UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"SISTEMA DE GESTIÓN DE RED BASADO EN EL MODELO FUNCIONAL SNMP DE LA IETF PARA MONITOREAR LOS RECURSOS DE LA RED LAN EN EL EDIFICIO DE EMAPA-I DE LA CIUDAD DE IBARRA"

TRABAJO PREVIO A LA OBTENCION DEL TÍTULO DE INGENIERÍA

EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: RICHARD ARMANDO MALLAMAS TITUAÑA

DIRECTOR: MSc. EDGAR MAYA

IBARRA – ECUADOR

2016

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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 determina 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 sentado mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
CÉDULA DE IDENTIDAD	1002956421
APELLIDOS Y NOMBRES	MALLAMAS TITUAÑA RICHARD ARMANDO
DIRECCIÓN	LUCIO PÁEZ Y ABELARDO MORAN 4-86
E-MAIL	richard_mallamas@hotmail.com
TELÉFONO FIJO	062-631-320
TELÉFONO MÓVIL	0985155075

DATOS DE LA OBRA	
TÍTULO	SISTEMA DE GESTIÓN DE RED BASADO EN EL MODELO FUNCIONAL SNMP DE LA IETF PARA MONITOREAR LOS RECURSOS DE LA RED LAN EN EL EDIFICIO DE EMAPA-I DE LA CIUDAD DE IBARRA
AUTOR	MALLAMAS TITUAÑA RICHARD ARMANDO
FECHA	ABRIL DEL 2016
PROGRAMA	PREGRADO
TÍTULO POR EL QUE SE OPTA	INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
DIRECTOR	MSc. EDGAR MAYA

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Richard Armando Mallamas Tituaña, con cédula de identidad Nro. 1002956421, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en 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. CONSTANCIA

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

En la ciudad de Ibarra, Abril de 2016

El Autor:
Richard Armando Mallamas Tituaña
CI.:1002956421

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, Richard Armando Mallamas Tituaña, con cédula de identidad Nro. 1002956421, 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 "**SISTEMA DE GESTIÓN DE RED BASADO EN EL MODELO FUNCIONAL SNMP DE LA IETF PARA MONITOREAR LOS RECURSOS DE LA RED LAN EN EL EDIFICIO DE EMAPA-I DE LA CIUDAD DE IBARRA**", que ha sido desarrollado para optar por el título de Ingeniera en Electrónica y Redes de Comunicación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en el formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

Firma

Nombre: Richard Armando Mallamas Tituaña

CI.:1002956421

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Richard Armando Mallamas Tituaña, declaro bajo juramento que el trabajo aquí escrito es de mi autoría; que 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 normativa vigente de la Universidad Técnica del Norte.

Firma

Nombre: Richard Armando Mallamas Tituaña

CI.:1002956421

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación "**SISTEMA DE GESTIÓN DE RED BASADO EN EL MODELO FUNCIONAL SNMP DE LA IETF PARA MONITOREAR LOS RECURSOS DE LA RED LAN EN EL EDIFICIO DE EMAPA-I DE LA CIUDAD DE IBARRA**" fue desarrollado en su totalidad por el Sr. Richard Armando Mallamas Tituaña, bajo mi supervisión.

MSc. Edgar Maya
DIRECTOR DE TESIS

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE
Y ALCANTARILLADO DE IBARRA

Ibarra, 17 de Diciembre del 2015

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Ibarra, por medio de la unidad de hardware y redes de datos.

CERTIFICA

Que el Sr. Mallamas Tituaña Richard Armando con C.I. 1002956421, realizó el tema de tesis: **"Sistema de gestión de red basado en el modelo funcional SNMP de la IETF para monitorear los recursos de la red LAN en el edificio de EMAPA-I de la ciudad de Ibarra"**. Los aplicativos referentes a este tema se encuentran operativos y funcionales por lo que se recibe el proyecto como culminado.

Es todo lo que podemos informar en honor a la verdad, dando potestad de uso del presente certificado dentro de los términos legales, en todo lo que sea necesario.

Atentamente,

EMPRESA PÚBLICA EMAPA-I
HARDWARE Y REDES

.....
Ing. Dario Páez
JEFE (E) TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EMAPA-I

DEDICATORIA

Este proyecto de titulación lo quiero dedicar a Dios, por haberme dejado alcanzar esta meta rodeado de la gente que tanto amo, mi familia, que son como ángeles que han llenado mi vida en cada momento.

Richard Mallamas

AGRADECIMIENTOS

Un agradecimiento muy especial a Dios por haberme dado tantas lecciones en estos últimos años, por ser mi fuerza y mi apoyo incondicional, gracias por tantas bendiciones recibidas. También quiero agradecer a mi familia, mis amigos, mis profesores, a la Universidad Técnica del Norte y a la empresa EMAPA-I, los cuales fueron parte importante en la elaboración de este proyecto. Imposible decir todos los nombres de las personas que participaron en el cumplimiento de este objetivo de vida, pero también es imposible dejar de mencionar a algunos como:

Mi mami Lucy y mi papá Marco, los cuales han sido el impulso para seguir adelante con sus tan humildes pero grandes consejos, por su amor, el que me ha llenado la vida de grandes bendiciones; además un agradecimiento a los amiguitos: Tony y Daya, que trajeron al mundo un nuevo miembro a la familia, el cual va inundando nuestros corazones con su alegría.

A la universidad técnica del norte por brindarme tantos conocimientos y experiencias únicas e inigualables, a sus profesores que han sido tanto una guía de conocimientos como de valores, los llevaré por siempre en mi corazón; en especial un agradecimiento a mi director de tesis, MSc. Edgar Maya, por sus consejos, por ayudarme a encaminar el tema de este proyecto y de igual forma a llevarlo a su culminación, con las pautas y lineamientos que hacían faltan.

A la empresa EMAPA-I, en especial al Ing. Danilo Maldonado y al Ing. Darío Páez, que tan humildemente me abrieron las puertas de la institución y que participaron tan amablemente en el desarrollo de este proyecto, simplemente fue un placer haber compartido tanto en esta institución a la cual le quedare infinitamente agradecido.

Por último y no por ello menos importante, quiero agradecer a los que considero mis amigos: Andrés y Diana, aunque no los vea seguido, siempre los tengo presentes, muchas de las cosas aprendidas juntos me ha llevado hasta aquí, gracias por tanto.

Richard Mallamas

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto consiste en diseñar un sistema de monitorización basado en el modelo funcional SNMP utilizando herramientas Open Source en un servidor proporcionado por EMAPA-I con el propósito de optimizar el desempeño de su red LAN y mejorar la productividad tecnológica de la institución.

En el primer capítulo se recopila la información relacionada con la administración de red y monitoreo basado en SNMP, se investiga sus funciones de operación, administración y mantenimiento, así como también se explicará las razones que motivaron al diseño de este proyecto indicando su importancia.

En el segundo capítulo se realiza el levantamiento de información del estado y ubicación de los equipos y servidores de la red LAN de EMAPA-I. Se documenta que equipos soportan el protocolo snmpv2 y se elabora un inventario de la información obtenida.

En el tercer capítulo se procede con la configuración del sistema de gestión en el servidor proporcionado por la empresa EMAPA-I en el cual se instalaran las herramientas de monitoreo en base a funciones SNMP de operación, administración, mantenimiento y seguridad para la red LAN de la institución. Luego en base a los resultados obtenidos se establece las notificaciones que el administrador recibe para controlar fallos que puedan presentarse. Además se realiza un estudio acerca de la transición de snmpv2 a snmpv3 para mantener niveles confiables de seguridad en el sistema de gestión. A continuación se realiza las pruebas de funcionamiento al sistema de monitoreo con el propósito de corregir inconsistencias que se puedan presentar en la ejecución del mismo.

En el cuarto capítulo se documenta detalladamente cada proceso realizado tanto en la detección como en la solución de fallas en un manual de procedimientos con el fin de que el administrador intervenga rápidamente en caso de presentarse algún inconveniente para así minimizar la interrupción del servicio de los usuarios.

