UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"GESTIÓN Y MONITOREO DE LA RED INTERNA DEL GOBIERNO PROVINCIAL DE IMBABURA MEDIANTE EL MODELO DE GESTIÓN ISO Y SOFTWARE LIBRE"

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

AUTOR: SARA CAROLINA CUCHALA VÁSQUEZ

DIRECTOR: ING. EDGAR MAYA

IBARRA-ECUADOR

2016

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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 DEL CONTACTO	
Cédula de Identidad	100315597-3
Apellidos y Nombres	Cuchala Vásquez Sara Carolina
Dirección	Pedro Rodríguez 1-81 y Eusebio Borrero
E-mail	sccuchalav@utn.edu.ec
Teléfono Fijo	062955519
Teléfono Móvil	0969058397
DATOS DE LA OBRA	
Título	"GESTIÓN Y MONITOREO DE LA RED INTERNA DEL GOBIERNO PROVINCIAL DE IMBABURA MEDIANTE EL MODELO DE GESTIÓN ISO Y SOFTWARE LIBRE"
Autor	Cuchala Vásquez Sara Carolina
Fecha	
Programa	Pregrado
Título por el que se aspira:	Ingeniería en Electrónica y Redes de Comunicación
Director	Ing. Edgar Maya

2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, SARA CAROLINA CUCHALA VÁSQUEZ, con cédula de identidad Nro. 100315597-3, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma 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 de 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 titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, al 3 día del mes de Marzo del 2016

……

Sara Carolina Cuchala Vásquez

100315597-3

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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

Yo, SARA CAROLINA CUCHALA VÁSQUEZ, con cédula de identidad Nro. 100315597-3, 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 autor del trabajo de grado denominado: "GESTIÓN Y MONITOREO DE LA RED INTERNA DEL GOBIERNO PROVINCIAL DE IMBABURA MEDIANTE EL MODELO DE GESTIÓN ISO Y SOFTWARE LIBRE", que ha sido desarrollado para optar el título de Ingeniería en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente. En mi condición de autor me reserva 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, al 3 día del mes de Marzo del 2016

.....

Sara Carolina Cuchala Vásquez

100315597-3

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Sara Carolina Cuchala Vásquez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte

……

Sara Carolina Cuchala Vásquez

100315597-3

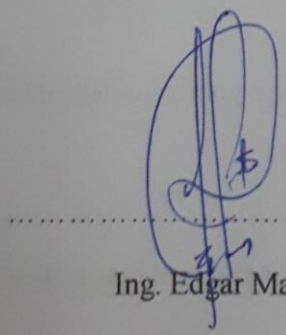
UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que la Tesis "GESTIÓN Y MONITOREO DE LA RED INTERNA DEL GOBIERNO PROVINCIAL DE IMBABURA MEDIANTE EL MODELO DE GESTIÓN ISO Y SOFTWARE LIBRE" ha sido realizada en su totalidad por la señorita: SARA CAROLINA CUCHALA VÁSQUEZ portador de la cédula de identidad numero:

100315597-3



.....

Ing. Edgar Maya.

Director de Tesis

AGRADECIMIENTO

Agradezco, ante todo a Dios, por ayudarme cada día en mi etapa estudiantil, hasta la culminación de este proyecto para cumplir el objetivo de graduarme como Ingeniera en Electrónica y Redes de Comunicación.

A mis padres, que cada día de una u otra manera supieron entenderme y apoyarme en toda esta etapa, por su paciencia y sabiduría, un millón de gracias.

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 y valores, para crecer como buenos profesionales. A mi director de tesis Ing. Edgar Maya, por su paciencia, guía y apoyo para el desarrollo de mi tesis.

De manera muy especial quiero expresar mi agradecimiento a la Dirección de TIC's de la Prefectura de Imbabura, Ing. Fernando Miño, Ing. Jaime Chuga, Ing. Roberto López, Ing. Viviana Tapia, ya que sin su colaboración no hubiera sido posible la finalización de este proyecto.

A mi persona especial Andrés, con su cariño y apoyo incondicional supo darme la fuerza para seguir adelante.

A todos mis amigos, que siempre tuvieron palabras de apoyo para lograr la realización de este proyecto.

DEDICATORIA

Este proyecto está dedicado a mis padres que con su sabiduría, entrega y dedicación han sabido motivarme toda la vida.

Mi padre cuya experiencia en su vida diaria me enseñó sobre todas las cosas a ser honesta y por sobre todo ética profesional y a no mirar por encima a los demás.

Mi madre, con su amor y comprensión ha sido mi mejor amiga en cada una de las etapas de mi vida.

Sarita Cuchala Vásquez

CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

Anexo A

Anexo B

Anexo C

RESUMEN

El presente proyecto de titulación, 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, así como sus componentes y servicios.

A partir de la información recolectada se inició la implementación de las áreas funcionales del estándar ISO, en cuanto a la gestión de configuración se utilizó el estándar IEEE 29148 para definir los requerimientos del software a implementarse en la red de la Prefectura de Imbabura, se escogió el Software Pandora FMS, el cual permite gestionar y monitorear los dispositivos de la red.

Para la gestión de fallos se elaboró un proceso de solución para los problemas que puedan aparecer en la red, y una plantilla para documentar los errores y forma de solución que se presenten. El software Pandora FMS permite crear alertas de advertencia y críticas, las cuales son enviadas al correo electrónico del administrador de la red, para que este pueda reconocer los errores que pueden ocasionarse y hallar una solución de manera efectiva.

Dentro de la gestión de prestaciones se realizó el monitoreo del rendimiento de la red, mediante la utilización del software el cual permite la visualización de eventos suscitados en la red mediante gráficas y reportes, los cuales se generan de acuerdo a la necesidad de información del responsable del manejo de la red de datos.

En cuanto a la gestión de contabilidad se visualizó los parámetros de los equipos, tales como número de usuarios conectados, estado de las interfaces de la red, capacidad de disco, uso de memoria, uso de procesador, estado de conexión entre otros.

En la gestión de seguridad se estableció una contraseña única para el usuario administrador y se estableció políticas de seguridad para el acceso a los equipos.

Finalmente se establece las políticas de gestión, un manual de procedimientos para el manejo correcto de las áreas funcionales del modelo ISO y un manual de administrador con las configuraciones realizadas, los cuales son entregados al Director del Departamento de Tecnologías de la Información de la Prefectura de Imbabura.

ABSTRACT

This titling project has been realized with the goal of offering a better network service for the citizens, ensuring the availability of Imbabura Prefecture's network. It's using ISO standard with its five functional areas: configuration, failures, accounting, performance and security.

During this project, network management has been defined and the SNMP protocol and its features as well. A logic and communication audit has been realized to determine the actual status, components and services network.

From the collected information, the implementation of functional areas of ISO standard was initiated. For configuration management, IEEE 29148 standard had been used to define the software requirements to be implemented in the Imbabura Prefecture's network. Pandora FMS, which manages and monitors network devices, has been selected.

For failure management, a process of solution for the problems which could appear in the network was elaborated, and a template to keep a record of the errors and its solutions as well. Warning and critical events are created in the Pandora FMS software. These alerts are sent to the network administrator's email, who can recognise the errors and find a solution in an effective time.

In network features management, a monitoring of network performance has been realized. Pandora FMS allows the visualization of raised events in the network through graphs and reports, which are generated in accordance with the necessity of the data network administrator.

In regards to accounting management, the equipment features such as number of online users, network interfaces status, disk capacity, used memory, used processor, connection status and others were visualized.

In security management, a unique password for the admin user and security policies for access to the equipment were stablished.

Finally, the management policies have been established. A process manual for the proper management of functional areas of ISO model and an admin manual with the realized configurations have been delivered to the IT Department Director of Imbabura Prefecture.

CAPITULO 1

1. ANTECEDENTES

En este capítulo se presenta el modelo de anteproyecto aprobado, el cual contiene la propuesta realizada para la implementación del plan de titulación.

1.1 Problema

Actualmente, el volumen de información que gestiona el Gobierno Provincial de Imbabura ha crecido exponencialmente de tal manera que la necesidad, ya no es solamente contar con una infraestructura de comunicaciones, sino más bien buscar mecanismos que permitan la detección, mitigación de problemas en la red y obtención de mejores tiempos de repuestas en el acceso a aplicaciones.

El Gobierno Provincial de Imbabura cuenta con una red en la cual no se ha determinado un manejo adecuado en cuanto a la gestión y monitoreo, lo que no ha permitido que el administrador pueda solucionar oportunamente los problemas que se presentan, tales como sobrecarga o falla de los servidores, fallos en la conexión, entre otros.

La Dirección de Tecnologías de la Información del Gobierno Provincial de Imbabura debe tener una constante evolución tecnológica, y ofrecer mayor disponibilidad, mejores tiempos de respuesta y funciones en la red, para esto es necesario generar informes detallados de su funcionamiento y mitigar los problemas que pueden aparecer, por lo cual es primordial aplicar un modelo para la gestión y monitoreo eficiente.

La red del Gobierno Provincial de Imbabura resguarda datos e información de gran importancia, debido al aumento de servicios prestados a los usuarios se han presentado problemas que perjudican su funcionamiento, los mismos que no han podido ser resueltos de manera eficiente y eficaz, por lo tanto el trabajo de grado busca implementar un modelo que

se acople a las necesidades de la institución para facilitar el trabajo del administrador en cuanto a monitoreo y gestión, lo cual permitirá prestar un mejor servicio a la ciudadanía.

1.2 Objetivos

1.2.1 Objetivo General

Implementar el modelo de gestión ISO en la red interna del Gobierno Provincial de Imbabura, mediante la gestión y monitoreo con software libre, con la finalidad de ayudar al administrador en la supervisión y mantenimiento del sistema, de tal manera que se pueda brindar un mejor servicio a la ciudadanía.

1.2.2 Objetivos Específicos

- Analizar el modelo de gestión ISO y el protocolo SNMP, para establecer los criterios que se deben aplicar y adecuar a las distintas necesidades de la red de la institución.

- Realizar una auditoría a la red del Gobierno Provincial de Imbabura para determinar los requerimientos del sistema para la implementación del protocolo SNMP.

- Determinar los requisitos del sistema mediante la utilización el estándar IEEE 29148 para la utilización de software libre en la implementación del modelo en la red local.

- Establecer jerarquías de red dependiendo de los equipos de mayor prioridad, mediante la utilización del estándar RMON de SNMP, para tener una clasificación de las fallas que puedan existir y realizar una distinción adecuada al momento del envío de las notificaciones.

- Realizar un manual de procedimientos de los parámetros de las áreas funcionales del modelo de gestión ISO para el uso del administrador de la red.

- Ejecutar pruebas del comportamiento de la red, de manera que se pueda mostrar el funcionamiento del modelo ISO implementado.

- Realizar un análisis de factibilidad técnico del proyecto, para determinar los beneficios obtenidos con la implementación del modelo de gestión y monitoreo.

1.3 Alcance

Este proyecto consiste en la Gestión y Monitoreo de la red interna del Gobierno Provincial de Imbabura utilizando el modelo ISO y software libre.

Inicialmente se realizará un análisis del protocolo SNMP y del modelo ISO, con sus fundamentos para la gestión y monitoreo de la red, a través de los recursos de software y hardware con los que cuenta el Gobierno Provincial de Imbabura se procederá a implementar el modelo para el monitoreo y gestión de la red, utilizando sus cinco áreas funcionales para los sistemas de gestión (FCAPS), las cuales se detallan a continuación:

1. En el área de gestión de configuración se procederá a efectuar un estudio de la infraestructura de Red del Gobierno Provincial de Imbabura, se determinará la situación actual, fortalezas y debilidades del entorno de la red, para lo que se utilizará una auditoría lógica y de comunicaciones de la red, lo cual determinará los diferentes requerimientos para la implementación del protocolo SNMP (Simple Network Management Protocol).

   A continuación se realizará un estudio de los requisitos del sistema para la utilización de software libre, el cual estará basado en el estándar IEEE 29148 (Systems and software engineering — Life cycle processes — Requirements engineering), de esta manera se podrá tener un análisis previo de las funcionalidades y características del sistema, los cuales deben cumplir con las necesidades de la red entre las que se puede mencionar el monitoreo de los recursos de hardware (espacio en el disco, memoria física y virtual, interfaces de red, carga del procesador) y él envió de notificaciones

de mayor prioridad vía correo electrónico para realizar la configuración del software de gestión, el cuál brindará la información al administrador para diagnosticar, aislar y resolver de manera oportuna los incidentes que se produzcan en la red, mediante inventarios, registro de topología de red de los equipos que se van a monitorear.

2. Para la gestión de fallos se utilizará un proceso para localizar, diagnosticar y corregir problemas en los equipos de la red, lo cual permitirá determinar una jerarquía de alarmas dependiendo de los dispositivos de mayor prioridad, a través del estándar RMON de SNMP el cual permite capturar la información de la red en tiempo real, estas notificaciones serán enviadas al administrador mediante el uso de correo electrónico, para que puedan ser identificadas y gestionadas oportunamente.

3. En cuanto a la gestión de prestaciones, se realizará una medición del rendimiento de los recursos de la red, informes, recopilación de datos estadísticos e historiales, los cuales permitirán el constante monitoreo de los equipos, así como también se elaborará manuales de las configuraciones realizadas tanto en hardware como en software, para facilitar la información para el administrador de la red, el cual podrá hacer uso en cualquier instante para la solución de problemas.

4. La gestión de contabilidad será realizada mediante el registro de la utilización de los recursos de la red.

5. La gestión de seguridad estará enfocada en proteger de ingresos no deseados a la administración de la red mediante el acceso, autorización y confidencialidad exclusivamente para el administrador, al sistema de gestión de dispositivos. De la misma manera los manuales serán entregados de manera específica al administrador así como las notificaciones serán dirigidas solo para él.

Se realizarán pruebas para verificar la implementación del modelo ISO en la red de la Institución utilizando el software escogido mediante el estándar IEEE 29148, como

sobrecargas a la red y a los procesadores , entre otras, lo que permitirá determinar que las notificaciones de mayor prioridad son enviadas directa y oportunamente al administrador.

Para terminar se realizará un análisis de factibilidad técnico de la implementación de las políticas de monitoreo y gestión de la red.

1.4 Justificación

Es de vital importancia conocer el estado de los diferentes recursos con los que cuenta la red tales como switch, routers, host y servidores, con la finalidad de prevenir fallos y detectar diferentes problemas al momento de la prestación de servicios a los usuarios de la red.

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.

En el año 2008, se firmó el decreto 1014 con el cual el Software Libre pasó a ser una política de Estado para ser adoptado por todas las entidades públicas, de esta manera la Institución cuenta con servidores basados en esta plataforma.

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.

1.5 Contexto de la Institución

1.5.1 Prefectura de Imbabura

En la página web de la Prefectura de Imbabura se encuentran descritos los pilares fundamentales de la institución los cuales se indican a continuación.

1.5.1.1 Misión

La Prefectura de Imbabura se consolida como una institución de derecho público, autónoma, descentralizada, transparente, eficiente, equitativa, incluyente y solidaria; líder del desarrollo económico, social y ambiental provincial.

1.5.1.2 Visión

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.

1.5.1.3 Objetivos Estratégicos

- Fomentar el desarrollo económico provincial
- Consolidar el sistema de transporte y movilidad provincial
- Implementar el sistema de gestión ambiental provincial con enfoque intercultural y visión de cuenca hidrográfica
- Diseñar políticas, planes y programas, tendientes a fortalecer la inclusión social, el desarrollo cultural que permitan hacer de Imbabura una provincia equitativa, solidaria e intercultural.
- Generar mecanismos de articulación y lineamientos para la coordinación endógena institucional e interinstitucional.
- Tecnificar los procesos de administración y gestión institucional.

1.5.1.4 Ubicación

La Prefectura de Imbabura se encuentra ubicada en la ciudad Ibarra, entre las calles Simón Bolívar y Miguel Oviedo, como se muestra en la Figura 1.

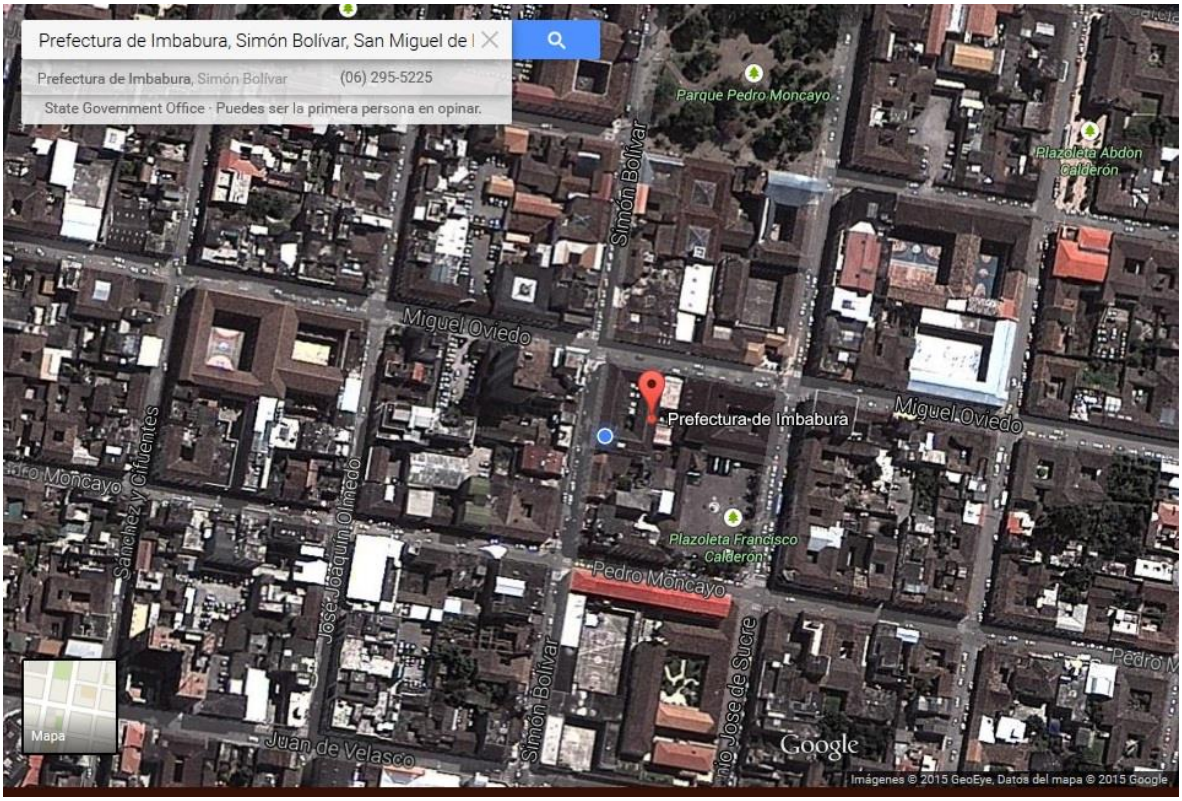


Figura 1. Ubicación Prefectura de Imbabura

Fuente: Recuperado de https://www.google.com.ec/maps/place/Prefectura+de+Imbabura/@0.3497107,-78.1174803,381m/data=!3m1!1e3!4m2!3m1!1s0x8e2a3cb64702d561:0xfb2189edff787e1b?hl=es-419

CAPITULO 2

2. Análisis del modelo ISO, Protocolo SNMP y situación actual de la red del Gobierno Provincial de Imbabura.

En este capítulo se estudia el modelo ISO y el protocolo SNMP en su versión actual. También se realiza el estudio de la situación actual de la Infraestructura de Red del Gobierno Provincial de Imbabura utilizando una auditoría lógica y de comunicaciones de la red.

2.1 Introducción a la gestión de redes

De acuerdo con Barba Martí (1999), la gestión de red trata sobre la planificación, la organización, la supervisión y el control de elementos de comunicaciones para garantizar un adecuado nivel de servicio, y de acuerdo con un determinado coste. Los objetivos principales de la gestión de red consisten en mejorar la disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad.

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.

Tradicionalmente, en la gestión de las redes se ha partido de soluciones propietarias y cerradas con un ámbito de actuación limitado a la propia empresa o dominio de la institución. Con el tiempo, la evolución tecnológica ha permitido la entrada de múltiples fabricantes de equipos, por tanto, bien sea porque ha ocurrido la absorción de empresas o bien por diversificación de las fuentes de los equipos, las redes actuales son cada vez más heterogéneas.

Uno de los problemas más graves que tienen estas redes es que los equipos que las constituyen son de fabricantes distintos, con lo cual la única forma de gestionarlas es a partir de sistemas de gestión que utilicen estándares abiertos con el fin de compatibilizar protocolos e información. De esta forma, durante la década de los noventa, se han ido desarrollando diversas iniciativas con el objetivo de ofrecer recomendaciones y estándares abiertos para tratar de dar solución a estas nuevas problemáticas, como por ejemplo mediante el protocolo de gestión SNMP o el CMIP.

Las recomendaciones sobre esta temática provienen de diversos grupos de estandarización. La más importante, la ITU–T, ha definido la red de gestión de las telecomunicaciones (TMN). Estas recomendaciones definen cinco áreas funcionales para la gestión de red, las de supervisión y fallos, configuración, tarificación, prestaciones y seguridad.

La organización de la gestión puede estructurarse también según un criterio temporal. De esta forma, se puede hablar de un control operacional que opera a muy corto plazo y a bajo nivel, una administración que opera a corto plazo y a bajo-medio nivel, un análisis de la gestión que opera a medio plazo y a medio-alto nivel y finalmente una planificación a largo plazo y a más alto nivel.

En el control operacional, las operaciones realizadas a este nivel deben quedar registradas, para su posterior análisis por el administrador de red. Es el caso de operaciones tales como la recogida de datos sobre prestaciones y utilización de la red, la evaluación de alarmas, la diagnosis de problemas, el arranque y la parada de los componentes de la red, la ejecución programada de pruebas preventivas, la modificación de configuraciones o la carga de nuevas versiones de software.

Las funciones principales de la administración consisten en seguir las tareas de control operacional y en elaborar informes periódicos para su posterior análisis. Por ello se ocupa de tareas como la evaluación de la calidad de servicio, la evaluación de tráfico, el mantenimiento de registro histórico de problemas, el mantenimiento de inventario, el mantenimiento de

configuraciones, la contabilidad de red y de control de acceso. El objetivo del análisis es garantizar la calidad de servicio y, finalmente, la planificación se encarga de las decisiones dependientes del negocio al que se dedica la empresa. Barba Martí (1999)

2.1.1 Gestión de redes

En el artículo de Millán Tejedor (1999), sostiene que la gestión de red se suele centralizar en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados en las distintas redes de la empresa en cuestión. Un centro de gestión de red dispone de tres tipos principales de recursos:

- **Métodos de gestión:** Definen las pautas de comportamiento de los demás componentes del centro de gestión de red ante determinadas circunstancias.

- **Recursos humanos:** Personal encargado del correcto funcionamiento del centro de gestión de red.

- **Herramientas de apoyo:** Herramientas que facilitan las tareas de gestión a los operadores humanos y posibilitan minimizar el número de éstos.

2.1.2 Arquitectura de gestión de redes

De acuerdo a Millán Tejedor (1999), los sistemas de gestión que existen actualmente, utilizan una estructura básica, conocida como paradigma gestor-agente, cuyo esquema queda reflejado en la Figura 2.

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.

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.

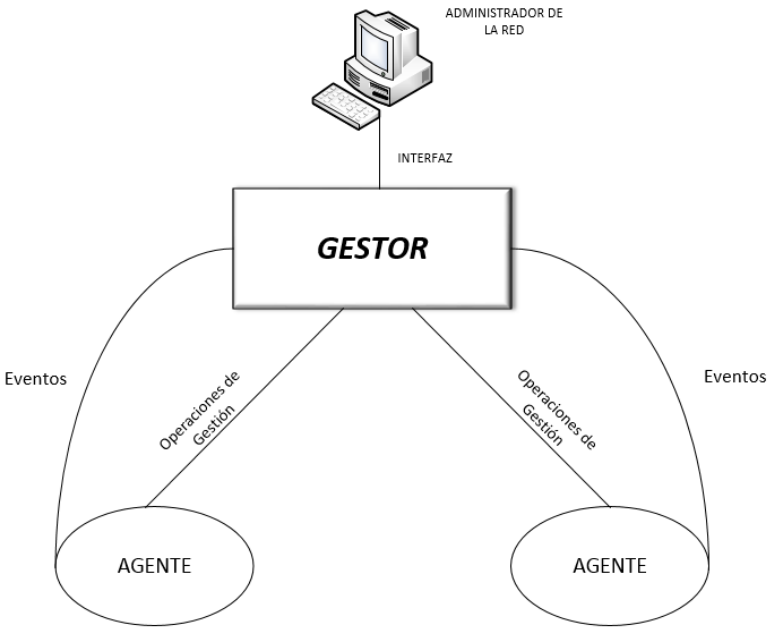


Figura 2. Arquitectura de Gestión de Redes

Fuente: Recuperado de http://www.ramonmillan.com/tutoriales/gestionred.php#Arquitectura

El principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada nodo gestionado información acerca del estado y las características de funcionamiento de un determinado recurso de la red. El gestor pide al agente, a través de un protocolo de gestión de red, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento.

Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia. Millán Tejedor (1999)

2.1.3 Modelo de gestión FCAPS

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.

En el informe de Bastidas, y otros (2011), se especifican las características de cada una de estas áreas.

2.1.3.1 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)*.

  La primera lleva a cabo un sondeo periódico de la red para averiguar qué elementos están activos y con qué características; la segunda averigua de qué forma están interconectados los distintos elementos de la red.
- *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. Bastidas, y otros (2011)

2.1.3.2 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.

2.1.3.3 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.

2.1.3.4 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.

2.1.3.5 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.

2.1.4 Monitoreo de red

2.1.4.1 Monitoreo

Bastidas y otros (2011), sostienen que el monitoreo de red es la parte de la gestión de red que se ocupa de la observación y análisis del estado y el comportamiento de los recursos gestionados. Abarca cuatro fases:

1. Definición de la información de gestión que se va a monitorizar.

2. Acceso a la información de monitorización. Las aplicaciones de monitoreo utilizan los servicios ofrecidos por un gestor para acceder a los datos de monitorización mantenidos por un agente. Las comunicaciones entre gestores y agentes se realizan gracias a los protocolos de gestión.

3. Diseño de políticas de monitorización. Se distinguen dos tipos de comportamiento.

    - Sondeo. En este caso el gestor pregunta periódicamente a los agentes por los datos de monitorización.
    - Informe de Eventos. Los agentes, por su propia iniciativa, informan a los gestores.

4. Procesado de la información de monitorización.

2.1.4.2 Control

La parte de control dentro de la gestión de redes es la encargada de modificar parámetros e invocar acciones en los recursos gestionados.

2.2 Protocolo SNMP

De acuerdo con Hillar (2004), "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.

2.2.1 Versiones SNMP

Según Zerga (2011) SNMP determina versiones para satisfacer distintas necesidades que se presentan en el manejo de redes.

2.2.1.1 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].

2.2.1.2 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.

Brinda mejoras en los aspectos de gestión tales como: funcionalidad (define las mejoras en cuanto a la estructura de la MIB, puede operar tanto como agente como gestores), eficiencia de operación (ofrece mayor eficiencia en la transferencia de información entre sistemas). El rendimiento se ve un poco afectado en función de que aumenta la seguridad con funciones de autenticación y encriptación.

[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

2.2.1.3 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.

Proporciona tanto modelos como niveles de seguridad, lo cual determina que mecanismo será empleado en el envío de un paquete SNMP.

Incorpora características de seguridad tales como: autenticación y control de la privacidad. La autenticación de SNMPv3, se lleva a cabo utilizando el Código de Autenticación de Mensaje Hash (HMAC), que se calcula mediante una función de Hash criptográfica en combinación con una clave secreta.

2.2.2 Componentes de SNMP

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

2.2.2.1 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.

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

2.2.2.2 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.

2.2.2.3 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.

2.2.3 Comandos básicos

Los dispositivos administrados son supervisados y controlados utilizando 4 comandos SNMP básicos: read, write, trap y operaciones de recorrido.

2.2.3.1 Read

Es utilizado por un NMS para supervisar los dispositivos administrados. El NMS examina diferentes variables que son mantenidas por los MD.

2.2.3.2 Write

Es utilizado por un NMS para controlar los MD. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

2.2.3.3 Trap

Es utilizado por los dispositivos administrados para reportar eventos de forma asíncrona a los Network Management Systems (NMS). Cuando cierto tipo de eventos ocurren, un MD envía un TRAP hacia el NMS.

2.2.3.4 Operaciones de recorrido (Traversal Operations)

Son utilizadas por los NMS para determinar cuáles variables son soportadas por los MD y obtener secuencialmente información en una tabla de variables, parecida a una tabla de enrutamiento.

2.2.4 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.

2.2.4.1 MIB-I

Constituye la primera MIB normalizada. Está formada con objetos de la torre de protocolos de TCP/IP.

2.2.4.2 MIB – II

Es la base de datos común para la gestión de equipos en Internet; ha sido actualizada varias veces por lo que actualmente se encuentra dividida en varios RFCs: RFC 4293[7], RFC 4022[8], RFC 4113[9], RFC 2863[10] y RFC 3418[11]. (Sosa, 2013)

2.2.4.3 Estructura

Cada tipo de objeto de una MIB tiene asociado un identificador de objeto (object identifier) que lo nombra y su organización es jerárquica (forma de árbol), este valor consiste en una secuencia de enteros no negativos.

El subárbol 1.3.6.1 es una sub rama de internet que define cuatro tipos de nodos internet o grupos:

- **Directory:** reservado para OSI directory (X.500).
- **mgmt:** destinado a objetos definidos por la IAB.
- **Experimental:** objetos usados en temas experimentales.
- **Private:** objetos definidos por empresas.

La estructura de estas MIBs está definida utilizando la sintaxis ASN.1. La MIB II se compone de los siguientes nodos estructurales:

- **System:** proporciona información genérica del sistema gestionado, por ejemplo donde se encuentra el sistema, quien lo administra, etc.

[7] **RFC 4293:** Base de información de gestión para el Protocolo de Internet (IP)
[8] **RFC 4022** Base de información de gestión para el Protocolo de Control de Transmisión (TCP)
[9] **RFC 4113:** Base de información de gestión para el Protocolo de Datagramas de Usuario (UDP)
[10] **RFC 2863:** El grupo de interfaces MIB
[11] **RFC 3418:** Base de Información de Gestión (MIB) para el Protocolo Simple de Administración de Red (SNMP)

- **Interfaces:** posee la información de las interfaces de red presentes en el sistema, incorpora estadísticas de los eventos ocurridos en el grupo.

- **Address Traslation (At):** es obsoleto, pero es mantenido para preservar compatibilidad con la MIB-I. En él se almacenan las direcciones de nivel de enlace correspondientes a una dirección IP.

- **IP:** en este grupo se almacena la información referente a la capa IP, tanto de configuración como de estadísticas.

- **ICMP:** se almacenan contadores de los paquetes ICMP entrantes y salientes.

- **TCP:** posee la información relativa a la configuración, estadísticas y estado del protocolo TCP.

- **UDP:** en este nodo esta la información correspondiente a la configuración y estadísticas del protocolo UDP.
- **EGP:** se encuentra agrupada la información de la configuración y operación del protocolo EGP.

- **Transmission:** contiene grupos referidos a las distintas tecnologías del nivel de enlace implementadas en las interfaces de red del sistema gestionado. (Sosa, 2013)

2.2.4.4 Sintaxis

El RFC 1155[12] define los siguientes tipos de objetos: primitivos y constructores. Estos son una clase de dato, los cuales definen la estructura de datos que el equipo necesita para entender y procesar información.

[12] **RFC 1155:** Estructura e identificación de información de gestión para redes basada en TCP/IP

2.2.4.4.1 Primitivos o Simples

Son aquellos que definen una instancia simple de objeto.

- **Integer:** representa objetos con un número entero.
- **Octet String:** utilizado para texto.
- **Null:** objeto que carece de valor.
- **Object Identifier:** utilizado por nodos estructurales
- **Sequence y Sequence of:** utilizado para arrays.

2.2.4.4.2 Constructores o Estructurados

Es una secuencia que permite generar listas o tablas para el lenguaje de programación utilizado por la MIB.

- **IpAddress:** utilizado para direcciones IP
- **Counter:** contadores
- **Gauge:** representa un entero no negativo que puede incrementar o decrementar.
- **Timeticks:** usado para medir tiempos
- **Opaque:** para cualquier otra sintaxis ASN.1.

2.2.5 Funcionamiento de SNMP

Según Hillar (2004), el funcionamiento de SNMP es muy sencillo. Desde la estación de administración se solicita la información a los agentes. Con toda esa información, se realizan el monitoreo y diagnósticos correspondientes y, si fuera necesario, se pueden administrar y configurar determinados parámetros de funcionamiento de los dispositivos de redes (agentes). En tal caso, desde la estación de administración se modifican valores de la MIB de un agente como se muestra en la Figura 3.

También, un agente puede notificar determinados eventos de importancia a la estación de administración, por ejemplo, cuando está teniendo problemas en su funcionamiento normal. Este comportamiento generalmente se puede configurar.

Al adquirir dispositivos para redes, es conveniente que ofrezcan soporte a SNMP, pues nos va a permitir utilizar estaciones de administración y muchas de las herramientas diseñadas para trabajar con este protocolo. Sin lugar a dudas, esto facilitará la administración y el monitoreo de la red.

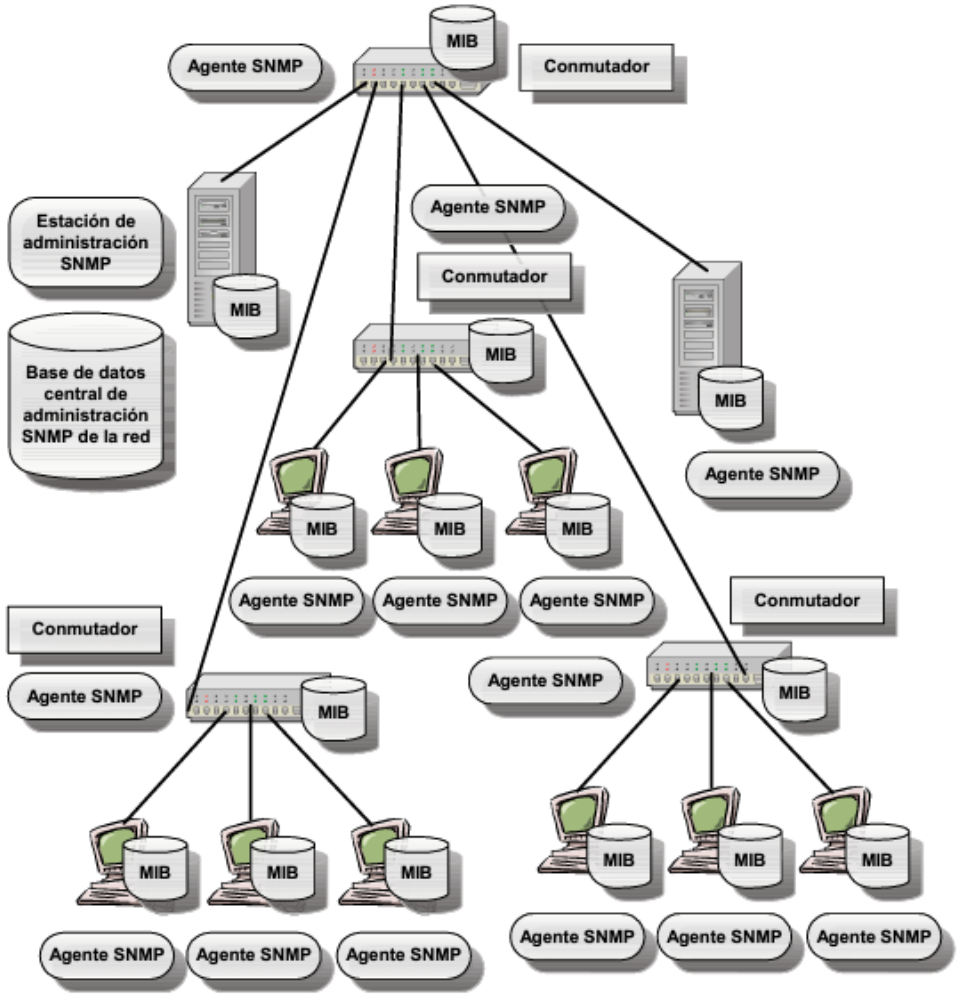


Figura 3. Esquema de los agentes y de la estación de administración SNMP en una LAN

Fuente: Redes: Diseño, Actualización y Reparación. Hillar, Gastón Carlos.

2.2.6 Tipos de mensajes

Cuando los programas de administración de SNMP envían solicitudes a un dispositivo de red, el software del agente de ese dispositivo recibe las solicitudes y recupera la información de las MIB. A continuación, el agente vuelve a enviar la información solicitada al programa de administración SNMP que lo inició.

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el formato mostrado en la Figura 4. A continuación se describe cada uno de sus campos.

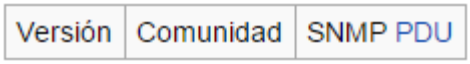


Figura 4. Formato mensajes SNMP
Fuente: Recuperado de http://www.ebah.com.br/content/ABAAAfctoAG/snmp

- **Versión:** versión de protocolo que se está utilizando (1 SNMPv1, 2 SNMPv2, 3 SNMPv3)
- **Comunidad:** utilizado para la autenticación, existe una comunidad de lectura llamada "public" y una de escritura llamada "private".
- **SNMP PDU:** contiene los datos del protocolo y depende de la operación que se ejecute.

Según (Zerga, SNMP, 2011), Para realizar estas tareas, el agente utiliza los siguientes tipos de mensaje:

2.2.6.1 GetRequest

A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso de la petición.

2.2.6.2 GetNextRequest

Utilizado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor del objeto, este tipo de mensaje se utiliza para repetir la operación con el siguiente objeto de la tabla.

2.2.6.3 SetRequest

Usado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

2.2.6.4 GetResponse

Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest o SetRequest.

2.2.6.5 GetBulkRequest

Utilizado por un NMS que usa la versión 2 o 3 del protocolo SNMP generalmente cuando es requerida una transmisión larga de datos.

2.2.6.6 InformRequest

Un NMS que utiliza la versión 2 o 3 de SNMP transmite este tipo de mensaje a otro NMS con las mismas características, para notificar información sobre objetos administrados.

Estos mensajes utilizan la estructura en el campo SNMP PDU mostrada en la Figura 5.

Tipo	Identificador	Estado de error	Índice de error	Enlazado de variables

Figura 5. Estructura SNMP PDU

Fuente: Recuperado de http://www.ebah.com.br/content/ABAAAfctoAG/snmp

Donde:

- **Identificador:** número utilizado por el NMS y el agente para enviar solicitudes y respuestas diferentes en forma simultánea.

- **Estado de error:** utilizado en los mensaje GetResponse, proporciona información adicional sobre la causa del problema, este campo puede tener los siguiente valores:
    - **0:** no hay error
    - **1:** demasiado grande
    - **2:** no existe la variable
    - **3:** valor incorrecto
    - **4:** valor de solo lectura
    - **5:** error genérico

- **Enlazado de variables:** nombres de variables con sus valores correspondientes.

2.2.6.7 Trap

Son los mensajes no solicitados enviados por los agentes al administrador, en caso de que ocurra algún evento inesperado, el formato de SNMP PDU es el mostrado en la Figura 6, y cada uno de sus campos se describen a continuación.

Tipo	Enterprise	Dirección del agente	Tipo genérico de trap	Tipo específico de trap	Timestamp	Enlazado de variables

Figura 6. SNMP PDU Mensaje Trap

Fuente: Recuperado de http://protocolo-snmp.blogspot.com/2011/06/tipos-de-mensaje.html

- **Enterprise:** identificación del subsistema de gestión que ha emitido el trap.

- **Dirección del agente:** dirección IP del agente que emitió el trap.

- **Tipo genérico de trap**
    - ***Cold start (0):*** *indica que el agente ha sido inicializado o reinicializado.*
    - ***Warm start (1):*** *indica que la configuración del agente ha cambiado.*
    - ***Link down (2):*** *indica que una interfaz de comunicación se encuentra inactiva.*
    - ***Link up (3):*** *indica que una interfaz de comunicación se encuentra activa.*
    - ***Authentication failure (4):*** *indica que el agente ha recibido un requerimiento de un NMS no autorizado.*
    - ***EGP neighbor loss (5):*** *indica cuando un equipo vecino se encuentra fuera de servicio.*
    - ***Enterprise (6):*** *son todos los nuevos trap incluidos por los vendedores.*

- **Tipo específico de trap:** usado por los trap privados, así como para precisar la información de un determinado trap genérico.

- **Timestamp:** indica el tiempo que ha transcurrido entre el reinicio del agente y la generación del trap.

- **Enlazado de variables:** utilizado para proporcionar información adicional sobre la causa del mensaje.

2.3 Situación actual

2.3.1 Dirección de Tecnologías de la Información y Comunicaciones (TICs)

Luego de haber asistido a la Dirección de TIC’s durante el proceso de implementación del proyecto de titulación se pudo identificar que ésta tiene los siguientes objetivos.

2.3.1.1 Objetivos

- Garantizar el buen funcionamiento de toda la red informática.
- Mantener y evaluar de manera continua los procesos que se operan en las unidades administrativas, financieras y operacionales de la Prefectura de Imbabura.
- Ofrecer asesoría y asistencia técnica en el área de redes y sistemas de información.
- Gestionar las mejoras tecnológicas para el buen funcionamiento de los recursos computacionales con que cuenta la Institución.

2.3.2 Red Interna 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.

2.3.2.1 Acceso a internet

La Red de la Prefectura de Imbabura está conectada a Internet mediante el proveedor de servicios CNT el cual brinda un ancho de banda de 30 [Mbps], con un límite de 3 [Mbps] para la red inalámbrica del edificio.

2.3.2.2 Estructura física

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 7.

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.

2.3.2.3 Backbone de fibra óptica

La Prefectura de Imbabura cuenta con fibra óptica, la cual se encuentra instalada entre pisos del edificio, es de tipo OM3 y brinda una velocidad de trasmisión de 10 Gbps, posee protección tipo armada para defensa contra roedores.

Para la conexión de la fibra óptica entre el edificio de la Prefectura de Imbabura y el Patronato de Acción Social (PAS) se realizó una instalación subterránea aplicando las normas y estándares de instalación.

Todos los conectores de fibra óptica son Tipo SC Múltiple, las bandejas son de 24 puertos e incluyen adaptadores tipo SC dúplex. Los Patch Cord de fibra son de tipo SC Full Dúplex de 3 metros.

2.3.2.4 Cableado estructurado

Todos los elementos del sistema de cableado estructurado instalado en la Prefectura de Imbabura son de Cat-6A. El paso de cable se encuentra realizado a través del sistema de

bandeja y escalerilla, instalados sobre el cielo falso de las oficinas de cada uno de los pisos del edificio.

Los Patch Panel poseen espacios para 24 salidas, los jack instalados son categoría 6A y cumplen el estándar ANSI/TIA 568-B2.10.

El cable que se conecta en cada uno de los puntos de datos es de cobre, tipo UTP categoría 6A, soporta aplicaciones 10 Gigabit Ethernet / 1000BASE-T / IEEE 802.3ab, cumple con los parámetros y todas las características eléctricas para el estándar TIA/EIA 568-B.2-1 e ISO/IEC 11801 Categoría 6.

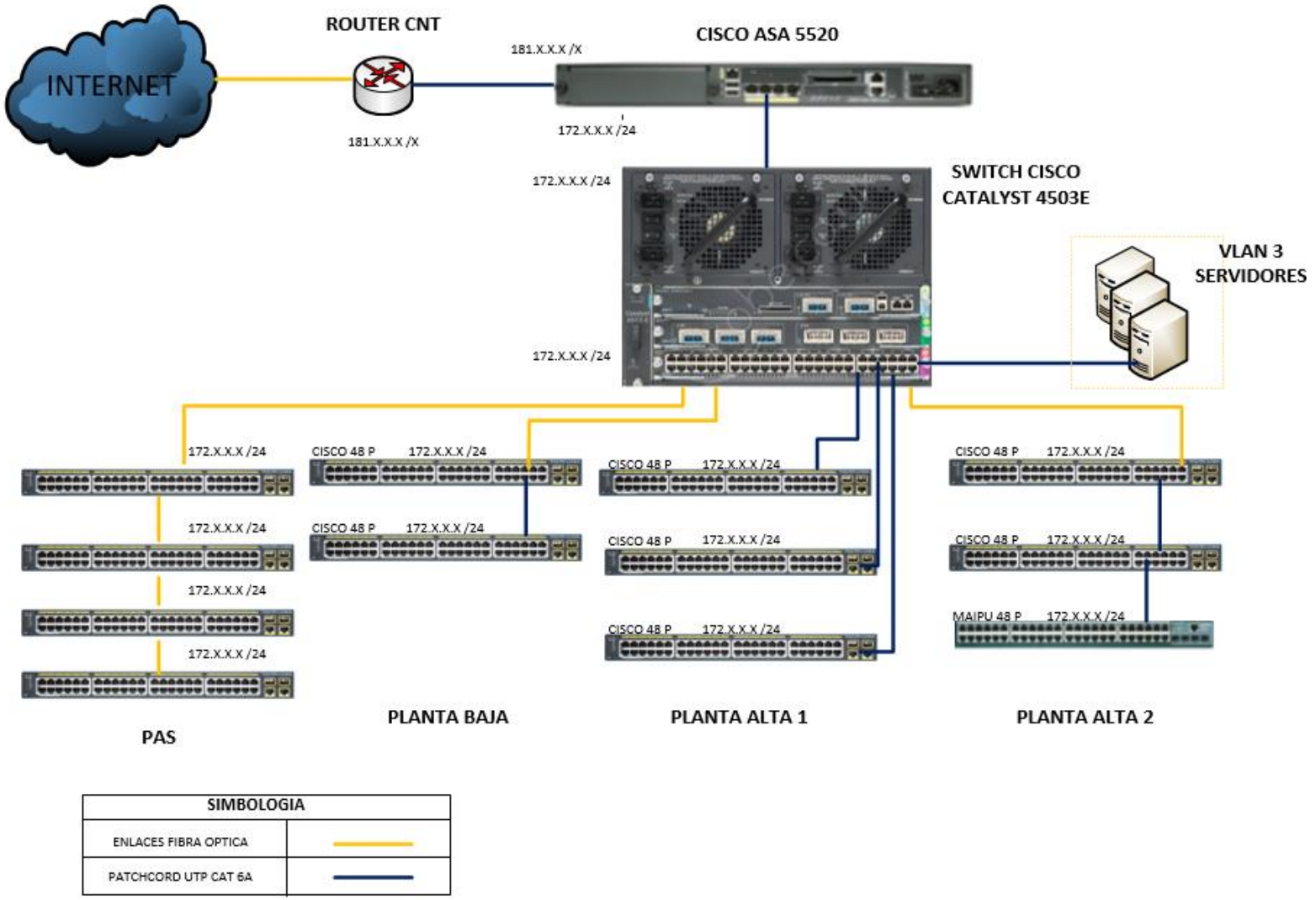


Figura 7. Topología Física de la Red

Fuente: Prefectura de Imbabura

2.3.2.5 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 8 se muestra la distribución de equipos activos en el cuarto de comunicaciones de la Prefectura de Imbabura.

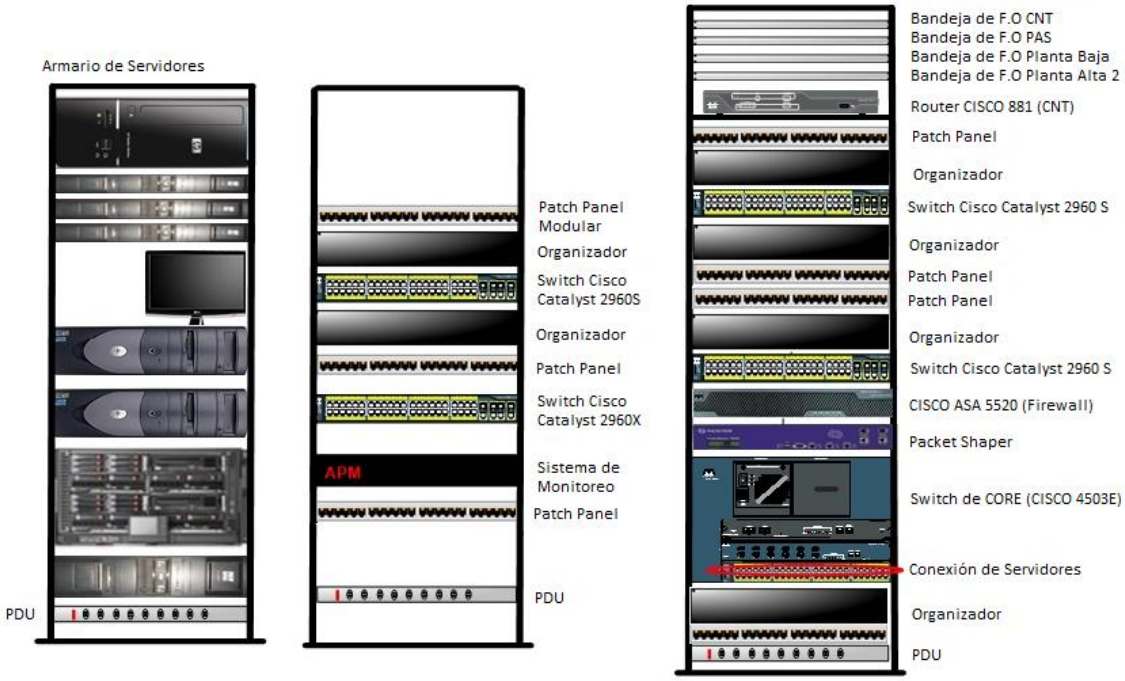


Figura 8. Distribución de Equipos en el Cuarto de Comunicaciones

Fuente: Prefectura de Imbabura

En la planta baja se encuentra ubicado un rack que se conecta al cuarto de comunicaciones y esta distribuido como se indica en la Figura 9.

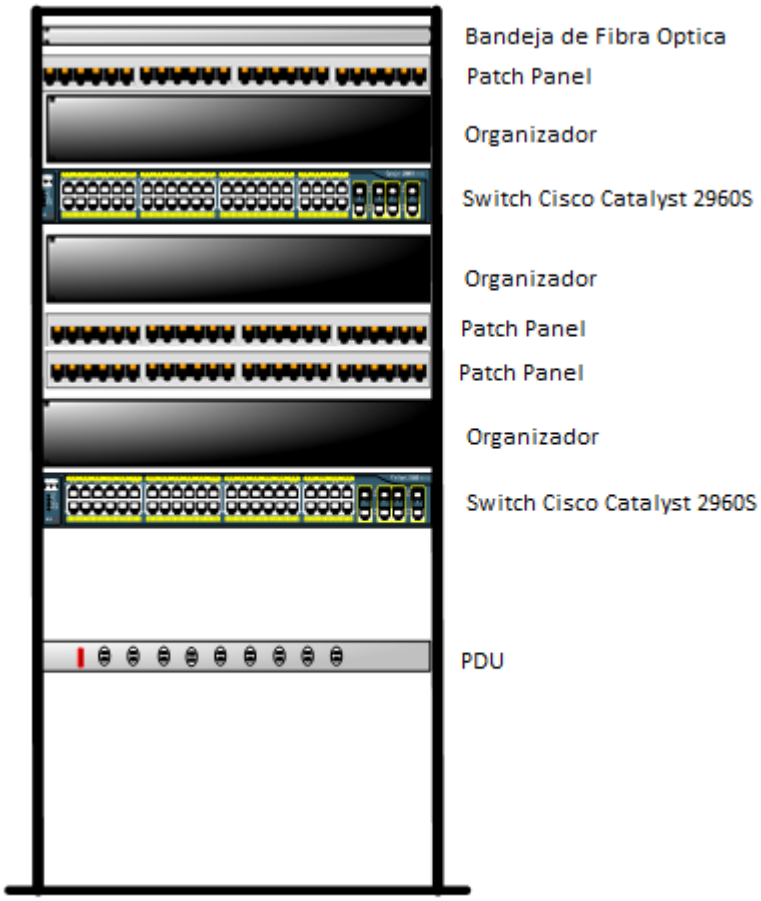


Figura 9. Distribución de equipos en el Rack de Planta baja de la Prefectura de Imbabura

Fuente: Prefectura de Imbabura

En la planta alta 2 se ubica un rack que se conecta al cuarto de comunicaciones y esta distribuido como se indica en la Figura 10.

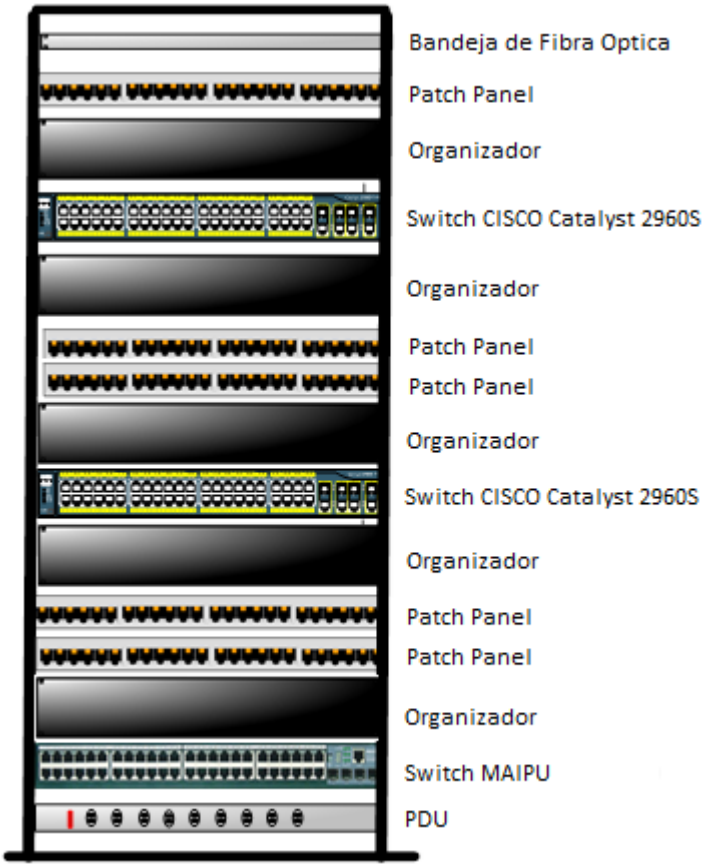


Figura 10. Distribución de equipos en el rack Planta alta 2 en la Prefectura de Imbabura

Fuente: Prefectura de Imbabura

2.3.2.6 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

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.

Tabla 1. Características Servidor BLADE

SERVIDOR BLADE	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	HP
Modelo	C3000
Procesador	Intel Xeon, Itanium, AMD Opteron
Memoria	Intercalable DDR ECC 2 a 1, ampliable a 12 GB (8GB con redundancia)
Tarjeta de Video	ATI Rage XL con memoria de video integrada de 8 MB
Tarjeta de Red	NC7781 10/100/1000 con función Wake On LAN (WOL)
Puertos	2 puertos SCSI q admiten un máximo de 8 unidades de disco internas
Disco Duro	8 cuchillas divididas entre 300GB y 500GB
Sistema Operativo	Windows Server, Windows 7, CentOS

Fuente: Recuperado de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04128340.pdf

El Servidor BLADE se encuentra dividido en tres partes con cuchillas HP Proliant BL460c, dos son Generación 7, y sus características se muestran en la Tabla 2 y una Generación 8 mostrada en la Tabla 3.

Tabla 2. Características HP Proliant BL460c G7

HP PROLIANT BL460c G7	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	HP
Modelo	Proliant BL460
Generación	Siete
Procesador	Intel Xeon 5500, Intel 5520 Chipset
Memoria	12 slots DIM, hasta 48GB usando PC3-10600 DDR3
Tarjeta de Video	ATI Rage XL con memoria de video integrada de 8 MB
Tarjeta de Red	NC553i Dual Port FlexFabric 10GB
Puertos	USB 2.0, SD-HC Card Slot
Disco Duro	4 cuchillas de 300GB
Sistema Operativo	Windows Server, Windows 7, CentOS

Fuente: Recuperado de http://www8.hp.com/h20195/v2/getpdf.aspx/c04123266.pdf?ver=1

Tabla 3. Características HP Proliant BL460c G8

HP PROLIANT BL460c G7	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	HP
Modelo	Proliant BL460
Generación	Ocho
Procesador	Intel Xeon E5-2670 v2
Memoria	64 GB PC3-14900R DDR3
Tarjeta de Red	2 Puertos, cada uno de 30 Gbps Full Duplex
Puertos	USB 2.0, SD-HC Card Slot
Disco Duro	4 cuchillas: 3 de 500GB y 1 de 300GB
Sistema Operativo	Windows Server, Windows 7, CentOS

Fuente: Recuperado de http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-9690ENW.pdf

Otros equipos que son utilizados como servidores se muestran en las tablas 4, 5, 6 y 7 presentadas a continuación.

Tabla 4. Características HP PROLIANT ML370

SERVIDOR PROLIANT (CORREO ELECTRÓNICO)	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	HP
Modelo	Proliant ML370
Generación	Tres
Procesador	Bidireccional Intel Xeon con tecnología Hyper-Threading
Memoria	Intercalable DDR ECC 2 a 1, Ampliable a 12 GB (8GB con redundancia)
Tarjeta de Video	ATI Rage XL con memoria de video integrada de 8 MB
Tarjeta de Red	NC7781 10/100/1000 con función Wake On LAN (WOL)
Puertos	2 puertos SCSI q admiten un máximo de 6 unidades de disco internas
Sistema Operativo	CentOS

Fuente: Recuperado de http://h10032.www1.hp.com/ctg/Manual/c00690216.pdf

Tabla 5. Características DELL Power Edge 2900

SERVIDOR Dell Power Edge 2900 (Gestión Documental)	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	DELL
Modelo	Power Edge 2900
Procesador	Intel Xeon 5000 con 3.0GHz de frecuencia
Memoria	Modulos DIMM 256MB/512MB/1GB/2GB/4GB con memoria intermedia completa
Tarjeta de Red	NIC Gigabit Ethernet Broadcom NetXtrem II
Tarjeta de Video	ATI ES1000 integrada con memoria de 16MB
Puertos	USB 2.0, SD-HC Card Slot
Disco Duro	SATA 250GB
Sistema Operativo	CentOS

Fuente: Recuperado de
http://www.dell.com/downloads/emea/products/pedge/es/PE2900_Spec_Sheet_Quad.pdf

Tabla 6. Características HP PROLIANT DL360 G6

SERVIDOR HP PROLIANT DL360 G6 (Geolocalización)	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	HP
Modelo	Proliant BL460
Generación	Seis
Procesador	Intel Xeon X5550
Memoria	12 GB PC3-1600R DIMM
Tarjeta de Red	HP NC 382i, Adaptador multifunción, puerto dual Gigabit
Tarjeta de Video	ATI ES1000, 32MB
Puertos	USB 2.0
Sistema Operativo	CentOS

Fuente: Recuperado de http://www.nts.nl/site/html/modules/pdf/Server/HP%20Proliant%20DL360G6.pdf

Además de estos equipos dentro del armario de servidores se encuentra ubicado un dispositivo para almacenamiento el cual presenta las características mostradas en la Tabla 7.

Tabla 7. Características HP Storage Works p2000

HP Storage Works p2000	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	HP
Modelo	Storage Works p2000
Puertos	Mini USB, Puerto Ethernet, Puerto de Expansión
Disco Duro	24 TB
Sistema Operativo	Windows Server, Windows 7, CentOS

Fuente: Recuperado de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04168365.pdf

2.3.2.7 Equipos y dispositivos de red

El edificio de la Prefectura de Imbabura está dividido en tres plantas, teniendo cada una diferentes departamentos con distintos números de usuarios, mediante la realización de un inventario se registró en detalle los equipos y dispositivos de red que se encuentran en cada una de las mismas.

2.3.2.7.1 Planta baja

En la planta baja del edificio se encuentran ubicadas las siguientes direcciones: Administrativa, Desarrollo Económico y Gestión Ambiental , Fiscalización, Infraestructura Física, Secretaria General y Talento Humano, lo cual se muestra en el Anexo E en los planos de la infraestrutura física del edificio.

En la tabla 8. se muestran los dispositivos de red ubicados en el rack de la planta baja con sus respectivas especificaciones técnicas.

Tabla 8. Características Switch CISCO 2960-S

SWITCH CISCO 2960-S	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	CISCO
Cantidad	2
Modelo	2960-S
Protocolo de Administración remota	RSPAN (Remote Switch Port Analyzer)
Número de Puertos	48 Gigabit Ethernet
Seguridad	• Defensa de amenazas (MAC, IP, ARP spoofing). • TrustSec: permite al usuario asegurar la red, datos y recursos con políticas basadas en control de accesos e identidad. • Otras características de seguridad avanzada.
Estándares	PoE 802.3af/at

Fuente: Recuperado de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html

En la tabla 9. se determinan los equipos de computo utilizados en cada una de las direcciones, mostrando sus especificaciones técnicas y la VLAN a la que pertenece cada uno.

Tabla 9. Inventario Equipos de Cómputo Planta Baja

N°	Tipo	Dirección	Subdirección	Tipo de procesador	Velocidad (Ghz)	Disco duro (GB)	Ram (MB)	Sistema operativo	VLAN
1	ESCRITORIO	Administrativa	Bodega	INTEL CORE 2 DUO	2.4	300	2	Windows XP	10
2	ESCRITORIO	Administrativa	Mecanica	INTEL CORE 2 DUO	3	298	2	Windows Vista	10
3	ESCRITORIO	Administrativa	Bodega	INTEL CORE i7	2,93	932	8	Windows 7	10
4	ESCRITORIO	Administrativa	Bodega	INTEL CORE 2 DUO	2,66	300	1,98	Windows XP	10
5	ESCRITORIO	Administrativa	Bodega	INTEL PENTIUM 4	3,4	149	1	Windows XP	10
6	ESCRITORIO	Administrativa	Bodega	INTEL PENTIUM 4	3	112	0,47	Windows XP	10
7	ESCRITORIO	Administrativa	Bodega	INTEL CORE i7	3	466	4	Windows 7	10
8	ESCRITORIO	Administrativa	Bodega	INTEL CORE 2 DUO	2,8	298	1	Windows XP	10
9	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Turismo	INTEL CORE 2 DUO	3	298	1	Windows 7	12
10	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Turismo	INTEL CORE i7	2,8	466	3	Windows XP	12
11	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Turismo	INTEL CORE 2 DUO	1,86	298	2	Windows XP	12
12	PORTATIL	Desarrollo Económico y Gestión Ambiental	Turismo	INTEL CORE i7	1,73	466	6	Windows 7	12

Tabla 9. Inventario Equipos de Cómputo Planta Baja

13	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Turismo	INTEL PENTIUM 4	3,2	75	0,48	Windows XP	12
14	ESCRITORIO	Fiscalización	Fiscalización					Windows 7	18
15	ESCRITORIO	Fiscalización	Fiscalización	INTEL CORE i5	2,93	932	8	Windows 7	18
16	ESCRITORIO	Fiscalización	Fiscalización	INTEL CORE 2 DUO	2,2	300	1	Windows 7	18
17	ESCRITORIO	Fiscalización	Fiscalización	INTEL CORE i5	2,93	932	8	Windows 7	18
18	ESCRITORIO	Fiscalización	Fiscalización	INTEL CORE 2 DUO	2,56	150	1	Windows XP	18
19	ESCRITORIO	Fiscalización	Fiscalización	INTEL CORE i7	3,4	466	4	Windows 7	18
20	ESCRITORIO	Fiscalización	Fiscalización	INTEL CORE i7	3,4	465	4	Windows 7	18
21	ESCRITORIO	Fiscalización	Fiscalización	INTEL CORE 2 DUO	2,93	300	4	Windows 7	18
22	PORTATIL	Fiscalización	Fiscalización	INTEL CORE i7	2,9	466	4	Windows 7	18

Fuente: Prefectura de Imbabura

2.3.2.7.2 Planta alta 1

En la planta alta 1 del edificio se encuentran ubicadas las oficinas de la Prefectura y la Viceprefectura, además de las siguientes direcciones: Administrativa, Coordinación General, Financiera, PAS, Procuraduría Síndica, Secretaría General, Talento Humano, Tecnologías de la Información, lo cual se muestra en el Anexo E en los planos de la infraestrutura física del edificio.

