de un sólo núcleo a 2GHz de reloj.
- Disco duro rápido, 7200rpm o equivalente.

De acuerdo a los requerimientos del software el administrador de la red de la Prefectura de Imbabura permitió la instalación del mismo en el Equipo HP PROLIANT DL360.

Este equipo tenía previamente instalado el Sistema Operativo CentOS 6.7 ya que en el se encuentra el servidor de geolocalización.

Para iniciar con la instalación se debe tener previamente los siguientes paquetes activos en el sistema operativo.

- Apache
- MySQL
- Postfix

- ***Configuración consola Pandora FMS:*** La configuración de la Consola de Pandora FMS se realiza de forma gráfica en cualquier navegador Web, para esto se debe colocar la dirección IP del servidor Pandora que es la que por defecto nos otorga la red de esta manera http://ipdelhost.pandora_console.

Dentro del navegador se configura los detalles de la base de datos de MySQL, de tal manera que Pandora FMS se instale automaticamente con todos los datos proporcionados.

- ***Configuración agente Pandora FMS:*** La configuración del agente Pandora es necesaria en los equipos de servidores, dependiendo del Sistema Operativo que estos posean, en servidores Linux la configuración se realiza por medio de la consola y en Servidores Windows esta es de manera gráfica.
  Los paquetes para la instalación en Linux y los archivos .exe para la instalación en Windows del agente se los puede encontrar en el Sitio Oficial de Descargas para Pandora FMS http://pandorafms.com/Community/download/es.

- ***Configuración Switch de CORE:*** La primera tarea a realizar para iniciar la configuración de este equipo es conocer si el protocolo SNMP está instalado en el equipo, a continuación habilitar las traps para el envío de notificaciones. Después de haber configurado SNMP es necesario realizar las configuraciones de monitoreo en la consola de Pandora FMS.
- ***Configuración Switch 2960***: Para realizar la configuración de los Switch de acceso 2960 se realizan los mismos pasos que en el Switch de CORE, teniendo en cuenta que SNMP debe estar habilitado correctamente en cada uno de estos equipos, para de esta manera poder crear los módulos para el monitoreo.
- ***Configuración equipos servidores LINUX:*** Primero se debe instalar el archivo rpm descargado de la página oficial de Pandora FMS, luego editar el archivo de configuración con la IP del servidor. En este archivo vienen predeterminados ciertos servicios para monitorear pero también se puede añadir más de acuerdo a las necesidades de monitoreo de la red.
  Despues de haber realizado estas configuraciones en el servidor se debe dirigir a la Consola de Pandora FMS en donde se puede observar que el servidor se añade automáticamente debido a la opción recontask de Pandora que permite realizar un barrido automático de todos lo equipos que tienen el agente en la red
- ***Configuración equipos servidores WINDOWS:*** La configuración del agente en Windows es sumamente sencilla ya que tan solo se debe descargar el mismo de la web oficial de Pandora FMS, e instalar el archivo ejecutable.

B. Gestión de fallos

Este tipo de gestión permite mantener un funcionamiento más óptimo de los elementos que conforman la red, trata de proteger que la red sufra de fallas que afecten un equipo o un servicio. Dentro de esta área se determina como localizar, diagnosticar y corregir problemas en los equipos de la red.

También se muestra la configuración de las alertas en el software Pandora FMS las cuales permiten el envío de notificaciones de fallos por correo electrónico al administrador de la red.

1) Proceso de Solución de fallos

- ***Identificación:*** La consola de Pandora FMS muestra de manera clara los problemas que afecten a cualquier dispositivo o equipo de la red, de la misma forma alerta al administrador sobre algun fallo que se produzca. De esta manera para identificar cualquier suceso se deben seguir los siguientes pasos:
  - ✓ Monitoreo de la consola de Pandora FMS, para detectar los equipos que se encuentren activos o sin fallas (color verde)
  - ✓ Cuando aparezca una alerta en el dispositivo, sea de advertencia (color amarillo) o crítica (color rojo), se debe identificar el evento, nombre del agente y la fecha.