ABSTRACT

The present project consists to designing a monitoring system based on the functional model "SNMP" by using Open Source tools in a network server provided by EMAPA-I with the intention of optimizing the performance of the network LAN and improving the technological productivity of the institution.

In the first chapter, is collected the information related to the network management and monitoring based on SNMP, are investigated their functions of operation, administration and maintenance, as well as also, will explain the reasons that motivated to the design of this project.

In the second chapter, are realized the raising of information of the condition and location of the equipments and the servers of the network EMAPA's LAN. Will be documented the equipments support the protocol snmpv2 and an inventory will be developed of the information obtained.

In the third chapter one proceeds with the configuration of the system of management in the servant provided by the company EMAPA-I, will be installed the tools of monitoring on the basis of functions SNMP of operation, administration, maintenance and security for the network LAN of the institution. Then, on the basis of the obtained results there are established the notifications that the administrator receives to control failures that they could present. In addition a study is realized for the transition of snmpv2 to snmpv3 to support reliable levels of safety in the system of management. Later the tests of functioning are realized to the system of monitoring by the intention of correcting inconsistencies that they could present in the execution of the same one.

In the fourth chapter, will be documented in detail every process so much in the detection as in the solution of faults in a manual of procedures in order which the administrator intervenes rapidly in case of appearing some disadvantage this way to minimize the interruption of the service of the users.

PRESENTACIÓN

Desde inicios de la era tecnológica se ha vuelto necesario compartir nuestros datos o recursos a través de un computador, para de esta manera realizar trabajos de una forma más rápida y eficiente, es por este motivo que a través de la Internet cada uno de nosotros nos hemos beneficiado de grandes cantidades de información, la cual cada vez se va actualizando debido a que las investigaciones realizadas a nivel mundial no cesan.

Existen muchos beneficios recibidos gracias a la Internet, además de brindarnos valiosa información, nos permite llevar a cabo negocios importantes a larga distancia, nos ayuda a relacionar con familiares o amigos que se encuentran muy alejados, de igual forma podemos realizar transacciones, pagos y consultas en nuestras cuentas de banco así como también administrar nuestro negocio o empresa. Estas características han ido creciendo, siendo hoy por hoy el pilar para la formación de nuevas oportunidades laborales.

En virtud de la importancia de la disponibilidad de estos servicios de infraestructura tecnológica, se han desarrollado modelos de referencia que se relacionan con la gestión de red, los cuales nos permiten identificar una falla, aislarla y corregirla en el menor tiempo posible, además nos presentan una base para la elaboración de un manual en el cual se documente los procedimientos realizados, con la intensión de suministrar información que facilite al administrador de red solucionar problemas similares, reduciendo de esta manera el tiempo que se emplearía en futuros mantenimientos, mejorando así la productividad tecnológica de una institución.

Uno de los estándares de gestión más usados en la actualidad es el SNMP, la demanda de los usuarios en distintos ámbitos de las comunicaciones le ha permitido seguir evolucionando, es por eso que se incrementaron funciones que le permiten trabajar en entornos cada vez más complejos con resultados satisfactorios, entre otras características que se detallarán más adelante en este documento.

ANTECEDENTES

- **Nombre del Proyecto**

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

- **Ubicación**

Ciudad: Ibarra
Provincia: Imbabura
País: Ecuador

- **Definición del Problema**

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

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

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

- **Objetivos**

Objetivo General

Implementar un sistema de gestión de red basado en el modelo funcional SNMP de la IETF, utilizando herramientas de software libre para monitorear los recursos de la red LAN en el edificio de EMAPA-I de la ciudad de Ibarra, con la finalidad de asegurar la disponibilidad de los recursos existentes.

Objetivos Específicos

- Estudiar la información relacionada con los elementos que componen el modelo funcional SNMP para disponer de pautas y criterios que permitan resolver las necesidades de la entidad.

- Analizar la situación actual de la red LAN del edificio de la empresa EMAPA-I mediante herramientas de software libre con el fin de identificar los equipos que soporten monitorización snmpv2, obtener un inventario inicial y definir los parámetros requeridos por cada uno de ellos.

- Escoger las herramientas de software libre para la monitorización de los recursos de acuerdo a los requerimientos institucionales analizados en base al estándar IEEE 29148 para la gestión de disponibilidad de servicios de la entidad.

- Elaborar el sistema de gestión de red en software libre con procedimientos de monitoreo basados en el modelo funcional SNMP con el fin de asegurar la disponibilidad de los recursos informáticos.

- Dar seguimiento al inventario y al uso de los recursos de la red LAN tomando en cuenta los parámetros del modelo funcional SNMP para mantener un registro de información constante.

- Detectar posibles inconsistencias en el sistema de gestión de red mediante pruebas de funcionamiento con el propósito de solucionarlas de manera inmediata.

- Realizar un estudio acerca de la transición de snmpv2 a snmpv3 para reforzar la seguridad del sistema de monitoreo.

- Realizar las pruebas que justifiquen el estudio de transición de snmpv2 a snmpv3 en el departamento financiero de la institución.

- Elaborar un manual de procedimientos que sirva de documento de apoyo al administrador de red en las actividades realizadas.

- Elaborar políticas y recomendaciones de acuerdo a los resultados obtenidos con el fin de que sean aplicadas por los usuarios para dar buen uso de los recursos.

- **Justificación**

La información que fluye dentro de las entidades tanto públicas como privadas es de vital importancia, por lo que deben cumplir estándares que garanticen de manera efectiva los derechos de disponibilidad de sus servicios, como lo establece el Plan Nacional de Desarrollo para el Buen Vivir, además como estrategia fomenta y promueve el desarrollo de software local, plataformas, sistemas, aplicaciones y contenidos que posibiliten a los ciudadanos y ciudadanas obtener provecho de las TIC en función de sus intereses y del contexto en el que se desenvuelven, a la vez el decreto

No. 1014 establece como política para las entidades públicas la utilización de Software Libre en sus sistemas y equipamientos informáticos, por lo que implementar un sistema de gestión de red con herramientas Open Source ayuda en gran parte a cumplir dichos requerimientos.

Por lo tanto la presente propuesta está orientada a monitorear recursos como: el uso de CPU, memoria, espacio en disco duro y conectividad, para garantizar la disponibilidad de los servidores de la red del edificio EMAPA-I según el modelo funcional SNMP ya que cualquier cambio no esperado puede retrasar el proceso tecnológico de la institución. A la vez con el uso de herramientas Open Source en el sistema de gestión de red que se implementará, se intenta reducir el alto costo del licenciamiento que representaría aplicar software propietario para brindar una solución similar.

- **Alcance**

El presente proyecto consiste en diseñar un sistema de monitorización basado en el modelo funcional SNMP utilizando herramientas Open Source en un servidor proporcionado por EMAPA-I con el propósito de optimizar el desempeño de su red LAN y mejorar la productividad tecnológica de la institución.

Como fase inicial se recopilará la información relacionada con la administración de red y monitoreo basado en SNMP para conocer detalladamente características, arquitectura, ventajas y desventajas que permitirán comprender el por qué se escogió este protocolo.

Para cubrir el modelo de gestión de red funcional SNMP, en la red se plantean las siguientes áreas que lo conforman:

La función de operación del modelo funcional SNMP se centrará en la elaboración de un registro topológico de la red LAN de EMAPA-I que nos permita conocer tanto el direccionamiento IP, ubicación física de host, de servidores y equipos de interconexión, además para analizar su estado operacional se configurará un servidor OCS Inventory NG con GLPI, el cual nos servirá para realizar la auditoria e inventario inicial de la red por

ser una herramienta que actúa como un administrador de recursos de información con una interfaz gráfica para su mejor interpretación, además nos ayudará a determinar si los equipos soportan características de monitorización snmpv2 con el fin de asegurar la interoperabilidad entre los equipos que van a formar parte del sistema de monitoreo. De acuerdo a los requerimientos institucionales analizados se seleccionarán las herramientas del sistema de gestión en base al estándar IEEE 29148 con la finalidad de obtener un diseño robusto, económico y confiable.