A continuación se detalla los dispositivos de red ubicados en el cuarto de comunicaciones, con sus respectivas especificaciones técnicas como se muestra en la Tabla 10.

Tabla 10. Características Router CISCO 881

CARACTERÍSTICAS	DESCRIPCIÓN
Cantidad	1
Marca	CISCO
Modelo	881
Memoria RAM	256 MB (Instalados) / 768 MB (máx)
Memoria Flash	128 MB
Protocolo de Direccionamiento	OSPF, RIP-1, RIP-2, BGP, EIGRP, HSRP, VRRP, NHRP, GRE
Protocolo de Interconexión de Datos	Ethernet, Fast Ethernet
Protocolo de Transporte	L2TP, IPSec
Protocolo de Administración Remota	Telnet, SNMPv3, HTTP, HTTPS, SSH

Fuente: Recuperado de http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html

Tabla 11. Características CISCO ASA 5520

FIREWALL ASA	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	CISCO
Modelo	ASA 5520
Número de Usuarios	750
Máximo Rendimiento (Mbps)	225 [Mbps]
Seguridad	Define las interfaces de Red y sus ajustes, maneja la entrada y salida del proveedor de servicios de nube, configura los protocolos de seguridad que soportan los dispositivos, configura los servidores de autenticación, filtros y listas de acceso para interfaces y usuarios.
Puertos	Puertos Ethernet, Puertos MGMT, Puerto de Consola

Fuente: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1932.pdf

Tabla 12. Características Switch CISCO 4503 - E

SWITCH DE CORE	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	CISCO
Modelo	4503-E Supervisor (CORE)
Número de Puertos	12 puertos de alta velocidad, 8 puertos SFP
Interfaces	• WS - X45 - Sup6L -E • WS - X4306 -GB (1000 BASE X)
Seguridad	IPSec, SSH, TLS
Protocolo de Administración Remota	SSH, SNMP, TELNET, TFTP
Estándar	FIPS (Federal Infomation Processing Standards) 140-2 (Security Requirements for Cryptographic Modules)
Software	IOS 12.2 (37) SG

Fuente: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1982.pdf

Tabla 13. Caracteristicas SWITCH CISCO 2960-S

SWITCH 2960-S	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Cantidad	3
Marca	CISCO
Modelo	2960-S
Numero de Puertos	48 Gigabit Ethernet
Protocolo de Administración Remota	RSPAN (Remote Switch Port Analyzer)
Seguridad	• Defensa de amenazas (MAC, IP, ARP spoofing) • TrustSec: permite al usuario asegurar la red, datos y recursos • Otras caracteristicas de seguridad avanzada
Estándares	PoE 802.3af/at

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html

Tabla 14. Características SWITCH CISCO 2960-X

SWITCH 2960-X	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Cantidad	1
Marca	CISCO
Modelo	2960-X
Número d Puertos	48 Gigabit Ethernet
Seguridad	Provee un rango de características de seguridad, para limitar el acceso a la red y mitigar amenazas
Protocolo de Administración remota	RSPAN (Remote Switch Port Analyzer)
Estándares	IEEE 802.1D Spanning Tree Protocol, IEEE 802.3af/ad/at/ah

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html

En la tabla 15 se muestra los equipos de computo correspondientes a esta planta, con sus respectivas características y la VLAN a la que pertenecen.

Tabla 15. Inventario de Equipos de Cómputo Planta Alta 1

N°	Tipo	Dirección	Subdirección	Tipo de Procesador	Velocidad (GHz)	Disco Duro (GB)	RAM (MB)	Sistema Operativo	VLAN
1	ESCRITORIO	Administrativa	Adquisiciones	INTEL CORE 2 DUO	2.2	232	1	Windows 7	10
2	PORTATIL	Administrativa	Administrativo	INTEL CORE 2 DUO	2.2	500	3	Windows 7	10
3	ESCRITORIO	Administrativa	Compras Públicas	INTEL CORE 2 DUO	2.93	290	3.24	Windows XP	10
4	ESCRITORIO	Administrativa	Compras Públicas	INTEL CORE 2 DUO	2.2	232	1	Windows 7	10
5	ESCRITORIO	Administrativa	Compras Públicas	INTEL CELERON	2.6	1000	6	Windows 7	10
6	ESCRITORIO	Administrativa	Compras Públicas	INTEL CORE i7	3.4	500	4	Windows 7	10
7	ESCRITORIO	Administrativa	Administrativo	INTEL CORE 2 DUO	3	298	2	Windows XP	10
8	ESCRITORIO	Administrativa	Administrativo	INTEL CELERON	2.6	1000	2	Windows 7	10
9	ESCRITORIO	Administrativa	Transportes	INTEL CORE i7	2.93	1000	8	Windows 7	10
10	ESCRITORIO	Administrativa	Transportes	INTEL CORE 2 DUO	2.93	298	4	Windows 7	10
11	ESCRITORIO	Administrativa	Transportes	INTEL CORE 2 DUO	2.4	298	2.39	Windows XP	10
12	PORTATIL	Coordinación General	Coordinación General	INTEL CORE i3	2.96	500	4	Windows 7	10

Tabla 15. Inventario de Equipos de Cómputo Planta Alta 1

13	ESCRITORIO	Coordinación General	Secretaria Coordinación General	INTEL PENTIUM R	3.4	160	1	Windows XP	10
14	ESCRITORIO	Financiero	Contabilidad	INTEL CORE 2 DUO	3	300	2	Windows Vista	10
15	ESCRITORIO	Financiero	Contabilidad	INTEL CELERON	2.6	1000	6	Windows 7	10
16	ESCRITORIO	Financiero	Contabilidad	INTEL CELERON	2.6	1000	6	Windows 7	10
17	ESCRITORIO	Financiero	Contabilidad	INTEL CORE 2 DUO	3.6	300	1	Windows XP	10
18	ESCRITORIO	Financiero	Contabilidad	INTEL CORE 2 DUO	2.93	320	4	Windows 7	10
19	ESCRITORIO	Financiero	Dirección Financiera	INTEL CORE i7	3.4	500	4	Windows 7	10
20	ESCRITORIO	Financiero	Tesorería	INTEL PENTIUM 4	3.2	112	0.49	Windows XP	10
21	ESCRITORIO	Financiero	Tesorería	INTEL CORE 2 DUO	3	300	2	Windows XP	10
22	ESCRITORIO	Financiero	Tesorería	INTEL PENTIUM 4	3.2	112	0.48	Windows XP	10
23	ESCRITORIO	Financiero	Secretaría Financiera	INTEL CORE i7	2.8	466	4	Windows 7	10
24	PORTATIL	Financiero	Dirección Financiera	INTEL CORE 2 DUO	2.2	466	3	Windows 7	10

Tabla 15. Inventario de Equipos de Cómputo Planta Alta 1

25	ESCRITORIO	Financiero	Presupuesto	INTEL CORE 2 DUO	2.2	233	1	Windows XP	10
26	ESCRITORIO	Financiero	Presupuesto	INTEL PENTIUM 4	3.4	186	0.49	Windows XP	10
27	ESCRITORIO	Financiero	Presupuesto	INTEL CORE 2 DUO	3	300	1	Windows XP	10
28	ESCRITORIO	PAS (Patronato de Acción Social)	Ciclos de Vida	INTEL CORE i7	3.4	466	4	Windows 7	13
29	ESCRITORIO	PAS (Patronato de Acción Social)	Directora	INTEL CORE i7	3.4	466	4	Windows 7 Professional	13
30	ESCRITORIO	PAS (Patronato de Acción Social)	Contabilidad	INTEL CORE 2 DUO	3	300	3	Windows 7	13
31	ESCRITORIO	PAS (Patronato de Acción Social)	Violencia Intrafamiliar	INTEL PENTIUM R	2	149	1	Windows 7 Professional	13
32	ESCRITORIO	PAS (Patronato de Acción Social)	Analista Desarrollo Social	INTEL CORE 2 DUO	2.93	300	4	Windows Vista	13
33	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad Médica PAS	INTEL PENTIUM R	1.6	230	0.55	Windows XP	13
34	ESCRITORIO	PAS (Patronato de Acción Social)	Compras Públicas	INTEL CORE i7	3.4	500	4	Windows 7	13
35	ESCRITORIO	PAS (Patronato de Acción Social)	Violencia Intrafamiliar	INTEL CORE 2 DUO	2.93	300	4	Windows Vista	13
36	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad Médica PAS	INTEL CORE 2 DUO	2.93	300	4	Windows 7	13

Tabla 15. Inventario de Equipos de Cómputo Planta Alta 1

37	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos	INTEL CORE i3	3.4	466	2	Windows 7	13
38	PORTATIL	PAS (Patronato de Acción Social)	Movilidad Humana	INTEL CORE i5	2.5	466	4	Windows 8	13
39	ESCRITORIO	PAS (Patronato de Acción Social)	Movilidad Humana	INTEL CORE i5	3.16	932	4	Windows 7 Professional	13
40	PORTATIL	PAS (Patronato de Acción Social)	Movilidad Humana	INTEL CORE i7	2.16	600		Windows 7 Home Premium	13
41	ESCRITORIO	PAS (Patronato de Acción Social)	Movilidad Humana	INTEL CORE i5	3.16	300	4	Windows 7	13
42	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos						13
43	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos						13
44	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos	INTEL CORE i3	3.16	47	2	Windows 7	13
45	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos						13
46	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos	INTEL CORE i3	3.16	466	2	Windows 7 Professional	13
47	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos						13
48	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos	INTEL CORE i3	3.3	466	2	Windows 7	13

Tabla 15. Inventario de Equipos de Cómputo Planta Alta 1

49	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos						13
50	ESCRITORIO	PAS (Patronato de Acción Social)	Unidad de Sordos						13
51	ESCRITORIO	PAS (Patronato de Acción Social)	Movilidad Humana	INTEL CORE i5	3.4	200	4	Windows 7	13
52	ESCRITORIO	Prefectura	Asesoría de Prefectura	INTEL CORE i7	2.8	466	4	Windows 7	5
53	ESCRITORIO	Prefectura	Asesoria de Prefectura	INTEL CORE 2 DUO	3		2	Windows 7	5
54	ESCRITORIO	Prefectura	Secretaría de Prefectura	INTEL CORE 2 DUO	3	300	1	Windows 7	5
55	ESCRITORIO	Procuraduría Síndica	Jurídico	INTEL CORE 2 DUO	2.36	300	4	Windows 7	6
56	ESCRITORIO	Procuraduría Síndica	Jurídico	INTEL CORE 2 DUO	2.33	300	4	Windows 7	6
57	ESCRITORIO	Procuraduría Síndica	Jurídico	INTEL CORE i7	3.4	466	4	Windows 7	6
58	ESCRITORIO	Procuraduría Síndica	Jurídico	INTEL CORE i5	3.2	466	2	Windows 7	6
59	ESCRITORIO	Procuraduría Síndica	Jurídico	INTEL CORE i5	3.2	466	2	Windows 7	6
60	ESCRITORIO	Procuraduría Síndica	Jurídico	INTEL CORE 2 DUO	2.66	149	1	Windows 7	6

Tabla 15. Inventario de Equipos de Cómputo Planta Alta 1

61	PORTATIL	Procuraduría Síndica	Jurídico	INTEL CORE i5	2.56	466	4	Windows 7	6
62	ESCRITORIO	Secretaria General	Secretaría General	INTEL PENTIUM 4	2.86	150	0.5	Windows XP	5
63	ESCRITORIO	Secretaria General	Secretaría General	INTEL CORE 2 DUO	3	300	1	Windows XP	5
64	ESCRITORIO	Secretaria General	Pro Secretaría General	INTEL CORE i5	2.53	466	4	Windows 7	5
65	ESCRITORIO	Secretaria General	Secretario General	INTEL CORE 2 DUO	3	466	1	Windows 7	5
66	ESCRITORIO	Talento Humano	Talento Humano	INTEL CORE 2 DUO	3.6	300	1	Windows XP	10
67	ESCRITORIO	Talento Humano	Talento Humano	INTEL CORE 2 DUO	3	300	1	Windows XP	10
68	ESCRITORIO	Talento Humano	Talento Humano	INTEL CORE i7	2.8	466	4	Windows 7	10
69	ESCRITORIO	Talento Humano	Talento Humano	INTEL CORE 2 DUO	2.66	300	1	Windows 7	10
70	ESCRITORIO	Talento Humano	Talento Humano	INTEL CORE 2 DUO	3	300	0.98	Windows XP	10
71	ESCRITORIO	Talento Humano	Talento Humano	INTEL CORE 2 DUO	2.66	300	1	Windows 7	10
72	ESCRITORIO	TIC’s	Dirección de Tecnologías de la Información	INTEL CORE i7	2.93	932	8	Windows 8	4

Tabla 15. Inventario de Equipos de Cómputo Planta Alta 1

73	ESCRITORIO	TIC's	Desarrollo de Software	XEON CPU E3-12220 V2	3.16	1000	16	Windows 7	4
74	PORTATIL	TIC's	Desarrollo de Software	INTEL CORE i5	1.7	300	4	Windows 8	4
75	ESCRITORIO	TIC's	Desarrollo de Software	INTEL CORE i5	3.2	466	4	Windows 7	4
76	PORTATIL	TIC's	Desarrollo de Software	INTEL CORE i7	2	730	6	Windows 7	4
77	PORTATIL	TIC's	Redes de Datos	17 PRIMERA GENERACIÓN	2	500	6	Linux	4
78	PORTATIL	TIC's	Soporte y Control	INTEL CORE i7	2	500	6	Windows 8	4
79	ESCRITORIO	TIC's	Desarrollo Web	INTEL CORE i7	2.93	1000	8	Windows 7	4
80	PORTATIL	TIC's	Desarrollo Web	INTEL CORE i7	2	250	6	Windows 7	4
81	PORTATIL	TIC's	Desarrollo Web	INTEL CORE i7	2.5	500	16	OS y YOSEMITE	4
82	ESCRITORIO	TIC's	Soporte y Control	INTEL CORE i7	2.93	1000	8	Windows 7	4
83	PORTATIL	TIC's	Desarrollo de Software	INTEL CORE i7	2	250	6	Windows 8	4
84	PORTATIL	TIC's	Soporte y Control	INTEL CORE i7	2.93	450	4	Windows 7	4
85	ESCRITORIO	Viceprefectura	Secretaría de Viceprefectura	INTEL CORE 2 DUO	2.33	300	3.23	Windows XP	5
86	ESCRITORIO	Viceprefectura	Asesoría de Viceprefectura	INTEL CORE i7	3.4	500	4		5

Fuente: Prefectura de Imbabura

2.3.2.7.3 Planta alta 2

En la planta alta 2 del edificio se encuentran ubicadas las siguientes direcciones: Cooperación Internacional, Desarrollo Económico y Gestión Ambiental, Planificación y Relaciones Públicas, lo cual se muestra en el Anexo E en los planos de la infraestrutura física del edificio.

En la tabla 16 y 17, se muestran los dispositivos de red ubicados en el rack de la planta alta 2 con sus respectivas especificaciones técnicas.

Tabla 16. Características SWITCH CISCO 2960-S

SWITCH 2960-S	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Cantidad	3
Marca	CISCO
Modelo	2960-s
Número de Puertos	48 Gigabit Ethernet
Protocolo de Administración Remota	RSPAN (Remote Switch Port Analyzer)
Seguridad	• Defensa de amenazas (MAC, IP, ARP spoofing) • TrustSec: permite al usuario asegurar la red, datos y recursos • Otras caracteristicas de seguridad avanzada
Estándares	PoE 802.3af/at

Fuente: Recuperado de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html

Tabla 17. Características Switch MAIPU

Switch MAIPU	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Marca	MAIPU
Modelo	My Power S3152
Número de Puertos	48
Seguridad	Seguridad e puertos, ACL's, filtros de dirección global, Anti-ARP spoofing, Anti-ARP scan
Estándares	IEEE 802.1q VLAN IEEE 802.1x IEEE 802.3u/z/ad/X
Software	IOS 6.1.22 (RL08-bq)

Fuente: Recuperado de http://www.intelek.cz/db/repository.nsf/v/FBB689D5416D4292C125774400257B9C/$file/Datasheet_Maipu_Switch_S3100_Series.pdf

En la tabla 18 se muestran los equipos de cómputo pertenecientes a esta planta, con sus respectivas características y la VLAN a la que pertenecen.

Tabla 18. Inventario de Equipos de Cómputo Planta Alta 2

N°	Tipo	Dirección	Subdirección	Tipo de Procesador	Velocidad (GHz)	Disco Duro (GB)	RAM (MB)	Sistema Operativo	VLAN
1	ESCRITORIO	Contraloría	Contraloría	INTEL CORE 2 DUO	3	300	1	Windows XP	10
2	PORTATIL	Cooperación Internacional	Cooperación Internacional	INTEL CORE i5	2.53	400	4	Windows 7	9
3	PORTATIL	Cooperación Internacional	Cooperación Internacional	INTEL CORE i3	2.2	466	3	Windows 7	9
4	ESCRITORIO	Cooperación Internacional	Cooperación Internacional	INTEL CORE 2 DUO	3	300	1	Windows XP	9
5	ESCRITORIO	Cooperación Internacional	Cooperación Internacional	INTEL CORE 2 DUO	3	320	1	Windows 7	9
6	ESCRITORIO	Cooperación Internacional	Cooperación Internacional	INTEL CORE 2 DUO	2.2	250	1	Windows XP	9
7	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL PENTIUM 4	3.4	149	1	Windows 7	12
8	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Producción	INTEL CORE i7	2.8	112	4	Windows 7	12
9	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Producción	INTEL PENTIUM 4	3.4	149	1	Windows XP	12
10	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL PENTIUM 4	3.4	149	1	Windows XP	12

Tabla 18. Inventario de Equipos de Cómputo Planta Alta 2

11	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL CORE i7	2.93	932	8	Windows 7	12
12	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL PENTIUM 4	3.4	149	1	Windows XP	12
13	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL PENTIUM 4	3.46	149	1	Windows XP	12
14	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL PENTIUM 4	3.2	49	0.49	Windows XP	12
15	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL CORE 2 DUO	3	298	1	Windows 7	12
16	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL CORE 2 DUO	2.2	233	1	Windows XP	12
17	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL PENTIUM 4	3.4	233	0.49	Windows XP	12
18	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Subdirección de Desarrollo Económico	INTEL PENTIUM 4	3.2	112	0.48	Windows XP	12
19	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL PENTIUM R	2.8	186	0.5	Windows 7	12
20	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL CORE 2 DUO	3	300	1	Windows 7	12
21	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL CORE 2 DUO	2.13	233	1.98	Windows XP	12
22	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL PENTIUM R	3.4	233	0.49	Windows XP	12

Tabla 18. Inventario de Equipos de Cómputo Planta Alta 2

23	ESCRITORIO	Desarrollo Económico y Gestión Ambiental Desarrollo Económico		INTEL CORE i7	2,8	500	4	Windows 7	12
24	PORTATIL	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental						12
25	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL CORE 2 DUO	3.6	320	1	Windows 7	12
26	PORTATIL	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL CORE 2 DUO	1.83	300	3	Windows 7	12
27	PORTATIL	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL CORE i5	2.53	500	4	Windows 7	12
28	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Desarrollo Económico	INTEL CORE 2 DUO	3	160	1	Windows XP	12
29	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Gestión Ambiental	INTEL CORE i7	3.4	466	4	Windows 7	12
30	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Proyecto CTB	INTEL PENTIUM 4	2.8	20	0.5	Windows XP	12
31	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Proyecto CEBADA	INTEL CORE 2 DUO	3	300	1	Windows XP	12
32	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Proyecto CEBADA	INTEL CORE 2 DUO	3	300	4	Windows XP	12
33	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Producción	INTEL CORE i7	2.8	699	4	Windows 7 Professional	12
34	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL CORE i7	2.93	932	8	Windows 7	12

Tabla 18. Inventario de Equipos de Cómputo Planta Alta 2

35	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL CORE i7	2.93	932	8	Windows 7	12
36	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL CORE i7	2.8	466	4	Windows 7	12
37	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL CORE i7	3.4	500	4	Windows 7	12
38	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL XEON ®	3.1	1000	16	Windows 7	12
39	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL PENTIUM 4	3.2	59	0.43	Windows XP	12
40	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL XEON ®	3.1	932	8	Windows 7 Professional	12
41	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL PENTIUM 4	3.1	310	4	Windows XP	12
42	ESCRITORIO	Desarrollo Económico y Gestión Ambiental	Recursos Hídricos	INTEL XEON ®	3.1	932	16	Windows 7 Professional	12
43	ESCRITORIO	Planificación	Participación Ciudadana	INTEL CORE i7	2.8	500	4	Windows 7	11
44	ESCRITORIO	Planificación	Planificación	INTEL CORE i7	2.93	932	8	Windows 7	11
45	PORTATIL	Planificación	Proyecto Unión Europea	INTEL CORE i5	1.6		6	Windows 7	11
46	ESCRITORIO	Planificación	Proyecto Unión Europea	INTEL CORE i5	3.1	466	4	Windows 7	11
47	ESCRITORIO	Planificación	Proyecto Unión Europea	INTEL CORE i5	3.1	466	4	Windows 7	11
48	ESCRITORIO	Planificación	Participación Ciudadana	INTEL PENTIUM 4	2.8	186	0.49	Windows XP	11

Tabla 18. Inventario de Equipos de Cómputo Planta Alta 2

49	ESCRITORIO	Planificación	Participación Ciudadana	INTEL CORE i7	2.8	466	4	Windows 7	11
50	ESCRITORIO	Planificación	Participación Ciudadana	INTEL PENTIUM 4	3.2	112	0.49	Windows XP	11
51	ESCRITORIO	Planificación	Planificación	INTEL CORE 2 DUO	3	298	2	Windows 7 Professional	11
52	ESCRITORIO	Planificación	Participación Ciudadana	AMD ATHION II	3	699	2	Windows 7 Professional	11
53	ESCRITORIO	Planificación	Participación Ciudadana	INTEL CORE 2 DUO	3	298	1	Windows XP	11
54	PORTATIL	Planificación	Planificación	INTEL CORE i7	2.9	466	4	Windows 7 Professional	11
55	PORTATIL	Planificación	Participación Ciudadana	INTEL CORE 2 DUO	2.2	466	3	Windows 7	11
56	ESCRITORIO	Planificación	Planificación	INTEL CORE i7	2.93	932	8	Windows 7	11
57	PORTATIL	Planificación	Proyecto Unión Europea	INTEL CORE i7	1.8	1000	8	Windows 8	11
58	PORTATIL	Planificación	Proyecto Unión Europea	INTEL CORE i5	1.6	1000	6	Windows 8	11
59	ESCRITORIO	Planificación	Planificación	INTEL CORE i7	3.4	500	4	Windows 7	11
60	ESCRITORIO	Planificación	Planificación	INTEL CORE 2 DUO	3	299	1	Windows 7 Professional	11
61	PORTATIL	Planificación	Planificación	INTEL CORE i7	2.93	1000	8	Windows 7	11
62	ESCRITORIO	Planificación	Planificación	INTEL CORE i7	2.93	1000	8	Windows 7	11
63	ESCRITORIO	Planificación	Secretaría de Planificación	INTEL CELERON	2.6	1000	6	Windows 7	11

Tabla 18. Inventario de Equipos de Cómputo Planta Alta 2

64	PORTATIL	Planificación	Subdirección de Planificación	INTEL CORE i7	2	700	6	Windows 7	11
65	ESCRITORIO	Relaciones Públicas	Comunicación	INTEL CORE 2 DUO	2.6	149	1	Windows XP	9
66	ESCRITORIO	Relaciones Públicas	Comunicación	AMD EI-2500	1.4	500	4	Windows 8.1 PRO	9
67	ESCRITORIO	Relaciones Públicas	Comunicación	AMD EI-2500	1.4	500	4	Windows 8.1 PRO	9
68	ESCRITORIO	Relaciones Públicas	Comunicación	QUAD CORE INTEL XEON	2.8	1000	6	OS X	9
69	ESCRITORIO	Relaciones Públicas	Comunicación	INTEL CORE 2 DUO	3	299	1	Windows 7	9
70	ESCRITORIO	Relaciones Públicas	Comunicación	iMAC CORE i7	3.4	1000	8	OS X	9
71	ESCRITORIO	Relaciones Públicas	Comunicación	AMD EI-2500	1.4	500	4	Windows 8.1 PRO	9
72	ESCRITORIO	Relaciones Públicas	Comunicación	INTEL CORE 2 DUO	2.6	160	1	Windows XP	9
73	ESCRITORIO	Relaciones Públicas	Comunicación	INTEL CORE 2 DUO	3	300	2	Windows 7	9
74	PORTATIL	Relaciones Públicas	Comunicación	INTEL CORE i5	2.53	500	4	Windows 7	9

Fuente: Prefectura de Imbabura

2.3.2.8 Direccionamiento IP

La red se encuentra conectada mediante la dirección pública 181.113.x.x /x, y tiene un direccionamiento IP privado previamente configurado, dividido en 24 VLANs con dirección 172.16.x.x /x, el cual está mostrado en la tabla 19.

Tabla 19. Distribución de VLANs de la Prefectura de Imbabura

NOMBRE VLAN	ID VLAN	RED	GATEWAY	INTERVALOS	BROADCAST
ADMINISTRACIÓN DE EQUIPOS	2	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
SERVIDORES	3	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
GESTIÓN TECNOLÓGICA	4	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
PREFECTURA	5	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
PROCURADURÍA	6	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
PLANIFICACION	7	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
GESTIÓN TÉCNICA	8	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
RELACIONES PÚBLICAS	9	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
ADMINISTRACIÓN GENERAL	10	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
INFRAESTRUCTURA FÍSICA	11	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
DESARROLLO ECONÓMICO	12	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
PAS	13	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
WIFI	14	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x

Tabla 19. Distribución de VLANs de la Prefectura de Imbabura

WIFI EXTERNA	15	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
BODEGA	16	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
FAUSTO-GIS	17	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
FISCALIZACIÓN	18	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
CONTRATACIÓN PÚBLICA	19	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
INVITADOS	30	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
RELOJES BIOMÉTRICOS	31	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
CÁMARAS	32	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
TELEFONÍA	40	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
MUTUALISTA	50	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x
ENLACE DE EQUIPOS	101	172.16.x.x/24	172.16.x.x	172.16.x.x – 172.16.x.x	172.16.x.x

Fuente: Prefectura de Imbabura

2.3.2.9 Distribución de IP públicas hacia los servidores

La distribución de IPs públicas para los distintos servidores que maneja la Prefectura de Imbabura se muestra en la Tabla 20.

Tabla 20. Distribución de IP Públicas Prefectura de Imbabura

IP PUBLICA	SERVIDOR	IP PRIVADA
181.113.x.x	Red	
181.113.x.x	Router CNT	
181.113.x.x	ASA	
181.113.x.x	www.imbabura.gob.ec	172.16.x.x
181.113.x.x	mail.imbabura.gob.ec	
181.113.x.x	www.imbabura.travel	172.16.x.x
181.113.x.x	documentacion.imbabura.gob.ec	
181.113.x.x	www.gisimbabura.gob.ec	172.16.x.x
181.113.x.x	Servidor GIS	
181.113.x.x	Estación base GIS	
181.113.x.x	intranet.imbabura.gob.ec www.gpi.gob.ec	172.16.x.x
181.113.x.x	gestion.imbabura.gob.ec www.gpigestion.gob.ec	172.16.x.x
181.113.x.x	build.imbabura.gob.ec	
181.113.x.x	live.imbabura.gob.ec	172.16.x.x
181.113.x.x	www.imbaburaturismo.gob.ec	172.16.x.x
181.113.x.x	www.chachimbiroep.gob.ec	
181.113.x.x	www.patronatoimbabura.gob.ec	
181.113.x.x	www.imbavial.gob.ec	172.16.x.x
181.113.x.x	Seguimiento vehículos Imbavial	

Fuente: Prefectura de Imbabura

2.3.2.10 Mapeo de la red

El mapeo de la red está dado por los puertos del Switch de acceso, esta información se obtuvo luego de realizar el estudio de la situación actual de la Prefectura de Imbabura, y no es susceptible a modificaciones ya que fue previamente revisada por el Director de TIC's.

La nomenclatura que se utiliza es la siguiente:

PB: Planta Baja

PA1: Planta Alta 1

PA2: Planta Alta 2

D: Punto (Datos, Video, Telefonía)

A: Rack (Identifica el rack)

En la tabla 21 se muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 1 de la planta baja están conectados.

Tabla 21. Distribución de Puntos de Cableado Planta Baja Switch 1

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS SWITCH**	**NOMBRE**
PB-D1	11	172.16.x.x (PUERTO 1)	INFRAESTRUCTURA FÍSICA
PB-D2	11	PUERTO 2	INFRAESTRUCTURA FÍSICA
PB-D3	17	PUERTO 3	GIS
PB-D4	11	PUERTO 4	INFRAESTRUCTURA FÍSICA
PB-D5	11	PUERTO 5	INFRAESTRUCTURA FÍSICA
PB-D6	11	PUERTO 6	INFRAESTRUCTURA FÍSICA
PB-D7	11	PUERTO 7	INFRAESTRUCTURA FÍSICA
PB-D8	11	PUERTO 8	INFRAESTRUCTURA FÍSICA
PB-D9	11	PUERTO 9	INFRAESTRUCTURA FÍSICA
PB-D10	14	PUERTO 10	WIFI
PB-D11	11	PUERTO 11	INFRAESTRUCTURA FÍSICA
PB-D12	11	PUERTO 12	INFRAESTRUCTURA FÍSICA
PB-D13	11	PUERTO 13	INFRAESTRUCTURA FÍSICA
PB-D14	11	PUERTO 14	INFRAESTRUCTURA FÍSICA
PB-D15	18	PUERTO 15	FISCALIZACIÓN
PB-D16	18	PUERTO 16	FISCALIZACIÓN
PB-D17	18	PUERTO 17	FISCALIZACIÓN
PB-D18	12	PUERTO 18	DESARROLLO ECONÓMICO
PB-D19	12	PUERTO 19	DESARROLLO ECONÓMICO
PB-D20	12	PUERTO 20	DESARROLLO ECONÓMICO
PB-D21	12	PUERTO 21	DESARROLLO ECONÓMICO
PB-D22	32	PUERTO 22	CAMARAS HALL
PB-D23	32	PUERTO 23	INFORMACIÓN

Tabla 21. Distribución de Puntos de Cableado Planta Baja Switch 1

PB-D24	5	PUERTO 24	INFORMACIÓN
PB-D25	5	PUERTO 25	INFORMACIÓN
PB-D26	14	PUERTO 26	AP
PB-D27	11	PUERTO 27	SALA DE REUNIONES
PB-D28	11	PUERTO 28	SALA DE REUNIONES
PB-D29	32	PUERTO 29	CÁMARA BIOMÉTRICOS
PB-D30	31	PUERTO 30	RELOJES BIOMÉTRICOS
PB-D31	31	PUERTO 31	RELOJES BIOMÉTRICOS
PB-D32	11	PUERTO 32	INFRAESTRUCTURA FÍSICA
PB-D33	11	PUERTO 33	INFRAESTRUCTURA FÍSICA
PB-D34	17	PUERTO 34	GIS
PB-D35	11	PUERTO 35	INFRAESTRUCTURA FÍSICA
PB-D36	14	PUERTO 36	WIFI INFRAESTRUCTURA
PB-D37	11	PUERTO 37	INFRAESTRUCTURA FÍSICA
PB-D38	11	PUERTO 38	INFRAESTRUCTURA FÍSICA
PB-D39	11	PUERTO 39	INFRAESTRUCTURA FÍSICA
PB-D40	11	PUERTO 40	INFRAESTRUCTURA FÍSICA
PB-D41	11	PUERTO 41	INFRAESTRUCTURA FÍSICA
PB-D42	18	PUERTO 42	INFRAESTRUCTURA FÍSICA
PB-D43	11	PUERTO 43	INFRAESTRUCTURA FÍSICA
PB-D44	11	PUERTO 44	INFRAESTRUCTURA FÍSICA
PB-D45	11	PUERTO 45	INFRAESTRUCTURA FÍSICA
PB-D46	18	PUERTO 46	FISCALIZACIÓN
PB-D47	ENLACE PB-PA1	ENLACE PB-PA1	

Fuente: Prefectura de Imbabura

La tabla 22 muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 2 de la planta baja están conectados.

Tabla 22. Distribución de Puntos de Cableado Planta Baja Switch 2

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS SWITCH**	**NOMBRE**
PB-D48	ENLACE PB-PA1	ENLACE PB-PA1	
PB-D49	12	172.16.x.x (PUERTO 1)	DESARROLLO ECONÓMICO
PB-D50	12	PUERTO 2	DESARROLLO ECONÓMICO
PB-D51	12	PUERTO 3	DESARROLLO ECONÓMICO
PB-D52	18	PUERTO 4	FISCALIZACIÓN
PB-D53	18	PUERTO 5	FISCALIZACIÓN
PB-D54	10	PUERTO 6	ADMINISTRACIÓN GENERAL
PB-D55	10	PUERTO 7	TRABAJO SOCIAL
PB-D56	10	PUERTO 8	ARCHIVO
PB-D57	10	PUERTO 9	ARCHIVO
PB-D58	10	PUERTO 10	ARCHIVO
PB-D59	10	PUERTO 11	ODONTÓLOGO
PB-D60	32	PUERTO 12	CÁMARA HALL PASILLO
PB-D61	31	PUERTO 13	CÁMARA FRENTE GARITA
PB-D62	40	PUERTO 14	GUARDIA
PB-D63	18	PUERTO 15	FISCALIZACIÓN
PB-D64	18	PUERTO 16	FISCALIZACIÓN

Fuente: Prefectura de Imbabura

En la tabla 23 se muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 1 ubicado en el cuarto de comunicaciones de la planta alta 1, están conectados.

Tabla 23. Distribución de Puntos de Cableado Planta Alta 1 Switch 1

GPI-PLANTA ALTA 1			
PUNTOS	**VLAN**	**PUERTOS SWITCH**	**NOMBRE**
PA1-D1	5	172.16.x.x (PUERTO 1)	PREFECTURA
PA1-D2	5	PUERTO 2	PREFECTURA
PA1-D3	5	PUERTO 3	PREFECTURA
PA1-D4	5	PUERTO 4	PREFECTURA
PA1-D5	5	PUERTO 5	PREFECTURA
PA1-D6	5	PUERTO 6	PREFECTURA
PA1-D7	5	PUERTO 7	PREFECTURA

Tabla 23. Distribución de Puntos de Cableado Planta Alta 1 Switch 1

PA1-D8	5	PUERTO 8	PREFECTURA
PA1-D9	5	PUERTO 9	PREFECTURA
PA1-D10	5	PUERTO 10	PREFECTURA
PA1-D11	5	PUERTO 11	PREFECTURA
PA1-D12	9	PUERTO 12	RELACIONES PÚBLICAS
PA1-D13	9	PUERTO 13	RELACIONES PÚBLICAS
PA1-D14	5	PUERTO 14	PREFECTURA
PA1-D15	5	PUERTO 15	PREFECTURA
PA1-D16	5	PUERTO 16	PREFECTURA
PA1-D17	5	PUERTO 17	AP
PA1-D18	5	PUERTO 18	PREFECTURA
PA1-D19	5	PUERTO 19	PREFECTURA
PA1-D20	5	PUERTO 20	PREFECTURA
PA1-D21	5	PUERTO 21	PREFECTURA
PA1-D22	5	PUERTO 22	PREFECTURA
PA1-D23	5	PUERTO 23	PREFECTURA
PA1-D24	5	PUERTO 24	PREFECTURA
PA1-D25	6	PUERTO 25	PROCURADURÍA
PA1-D26	6	PUERTO 26	PROCURADURÍA
PA1-D27	6	PUERTO 27	PROCURADURÍA
PA1-D28	6	PUERTO 28	PROCURADURÍA
PA1-D29	6	PUERTO 29	PROCURADURÍA
PA1-D30	6	PUERTO 30	PROCURADURÍA
PA1-D31	6	PUERTO 31	PROCURADURÍA
PA1-D32	10	PUERTO 32	ADMINISTRACIÓN GENERAL
PA1-D33	10	PUERTO 33	ADMINISTRACIÓN GENERAL
PA1-D34	10	PUERTO 34	ADMINISTRACIÓN GENERAL
PA1-D35	10	PUERTO 35	ADMINISTRACIÓN GENERAL
PA1-D36	10	PUERTO 36	ADMINISTRACIÓN GENERAL
PA1-D37	10	PUERTO 37	ADMINISTRACIÓN GENERAL
PA1-D38	10	PUERTO 38	ADMINISTRACIÓN GENERAL
PA1-D39	10	PUERTO 39	ADMINISTRACIÓN GENERAL
PA1-D40	9	PUERTO 40	RELACIONES PÚBLICAS
PA1-D41	9	PUERTO 41	RELACIONES PÚBLICAS
PA1-D42	4	PUERTO 42	GESTIÓN TECNOLÓGICA

Tabla 23. Distribución de Puntos de Cableado Planta Alta 1 Switch 1

PA1-D43	4	PUERTO 43	GESTIÓN TECNOLÓGICA
PA1-D44	4	PUERTO 44	GESTIÓN TECNOLÓGICA
PA1-D45	4	PUERTO 45	GESTIÓN TECNOLÓGICA
PA1-D46	4	PUERTO 46	GESTIÓN TECNOLÓGICA

Fuente: Prefectura de Imbabura

En la tabla 24 se muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 2 ubicado en el cuarto de comunicaciones de la planta alta 1, están conectados.

Tabla 24. Distribución de Puntos de Cableado Planta Alta 1 Switch 2

GPI-PLANTA ALTA 1			
PUNTOS	**VLAN**	**PUERTOS SWITCH**	**NOMBRE**
PA1-D47	4	172.16.x.x (PUERTO 1)	GESTIÓN TECNOLÓGICA
PA1-D48	4	PUERTO 2	GESTIÓN TECNOLÓGICA
PA1-D49	10	PUERTO 3	ADMINISTRACIÓN GENERAL
PA1-D50	10	PUERTO 4	ADMINISTRACIÓN GENERAL
PA1-D51	10	PUERTO 5	ADMINISTRACIÓN GENERAL
PA1-D52	4	PUERTO 6	GESTIÓN TECNOLÓGICA
PA1-D53	10	PUERTO 7	ADMINISTRACIÓN GENERAL
PA1-D54	10	PUERTO 8	ADMINISTRACIÓN GENERAL
PA1-D55	10	PUERTO 9	ADMINISTRACIÓN GENERAL
PA1-D56	4	PUERTO 10	GESTIÓN TECNOLÓGICA
PA1-D57	4	PUERTO 11	GESTIÓN TECNOLÓGICA
PA1-D58	4	PUERTO 12	GESTIÓN TECNOLÓGICA
PA1-D59	10	PUERTO 13	ADMINISTRACIÓN GENERAL
PA1-D60	4	PUERTO 14	GESTIÓN TECNOLÓGICA
PA1-D61	10	PUERTO 15	ADMINISTRACIÓN GENERAL
PA1-D62	10	PUERTO 16	ADMINISTRACIÓN GENERAL
PA1-D63	10	PUERTO 17	ADMINISTRACIÓN GENERAL
PA1-D64	10	PUERTO 18	ADMINISTRACIÓN GENERAL
PA1-D65	10	PUERTO 19	ADMINISTRACIÓN GENERAL
PA1-D66	10	PUERTO 20	ADMINISTRACIÓN GENERAL
PA1-D67	10	PUERTO 21	ADMINISTRACIÓN GENERAL

Tabla 24. Distribución de Puntos de Cableado Planta Alta 1 Switch 2

PA1-D68	10	PUERTO 22	ADMINISTRACIÓN GENERAL
PA1-D69	10	PUERTO 23	ADMINISTRACIÓN GENERAL
PA1-D70	10	PUERTO 24	ADMINISTRACIÓN GENERAL
PA1-D71	10	PUERTO 25	ADMINISTRACIÓN GENERAL
PA1-D72	10	PUERTO 26	ADMINISTRACIÓN GENERAL

Fuente: Prefectura de Imbabura

En la tabla 25 se muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 3 de la planta alta 1 ubicado en el cuarto de comunicaciones de la planta alta 1, están conectados.

Tabla 25. Distribución de Puntos de Cableado Planta Alta 1 Switch 3

GPI-PLANTA ALTA 1			
PUNTOS	**VLAN**	**PUERTOS SWITCH**	**NOMBRE**
PA1-D73	5	172.16.x.x (PUERTO 1)	PREFECTURA
PA1-D74	5	PUERTO 2	PREFECTURA
PA1-D75	5	PUERTO 3	PREFECTURA
PA1-D76	6	PUERTO 4	AP PROCURADURIA
PA1-D77	5	PUERTO 5	PREFECTURA
PA1-D78	5	PUERTO 6	PREFECTURA
PA1-D79	10	PUERTO 7	ADMINISTRACIÓN GENERAL
PA1-D80	5	PUERTO 8	PREFECTURA
PA1-D81	5	PUERTO 9	PREFECTURA
PA1-D82	5	PUERTO 10	PREFECTURA
PA1-D83	5	PUERTO 11	PREFECTURA
PA1-D84	9	PUERTO 12	RELACIONES PÚBLICAS
PA1-D85	4	PUERTO 37	PROYECTOR GESTIÓN TECNOLÓGICA
PA1-D86	9	PUERTO 36	RELACIONES PÚBLICAS
PA1-D87	5	PUERTO 35	PREFECTURA
PA1-D88	10	PUERTO 34	ADMINISTRACIÓN GENERAL
PA1-D89	10	PUERTO 33	ADMINISTRACIÓN GENERAL

Tabla 25. Distribución de Puntos de Cableado Planta Alta 1 Switch 2

PA1-D90	9	PUERTO 32	RELACIONES PÚBLICAS
PA1-D91	9	PUERTO 31	RELACIONES PÚBLICAS
PA1-D92	10	PUERTO 30	ADMINISTRACIÓN GENERAL
PA1-D93	10	PUERTO 29	ADMINISTRACIÓN GENERAL
PA1-D94	10	PUERTO 28	ADMINISTRACIÓN GENERAL
PA1-D95	10	PUERTO 27	ADMINISTRACIÓN GENERAL
PA1-D96	10	PUERTO 26	ADMINISTRACIÓN GENERAL
PA1-D97	10	PUERTO 25	ADMINISTRACIÓN GENERAL
PA1-D98	10	PUERTO 24	ADMINISTRACIÓN GENERAL
PA1-D99	10	PUERTO 23	ADMINISTRACIÓN GENERAL
PA1-D100	10	PUERTO 22	ADMINISTRACIÓN GENERAL
PA1-D101	10	PUERTO 21	ADMINISTRACIÓN GENERAL
PA1-D102	4	PUERTO 20	GESTIÓN TECNOLÓGICA
PA1-D103	4	PUERTO 19	GESTIÓN TECNOLÓGICA
PA1-D104	4	PUERTO 18	GESTIÓN TECNOLÓGICA
PA1-D105	6	PUERTO 17	PROCURADURÍA
PA1-D106	10	PUERTO 16	ADMINISTRACIÓN GENERAL
PA1-D107	4	PUERTO 15	GESTIÓN TECNOLÓGICA
PA1-D108	10	PUERTO 14	ADMINISTRACIÓN GENERAL
PA1-D109	4	PUERTO 13	CAMARA GESTIÓN TECNOLÓGICA
PA1-D110	4	PUERTO 38	CAMARA GESTIÓN TECNOLÓGICA

Fuente: Prefectura de Imbabura

En la tabla 26 se muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 1 de la planta alta 2, están conectados.

Tabla 26. Distribución de Puntos de Cableado Planta Alta 2 Switch 1

GPI-PLANTA ALTA 2			
PUNTOS	**VLAN**	**PUERTOS SWITCH**	**NOMBRE**
PA2-D1	7	172.16.x.x (PUERTO 1)	PLANIFICACIÓN (AP)
PA2-D2	7	PUERTO 2	PLANIFICACIÓN
PA2-D3	7	PUERTO 3	PLANIFICACIÓN
PA2-D4	7	PUERTO 4	PLANIFICACIÓN

Tabla 26. Distribución de Puntos de Cableado Planta Alta 2 Switch 1

PA2-D5	7	PUERTO 5	PLANIFICACIÓN
PA2-D6	7	PUERTO 6	PLANIFICACIÓN
PA2-D7	7	PUERTO 7	PLANIFICACIÓN
PA2-D8	7	PUERTO 8	PLANIFICACIÓN
PA2-D9	7	PUERTO 9	PLANIFICACIÓN
PA2-D10	7	PUERTO 10	PLANIFICACIÓN
PA2-D11	7	PUERTO 11	PLANIFICACIÓN
PA2-D12	7	PUERTO 12	PLANIFICACIÓN
PA2-D13	7	PUERTO 13	PLANIFICACIÓN
PA2-D14	7	PUERTO 14	PLANIFICACIÓN
PA2-D15	7	PUERTO 15	PLANIFICACIÓN
PA2-D16	17	PUERTO 16	FAUSTO GIS
PA2-D17	7	PUERTO 17	PLANIFICACIÓN
PA2-D18	7	PUERTO 18	PLANIFICACIÓN
PA2-D19	17	PUERTO 19	FAUSTO GIS
PA2-D20	17	PUERTO 20	FAUSTO GIS
PA2-D21	7	PUERTO 21	PLANIFICACIÓN
PA2-D22	7	PUERTO 22	PLANIFICACIÓN
PA2-D23	7	PUERTO 23	PLANIFICACIÓN
PA2-D24	7	PUERTO 24	PLANIFICACIÓN (AP)
PA2-D25	17	PUERTO 25	FAUSTO GIS
PA2-D26	8	PUERTO 26	GESTIÓN TÉCNICA
PA2-D27	8	PUERTO 27	GESTIÓN TÉCNICA
PA2-D28	8	PUERTO 28	GESTIÓN TÉCNICA
PA2-D29		PUERTO 29	SALA DE REUNIONES
PA2-D30		PUERTO 30	SALA DE REUNIONES
PA2-D31		PUERTO 31	TURISMO
PA2-D32		PUERTO 32	TURISMO
PA2-D33		PUERTO 33	TURISMO
PA2-D34		PUERTO 34	TURISMO
PA2-D35		PUERTO 35	FORESTACIÓN Y BIODEVERSIDAD
PA2-D36		PUERTO 36	FORESTACIÓN Y BIODEVERSIDAD
PA2-D37		PUERTO 37	FORESTACIÓN Y BIODEVERSIDAD
PA2-D38		PUERTO 38	FORESTACIÓN Y BIODEVERSIDAD
PA2-D39		PUERTO 39	FORESTACIÓN Y BIODEVERSIDAD

Tabla 26. Distribución de Puntos de Cableado Planta Alta 2 Switch 1

PA2-D40		PUERTO 40	CUENCAS HIDROGRÁFICAS
PA2-D41		PUERTO 41	CUENCAS HIDROGRÁFICAS
PA2-D42		PUERTO 42	CUENCAS HIDROGRÁFICAS
PA2-D109	13	PUERTO 43	RADIO PAS
PA2-D110	50	PUERTO 44	RADIO BODEGA
PA2-D111	50	PUERTO 45	RADIO UBIQUITI
PA2-D113	50	PUERTO 46	RADIO UBIQUITI
PA2-D112	TRUNK	PUERTO 47	RADIO MUTUALISTA

Fuente: Prefectura de Imbabura

En la tabla 27 se muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 2 de la planta alta 2, están conectados.

Tabla 27. Distribución de Puntos de Cableado Planta Alta 2 Switch 2

GPI-PLANTA ALTA 2			
PUNTOS	**VLAN**	**PUERTOS SWITCH**	**NOMBRE**
PA2-D48		172.16.x.x (PUERTO 1)	
PA2-D49	12	PUERTO 2	DESARROLLO ECONÓMICO
PA2-D50	12	PUERTO 3	DESARROLLO ECONÓMICO
PA2-D51	12	PUERTO 4	DESARROLLO ECONÓMICO
PA2-D52	12	PUERTO 5	DESARROLLO ECONÓMICO
PA2-D53	12	PUERTO 6	DESARROLLO ECONÓMICO
PA2-D54	12	PUERTO 7	DESARROLLO ECONÓMICO
PA2-D55	12	PUERTO 8	DESARROLLO ECONÓMICO
PA2-D56	12	PUERTO 9	DESARROLLO ECONÓMICO
PA2-D57	12	PUERTO 10	DESARROLLO ECONÓMICO
PA2-D58	12	PUERTO 11	DESARROLLO ECONÓMICO
PA2-D59		PUERTO 12	EDUCACIÓN Y GESTIÓN AMBIENTAL
PA2-D60	12	PUERTO 13	DESARROLLO ECONÓMICO
PA2-D61	12	PUERTO 14	DESARROLLO ECONÓMICO
PA2-D62	12	PUERTO 15	DESARROLLO ECONÓMICO
PA2-D63	12	PUERTO 16	DESARROLLO ECONÓMICO
PA2-D64	9	PUERTO 17	RELACIONES PÚBLICAS

Tabla 27. Distribución de Puntos de Cableado Planta Alta 2 Switch 2

PA2-D65	9	PUERTO 18	RELACIONES PÚBLICAS
PA2-D66	9	PUERTO 19	RELACIONES PÚBLICAS
PA2-D67	9	PUERTO 20	RELACIONES PÚBLICAS
PA2-D68	12	PUERTO 21	DESARROLLO ECONÓMICO
PA2-D69	12	PUERTO 22	DESARROLLO ECONÓMICO
PA2-D70	12	PUERTO 23	DESARROLLO ECONÓMICO
PA2-D71	12	PUERTO 24	DESARROLLO ECONÓMICO
PA2-D72	12	PUERTO 25	DESARROLLO ECONÓMICO
PA2-D73	12	PUERTO 26	DESARROLLO ECONÓMICO
PA2-D74	12	PUERTO 27	DESARROLLO ECONÓMICO
PA2-D75	12	PUERTO 28	DESARROLLO ECONÓMICO
PA2-D76	12	PUERTO 29	DESARROLLO ECONÓMICO
PA2-D77	12	PUERTO 30	DESARROLLO ECONÓMICO
PA2-D78	12	PUERTO 31	DESARROLLO ECONÓMICO
PA2-D79	12	PUERTO 32	DESARROLLO ECONÓMICO
PA2-D80	12	PUERTO 33	DESARROLLO ECONÓMICO
PA2-D81	12	PUERTO 34	DESARROLLO ECONÓMICO
PA2-D82	12	PUERTO 35	DESARROLLO ECONÓMICO
PA2-D83	12	PUERTO 36	DESARROLLO ECONÓMICO
PA2-D84	12	PUERTO 37	DESARROLLO ECONÓMICO
PA2-D85	12	PUERTO 38	DESARROLLO ECONÓMICO
PA2-D86	12	PUERTO 39	DESARROLLO ECONÓMICO
PA2-D87	12	PUERTO 40	DESARROLLO ECONÓMICO
PA2-D88	12	PUERTO 41	DESARROLLO ECONÓMICO
PA2-D89	12	PUERTO 42	DESARROLLO ECONÓMICO
PA2-D90		PUERTO 43	EDUCACIÓN Y GESTIÓN AMBIENTAL
PA2-D91	12	PUERTO 44	DESARROLLO ECONÓMICO
PA2-D92	12	PUERTO 45	DESARROLLO ECONÓMICO
PA2-D93	12	PUERTO 46	DESARROLLO ECONÓMICO
		PUERTO 47	OBS: PUERTO 47-48 TRUNK

Fuente: Prefectura de Imbabura

En la tabla 28 se muestra la distribución dada para los puntos de red de los departamentos que conforman la institución, se indica a que VLAN pertenece cada uno y a que puerto del Switch 3 de la planta alta 2, están conectados.

Tabla 28. Distribución de Puntos de Cableado Planta Alta 2 Switch 3 (MAIPU)

GPI-PLANTA ALTA 2			
PUNTOS	**VLAN**	**PUERTOS SWTICH**	**NOMBRE**
PA2-D94	12	172.16.x.x (PUERTO 1)	DESARROLLO ECONÓMICO
PA2-D95	12	PUERTO 2	DESARROLLO ECONÓMICO
PA2-D96	12	PUERTO 3	DESARROLLO ECONÓMICO
PA2-D97	12	PUERTO 4	DESARROLLO ECONÓMICO
PA2-D98	12	PUERTO 5	DESARROLLO ECONÓMICO
PA2-D99	12	PUERTO 6	DESARROLLO ECONÓMICO
PA2-D100	9	PUERTO 7	RELACIONES PÚBLICAS
PA2-D101	9	PUERTO 8	RELACIONES PÚBLICAS
PA2-D102	9	PUERTO 9	RELACIONES PÚBLICAS
PA2-D103	9	PUERTO 10	RELACIONES PÚBLICAS
PA2-D104	9	PUERTO 11	RELACIONES PÚBLICAS
PA2-D105	9	PUERTO 12	RELACIONES PÚBLICAS
PA2-D106		PUERTO 13	CONTRALORÍA
PA2-D107		PUERTO 14	CONTRALORÍA
PA2-D108	9	PUERTO 15	RELACIONES PÚBLICAS

Fuente: Prefectura de Imbabura

2.3.2.11 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 red de la Prefectura de Imbabura , se procede a la implementación del modelo de gestión ISO en conjunto con la elección del software de monitoreo.

Capitulo 3.

3. Implementación del modelo de gestión, monitoreo de la red y establecimiento de políticas.

En este capítulo se realizó del SRS (Software Requirements Specifications) planteado por el estándar IEEE 29148, el cual consiste de un informe detallado sobre los requerimientos del sistema para escoger la mejor alternativa de software libre, también se efectuó la implementación del modelo ISO, utilizando el modelo de gestión FCAPS con sus pasos correspondientes. Se especifica las políticas de gestión y el manual de procedimientos que se implementarán de acuerdo a las necesidades de la institución.

3.1 Implementación del modelo de gestión

Para la implementación del modelo de gestión propuesto por la ISO se aplican sus cinco áreas funcionales las cuales fueron descritas en el apartado 2.1.3.

3.1.1 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 elemento de la red.

3.1.1.1 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 29 se muestran varios tipos de software de monitoreo identificando las prestaciones que estos brindan.

Tabla 29. Comparación de Software de Monitoreo

NOMBRE	CACTI	ZENOSS	NMAP	OP MANAGER	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

Fuente: Recuperado de http://gestoresdered.blogspot.com/2012/05/monitoreo-de-red.html

3.1.1.1.1 Estandar IEEE 29148

IEEE (2011), 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." IEEE (2011)

3.1.1.1.2 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. Este se muestra en el documento presentado a continuación:

DOCUMENTO DE ESPECIFICACIÓN DE REQUERIMIENTOS	
PREFECTURA DE IMBABURA	**CASO:** Prefectura de Imbabura
Realizado por	Sara Carolina Cuchala Vásquez
Revisado por	Ing. Fernando Miño / Director de TIC's

CONTENIDOS

1. Introducción
   - 1.1 Propósito del sistema
   - 1.2 Alcance del sistema
2. Descripción general del producto
   - 2.1 Perspectiva del producto
   - 2.2 Funciones del producto
   - 2.3 Características del usuario
   - 2.4 Limitaciones
3. Referencias
4. Requerimientos del Sistema
   - 4.1 Requerimientos funcionales
   - 4.2 Requerimientos mínimos
   - 4.3 Estructura del sistema

1. INTRODUCCION

1.1 Propósito del Sistema

La Prefectura de Imbabura ha visto la necesidad de la implementación de un software de monitorización orientado a todo tipo de entornos y que sea suficientemente flexible como para gestionar y controlar toda la infraestructura de red.

La Dirección de Tecnología de Información de la entidad tiene como propósito que este sistema debe ser capaz de monitorear en la misma plataforma; herramientas, sistemas de última generación, dispositivos de red antiguos, de difícil acceso y poca compatibilidad.

1.2 Alcance del Sistema

El software de gestión y monitoreo debe soportar dispositivos de red, servidores y equipos de computo, con sistemas operativos de software libre como CentOS y sistemas operativos que no tienen licencia gratuita como Windows o Mac OS.

El software deberá poder emplearse con éxito no sólo para el monitoreo del sistema, sino para todo tipo de dispositivos de red, ya sea usando SNMP (versiones 1,2,3), o mediante los protocolos TCP, SMP, FTP, DNS, HTTP, ICMP o UDP.

2. DESCRIPCIÓN GENERAL DEL PRODUCTO

2.1 Perspectiva del Producto

Se solicita que el software inicialmente sea 100% de código abierto, pero con su implementación y pruebas correspondientes de su correcto funcionamiento, si este tiene una versión pagada se considerará adquirirla en un futuro.

El sistema de gestión y monitoreo debe poder procesar grandes volúmenes de información y trabajar con varios dispositivos a la vez.

2.2 Funciones del Producto

- *Auto descubrimiento:* el software debe permitir detectar los discos duros, las particiones o las bases de datos en un servidor.
- *Auto exploración:* En remoto, y usando la red, debe detectar los sistemas activos, catalogarlos según su sistema operativo, y empezar a monitorizarlos, además debe realizar la topología de red de lo servicios monitoreados
- *Monitorizar:* el sistema debe obtener información de los dispositvos conectados, permitir añadir equipos, generar reportes y brindar una interfaz gráfica para su manejo.
- *Controlar:* Es necesario que el software permita realizar tareas como levantar servicios, borrar ficheros temporales o ejecutar procesos, arrancar servicios, etc de manera remota
- *Alertar y notificar:* Tan importante como detectar un fallo es avisar de él. El sistema debe brindar una variedad de formas y formatos de notificación. Se solicita que estos informes puedan ser enviados al correo electrónico del administrador de la red.
- *Visualizar y analizar:* Monitorizar no sólo es recibir un trap o visualizar un servicio caído, es presentar informes de tendencias, gráficas resumen de datos, generar portales de usuarios, delegar informes a terceros o definir sus propias gráficas y tablas. Por lo que el software escogido debe brindar todas estas funciones.
- *Inventariar:* Debe permitir realizar inventarios flexibles y dinámicos, notificar cambios los cuales podrán ser usados para elaborar listados.

2.3 Características del Usuario

- Administrador de red con conocimiento técnico.
- Operadores con conocimientos técnicos de la situación, o conocimiento puntual de algún servicio.
- La estructura administrativa de la Dirección de Tecnologías de Información de la Prefectura de Imbabura permite que una persona, o varias, encargadas del funcionamiento de la red miren constantemente el sistema.

2.4 Limitaciones

La falta de información sobre sistemas de monitoreo han hecho que no se implemente un software que realice esta función a pesar de la necesidad que existe de conocer constantemente el estado de la red

3. REFERENCIAS

- www.imbabura.gob.ec

- Ing. Fernando Miño / Director de Departamento de Tecnologías de Información de la Prefectura de Imbabura
- Ing. Jaime Chuga / Ingeniero de Infraestructura de Departamento de Tecnologías de Información de la Prefectura de Imbabura

4. REQUERIMIENTOS DEL SISTEMA

4.1 Requerimientos Funcionales

- Gestión y monitoreo de dispositivos de red
- Monitoreo de servidores Windows y Linux
- Generación de informes
- Reconocimiento automático de la red
- Manejo de varios dispositivos de red a la vez
- Fácil instalación
- Interfaz gráfica
- Envío de notificaciones por correo electrónico

4.2 Requerimientos de usabilidad

El software debe permitir que el ingreso al sistema sea mediante un solo usuario y contraseña para que el jefe de recursos quien es el responsable de la red, designe a una persona para que utilice el servidor

4.3 Requerimientos de rendimiento

El sistema debe funcionar 24/7, de tal manera que si existe alguna falla el administrador de la red sea informado inmediatamente.

4.4 Requerimientos de bases de datos

El servidor deberá funcionar con MySQL, el cual está instalado en el mismo equipo en el cuál se implementará el software escogido. En resumen el software deberá tener:

- Dirección IP de su MySQL Server.
- Usuario con privilegios para crear bases de datos y usuarios.
- Password del usuario con privilegios.

4.5 Atributos del sistema de software

- Versión libre capaz de monitorizar varios nodos

- Cubrir sin limitaciones una monitorización de red, de servidores y de aplicaciones. Con funcionalidades completas de informes, alertas, integraciones con terceros, etc.
- Tener su propia arquitectura
- Poseer auto descubrimiento de redes es decir debe ser capaz de encontrar automáticamente todos los elementos que componen una red.
- Poseer información oficial y tutoriales sobre su uso

3.1.1.2 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 apartado 3.1.1.1, y la Tabla 29, que realiza una comparación entre varios software de acceso gratuito que brinda el mercado, como indica la Tabla 30.

Tabla 30. Comparación de Software en base a SRS

NOMBRE		CACTI	PANDORA FMS	NAGIOS	ZENOSS	NMAP	OPMANAGER	PRTG NETWORK MONITOR
REQUERIMIENTOS FUNCIONALES	Gestión y monitoreo de dispositivos de red	Si	Si	Si	Si	Si	Si	No
	Monitoreo de Servidores Windows y Linux	Si	Si	Si	Si	Si	Si	Si
	Generación de informes	No	Si	Si	Si	No	Si	No
	Reconocimiento Automático de la red	Si	Si	No	No	Si	No	No
	Manejo de varios dispositivos a la vez	No	Si	No	No	No	No	Si
	Facil instalación	Si	Si	No	No	Si	Si	Si
	Interfaz gráfica	Si	Si	Si	Si	Si	Si	Si
	Envío de notificaciones por correo electrónico	Si	Si	Si	Si	No	Si	No
REQUERIMIENTOS DE USABILIDAD	Ingreso al sistema con un solo usuario y contraseña	Si	Si	Si	Si	No	Si	Si
REQUERIMIENTOS DE RENDIMIENTO	Funcionamiento 24/7	Si	Si	Si	Si	No	Si	Si
REQUERIMIENTOS DE BASE DE DATOS	MySQL	Si	Si	No	Si	No	Si	Si

Fuente: Autor

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.

3.1.1.3 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.

Los servidores de Pandora FMS están siempre en funcionamiento y verifican permanentemente si algún elemento tiene algún problema y si está definido como alerta. Si ocurre esto, éste ejecuta la acción definida en la alarma, tal como enviar un SMS, un correo electrónico, o activar la ejecución de un script.

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 11 se muestra el modelo de la arquitectura del software.

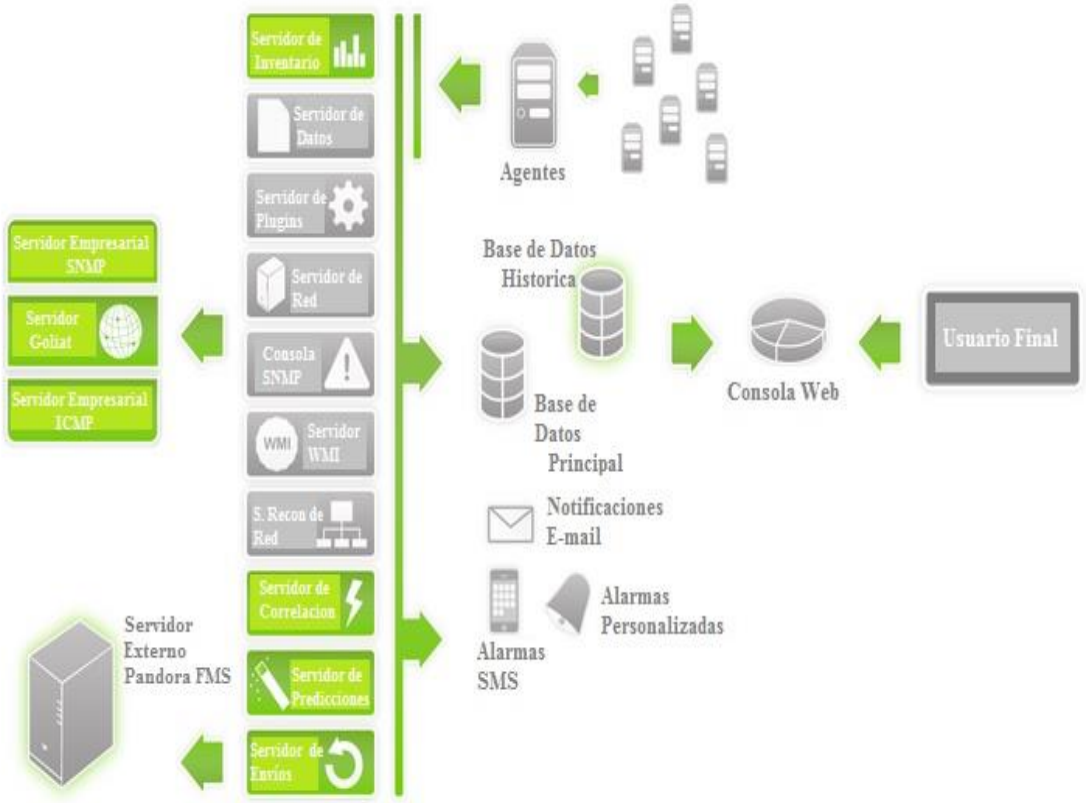


Figura 11. Arquitectura Pandora FMS

Fuente: Recuperado de

http://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Arquitectura#Arquitectura_de_Pandora_FMS

3.1.1.4 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 cuyas especificaciones técnicas fueron descritas en la Tabla 6.