- ***Aislamiento de la falla:*** Se debe aislar el dispositivo que provoca el problema, obtener la información del usuario sobre las actividades que realizó antes y durante la falla, además es necesario que los usuarios informen al administrador de red y no traten de arreglar ellos solos la falla producida.
- ***Reacción ante la falla:*** El personal encargado de la administración de red debe seguir los siguientes pasos al producirse una falla:
  - ✓ Asignación de recursos humanos y tecnológicos para resolver la falla.
  - ✓ Determinación de áreas y niveles críticos
  - ✓ Determinar la incidencia de los fallos
- ***Solución de la falla:*** Luego de haber detectado, aislado y reaccionado de una manera efectiva cuando apareció la falla, se procede a hallar su solución partiendo desde la opción más sencilla hasta la más compleja. Los procesos que se realizaron para la resolución de fallos deben documentarse de manera adecuada.
- ***Alertas de Pandora FMS:*** Una alerta es la reacción del servidor de Pandora FMS a un valor «fuera de rango» de un módulo, la cual es configurable y puede consistir en enviar un correo electrónico o un SMS al administrador, enviar un trap SNMP, redactar el incidente en el registro del sistema, etc. En el caso de la Prefectura de Imbabura se realizará el envio de correo electrónico al administrador.
  Las alertas de Pandora FMS están formadas como se observa en la Figura 5.

Fig. 5. Estructura de alertas de Pandora FMS

- ***Configuración de alertas por correo electrónico:*** Para realizar esta configuración es necesario tener instalado en el sistema el paquete Postfix y además tener una cuenta de correo electrónico de Gmail, ya que Pandora FMS utiliza el smtp de este servidor de correo para evitar que se realicen negociaciones extras durante el envío de las alertas.

C. *Gestión de prestaciones*

En esta área se realiza una medición del rendimiento de los recursos de la red, mediante el constante monitoreo de los equipos, además se entregó el manual de administrador, al responsable de la red, este contiene todas las configuraciones realizadas para el funcionamiento del Servidor Pandora FMS.

En la figura 6 y 7 se puede observar el ejemplo del monitoreo del servidor Web.

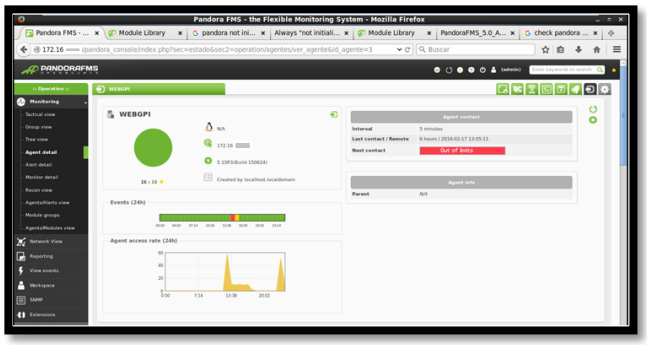

Fig. 6. Servidor Web Activo en Consola Pandora FMS

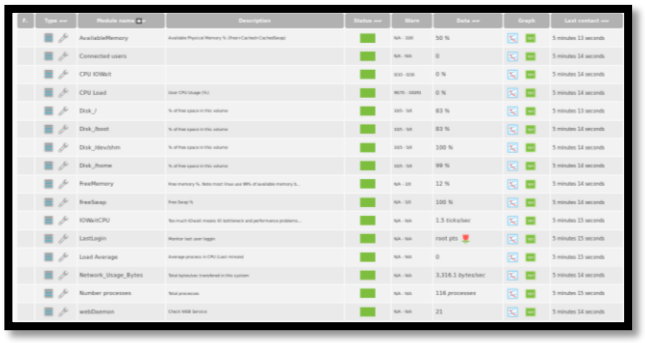

Fig. 7. Servicios monitoreados del Servidor Web

D. *Gestión de contabilidad*

Dentro de esta área se realiza el registro de todos los dispositivos que ingresan tanto a la red como al sistema de monitoreo los cuales deben cumplir con las configuraciones necesarias para evitar fallos imprevistos en la red.

Esto será documentado en el documento de Excel que la Dirección de Tecnologías de información ya poseía anteriormente. Pandora FMS permite que se registren todos los dispositivos en su sección de agentes monitoreados, aquí se guarda un registro de cada uno de los equipo que se encuentran ingresados en el software. Esto se indica en la Figura 8.

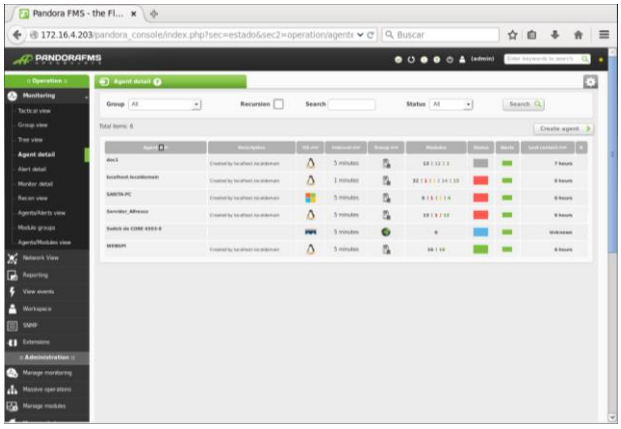

Fig. 8. Agentes monitoreados en consola Pandora FMS

E. *Gestión de seguridad*

En cuanto a la parte del modelo FCAPS que concierne a la seguridad se determinó que solo el administrador de la red pueda tener acceso al Servidor de Pandora FMS, para esto se realizó el cambio de la contraseña por defecto que brinda Pandora al instalar el sistema.