En la función de administración se centrará en la recolección de datos, estadísticas de los estados de las interfaces, carga de CPU, carga de memoria física, carga de memoria virtual y los umbrales de uso de los equipos computacionales de la red LAN, los cuales se encuentran en entornos Windows y Linux, a continuación se entregará al administrador información que le permita interpretar las estadísticas resultantes para dar una pronta solución a problemas que se susciten. Además se elaborará un manual en formato de texto tanto de las configuraciones como de las funciones con las que cuenta el sistema de monitorización, el cual servirá de apoyo al departamento de informática en el seguimiento continuo del sistema de gestión y a la vez sean de apoyo para añadir nuevos servidores, equipos o personal al sistema de monitoreo.

En la función de mantenimiento se determinará el comportamiento de la red mediante la interpretación de los resultados estadísticos, de haber interrupción en la disponibilidad de algún elemento gestionado se procederá a evaluar posibles soluciones que permitan la identificación de la falla, con el objetivo de aislarla y corregirla en el menor tiempo posible, para lo cual se utilizará la interpretación de intercambio de mensajes SNMP entre los agentes y el gestor, luego mediante los resultados que se obtengan se definirán umbrales y se enviaran traps en caso de la superación de los mismos. Además se establecerá parámetros de envió, control y registro de notificaciones significativas de acuerdo a las necesidades de EMAPA-I, con el fin de que el administrador intervenga rápidamente en caso de presentarse algún inconveniente minimizando la interrupción del servicio de los usuarios, también se ofrecerá al administrador de red mecanismos que permitan activar, modificar y desactivar el sistema de monitorización, mediante el ingreso a la plataforma a través de una autenticación robusta, de tal manera que se impida el acceso a personal no autorizado.

También se abarcará la función de seguridad mediante un estudio que sirva al administrador de red en un futuro realizar la transición de snmpv2 a snmpv3, por ser un protocolo más robusto en términos de autenticación y privacidad, para lo cual se recolectará información sobre esta versión del protocolo, se investigará las posibles soluciones de software libre, se determinará tanto las herramientas como la evaluación del impacto de la transición. Las pruebas del estudio efectuado se realizarán en el departamento financiero de la institución, donde por tener información confidencial se requiere monitoreo con cierto nivel de seguridad.

Se realizará un manual de procedimientos que estará disponible para el personal encargado de la administración, así como también se elaborará políticas y recomendaciones a los usuarios de la red a fin de garantizar el constante seguimiento de los recursos y la buena utilización de los mismos.

Posteriormente se verificará el funcionamiento del sistema de gestión en cada una de sus fases, para lo que se evaluará el cumplimiento de las políticas establecidas en el sistema de monitoreo, con el propósito de corregir inconsistencias que se puedan presentar en la ejecución del mismo.

CAPÍTULO 1: MARCO TEÓRICO

Este capítulo recopilará la información relacionada con la administración de red y monitoreo basado en SNMP, se investigará sus funciones de operación, administración y mantenimiento, así como también se explicará las razones que motivaron al diseño de este proyecto indicando su importancia y detallando lo que se pretende conseguir con su diseño.

1.1. GESTIÓN DE RED

En el momento que una empresa trabaja con sistemas computacionales, se tiende a buscar herramientas que puedan brindar un servicio competitivo al cliente, es por este motivo que cada vez surgen nuevos retos que involucran mantener disponibilidad en la red, lo cual resulta complicado debido a que muchos de los componentes de red son heterogéneos.

Martí (1999) refiere que "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".

Casares (2001), define a la gestión de red como la "planificación, organización, supervisión y control de elementos de comunicaciones para garantizar un nivel de servicio, de acuerdo a un coste y a un presupuesto, utilizando los recursos de forma óptima y eficaz".

Saydam & Magedanz (1996), citan que "la gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable".

Black (1995), menciona que “el término gestión se define para incluir tareas de planificación, monitoreo, tratamiento estadístico, control de las actividades y recursos en una red”.

Uno de los puntos que se puede apreciar de lo dicho anteriormente es que la gestión de red reúne una serie de características organizadas que permiten a un sistema computacional garantizar un alto porcentaje de eficacia y eficiencia de sus recursos informáticos a un costo asequible para la empresa.

1.1.1. Objetivo de la gestión de red

El objetivo de la gestión de red según los autores Subramanian, A & Timothy A. (2010) es asegurar que los usuarios de la red se beneficien de los servicios de tecnología de información con la calidad de servicio que ellos esperan.

Para lograr cumplir este objetivo, en un ambiente empresarial se debería elaborar un manual de procedimientos en el cual adjuntemos información sobre las actividades, métodos, consideraciones de hardware, software, y configuraciones que se encuentren dentro del sistema, evaluarlas cada cierto tiempo, ya que cualquier modificación no planificada puede producir daños en la infraestructura tecnológica, lo que puede generar un gran impacto económico en el futuro.

1.1.2. Elementos de la gestión de red

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

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

La segunda entidad, el agente, es un software dentro del dispositivo que se desea gestionar. Debido a la gran complejidad que presentan las redes actualmente, los fabricantes agregan agentes en sus equipos para dar flexibilidad a la gestión de red.

Los agentes son los que perciben alguna inconsistencia dentro del dispositivo, y envía un aviso al gestor para alertarlo de su situación actual.

1.1.3. Funciones de gestión de red

Podemos dividir las funciones de la gestión de red en dos grandes procesos:

- Monitorización
- Control

El primero como lo menciona Orozco P. (2010), pretende obtener datos de la situación actual de los recursos de la red y el segundo, mediante las estadísticas obtenidas, propone configuraciones para mejorar el servicio que se está ofreciendo.

1.1.3.1. Monitorización

Dentro de la monitorización tenemos dos enfoques:

- Monitoreo activo

Se realiza pruebas de conectividad en la red periódicamente con el fin de verificar los tiempos de respuesta correspondientes a la comunicación de dos puntos remotos. En este caso los equipos gestionados esperan la petición para responder.

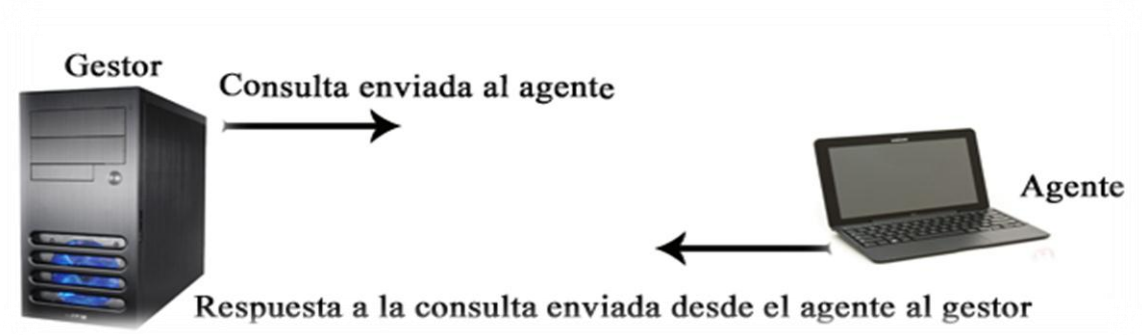


Figura 1 Procedimiento de Monitoreo Activo
Fuente: Adaptado de: Subramanian, A & Timothy A. (2010). Network Management

- Monitoreo pasivo

Obtiene datos mediante herramientas de recolección y análisis del tráfico de la red, los recursos son quienes dan notificación sobre su estado al gestor.