Este equipo tenía previamente instalado el Sistema Operativo CentOS 6.7 ya que en el se encuentra el servidor de geolocalización. En el Anexo A se muestra los pasos para instalar este sistema operativo.

Para iniciar con la instalación se debe tener previamente los siguientes paquetes activos en el sistema operativo, este proceso se describe paso a paso en el Anexo B.

- Apache
- MySQL
- Postfix

3.1.1.5 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. Los pasos a seguir para esta configuración se muestran en el Anexo C.

3.1.1.6 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.

El proceso de instalación de los agentes en los servidores se detalla en el Anexo C.

3.1.1.7 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 para esto se realizó una conexión Telnet utilizando el Software PuTTY13 como se muestra en la Figura 12.

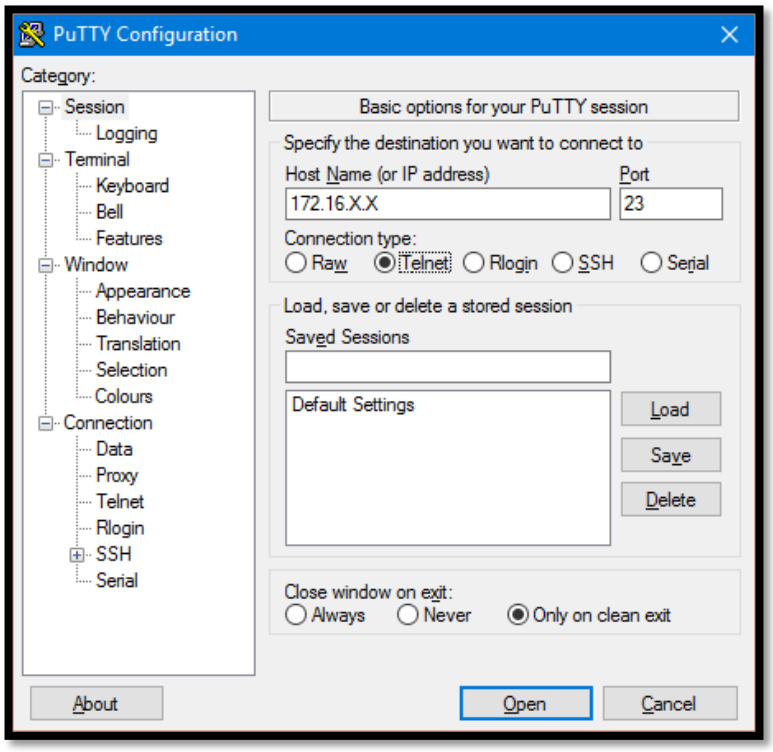


Figura 12. Conexión Telnet con Switch de CORE

Fuente: Consola PuTTY

[13] **PUTTY:** es un cliente SSH, Telnet, login, y TCP raw con licencia libre

Luego de iniciar la sesión Telnet utilizar el comando para mostrar si SNMP está habilitado, como se muestra en la Figura 13 el Switch de CORE ya tiene habilitado el protocolo.

```
>show snmp
```

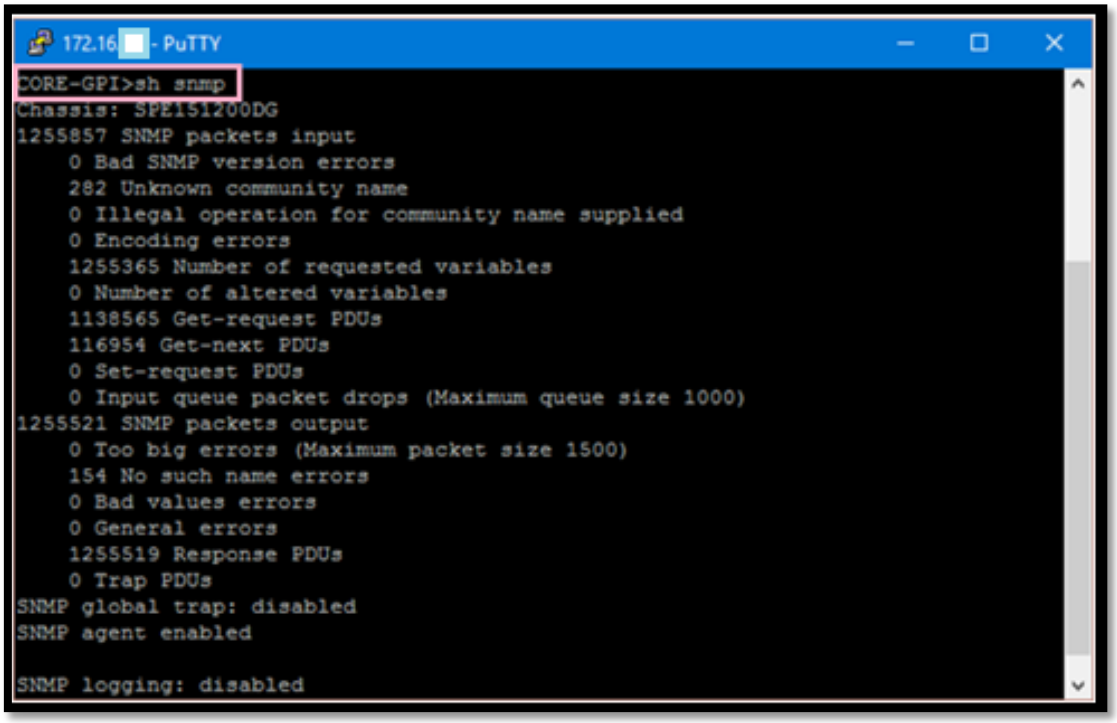


Figura 13. Comando para mostrar Habilitación de SNMPv2c

Fuente: Consola PuTTY

En este caso a pesar de haber habilitado el protocolo este no tenía configurado el envio de traps. Para esto primero se debe configurar el servidor al cual se van enviar utilizando el comando:

```
>snmp-server host <IP Address> version <v1 or 2c> <RO community string>
```

En este caso en el campo IP Address se refiere a la IP del Servidor Pandora, además se utilizará la versión 2c del protocolo y la comunidad Read-Only, esta configuración se muestra en la Figura 14.

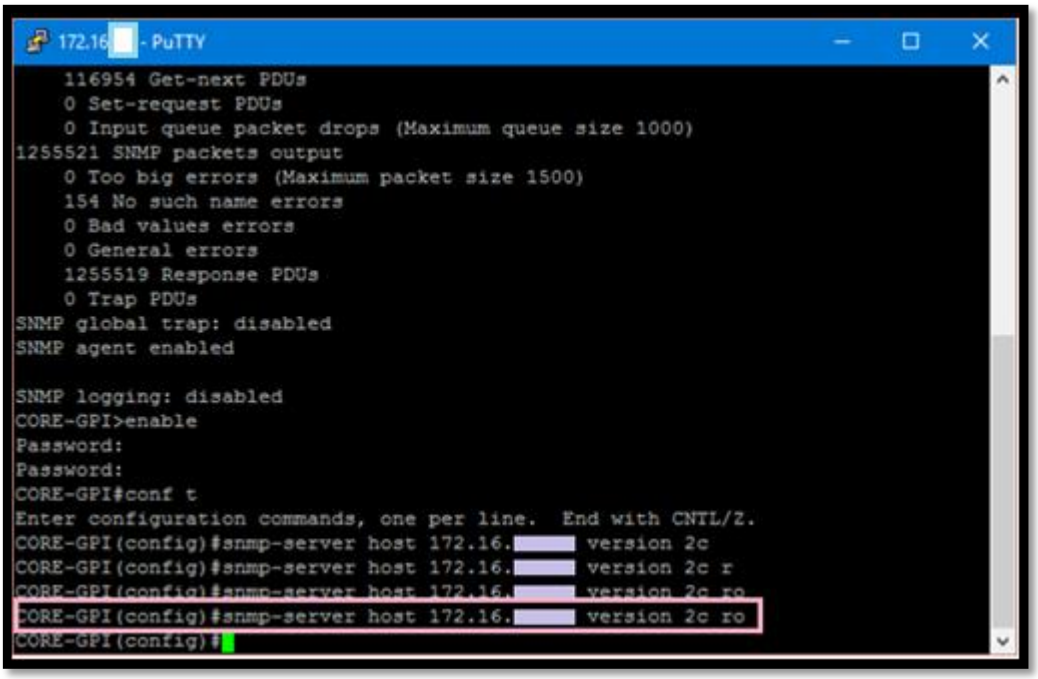


Figura 14. Configuración del Servidor al que se dirigen las traps

Fuente: Consola PuTTY

Por último se habilitan los Traps SNMP con el comando que se muestra a continuación:

```
>snmp-server enable traps [tipo de notificación][opción de notificación]
```

Para saber que tipo de traps se pueden activar, se utiliza un signo de incognita (?) al final del comando como se muestra en la Figura 15.

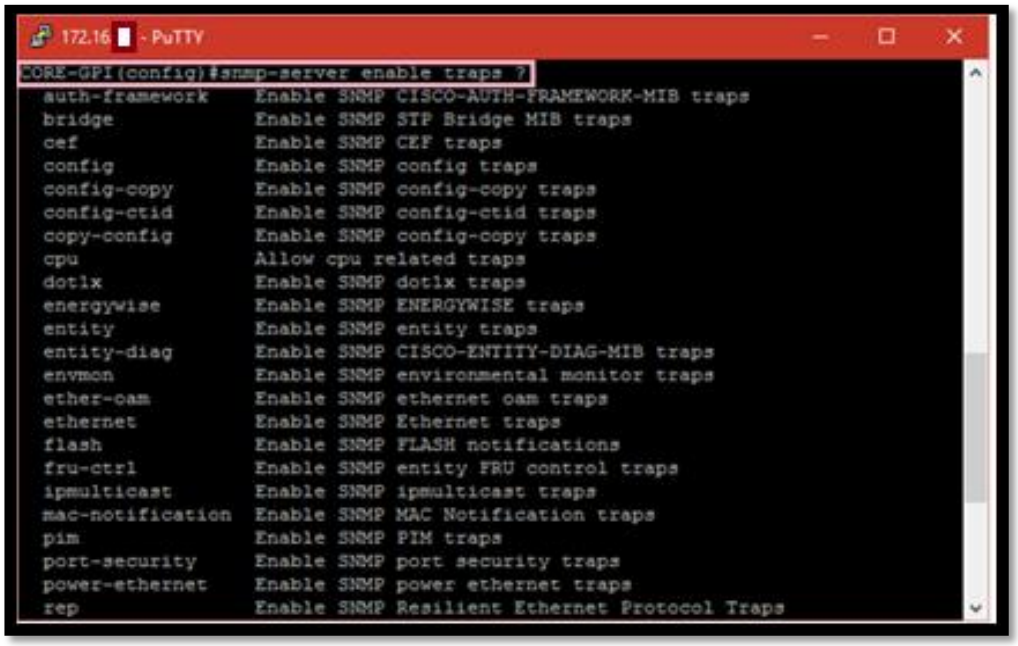


Figura 15. Tipos de Traps

Fuente: Consola PuTTY

Debido a una solicitud del administrador de la red se habilito todas las Traps en el Switch de CORE tal como se muestra en la Figura 16.

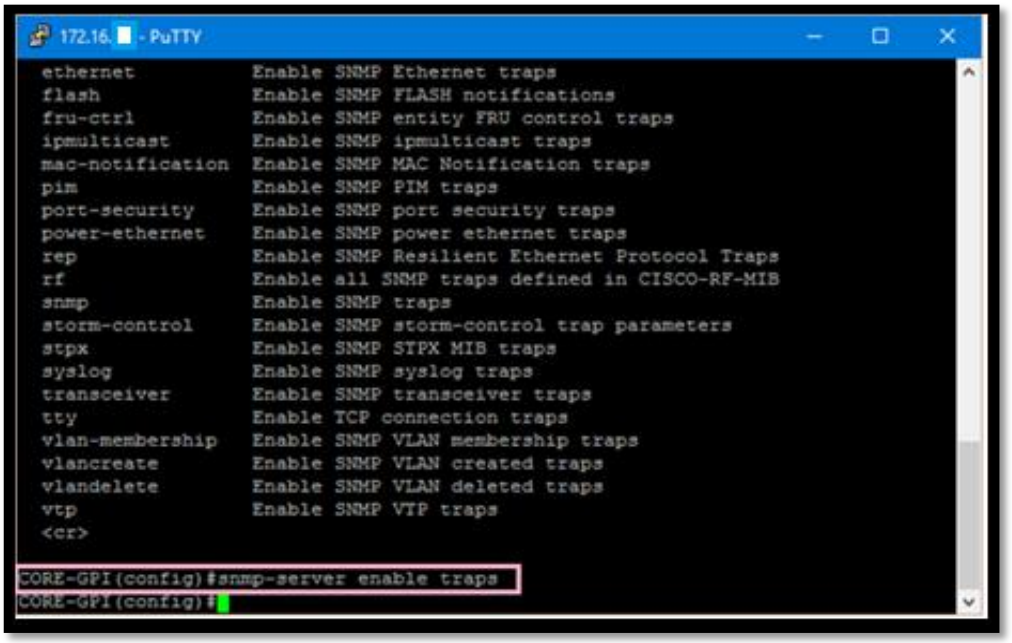


Figura 16. Habilitación Traps SNMP

Fuente: Consola PuTTY

Los tipos de traps que se pueden habilitar en el Switch de CORE se describen a continuación en la Tabla 31.

Tabla 31. Tipos de Trap a activarse

TIPO DE TRAP	TIPO DE NOTIFICACIÓN
auth-framework	Envía las notificaciones de CISCO-AUTH-FRAMEWORK-MIB
bridge	Envía las notificaciones de puente STP de la MIB
cef	Envía notificaciones CEF (Cisco Express Forwarding)
config	Envía las notificaciones de la configuración
config_copy	Envía las notificaciones de copia de la configuración
config_ctid	Envía las notificaciones de rastreo de configuración
copy-config	Envía las notificaciones de copia de la configuración
cpu	Permite notificaciones relativas al CPU
energywise	Notificaciones de nivel de energía
entity	Notificaciones de modificaciones del Management Information Base de la Manda entidad (MIB).
entity-diag	Notificaciones de CISCO-ENTITY-DIAG-MIB
envmon	Notificaciones del monitor de ambiente
ether-oam	Notificaciones Ethernet oam
ethernet	Envía notificaciones Ethernet
flash	Notificaciones FLASH
fru-ctrl	Envía notificaciones Control FRU
ipmulticast	Notificaciones de multicast
mac-notification	Notificaciones de la MAC del equipo
Pim	Envía notificaciones PIM
port-security	Envía notificaciones de seguridad del puerto
power-ethernet	Envia notificaciones de power – Ethernet
Rep	Envia notificaciones de Resilient Ethernet Protocol
Rf	Permite el envío de todas las notificaciones definidas en CISCO-RF-MIB

Tabla 30. Tipos de Trap a activarse

snmp	Envía las notificaciones del Simple Network Management Protocol (SNMP)
storm-control	Envía notificaciones de parámetros de storm – control
Stpx	Notificaciones STPX MIB
syslog	Envía las notificaciones de mensajes de error (Syslog MIB de Cisco).
transceiver	Envía notificaciones del transceiver
Tty	Envía notificaciones de conexión TCP
vlan-membership	Permite notificaciones de autenticación de VLAN
vlancreate	Permite notificaciones de creación de VLAN
vlandelete	Permite notificaciones de borrado de VLAN
Vtp	Notificaciones VTP

Fuente: Consola PuTTY

Después de haber configurado SNMP es necesario realizar las configuraciones de monitoreo en la consola de Pandora FMS las cuales están presentadas en el Anexo C.

3.1.1.8 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.

3.1.1.9 Configuración Equipos Servidores Linux

Para iniciar la configuración del servidor en Linux es necesario que el agente este instalado correctamente en el equipo.

El acceso a este servidor se realizó mediante una conexión SSH para lo que se utilizó el programa PuTTY para establecer esta conexión como se muestra en la Figura 17.

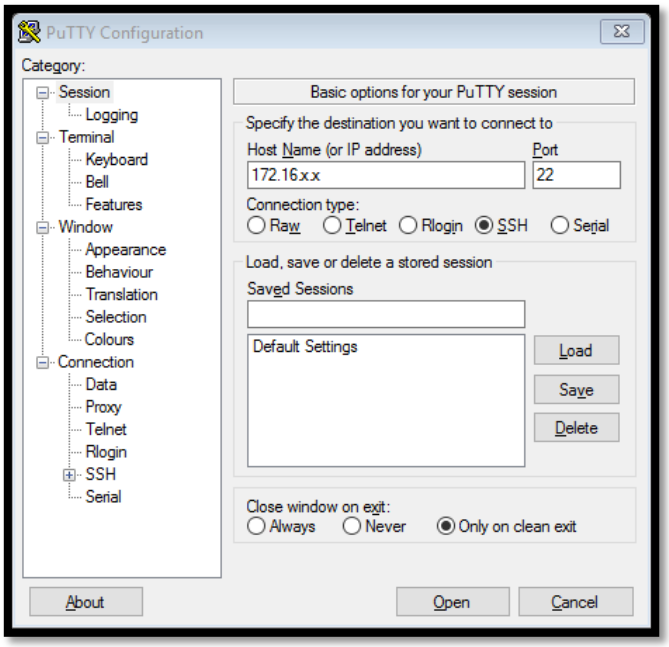


Figura 17. Conexión SSH con Servidor Web

Fuente: Consola PuTTY

Una vez dentro de la consola de servidor se debe editar el archivo del agente de pandora, para lo que se ingreso al directorio donde este se encuentra, utilizando los comandos que se muestran en la Figura 18.

```
#cd /etc/pandora
```

```
#vi pandora_agent.conf
```

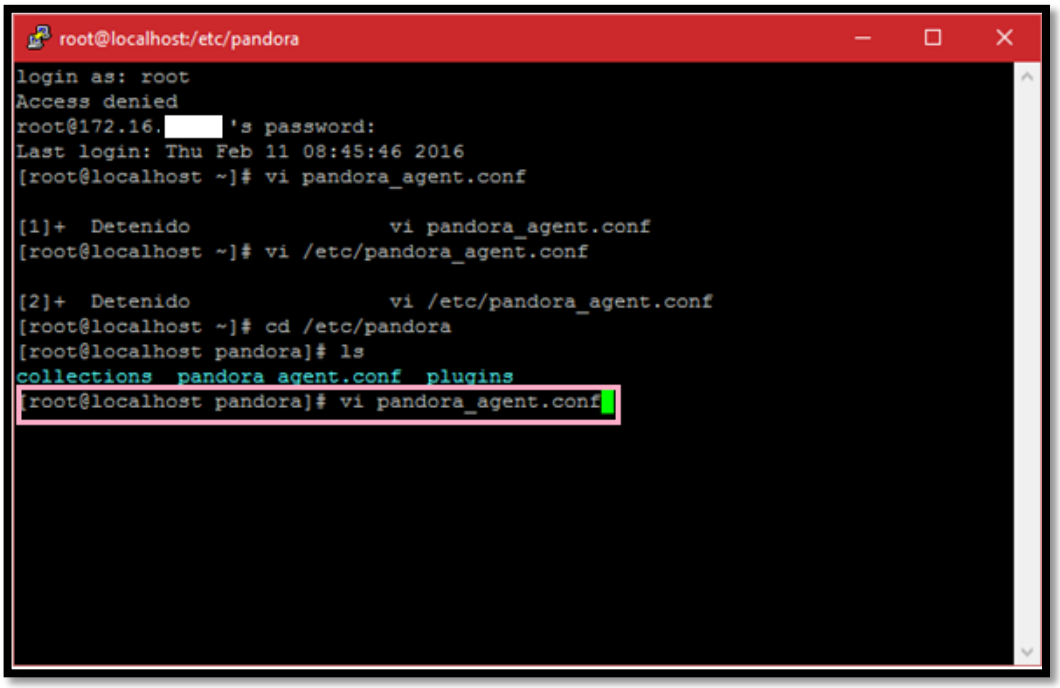


Figura 18. Ingreso archivo de Configuración Agente Pandora FMS

Fuente: Consola PuTTY

Dentro de este archivo se debe colocar de IP del Servidor Pandora FMS como se muestra en la Figura 19.

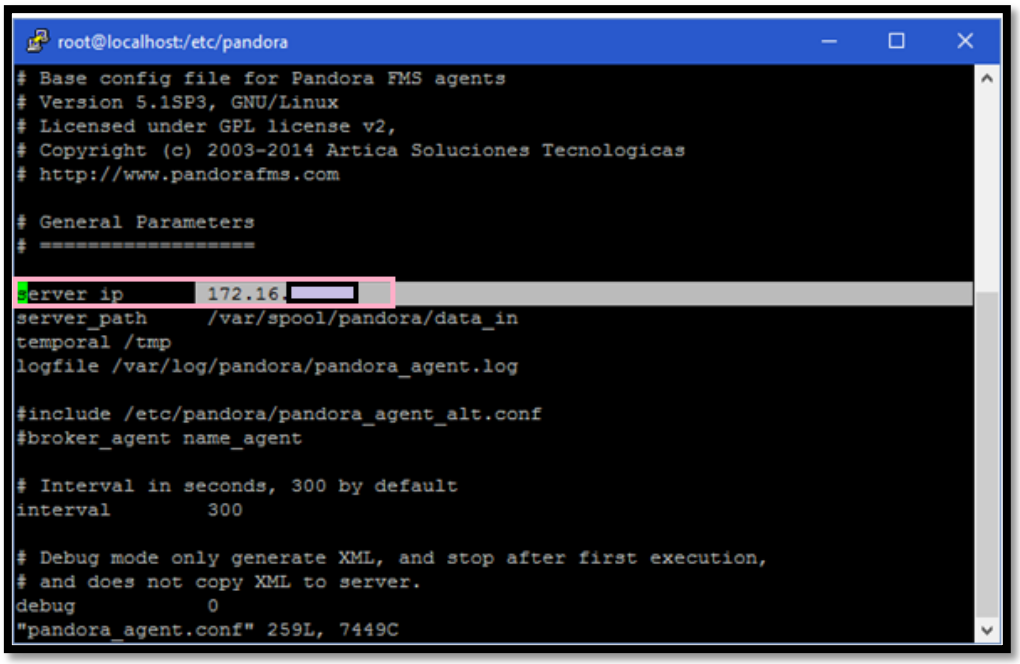


Figura 19. Archivo de Configuración Agente Pandora FMS

Fuente: Consola PuTTY

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, algunos ejemplos de servicios se nombran a continuación.

- **Monitorear WEB:** para el monitoreo del protocolo htttp se incluyen los parámetros mostrados a continuación:
  module_begin
  module_name_webDaemon
  module_type generic proc
  module_exec ps –Af | grep httpd |grep –v “grep” |wc –l
  module_descripTion Check WEB service
  module_end

- **Monitorear FTP:** para el monitoreo del protocolo ftp se incluyen los parámetros mostrados a continuación:
  module_begin
  module_name_ftpDaemon
  module_type generic proc
  module_exec ps –Af | grep vsftpd |grep –v “grep” |wc –l
  module_descripTion Check VSFTPD service
  module_end

- **Monitorear DNS:** para monitorear el estado de la reoslución de nombres se incluyen los parámetros mostrados a continuación:
  module_begin
  module_name_namedDaemon
  module_type generic proc
  module_exec ps –Af | grep named |grep –v “grep” |wc –l
  module_descripTion Check named service
  module_end

- **Monitorear DHCP:** para el monitoreo de la asignación de direcciones se incluyen los parámetros mostrados a continuación:
  module_begin
  module_name_dhcpDaemon
  module_type generic proc
  module_exec ps –Af | grep dhcpd |grep –v “grep” |wc –l
  module_descripTion Check dhcpd service
  module_end

- **Monitorear CORREO:** para el monitoreo del envío de correo electrónico mediante PostFix se incluyen los parámetros mostrados a continuación:
  module_begin
  module_name_postfixDaemon
  module_type generic proc
  module_exec ps –Af | grep postfix |grep –v “grep” |wc –l
  module_descripTion Check postfix service
  module_end

A continuación se debe regresar al directorio root y reiniciar el agente pandora con el comando que se muestra en la Figura 20.

```
# /etc/init.d/pandora_agent_daemon restart
```

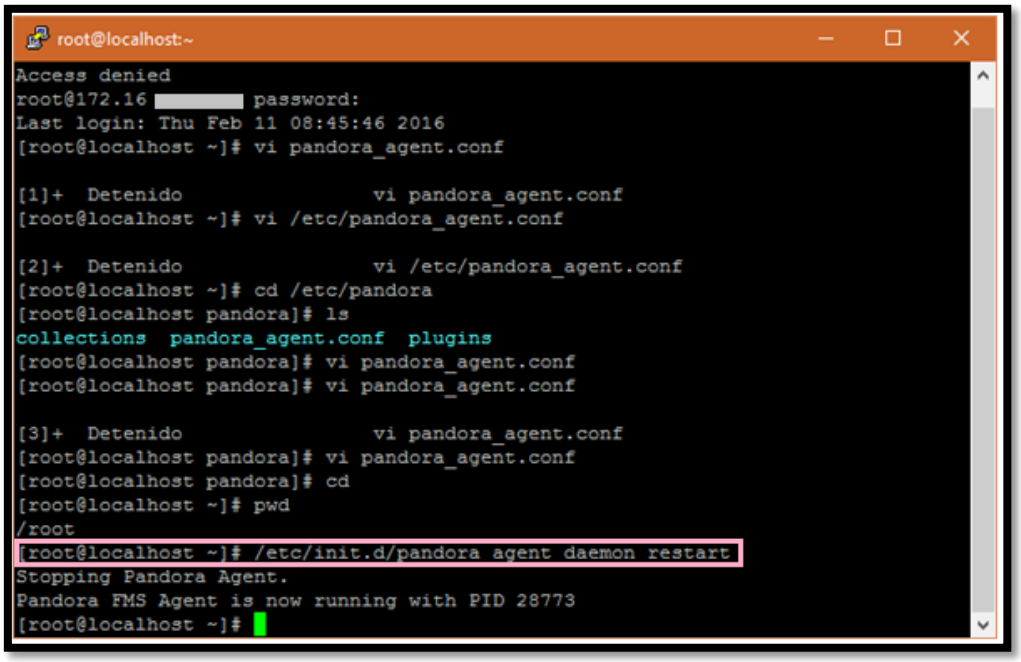


Figura 20. Reinicio Agente Pandora

Fuente: Consola PuTTY

Luego de reiniciar se comprueba conectividad entre el servicio monitoreado y el servidor Pandora, si no existen errores el ping deberá ser exitoso como se muestra en la Figura 21.

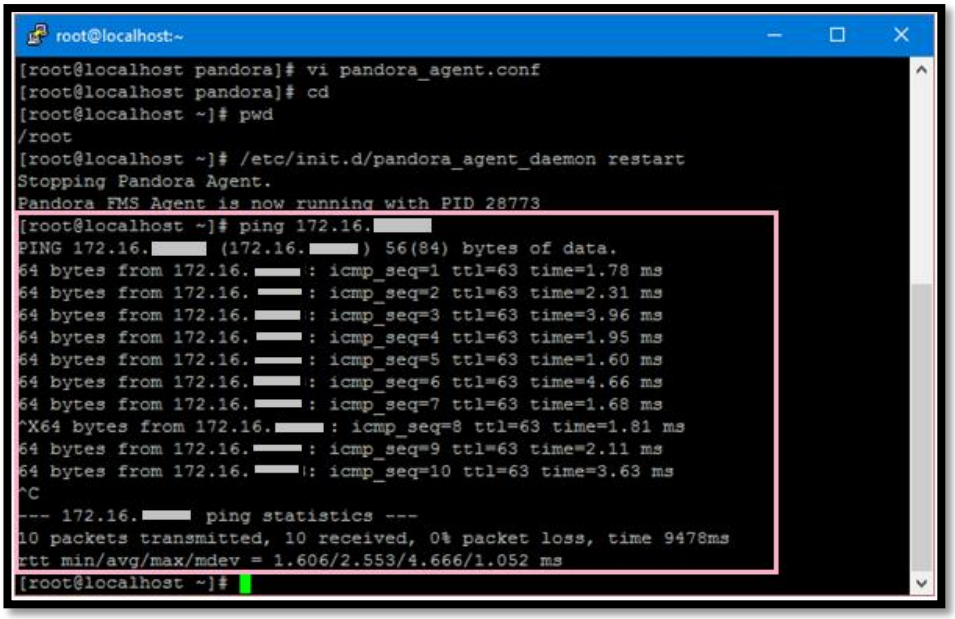


Figura 21. Ping entre Servidor Pandora y Servidor Web

Fuente: Consola PuTTY

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. Este proceso se encuentra descrito en el Anexo C.

3.1.1.10 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, esto pasos se encuentran descritos en el Anexo C.

3.1.2 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.

3.1.2.1 Proceso de solución de fallos

3.1.2.1.1 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.

El servidor de Pandora FMS se configuró para realizar un reconocimiento de red cada 10 minutos como se observa en la Figura 22, lo que permite mantener una adecuada vigilancia de los dispositivos.

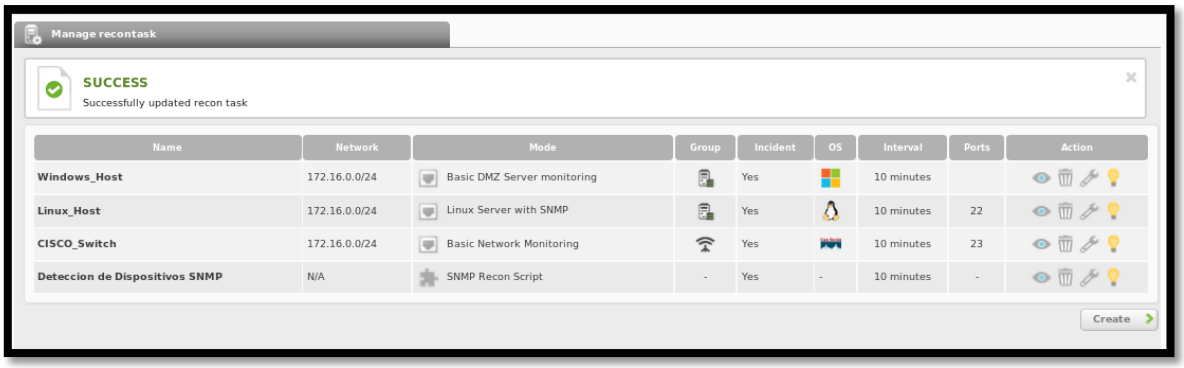


Figura 22. Reconocimiento de Red
Fuente: Consola Pandora FMS

3.1.2.1.2 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.

3.1.2.1.3 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

3.1.2.1.4 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. Para esto, se presenta la plantilla mostrada a continuación en donde el administrador de red o los responsables de mitigar las fallas puedan describir lo sucedido.

PREFECTURA DE IMBABURA	**REPORTE DE FALLAS – DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN**			
Reportado por:		Número de Reporte:		
Área / Departamento:		Fecha:	Hora:	
Descripción del Problema :				
Posibles Causas:				
Tipo de Fallo	Red	PC	Impresora	Otros
Nivel de Criticidad	Poco	Algo	Crítico	Muy Crítico
Medidas de aislamiento tomadas:				
Solución:				
Solucionado por:		Tiempo Empleado:		
Observaciones:				

En el Anexo D se muestra la forma en que se llenó esta plantilla luego de una falla en el servidor WEB.

3.1.2.2 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.

Una alerta es, básicamente, cualquier acción que pueda ser desencadenada por un script configurado en el sistema operativo donde corre el servidor de Pandora FMS que procesa el módulo. (Pandora FMS)

3.1.2.2.1 Estructura de las alertas de Pandora FMS

Las alertas de Pandora FMS están formadas como se observa en la Figura 23.

Figura 23. Estructura de Alertas Pandora FMS

Fuente: Recuperado de http://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Alertas#Introducci.C3.B3n_al_sistema_de_alertas_actual

Donde:

- **Comando:** define la operación a realizar cuando se dispara la alerta.

- **Acción:** relaciona un comando con una plantilla y permite personalizar la ejecución del comando usando tres parámetros genéricos Field 1, Field 2 y Field 3. Estos parámetros permiten personalizar la ejecución del comando, ya que son los que se pasarán en el momento de la ejecución como parámetros de entrada.

- **Plantilla:** se definen parámetros genéricos de la alertas que son: las condiciones de disparo, acciones de disparo y recuperación de la alerta.

    - **Condiciones de disparo:** son las condiciones bajo las que se disparará la alerta, por ejemplo: superar cierto umbral, estar en estado crítico, etc.
    - **Acciones de disparo:** es la configuración de las acciones que se realizarán al disparar la alerta.
    - **Recuperación de alerta:** es la configuración de las acciones que se realizarán cuando el sistema se recupere de la alerta. (Pandora FMS)

3.1.2.2.2 Tipos de alertas

Pandora FMS maneja varios tipos de alertas: las alertas simples, las alertas sobre eventos, y las alertas sobre traps SNMP.

Las alertas simples se dividen en dos condiciones: de advertencia y critica.

3.1.2.2.3 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.

Para iniciar la definición y envió de alertas en el archivo de configuración de Pandora se debe tener comentadas las líneas que se muestran en la Figura 24.

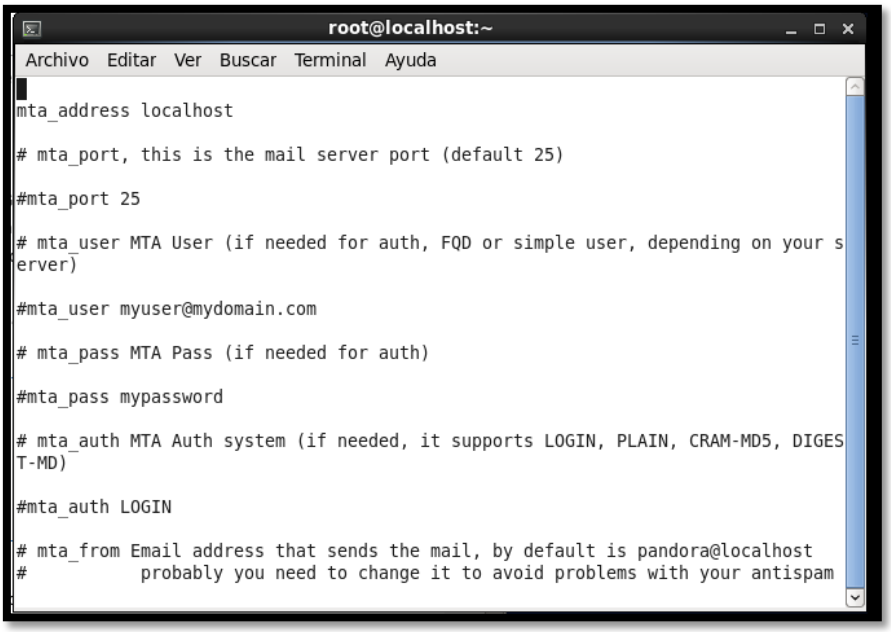


Figura 24. Archivo de Configuración Pandora FMS

Fuente: Consola CentOS

Luego de haber comprobado que estas líneas estén comentadas dirigirse a la consola de Pandora y en la pestaña Administration escoger Manage Alerts y la opción Action como se muestra en la Figura 25.

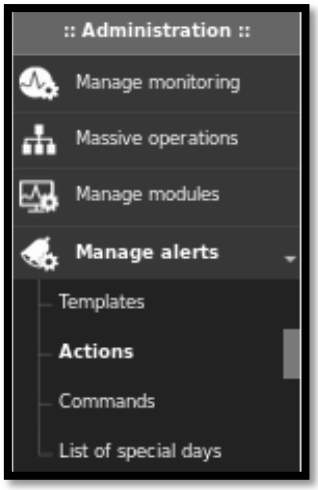


Figura 25. Pestaña de Configuración de Alertas

Fuente: Consola Pandora FMS

Dentro de este menú se debe editar la alerta por defecto Mail to XXX que se muestra en la figura 26, de esta manera se añade el destinatario de correo al que le llegaran las alertas.

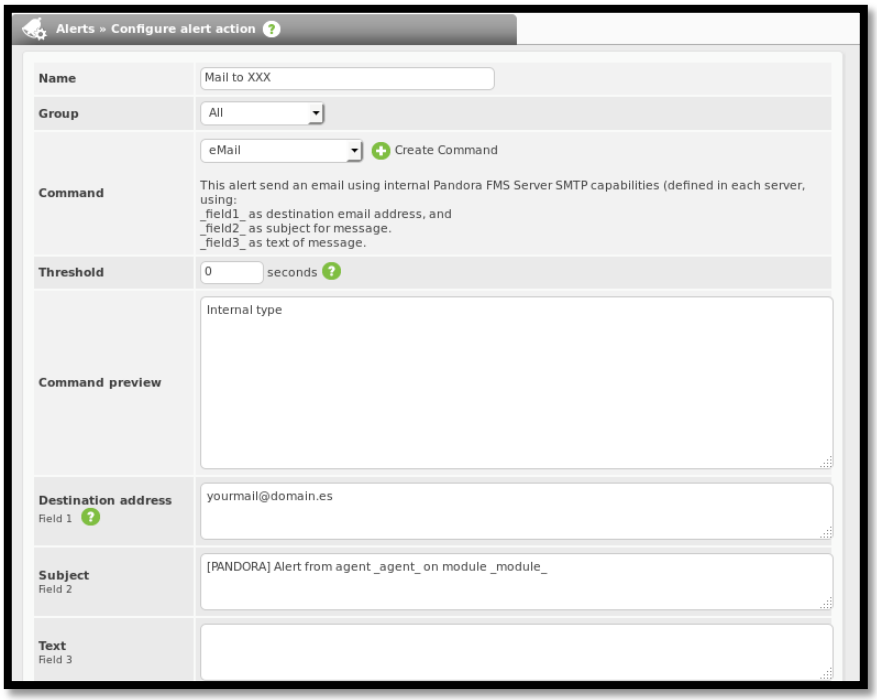


Figura 26. Configuración de e-mail

Fuente: Consola Pandora FMS

A continuación se crean las alertas en cada dispositivo de red y equipos monitoreados, en la Figura 27 se muestra la configuración de una alerta de condición de advertencia para el Switch de CORE.

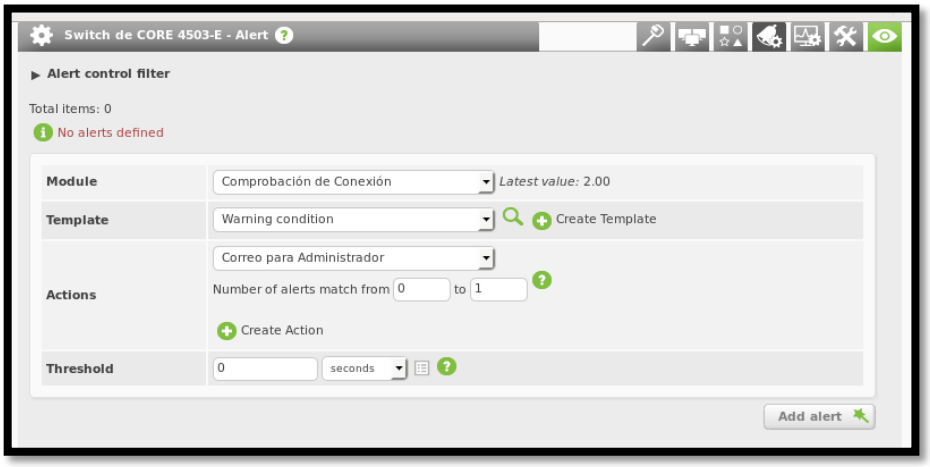


Figura 27. Definición de Alerta

Fuente: Consola Pandora FMS

Una vez que la alerta se dispare esta será enviada al correo del administrador de la manera que se indica en la Figura 28.

Figura 28. Correo de Alerta Crítica
Fuente: Consola Pandora FMS

3.1.3 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 mostrado en el Anexo C, al responsable de la red, este contiene todas las configuraciones realizadas para el funcionamiento del Servidor Pandora FMS.

3.1.3.1 Monitoreo Switch de CORE

Con las configuraciones de los parámetros definidos se puede observar que el SWITCH comienza a enviar los datos sobre los servicios solicitados como se muestra en la Figura 29.

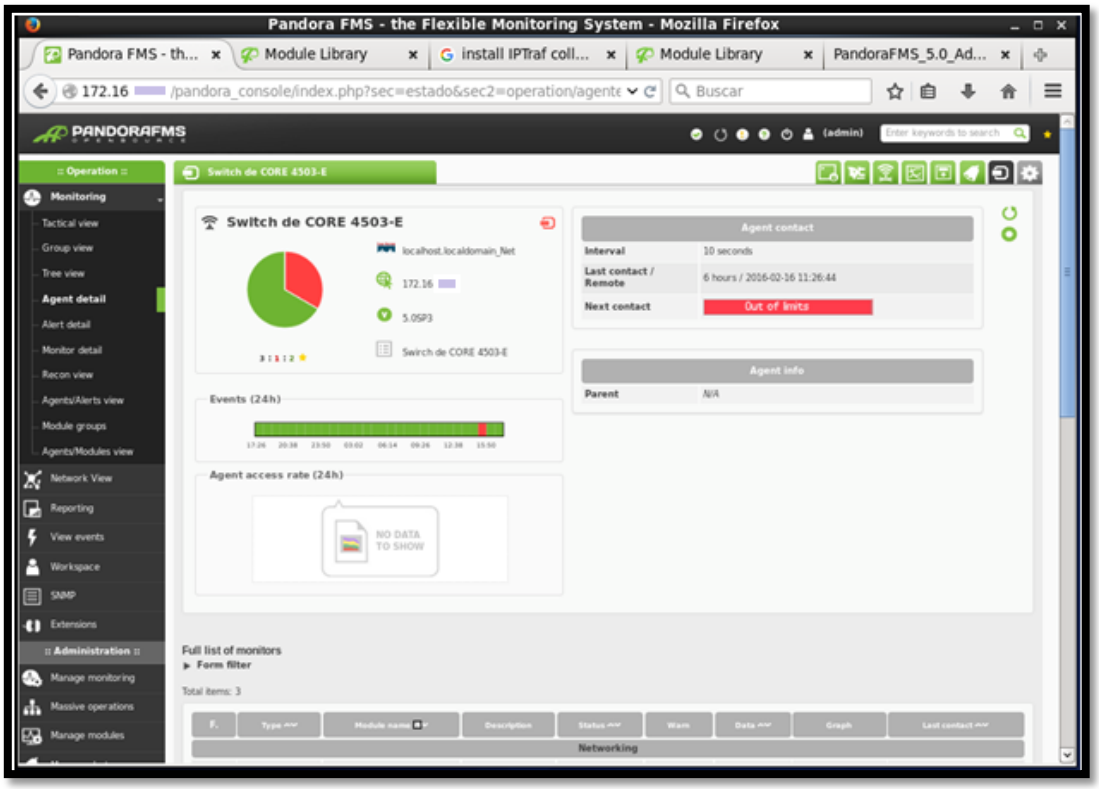


Figura 29. Vista General del Monitoreo Switch de CORE

Fuente: Consola Pandora FMS

Por parte del administrador de la red se pidió el monitoreo de dos módulos en especial la comprobación de conexión y latencia del equipo.

Para la comprobación de la conexión se creó un módulo con la opción Host Alive como se muestra en la Figura 30, esta representa un ping hacia el equipo.

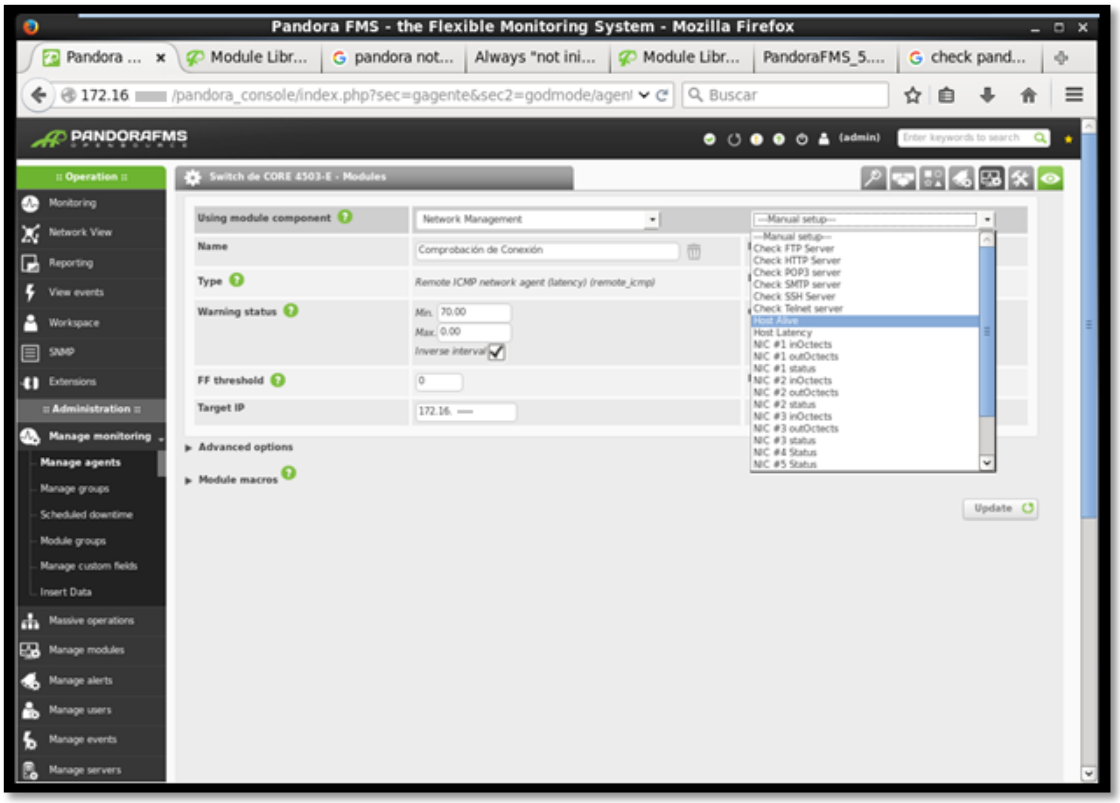


Figura 30. Creación del Módulo Comprobación de Conexión

Fuente: Consola Pandora FMS

Para la latencia del equipo se utilizo la opción Host Latency indicado en la Figura 31, este devuelve el tiempo en milisegundos que se tarda el equipo en hacer contacto con el servidor.

Si se han configurado correctamente los módulos estos aparecerán sin ningún error o advertencia dentro de la consola como se muestra en la Figura 32.

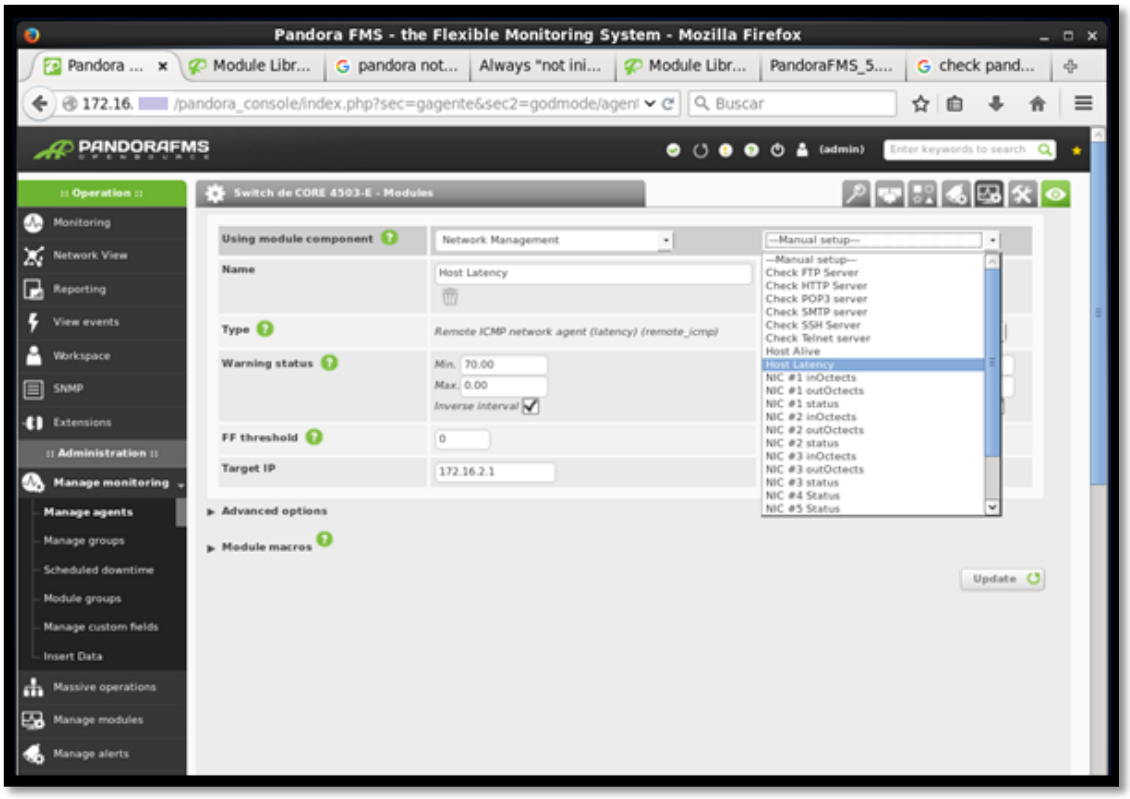


Figura 31. Creación del Módulo Latencia

Fuente: Consola Pandora FMS

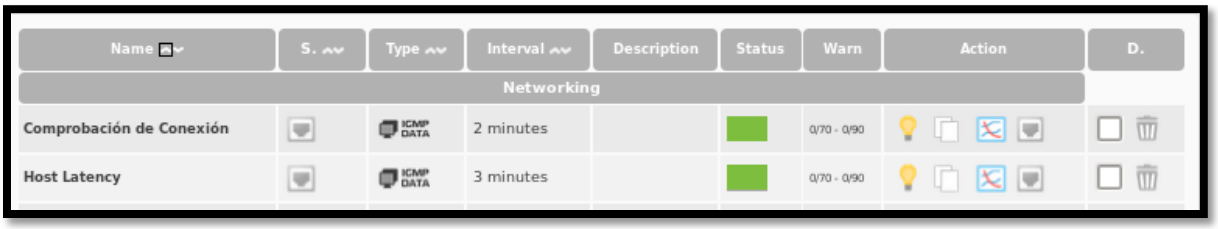


Figura 32. Módulos creados en SWITCH de CORE

Fuente: Consola Pandora FMS

Para conocer el detalle de este monitoreo se ingresó a los gráficos generados por cada uno de ellos en distintas horas del día. En cuanto a la comprobación de conexión se puede observar que no hubo ningún cambio crítico, pero si hubo un pico que pudo haber generado una advertencia, como se muestra en la Figura 33.

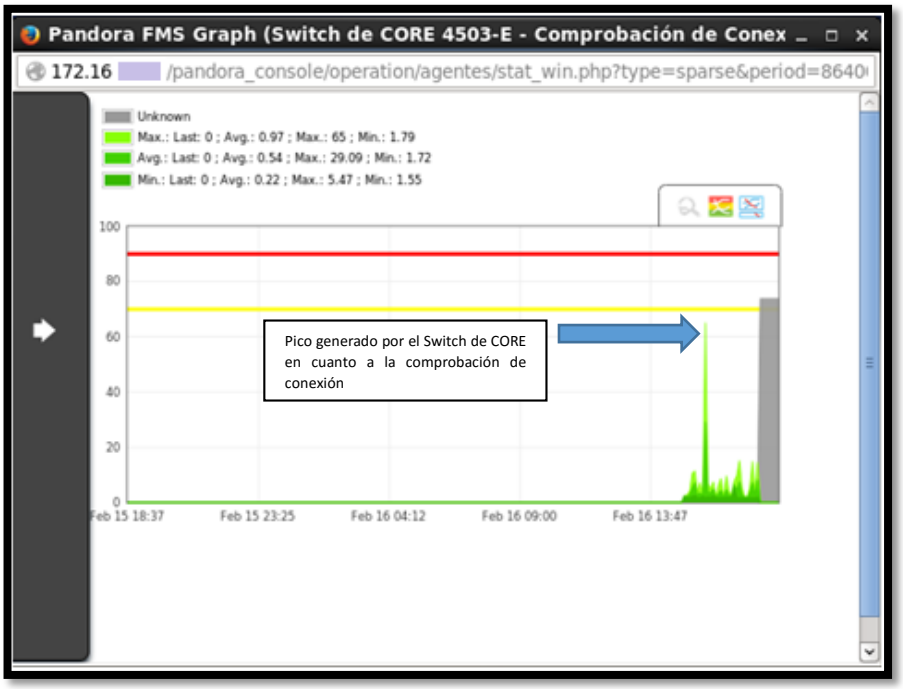


Figura 33. Grafico Generado de Comprobación de Conexión

Fuente: Consola Pandora FMS

En cuanto al módulo de Latencia se pudo observar que nunca hubo un estado crítico que motivará una alerta del equipo, esto se indica en la Figura 34.

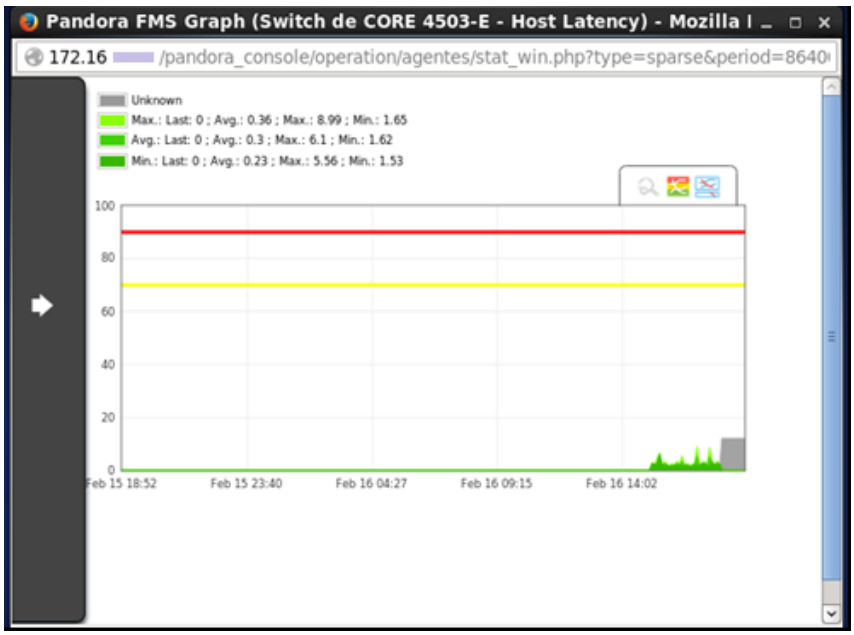


Figura 34. Gráfico Generado de la Latencia

Fuente: Consola Pandora FMS

3.1.3.2 Monitoreo Switch 2960

Para realizar el monitoreo 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.

Con objeto de la documentacion se tomo en cuenta los 2 switch de acceso principales que se encuentran en el cuarto de equipos, los cuales se conectan a los dos pisos del edificio indistintamente. En cada uno se creo distintos modulos de monitoreo a continuación se observa los resultados obtenidos en los graficos generados por Pandora FMS.

3.1.3.2.1 Switch de cuarto de comunicaciones #1

En la Figura 35 se observa que este Switch está configurado correctamente y recibiendo todas las señales de monitoreo creadas en el Servidor Pandora.

Figura 35. Vista General monitoreo Switch 1

Fuente: Consola Pandora FMS

En este Switch se configuro el monitoreo de accesos Telnet y de Host Alive para comprobar la conexión de este a la red, en cuanto a los resultados de este monitoreo se observa en las Figuras 36 y 37 respectivamnete que se realizó una conexión por Telnet y la conexión estuvo normal la mayoría del día excepto por picos pero los cuales no fueron críticos ya que no generaron alertas.

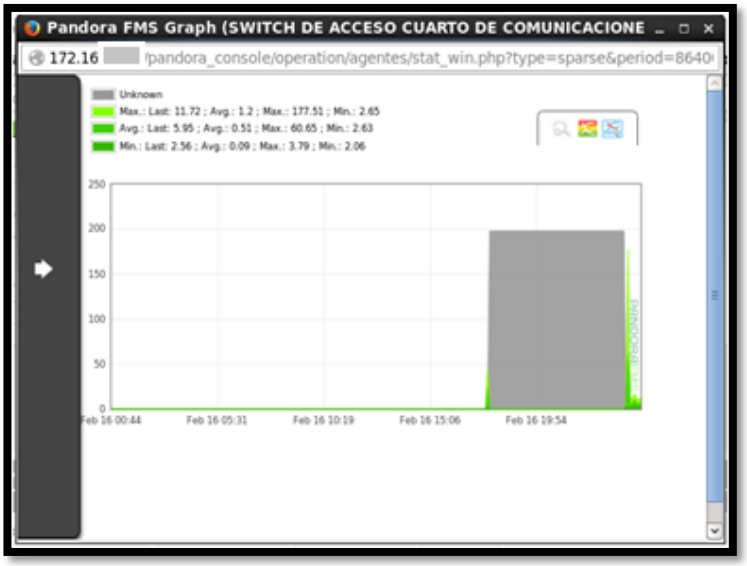


Figura 36. Monitoreo Host Alive Switch 1

Fuente: Consola Pandora FMS

Figura 37. Monitoreo Telnet Switch 1

Fuente: Consola Pandora FMS

3.1.3.2.2 Switch de cuarto de comunicaciones #2

En la Figura 38 se observa que este Switch está configurado correctamente y recibiendo todas las señales de monitoreo creadas en el Servidor Pandora.

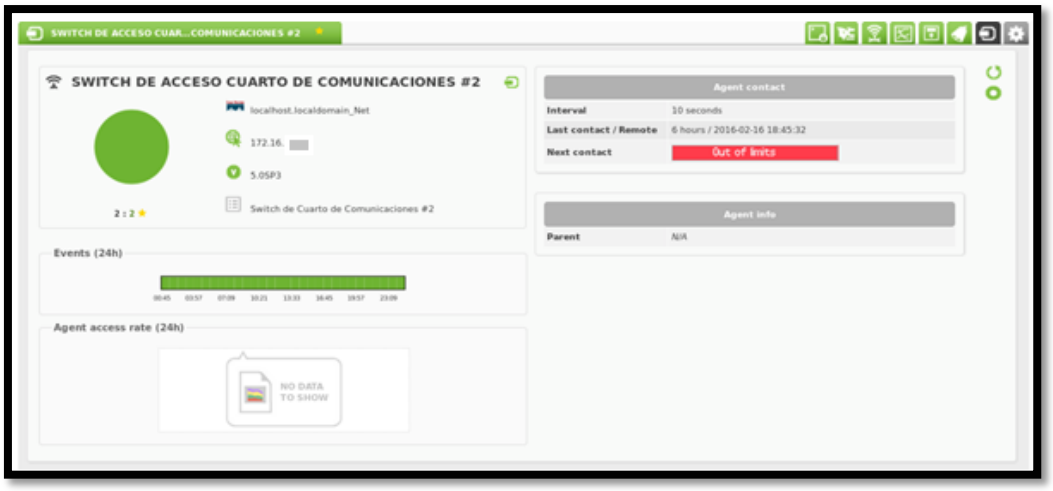


Figura 38. Vista general monitoreo Switch 2

Fuente: Consola Pandora FMS

El monitoreo de la velocidad a la que se conecta la interfaz FastEthernet0 del Switch se muestra En la Figura 39.

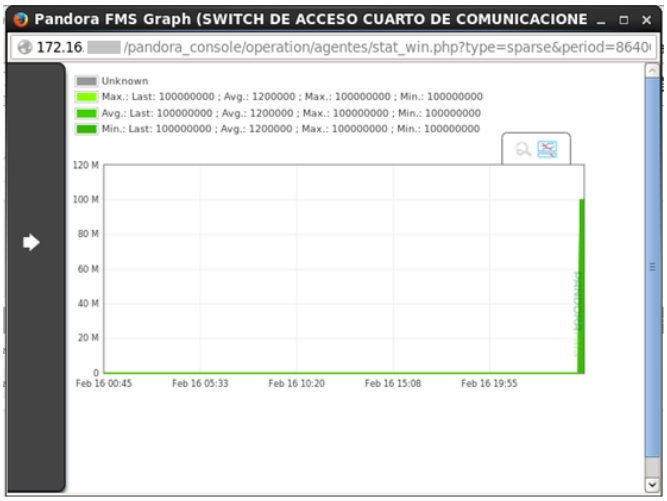


Figura 39. Velocidad de interfaz

Fuente: Consola Pandora FMS

3.1.3.3 Monitoreo de servidores

Como se explicó en el Capítulo 2, se realizó el monitoreo de 2 servidores que son considerados como los que más cargas producen a la red en horas de funcionamiento.

3.1.3.3.1 Monitoreo servidor web (Linux)

En las Figuras 40 y 41 se puede observar que el Servidor se encuentra añadido correctamente y el monitoreo de servicios para diferentes aspectos como memoria disponible, uso del cpu, memoria libre, uso de bytes, numero de procesos activados entre otros esta activado. Estos módulos se añaden mediante una plantilla que brinda Pandora FMS para el monitoreo de servidores.