1) Políticas de seguridad: Para garantizar que tanto los dispositivos de red, equipos e información de la red de la Prefectura de Imbabura sean precautelados, en conjunto con el administrador de la red se definió las siguientes políticas de seguridad:

- El acceso a los dispositivos de red debe ser posible solo bajo una contraseña asignada al administrador de la red, para que el permita el acceso y administración remota cuando lo crea necesario.
- El establecimiento de políticas de gestión permiten asegurar un accionar de manera eficiente cuando exista algún cambio o violación de seguridad dentro de la infraestructura de red.
- Es necesario definir acuerdos de confidencialidad para salvaguardar la información crítica que maneja la red de la Prefectura de Imbabura.
- Es fundamental seguir de manera ordenada el manual de procedimientos para evitar vulnerabilidades en la red.

F. Políticas de gestión para el monitoreo de la red:

Las políticas de gestión, están fundamentadas en las áreas funcionales del modelo de gestión del estándar ISO y son dirigidas, en el caso de la Prefectura de Imbabura al Jefe de Procesos quien es el responsable del manejo de la red, el cual tiene el compromiso de cumplirlas, para asegurar la disponibilidad y buen manejo de los equipos.

Las políticas de gestión presentadas a continuación fueron establecidas luego de haber realizado el estudio de las áreas funcionales del estándar ISO y la auditoría lógica y de comunicaciones de la red interna de la Prefectura de Imbabura.

Estas políticas cumplen la función de generar reglas para el buen funcionamiento del modelo de gestión, de tal manera que el encargado del manejo de la red pueda actuar de forma ordenada e imediata frente a cualqueir inconveniente que presente el entorno de los dispositivos de red, garantizando así la disponibilidad de la red y los servicios prestados a la ciudadanía.

Las políticas de gestión también se relacionan directamente con la implementación del software de gestión y el manual de procedimientos.

*1) Políticas para la gestión de la red interna:*Estas políticas permitirán que la Prefectura de Imbabura acepte este documento, y se comprometa a seguirlo de manera ordenada.

2) Políticas para la gestión de configuración: En cuanto a la gestión de configuración se indican las políticas para la configuración de software, equipos y dispositivos de red.

- Ingreso de dispositivos de red al software de gestión
- Configuración de dispositivos de red
- Configuración de equipos de servidores Linux
- Configuración de equipos de servidores Windows
- Documentación de configuraciones

3) Políticas para la gestión de fallos: Las políticas de la gestión de fallos muestran los pasos a seguir cuando exista algún problema en la red.

- Manejo de fallos
- Manejo de umbrales
- Notificación de eventos

4) Políticas para la gestión de contabilidad: Dentro de la gestión de contabilidad las políticas determinan como debe realizarse el inventario de equipos y dispositivos de red.

- Parámetros de Monitoreo

5) Políticas para la gestión de prestaciones: Dentro de esta parte del modelo ISO las políticas determinan la forma de monitoreo y los reportes a recoger de la red.

- Recolección de datos de rendimiento de la red
- Generación de reportes

6) Políticas para la gestión de seguridad: Estas políticas permiten definir la manera de acceder tanto al software, como a los dispositivos gestionados. Además de normas para el control de acceso a usuarios

- Control de acceso al software
- Control de acceso a los dispositivos gestionados
- Control de acceso a usuarios

G. Manual de procedimientos para la gestión de configuración

La Dirección de TIC's de la Prefectura de Imbabura tiene la obligación de mantener funcionales las tareas informáticas que se realizan dentro de sus diferentes dependencias, para brindar un buen servicio d a la ciudadanía, por esta razón los equipos y dispositivos de red deben mantener altos niveles de funcionamiento y disponibilidad.

El presente manual de procedimientos está estructurado en base a cada área de gestión de red determinadas por el estándar ISO, el cuál deberá ser utilizado por el administrador de red para diagnosticar y corregir problems de manera oportuna.