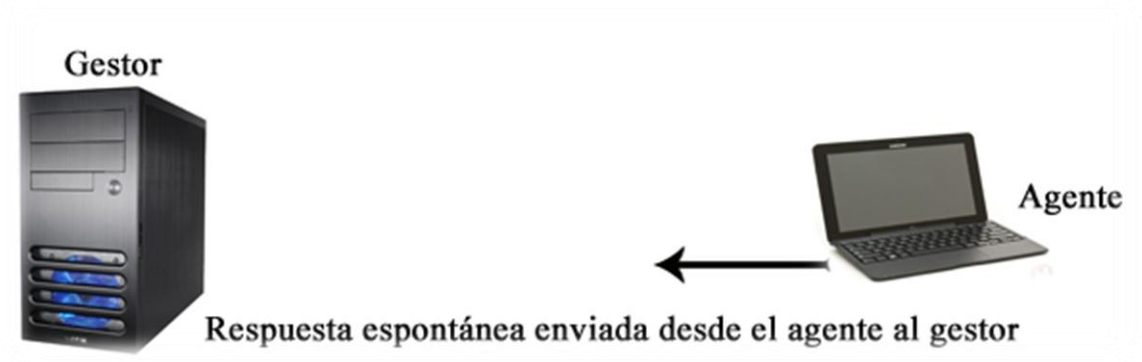


Figura 2 Procedimiento de Monitoreo Pasivo
Fuente: Adaptado de: Subramanian, A. & Timothy A. (2010). Network Management

1.1.3.2. Control

El control según menciona Orozco P. (2010), es el proceso que se encarga de mejorar el sistema, por ejemplo, si un nodo en la red es dado de baja, el monitoreo se encargaría de descubrir cuál fue la falla en el enlace, por su parte el control evalúa que comportamientos dieron lugar a la falla del enlace, para luego proponer criterios para optimar el sistema.

1.2. MODELOS DE GESTIÓN DE RED

Como anteriormente se mencionó, actualmente los fabricantes agregan agentes en sus equipos para dar flexibilidad a la gestión de red, sin embargo existen una variedad de proveedores que ofrecen servicios competitivos, que implica en muchas ocasiones heterogeneidad de dispositivos dentro de una misma empresa, por tanto usar solo un agente para monitorear el sistema es muy limitado, es por eso que la búsqueda de interoperabilidad entre los gestores y agentes se vuelve un aspecto sumamente necesario.

La gestión de red con interoperabilidad, para los autores Subramanian, A & Timothy A. (2010), se presenta cuando dos sistemas de proveedores A y B disponen de mensajes de gestión comunes entre sí.

Los mensajes consisten en información de lectura de tráfico de datos (tipo, identificación, y el estado de los objetos gestionados, etc.) y los controles de gestión (establecer y cambiar la configuración de un objeto).

El intercambio de mensajes se realiza mediante un conjunto de protocolos estandarizados de gestión, para cumplir con este fin se han establecido normas por organizaciones de normalización, las cuales progresan conjuntamente con las necesidades de los usuarios.

Para el estudio de este trabajo de investigación se relacionará tres estándares de gestión que por su funcionalidad son los más utilizados dentro de las telecomunicaciones las cuales se resume algunas de las características de los modelos de gestión en la tabla 1, aún hay más formas de organizar una red, pero debido al conjunto de características que contienen las mencionadas a continuación, se las considera un buen punto de inicio para la comprensión de las diferentes funciones asociadas con la administración de red.

Tabla 1. Modelos de Gestión

Modelo	Características
OSI	✓ Norma internacional (Norma ISO / OSI) ✓ Gestión de las comunicaciones de datos de red LAN y WAN ✓ El más completo ✓ Orientada a objetos ✓ Consume gran recurso en su aplicación
SNMP	✓ Estándar de la industria (IETF) ✓ Previsto originalmente para el manejo de los componentes de Internet. Actualmente adoptado para WAN y sistemas de telecomunicaciones ✓ Fácil de implementar ✓ Más ampliamente implementado
TMN	✓ Norma internacional (UIT-T) ✓ Gestión de la red de telecomunicaciones ✓ Con base en el modelo de gestión de red OSI ✓ Las direcciones tanto de la red y los aspectos administrativos de la gestión

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

1.2.1. Modelo de gestión OSI[1]

El modelo de gestión de red OSI es un estándar ISO[2] y es el más completo de todos, pues surgió de la necesidad de administrar las siete capas del cual está estructurado, siendo fundamental para la comprensión del resto de modelos de gestión.

1.2.2. Modelo de gestión TMN

El modelo de gestión de red TMN[3] según Pras A. (1999), está definido por la UIT-T y tiene una fuerte relación con el modelo OSI. TMN nace con el mismo propósito, el cual fue

[1] **OSI:** Open System Interconnection
[2] **ISO:** International Organization for Standardization
[3] **TMN:** Telecommunications Management Network

disminuir la heterogeneidad en los dispositivos de red, este modelo está formado por amplias características que son de gran utilidad para los grandes proveedores de servicios de telecomunicaciones.

1.3. MODELO DE GESTIÓN SNMP

- **Introducción**

La historia de la gestión SNMP[4] se remonta a 1970 en la gestión de Internet, pues con el crecimiento progresivo de Internet se convirtió en esencial tener la capacidad de controlar de forma remota los encaminadores de red y configurar puertas de enlace.

El protocolo SGMP[5] fue desarrollado para este propósito como solución provisional. Incluso la gestión SNMP pretendía ser otro recurso provisional, pues la solución a largo plazo, CMIP, fue diseñado teniendo en cuenta SNMP, solucionando sus errores y fallos, convirtiéndose en un gestor más potente, no obstante su gran complejidad desestimo su uso sobre todo en redes empresariales, de esta manera SNMP tuvo una buena acogida y actualmente es el más difundido y usado, por lo cual, se ha convertido en un estándar de facto.

Los dos principales estándares de gestión son desarrollados por el Grupo de Trabajo de Internet (IETF) y OSI desarrollado por la ISO del cual se habló anteriormente. El IETF[6], por su parte, es un grupo de trabajo con una organización informal que contribuye a la ingeniería y evolución de las tecnologías de Internet, el cual tiene la responsabilidad de desarrollar los estándares de Internet, incluidos las normas de gestión de red, los documentos de estas normas están disponibles gratuitamente en las RFC[7], las cuales según el IETF, son un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y

[4] **SNMP:** Protocolo Simple de Administración de Red
[5] **SGMP:** Protocolo Simple de Vigilancia de Gateway
[6] **IETF:** Grupo de Trabajo de Internet
[7] **RFC:** Petición de comentarios

discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.

- **Gestión basada en SNMP**

SNMP describe el paradigma gestor-agente, utilizado también por los principales modelos de gestión de red de nuestros días, como TMN o CMIP. Como se mencionó anteriormente, hay dos tipos de entidades: en primer lugar, un gestor, que es un servidor que ejecuta algún sistema de software que puede manejar las tareas de administración de una red, es el que consulta a un agente (router, switch, servidores, etc.) una información en específico, la cual puede ayudar a determinar si se ha producido algún tipo de evento no programado en la red. En segundo lugar, un agente, que es un software que se ejecuta en los dispositivos de red que se está administrando.

Según los autores, Douglas, M. & Schmidt K. (2009), citan que la información que se envía entre estas dos entidades debe ser interpretada tanto semántica como sintácticamente, además que el agente debe responder a cualquier sistema de gestión que se comunica con él a través de SNMP. Por lo tanto, un gestor puede administrar uno a varios agentes o a su vez, varios gestores pueden interactuar con uno o varios agentes así como se indica en la figura 3.