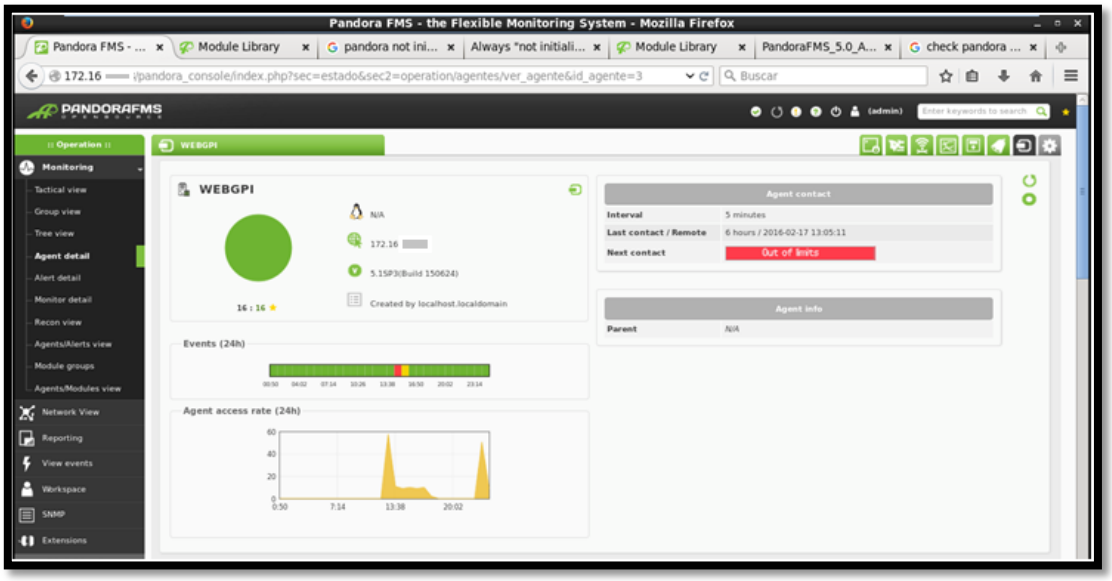
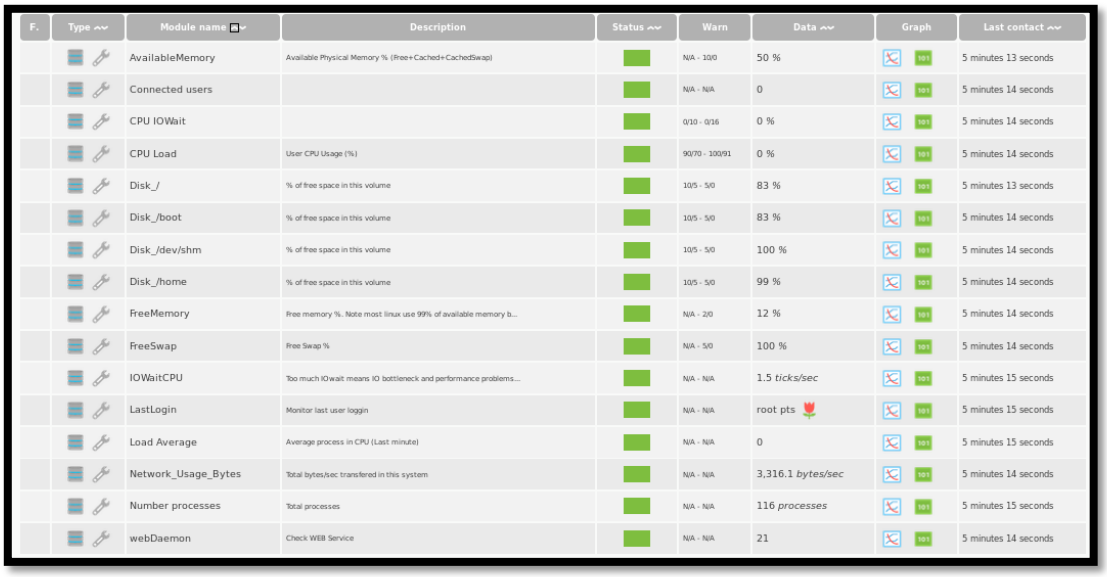


Figura 40. Servidor Web Activo en Consola Pandora FMS

Fuente: Consola Pandora FMS



F.	Type	Module name	Description	Status	Warn	Data	Graph	Last contact
		AvailableMemory	Available Physical Memory % (Free+Cached+CachedSwap)		N/A - 10/0	50 %		5 minutes 13 seconds
		Connected users			N/A - N/A	0		5 minutes 14 seconds
		CPU IOWait			0/10 - 0/16	0 %		5 minutes 14 seconds
		CPU Load	User CPU Usage (%)		90/70 - 100/91	0 %		5 minutes 14 seconds
		Disk_/	% of free space in this volume		10/5 - 5/0	83 %		5 minutes 13 seconds
		Disk_/boot	% of free space in this volume		10/5 - 5/0	83 %		5 minutes 14 seconds
		Disk_/dev/shm	% of free space in this volume		10/5 - 5/0	100 %		5 minutes 14 seconds
		Disk_/home	% of free space in this volume		10/5 - 5/0	99 %		5 minutes 14 seconds
		FreeMemory	Free memory %. Note most linux use 99% of available memory b...		N/A - 2/0	12 %		5 minutes 14 seconds
		FreeSwap	Free Swap %		N/A - 5/0	100 %		5 minutes 14 seconds
		IOWaitCPU	Too much IOwait means IO bottleneck and performance problems....		N/A - N/A	1.5 *ticks/sec*		5 minutes 15 seconds
		LastLogin	Monitor last user loggin		N/A - N/A	root pts		5 minutes 15 seconds
		Load Average	Average process in CPU (Last minute)		N/A - N/A	0		5 minutes 15 seconds
		Network_Usage_Bytes	Total bytes/sec transfered in this system		N/A - N/A	3,316.1 *bytes/sec*		5 minutes 14 seconds
		Number processes	Total processes		N/A - N/A	116 *processes*		5 minutes 15 seconds
		webDaemon	Check WEB Service		N/A - N/A	21		5 minutes 14 seconds

Figura 41. Servicios monitoreados del Servidor Web

Fuente: Consola Pandora FMS

Para conocer el detalle de este monitoreo se ingreso a los gráficos generados por cada uno de ellos en distintas horas del día.

En la Figura 42 se puede observar el total de memoria libre del servidor y muestra que tiene el 52% de memoria libre por lo que no genera ninguna alerta.

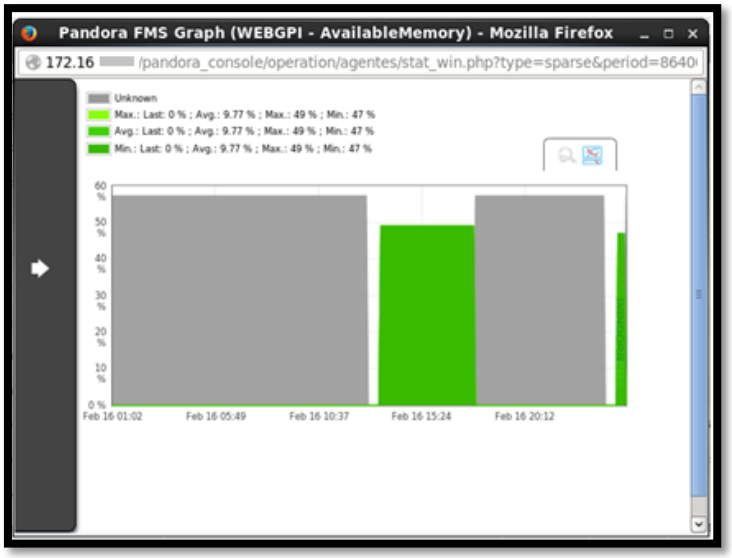


Figura 42. Memoria Libre Servidor Web

Fuente: Consola Pandora FMS

En la Figura 43 se puede observar la carga del CPU la cual en su mayor pico del dia se encuentra en un 20% por lo tanto es estable.

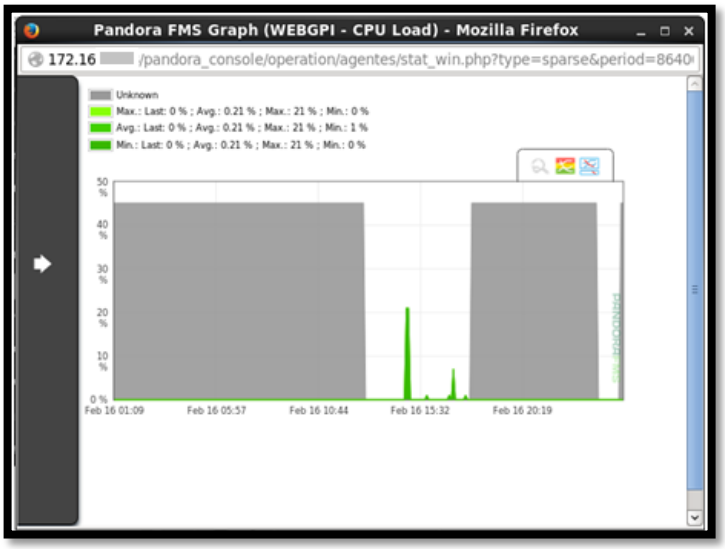


Figura 43. Carga del CPU del Servidor Web

Fuente: Consola Pandora FMS

En cuanto al uso de la red en bytes se puede observar que el pico máximo de uso es de 75 Kbps lo cual no afecta el rendimiento de la red y no genera ninguna alerta, esto se muestra en la Figura 44.

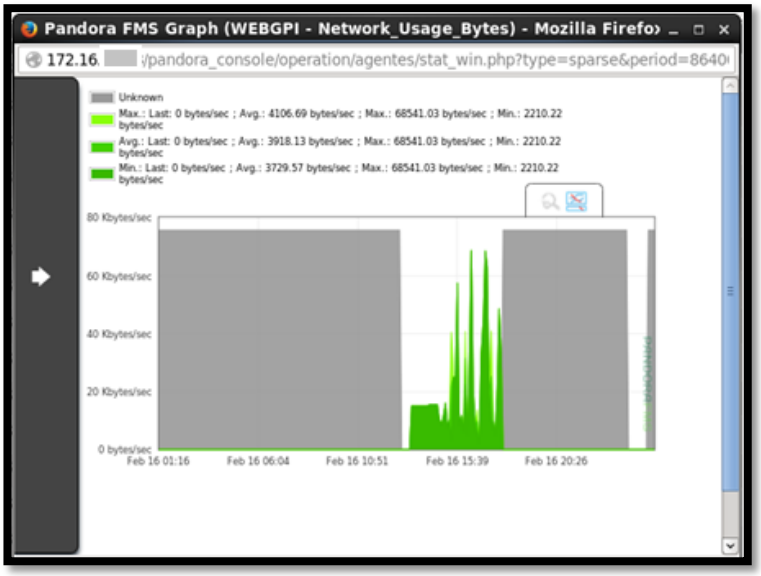


Figura 44. Uso de la Red en Bytes del Servidor web

Fuente: Consola Pandora FMS

De esta manera se puede revisar todas las estadísticas de los distintos servicios monitoreados, tomando en cuenta estos datos se puede ver que el servidor está funcionando correctamente y no tiene sobrecargas de ningún tipo.

3.1.3.3.2 Monitoreo servidor de gestión de archivos (Linux)

Para realizar el monitoreo de este servidor se realizan los mismos pasos que en el Servidor Web, ya que ambos trabajan con el Sistema Operativo CentOS, se debe tener en cuenta que se debe realizar la comprobación de conexión entre el Servidor Pandora y el Servidor de Gestión de Archivos, en la Figura 45 se muestra la prueba de conectividad.

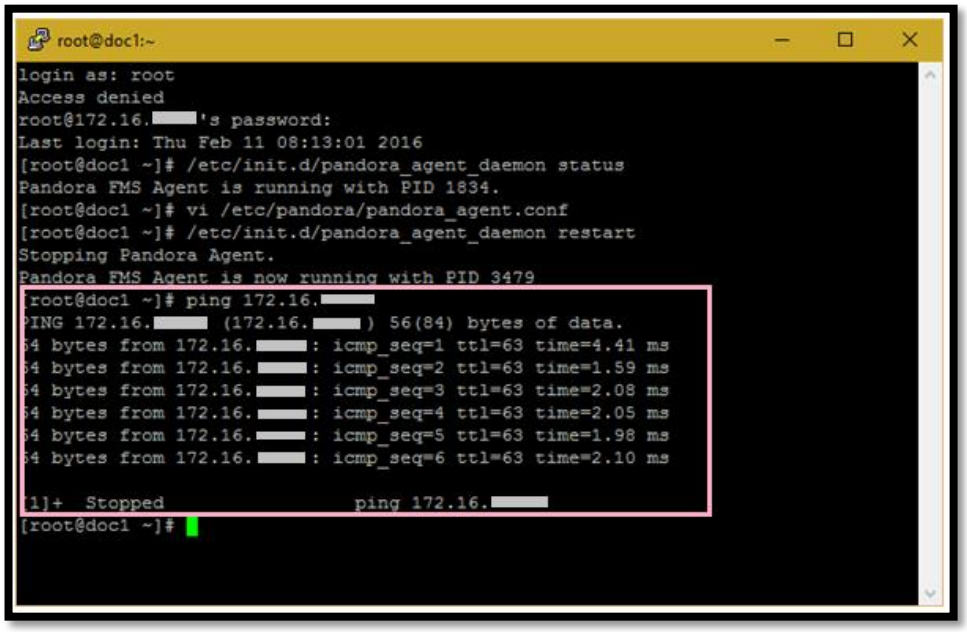


Figura 45. Ping entre Servidor de Archivos y Servidor Pandora FMS
Fuente: Consola Pandora FMS

Luego de la configuraciones necesarias En las Figuras 46 y 47 se puede observar que el servidor se encuentra añadido correctamente y el monitoreo de servicios para diferentes aspectos como memoria disponible, uso del cpu, memoria libre, uso de bytes, numero de procesos activados entre otros está activado.

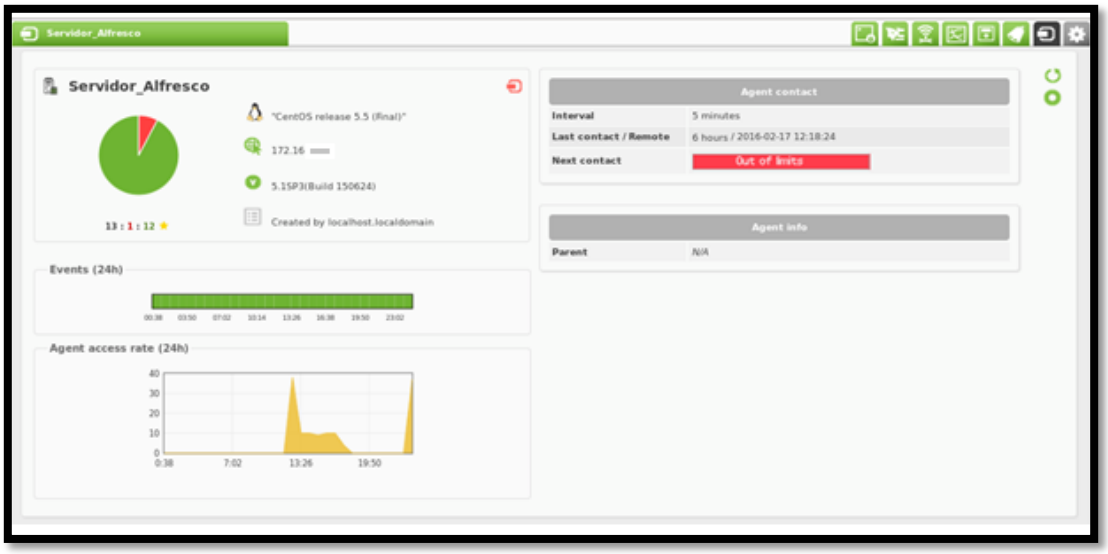


Figura 46. Servidor Gestión de Archivos Activo en Consola Pandora FMS

Fuente: Consola Pandora FMS

Figura 47. Servicios Monitoreados del Servidor de Gestión de Archivos

Fuente: Consola Pandora FMS

En las figura 48, 49, 50 y 51 se muestran algunos gráficos del monitoreo de este equipo, el cual llega a tener muy poca memoria libre, ya que este almacena toda la información de procesos y contratos de la Prefectura de Imbabura, debido a la seguridad que debe tener el manejo de este servidor solo una persona maneja el sistema lo cual se denota en el número de usuarios conectados.

Figura 48. Memoria Disponible Servidor de Gestión de Archivos

Fuente: Consola Pandora FMS

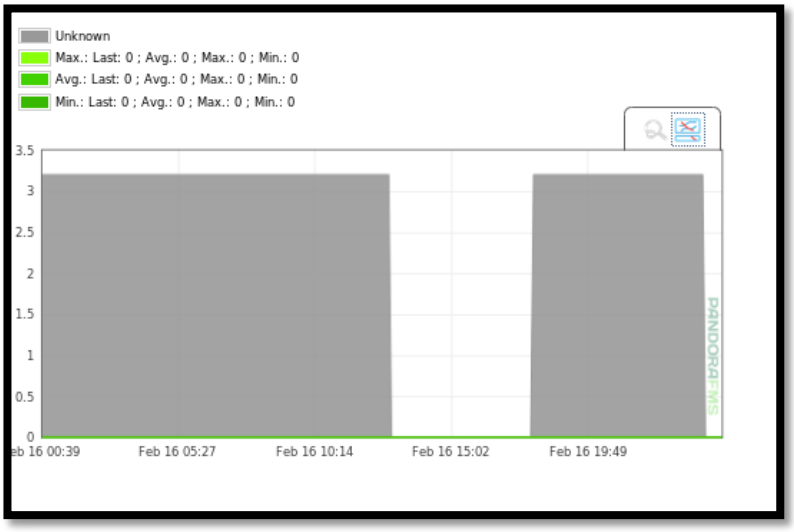


Figura 49. Usuarios Conectados Servidor de Gestión de Archivos

Fuente: Consola Pandora FMS

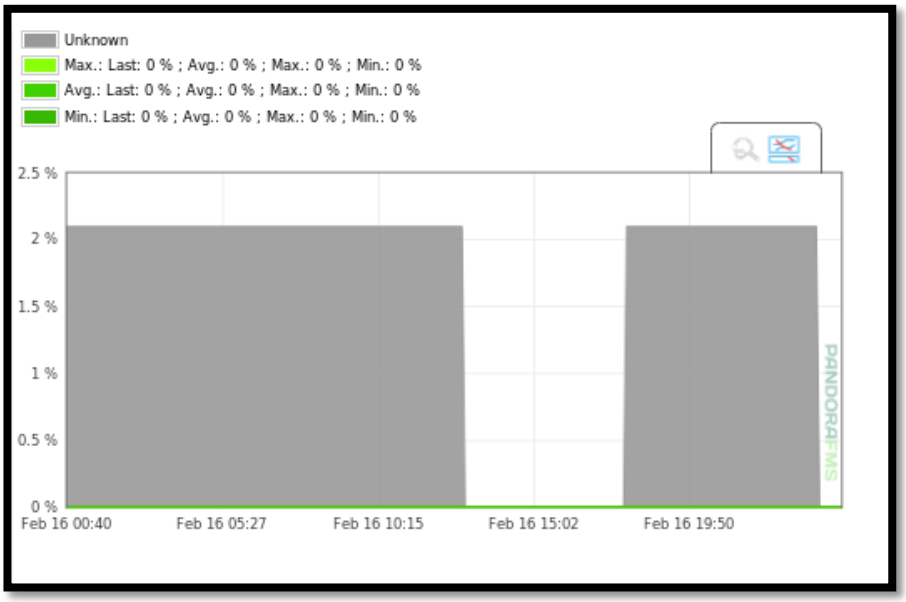


Figura 50. Memoria Libre Servidor de Gestión de Archivos

Fuente: Consola Pandora FMS

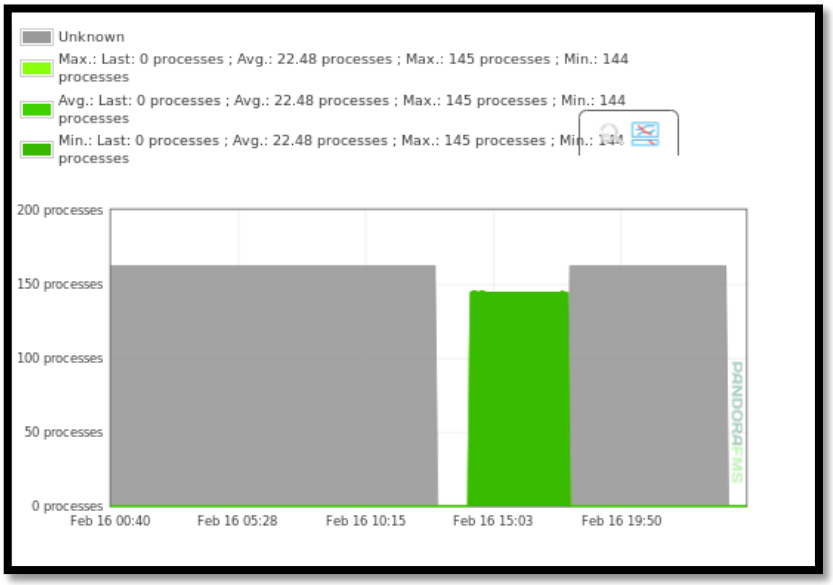


Figura 51. Número de Procesos Servidor de Gestión de Archivos

Fuente: Consola Pandora FMS

3.1.4 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, su formato se muestra en la Figura 53.

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 52.

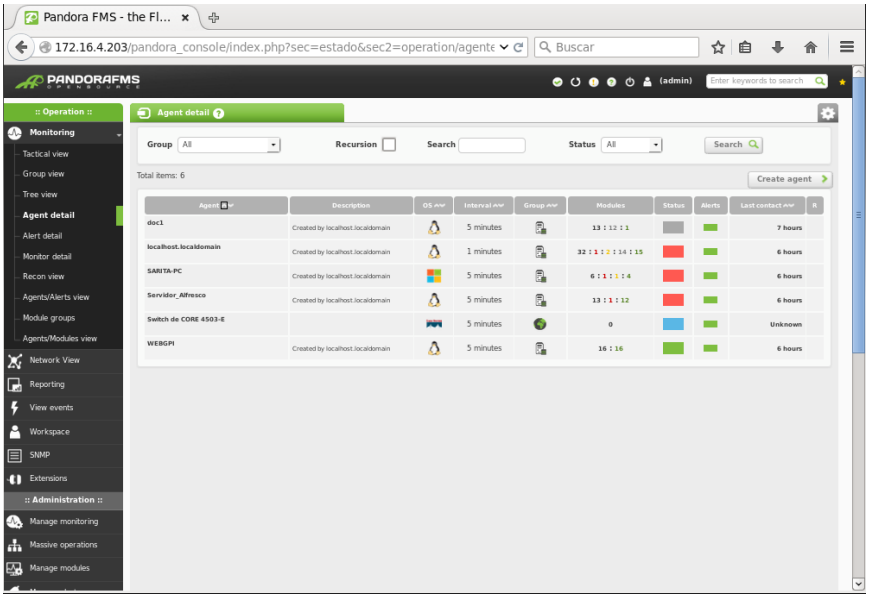


Figura 52. Agentes monitoreados en consola Pandora FMS

Fuente: Consola Pandora FMS

INVENTARIO DEL PARQUE INFORMÁTIVO PREFECTURA DE IMB

DIRECCIÓN DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

PREFECTURA DE IMBABURA

PREFECTURA DE IMBABURA
Dirección de Tecnologías de la Información y Comunicación

NÚMERO	TIPO(escritorio/tatil	CÓDIGO ACTIV FIJO/CI	DIR. IP	PISO	DIRECCIÓN	SUBDIRECCIÓN	RESPONSABLE	SISTEMA OPERATIVO	N LICENCIA	
1	ESCRITORIO	35	no se puede ver	PLANTA BAJA	ADMINISTRATIVA	BODEGA	XAVIER CARDENAS	WINDOWS XP	P6JGJ-PFW6P-9XPJX-2RHYC-W9PDC-X13-2	MICROSOFT OFFICE 2
2	ESCRITORIO	110	172.16.16.57	PLANTA BAJA	ADMINISTRATIVA	MECANICA	ANDRES CORREA	WINDOWS VISTA	RDWRJ-XYHKC-3P6TT-MV2QC-3FB3J-X13-7	MICROSOFT OFFICE 2
3	ESCRITORIO	36	172.16.16.55	PLANTA BAJA	ADMINISTRATIVA	BODEGA	WILLIAM ORTEGA	WINDOWS 7	2WTWD-6XYD6-6YF33-MR2Y8-CVDDF-X15-	MICROSOFT OFFICE 2
4	ESCRITORIO	31	172.16.16.52	PLANTA BAJA	ADMINISTRATIVA	BODEGA	JOFRE AYALA	WINDOWS XP	SIN LICENCIA	MICROSOFT OFFICE 2
5	ESCRITORIO	193	172.16.16.50	PLANTA BAJA	ADMINISTRATIVA	BODEGA	GRECIA ROCAFUERTE	WINDOWS XP	XF93B-7XXFY-YYMMM-HTYFP-8W8PB	MICROSOFT OFFICE 2
6	ESCRITORIO	313	172.16.16.53	PLANTA BAJA	ADMINISTRATIVA	BODEGA	FRANKLIN VASQUEZ	WINDOWS XP	RDGXY-QR6K6-3WFXD-XBJTV-TXB3M	MICROSOFT OFFICE 2
7	ESCRITORIO	5486	172.16.16.58	PLANTA BAJA	ADMINISTRATIVA	BODEGA	RUBEN ARMANDO MORA	WINDOWS 7	QV383AV#006	MICROSOFT OFFICE 2
8	ESCRITORIO	33	172.16.16.54	PLANTA BAJA	ADMINISTRATIVA	BODEGA	FERNANDO QUINTERO	WINDOWS XP	H6BK8-74XBT-F7VPP-6BRXW-6HBHR-X13-23	MICROSOFT OFFICE 2
9	ESCRITORIO	30	172.16.10.62	PLANTA ALTA 1	ADMINISTRATIVA	ADQUISICIONES	DIEGO URVINA	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
10	PORTÁTIL	1539	172.16.10.10	PLANTA ALTA 1	ADMINISTRATIVA	ADMINISTRATIVO	AMPARITO POSSO	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
11	ESCRITORIO	48	172.16.10.56	PLANTA ALTA 1	ADMINISTRATIVA	COMPRAS PÚBLICAS	MARCELO GUEVARA	WINDOWS XP	SIN LICENCIA	MICROSOFT OFFICE 2
12	ESCRITORIO	43	172.16.10.183	PLANTA ALTA 1	ADMINISTRATIVA	COMPRAS PÚBLICAS	EDISON CAVIEDES	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
13	ESCRITORIO	6483	172.16.10.57	PLANTA ALTA 1	ADMINISTRATIVA	COMPRAS PÚBLICAS	PABLO VALDOSPINOS	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
14	ESCRITORIO	5501	172.16.10.188	PLANTA ALTA 1	ADMINISTRATIVA	COMPRAS PÚBLICAS	ALEXANDRA GUALPA	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
15	ESCRITORIO	26	172.16.10.153	PLANTA ALTA 1	ADMINISTRATIVA	ADMINISTRATIVO	MARÍA JUDITH PROAÑO	WINDOWS XP	8TRTV-MC4TX-4HXHX-X29R6-RHM92	MICROSOFT OFFICE 2
16	ESCRITORIO	6485	172.16.10.38	PLANTA ALTA 1	ADMINISTRATIVA	ADMINISTRATIVO	MARCELO ORTIZ	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
17	ESCRITORIO	34	172.16.10.41	PLANTA ALTA 1	ADMINISTRATIVA	TRANSPORTES	PABLO VASQUEZ	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
18	ESCRITORIO	35	172.16.10.40	PLANTA ALTA 1	ADMINISTRATIVA	TRANSPORTES	KLEVER DIAZ	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
19	ESCRITORIO	32	172.16.10.111	PLANTA ALTA 1	ADMINISTRATIVA	TRANSPORTES	JESICA PRECIADO	WINDOWS XP	PCBBV-89G24-43HTC-6PCQF-VRWVM	MICROSOFT OFFICE 2
20	ESCRITORIO	173	172.16.50.252	PLANTA ALTA 2	CONTRALORIA	CONTRALORIA	LUZ MARIA MALDONADO	WINDOWS XP	SIN LICENCIA	MICROSOFT OFFICE 2
21	PORTÁTIL	65	172.16.23.3	PLANTA ALTA 2	COOPERACIÓN INTERNACIONAL	COOPERACION INTERNACIONAL	OSCAR PEREZ	WINDOWS 7	C3426-DTHBC-FH7W5-34VPX-MTB67	MICROSOFT OFFICE 2
22	PORTÁTIL	6145	172.16.22.30	PLANTA ALTA 2	COOPERACIÓN INTERNACIONAL	COOPERACION INTERNACIONAL	CARLOS MERIZALDE	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
23	ESCRITORIO	215	172.16.8.25	PLANTA ALTA 2	COOPERACIÓN INTERNACIONAL	COOPERACION INTERNACIONAL	BORIS LOPEZ	WINDOWS XP	H63FD-7QX87-4PC4P-DPKWG-PWVY6	MICROSOFT OFFICE 2
24	ESCRITORIO	214	172.16.8.14	PLANTA ALTA 2	COOPERACIÓN INTERNACIONAL	COOPERACION INTERNACIONAL	ROBERTO MONTESDEOCA	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
25	ESCRITORIO	27	172.16.8.23	PLANTA ALTA 2	COOPERACIÓN INTERNACIONAL	COOPERACION INTERNACIONAL	ELIZABETH VASQUEZ	WINDOWS XP	SIN LICENCIA	MICROSOFT OFFICE 2
26	PORTÁTIL	5523	172.16.5.150	PLANTA ALTA 1	COORDINACION GENERAL	COORDINACION GENERAL	MARCO JARRIN	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2
27	ESCRITORIO	183	172.16.5.80	PLANTA ALTA 1	COORDINACION GENERAL	SECRETARIA COORDINACION GENERAL	SHIRLEY ALMEIDA	WINDOWS XP	SIN LICENCIA	MICROSOFT OFFICE 2
28	ESCRITORIO	219	172.16.12.20	PLANTA BAJA	DESARROLLO ECONOMICO Y GESTION AMBIE	TURISMO	DIEGO SALAZAR	WINDOWS 7	SIN LICENCIA	MICROSOFT OFFICE 2

COMPUTADORAS | IMPRESORAS Y OTROS

LISTO

Figura 53. Inventario Parque Informático

Fuente: Prefectura de Imbabura

3.1.5 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.

Figura 54. Entrada al Servidor de Pandora FMS
Fuente: Consola Pandora FMS

3.1.5.1 Cambio de Contraseña por defecto del Sistema

Este cambio es muy sencillo simplemente se debe dirigir a la opción Workspace – Edit my User, esta opción se muestra en la Figura 55.

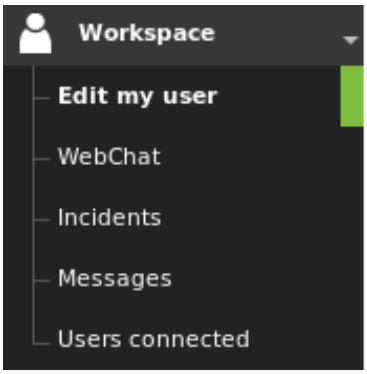


Figura 55. Pestaña Workspace
Fuente: Consola Pandora FMS

En la pantalla mostrada en la Figura 56 se edita la nueva contraseña la cual será brindada solo al administrador de la red, hacer clic en el boton Update y la contraseña será cambiada automaticamente.

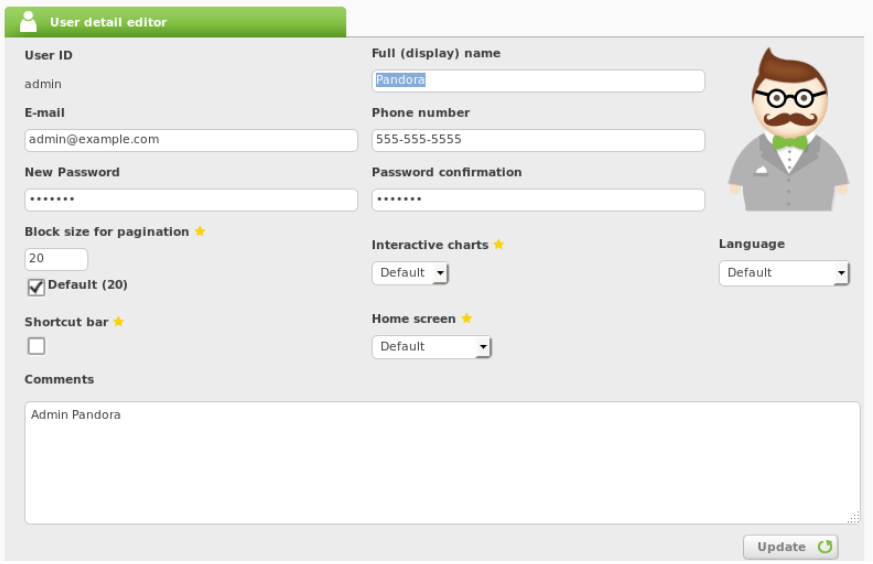


Figura 56. Pantalla para editar la contraseña del Usuario

Fuente: Consola Pandora FMS

3.1.5.2 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.

3.2 Politicas 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.

A continuación se presenta un manual con cada una de las políticas de gestión para la red de datos de la Prefectura de Imbabura, su principal función es crear reglas para que exista un buen uso del software de gestión instalado, y se pueda facilitar la detección y solución de errores que puedan presentarse.

3.2.1 Introducción

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 mostrado en el apartado 3.1.1.5, y el manual de procedimientos que se muestra en la sección 3.3 del documento.

PREFECTURA DE IMBABURA		
Políticas de Gestión para la Red Interna		
PREFECTURA DE IMBABURA	**Elaborado por:**	Sara Cuchala
	Revisado por:	Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información

I. PROPÓSITO

Este documento permitirá dar a conocer las políticas de gestión que deberán cumplirse por el responsable de la administración de la red, de tal manera que se pueda garantizar su disponibilidad y rendimiento.

II. CONCEPTOS PREVIOS

- **Gestión De Red:** mediante la integración de hardware, software y elementos humanos, la gestión de red permite configurar, analizar y evaluar los recursos de red de manera eficaz, para poder garantizar la disponibilidad de la red hacia los usuarios.
- **Políticas de Gestión:** es una manual que permite al administrador de la red manejar de forma ordenada cualquier suceso que pueda presentarse en la red
- **Monitoreo de Red:** permite de manera oportuna detectar, diagnosticar y hallar una forma de resolver rápidamente los problemas de desempeño de la red.

III. GENERALIDADES

a) Las políticas de gestión mostradas en este documento, podrán ser susceptibles a cambios, siempre y cuando se cumplan las reglas establecidas por el modelo.

b) El personal de la Dirección de Tecnologías que utilice las políticas de gestión, deberá tratar de cumplir el orden de las mismas, para la solución de errores que se susciten en la red.

c) Este documento está realizado como una guía para el personal encargado del sistema de monitoreo de red implementado.

IV. ESTRUCTURA ADMINISTRATIVA

a) Director

Es el jefe de la Dirección de Tecnologías de la Información, bajo su jurisdicción está la aceptación de las políticas de gestión, en conformidad con el Jefe de Operaciones.

b) Jefe de Operaciones

Es la persona encargada de ver el estado de la red, y asegurar su disponibilidad, mantenimiento y rendimiento, tiene bajo su dirigencia dos ingenieros en infraestructura que se encargan del correcto funcionamiento del cuarto de comunicaciones.

V. VALIDEZ

Este documento tendrá validez desde el momento de su aceptación por el personal correspondiente de la Dirección de Tecnologías de la Información de la Prefectura de Imbabura. Este manual para las políticas de gestión podrá ser actualizado conforme a las necesidades de la infraestructura de red de la institución.

VI. REFERENCIA

En la actualidad no existe un formato para la presentación de las políticas de gestión por lo que este documento se realiza en base a las configuraciones realizadas en el sistema de gestión y monitoreo.

Este documento toma como referencia la tesis realizada en el GAD de Ibarra (Ayala Viviana, 2015, págs. 101-113)

VII. ESTRUCTURA DE LAS POLÍTICAS DE GESTIÓN

Las políticas de Gestión se realizarán de acuerdo al modelo ISO utilizando sus cinco áreas funcionales.

7.1 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.

7.2 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.

1. Ingreso de dispositivos de red al software de gestión
2. Configuración de dispositivos de red
3. Configuración de equipos de servidores Linux
4. Configuración de equipos de servidores Windows
5. Documentación de configuraciones

7.3 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.

1. Manejo de fallos
2. Manejo de umbrales
3. Notificación de eventos

7.4 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.

1. Parámetros de Monitoreo

7.5 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.

1. Recolección de datos de rendimiento de la red
2. Generación de reportes

7.6 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

1. Control de acceso al software
2. Control de acceso a los dispositivos gestionados

3. Control de acceso a usuarios

VIII. TÉRMINOS Y DEFINICIONES

- **Prefectura de Imbabura:** entidad encargada de brindar obras y servicios a la ciudanía de la provincia de Imbabura.
- **Dirección de TIC's:** Departamento de Tecnologías de Información de la Prefectura de Imbabura, encargado de manejar el software y hardware de la red de la institución.
- **Hardware:** componentes físicos que funcionan dentro de un sistema informático.
- **Software:** componentes lógicos que hacen posible la realización de tareas informáticas.
- **Dispositivos de red:** equipos que permiten la interconexión y comunicación entre distintas dependencias.
- **Disponibilidad:** este término indica que los equipos y servicios siempre deben estar activos en la red.
- **ISO:** Organización Internacional de Estándares, se encarga de la evaluación, gestión y puesta en práctica de procedimientos, normas de fabricación, comercio y comunicación, aceptadas y legalmente reconocidas.
- **SNMP:** Protocolo simple de administración de red, permite supervisar, analizar y comunicar información del estado de una gran variedad de equipos de red.
- **Reporte:** informe que puede obtenerse en forma impresa o digital, contiene información del estado de los dispositivos gestionados.
- **Notificación:** es un aviso por correo electrónico cuando algún dispositivo de la red este fallando.
- **Alertas:** Permiten avisar al administrador de red cuando un módulo ha pasado a un estado de advertencia o crítico.

IX. DESARROLLO DE LAS POLÍTICAS DE GESTIÓN

PREFECTURA DE IMBABURA		
	CODIGO	POL-PI-001
	DOMINIO	1. Políticas para la gestión de la red interna
	ENCARGADO	Director y Jefe de Operaciones
1.1 Objetivos de las políticas de gestión		**Art 1.** Dar a conocer el funcionamiento del sistema de gestión al personal responsable de la administración de red, mediante la entrega de información sobre los lineamientos que se deben cumplir, para garantizar la disponibilidad de la red

	identificando los problemas que puedan apareces en los dispositivos gestionados
1.2 Elaboración de documento	**Art 2.** Se elaborará un manual de políticas y procedimientos para la gestión de la red interna, siguiendo las áreas funcionales del estándar de gestión ISO.
1.3 Revisión políticas de gestión	**Art 3.** El manual de políticas y procedimientos deberá ser revisado por el jefe de Dirección de TIC's de la Prefectura de Imbabura, para que tome el compromiso de la utilización de los mismos para garantizar el buen funcionamiento del sistema de gestión

PREFECTURA DE IMBABURA		
	CODIGO	POL-PI-002
	DOMINIO	2. Políticas para la gestión de configuración
	ENCARGADO	Jefe de Operaciones
2.1 Ingreso de dispositivos de red al software de gestión		**Art 4.** El jefe de operaciones debe garantizar se mantenga actualizado el inventario de equipos activos que mantiene la red de la Prefectura de Imbabura.
		Art 5. Para ingresar un dispositivo de red al software de gestión el Jefe de Operaciones deberá documentar el equipo con toda su información y características en un documento de Excel.
		Art 6. Se debe analizar el estado de la red antes de ingresar cualquier dispositivo.
		Art 7. Luego de agregar el dispositivo deberá verificar que este se encuentre activo luego de la realización del barrido de la red en el software de gestión.
2.2 Configuración de Dispositivos de Red		**Art 8.** Habilitar el protocolo SNMPv2 en el equipo indicando la comunidad de administración y los permisos que pueden ser de lectura o escritura.
		Art 9. Configurar los módulos en la consola Web de Pandora FMS.

	Art 10. Definir los equipos y los servicios a monitorear desde la Consola de Pandora FMS
	Art 11. Seleccionar los grupos a los que pertenecerá cada equipo en la red y configurar las condiciones en las que se recibirán notificaciones de cada uno de los dispositivos.
	Art 12. Configurar las cuentas de correo que recibirán las notificaciones emitidas por Pandora FMS.
	Art 13. Realizar una comprobación y recolección de información sobre las configuraciones realizadas.
2.3 Configuración de Equipos Servidores Linux	**Art 14.** Instalar el agente de monitoreo pandora_agent en el equipo LINUX.
	Art 15. Configurar el archivo /etc/pandora/pandora_agent.conf indicando la IP del servidor PANDORA FMS al cual se devolverá la información de los recursos del equipo.
	Art 16. Configurar el agente remoto en la Consola de Pandora FMS.
	Art 17. Configurar los módulos (servicios) que van a ser monitoreados en la consola.
	Art 18. Seleccionar el grupo al que pertenecerá cada equipo en la red y configurar las notificaciones del dispositivo.
	Art 19. Configurar las cuentas de correo que recibirán las notificaciones emitidas por PANDORA FMS.
	Art 20. Realizar una comprobación y recolección de información sobre las configuraciones realizadas.
2.4 Configuración de Equipos Servidores Windows	**Art 21.** Instalar el agente de monitoreo Pandora FMS Windows Agent en el equipo WINDOWS.
	Art 22. Configurar el agente indicando la IP del servidor PANDORA FMS al cual se devolverá la información de los recursos del equipo.

	Art 23. Configurar el agente remoto en la Consola de Pandora FMS.
	Art 24. Configurar los módulos (servicios) que van a ser monitoreados en la consola
	Art 25. Seleccionar el grupo al que pertenecerá cada equipo en la red y configurar las notificaciones del dispositivo.
	Art 26. Configurar las cuentas de correo que recibirán las notificaciones emitidas por PANDORA FMS.
	Art 27. Realizar una comprobación y recolección de información sobre las configuraciones realizadas.
2.5 Documentación de configuraciones	**Art 28.** Antes de realizar cualquier cambio a las configuraciones de los equipos o servidores el jefe de operaciones debe asegurarse que se haya realizado un respaldo con la configuración anterior del equipo
	Art 29. El administrador de la red deberá documentar todos los cambios en cuanto a configuración realizados en la red.

PREFECTURA DE IMBABURA		
	CODIGO	POL-PI-003
	DOMINIO	3. Políticas para la gestión de fallos
	ENCARGADO	Jefe de Operaciones
3.1 Manejo de Fallos		**Art 30.** Las fallas que pueda presentar la red deberán ser visualizadas en el sistema de monitoreo de la Consola de Pandora FMS o mediante las notificaciones de correo electrónico que el software de monitoreo envía.
		Art 31. El jefe de operaciones deberá designar a la persona responsable para poder diagnosticar y corregir cualquier error de la red.
		Art 32. El responsable de la red deberá encontrar la solución para el problema que se presente en la red de la manera más eficiente, es decir en un

	corto tiempo, de esta manera se asegura la disponibilidad de servicios en la red.
	Art 33. Se sugiere tomar en cuanto los estados de advertencia que muestra el software de monitoreo para evitar que surjan problemas serios en la red.
3.2 Manejo de Umbrales	**Art 34.** El responsable del manejo de la red deberá revisar los umbrales establecidos por el software de gestión, los cuales se dividen en normal, advertencia y crítico, para estar alerta cuando se dispare una alarma indicado un estado crítico de cualquier dispositivo de la red.
3.3 Manejo de eventos	**Art 35.** Gracias al envío de notificaciones por correo electrónico que brinda Pandora FMS el administrador de la red, deberá ubicar de manera oportuna el fallo ocurrido y solucionarlo de la manera más eficiente posible.

PREFECTURA DE IMBABURA		
	CODIGO	POL-PI-004
	DOMINIO	4. Políticas para la gestión de contabilidad
	ENCARGADO	Jefe de Operaciones
4.1 Parámetros de Monitoreo		**Art 36.** Todos los dispositivos que se ingresen al software de monitoreo deben cumplir con las configuraciones necesarias para evitar fallos improvistos en la red.
		Art 37. El jefe de operaciones deberá conocer el funcionamiento de cada uno de los dispositivos de la red, para poder identificar los parámetros que muestra el software de gestión.

PREFECTURA DE IMBABURA		
	CODIGO	POL-PI-005
	DOMINIO	5. Políticas para la gestión de prestaciones
	ENCARGADO	Jefe de Operaciones
5.1 Recolección de datos de rendimiento de la red		**Art 38.** Gracias a la Consola de Pandora FMS el responsable de la red podrá observar mediante

	gráficos y topologías el rendimiento y activación de los equipos ingresados al sistema.
	Art 39. El responsable de la red podrá visualizar el consumo de ancho de banda de las interfaces de los equipos monitoreados mediante gráficos, gracias a la utilización de SNMP dentro del software de monitoreo.
5.2 Generación de Reportes	**Art 40.** El responsable de la red podrá generar reportes en la Consola de Pandora FMS de acuerdo a los requerimientos de la Dirección.
	Art 41. Los reportes servirán como información acerca de los recursos monitoreados, podrán obtenerse en el momento requerido. Se sugiere que se utilice medios digitales para visualizar los informes, de esta manera se evitará el consumo innecesario de papel que generan las impresiones.

PREFECTURA DE IMBABURA	**PREFECTURA DE IMBABURA**	
	CODIGO	POL-PI-006
	DOMINIO	6. Políticas para la gestión de seguridad
	ENCARGADO	Jefe de Operaciones
6.1 Control de Acceso al Software		**Art 42.** Como se indicó en el documento el acceso será únicamente para el responsable de la red, el cual tendrá la potestad de crear el acceso para usuarios con los privilegios que considere necesarios.
		Art 43. Las notificaciones generadas en el Software por los dispositivos gestionados serán enviadas únicamente al administrador de la red.
6.2 Control de Acceso a los dispositivos gestionados		**Art 44.** El sistema instalado puede estar sujeto a modificaciones, actualizaciones o ingreso de nuevos equipos, esto será de única responsabilidad del responsable de la red.
		Art 45. El acceso a cada uno de los dispositivos debe tener contraseñas las cuales deben ser asignadas únicamente por el responsable de la red.

6.3 Control de Acceso a usuarios	**Art 46.** El responsable de la red será el único con la potestad de agregar o quitar usuarios tanto a la red, como al sistema de monitoreo.

3.3 Manual de procedimientos

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.

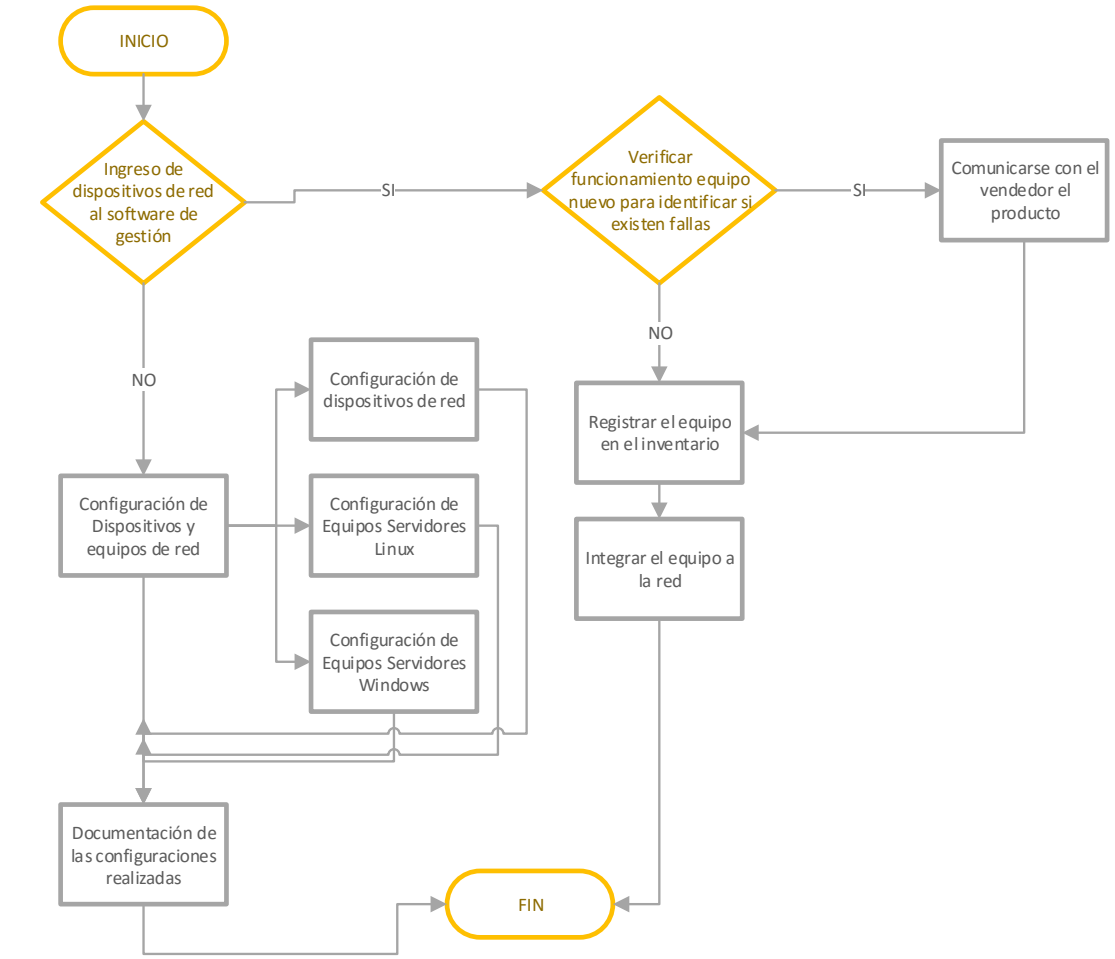
3.3.1 Manual de procedimientos para la gestión de configuración

PREFECTURA DE IMBABURA			
PREFECTURA DE IMBABURA	**PROCEDIMIENTOS PARA LA GESTIÓN DE CONFIGURACION**		
Versión: 1.0	**Revisado por:** Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información		
	Elaborado por: Sara Carolina Cuchala Vásquez		
Código: MP-PI-001	GAD PROVINCIAL DE IMBABURA		
N°	**Actividad**	**Descripción**	**Responsable**
1	Ingreso de dispositivos de red al software de gestión	Para ingresar un equipo nuevo a la red se debe: - Verificar su funcionamietno y que no existan fallas	Jefe de operaciones

		- Registrarlo en el inventario - Integrarlo a la red	
2	Configuración de dispositivos de red	Para ingresar un equipo al software de gestión se debe: - Verificar las configuraciones iniciales del equipo. - Verificar si el protocolo SNMP está activo - Añadir el equipo a la consola de Pandora FMS, como se muestra en el Anexo C - Realizar las configuraciones de modulos y alertas	Jefe de operaciones
3	Configuración de equipos servidores Linux	Para ingresar un equipo Linux al software de gestión se debe: - Instalar el agente en el equipo, como se muestra en el anexo C. - Añadir el equipo a la consola de Pandora FMS. - Realizar las configuraciones de modulos y alertas.	Jefe de operaciones
4	Configuración de equipos servidores Windows	- Instalar el agente en el equipo, como se muestra en el anexo C. - Añadir el equipo a la consola de Pandora FMS. Realizar las configuraciones de modulos y alertas.	Jefe de operaciones

5	Documentación de configuraciones	La documentación de configuraciones se encuentra almacenada en el Anexo C (Manual de Administrador) este contiene: - Configuración de consola de Pandora FMS - Configuración agente Linux - Configuración de agente Windows - Creación de módulos de monitoreo - Generación de reportes	Jefe de operaciones

FLUJOGRAMA:

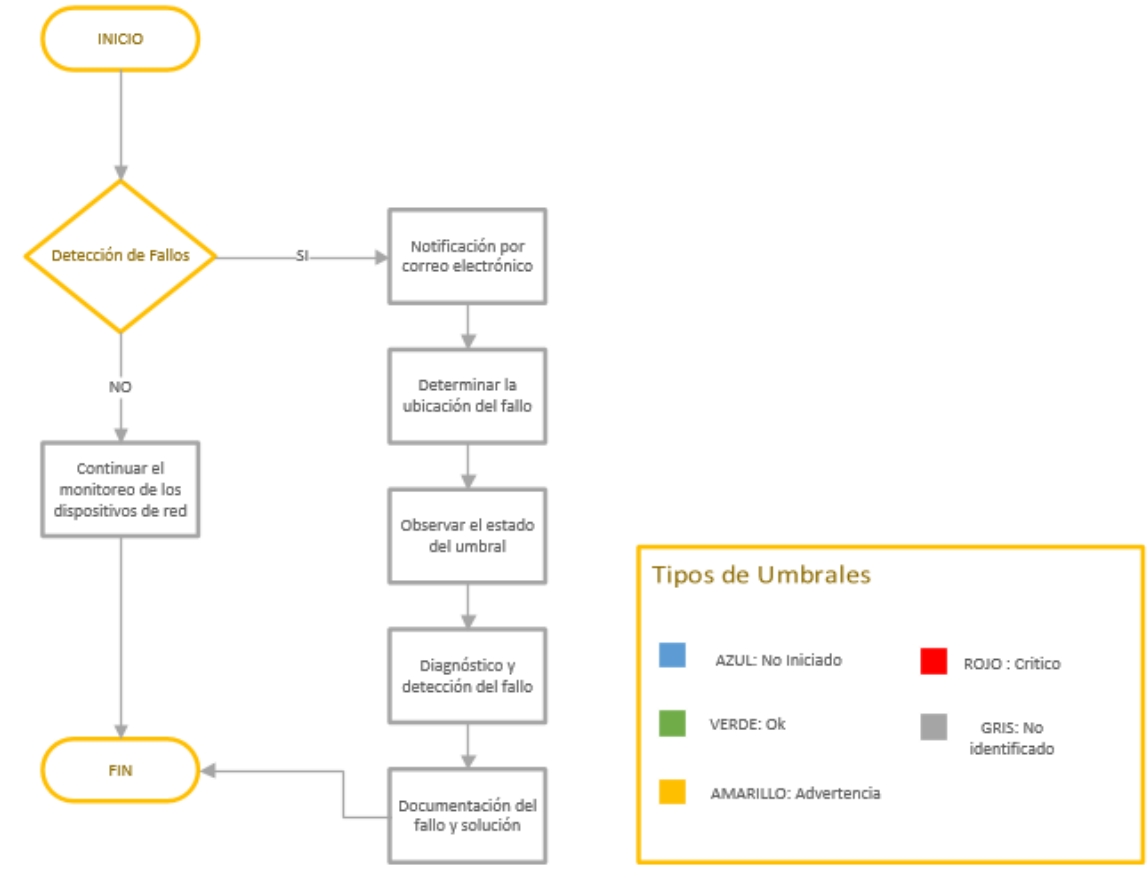


3.3.2 Manual de procedimientos para la gestión de fallos

<table>
<tr><td colspan="4">PREFECTURA DE IMBABURA</td></tr>
<tr><td>PREFECTURA DE IMBABURA</td><td colspan="3">PROCEDIMIENTOS PARA LA GESTIÓN DE FALLOS</td></tr>
<tr><td rowspan="2">Versión: 1.0</td><td colspan="3">Revisado por: Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información</td></tr>
<tr><td colspan="3">Elaborado por: Sara Carolina Cuchala Vásquez</td></tr>
<tr><td>Código: MP-PI-002</td><td colspan="3">GAD PROVINCIAL DE IMBABURA</td></tr>
<tr><td>N°</td><td>Actividad</td><td>Descripción</td><td>Responsable</td></tr>
<tr><td>1</td><td>Detección de Fallo</td><td>- Monitorear mediante la Consola Web de Pandora FMS el estado de los dispositivos
- Identificar la notificación del fallo enviada por correo electrónico</td><td>Jefe de operaciones</td></tr>
<tr><td>2</td><td>Aislamiento del Fallo</td><td>- Determinar la ubicación donde se produce el problema en la red
- Pandora FMS divide en estados los umbrales para verificar los fallos.
Azul: No iniciado
Verde: Normal
Amarillo: Advertencia
Rojo: Estado crítico
Gris: Desconocido</td><td>Jefe de operaciones</td></tr>
<tr><td>3</td><td>Diagnostico y corrección del fallo</td><td>- Realiza un seguimiento y control del prblema</td><td>Jefe de operaciones</td></tr>
</table>

		desde que se lo detectas hasta hallar la solución - Determinación de la solución para el problema de la red - Realizar un respaldo de las configuraciones del equipo o dispositivo de red. - Corregir el fallo con la solución planteada	
4	Documentación	Se debe documentar todas las fallas producidas en la red en conjunto con su solución.	Jefe de operaciones

FLUJOGRAMA:

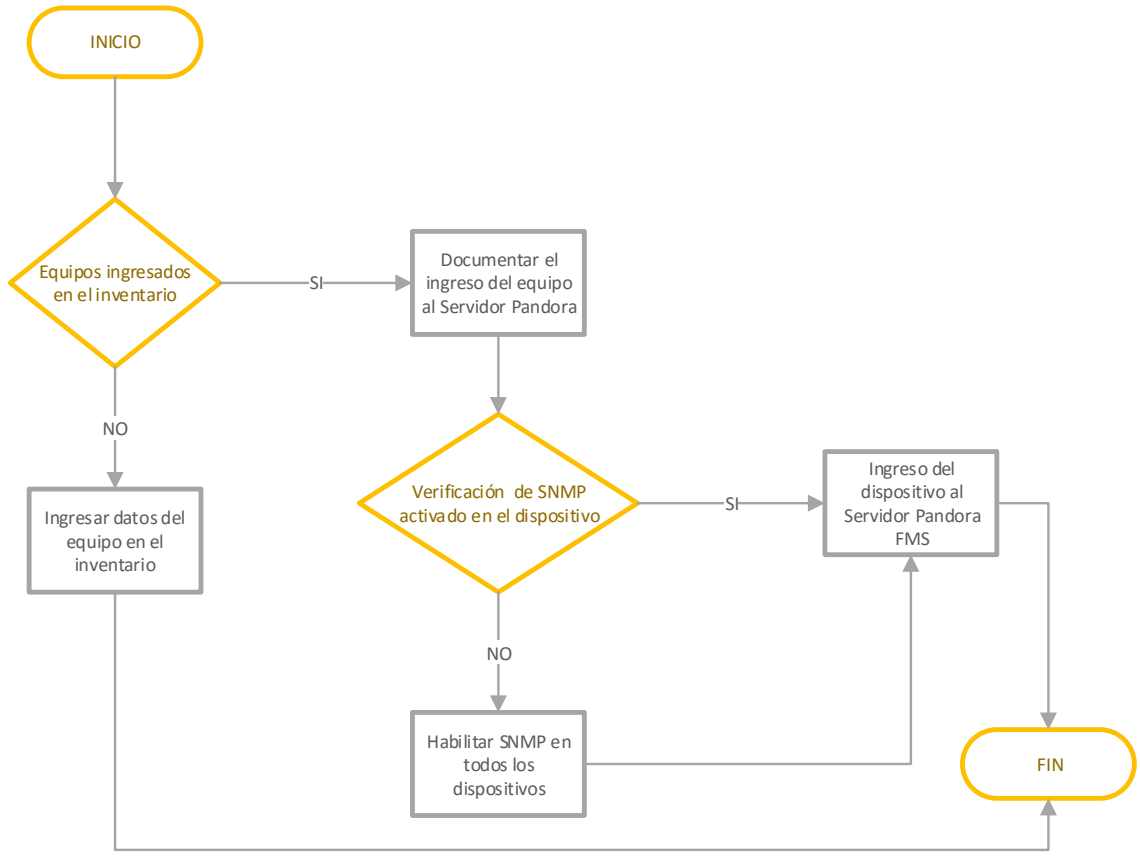


3.3.3 Manual de procedimientos para la gestión de contabilidad

<table>
<tr><td colspan="4">PREFECTURA DE IMBABURA</td></tr>
<tr><td>PREFECTURA DE IMBABURA</td><td colspan="3">PROCEDIMIENTOS PARA LA GESTIÓN DE CONTABILIDAD</td></tr>
<tr><td rowspan="2">Versión: 1.0</td><td colspan="3">Revisado por: Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información</td></tr>
<tr><td colspan="3">Elaborado por: Sara Carolina Cuchala Vásquez</td></tr>
<tr><td>Código: MP-PI-003</td><td colspan="3">GAD PROVINCIAL DE IMBABURA</td></tr>
<tr><td>N°</td><td>Actividad</td><td>Descripción</td><td>Responsable</td></tr>
<tr><td>1</td><td>Inventario de recursos de la red</td><td>- Todos los equipos y dispositivos deben estar ingresados en el inventario de la red.
- Para monitorear un equipo se debe documentar en el inventario si este a sido ingresado al Servidor Pandora.</td><td>Jefe de operaciones</td></tr>
<tr><td>2</td><td>Caraterísticas de los dispositivos</td><td>- Verificar si el equipo ha ser gestionado tiene habilitado SNMP
- Si un dispositivo no tiene activado SNMP el administrador debe hacerlo siguiendo los pasos mostrados en el apartado 3.1.1.5</td><td>Jefe de operaciones</td></tr>
<tr><td>3</td><td>Ingreso al sistema de gestión</td><td>- El dispositivo puede ser ingresado al Servidor Pandora FMS luego de</td><td>Jefe de operaciones</td></tr>
</table>

		haber sido registrado en inventario de equipos.	