1) Manual de procedimientos para la gestión de configuración:

- Ingreso de dispositivos de red al software de gestión
- Configuración de dispositivos de red
- Configuración de equipos servidores LINUX
- Configuración de equipos servidores WINDOWS
- Documentación de configuraciones

2) Manual de procedimientos para la gestión de fallos:

- Detección de fallo
- Aislamiento del fallo
- Documentación

3) Manual de procedimientos para la gestión de contabilidad:

- Inventario de recursos de la red
- Características de los dispositivos
- Ingreso al sistema de gestión

4) Manual de procedimientos para la gestión de prestaciones:

- Recolección de datos de rendimiento de la red
- Generación de reportes
- Entrega de manuales

5) Manual de procedimientos para la gestión de seguridad:

- Control de acceso al software
- Control de acceso a los dispositivos gestionados
- Control de acceso a usuarios

V. CONCLUSIONES

La implementacion de un modelo de gestión ISO en la red interna de la Prefectura de Imbabura, es de gran importancia ya que debido a la disponibilidad que deben mantener los equipos de la misma, el administrador sintió la necesidad de un software que le permitiera la supervisión y mantenimiento del sistema, de esta manera se puede brindar un mejor servicio tanto a los usuarios internos como a la ciudadanía en general.

Gracias al análisis del modelo de gestión ISO y el protocolo SNMP se logró identificar las 5 áreas de gestión indispensables para un correcto manejo de equipos y servicios, esto permitió utilizarlas en la implementación del software de acuerdo a las necesidades que presento la infraestructura de red de la Prefectura de Imababura.

Gracias a la ayuda del personal de la Dirección de Tecnologías de la Información se pudo identificar la areás criticas que debian tener prioridad al ser monitoreadas, además se brindo acceso a cada uno de los equipos para determinar si estaba habilitado el protocolo SNMP, para esto se identifico las caracteristicas y funciones de cada uno.

A través del formato establecido por el estándar IEEE 29148 se determinó que el software a utilizarse es Pandora FMS, herramienta que proporciona soluciones para un manejo óptimo de las partes que componen la infraestructura red, brindando al administrador las funciones necesarias en tiempo real y con un interfaz gráfica de las opciones para gestión y monitoreo.

En cuanto a las jerarquías de red se tomó en cuenta que las notificaciones que tienen mayor prioridad son las del switch de acceso, para luego tomar en cuenta los switch de distribución y las alertas que puedan generar los servidores serán importantes pero no tienen la mayor prioridad, para esto se utilizó la opción de Pandora para el envió de correo eletrónico al administrador de la red, en cuanto se generen alertas de advertencia y críticas.

Luego de la implementación del servidor Pandora FMS se elaboró un manual de procedimientos de las áreas funcionales del modelo de gestión ISO, utilizando políticas de gestión que permiten al administrador de la red utilizar estos procesos de manera adecuada, este documento fue revisado por el Director del Departamento de Tecnologías de la información, y tuvo aceptación ya que permitirá manejar de forma mas ordenada el funcionamiento de los recursos de la red.

Se realizaron pruebas de funcionamiento en los equipos solicitados por el administrador de la red y se pudo identificar como se comporta el Software Pandora FMS en cuanto al envío de alertas y generación de reportes, lo cuál ayuda al administrador en la supervisión y mantenimiento de los servicios y equipos de red.

En cuanto al análisis de factibilidad técnica se pudo valorar el recurso de hardware, software y humano de la Prefectura de Imbabura y se lleg a la conclusión que la implementación del proyecto es de suma importancia para un manejo adecuado de la red, garantizando su disponibilidad en momentos críticos.

REFERENCIAS

Ayala Yandún, V. (2015). Modelo de gestión de red funcional en la red local de datos del Gobierno Autónomo Descentralizado de San MIguel de Ibarra basado en el estándar ISO. Ibarra.

Barba Martí, A. (1999). Gestión de Red. Barcelona: Editorial Universidad Politécnica de Cataluña.

Bastidas, J., Contreras , Y., Galito, Y., Ochoa, A., Pulido , Y., & Romero, R. (2011). FCAPS. Caracas: Escuela Técnica Militar “Núcleo Comunicaciones y Electrónica”.