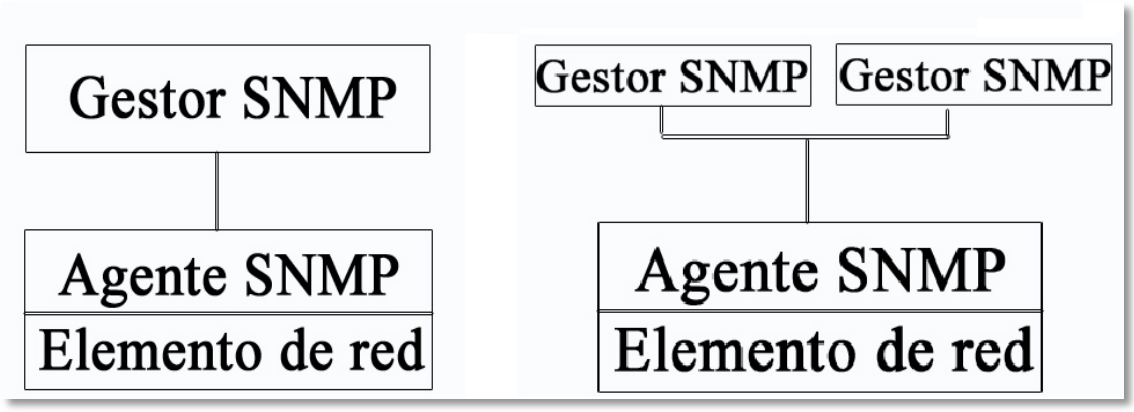


Figura 3 a) Un gestor-Un agente **b)** Múltiples gestores-Un agente
Fuente: Adaptado de: Douglas, M. & Schmidt K. (2009). Essential SNMP.

Hoy en día, la mayoría de los dispositivos IP[8] vienen con algún tipo de agente SNMP incorporado, el hecho de los proveedores de dispositivos estén dispuestos a implementar agentes en muchos de sus productos ayuda en gran medida la administración del sistema.

1.3.1. Arquitectura de administración SNMPv1

La arquitectura de administración SNMP se describe en el RFC 1157, la misma que se indica en la figura 4, en donde se especifica que la comunicación de información entre las entidades de gestión se realiza a través del intercambio de cinco mensajes de protocolo. Tres de ellos (get-request, get-next-request, set response) son iniciados por el proceso de aplicación del gestor. Los otros dos mensajes (get-response y trap) son generados por el proceso del agente.

En el esquema de administración SNMP, el gestor supervisa la red mediante el sondeo o encuesta a los agentes en cuanto a su situación y características, sin embargo la eficiencia se incrementa en agentes generadores de mensajes de alarma no solicitados, es decir por traps los cuales se representan en la figura 4.

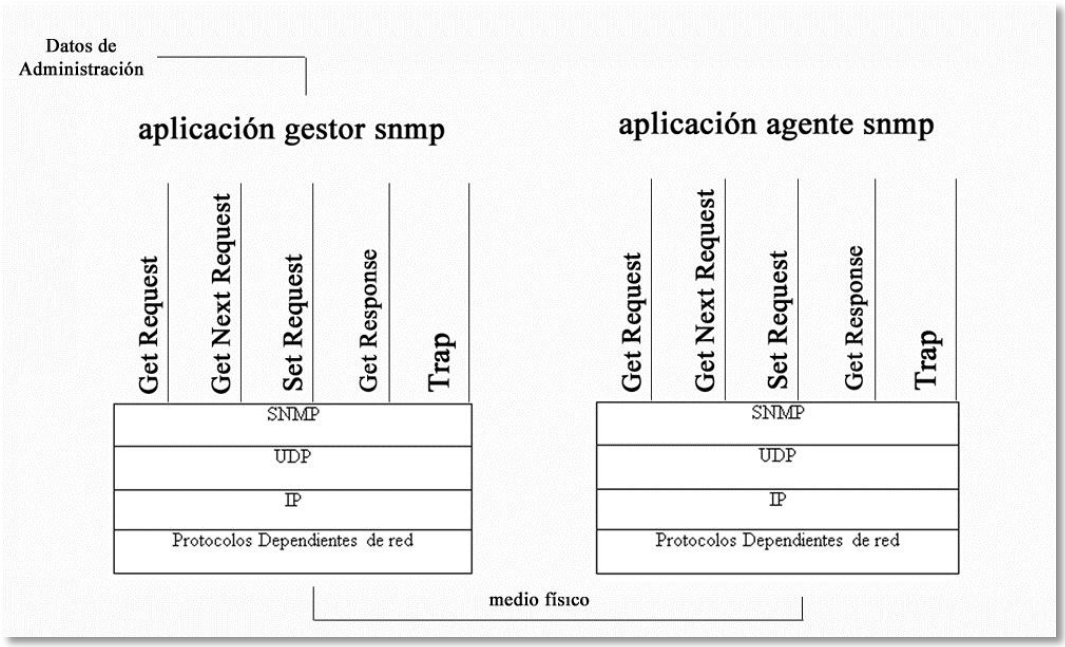


Figura 4 Arquitectura de Administración SNMP
Fuente: Adaptado de: Subramanian, A. & Timothy A. (2010). *Network Management*

[8] **IP:** Protocolo Internet

A continuación se describe brevemente la función que cumplen los mensajes PDU[9] de SNMPv1.

- **Get Request:** Es generado por el proceso de gestión para solicitar el valor de un objeto, el valor de un objeto es una variable escalar.
- **Get Next Request:** Muy similar al Get Request, en muchas situaciones un objeto puede tener varios valores debido a las múltiples instancias del objeto, por ejemplo la tabla de enrutamiento de un router, que tiene varios valores para cada objeto.
- **Set Request:** Es generado por el proceso de gestión para inicializar o restablecer el valor de una variable de un objeto.
- **Get Response:** Es generado por un proceso de agente, se genera solo en la recepción de un get-request, get-next-request o set-request de un proceso de gestión. Tras la recepción del PDU Get Response, la entidad de protocolo de recepción presenta sus contenidos a su entidad de aplicación SNMP.
- **Trap:** Es un mensaje no solicitado, generado por un proceso de agente sin ningún mensaje o evento que llega desde el proceso del gestor. Por ejemplo cuando el agente se da cuenta de que un parámetro no establecido ha surgido en el dispositivo

Para intercambiar información entre procesos de agentes y gestores tiene que haber un entendimiento común tanto en la sintaxis y la semántica del objeto gestionado por el sistema administrativo de red.

La estructura o sintaxis de gestión de información (SMI): Según el RFC 1155, la SMI proporciona una manera de definir objetos gestionados y su comportamiento, es un conjunto de reglas que define las características de los objetos de la red.

En SNMP, según el IETF, un objeto gestionado es una de cualquier cantidad de características de un dispositivo administrado, por ejemplo puede ser la interfaz de un router, continuando con el ejemplo este objeto gestionado a su vez tiene una o varias

[9] **PDU:** Unidades de datos de protocolo

instancias en particular que necesitamos monitorear tal como su velocidad, su actual estado operativo, etc

La sintaxis de un tipo de objeto se define utilizando la notación ASN.1[10], SMI está enfocado solo con el tipo de objeto y no con la instancia del objeto.

Cada objeto gestionado se puede dividir en 3 atributos:

- **Nombre:** El nombre o identificador del objeto (OID), define de forma única un objeto gestionado. Según la norma ISO/IEC 8824-1, los objetos gestionados se organizan en una jerarquía tipo árbol, y se representa por una cadena de caracteres que se componen de una serie de números enteros o nombres separados por puntos, estos caracteres ordenados jerárquicamente representan un objeto gestionado dentro del agente.

La figura 5 muestra los niveles de esta jerarquía árbol y sus sub-nodos bajo el nodo internet, donde se puede observar que bajo el nodo raíz tenemos tres sub-nodos con un valor numérico cada uno. En la figura 5, iso (1) es el único que tiene sub-nodos porque los otros dos no se refieren a SNMP por lo tanto no se discutirá de ellos en esta investigación. De esta forma cualquier objeto en el MIB de internet se iniciara con el prefijo 1.3.6.1 que es el valor asignado jerárquicamente a internet.