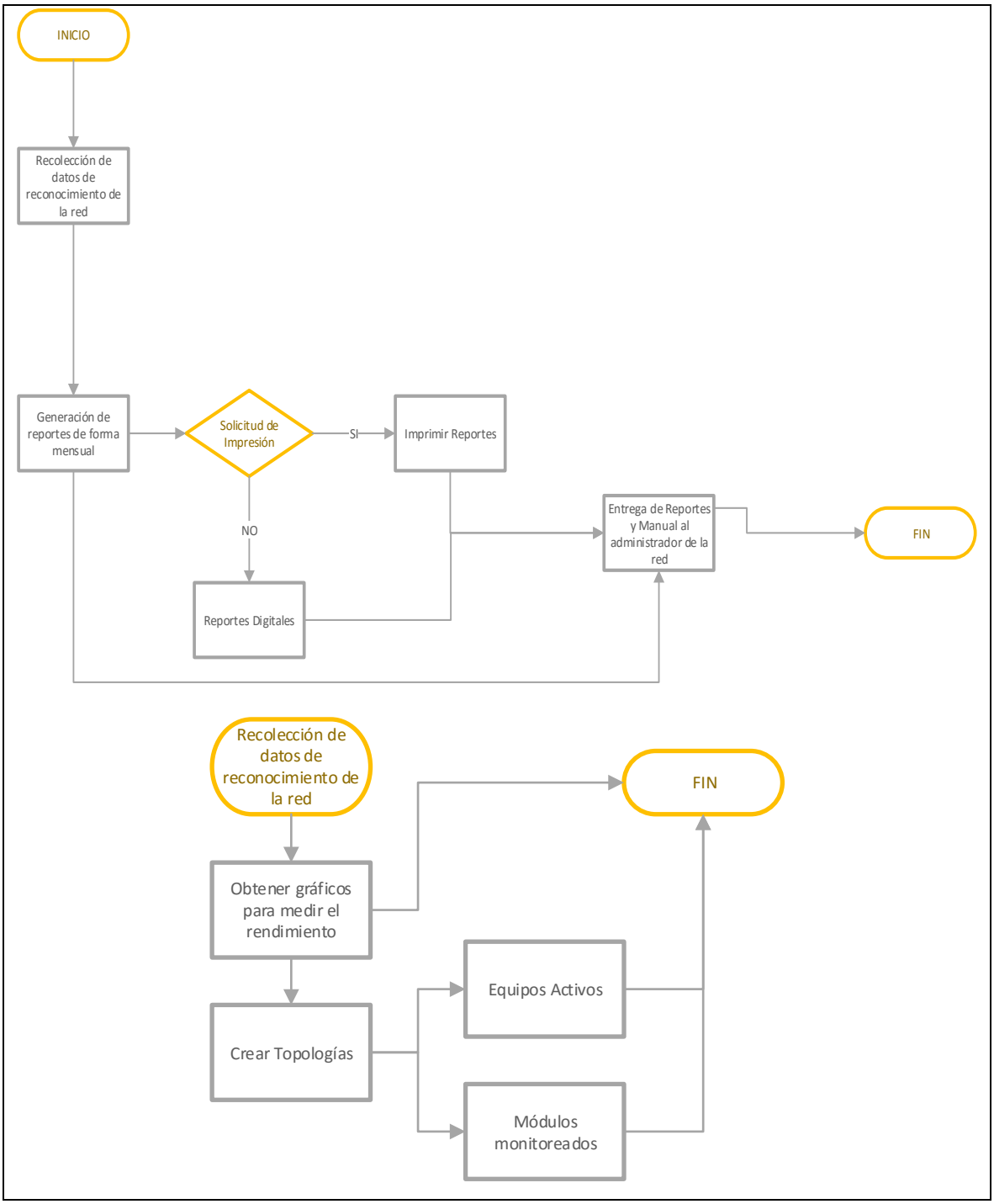
FLUJOGRAMA:



3.3.4 Manual de procedimientos para la gestión de prestaciones

PREFECTURA DE IMBABURA			
PREFECTURA DE IMBABURA	**PROCEDIMIENTOS PARA LA GESTIÓN DE PRESTACIONES**		
Versión: 1.0	**Revisado por:** Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información		
	Elaborado por: Sara Carolina Cuchala Vásquez		
Código: MP-PI-004	GAD PROVINCIAL DE IMBABURA		
N°	**Actividad**	**Descripción**	**Responsable**

1	Recolección de datos de rendimiento de la red	Mediante la Consola Web de Pandora se pueden visualizar: gráficos, topologías, equipos activos ingresados al sistema - Obtener gráficos para medir el rendimiento de la red. - Crear topologías para observar los equipos activos y modulos monitoreados	Jefe de operaciones
2	Generación de Reportes	- Generar reportes de forma mensual para visualizar los estados que ha presentado la red. - Los reportes solo deberan ser impresos si asi lo solicita el Director caso contrario deberan ser entregados en forma digital para evitar el consumo excesivo de papel. - Los informes deberán ser entregados al Director de TIC's para su evaluación.	Jefe de operaciones
3	Entrega de manuales	- Al finalizar el proyecto se entregó el manual de administrador del Sistema de gestión y Monitoreo	Jefe de operaciones
FLUJOGRAMA:			

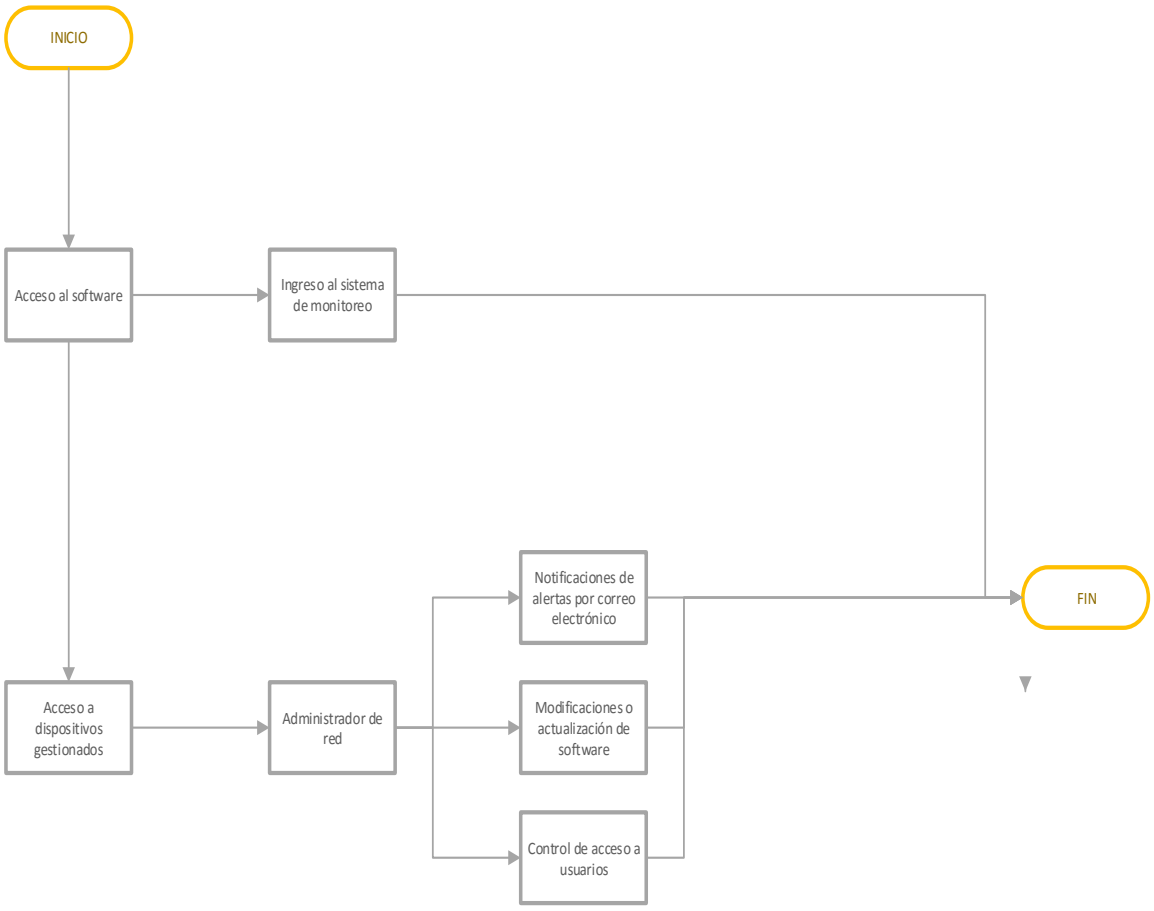

INICIO
Recolección de datos de reconocimiento de la red
Generación de reportes de forma mensual
Solicitud de Impresión
SI
Imprimir Reportes
NO
Reportes Digitales
Entrega de Reportes y Manual al administrador de la red
FIN
Recolección de datos de reconocimiento de la red
FIN
Obtener gráficos para medir el rendimiento
Crear Topologías
Equipos Activos
Módulos monitoreados

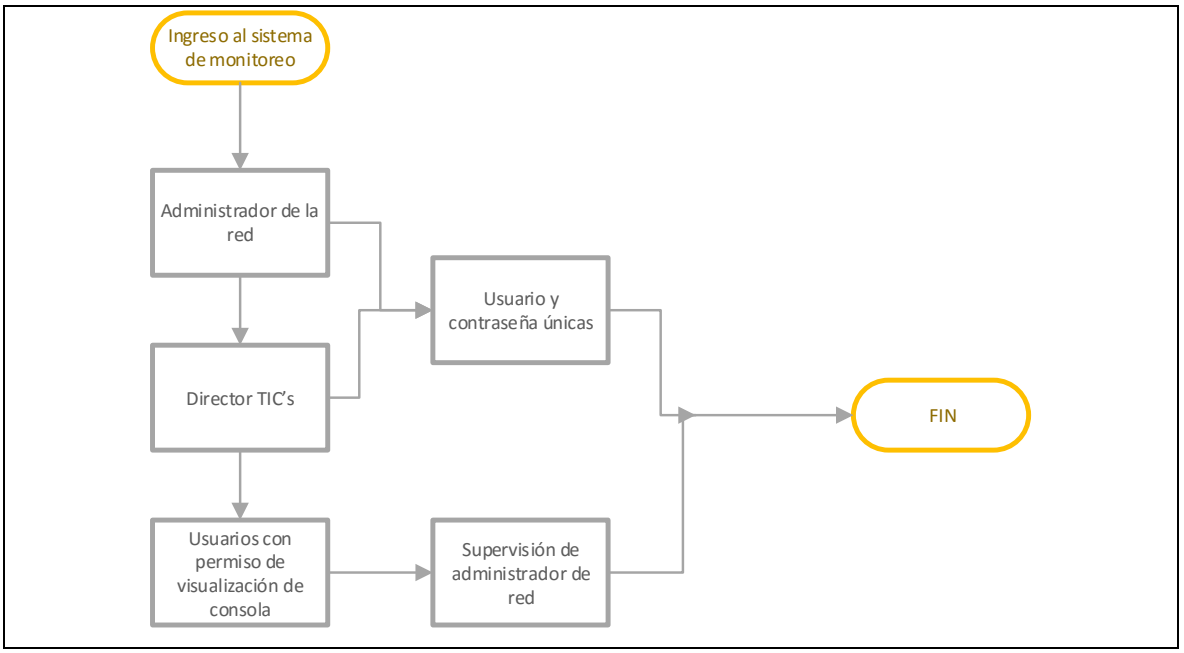
3.3.5 Manual de procedimientos para la gestión de seguridad

<table>
<tr><td colspan="4">PREFECTURA DE IMBABURA</td></tr>
<tr><td colspan="2">PREFECTURA DE IMBABURA</td><td colspan="2">PROCEDIMIENTOS PARA LA GESTIÓN DE SEGURIDAD</td></tr>
<tr><td colspan="2" rowspan="2">Versión: 1.0</td><td colspan="2">Revisado por: Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información</td></tr>
<tr><td colspan="2">Elaborado por: Sara Carolina Cuchala Vásquez</td></tr>
<tr><td colspan="2">Código: MP-PI-005</td><td colspan="2">GAD PROVINCIAL DE IMBABURA</td></tr>
<tr><td>N°</td><td>Actividad</td><td>Descripción</td><td>Responsable</td></tr>
<tr><td>1</td><td>Control de Acceso al Software</td><td>- Al servidor de monitoreo solo puede tener acceso el administrador de la red o el Director de TIC´s usando el mismo usuario y contraseña únicas otorgadas al responsable de la red.
- Los usuarios que no tengan los permisos necesarios podran observar la Consola de Pandora FMS bajo la supervisión del responsable de la red.
- Las notificaciones enviadas por correo electrónico srán dirigidas directamente al correo del administrador de la red.
- Las modificaciones, actualizaciones, o ingreso de nuevos equipos son reponsabilidad del administrador de la red.</td><td>Jefe de operaciones</td></tr>
</table>

2	Control de acceso a los dispositivos gestionados	- El administrador de la red es el único que puede acceder a los equipos con las contraseñas creadas de forma local o remota.	Jefe de operaciones
3	Control de acceso a usuarios	- Solo el administrador de la red puede agregar o quitar usuarios, a la red o al sistema de gestión	Jefe de operaciones

FLUJOGRAMA:




Ingreso al sistema de monitoreo
Administrador de la red
Director TIC's
Usuarios con permiso de visualización de consola
Usuario y contraseña únicas
Supervisión de administrador de red
FIN

Capítulo 4

4. Análisis de factibilidad de la implementación del proyecto

En este capítulo se desarrollaron diferentes pruebas de funcionamiento y desempeño de la red. Además un análisis de factibilidad para determinar las ventajas obtenidas luego de la aplicación del proyecto.

4.1 Pruebas de funcionamiento

Con la finalidad de realizar las pruebas de funcionamiento se evaluó los resultados del monitoreo de la red en diferentes días y horarios del uso de la misma, así como las alertas que podrían enviarse cuando uno de los dispositivos entraban en un estado de advertencia o crítico.

4.1.1 Topologías del monitoreo de la red

Esta es una herramienta brindada por el Software Pandora FMS la cual permite observar la topología de los equipos y servicios que están siendo monitoreados, esto es de suma importancia ya que permite ver el estado en que se encuentran los mismos.

Para hacer uso de esta herramienta se debe escoger en el Menú Monitoring la opción Network View en la Consola de Pandora como se muestra en la Figura 57.

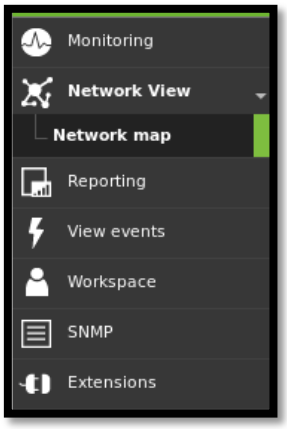


Figura 57. Opción Network View
Fuente: Consola Pandora FMS

Como se observa en la Figura 58 dentro de esta opción se puede crear la topología de acuerdo a las necesidades que se necesite visualizar.

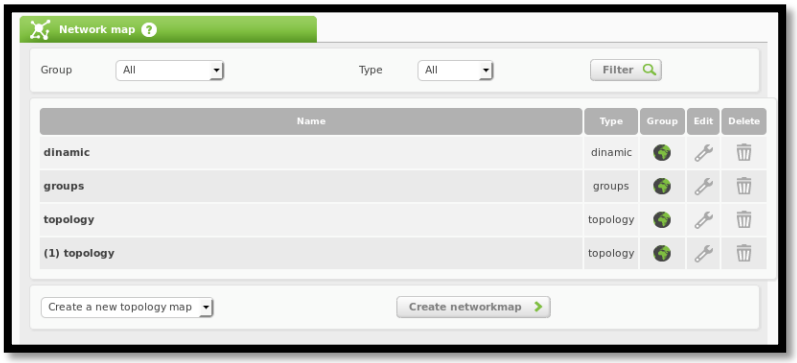


Figura 58. Ventana para crear Topologías de la Red
Fuente: Consola Pandora FMS

Para el caso de la Prefectura de la red se realizó la topología de la red principal con los equipos monitoreados como se observa en la Figura 59, aquí se puede observar cada uno de los dispositivos de red y servidores que estan siendo monitoreados.

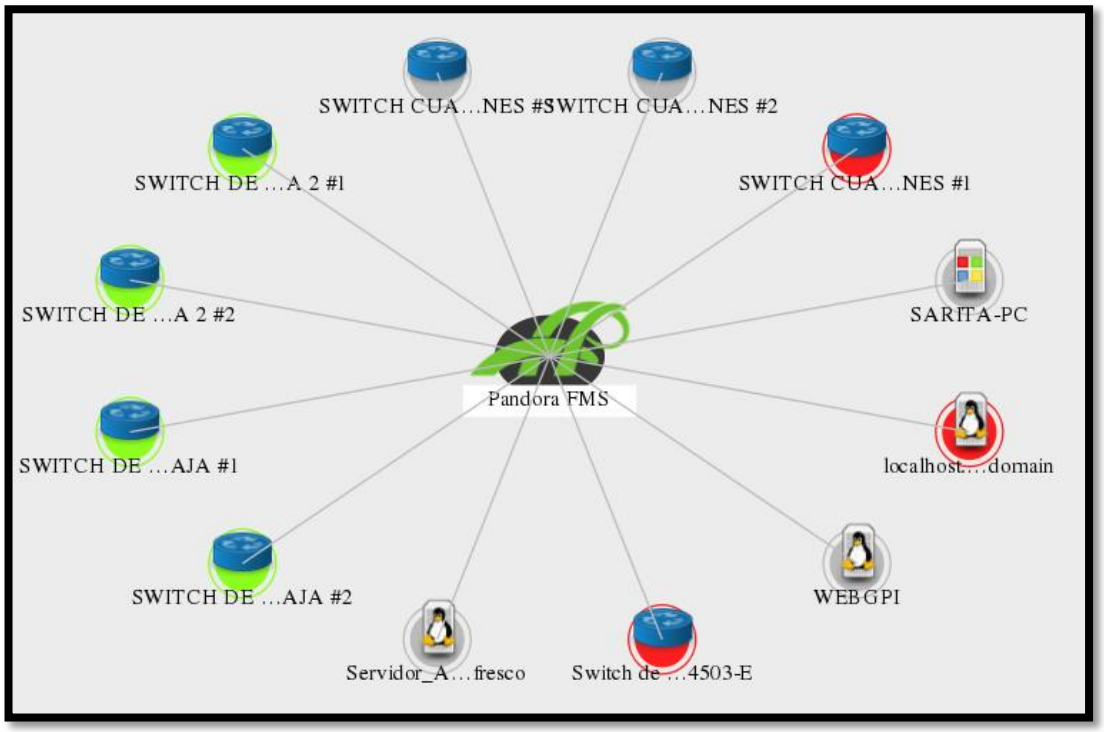


Figura 59. Topología General de la Red

Fuente: Consola Pandora FMS

En la Figura 60 se muestra la topología de equipos y servicios monitoreados en toda la red. Dentro de esta imagen se puede observar el estado de los módulos creados para el monitoreo, los cuales están definidos por colores como se indicó en el manual de procedimientos en la sección 3.3.2.

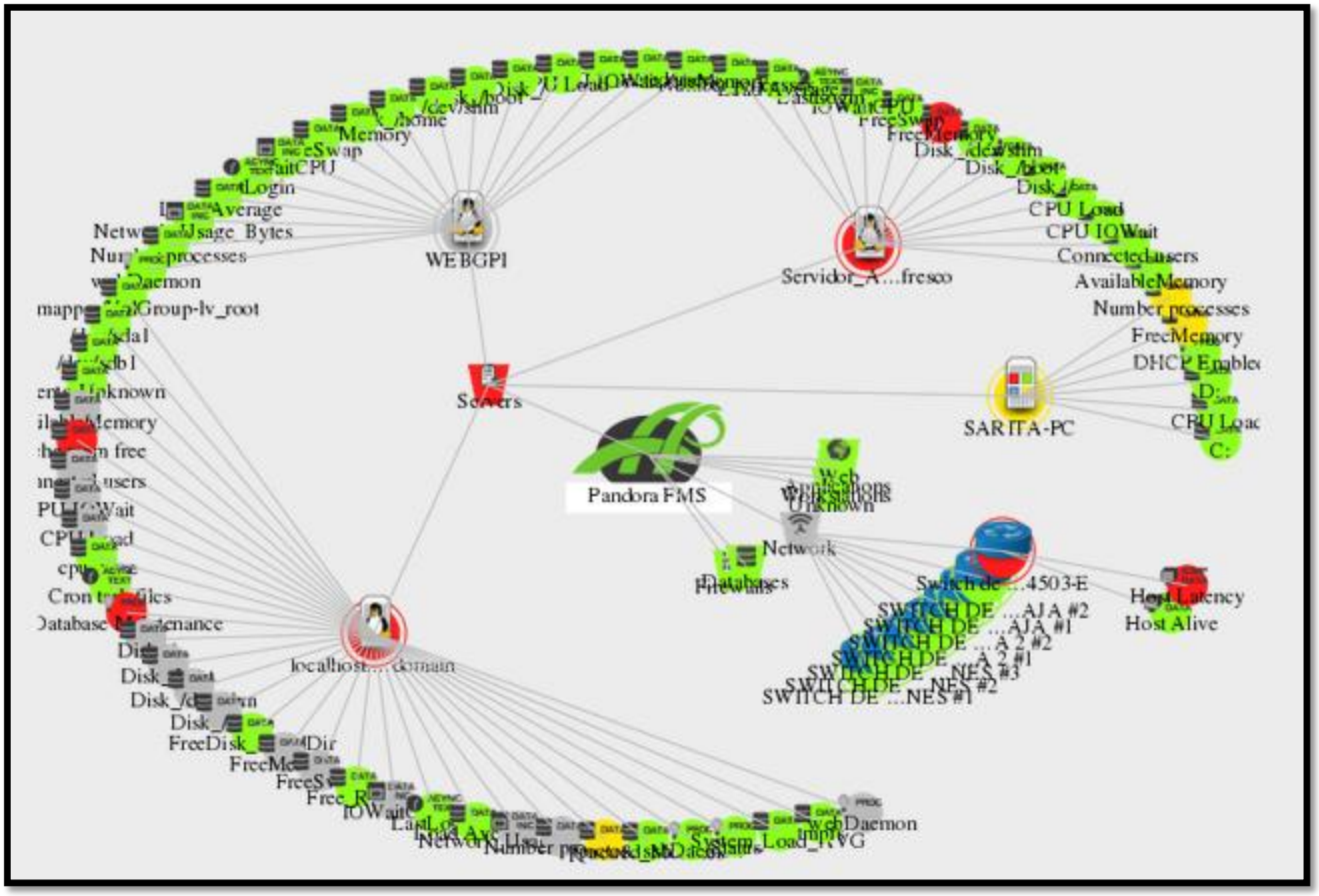


Figura 60. Topología de Servicios Monitoreados

Fuente: Consola Pandora FMS

Para poder observar los servicios monitoreados se creó una topología en grupos, en la Figura 61, 62, 63 y 64 se muestran los equipos de red monitoreados por cada planta del edificio, con cada uno de los módulos activados para el monitoreo.

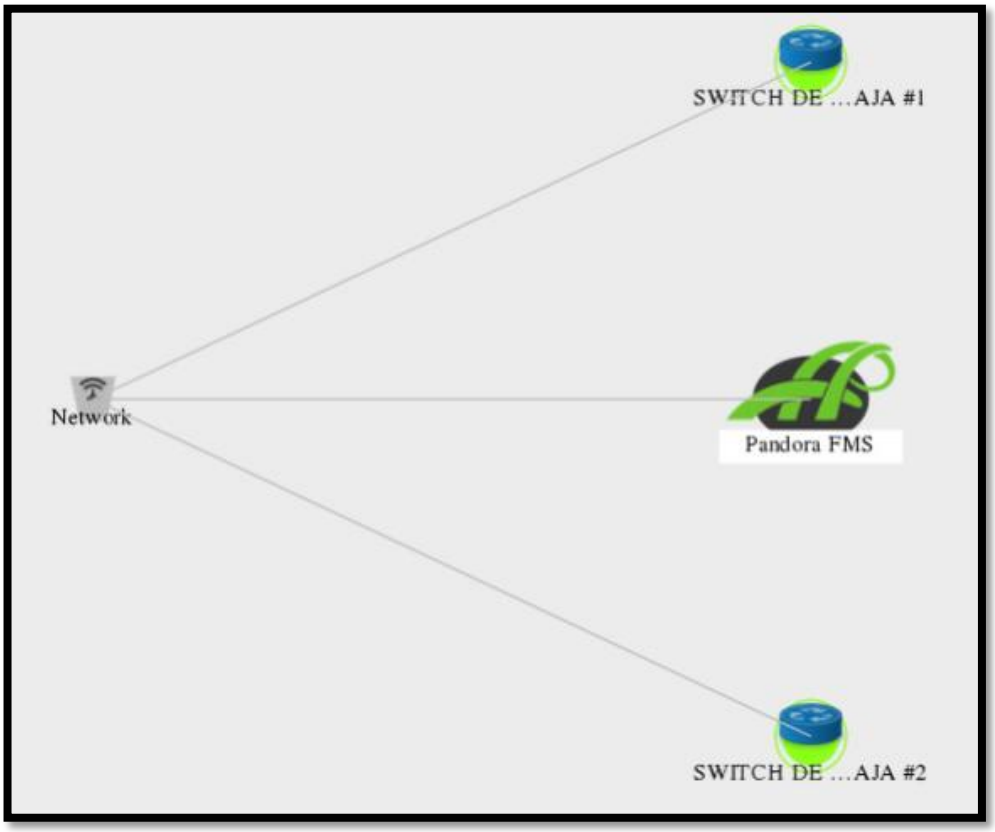


Figura 61. Equipos de Red Monitoreados Planta Baja

Fuente: Consola Pandora FMS

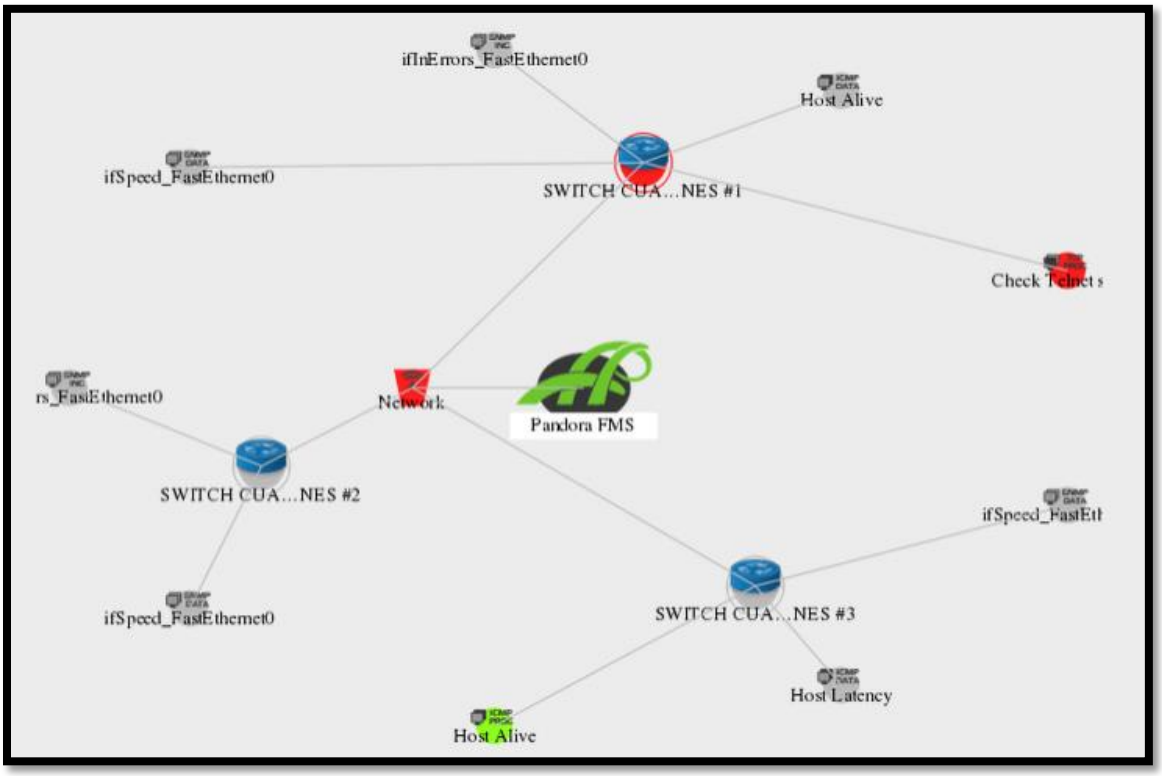


Figura 62. Equipos de Red Monitoreados Planta Alta 1

Fuente: Consola Pandora FMS

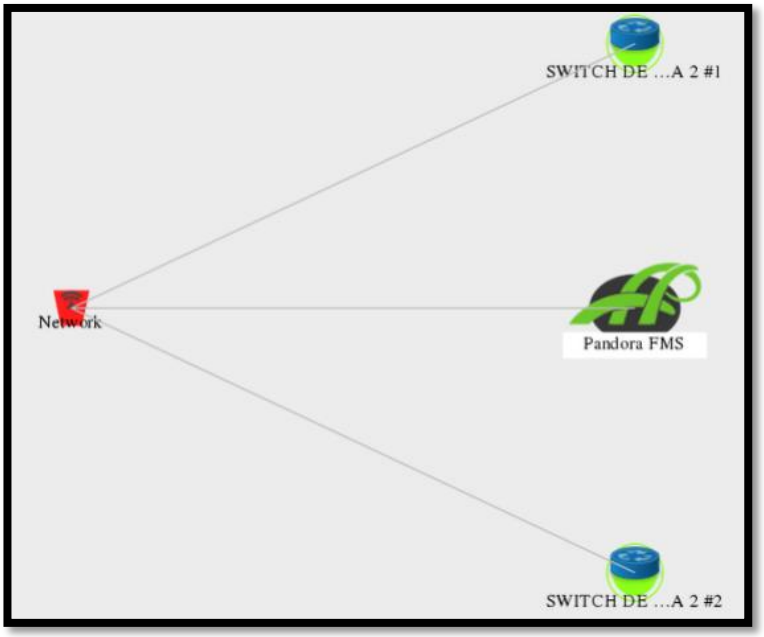


Figura 63. Equipos de Red Monitoreados Planta Alta 1

Fuente: Consola Pandora FMS

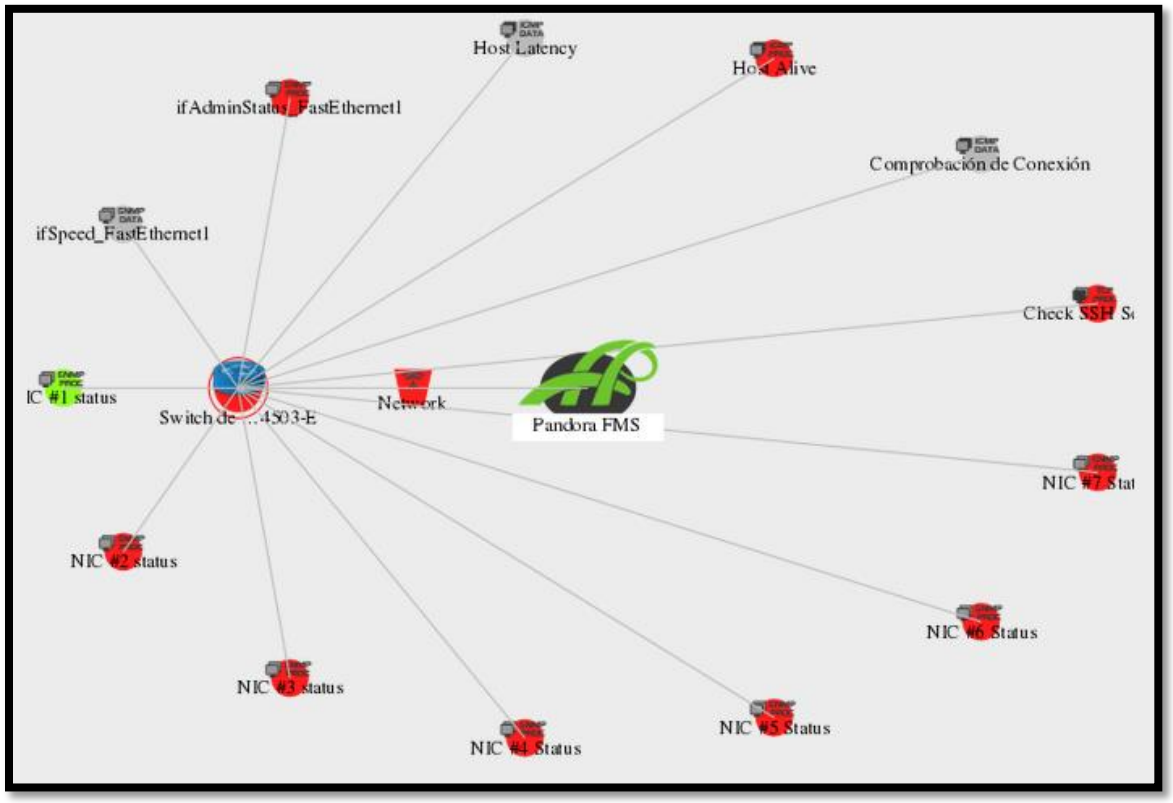


Figura 64. Equipos de Red Monitoreados (SWITCH DE CORE)

Fuente: Consola Pandora FMS

En la Figura 65 se indica la topología del monitoreo de los servidores. Dentro de la cual se puede ver los módulos creados para el monitoreo, al momento de la captura el Servidor Web tenía todos sus modulos en estado normal, pero el servidor Alfresco genero una alerta crítica debido a que la cantidad de memoria libre llegó a un umbral del 90% esto debido a que este servidor maneja todos los archivos ingresados a la Prefectura de Imbabura, para esto el administrador realizó un respaldo de la información almacenada.

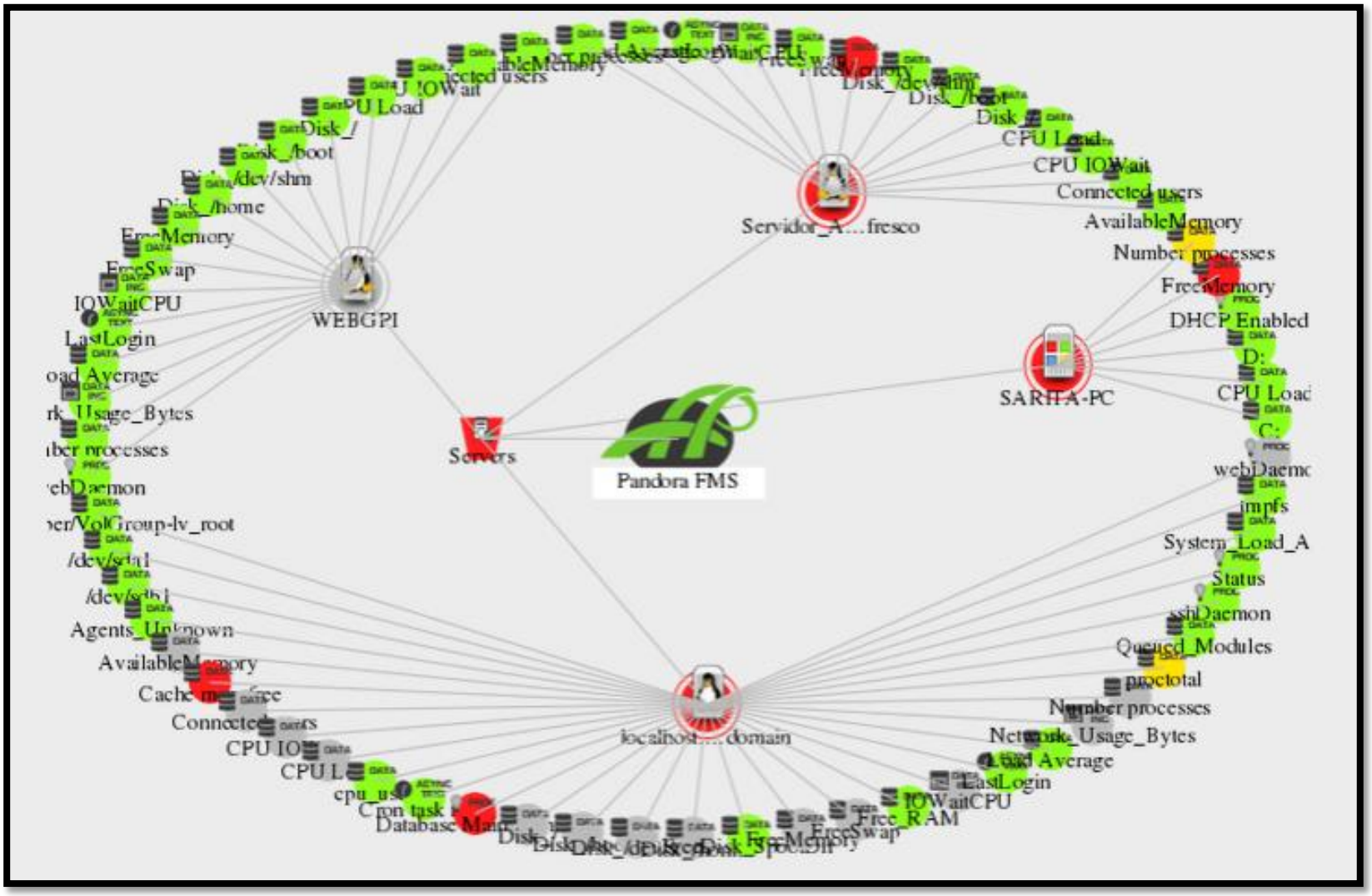


Figura 65. Servidores Monitoreados

Fuente: Consola Pandora FMS

4.1.2 Análisis de monitoreo switch de CORE

Pandora FMS permite al administrador visualizar en su consola el nombre del dispositivo gestionado, servicio que esta monitoreando, estado, tiempo de chequeo, duración y la información del servicio en tiempo real, como se muestra en la Figura 66.

Figura 66. Estado en tiempo real del Switch de CORE

Fuente: Consola Pandora FMS

La comprobación de conexión, latencia y host alive del Switch CORE no superan el pico de utilización durante el periodo de monitoreo por lo que se deduce que el dimensionamiento de los equipos de la red se ajustan a las necesidades que presenta la infraestructura de red, esto se muestra en las Figuras 67, 68 y 69.

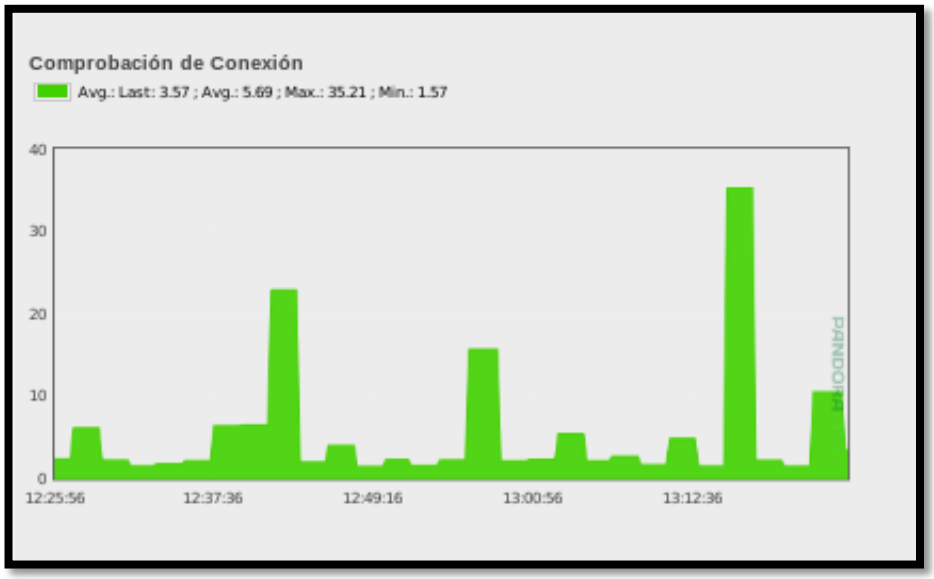


Figura 67. Comprobación de Conexión Switch de CORE

Fuente: Consola Pandora FMS

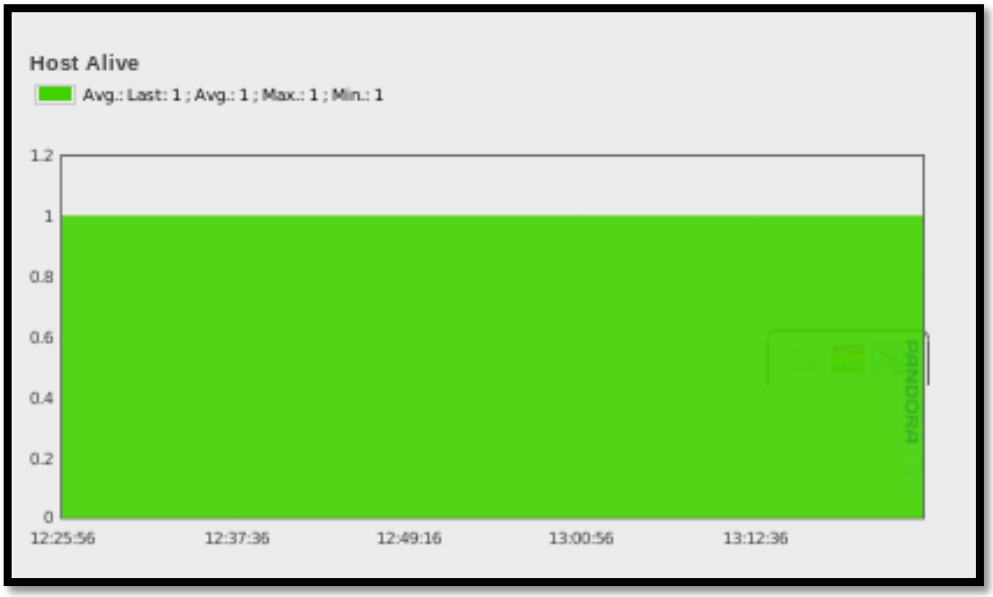


Figura 68. Host Alive Switch de CORE

Fuente: Consola Pandora FMS

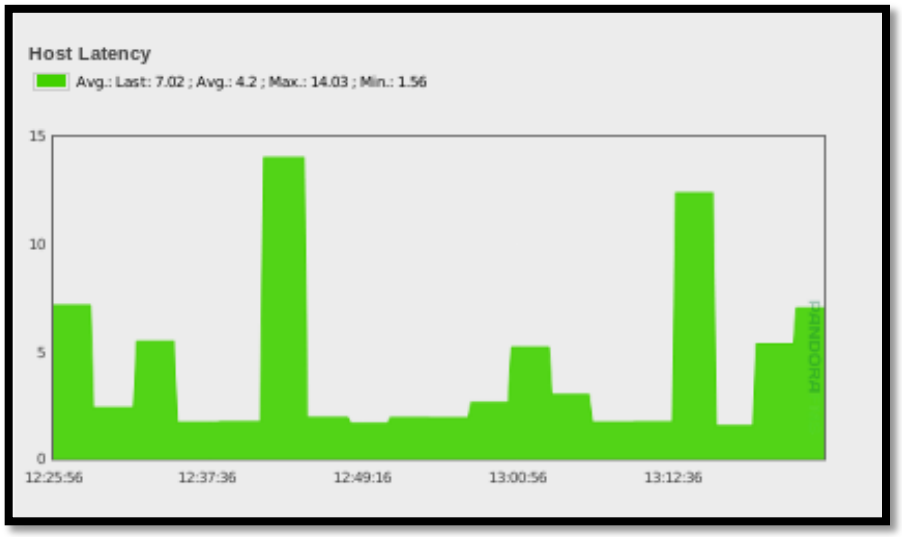


Figura 69. Latencia Switch de CORE

Fuente: Consola Pandora FMS

Además Pandora FMS permite visualizar mediante gráficos el rendimiento de cada interfaz de los enlaces críticos de la red local de datos de la Prefectura de Imbabura. En la Figura 70 se puede observar el ancho de banda consumido y el estado de conexión de una interfaz de red.

Figura 70. Estado de Interfaz de red del Switch de CORE

Fuente: Consola Pandora FMS

La velocidad de transmisión que manejan los enlaces de la red de la institución son de tipo Gigabit-Ethernet para la capa de distribución por esta razón el ancho de banda que ocupe la red no provoca una saturación de enlaces o cuellos de botella, a pesar de esto Pandora FMS permite configurar alertas en caso de que se sobrepase el consumo de ancho de banda normal.

4.1.3 Análisis de monitoreo switch de acceso 2960

4.1.3.1 Switch de acceso #1

En la Figura 71 se muestra el estado del monitoreo del Switch de Acceso #1 ubicado en el cuarto de comunicaciones.

Figura 71. Estado en tiempo real del Switch de Acceso #1
Fuente: Consola Pandora FMS

La comprobación de conexión, host alive y latencia del Switch de Acceso #1 no superan el pico de utilización durante el periodo de monitoreo por lo que estos parametros se ajustan a las necesidades que presenta la infraestructura de red, esto se muestra en las Figuras 72 y 73.

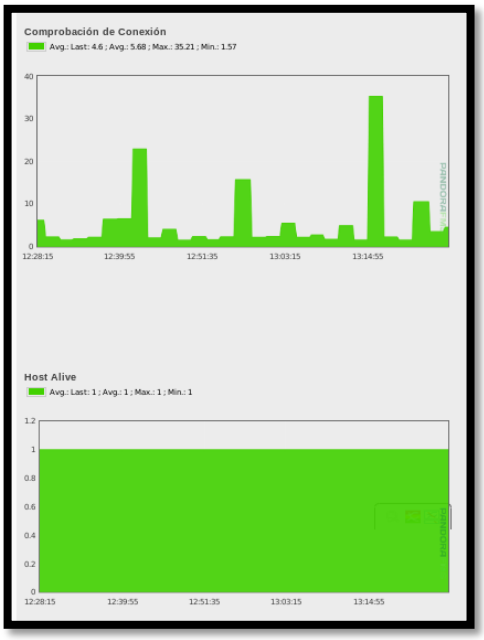


Figura 72. Comprobación de Conexión y Host Alive Switch de Acceso #1

Fuente: Consola Pandora FMS

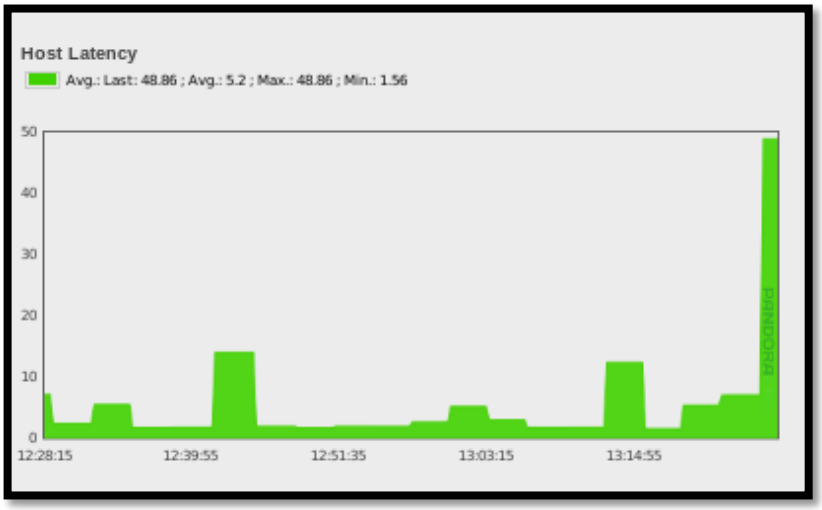


Figura 73. Latencia Switch de Acceso #1

Fuente: Consola Pandora FMS

En cuanto a los gráficos el rendimiento de cada interfaz de los enlaces críticos de la red,. en la Figura 74 y 75 se puede observar el ancho de banda consumido y el estado de conexión de una interfaz de red.

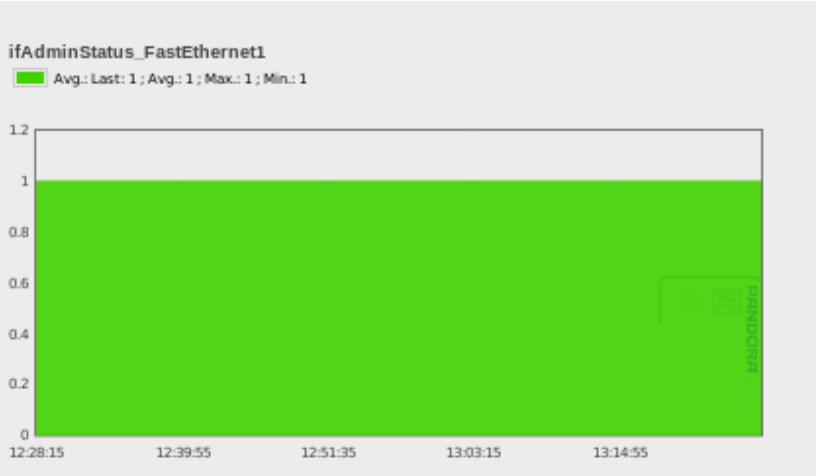


Figura 74. Estado de Interfaz de red del Switch de Acceso #1

Fuente: Consola Pandora FMS

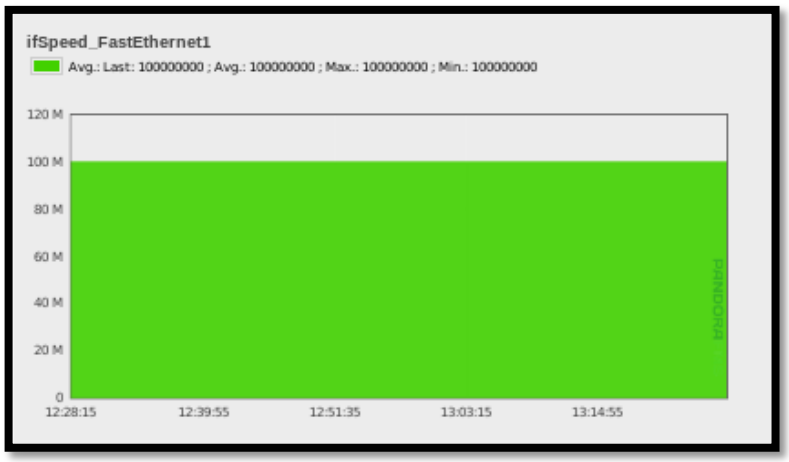


Figura 75. Estado de Interfaz de red del Switch de Acceso #1

Fuente: Consola Pandora FMS

4.1.3.2 Switch de acceso #2

En la Figura 76 se muestra el estado del monitoreo del Switch de Acceso #2 ubicado en el cuarto de comunicaciones.

Figura 76. Estado en tiempo real del Switch de Acceso #2

Fuente: Consola Pandora FMS

La comprobación de host alive y latencia del Switch de Acceso #2 no superan el pico de utilización durante el periodo de monitoreo por lo que estos parametros se ajustan a las necesidades que presenta la infraestructura de red, esto se muestra en las Figuras 77 y 78.

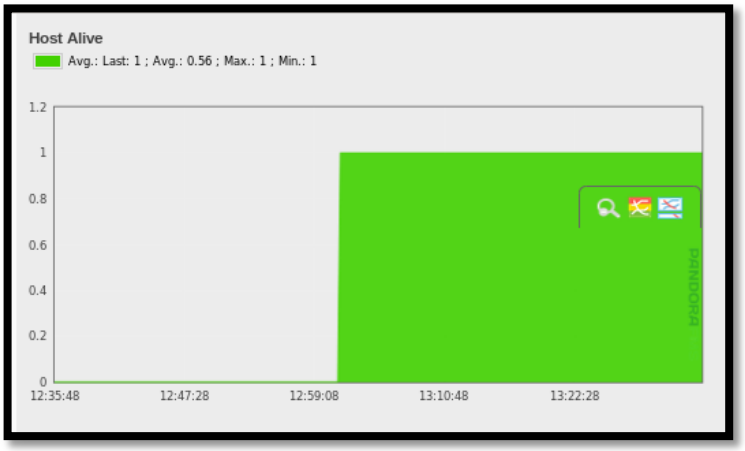


Figura 77. Comprobación Host Alive Switch de Acceso #2

Fuente: Consola Pandora FMS

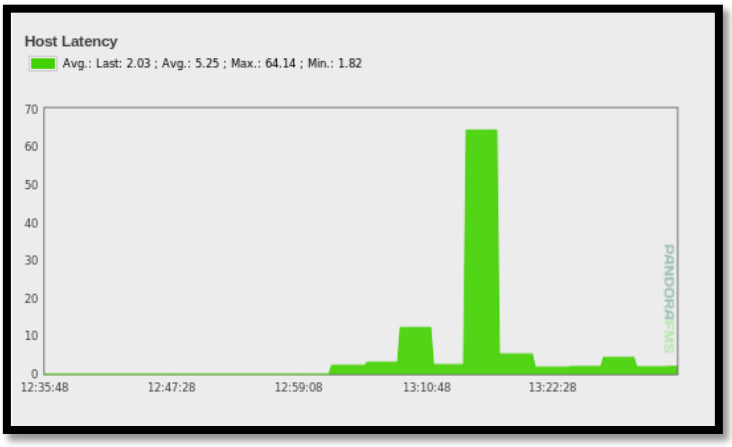


Figura 78. Latencia Switch de Acceso #2

Fuente: Consola Pandora FMS

En cuanto a los gráficos el rendimiento de cada interfaz de los enlaces críticos de la red,. en la Figura 79 se puede observar el ancho de banda consumido de una interfaz de red.

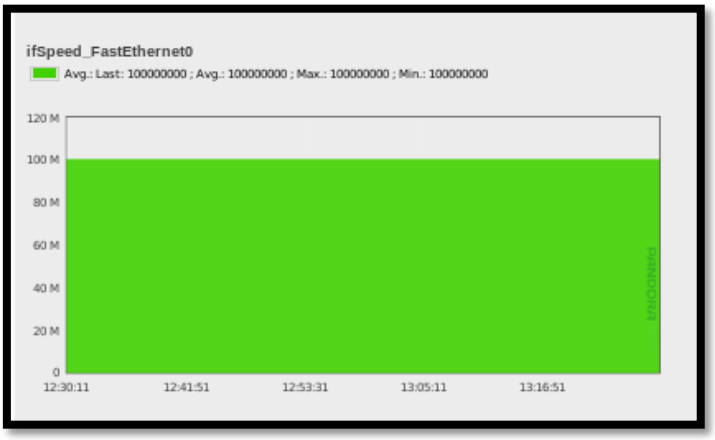


Figura 79. Estado de Interfaz de red del Switch de Acceso #1

Fuente: Consola Pandora FMS

4.1.4 Análisis de monitoreo servidor web

En la Figura 80 se muestra el estado del monitoreo del Servidor Web, además se puede observar todos los modulos configurados en la Figura 81.

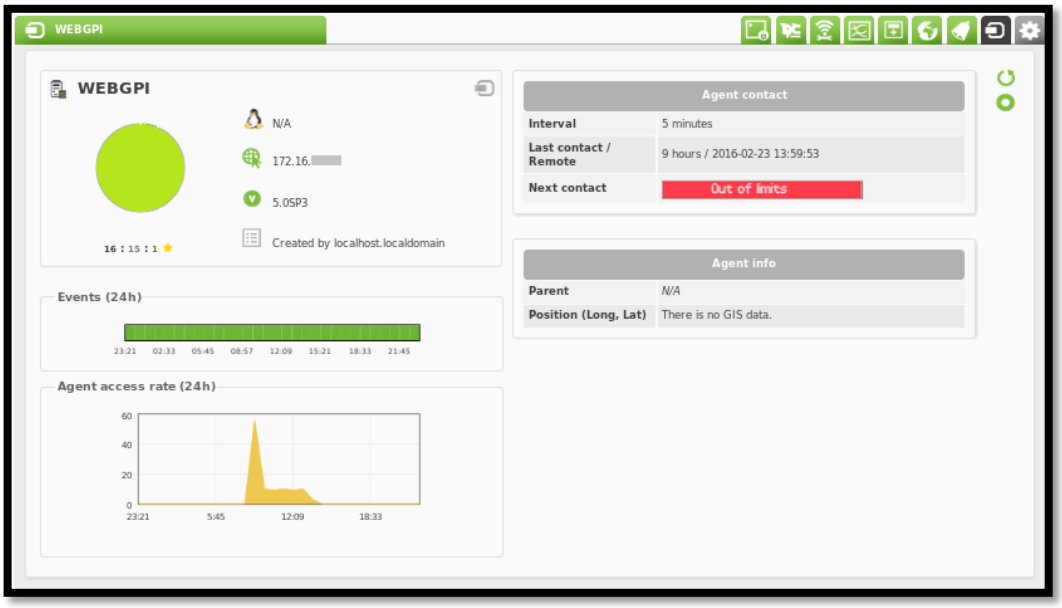


Figura 80. Estado en tiempo real del Servidor Web

Fuente: Consola Pandora FMS

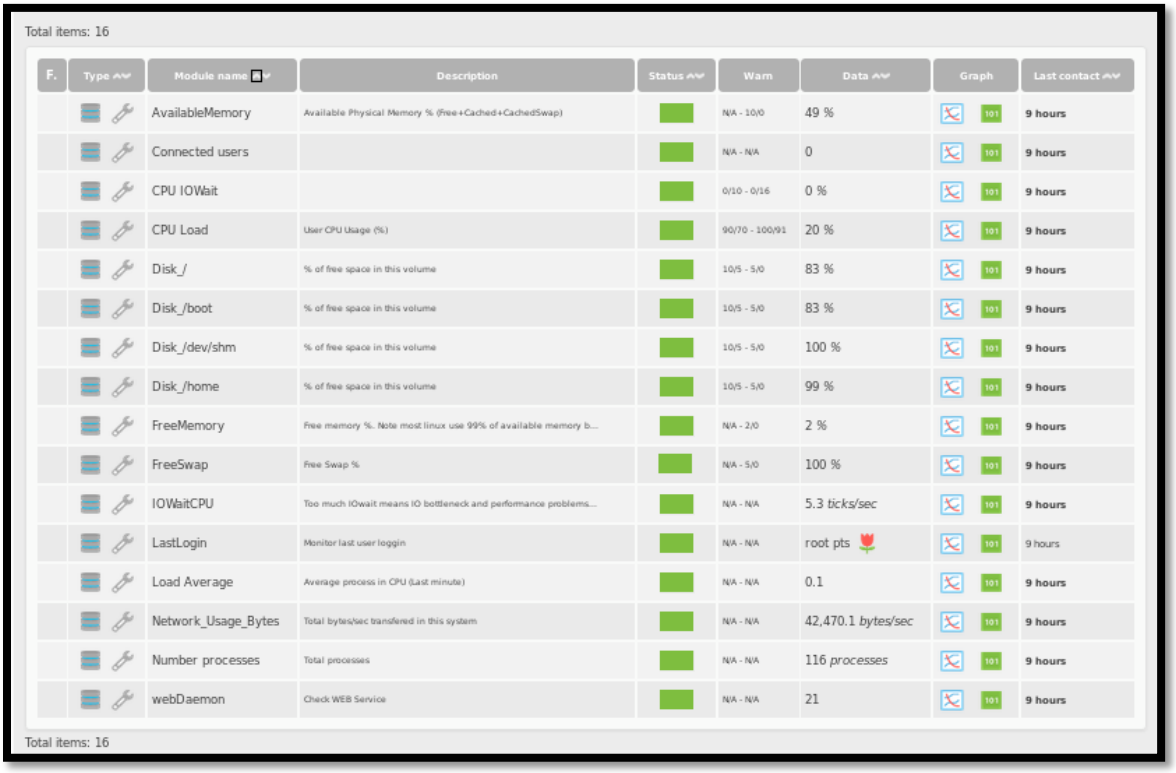


Figura 81. Módulos de monitoreo configurados en el Servidor Web

Fuente: Consola Pandora FMS

4.1.5 Análisis de monitoreo servidor de gestión de archivos

En la Figura 81 se muestra el estado del monitoreo del Servidor de Gestión de Archivos (Alfresco), además se puede observar todos los modulos configurados en la Figura 82.

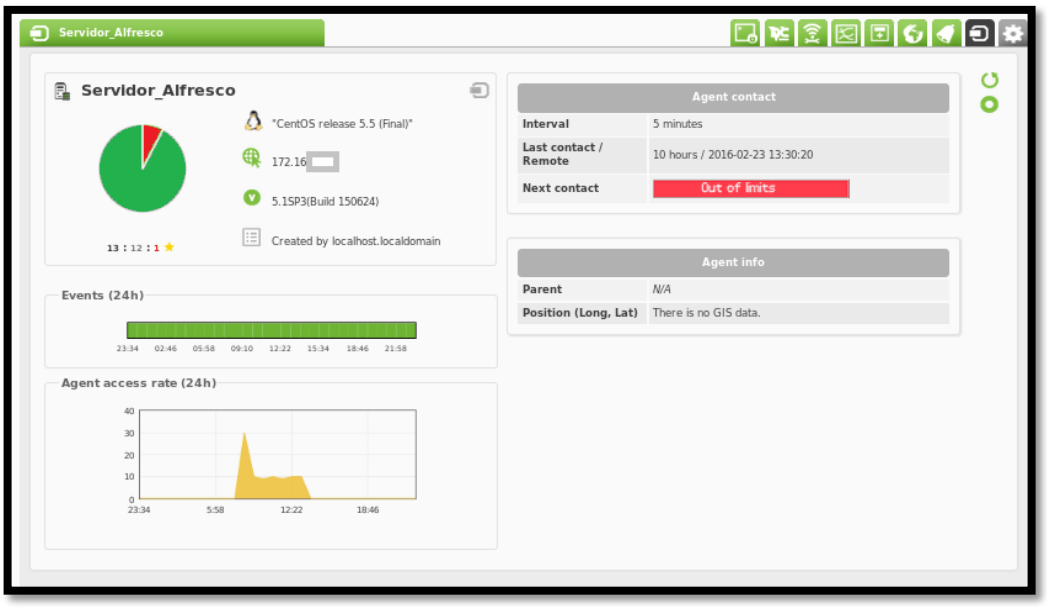


Figura 82. Estado en tiempo real del Servidor de Gestión de Archivos

Fuente: Consola Pandora FMS

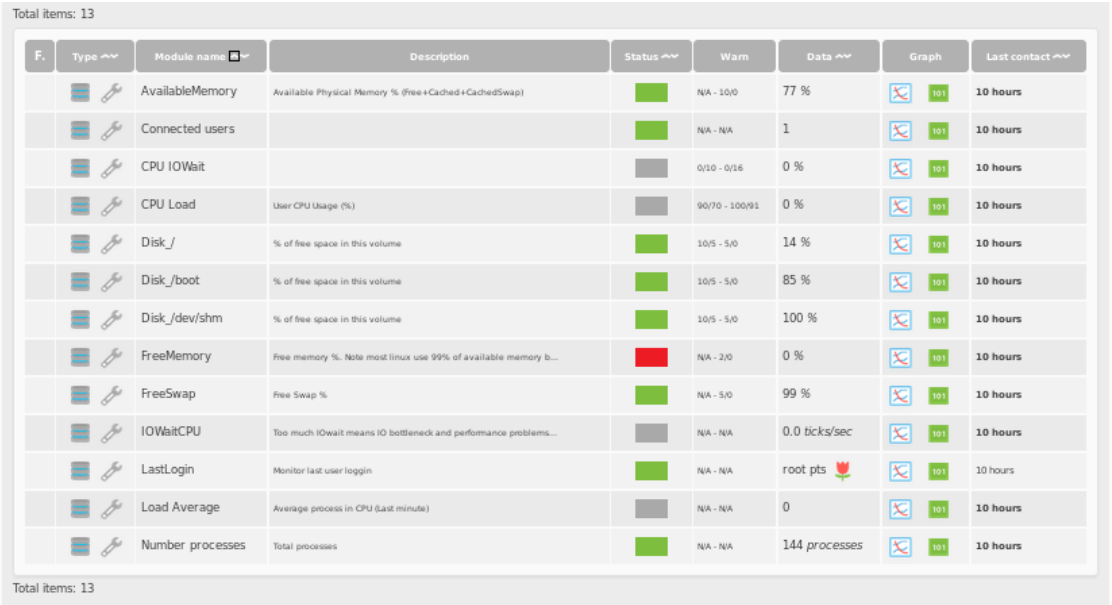


Figura 83. Módulos de monitoreo configurados en el Servidor de Gestión de Archivos

Fuente: Consola Pandora FMS

En este servidor se puede observar que se generó un estado crítico el cual se presenta en rojo y se refiere a la memoria libre del equipo, se advirtió al administrador de la red sobre este problema y libero el espacio en disco realizando un respaldo de los archivos subidos durante 3 meses, de esta manera se soluciona el problema de memoria disponible en el dispositivo.

4.2 Análisis de factibilidad técnico

Para determinar si el proyecto es factible, se debe realizó una serie de evaluaciones las cuales permiten establecer si el hardware, software y recurso humano con el que se cuenta, posee las capacidades técnicas necesarias para garantizar la viabilidad de la implementación del modelo de gestión ISO y el software Pandora FMS.

4.2.1 Recurso tecnológico y humano

El recurso tecnológico se evaluó en términos generales tomando en cuenta el hardware y software utilizado para la instalación del sistema de gestión.

Luego, el recurso humano se evaluado tomando en cuenta que el personal de la Prefectura de Imbabura, principalmente el administrador de la red cuenta con los conocimientos técnicos necesarios para desarrollar el proyecto propuesto.

4.2.1.1 Software necesario

En base al estudio realizado para el Software Pandora FMS, se pudo determinar que a pesar de existir las instalaciones del servidor tanto en tecnologías de licenciamiento libre y pagado, la mejor alternativa fue escoger el Software Libre en este caso el Sistema Operativo CentOS que es la mejor opción en cuanto a seguridad para el manejo de servidores, además la Prefectura de Imbabura utiliza este sistema en la mayoría de sus aplicaciones instaladas, después de una evaluación de los recursos requeridos por Pandora FMS se determinó que los programas a utilizar para un manejo correcto del programa son los siguientes:

- **Gestor de base de datos (MySQL)**

Este software proporciona un servidor de base de datos SQL (Structures Query Language) veloz, multihilo, multiusuario y robusto. El servidor está proyectado tanto para sistemas críticos en producción soportando cargas intensas de trabajo como para sistemas de desarrollo masivo de software. Tiene una licencia dual, es decir se puede utilizar de forma gratuita bajo licencia GNU, o con licencias comerciales. (Master Magazine, 2015)

Este software es importante para el servidor de monitoreo ya que Pandora FMS utiliza una base de datos MySQL, la cual se mantiene de forma asíncrona con todos los datos recogidos, realizando un enlace temporal de todo lo que recibe y normalizando todos los datos de las diversas fuentes 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 el servidor no requiera ningún tipo de administración de base de datos ni proceso manual asistido por un operador o administrador. Esto se realiza por medio de una purga periódica de los datos pasada una fecha (90 días de forma predeterminada), así como una compactación de los datos que tienen más de un número determinado y configurable de días de antigüedad (30 días de forma predeterminada). (Pandora FMS Enterprise, 2015)

- **Servidor web (Apache)**

Debido a que Pandora FMS es un sistema orientado a Web, se procedió a instalar el servidor Apache el cual es altamente configurable, admite bases de datos de autenticación y negociado de contenido, además permite montar un servidor web en cualquier equipo y casi cualquier sistema operativo.

4.2.1.2 Hardware necesario

Se determinó los requerimientos mínimos en hardware con los que debería contar el equipo para lograr un ambiente óptimo de desarrollo. Para esto el Director de la Dirección de Tecnologías de la Información de la Prefectura de Imbabura determinó que el Servidor Pandora FMS sea instalado en el equipo HP Proliant BL360 G6, las características del mismo fueron descritas en el Capitulo 2 del proyecto en la Tabla 6.