CISCO. (2013). Catalyst 4500 Series Switches. Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/data_sheet_c78-530856.pdf

CISCO. (Mayo de 2013). Catalyst 4503-E. Obtenido de http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1982.pdf

CISCO. (19 de Febrero de 2013). CISCO ASA 5520. Obtenido de http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1932.pdf

CISCO. (2014). Cisco 880 Series Integrated Services Routers. Obtenido de http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.pdf

CISCO. (2015). Cisco Line Cards. Obtenido de http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-4500-series-line-cards/product_data_sheet0900aecd802109ea.pdf

CISCO. (2016). Cisco Catalyst 2960-X Series Switches. Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.pdf

CISCO. (s.f.). Cisco Catalyst 2960 Series Switches. Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html

DELL. (Mayo de 2006). Servidor DELL PowerEdge 2900. Obtenido de http://www.dell.com/downloads/emea/products/pedge/es/PE2900_Spec_Sheet_Quad.pdf

Ebah Comunidad. (s.f.). Obtenido de Protocolo de Gestion de Redes: http://www.ebah.com.br/content/ABAAAfctoAG/snmp

Hewlett Packard Enterprise. (25 de Noviembre de 2015). HPE MSA P2000 G3 MSAS. Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04168365.pdf

Hewlett Packard Enterprise. (22 de Enero de 2016). HPE BladeSystem c3000 Enclosure. Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04128340.pdf

Hillar, G. (2004). Redes: Diseño, Actualización y Reparación. Buenos Aires: Hispano Americana S.A. - H.A.S.A. .

HP. (Marzo de 2003). Servidor Proliant ML370 G3. Obtenido de http://h10032.www1.hp.com/ctg/Manual/c00690216.pdf

HP. (14 de Octubre de 2011). HP Proliant DL360 G6. Obtenido de http://www.nts.nl/site/html/modules/pdf/Server/HP%20Proliant%20DL360G6.pdf

HP. (1 de Marzo de 2013). HP Proliant BL460c G7 Server Blade. Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04128282.pdf

HP. (Agosto de 2013). HP Proliant BL460c G8. Obtenido de http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-9690ENW.pdf

IEEE. (2011). IEEE Standard. Obtenido de https://standards.ieee.org/findstds/standard/29148-2011.html

MAIPU. (s.f.). MyPower S3100 Series Switch. Obtenido de http://www.intelek.cz/db/repository.nsf/v/FBB689D5416D4292C125774400257B9C/$file/Datasheet_Maipu_Switch_S3100_Series.pdf

Master Magazine. (2015). Definición de MySQL. Obtenido de http://www.mastermagazine.info/termino/6051.php

Millán Tejedor, R. (1999). Consultoría Estratégica en Tecnologías de la Información y la Comunicación. Obtenido de http://www.ramonmillan.com/tutoriales/gestionred.php

Pandora FMS Enterprise. (2015). Pandora Documentation. Obtenido de Arquitectura de Pandora FMS: http://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Arquitectura#Base_de_datos_de_Pandora_FMS

Pandora FMS Enterprise. (2015). Pandora Documentation. Obtenido de Guía de administración (Versión en Español): http://wiki.pandorafms.com/index.php?title=Pandora:Documentation

Pandora FMS. (s.f.). Pandora Documentation. Obtenido de http://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Alertas#Introducci.C3.B3n

Prefectura de Imbabura. (2015). Prefectura de Imbabura. Obtenido de http://www.imbabura.gob.ec/

Sosa, V. (2013). Management Information Base. Obtenido de http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf

Zerga, D. (27 de Junio de 2011). SNMP. Obtenido de Tipos de Mensaje: http://protocolo-snmp.blogspot.com/2011/06/tipos-de-mensaje.html

Zerga, D. (26 de Junio de 2011). SNMP. Obtenido de Versiones de SNMP: http://protocolo-snmp.blogspot.com/2011/06/versiones-de-snmp.html

Edgar A. Maya nació el 22 de Abril de 1980, Obtuvo el título de Ingeniero en Sistemas Computacionales de la Universidad técnica del Norte (2006), posee un Diplomado Superior en Investigación (2009) y el título de Magister en Redes de Comunicaciones (2014). Obtuvo las certificaciones como instructor de la Academia CISCO-UTN en los cuatro niveles de CCNA e IT Essentials en la Academia CISCO ESPOL de la ciudad de Guayaquil. Ha participado en varios seminarios, talleres, y cursos de especialización con 1146 horas de formación académica profesional y en proyectos de investigación. Actualmente se desempeña como docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la FICA en la Universidad Técnica del Norte y como instructor de la Academia CISCO-UTN.

Sara C. Cuchala nació el 13 de Octubre de 1986, realizó sus estudios primarios en la Escuela “4 de Julio”. En el año 2004 obtuvo su título de Bachiller en ciencias especialización físico matemáticas en el colegio “Liceo Aduanero”. Actualmente, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.