[10] ASN.1: Notación sintáctica abstracta

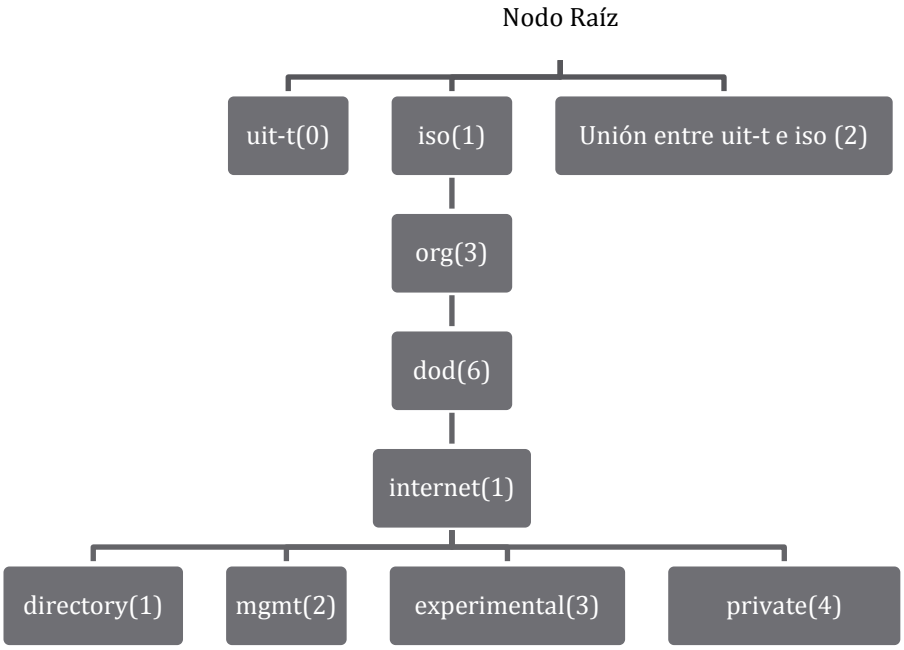


Figura 5 Árbol de objetos SMIv1
Fuente: Adaptado de: Norma ISO/IEC 8824-1. (2008).Información Technology**.**

Los 4 sub-nodos bajo el nodo internet se presentan a continuación:

- En primer lugar el nodo directory (1), es un nodo reservado para un uso futuro del directorio de OSI en la internet.
- En segundo lugar el nodo mgmt (2), se utiliza para identificar los objetos de administración de internet.
- En tercer lugar el nodo experimental (3), el cual fue creado para propósitos de prueba e investigación IETF.
- Y por último el nodo private (4), en el cual los proveedores comerciales son los responsables de los objetos bajo este nodo.

- **Tipo y sintaxis:** El tipo de datos de un objeto gestionado se define utilizando un subconjunto de ASN.1, que es una forma de especificar como se representa y se transmite datos entre gestores y agentes.

SMIv1 define varios tipos de objetos a través de características ASN.1, en el Anexo A se enumeran algunos de estos tipos de objetos soportados por SMIv1.

- **Codificación**: Se especifica en las recomendaciones X.690 del estándar UIT-T, también en el estándar ISO/IEC 8825-1. Las reglas de codificación básica (BER) permiten traducir una estructura de datos en una secuencia de bytes y viceversa, es un algoritmo con el cual se obtienen bytes de un dato ASN.1. Los datos ASN.1 no son útiles hasta que no se codifican en una secuencia de octetos, los mismos que deben poder decodificarse en el destino para que tanto el emisor y el receptor puedan entenderse.

La base de información de administración (MIB): Se puede considerar como una base de datos de objetos gestionados que rastrea el agente. Cualquier tipo de estado o información estadística que se puede acceder por el sistema de administración de red se define en una MIB.

Hay objetos genéricos que son definidos por el IETF y pueden ser administrados por cualquier sistema de administración de red compatible con SNMP, la norma MIB-II especificada en el RFC 1213, define las variables para algunas características de los dispositivos por ejemplo los estadísticos funcionales de un interfaz de un host, bytes enviados o recibidos, etc.

MIB-II pretende proporcionar información general de gestión TCP/IP pero no cubre todos los elementos posibles que un proveedor puede querer administrar en particular, por lo que a los proveedores se les permite definir variables MIB para su propio uso, por ejemplo si un proveedor ofrece un dispositivo al mercado, el agente integrado dentro de su dispositivo responderá a un sistema de administración de red definido por MIB-II y probablemente también incluya un MIB para alguna característica nueva que requiera ser administrada.

Los objetos gestionables por SNMP se agrupan por una serie de características que estos tienen en común, los grupos facilitan la asignación lógica de los identificadores de objeto. Hay 11 grupos MIB-II definidos en la estructura de árbol SMI, los cuales se representan en la figura 6.

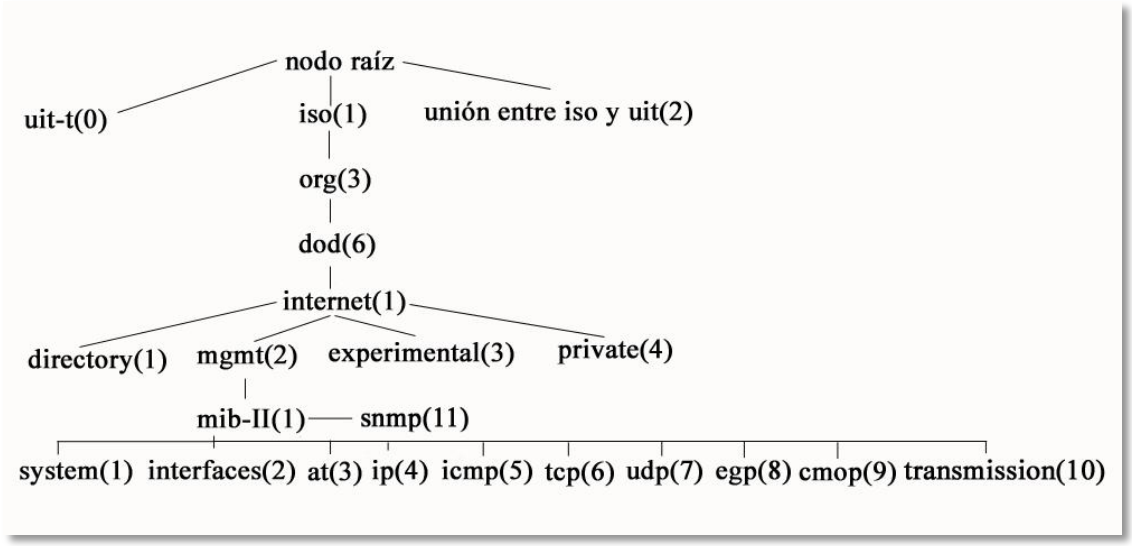


Figura 6 Grupo de objetos del árbol de objetos SMIv1
Fuente: Adaptado de: Norma ISO/IEC 8824-1. (2008).Información Technology**.**

En el Anexo A se describe brevemente cada grupo de objetos MIB-II, además se señalaran algunos de los objetos con los cuales se encuentran conformados.

1.3.2. Protocolo SNMPv2

SNMPv2 se desarrolló cuando se hizo evidente que las normas de gestión de red OSI no iban a ser implementadas en un futuro cercano. El grupo de trabajo que fue encargado por el IETF para definir SNMPv2 lo lanzó en 1996.

- **Principales cambios en SNMPv2**

Los componentes básicos de la gestión de la red en SNMPv2 son los mismos que la versión 1, los cuales son: el agente y el gestor. Algunas diferencias significativas entre SNMPv1 y SNMPv2 hacen incompatibles estas versiones, por lo que en el RFC 1908 se presentan esquemas de aplicación para la coexistencia entre ellas.

Entre los aspectos que se añadieron en la versión 2 según el RFC 1901 se mencionan los siguientes:

- Se añadieron dos mensajes importantes:

    - **Mensaje "Bulk Data Transfer".-** Es la capacidad de solicitar y recibir datos de forma masiva, esto acelera el proceso de get-next-request y es especialmente útil para recuperar datos de tablas.

    - **Mensaje "manager to manager".-** Trata con la interoperabilidad entre dos sistemas de gestión de red. Esto extiende la comunicación de mensajes de gestión entre los sistemas de administración y por lo tanto hace que los sistemas sean interoperables.

- **Mejoras en la estructura de información de gestión (SMI).-** En SNMPv1, SMI se define como STD16, que se describe en RFC 1155 y 1212 junto con el RFC 1215 que describe trampas. Los cuales se han fortalecido y reescrito en el RFC 2578 para SMI en SNMPv2. SMIv2 se divide en tres partes: definiciones de módulo, definiciones de objeto y definiciones de trampa.