4.2.1.3 Recurso humano técnico

En cuanto al personal que maneja la red, la Dirección de TIC's de la Prefectura de Imbabura se encuentra organizada de la siguiente manera:

4.2.1.3.1 Director del departamento

Es el jefe de la Dirección de Tecnologías de la Información, bajo su jurisdicción está el manejo de las areas de infraestructura y de software.

4.2.1.3.2 Jefe de operaciones

Es la persona encargada de ver el estado de la red, y asegurar su disponibilidad, mantenimiento y rendimiento, tiene bajo su dirigencia dos Ingenieros en Infraestructura.

4.2.1.3.3 Ingeniero de infraestructura

Se encarga del correcto funcionamiento del cuarto de comunicaciones.

Luego de haber descrito la estructura organizacional del área de Infraestructura se puede determinar que cada una de las personas que lo conforman tienen el conocimiento adecuado para realizar el manejo del sistema de gestión, además debido a esta estructura administrativa cada uno tiene funciones a cumplir, es decir todo se realiza de manera organizada.

4.2.2 Evaluación final

Al culminar el estudio de factibilidad técnica se establece que la Prefectura de Imbabura cuenta con todos los parametros necesarios para la utilización del software de gestión propuesto, además este cumple a cabalidad las expectativas planteadas por el personal de la Dirección de Tecnologías de las Información tal como se pudo mostrar en las pruebas de funcionamiento realizadas al sistema.

Capítulo 5

5.1 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 tomo en cuenta que las notificaciones que tienen mayor prioridad son las de el 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 criticas.

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.

5.2 Recomendaciones

La Prefectura de Imbabura al ser una entidad pública que brinda servicios a la ciudadanía, debe mantener una alta disponibilidad en cuanto a su conexión a internet, por lo que se recomienda utilizar el sistema de monitoreo y gestión para garantizar que este servicio no se pierda y si existe algún error solucionarlo de la manera más eficaz.

Para la gestión de configuraciones, es importante mantener actualizados los sistemas operativos que se manejan en los dispositivos de la institución de esta manera se garantizará que el Software instalado no genere errores por falta de actualizacion de ciertos paquetes.

La gestión de fallos es de suma importancia para el manejo correcto de una red, por lo que se recomienda al personal que administra la red, revise de manera constante los fallos que puedan producirse y no ignore los correos electrónicos de notificación de los problemas.

En cuanto a la gestión de contabilidad, se recomienda que cualquier modificación al software o incremento de equipos en el mismo sean documentados y guardados para tener un historial de los cambios que se puedan producir a futuro en la red.

Para un correcto manejo de la gestión de prestaciones, es necesario que las personas responsables de la red utilicen el manual de administrador y las politicas de gestión entregadas en la Dirección de TIC’s, ya que este permitirá manejar de manera adecuada tanto los equipos como el software de gestión.

Pandora FMS tambien brinda una plataforma de monitoreo para dispositivos moviles, tales como teléfonos o tablets, por lo que se recomienda que si el administrador de la red cree necesario utilizar este servicio este sea ocupado solamente por el y que ninguna otra persona tenga acceso a este dispositivo, esto por motivos de seguridady confidencialidad para el manejo de la red.

GLOSARIO DE TÉRMINOS

A

ANSI

American National Standards Institute. Es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos., 39

ASN.1

Abstract Syntax Notation One, fue desarrollado como parte de la capa 6 del modelo de referencia OSI. Esta notación proporciona un nivel de abstracción similar al ofrecido por lenguajes de programación de alto nivel., 27

C

CISCO

Es una empresa global con sede en San José (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones., 37

CMIP

Protocolo de administración de información común, es un protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red y la gerencia de los agentes., 12

CNT

Corporación Nacional de Telecomunicaciones CNT EP es la empresa pública de telecomunicaciones del Ecuador., 37

E

EGP

Es un protocolo estándar usado para intercambiar información de encaminamiento entre sistemas autónomos. Las puertas de enlace o pasarelas EGP solamente pueden retransmitir información de accesibilidad para las redes de su sistema autónomo (AS)., 29

EIA

Electronics Industry Alliance. Es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos, cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política., 39

H

HMAC

Código de autentificación de mensajes en clave-hash, es una construcción específica para calcular un código de autentificación de mensaje que implica una función hash criptográfica en combinación con una llave criptográfica secreta., 24

I

ICMP

Protocolo de mensajes de control de Internet, es un protocolo que permite administrar información relacionada con errores de los equipos en red., 28

IEEE

Es una organización sin ánimo de lucro, la mayor asociación del mundo para el desarrollo tecnológico. Su nombre completo es el Instituto de Ingenieros Eléctricos y Electrónicos, 4

IP

Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados. El IP no cuenta con la

BIBLIOGRAFÍA

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

ANEXO A. INSTALACIÓN DE CENTOS

- Ingresar en la página oficial de CentOS y descargar la versión que se necesite

Figura A 1. Página Oficial para descarga de CentOS

Fuente: https://www.centos.org/download/

- Luego de haber descargado el instalador, en la pantalla inicial de CentOS escoger la opción que mejor convenga al usuario

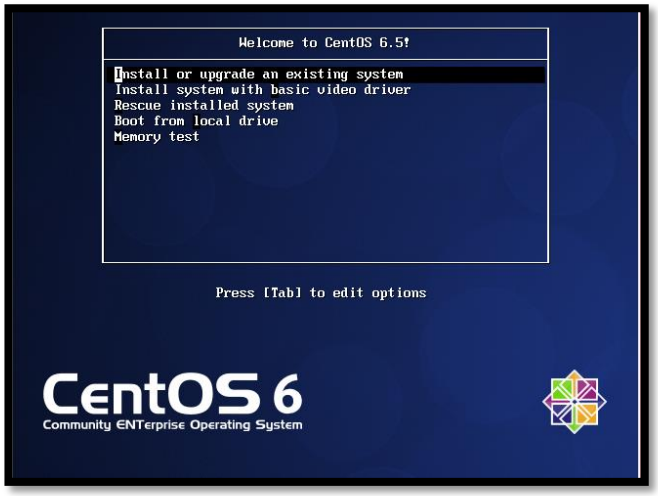


Figura A 2. Pantalla Inicial de CentOS

Fuente: CentOS

- En la opción Disco encontrado se debe escoger Skip

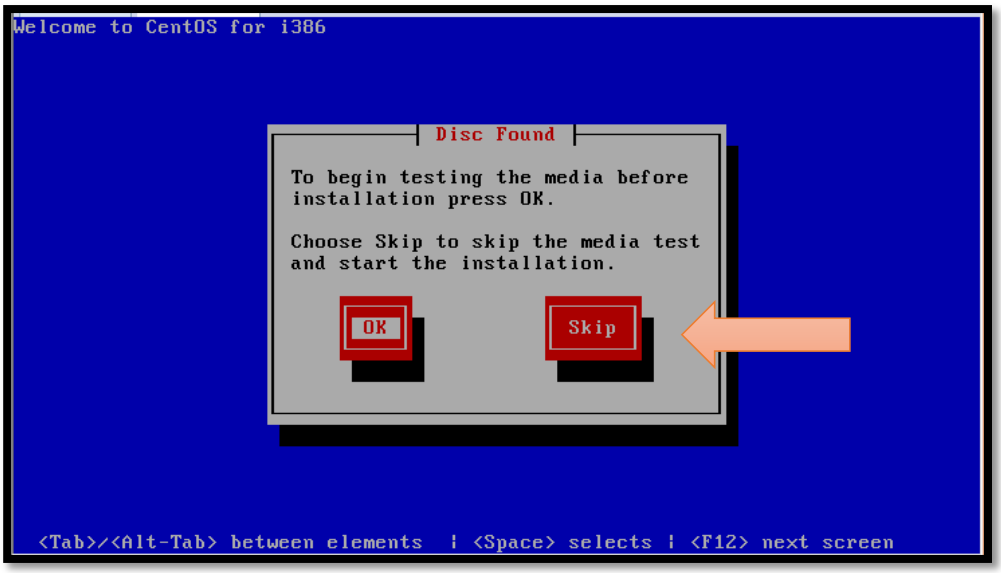


Figura A 3. Opción Disco Encontrado

Fuente: CentOS

- Aparece la pantalla de inicio de instalación de CentOS

Figura A 4. Inicio de Instalación de CentOS

Fuente: CentOS

- Escoger el idioma del sistema operativo

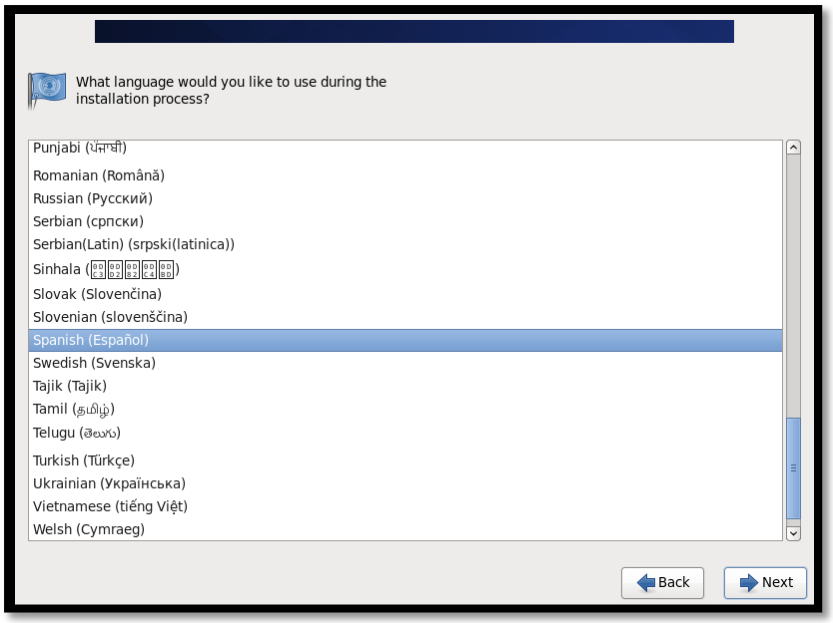


Figura A 5. Selección de Idioma

Fuente: CentOS

- Escoger el idioma del teclado

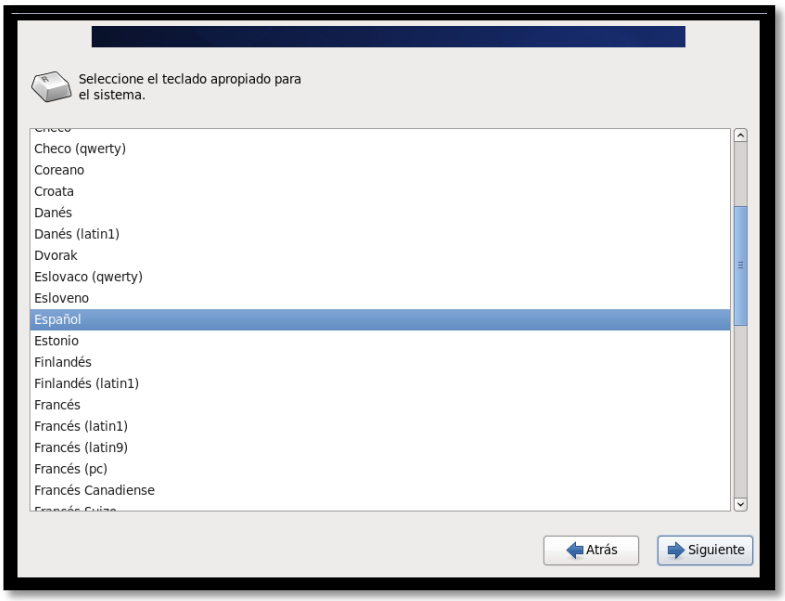


Figura A 6. Selección de Idioma del Teclado

Fuente: CentOS

- Escoger la opción para el dispositivos de almacenamiento básicos

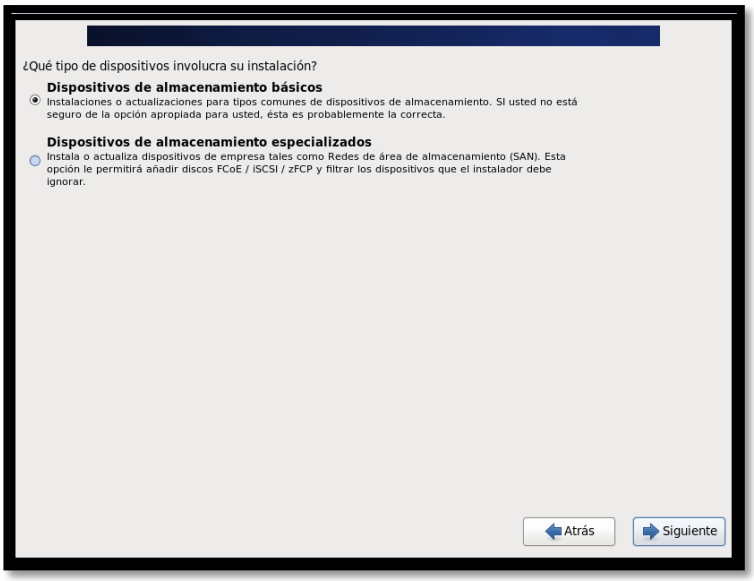


Figura A 7. Dispositivos de almacenamiento

Fuente: CentOS

- Asignar el nombre del host

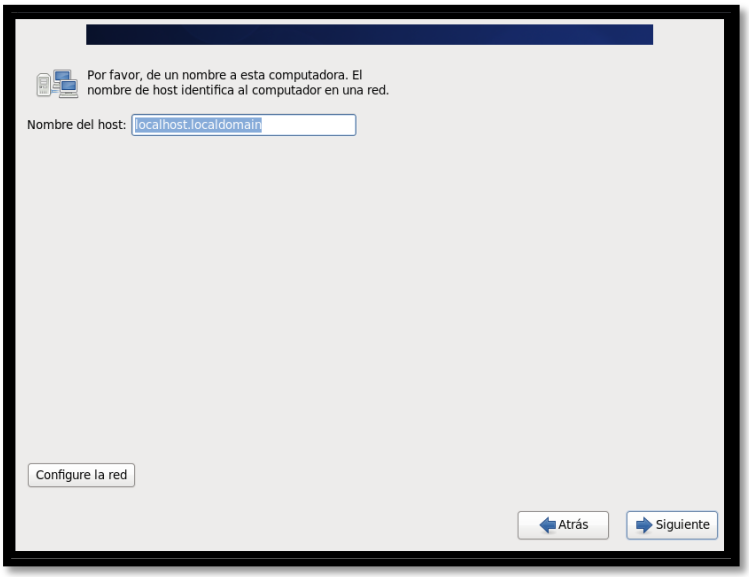


Figura A 8. Configuración Nombre del Host

Fuente: CentOS

- Se debe escoger la región en que se encuentra la PC para establecer la zona horaria

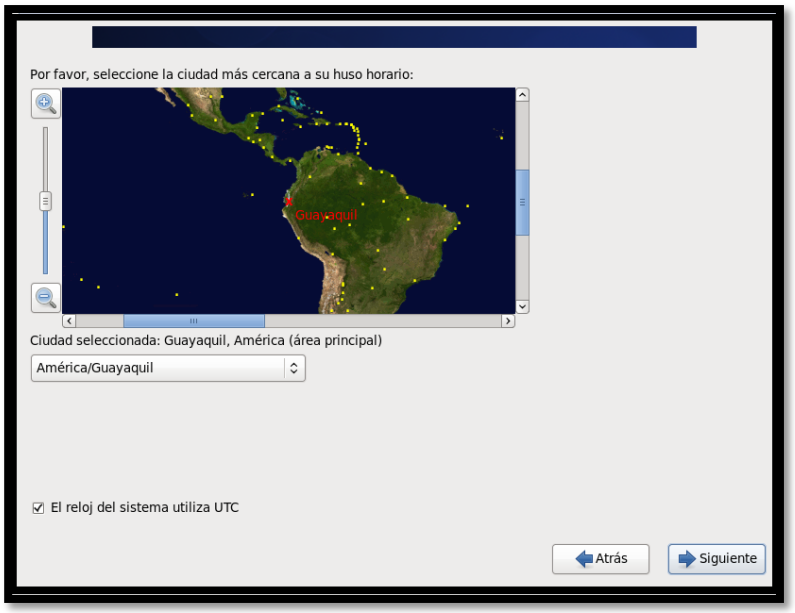


Figura A 9. Configuración de Región

Fuente: CentOS

- Escoger la contraseña para root

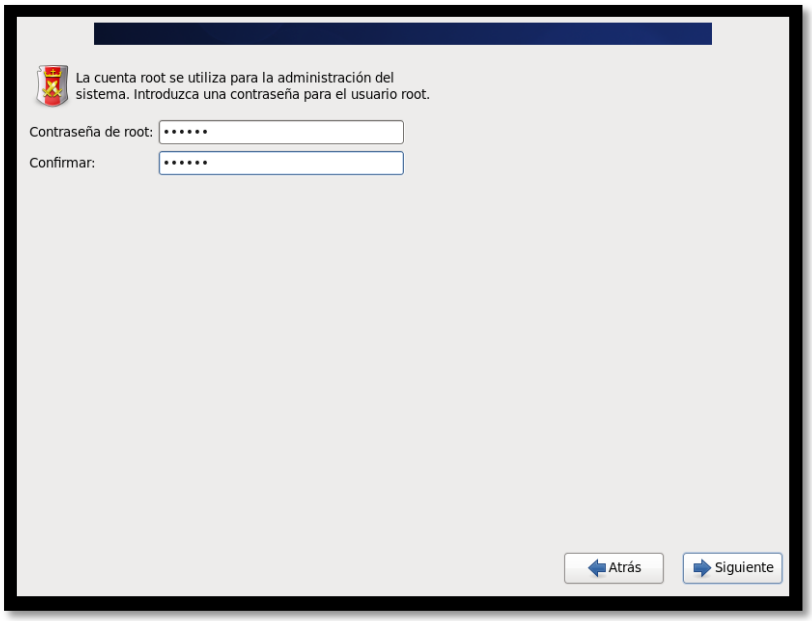


Figura A 10. Configuración de contraseña

Fuente: CentOS

- Escoger la opción de la forma en que se desee instalar

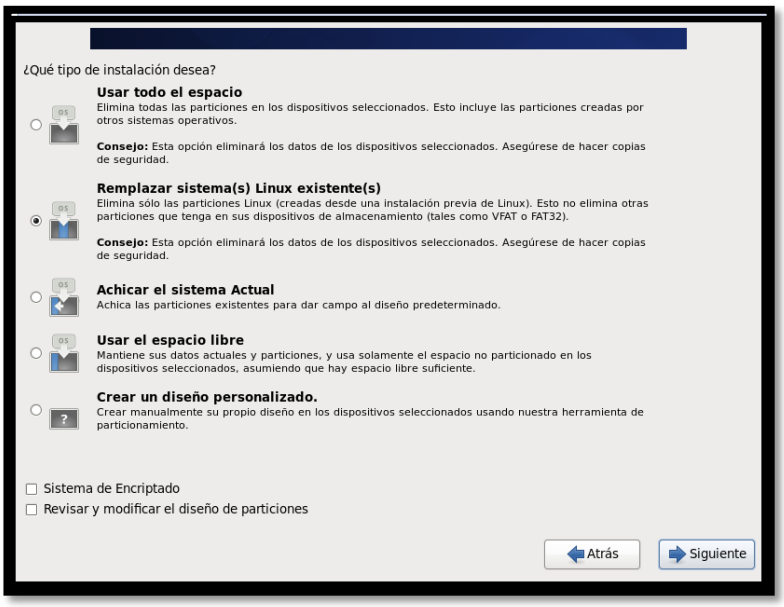


Figura A 11. Forma de Instalación

Fuente: CentOS

- Escoger la opción para cambiar los discos

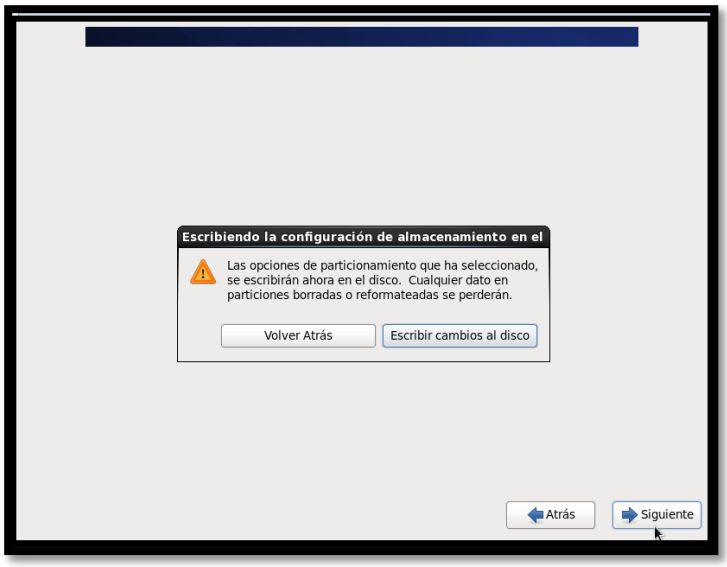


Figura A 12. Partición de Discos

Fuente: CentOS

- Escoger la opción de escritorio

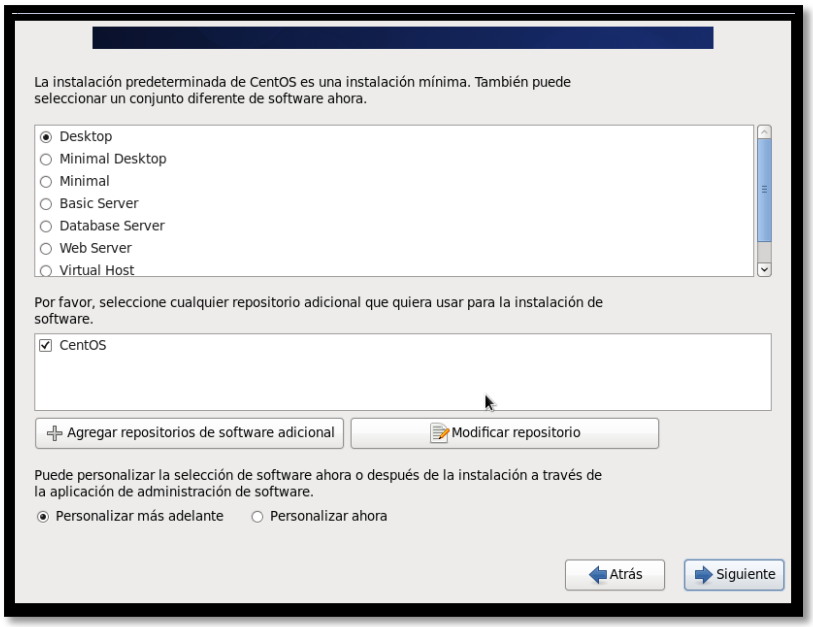


Figura A 13. Selección de software extra

Fuente: CentOS

- Esperar a que se descarguen todo los paquetes necesarios para la instalación

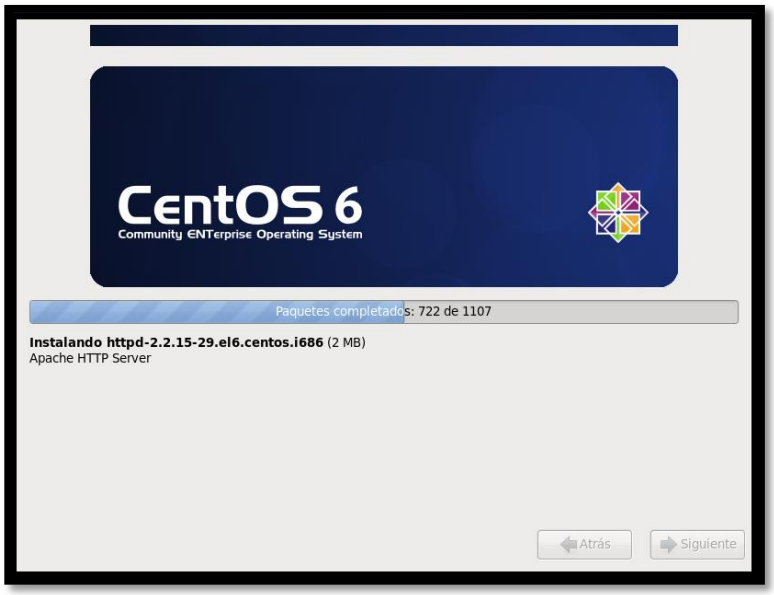


Figura A 14. Descarga e Instalación de Paquetes

Fuente: CentOS

- Finalizar la instalación

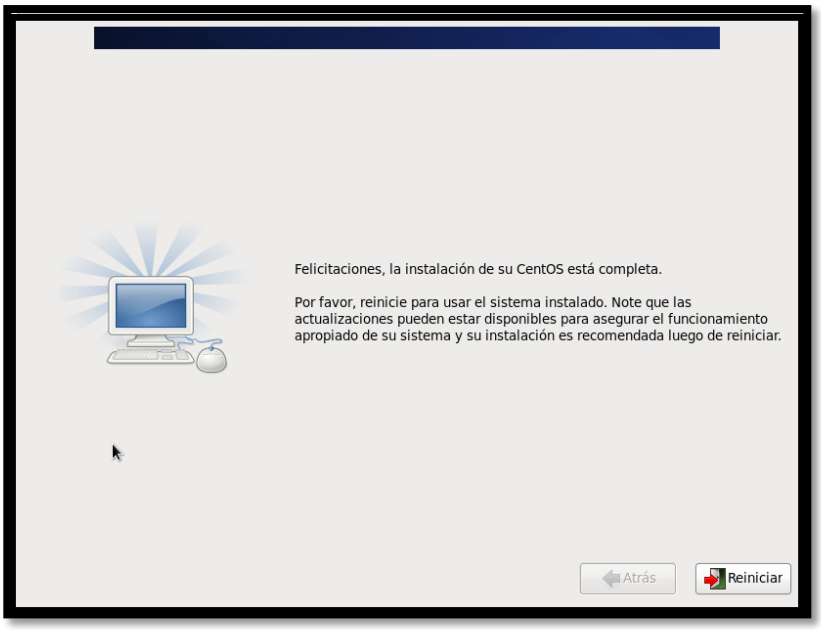


Figura A 15. Finalización de Instalación

Fuente: CentOS

- Configurar el inicio de sesión CentOS

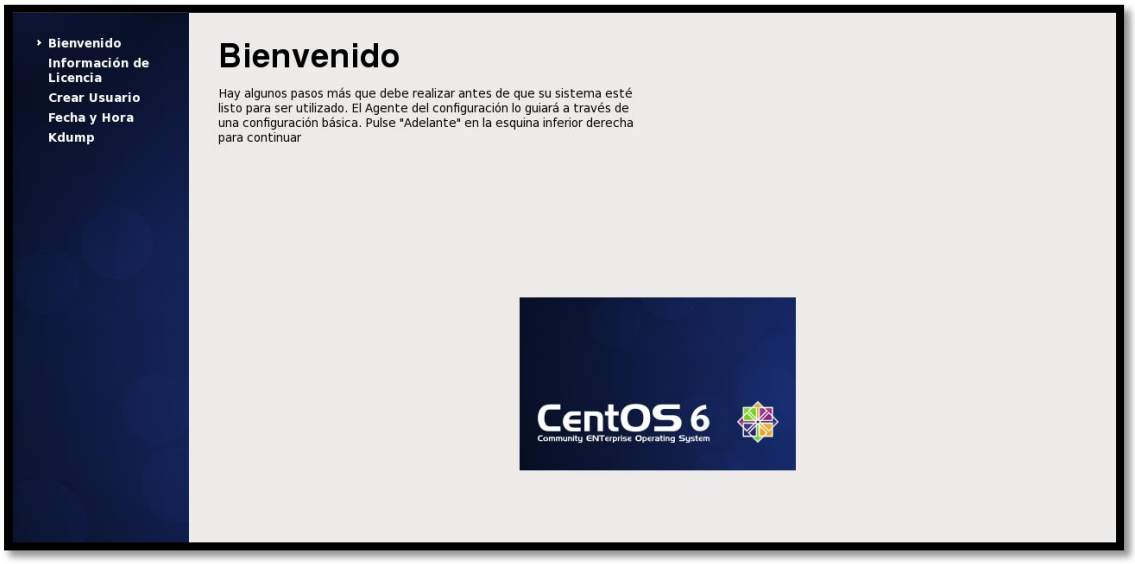


Figura A 16. Configuración Inicio de Sesión

Fuente: CentOS

- Aceptar el acuerdo de licencia

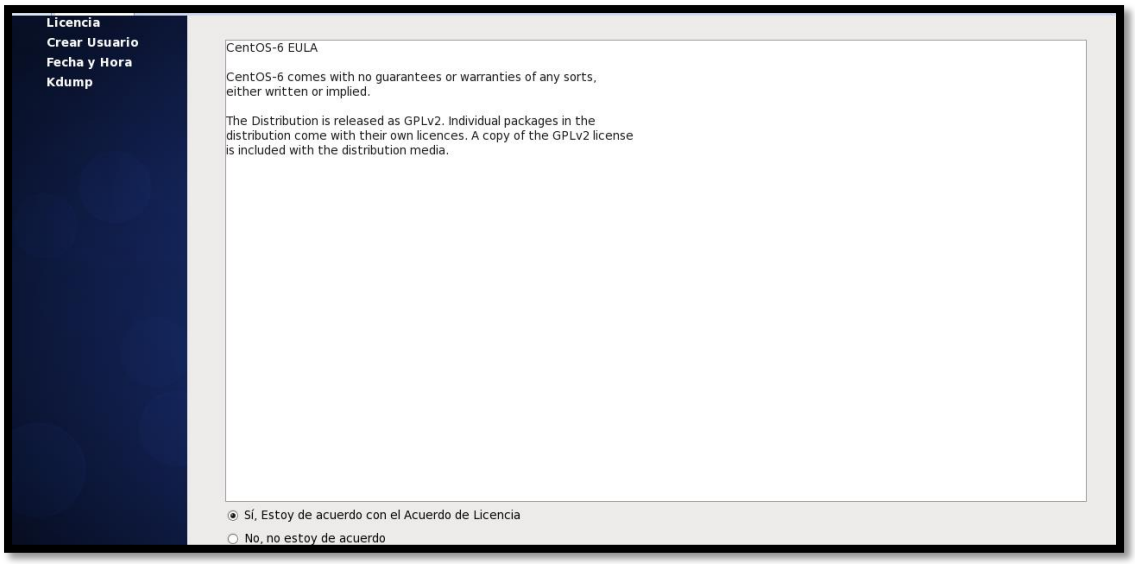


Figura A 17. Acuerdo de Licencia

Fuente: CentOS

- Si se desea se debe crear el usuario para inicio de sesión

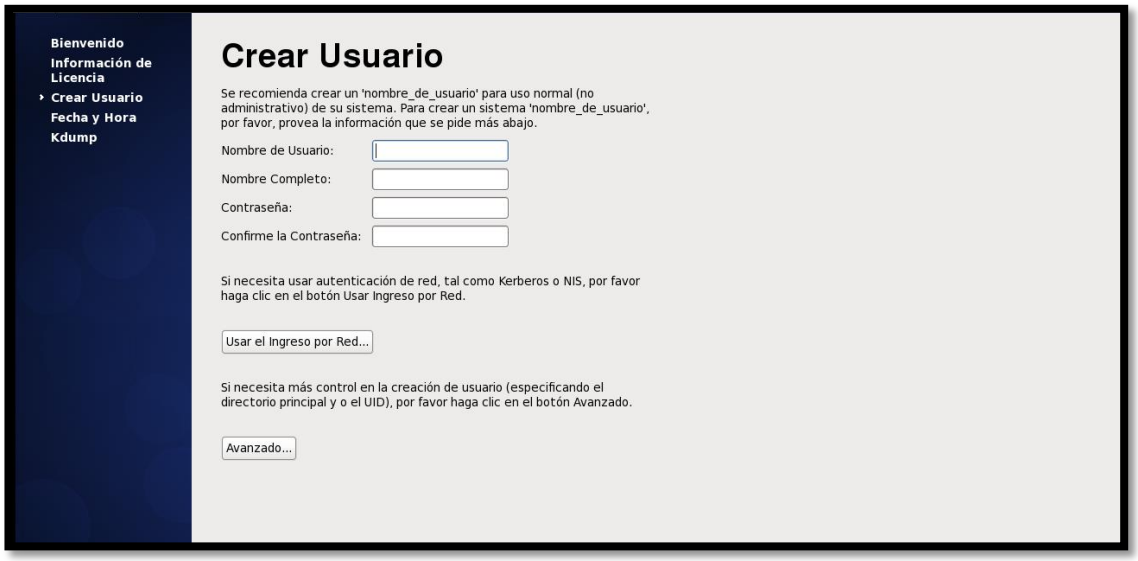


Figura A 18. Creación de Usuario

Fuente: CentOS

- Configurar la fecha y hora del sistema

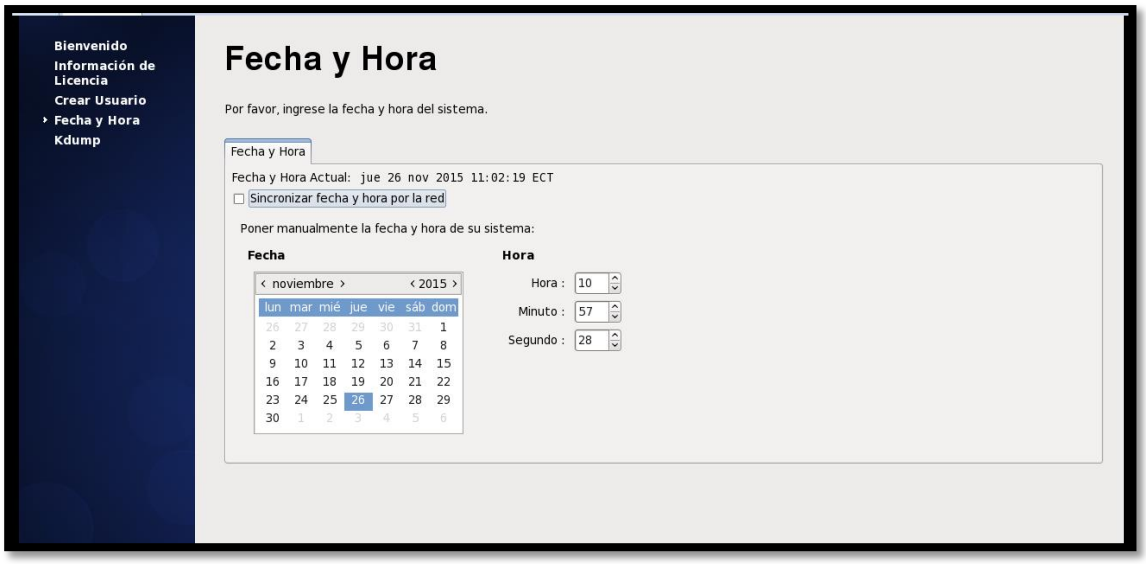


Figura A 19. Configuración de Fecha y Hora del Sistema

Fuente: CentOS

- Al finalizar la configuración, se puede ingresar al sistema operativo

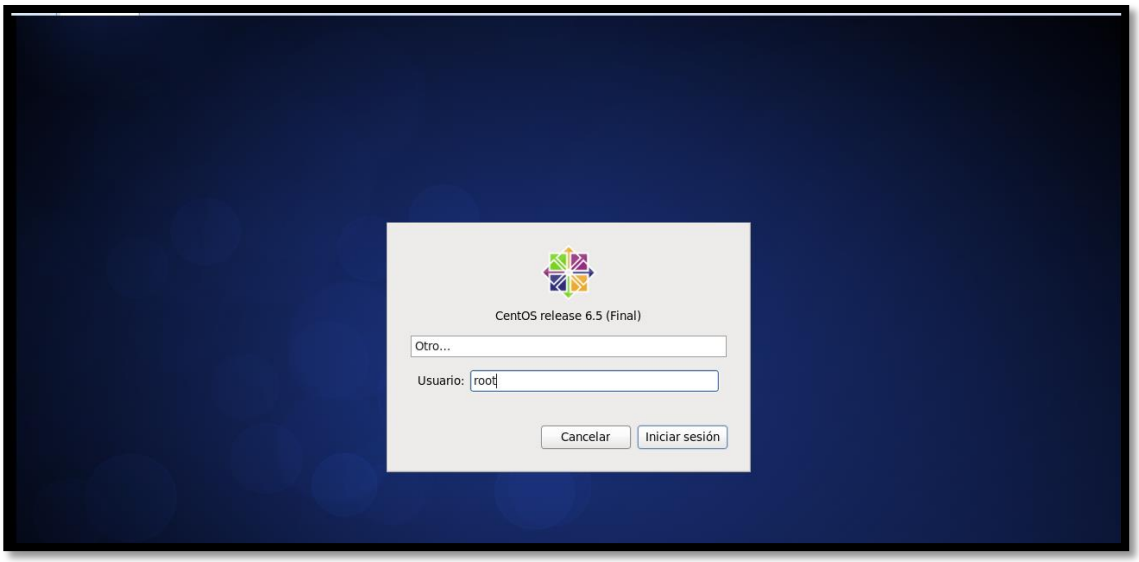


Figura A 20. Pantalla de Inicio de sesión de CentOS

Fuente: CentOS

- Dentro del sistema operativo se debe configurar de la tarjeta de red en el siguiente archivo

/etc/sysconfig/network-scripts/ifcfg-eth0

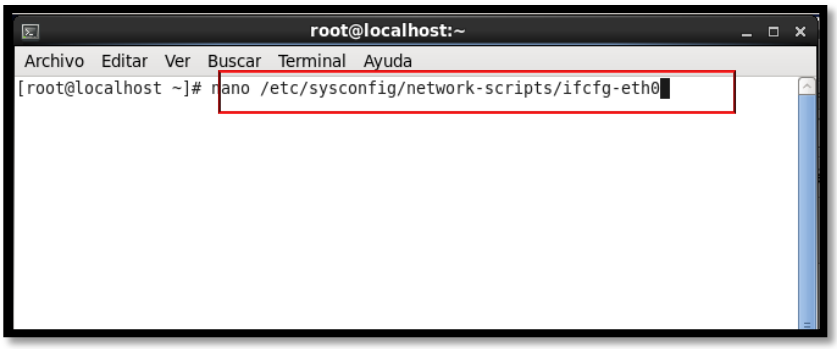


Figura A 21. Comando para ingresar al archivo de configuración de red

Fuente: Consola CentOS

- En el archivo configurar las opciones de la red para estabilizar el servidor y que no pierda conectividad.

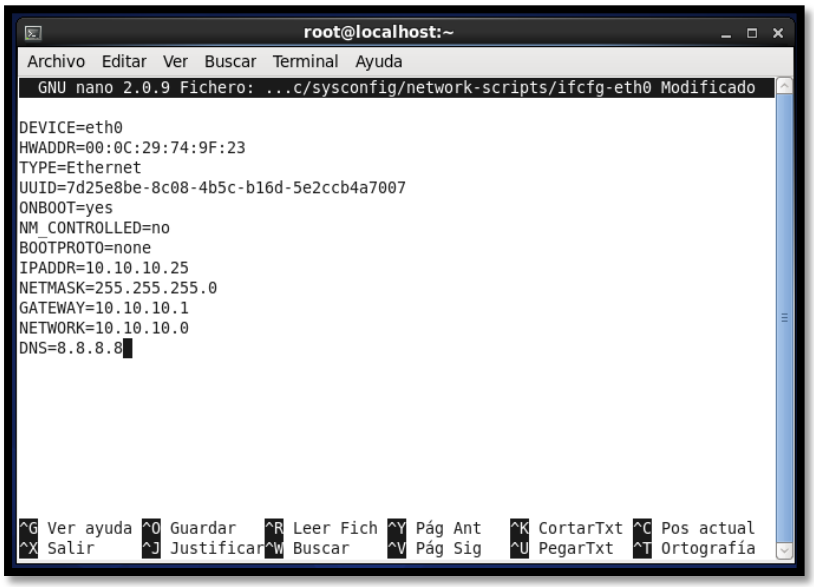


Figura A 22. Archivo de configuración de red

Fuente: Consola CentOS

- Por ultimo para que los cambios realizados se guarden se debe reiniciar el servicio

```
#service network restart
```

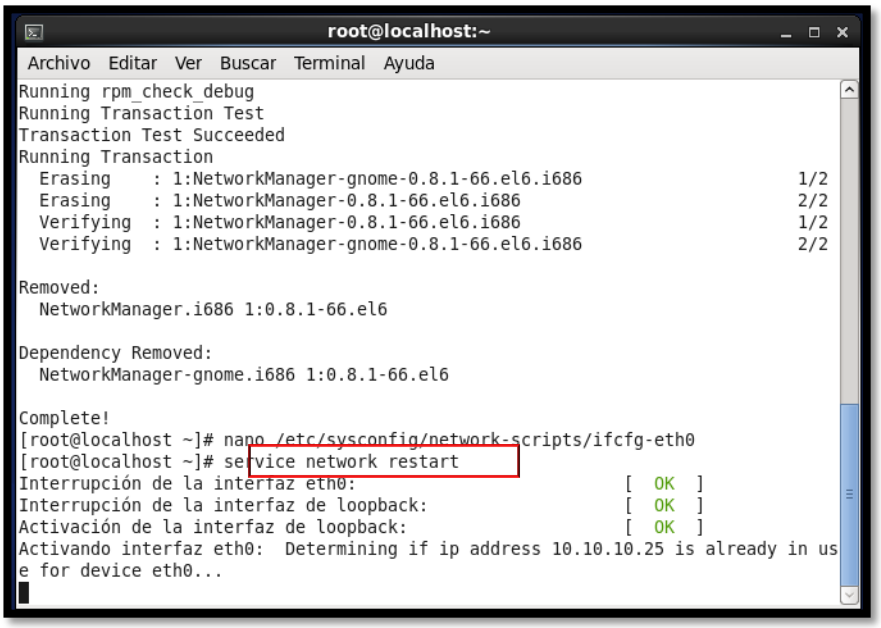


Figura A 23. Reinicio del servicio

Fuente: Consola CentOS

ANEXO B. INSTALACIÓN DE REQUERIMIENTOS PARA PANDORA FMS

B1. Instalación Servidor Apache

- Instalar el paquete httpd mediante el comando

```
#yum install httpd
```

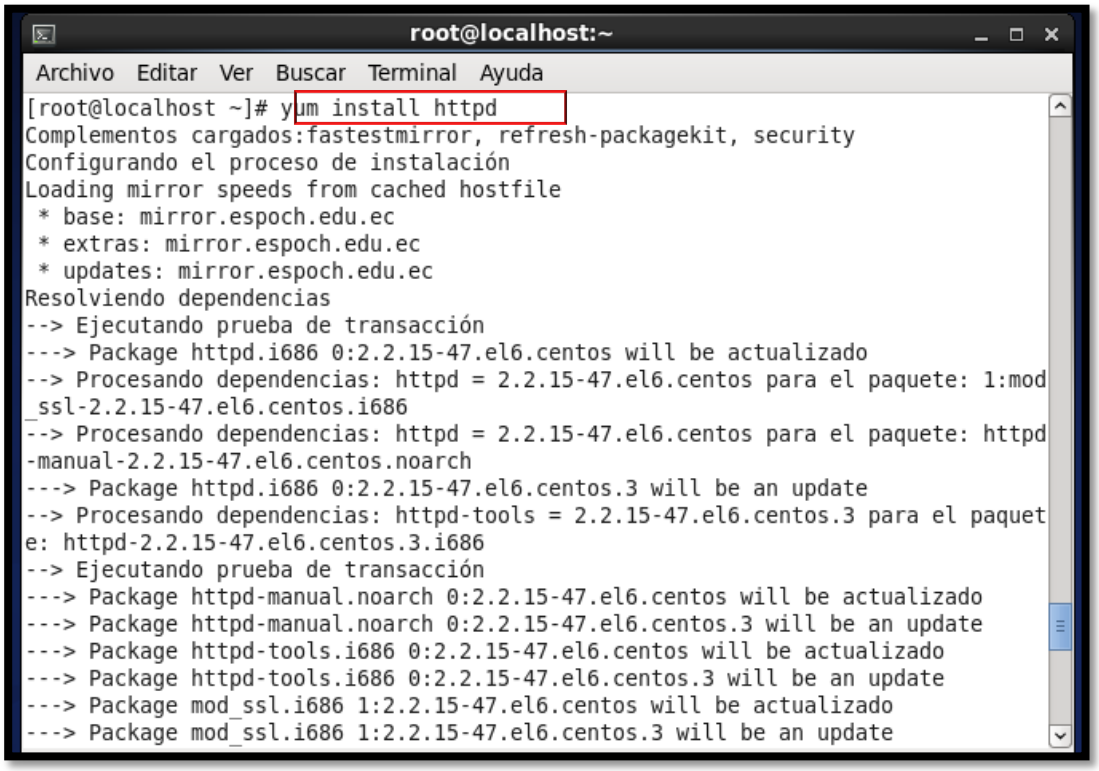


Figura B 1. Instalación de Apache

Fuente: Consola CentOS

- Iniciar el servicio httpd con el siguiente comando

```
#service httpd start
```

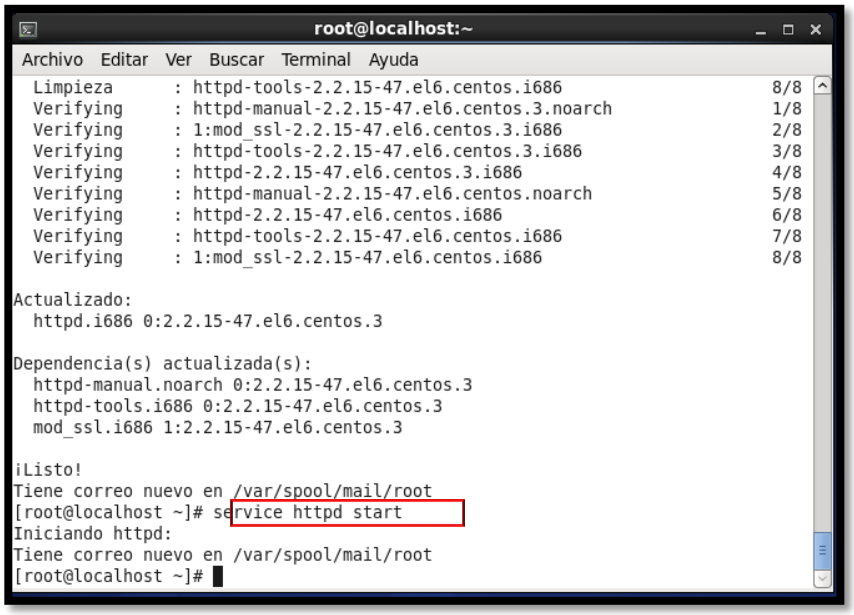


Figura B 2. Reinicio del Servicio http

Fuente: Consola CentOS

- Para comprobar que se ha instalado correctamente en el navegador se inserta la dirección IP y aparecerá la página mostrada.

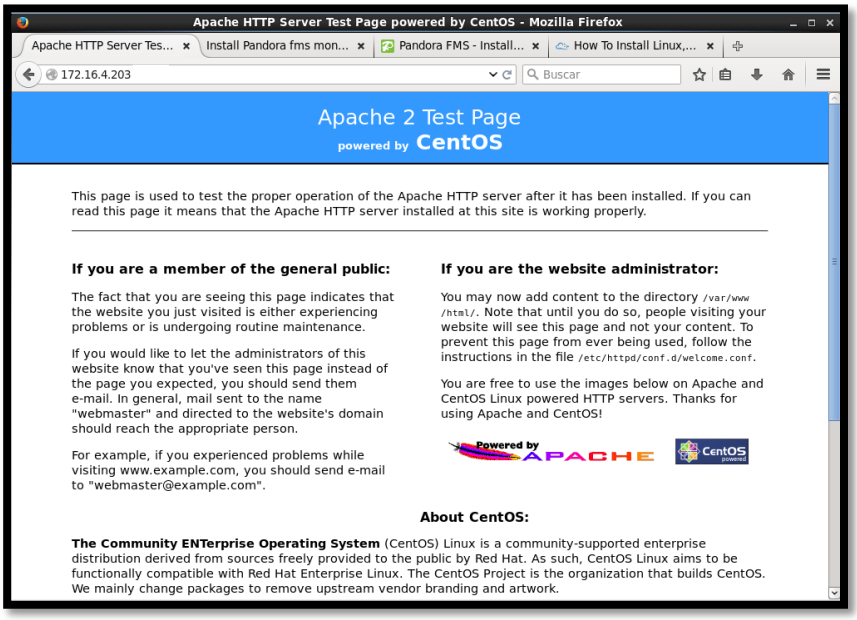


Figura B 3. *Pantalla de Apache luego de instalación*

Fuente: Apache

- Por último el servicio debe iniciar por default al encender la maquina con el comando

```
#chkconfig httpd on
```

Figura B 4. Inicio al encender la maquina

Fuente: Consola CentOS

B2. Instalación de MySQL

- Instalar el paquete mysql-server

```
#yum install mysql-server
```

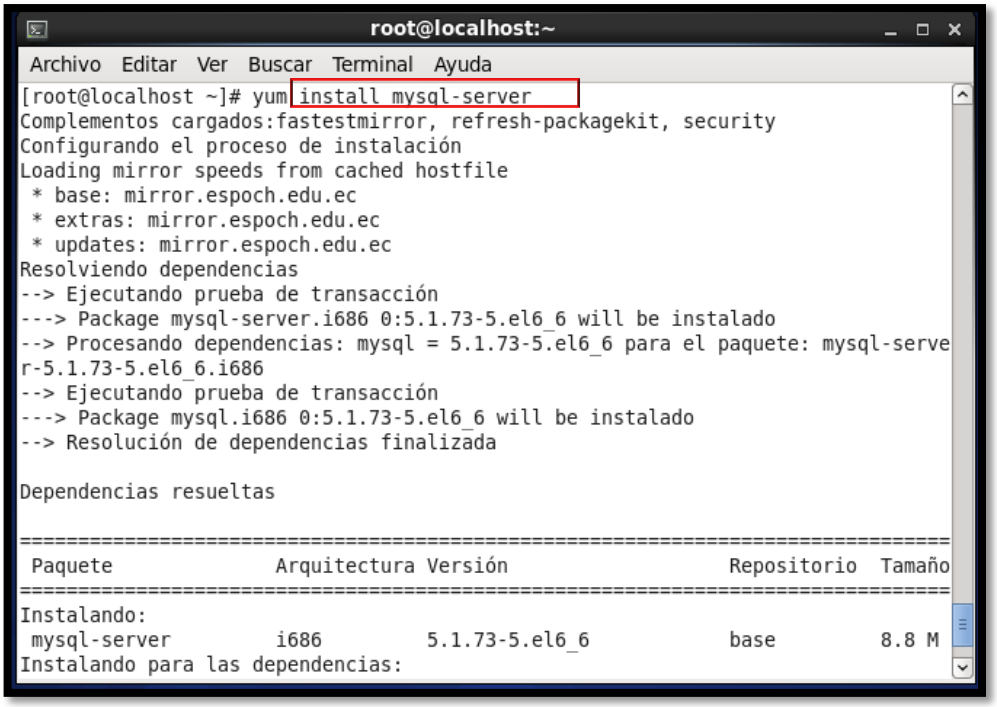


Figura B 5. Instalación paquete MySQL

Fuente: Consola CentOS

- Iniciar el servicio mysqld

```
#service mysqld start
```

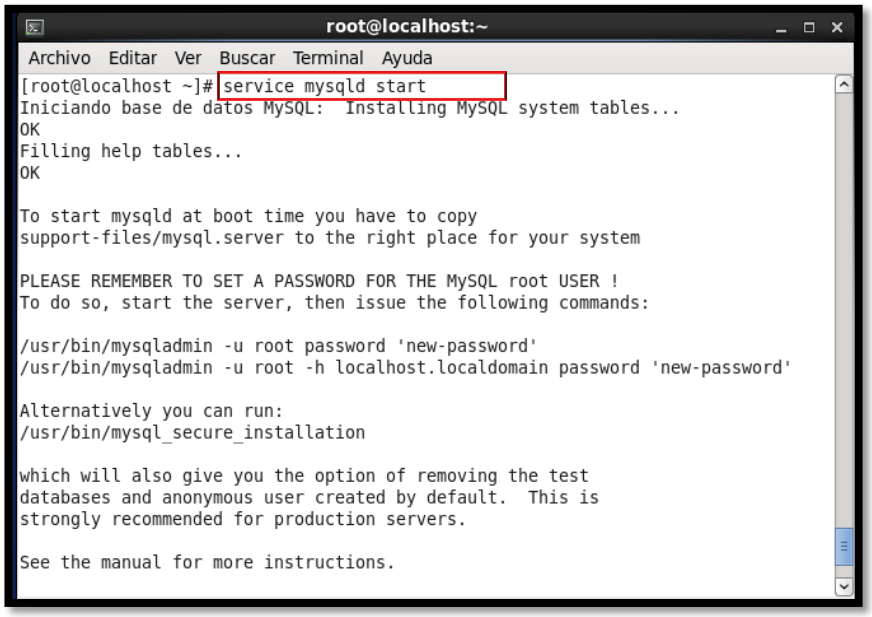


Figura B 6. Inicio del servicio MySQL

Fuente: Consola CentOS

- Ingresar la contraseña root del equipo

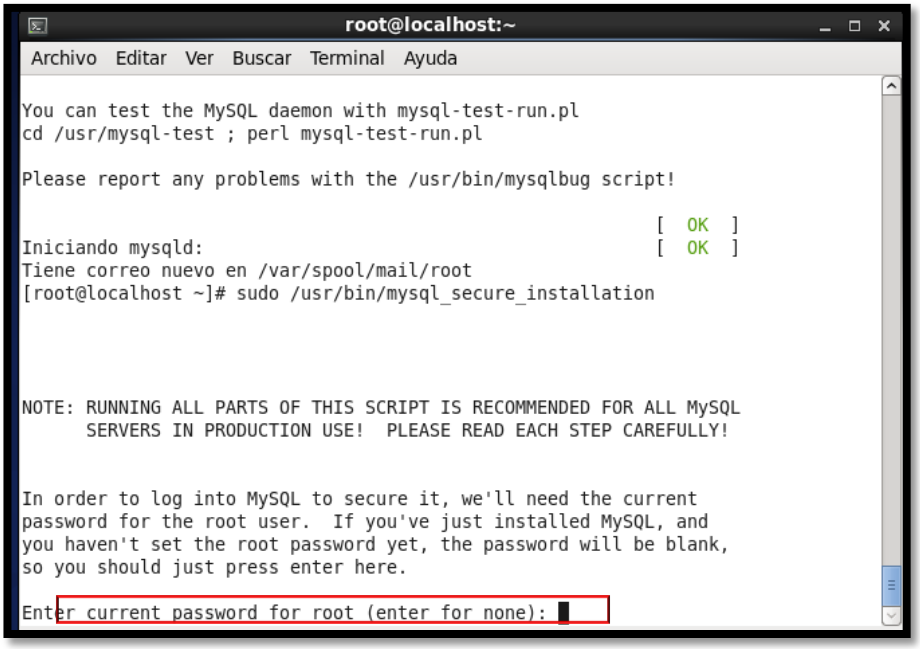


Figura B 7. Ingreso de contraseña root

Fuente: Consola CentOS

- Colocar Enter en la opción mostrada y luego escribimos la contraseña para root de MySQL

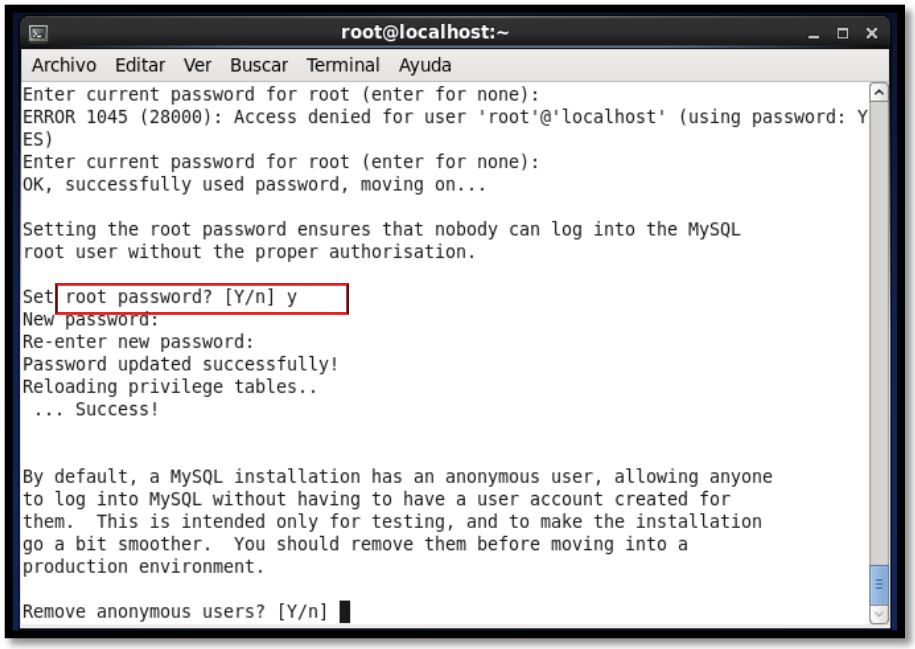


Figura B 8. Configuración de contraseña MySQL

Fuente: Consola CentOS

- A continuación colocar si a todas las opciones que presente la aplicación.
- Para que el servicio de MySQL se inicia por default al encender el sistema colocar el siguiente comando

```
#chkconfig –level 2345 mysqld on
```

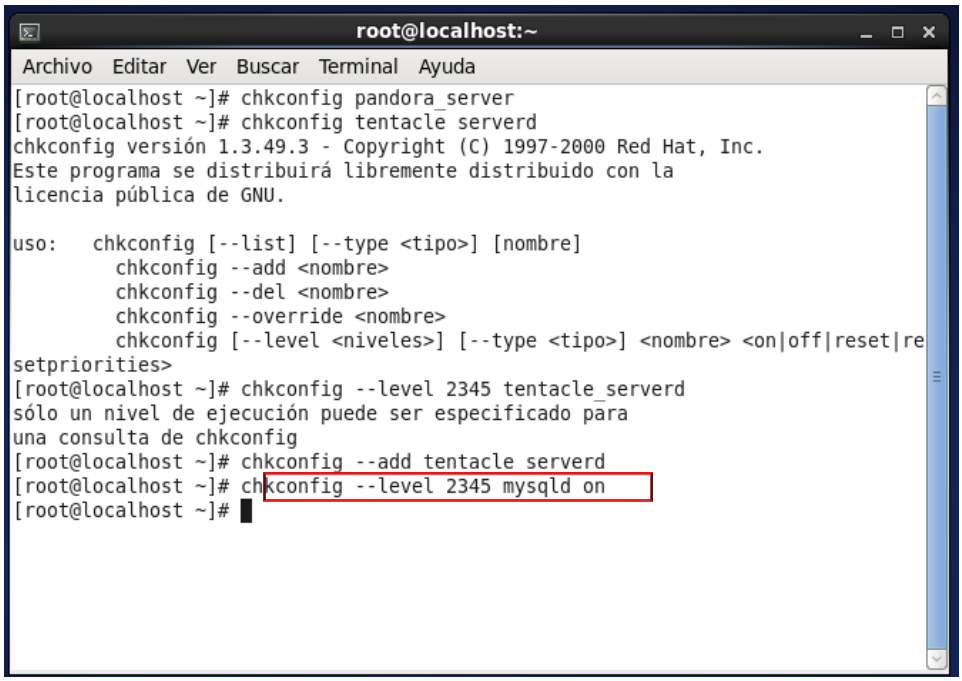


Figura B 9. Inicio por default de MySQL

Fuente: Consola CentOS

B3. Instalación de Postfix

- Instalar el paquete de postfix con el siguiente comando

```
#yum install postfix
```

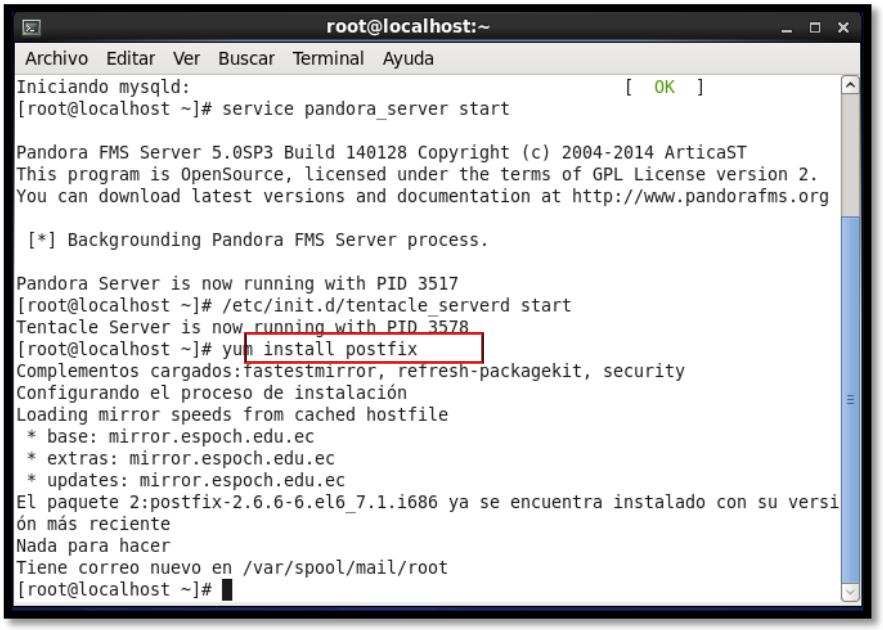


Figura B 10. Instalación de PostFix

Fuente: Consola CentOS

- En este caso ya se encuentra instalado entonces se procede a modificar la configuración de PostFix en el siguiente archivo

```
#/etc/postfix/main.cf
```

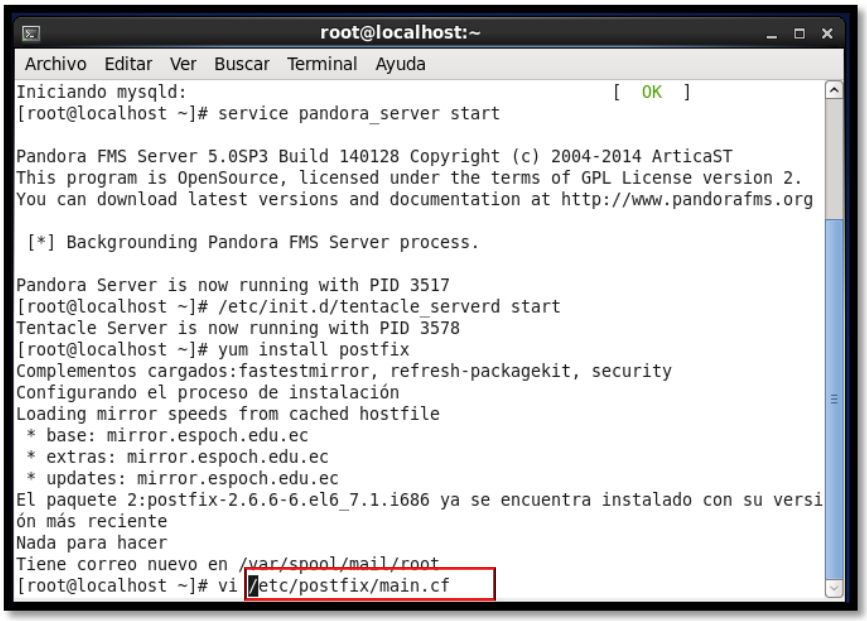


Figura B 11. Comando para configurar archivo de PostFix

Fuente: Consola CentOS

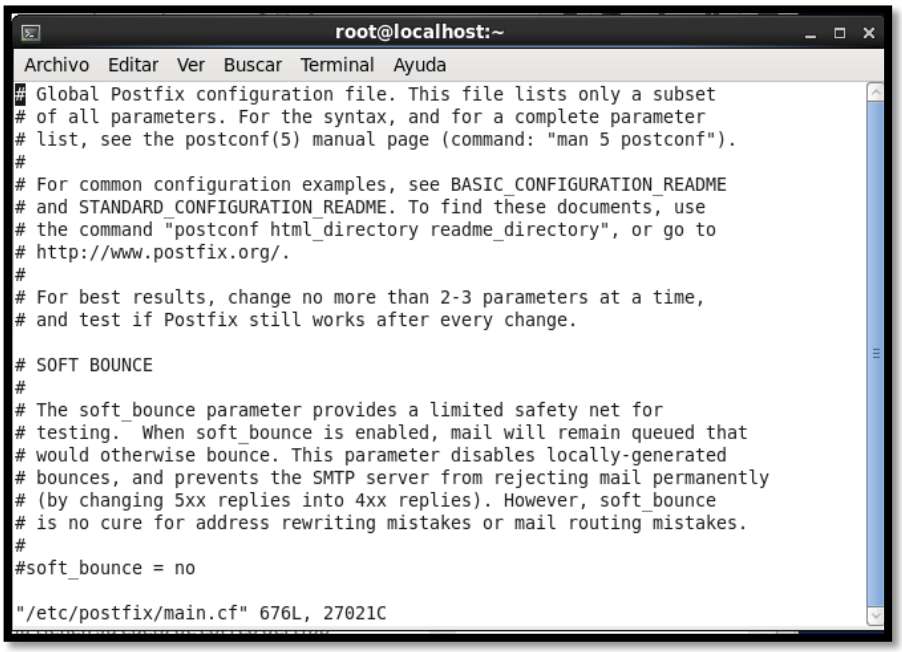


Figura B 12. Archivo de Configuración de PostFix

Fuente: Consola CentOS

- Dentro de este archivo se debe editar las siguientes líneas

```
inet_interfaces = all

mydomain  = midominio.org

myorigin = $mydomain

mydestination = $mydomain, $myhostname, localhost

home_mailbox = Maildir/
```

- Añadir el servicio al inicio del sistema con el siguiente comando

```
#chkconfig postfix on
```

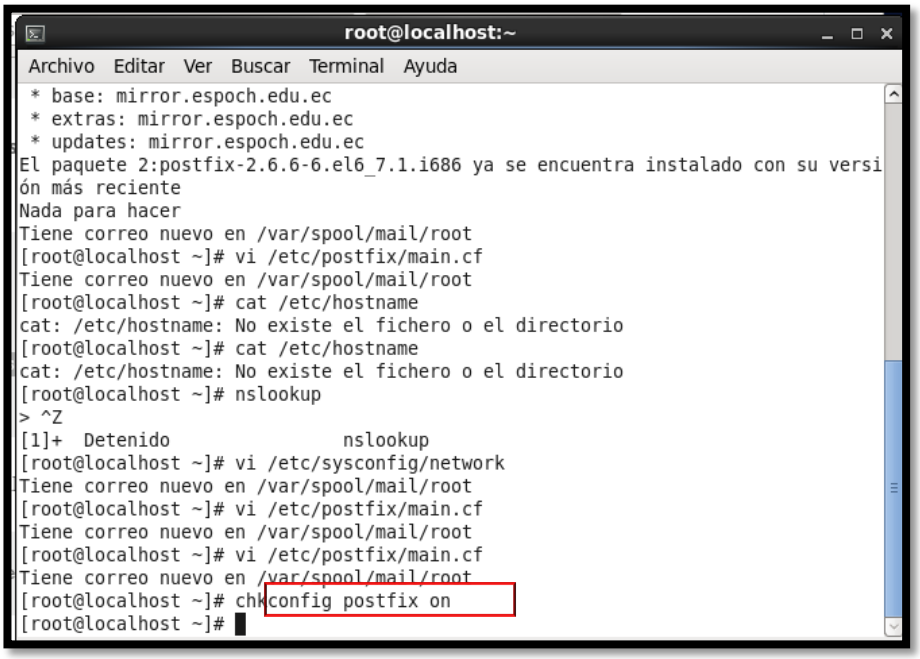


Figura B 13. Inicio por default de Servicio PostFix

Fuente: Consola CentOS

- Reiniciar el servicio con el comando

```
#service postfix restart
```

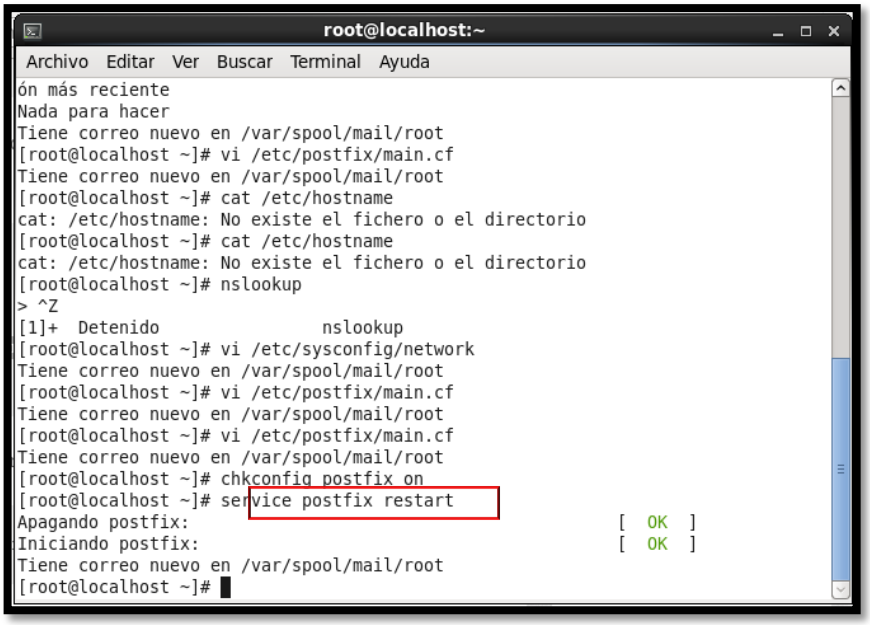


Figura B 14. Reinicio del Servicio PostFix

Fuente: Consola CentOS

- Por defecto todos los usuarios definidos en el sistema tienen su cuenta de correo del tipo usuario@midominio.org
- Crear la carpeta Maildir en el directorio mostrado para que se guarden en ella automáticamente los usuarios añadidos al sistema y los correos electrónicos recibidos.

```
# mkdir /etc/skel/Maildir
```

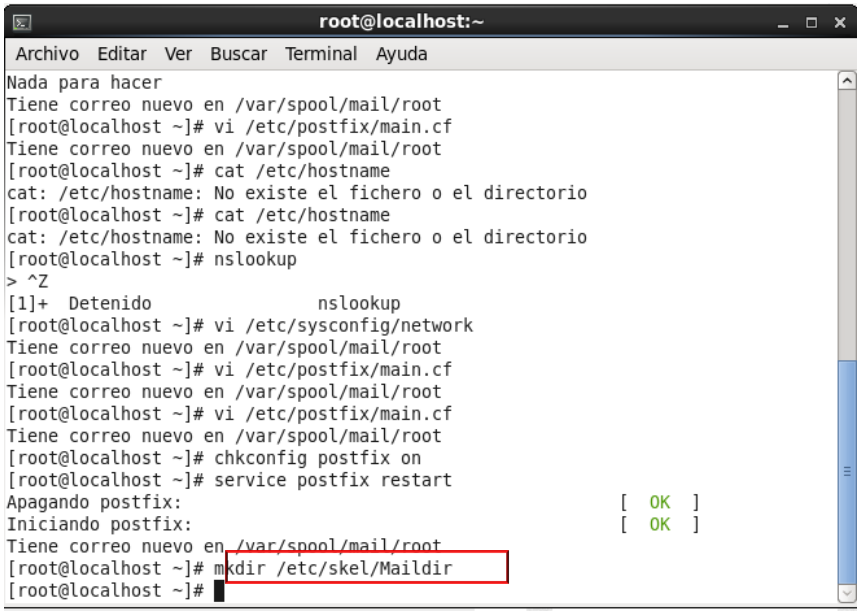


Figura B 15. Creación de carpeta Maildir

Fuente: Consola CentOS

- Crear el archivo para leer el contenido de la carpeta creada anteriormente con el siguiente comando

```
# touch /etc/skel/.muttrc
```

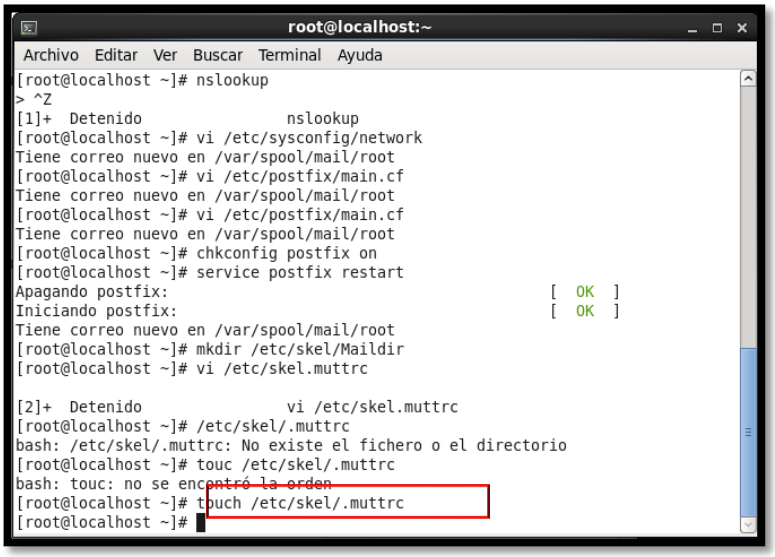


Figura B 16. Creación de archivo para lectura de correos

Fuente: Consola CentOS

- Se procede a editar el archivo con las configuraciones mostradas en la figura

Figura B 17. Configuración de archivo para recibir correos

Fuente: Consola CentOS

- A continuación se crea usuarios para probar el envío de correos

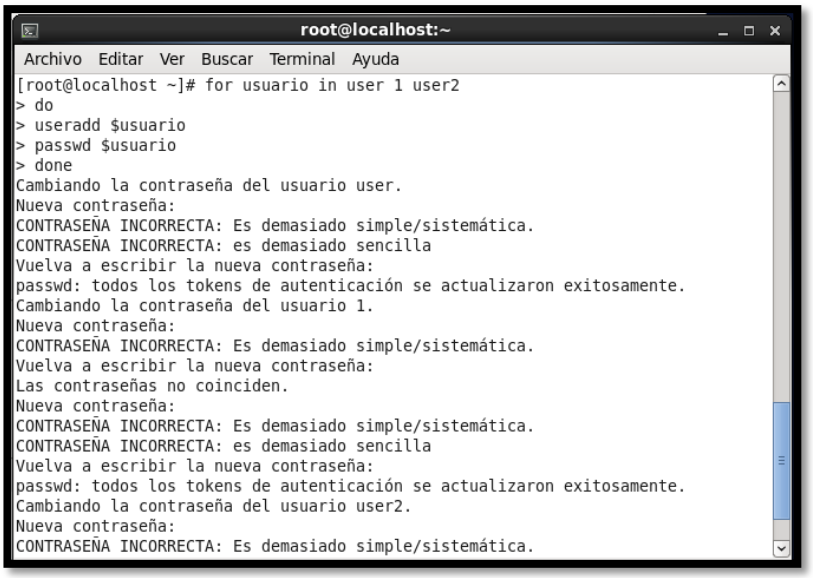


Figura B 18. Creación de Usuario para prueba

Fuente: Consola CentOS

- Para poder comprobar el envío de correo es necesario tener instalado telnet para lo cual se debe instalar el paquete con los siguiente comandos.

```
# yum –y install telnet

#yum install telnet-server
```

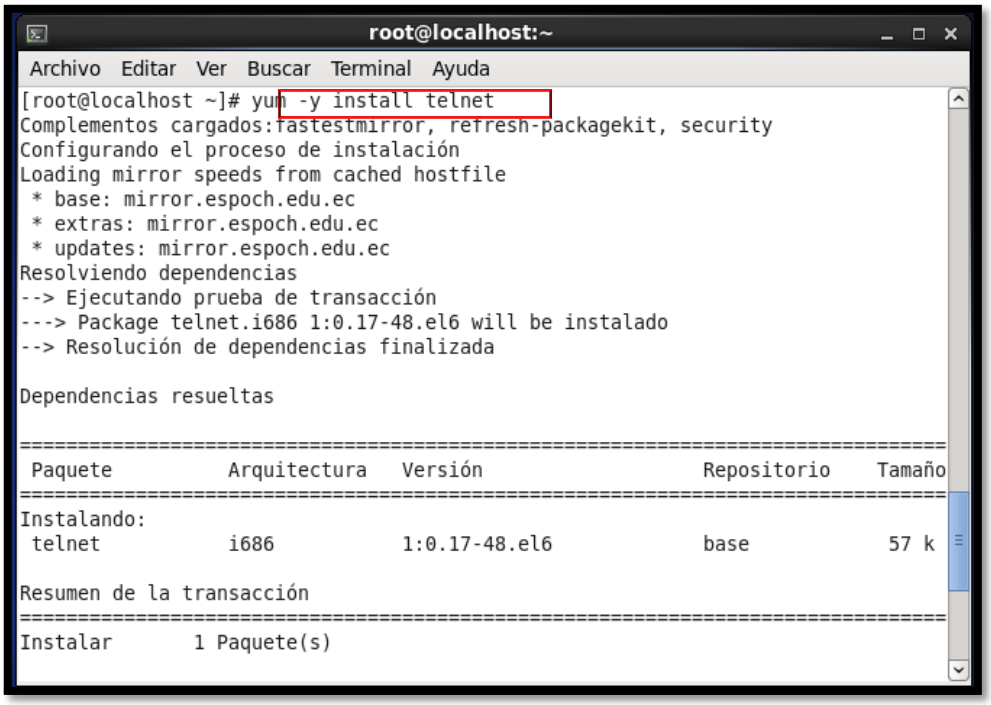


Figura B 19. Comando para instalar Telnet

Fuente: Consola CentOS

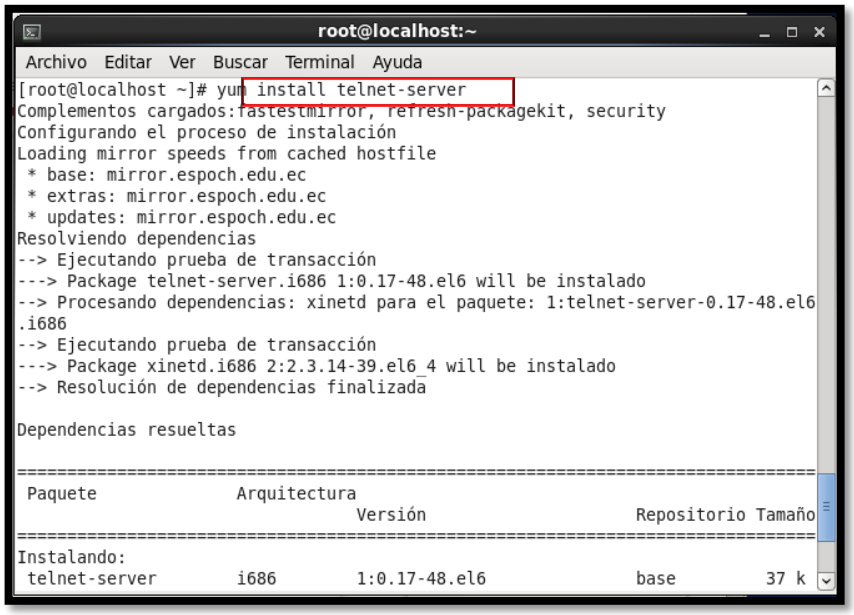


Figura B 20. Comando para instalación de Telnet

Fuente: Consola CentOS

- A continuación se debe acceder al archivo

/etc/xineted.d/telnet

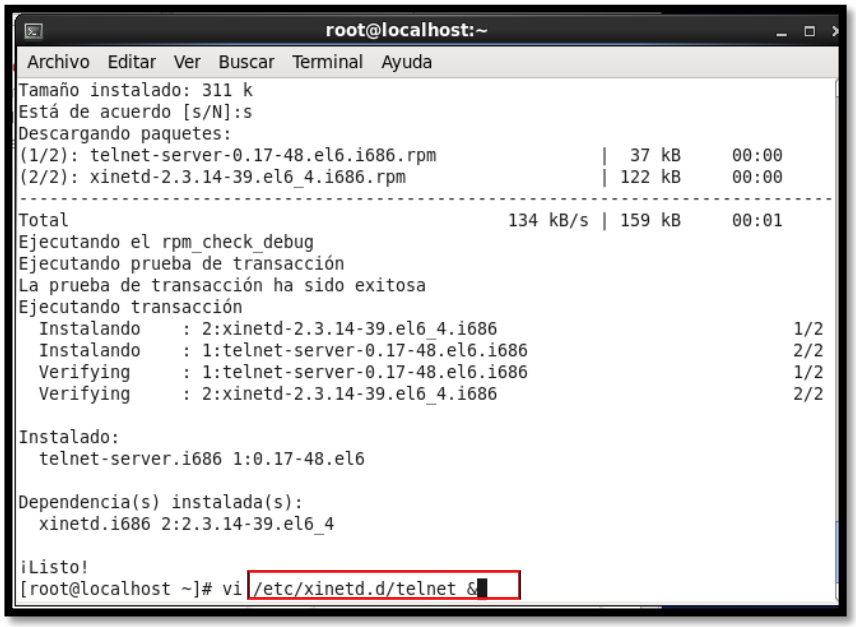


Figura B 21. Ingreso al archivo de configuración de Telnet

Fuente: Consola CentOS

- Dentro de este archivo cambiar la línea disable=yes por disable=no

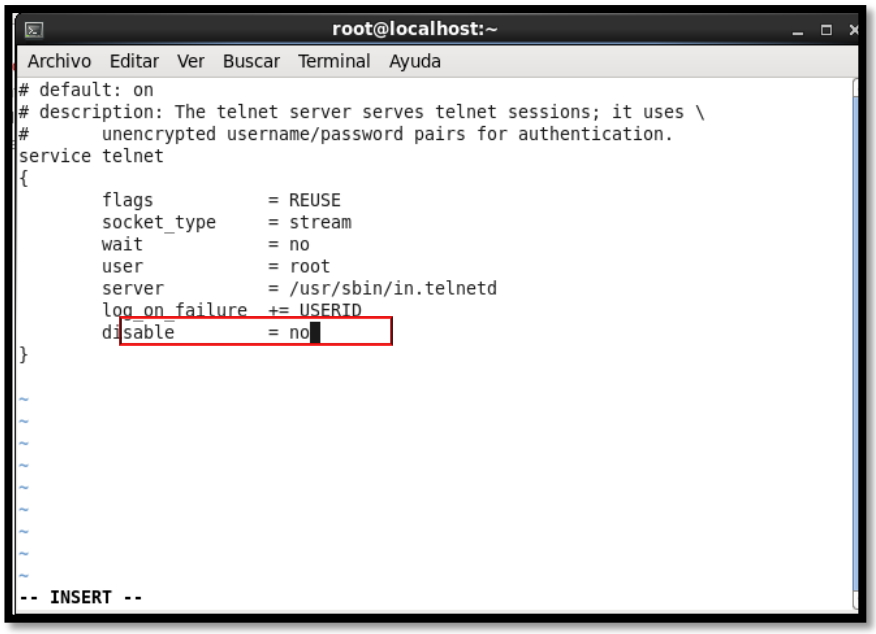


Figura B 22. Archivo de configuración de Telnet

Fuente: Consola CentOS

- A continuación se debe abrir el puerto 23 del firewall para esto se debe dirigir al menú sistema, escoger administración y luego cortafuegos.

Figura B 23. Menú Sistema

Fuente: CentOS

- En la opción otros puertos escoger añadir y escoger el puerto 23 de Telnet, luego se debe hacer clic en aceptar y el puerto se añade.

Figura B 24. Añadir el Puerto para Telnet

Fuente: CentOS

Figura B 25. Puerto 23 de Telnet

Fuente: CentOS

Figura B 26. Puerto de Telnet añadido

Fuente: CentOS

- A continuación probar Telnet con el protocolo SMTP

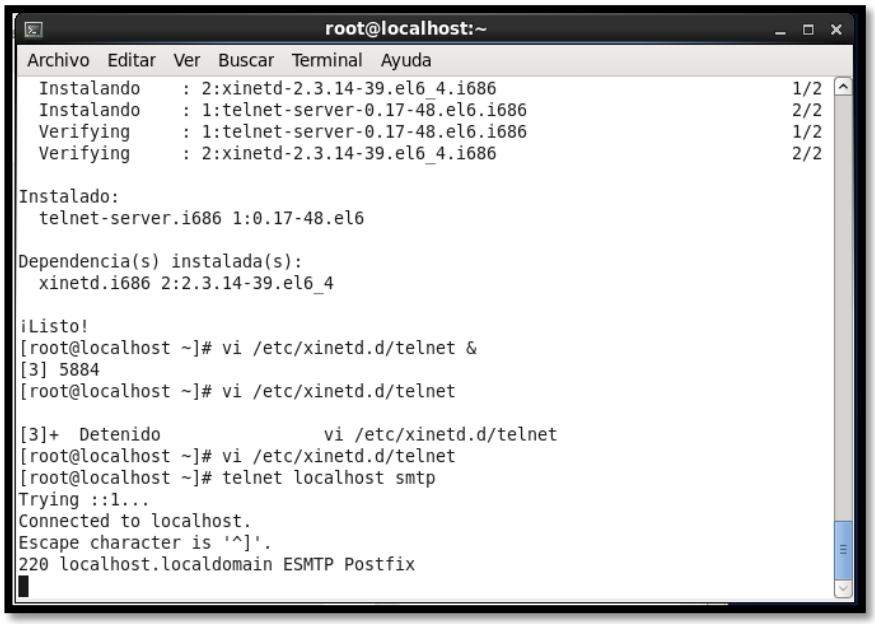


Figura B 27. Telnet al protocolo SMTP

Fuente: Consola CentOS

- Añadir las siguientes líneas para envió de correo.

```
220 mail.midominio.org ESMTP Postfix
ehlo local
250-mail.midominio.org
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: test@test.org
250 2.1.0 Ok
rcpt to: user1@midominio.org
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: hola
primer correo de prueba
.
250 2.0.0 Ok: queued as 0E32477
```

- Comprobar en el log que se haya enviado el correo y el servidor PostFix estará funcionando

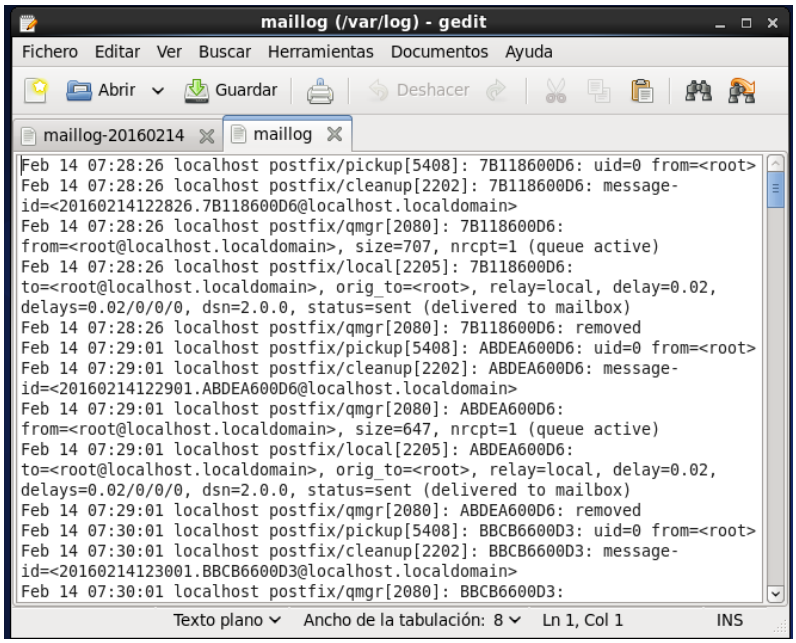


Figura B 28. Comprobación de Correo enviado

Fuente: Consola CentOS

ANEXO C: MANUAL DE ADMINISTRADOR DE PANDORA FMS

C1. Instalación Pandora FMS

- Descargar los archivos .rpm de la consola, el agente, servidor y wmic[14] de Pandora FMS desde las siguientes direcciones web. Para esto se utiliza el comando wget en la consola de CentOS.

https://sourceforge.net/projects/pandora/files/Pandora%20FMS%205.0/FinalSP3/RHEL_CentOS/pandorafms_agent_unix-5.0SP3-1.noarch.rpm/download?use_mirror=heanet&r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2FPandora%2520FMS%25205.0%2FFinalSP3%2FRHEL_CentOS%2F&use_mirror=heanet

http://downloads.sourceforge.net/project/pandora/Pandora%20FMS%205.0/FinalSP3/RHEL_CentOS/pandorafms_server-5.0SP3-1.noarch.rpm?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2FPandora%2520FMS%25205.0%2FFinalSP3%2FRHEL_CentOS%2F&ts=1395336686&use_mirror=freefr

http://downloads.sourceforge.net/project/pandora/Pandora%20FMS%205.0/FinalSP3/RHEL_CentOS/pandorafms_console-5.0SP3-1.noarch.rpm?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2FPandora%2520FMS%25205.0%2FFinalSP3%2FRHEL_CentOS%2F&ts=1395336727&use_mirror=skylink

[14] **WMIC:** Windows Management Instrumentation Command-line

http://downloads.sourceforge.net/project/pandora/Tools%20and%20dependencies%20%28All%20versions%29/RPM%20CentOS%2C%20RHEL/wmic-4.0.0SVN-2.1.el5.centos.noarch.rpm?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2FTools%2520and%2520dependencies%2520%28All%2520versions%29%2FRPM%2520CentOS%2C%2520RHEL%2F&ts=1395337829&use_mirror=garr

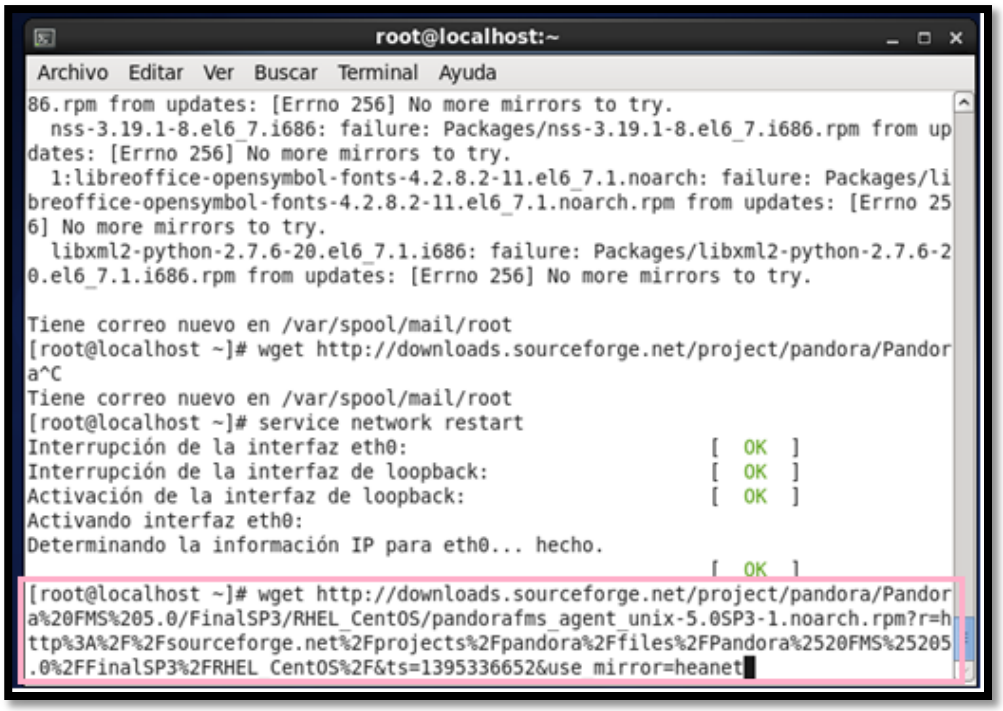


Figura C 1. Descarga Agente Pandora FMS

Fuente: Consola de CentOS

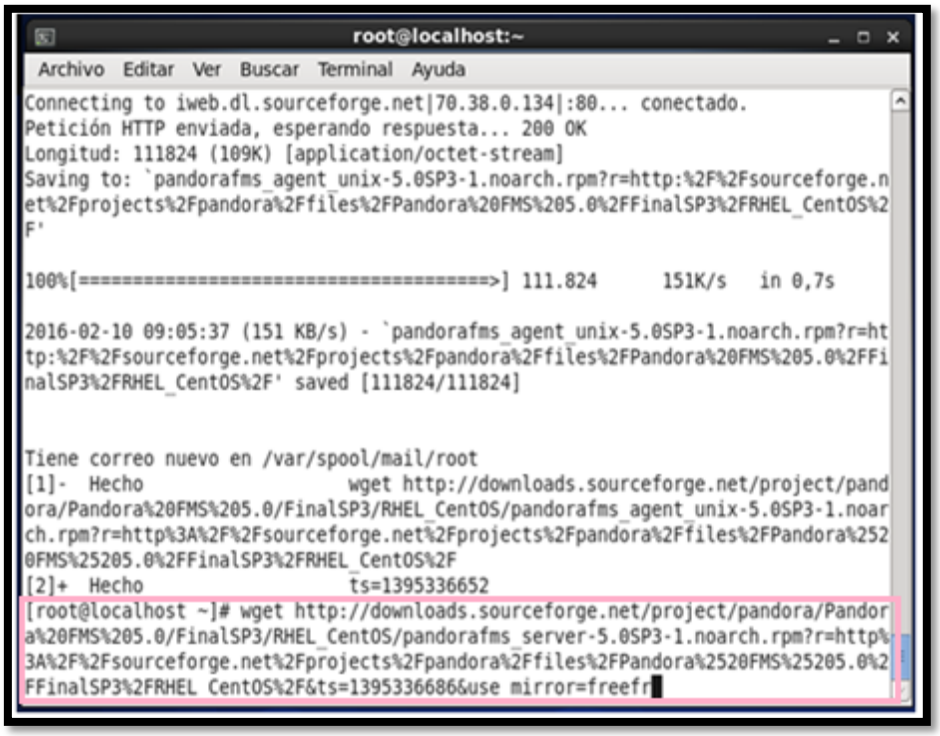


Figura C 2. Descarga Servidor Pandora FMS

Fuente: Consola de CentOS

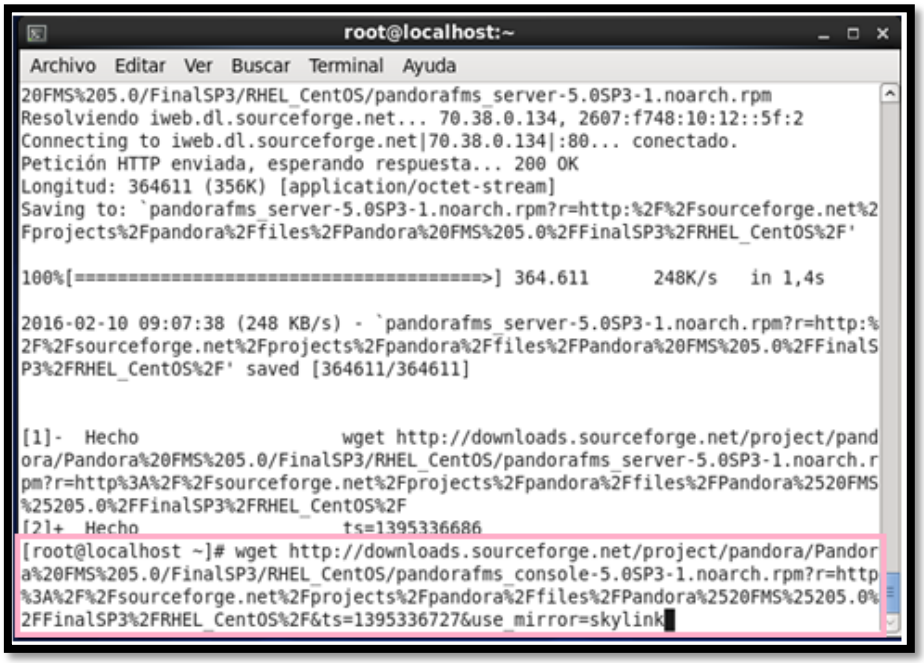


Figura C 3. Descarga Consola Pandora FMS

Fuente: Consola de CentOS

Figura C 4. Descarga Herramienta WSDI Pandora FMS

Fuente: Consola de CentOS

- Mover los archivos para que todos los paquetes .rpm se encuentren en una misma carpeta, utilizando el comando mv en la Consola de CentOS.

```
# mv pandorafms_console-5.0SP3-
1.noarch.rpm\?r\=http\:%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2FPandora%2
0FMS%205.0%2FFinalSP3%2FRHEL_CentOS%2F pandorafms_console-5.0SP3-1.noarch.rpm
```

```
#mv pandorafms_server-5.0SP3-
1.noarch.rpm\?r\=http\:%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2FPandora%2
0FMS%205.0%2FFinalSP3%2FRHEL_CentOS%2F pandorafms_server-5.0SP3-1.noarch.rpm
```

```
#mv pandorafms_agent_unix-5.0SP3-
1.noarch.rpm\?r\=http\:%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2FPandora%2
0FMS%205.0%2FFinalSP3%2FRHEL_CentOS%2F pandorafms_agent_unix-5.0SP3-1.noarch.rpm
```

```
#mv wmic-4.0.0SVN-
2.1.el5.centos.noarch.rpm\?r\=http\:%2F%2Fsourceforge.net%2Fprojects%2Fpandora%2Ffiles%2F
Tools%20and%20dependencies%20\(All%20versions\)%2FRPM%20CentOS\,%20RHEL%2F
wmic-4.0.0SVN-2.1.el5.centos.noarch.rpm
```

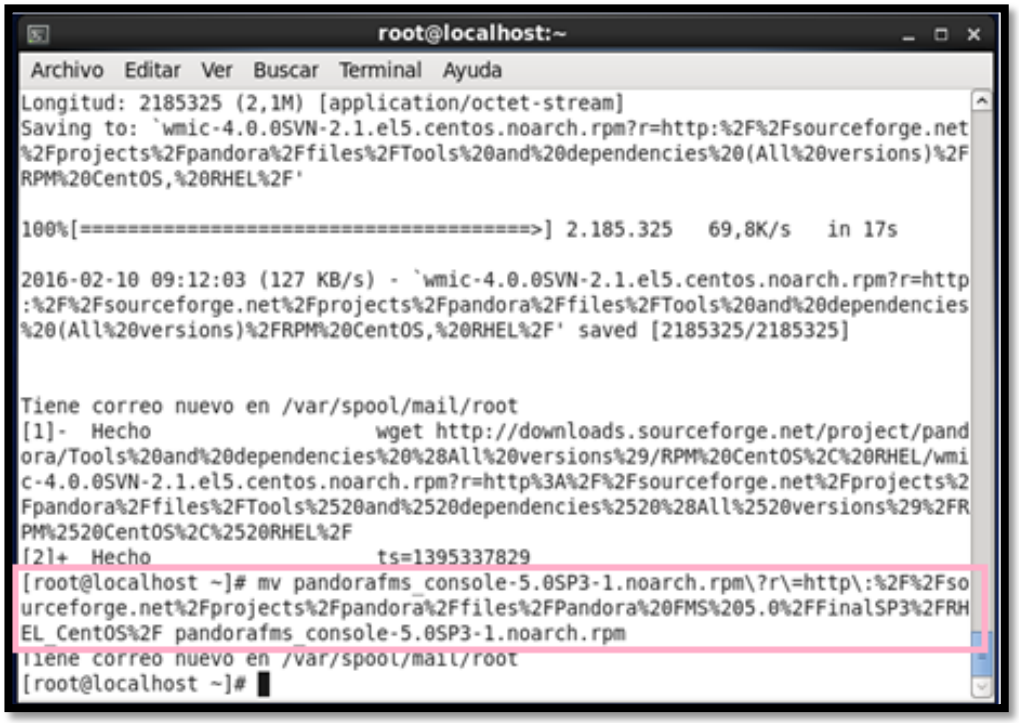


Figura C 5. Cambio de carpeta archivo rpm de Consola Pandora FMS

Fuente: Consola de CentOS

Figura C 6. Cambio de carpeta archivo rpm de Pandora FMS Server

Fuente: Consola de CentOS

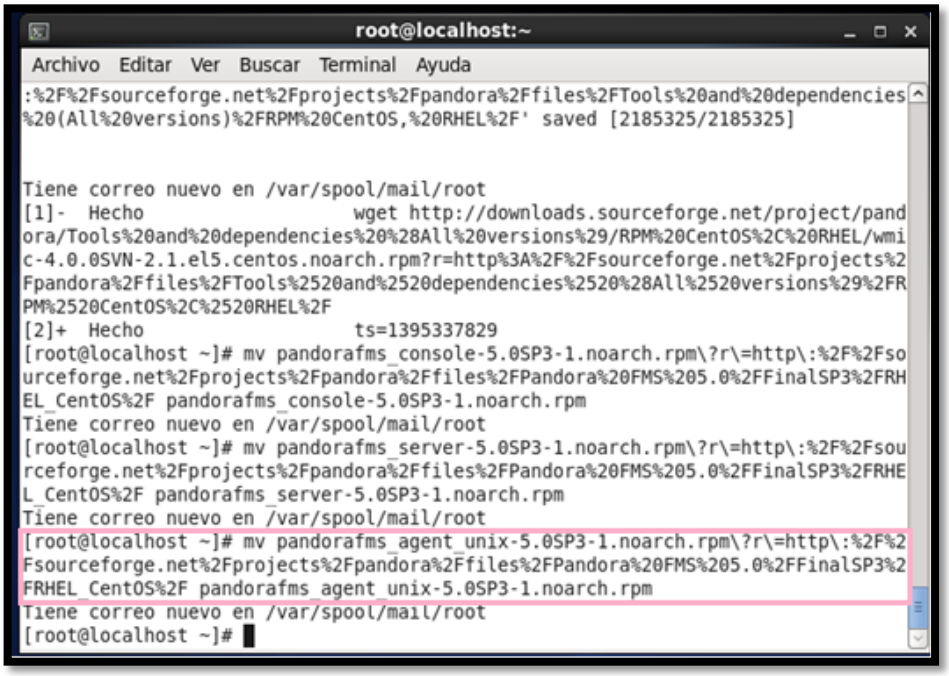


Figura C 7. Cambio de carpeta archivo rpm de Agente Pandora FMS

Fuente: Consola de CentOS

Figura C 8. Cambio de carpeta archivo rpm de Herramienta WSDI de Pandora

Fuente: Consola de CentOS

- Instalar los cuatro paquetes descargados utilizando el comando yum en el orden indicado a continuación.

```
#sudo yum localinstall pandorafms_console-5.0SP3-1.noarch.rpm
```

```
#sudo yum localinstall wmic-4.0.0SVN-2.1.el5.centos.noarch.rpm
```

```
#sudo yum localinstall pandorafms_server-5.0SP3-1.noarch.rpm
```

```
#sudo yum localinstall pandorafms_agent_unix-5.0SP3-1.noarch.rpm
```

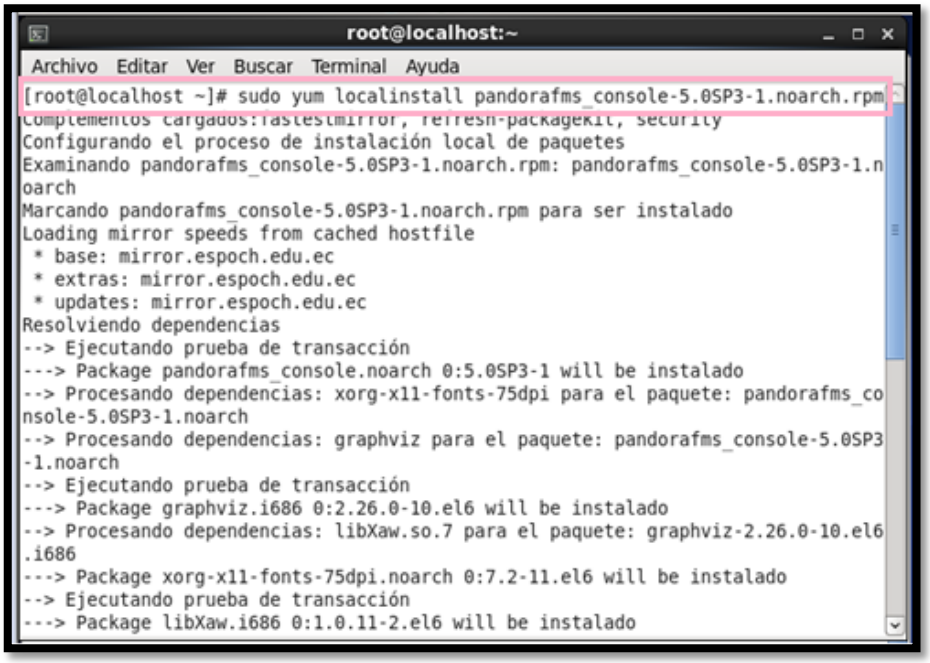


Figura C 9. Instalación Consola Pandora FMS

Fuente: Consola de CentOS

Figura C 10. Instalación Herramienta WSDI

Fuente: Consola de CentOS

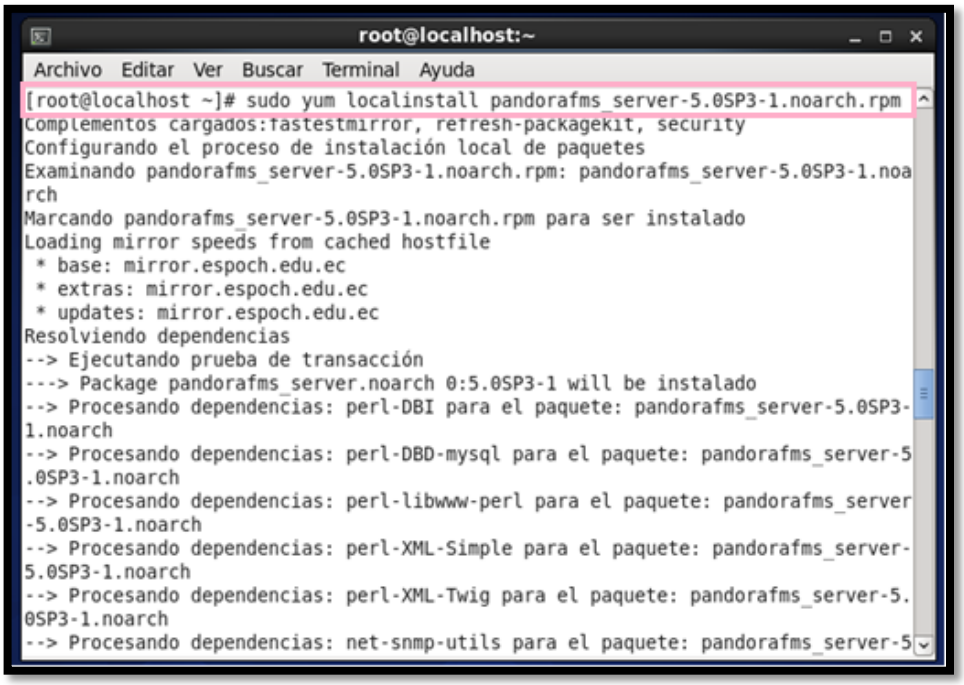


Figura C 11. Instalación Pandora FMS Server

Fuente: Consola de CentOS

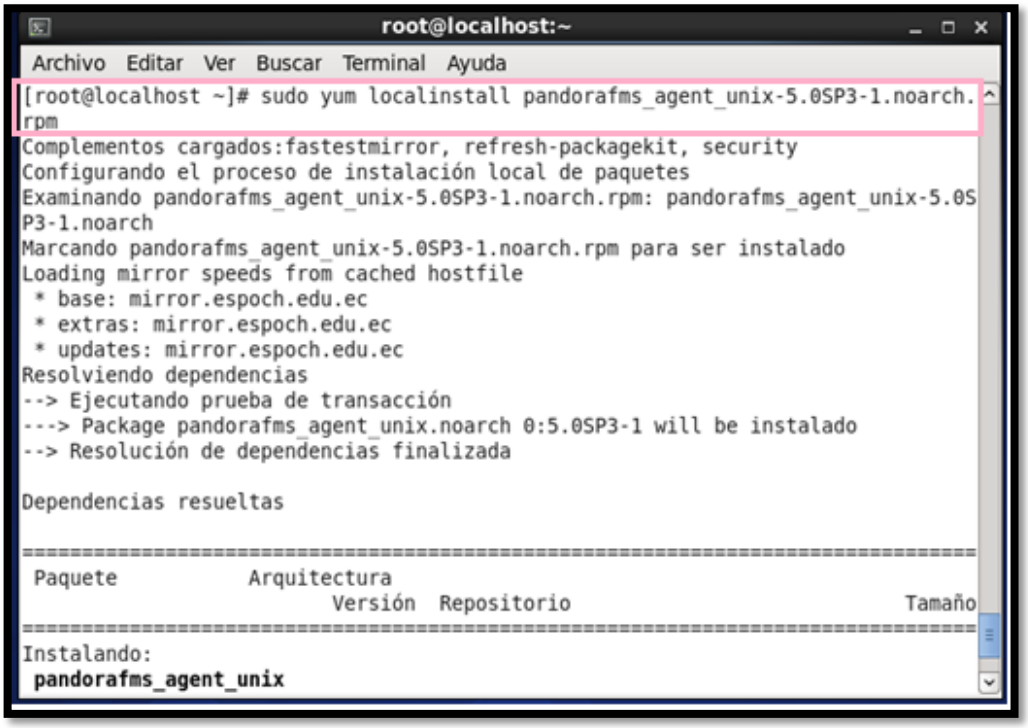


Figura C 12. Instalación Agente Pandora FMS

Fuente: Consola de CentOS

C2.Configuración servidor de Pandora FMS

- Iniciar abriendo el archivo de configuración de consola de Pandora FMS en un editor de archivos con el comando.

```
# vi /var/www/html/pandora_console/include/config.php
```

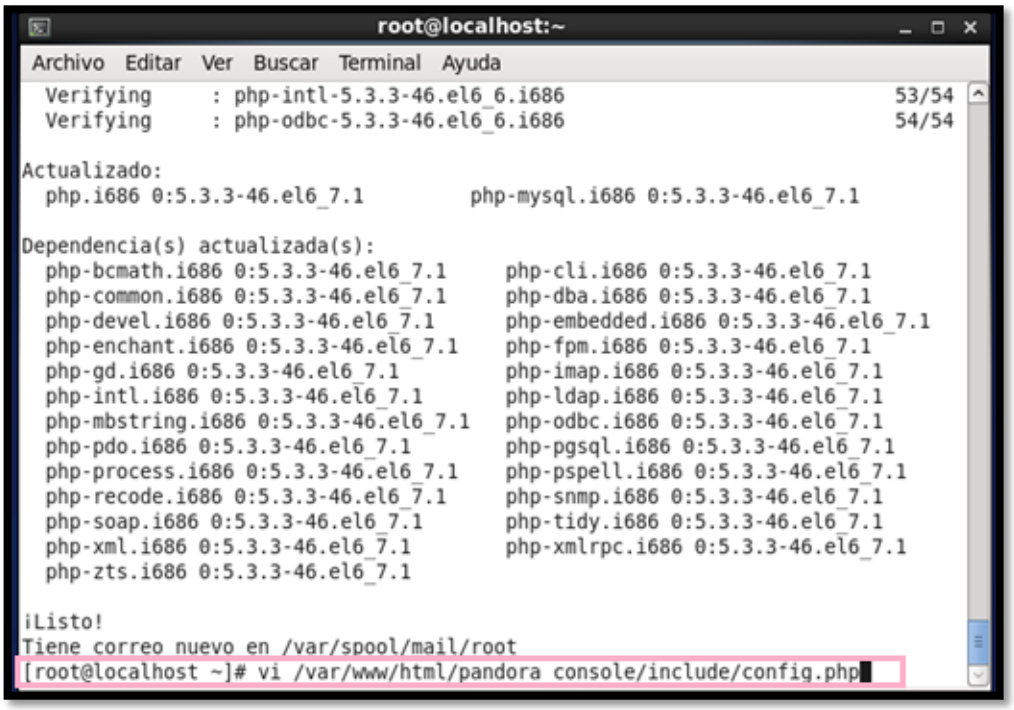


Figura C 13. Comando para abrir archivo de Configuración de Configuración de Consola Pandora FMS

Fuente: Consola de CentOS

- Copiar la contraseña MySQL que se encuentra dentro de este archivo

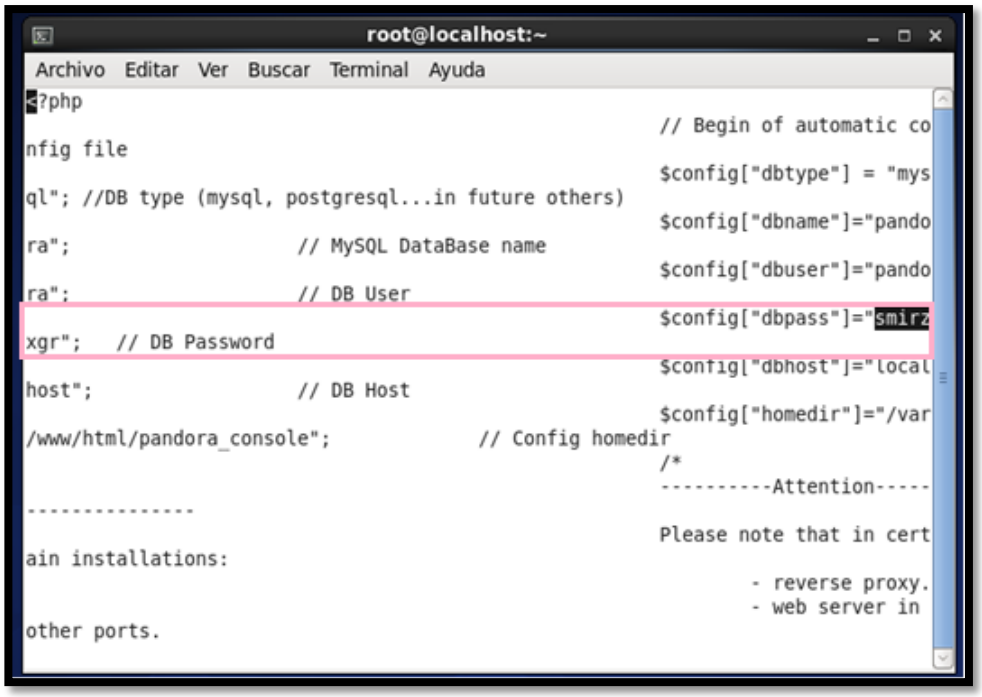


Figura C 14. Archivo de Configuración de Configuración de Consola Pandora FMS

Fuente: Consola de CentOS

- Abrir el archivo de configuración de Pandora Server con un editor de archivos con el comando.

```
#vi /etc/pandora/pandora_server.conf
```

Figura C 15. Comando para abrir archivo de Configuración de Configuración del Servidor Pandora FMS

Fuente: Consola de CentOS

- Dentro del archivo de Configuración Pegar la contraseña MySQL en el lugar mostrado.

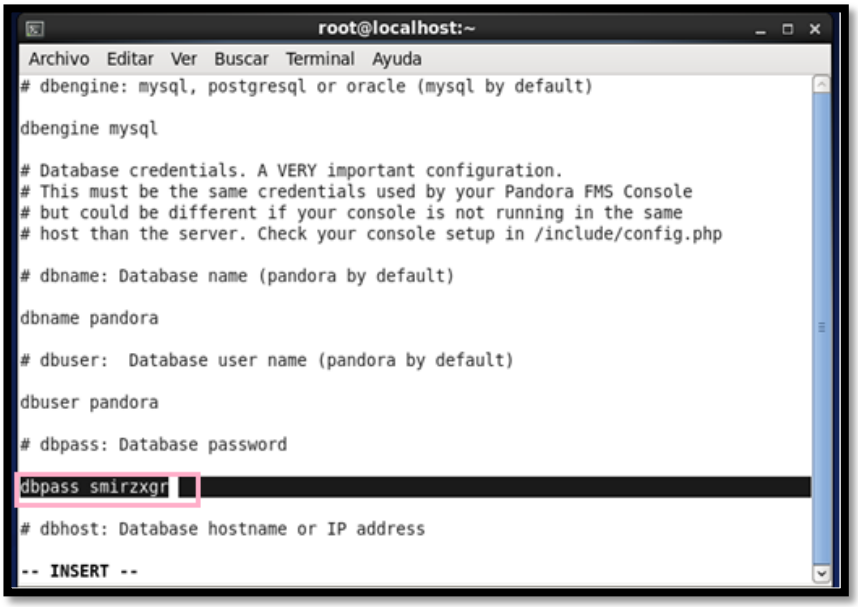


Figura C 16. Archivo de Configuración Servidor Pandora FMS

Fuente: Consola de CentOS

- Luego de realizar este cambio se debe reiniciar el Servidor Pandora con los comandos indicados..

```
# /etc/init.d/pandora_server restart
```

```
# /etc/init.d/tentacle_serverd restart
```

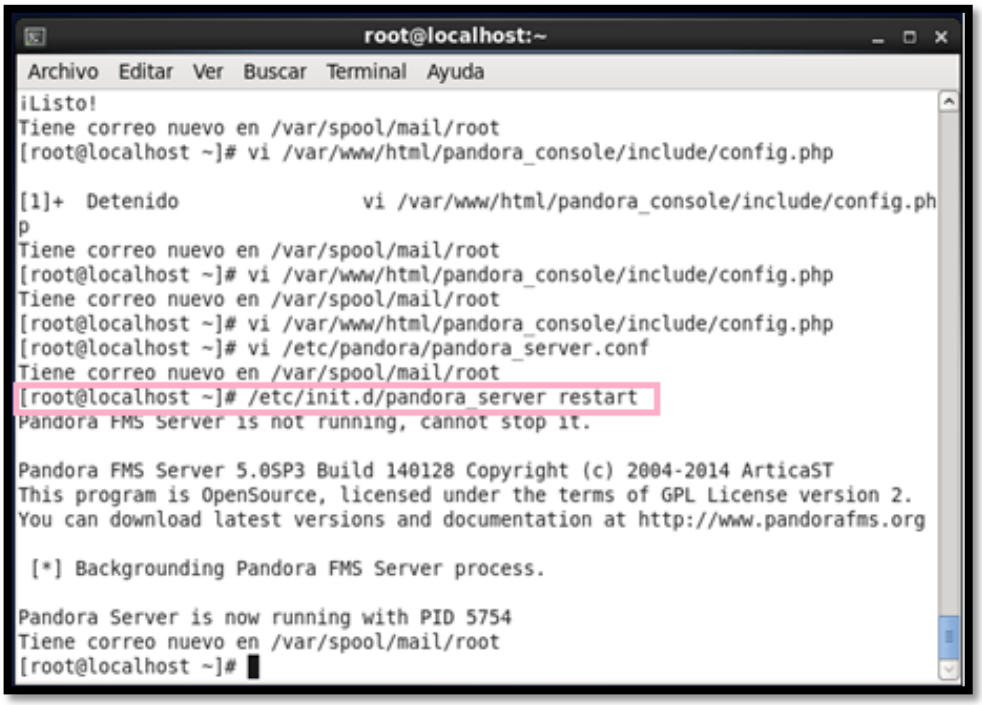


Figura C 17. Reinicio Servidor Pandora FMS

Fuente: Consola de CentOS

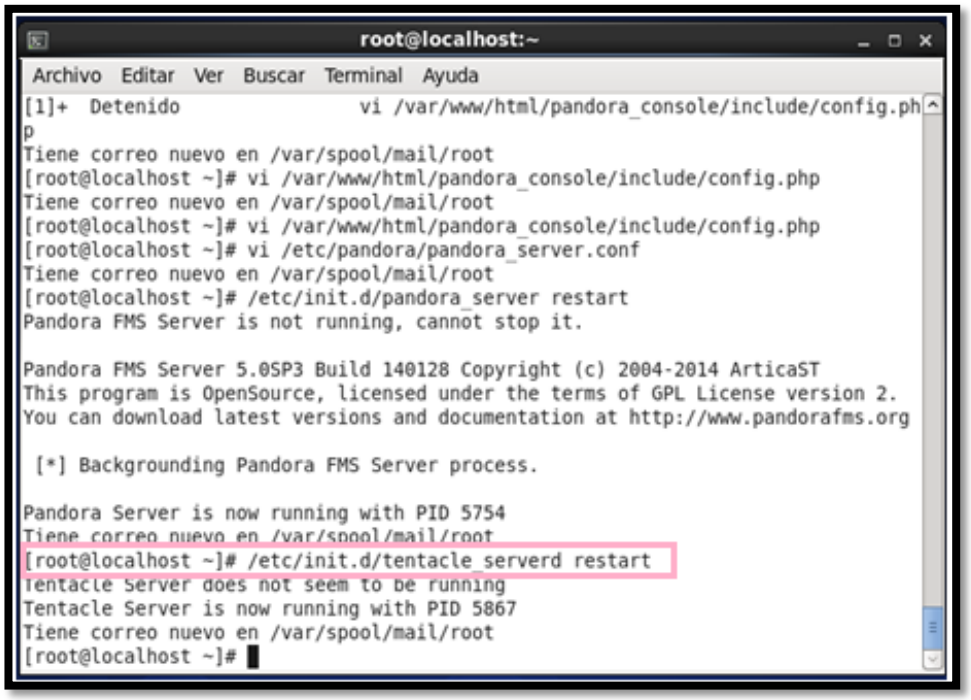


Figura C 18. Reinicio Tentacle Server

Fuente: Consola de CentOS

C3.Configuración Consola de Pandora FMS

- Ingresar en el navegador web la dirección del servidor como se indica en la Figura D1

ipdelhost/pandora_console/

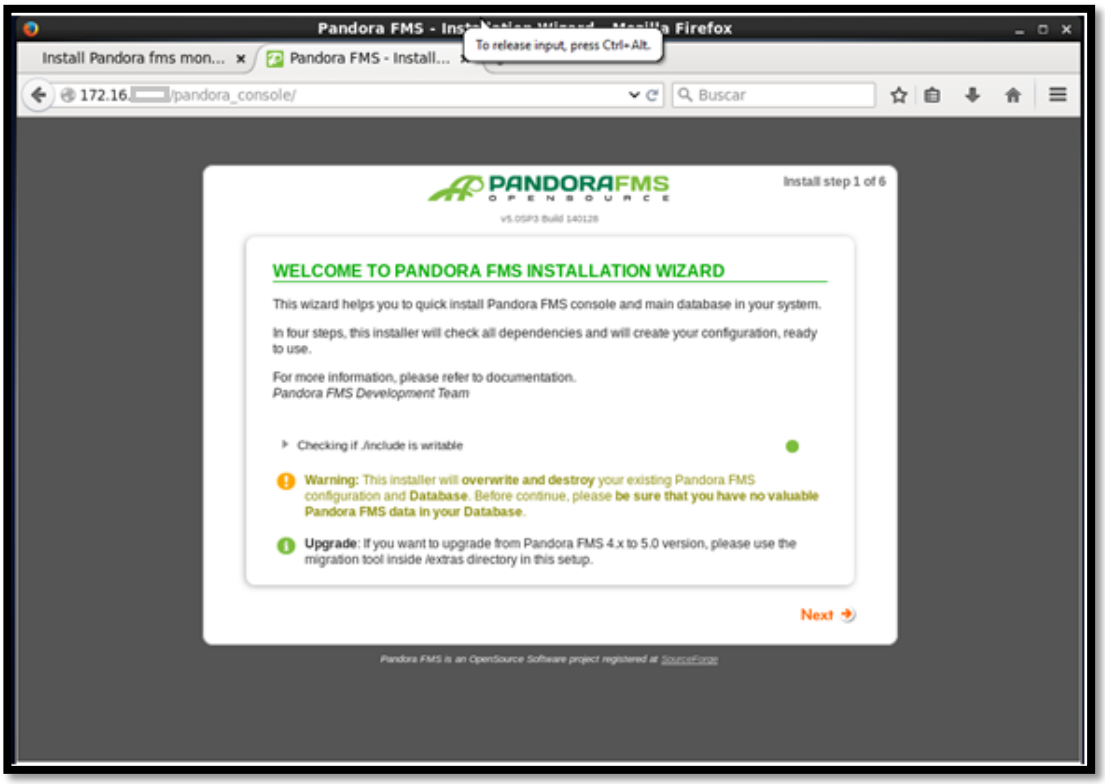


Figura C 19. Pantalla inicial de la Consola de Pandora FMS

Fuente: Consola Pandora FMS

Nota: Para empezar a configurar la consola es necesario que se encuentre instalado los paquetes de Apache y MySQL

- Aceptar las Condiciones de Uso

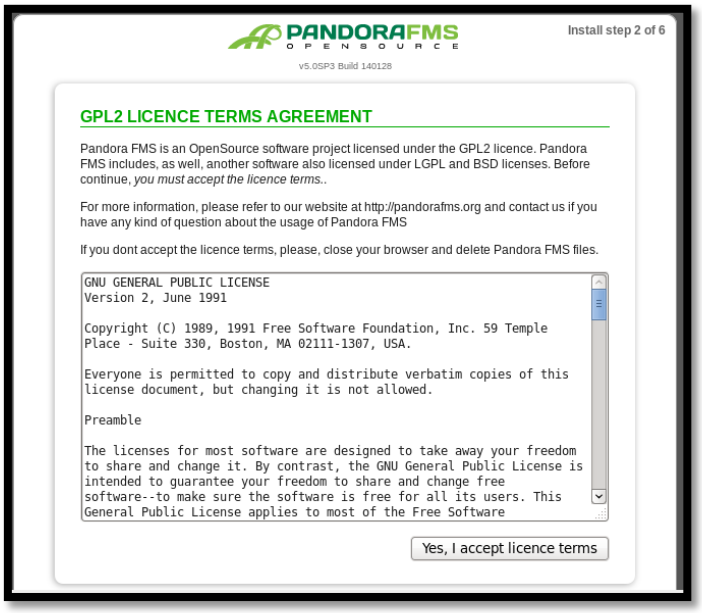


Figura C 20. Condiciones de Uso

Fuente: Consola Pandora FMS

- A continuación el sistema verifica las instalaciones necesarias

Figura C 21. Verificación de paquetes instalados

Fuente: Consola Pandora FMS

- Colocar los datos de la base de datos

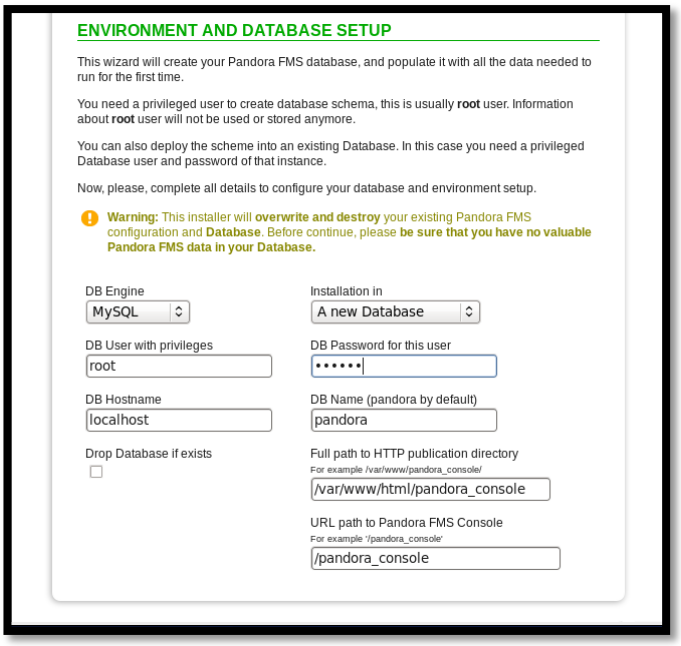


Figura C 22. Ingreso de información de la base de datos

Fuente: Consola Pandora FMS

- A continuación se visualiza la información de la base de datos creada

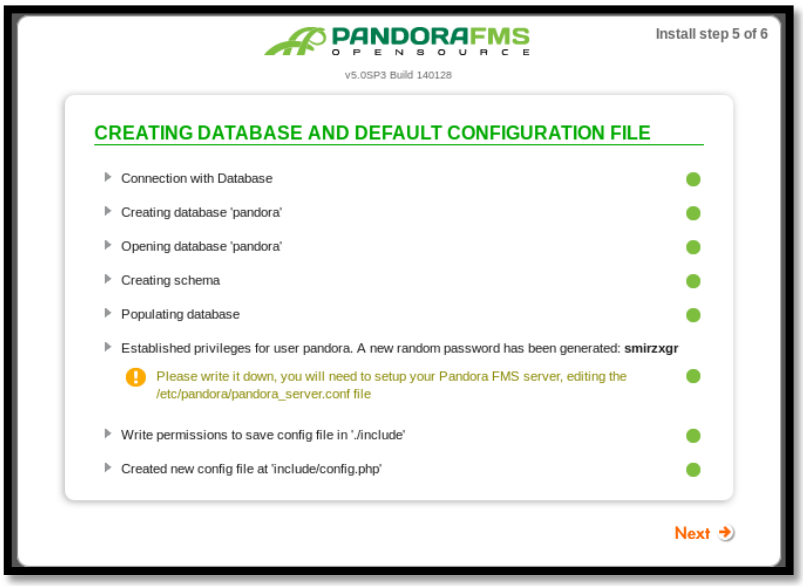


Figura C 23. Visualización de la base de datos creada

Fuente: Consola Pandora FMS

- Finalizada la instalación hacer clic para entrar a la consola de pandora

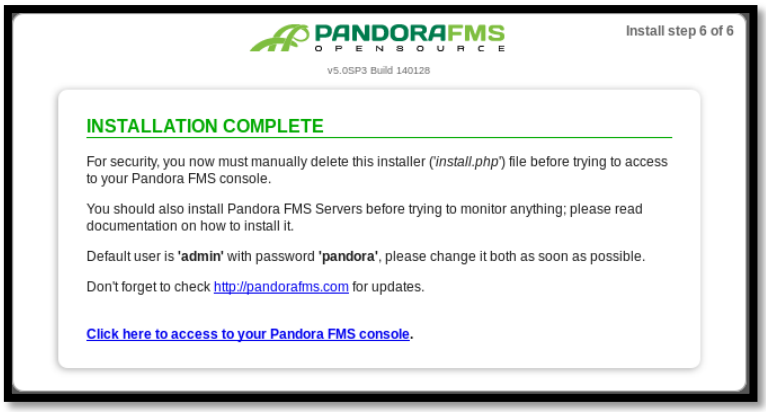


Figura C 24. Instalación finalizada de la Consola

Fuente: Consola Pandora FMS

Figura C 25. Instalación Activa de la Consola de Pandora FMS

Fuente: Consola Pandora FMS

Nota: Luego de finalizada la instalación para iniciar la consola Pandora FMS es necesario borrar el archivo install.php caso contrario no se podrá acceder a la consola y saldrá el mensaje de advertencia mostrado en la Figura C25.