- **Mejoras en las tablas.-** En SMIv2 se definen dos tipos de tablas: aquellas que tan solo pueden crear o borrar filas el agente, y aquellas en las que si puede modificar el gestor.

- **Mejoras en MIB.-** En SNMP el nodo de internet en el MIB tiene dos nuevos subgrupos: seguridad y snmpv2.

1.3.2.1. Arquitectura de administración SNMPv2

Hay mejoras significativas en la arquitectura SNMPv2 como por ejemplo la adición de dos mensajes como se puede observar en la figura 7.

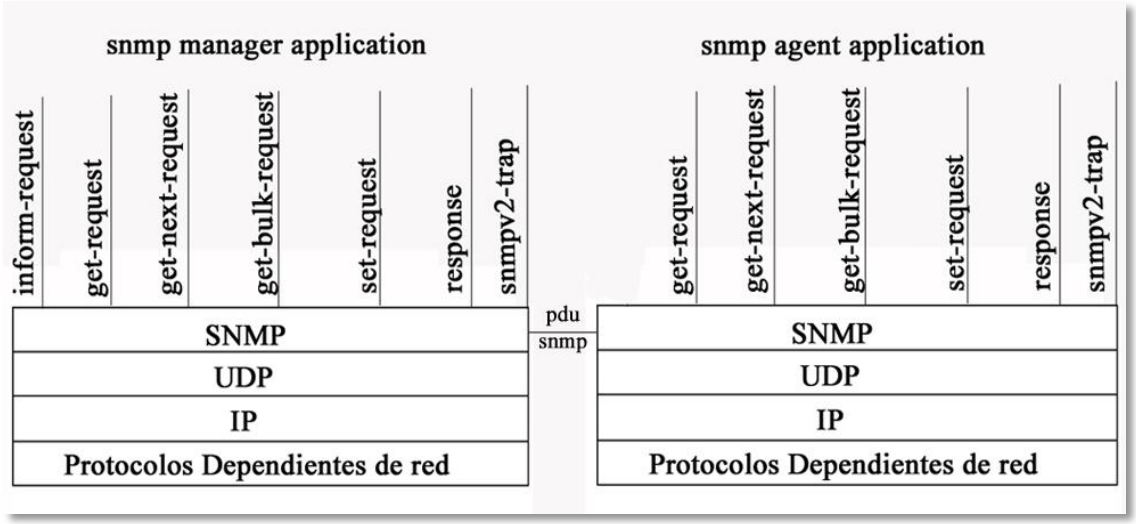


Figura 7 Arquitectura de Administración SNMPv2
Fuente: Adaptado de: Subramanian, A. & Timothy A. (2010). Network Management

Los mensajes: get-request, get-next-request y set-request son los mismos que en la versión 1 y se generan por la aplicación del gestor.

El mensaje **response** también es el mismo que **get-response** en la versión 1 y ahora es generado por las aplicaciones de agente y gestor.

- Es generado por la aplicación del agente en respuesta a un mensaje o conjunto de mensajes de la aplicación del gestor.
- Es generado por la aplicación de gestor en respuesta a un mensaje de petición de la aplicación del agente.

El mensaje **inform-request** proporciona un mecanismo de intercambio de información, errores a otros dispositivos. Es una aplicación de gestor y se transmite a otra aplicación de gestor, esta operación puede ser útil cuando se presenta la necesidad de más de un sistema de administración en la red.

El mensaje **get-bulk-request** es generado por la aplicación de gestor que se utiliza para transferir grandes cantidades de datos desde el agente al gestor, permite recuperar una gran parte de una tabla a la vez.

El mensaje **trap** es un mensaje originado en el agente para informar que algún suceso fuera de lo planificado ha sucedido.

1.3.2.2. La estructura o sintaxis de gestión de información (SMIv2)

Hay varios cambios en SMI en su versión 2, así como mejoras las cuales se especifican en el RFC 2578, esta versión de SMI se divide en las siguientes partes:

- **Definición de módulos:** Describe la semántica de un módulo de información y se definen formalmente por un macro ASN.1 llamado: MODULE-IDENTITY

- **Definición de objetos:** Se utilizan para describir los objetos gestionados, para lograr esto se utiliza un macro ASN.1 llamado: OBJECT-TYPE que transmite tanto la sintaxis y la semántica del objeto administrado.

- **Definición de Notificaciones:** Las notificaciones en SMIv2 es equivalente a la trampa en SMIv1. En SMIv1, la trampa se especifica por un macro en ASN.1 llamado: TRAP-TYPE. En SMIv2 la notificación se especifica mediante un macro en ASN.1 llamado: NOTIFICATION-TYPE, el cual transmite tanto la sintaxis y la semántica de una notificación.

SMIv2 define varios tipos de objetos a través de características ASN.1, en el Anexo A se enumeran algunos de estos tipos de objetos soportados por SMIv2.

1.3.2.3. La base de información de administración (MIB-II)

Se especifica en el RFC 3418, en donde se indica que se añadieron dos nuevos módulos en el MIB internet: seguridad y snmpv2. El módulo de snmpv2 tiene tres sub-módulos: snmpDomains, snmpProxys, snmpModules, los cuales se representan en la figura 8.

- **snmpDomains:** Extiende los estándares SNMP para enviar mensajes de gestión a través de protocolos de transmisión distintos a UDP que es la forma predominante y preferida de transportación.

- **snmpProxy:** Dado que UDP es el protocolo preferido para enviar mensajes de gestión, los sistemas que utilizan otro protocolo necesitan un servicio proxy para asignar a UDP, pero no se ha trabajado por ahora en snmpProxy.

- **snmpModules:** Hay dos módulos bajo este nodo: snmpMIBObjects y snmpMIBConformance, donde se aborda los nuevos objetos introducidos en snmpv2 así como aquellos que son obsoletos.

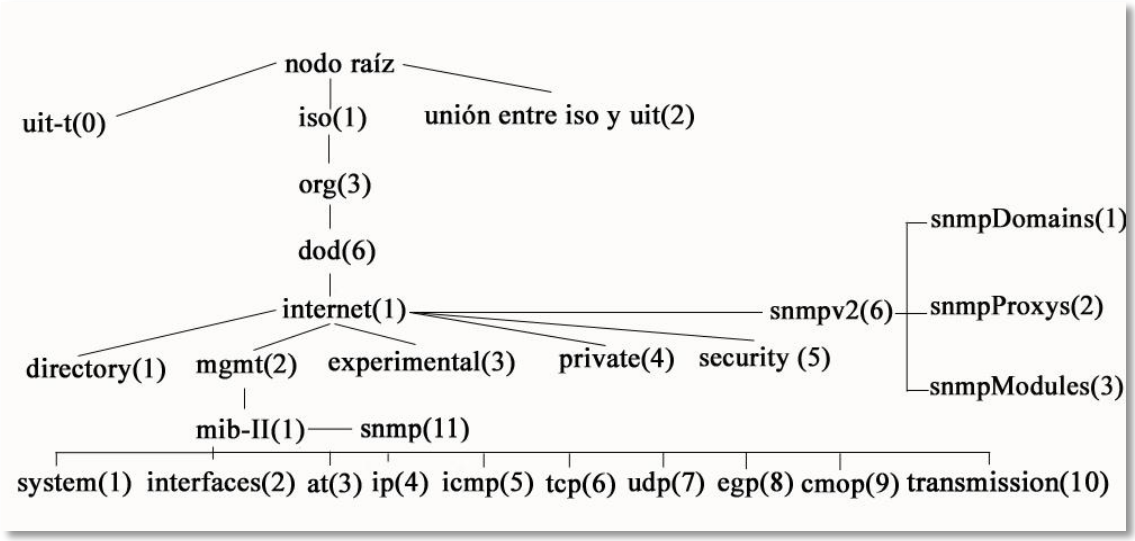


Figura 8 Grupo de objetos del árbol de objetos SMIv2
Fuente: Adaptado de: Norma ISO/IEC 8824-1. (2008).Información Technology.