Figura C 26. Advertencia de Inicio de la Consola de Pandora FMS

Fuente: Consola Pandora FMS

- Este archivo está ubicado en la carpeta mostrada a continuación, se debe entrar en la carpeta y borrar el archivo mencionado

```
/var/www/html/pandora_console
```

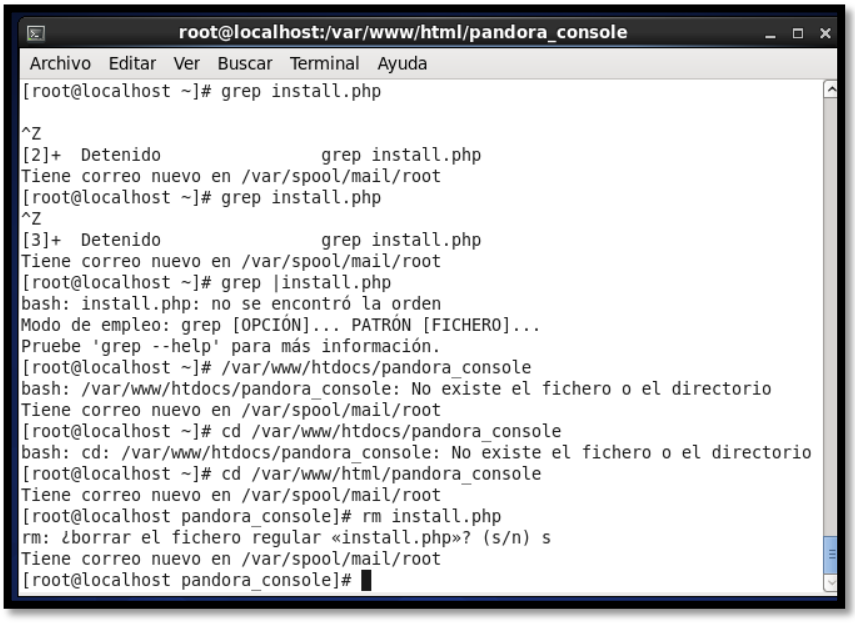


Figura C 27. Borrar archivo install.php

Fuente: Consola Pandora FMS

- Para ingresar a la consola en el navegador web se debe ingresar la siguiente dirección

ipdelhost/pandora_console/index.php

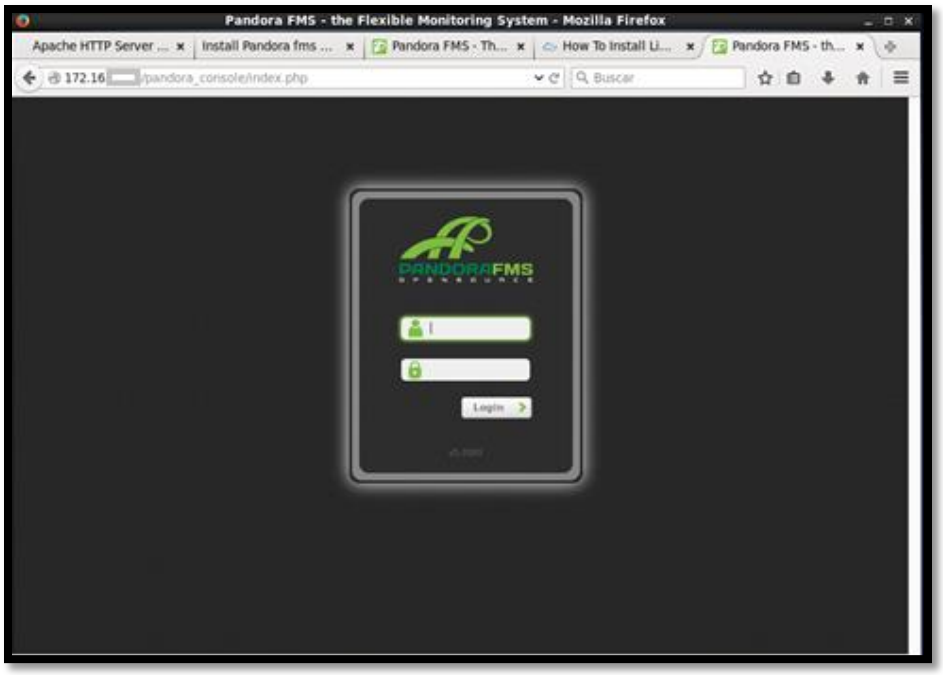


Figura C 28. Pantalla inicial de la Consola de Pandora FMS

Fuente: Consola Pandora FMS

- Ingresar el nombre de usuario y contraseña por defecto que brinda pandora

Usuario: admin Password: pandora

Figura C 29. Ingreso a la Consola de Pandora FMS

Fuente: Consola Pandora FMS

- A continuación se abre la consola de pandora para iniciar el monitoreo

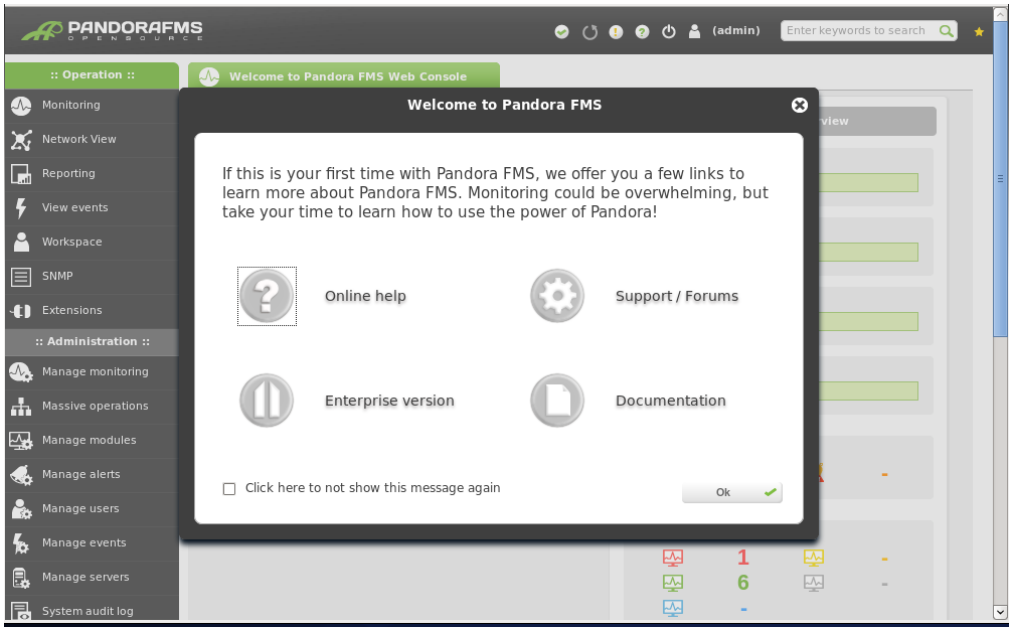


Figura C 30. Pantalla Inicial Consola Pandora FMS

Fuente: Consola Pandora FMS

C4.Configuración Agente Linux

- En el caso de la Prefectura de Imbabura todos los servidores se encuentran en modo consola por lo tanto para descargar un archivo se debe buscar la dirección en los repositorio de Pandora el cual nos va a permitir obtener el paquete para el agente.

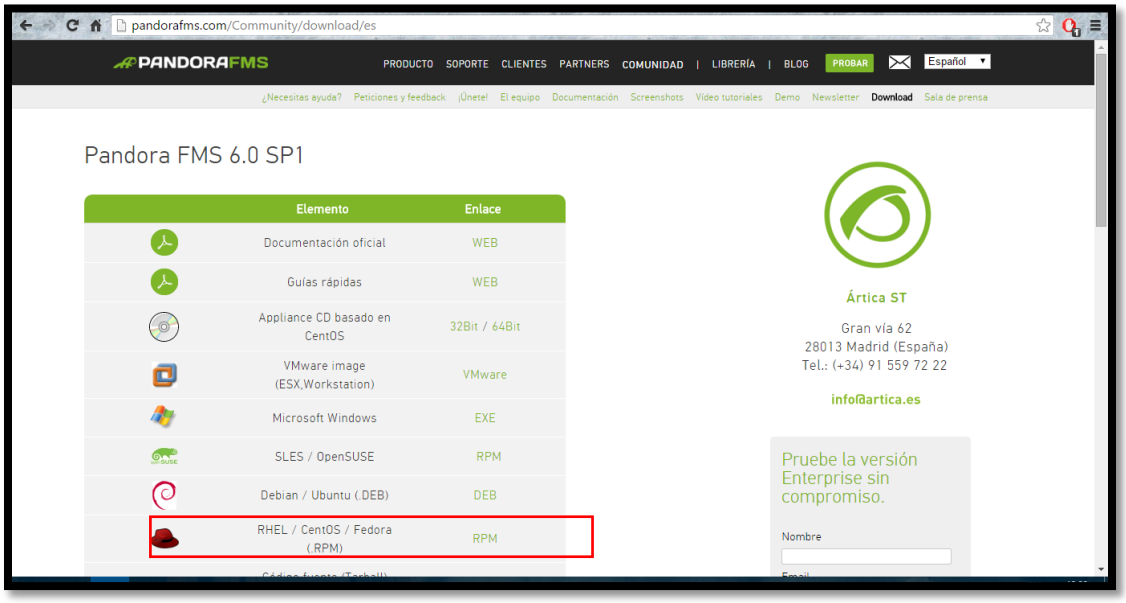


Figura C 31. Página para descarga del Agente de Pandora FMS

Fuente: Consola Pandora FMS

- En este caso se escoge el paquete RPM para CentOS y de esta manera se obtiene la dirección para descargar el agente

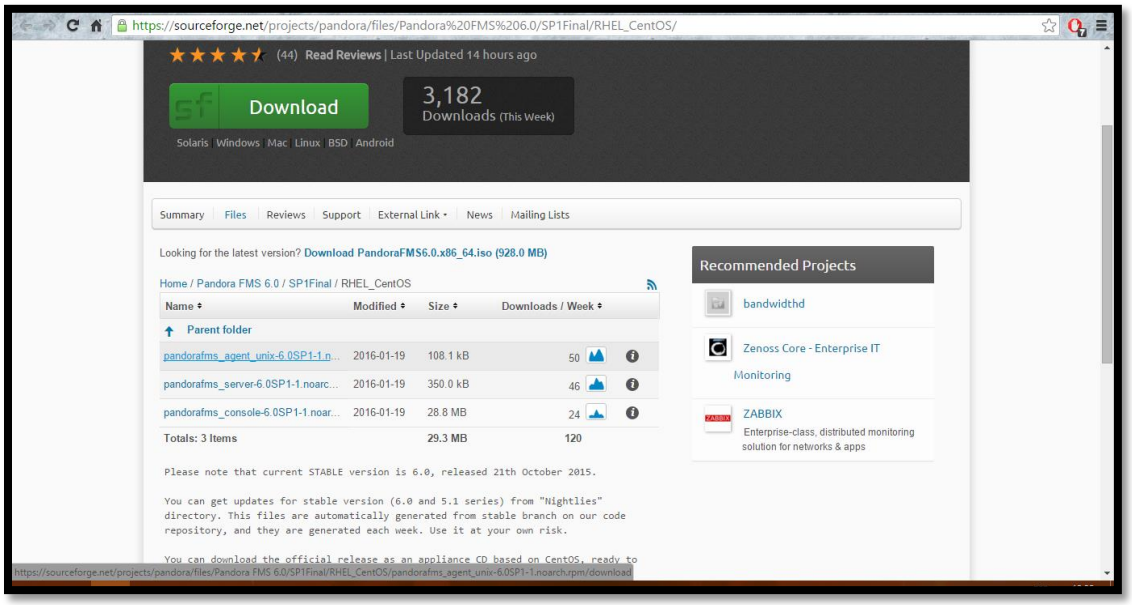


Figura C 32. Link para la descarga del archivo rpm

Fuente: Consola Pandora FMS

- Con el comando wget se obtiene el paquete en la consola de CentOS

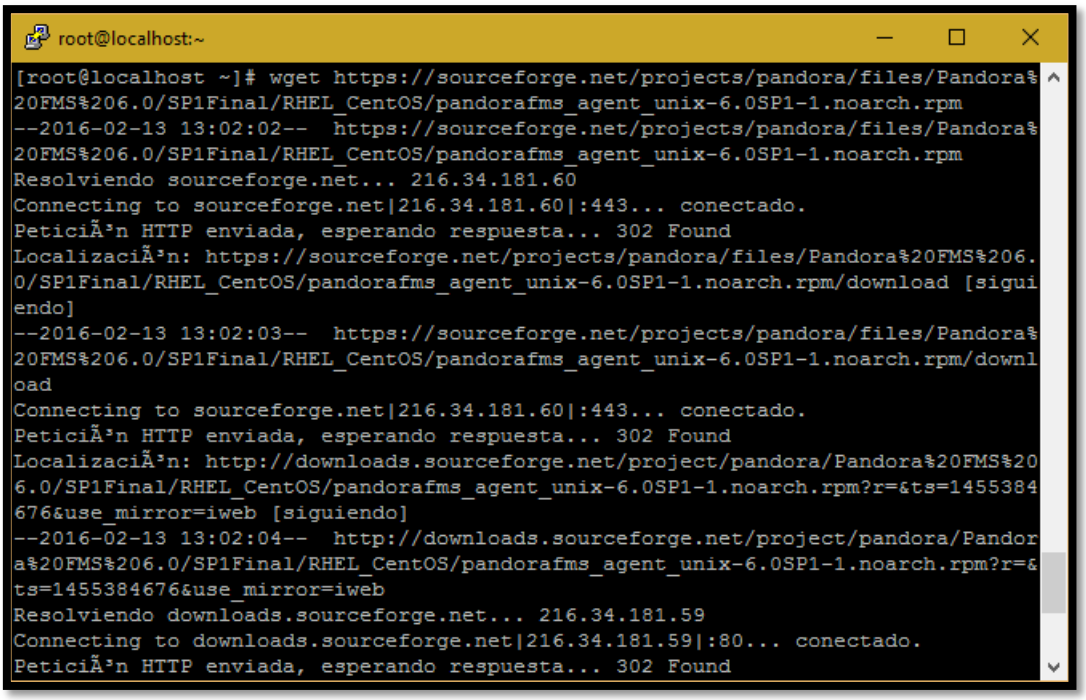


Figura C 33. Descarga de archivo rpm

Fuente: Consola Pandora FMS

C5.Configuración Agente Windows

- Descargar el agente para el Sistema Operativo Windows desde la página oficial de Pandora FMS

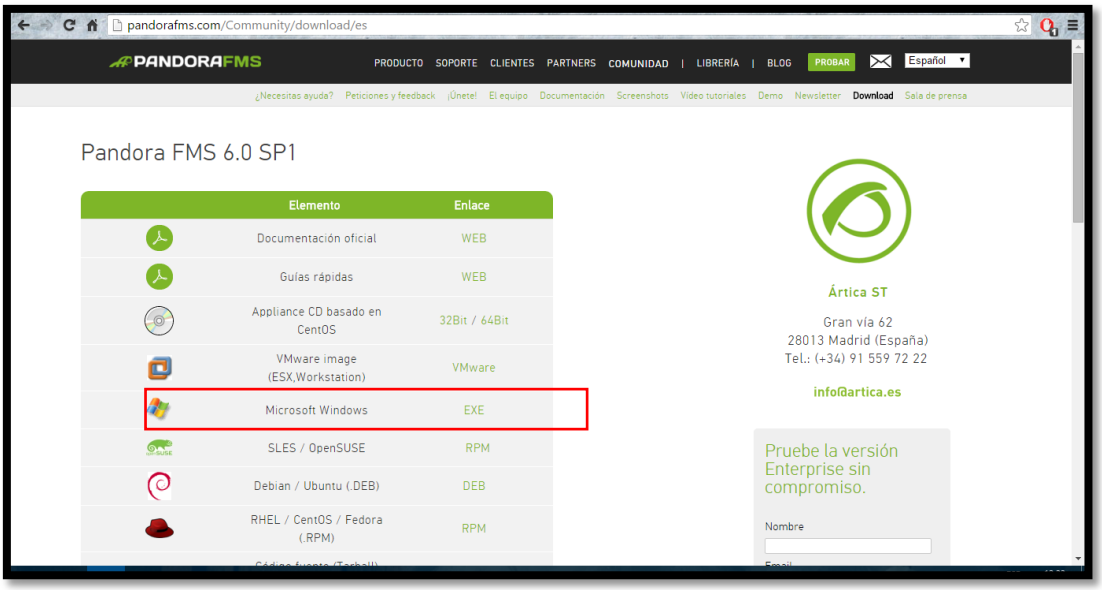


Figura C 34. Página para descarga del Agente de Pandora FMS

Fuente: Consola Pandora FMS

- Ejecutar el archivo .exe descargado

Figura C 35. Icono de archivo .exe de agente de Pandora FMS

Fuente: Escritorio Windows 10

- Escoger el idioma para la instalación

Figura C 36. Idioma para la instalación

Fuente: Agente Pandora FMS

- Presionar siguiente en la pantalla inicial de la instalación de Pandora FMS

Figura C 37. Pantalla Inicial Instalación Agente Pandora

Fuente: Agente Pandora FMS

- Aceptar el Acuerdo de Licencia

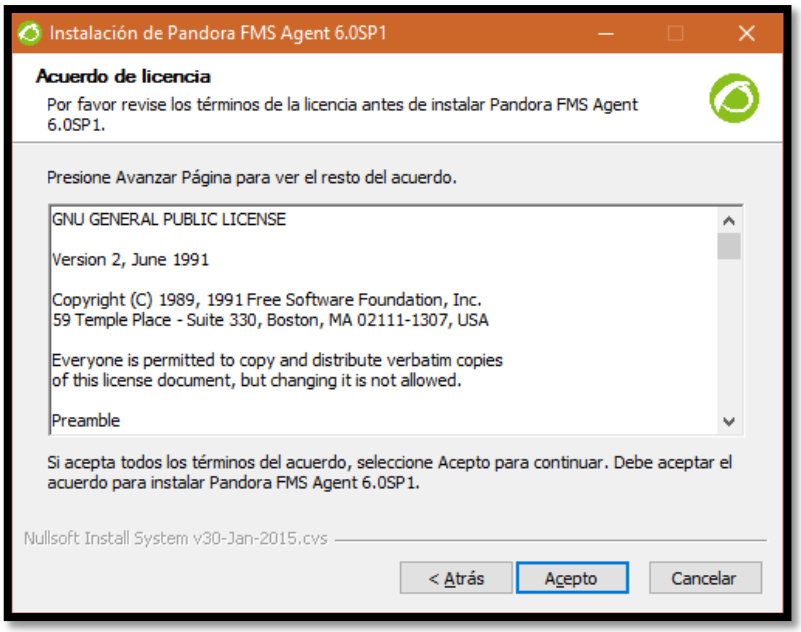


Figura C 38. Acuerdo de Licencia Pandora FMS

Fuente: Agente Pandora FMS

- Escoger el directorio en el cual se va a guardar el agente.

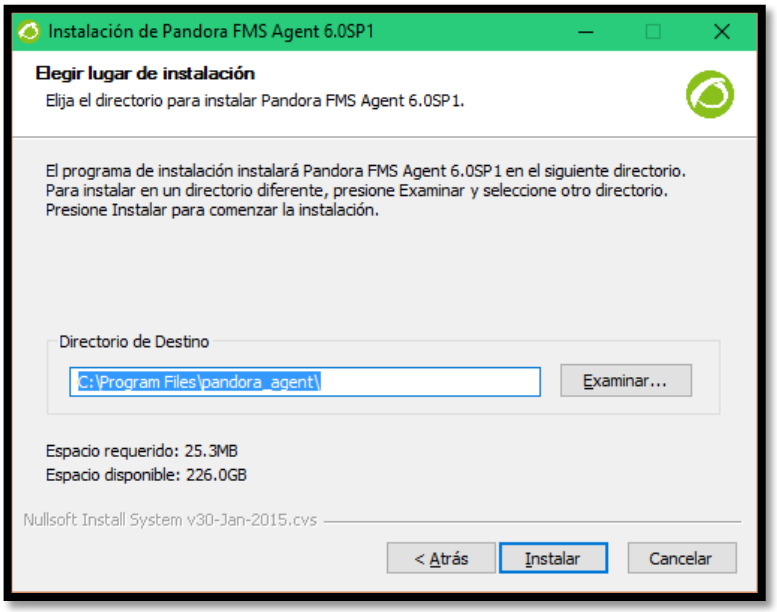


Figura C 39. Escoger directorio para guardar el agente Pandora

Fuente: Agente Pandora FMS

- Esperar mientras se instalan los componentes del agente

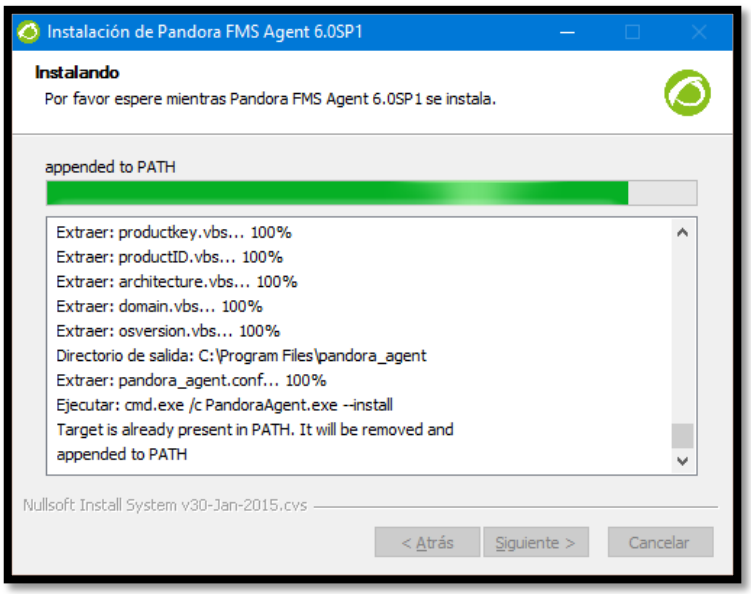


Figura C 40. Instalación de componentes agente Pandora FMS

Fuente: Agente Pandora FMS

- Escribir los datos del Servidor Pandora FMS

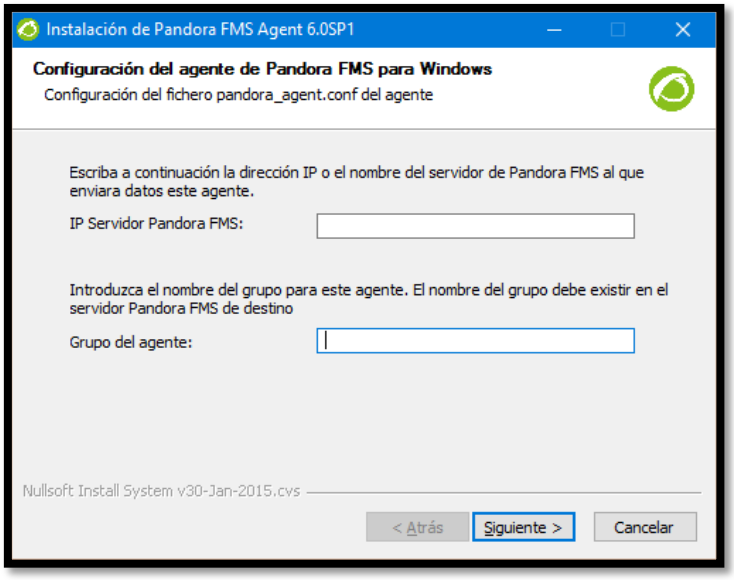


Figura C 41. Ingreso de Datos Servidor Pandora FMS

Fuente: Agente Pandora FMS

- Finalizar la instalación

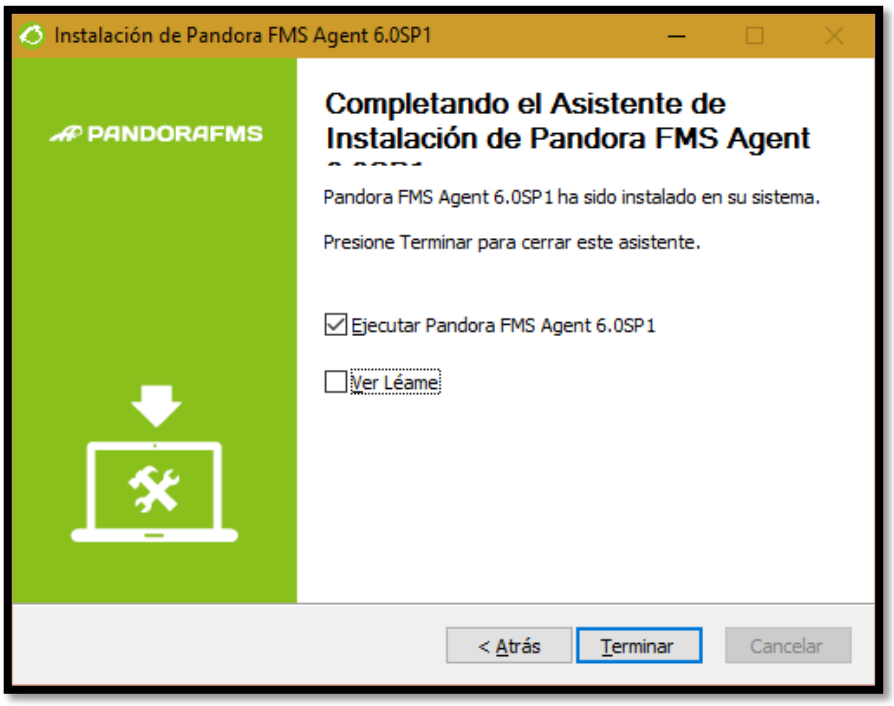


Figura C 42. Instalación finalizada del agente Pandora FMS

Fuente: Agente Pandora FMS

C6.Creación del Barrido de la Red

- Para que aparezcan los servidores que se van a monitorear en la red es necesario crear un barrido de la red para esto se debe dirigir al Menú Administration, escoger el menú Manage Servers y la opción Manage recontask.

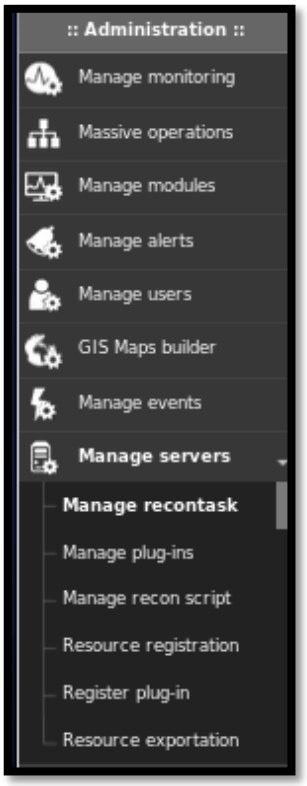


Figura C 43. Escoger Recontask

Fuente: Consola Pandora FMS

- Crear las opciones para el barrido de la red de los diferentes tipos de equipos que se van a monitorear, haciendo clic en el botón Create

Figura C 44. Botón Create de Recontask

Fuente: Consola Pandora FMS

- Dentro de esta ventana se crea las diferentes tareas de barrido.

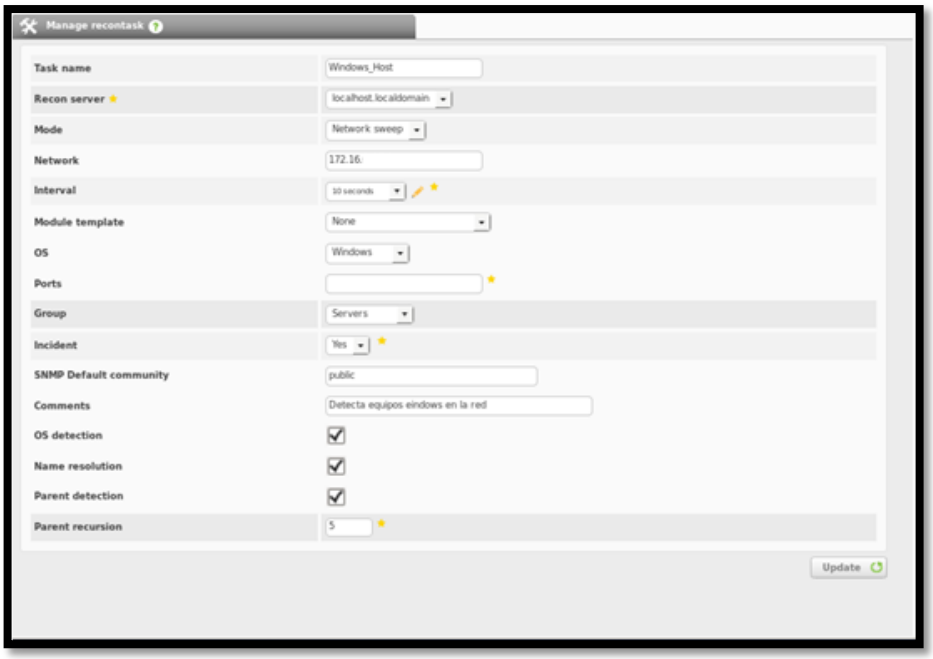


Figura C 45. Creación de barrido equipos Windows

Fuente: Consola Pandora FMS

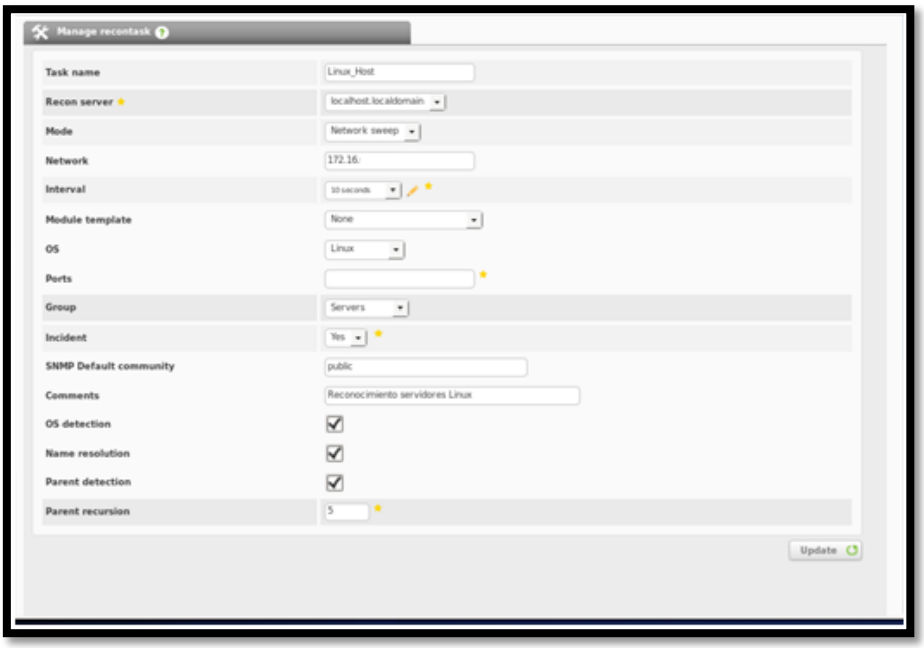


Figura C 46. Creación de barrido equipos Linux

Fuente: Consola Pandora FMS

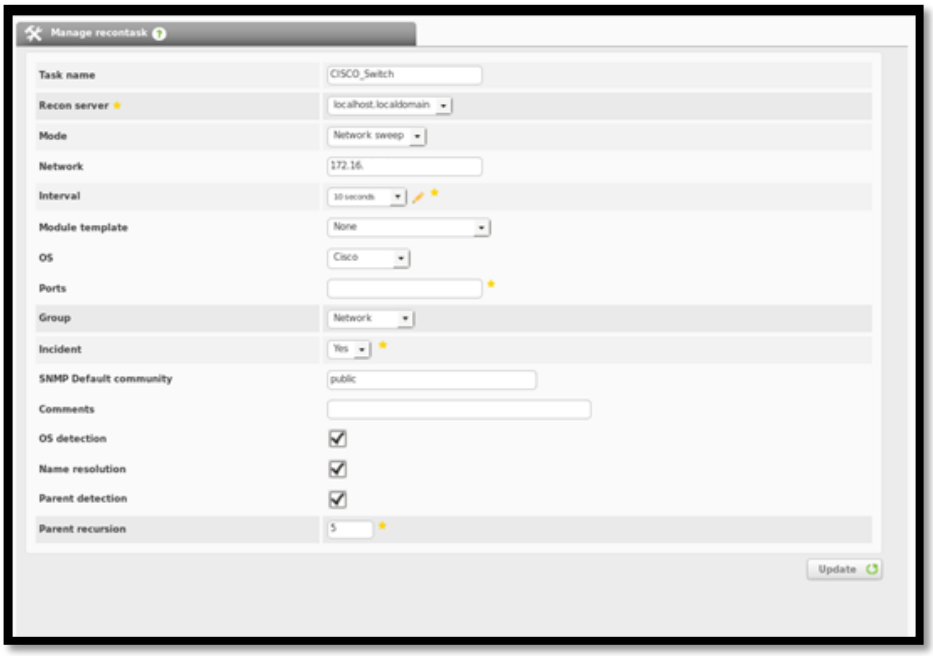


Figura C 47. Creación de barrido equipos CISCO

Fuente: Consola Pandora FMS

Figura C 48. Creación de barrido equipos CISCO

Fuente: Consola Pandora FMS

Nota: En el caso de la red de la Prefectura de Imbabura se ha creado tres opciones de barrido para los tipos de equipos que son Windows, Linux y CISCO. Y un reconocimiento de dispositivos que tengan activado SNMP.

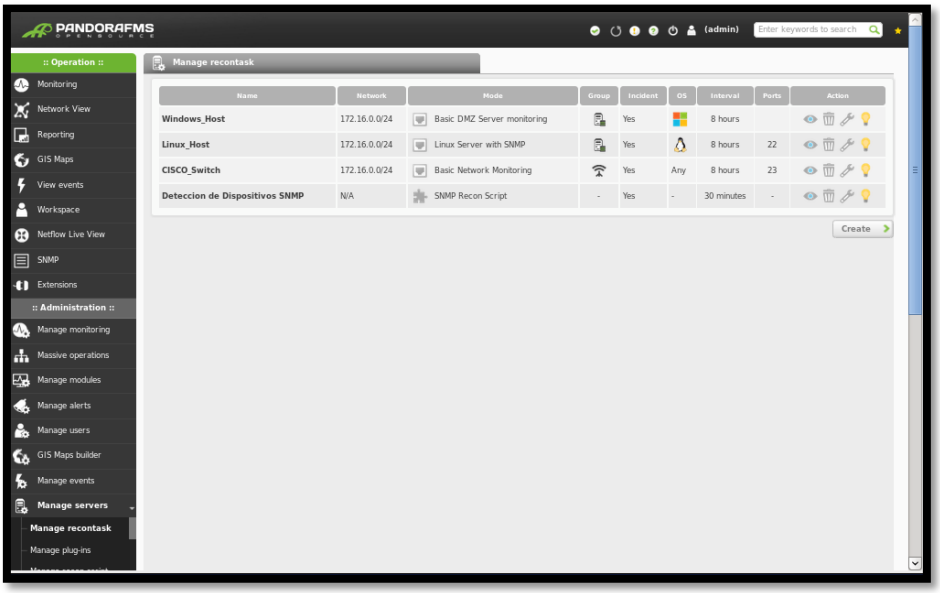


Figura C 49. Tareas de barrido creadas

Fuente: Consola Pandora FMS

C7.Creación de un agente

- Si luego de haber creado las tareas de barrido de red ciertos dispositivos aún no aparecen Pandora FMS brinda la posibilidad de crear agentes directamente para esto es necesario dirigirse al Menú Administration, Manage Monitorins

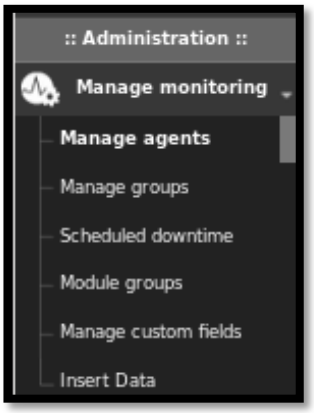


Figura C 50. Escoger Manage agents

Fuente: Consola Pandora FMS

- Como ejemplo de esta creación se añadió el agente Servidor Web

Figura C 51. Creación de Agente Servidor Web

Fuente: Consola Pandora FMS

- En la figura se pueden observar los agentes creados o los añadidos mediante el barrido de la red.

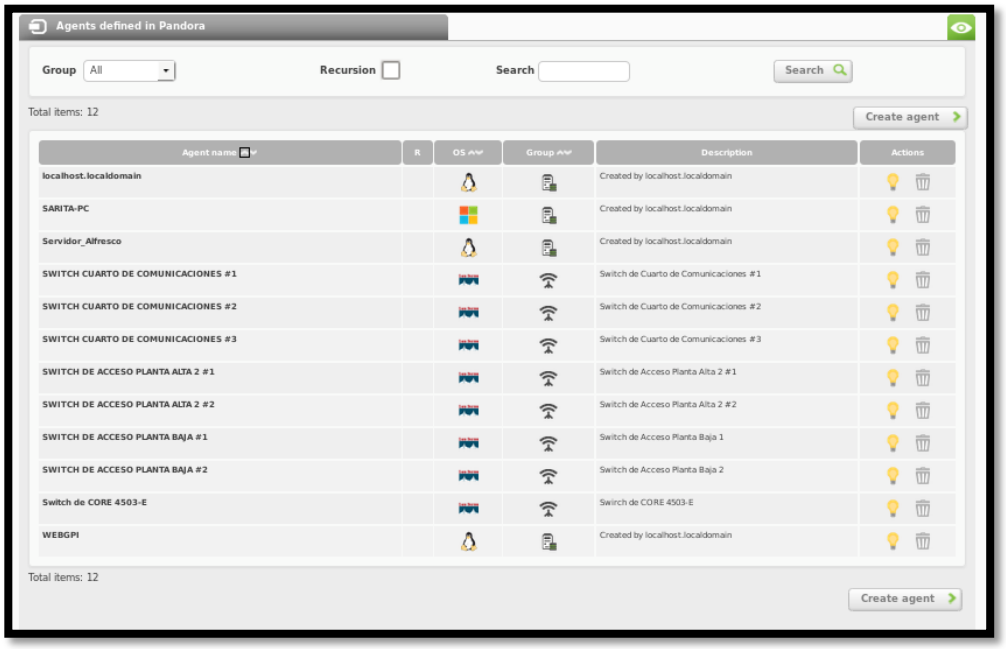


Figura C 52. Agentes que aparecen en la Consola de Pandora FMS

Fuente: Consola Pandora FMS

C8.Creación de Módulos de Monitoreo

- Para asignar los valores a monitorizar se debe acceder al menú Manage Monitoring y escoger el agente a gestionar, a continuación se utiliza la opción modules

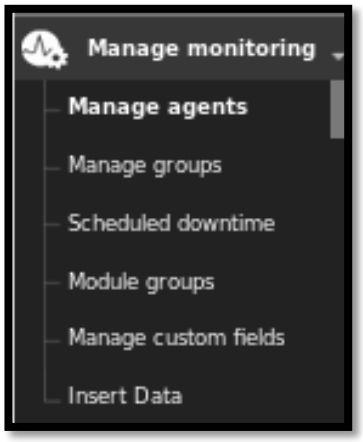


Figura C 53. Escoger Manage agents

Fuente: Consola Pandora FMS

- Escoger la opción crear a new data server module

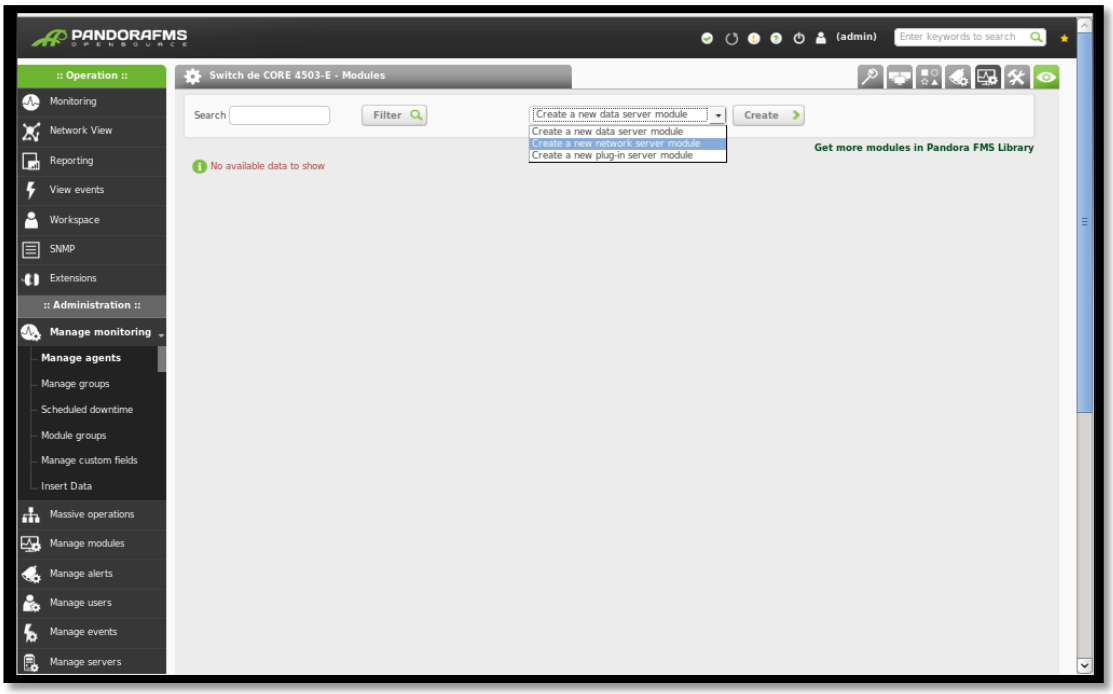


Figura C 54. Tipo de Modulo a crearse

Fuente: Consola Pandora FMS

- En tipo se debe seleccionar el tipo de dato a obtener

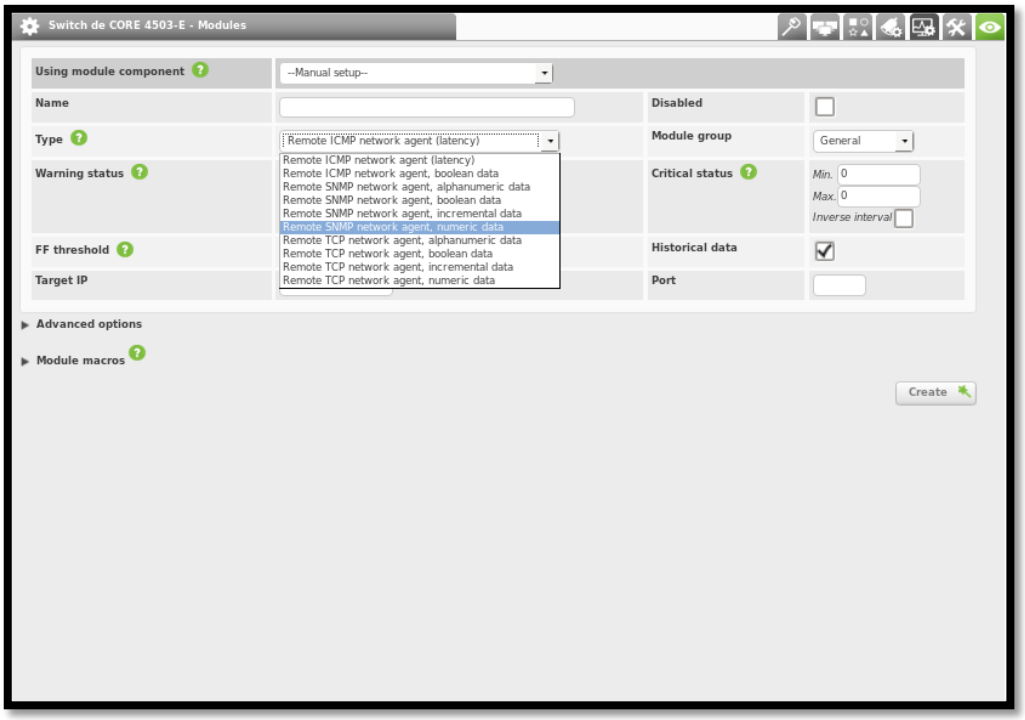


Figura C 55. Tipo de dato a obtener

Fuente: Consola Pandora FMS

- Las posibilidades para SNMP son:

  - ***Remote SNMP network agent, alphanumeric data:*** texto
  - ***Remote SNMP network agent, Boolean data:*** si/no, true/false, 1/0
  - ***Remote SNMP network agent, incremental data:*** número incremental que siempre va creciendo. Por ejemplo, para un Switch en el caso del monitor o módulo para obtener los bytes enviados y bytes recibidos en una boca.
  - ***Remote SNMP network agent, numeric data:*** número

- Introducir los demás datos para el agente.

  - **Nombre:** nombre descriptivo del agente a monitorearse.
  - **IP objetivo:** debe aparecer la IP utilizada al crear el agente, si no aquí se debe ingresar la IP del equipo a monitorear.
  - **Umbral Warning, Umbral Crítico:** en este lugar se establece los valores que se consideren harían cambiar el estado del módulo sea este de advertencia o crítico, según estos niveles se disparan las alarmas.
  - **Comunidad SNMP:** nombre de la comunidad a la que se tiene acceso, por defecto suele ser “public”.
  - **SNMP OID:** introducir el MIB OID del valor SNMP del que se desee obtener los datos.
  - **SNMP versión:** versión del protocolo SNMP soportada por el dispositivo del cual se quieren obtener los datos.

C9. Tipos de Vistas para el Monitoreo

- **Vista de agente / modulo:** Esta sección muestra una tabla con los módulos y los agentes y el estado de cada módulo. Se accede desde el Menú Monitoring - Views - Agents/Modules view.

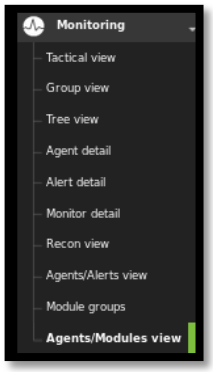


Figura C 56. Menú Vista de agente/modulo

Fuente: Consola Pandora FMS

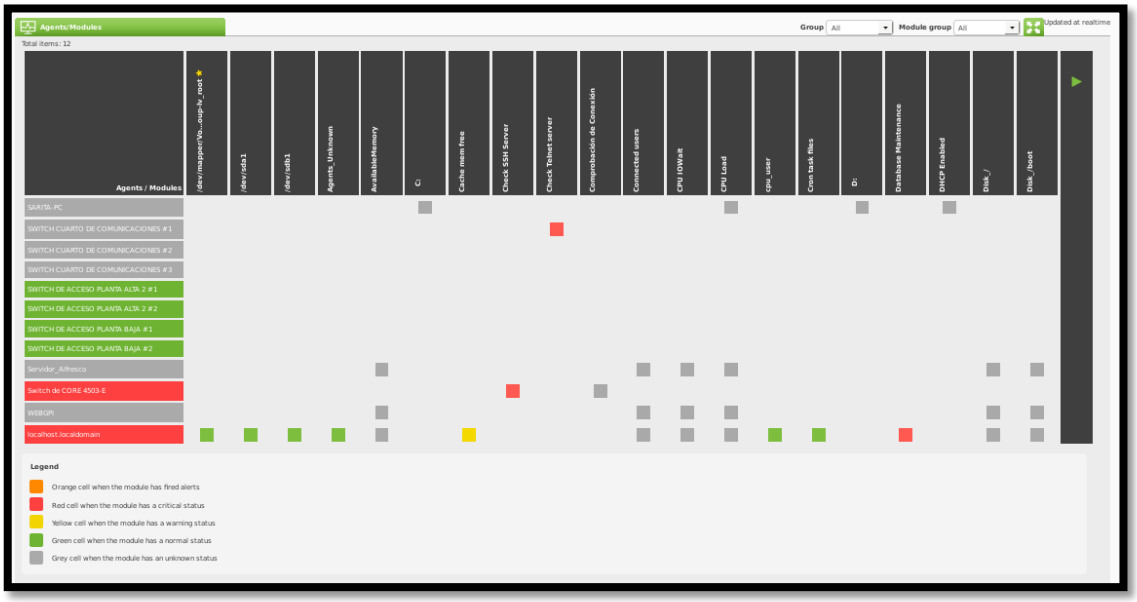


Figura C 57. Vista agente/modulo

Fuente: Consola Pandora FMS

- **Vista de grupos de módulos:** Esta sección permite tener una visión total en una tabla de los módulos por su estado, en función del module group y el grupo. Se accede a esta opción desde Monitoring - Module groups como se muestra en la Figura D38.

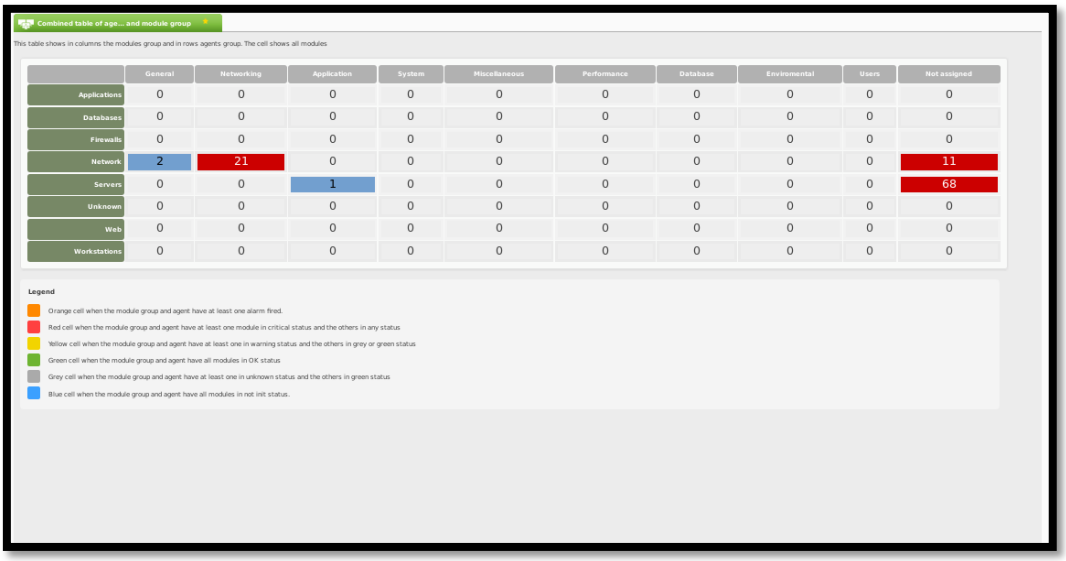


Figura C 58. Vista de grupos de módulos

Fuente: Consola Pandora FMS

Como se observa en la Figura, se ve una matriz con el número de módulos por grupo de agentes y con diferentes colores según haya módulos en estado Critical, Warning o OK.

- **Vista de árbol:** Esta vista permite la visualización de los monitores de los agentes en forma de árbol. Se accede a través de Monitoring - Tree view como se muestra en la Figura D38.

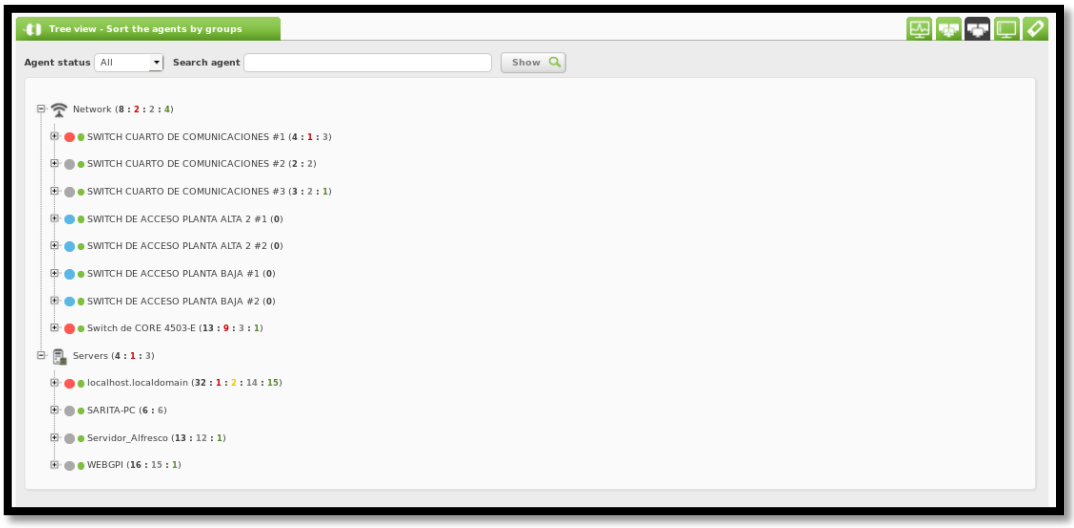


Figura C 59. Vista de árbol

Fuente: Consola Pandora FMS

- Es posible ordenar los agentes por: Módulos, Políticas, Grupo de Módulos, Grupo y Sistema Operativo. La vista por defecto es la ordenada por grupos. En este nivel, se muestra un recuento del número de agentes en estado normal (color verde), critical (color rojo), warning (color amarillo) y unknown (color gris). Pinchando sobre el nombre del agente, aparece a la derecha información sobre el mismo: nombre, ip, fecha de la última actualización, sistema operativo, etc; así como una gráfica de eventos y otra de accesos.

- Se puede filtrar por estado del módulo (Critical, Normal, Warning y Unknown) y realizar búsquedas por nombre de agente.

C10. Generación de Reportes

Con Pandora FMS es posible crear informes personalizados con información de los agentes, se puede seleccionar, igual que con las gráficas de usuario, diferentes módulos de diferentes agentes. Los datos se visualizan de diferentes formas en función del tipo de elemento de informe que se desee añadir.

- **Creación de un reporte:** Para añadir un reporte se va a Reporting - Custom reporting. Aparece una lista con todos los informes creados, para crear un informe se debe hacer click en “Create Report”

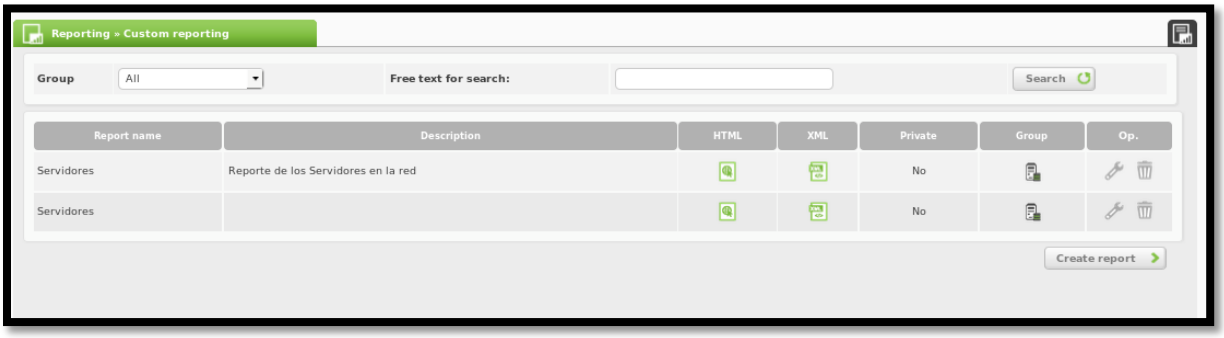


Figura C 60. Creación de Reportes

Fuente: Consola Pandora FMS

- A continuación aparece un formulario donde se puede poner el nombre del informe y seleccionar el grupo al que pertenece, también si el informe es privado o no y la descripción del mismo. Cuando los campos estén llenos pulsar en el botón Save.

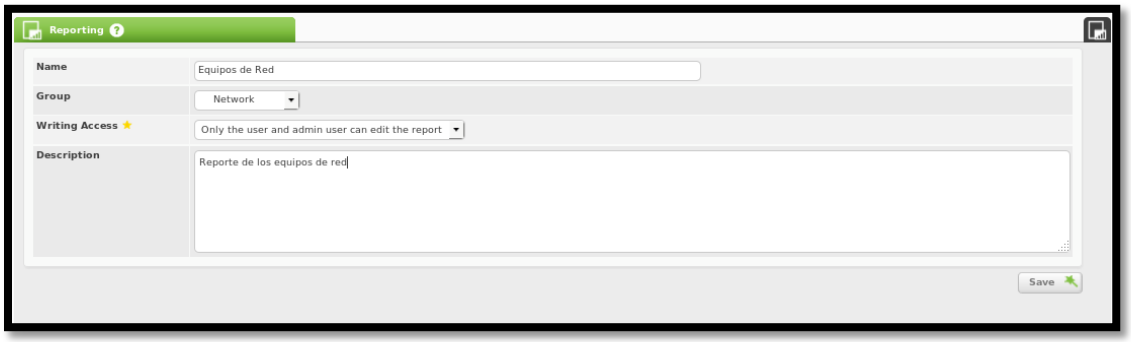


Figura C 61. Formulario para creación de reporte

Fuente: Consola Pandora FMS

- **Edición de un informe:** Para editar un Informe se va a Reporting - Custom Reporting. Aparece una lista con todos los informes creados, para editar un informe se pulsa en el nombre del informe, y para crear los ítems a mostrar se escoge la pestaña List Ítems y aquí se puede crear los reportes que se necesita de acuerdo a las necesidades del administrador de la red

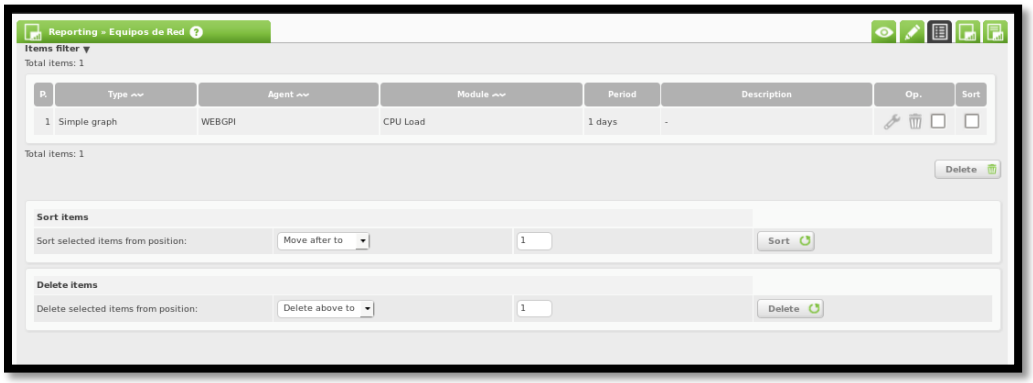


Figura C 62. Ítem List de reports

Fuente: Consola Pandora FMS

- Si es un informe extenso es decir tiene demasiados ítems, dispone en la parte de arriba un formulario para filtrar por distintos criterios. Para la documentación se muestra el ítem de Carga de CPU del Servidor Web de la Prefectura de Imbabura en diferentes fechas de monitoreo.

Figura C 63. Carga de CPU del Servidor Web

Fuente: Consola Pandora FMS

Figura C 64. Carga de CPU del Servidor Web

Fuente: Consola Pandora FMS

ANEXO D. PLANTILLA DE DOCUMENTACIÓN DE FALLAS

PREFECTURA DE IMBABURA	**REPORTE DE FALLAS – DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN**			
Reportado por: Edgar Martínez	Número de Reporte: 1			
Área / Departamento: TIC's	Fecha:23/02/2015	Hora: 14:20		
Descripción del Problema : Se notifico a la Dirección que no se podía accedder a la página Web de la Prefectura de Imbabura				
Posibles Causas:				
Tipo de Fallo	Red	PC	Impresora	Otros
Nivel de Criticidad	Poco	Algo	Crítico	Muy Crítico
Medidas de aislamiento tomadas: se verificó en el software de monitoreo todos los módulos para identificar la falla				
Solución: Se encontró que se había excedido el número de procesos en el servidor, para lo cual se reinicio el mismo, de esta manera se logro ingresar nuevamente a la página web de la institución				
Solucionado por: Edgar Martínez	Tiempo Empleado: 2 horas			
Observaciones:				

ANEXO E. PLANOS DE INFRAESTRUCTURA FÍSICA

PREFECTURA DE IMBABURA

Ibarra, 02 de marzo del 2016

Ing. Fernando Miño Ortega, Director de Tecnologías de la Información del Gobierno Provincial de Imbabura.

CERTIFICADO:

La Dirección de Tecnologías de la Información del Gobierno Provincial de Imbabura certifica que el proyecto de Tesis "GESTION Y MONITOREO DE LA RED INTERNA DEL GOBIERNO PROVINCIAL DE IMBABURA MEDIANTE EL MODELO DE GESTION ISO Y SOFTWARE LIBRE" propuesto por la Srta. Cuchala Vasquez Sara Carolina, con número de cédula 1003155973, estudiante de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, ha sido revisado e implementado en esta Institución y de esta manera cumple con el objetivo del proyecto propuesto.

Atentamente,

Ing. Fernando Miño Ortega
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN
GOBIERNO PROVINCIAL DE IMBABURA