En el Anexo A se describe brevemente cada grupo de objetos MIB-II en snmpv2, además se señalaran algunos de los cambios en los objetos con los cuales se encuentran conformados.

1.3.2.4. Operaciones y formato del PDU de SNMP v2

Las operaciones de protocolo snmpv1 se basan en un modelo administrativo de la comunidad que es el mismo que en snmpv2.

En el RFC 3416 se especifican 7 operaciones en el protocolo snmpv2:

- **Estructura de datos del PDU en snmpv2**

La estructura de datos del PDU en snmpv2, según el RFC 3416, se ha estandarizado a un formato común para todos los mensajes, mejorando así la eficiencia y el rendimiento en el intercambio de mensajes entre los sistemas, la mejora más significativa es llevar la estructura de datos de la trampa en el mismo formato que el resto.

La estructura del mensaje PDU genérico se muestra en la figura 9, el campo tipo PDU es indicado por un INTEGER y se enumeran en la tabla. Los campos error-status y error-media se establecen en cero o son ignorados en los mensajes set, get-request, y get-next-request. El campo error-status se establece a cero en el mensaje de get-response si no hay error, de lo contrario se indica el tipo de error. El campo variables-binding son un conjunto de pares atributo/valor que identifican los objetos MIB en la UDP.

Los tipos de mensajes PDU: Get-Request, Get-Next-Request, Set-Request, Trap, Inform-Request, en SNMPv2 se representan de la siguiente manera:

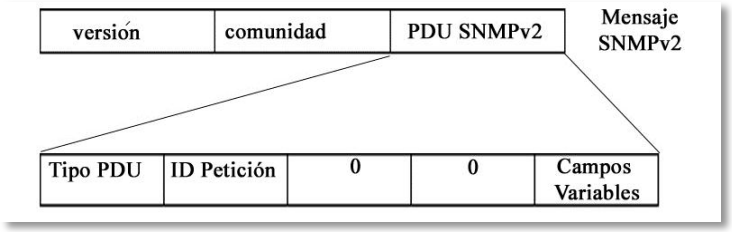


Figura 9 PDU Get-Request, Get-Next-Request, Set-Request, Trap, Inform-Request.
Fuente: Adaptado de: RFC 3416. (2002). Version 2 of the Protocol Operations for the Simple Network Management Protocol.

El tipo de mensaje PDU Response, en SNMPv2 se representa de la siguiente manera:

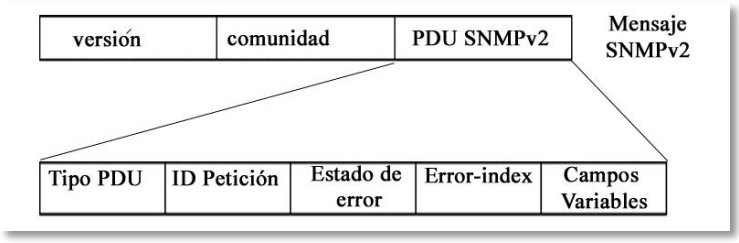


Figura 10 PDU Response.
Fuente: Adaptado de: RFC 3416. (2002). Version 2 of the Protocol Operations for the Simple Network Management Protocol.

El tipo de mensaje PDU Get-Bulk-Request, en SNMPv2 se representa de la siguiente manera:

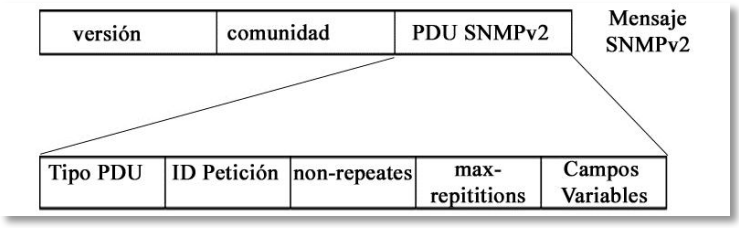


Figura 11 PDU Get-Bulk-Request.
Fuente: Adaptado de: RFC 3416. (2002). Version 2 of the Protocol Operations for the Simple Network Management Protocol.

Se puede observar que el formato de del mensaje get-bulk-request difieren en el tercer y cuarto campo, donde el campo "non-repeaters" indican el número de valores de los campos no repetitivos solicitados y el campo "max-repetitions" define la cantidad máxima de las instancias solicitadas.

En el Anexo A se especifica los valores para los tipos de PDU y campos "error-status" en el PDU snmpv2.

1.3.3. Protocolo SNMPv3

La seguridad ha sido la mayor debilidad de SNMP desde el principio, la autenticación en SNMPv1 y SNMPv2 equivale a una contraseña que se transmite en texto plano entre el gestor y agente, lo cual no da un nivel de seguridad alto a la red. El protocolo SNMPv3 aborda los problemas de seguridad que han afectado tanto a estas dos versiones anteriores, los cuales se ven especificados en el RFC 2570.

- **Cambios en SNMPv3**

Aunque SNMPv3 no realiza cambios en el protocolo, aparte de la adición de la seguridad criptográfica, sus desarrolladores han logrado hacer que las cosas se ven muy diferentes mediante la introducción de nuevas convenciones textuales, conceptos y terminologías. El cambio más importante es que la versión 3 abandona la noción de gestor y agente, tanto los gestores y agentes ahora se denominan entidades SNMP. Cada entidad se compone de un motor SNMP y una o más aplicaciones SNMP, que se discutirá más adelante. Estos nuevos conceptos son importantes porque definen una arquitectura, más que simplemente un conjunto de mensajes, la arquitectura nos ayuda a separar diferentes piezas del sistema SNMP de tal manera que hace que una aplicación segura sea posible.

1.3.3.1. El motor SNMPv3

El motor se compone de cuatro piezas: el despachador, el subsistema de procesamiento de mensajes, el subsistema de seguridad y el subsistema de control de acceso los cuales se especifican en el RFC 3412 y se presenta un breve resumen a continuación.

- El trabajo del despachador es enviar y recibir mensajes, se trata de determinar la versión de cada mensaje recibido (v1, v2, v3) y si la versión es soportada, se dirige el mensaje al subsistema de procesamiento de mensajes. El despachador también envía mensajes SNMP a otras entidades.

- El subsistema de procesamiento de mensajes prepara mensajes para ser enviados y extrae datos de mensajes recibidos, puede contener varios módulos de procesamiento de mensajes, por ejemplo puede tener módulos para el procesamiento de peticiones SNMPv1, SNMPv2, y SNMPv3. También puede contener un módulo para otros modelos de procesamiento que aún no se han definido.

- El subsistema de seguridad proporciona servicios de autenticación y privacidad. La autenticación utiliza cualquiera de las cadenas de comunidad SNMP (v1 y v2) o la

autenticación basada en el usuario SNMPv3. La autenticación basada en el usuario utiliza los algoritmos MD5[11] o SHA[12] para autenticar a los usuarios sin necesidad de enviar una contraseña en texto plano. El servicio de privacidad utiliza el algoritmo DES[13] para descifrar los mensajes SNMP. Actualmente, DES es el único algoritmo utilizado.

- El subsistema de control de acceso se encarga de controlar el acceso a los objetos MIB, puede controlar que objetos puede acceder un usuario y que operaciones se le permite llevar a cabo en esos objetos. Por ejemplo, es posible limitar el acceso de lectura-escritura de un usuario a determinadas partes del árbol de MIB-II, mientras se puede permitir el acceso de solo lectura a todo el árbol.

1.3.3.2. Aplicaciones SNMPv3

La versión 3, según el RFC 3413 divide a la mayor parte de lo que hemos llegado a considerar como SNMP en una serie de aplicaciones:

- **Command generator.-** Una aplicación de generador de comandos SNMP: get, getnext, getbulk, set requests, y procesador de las respuestas a las solicitudes que se generó. Esta aplicación se lleva a cabo por una estación de administración de red, por lo que puede realizar consultas y peticiones a entidades.

- **Command responder. -** Responde a los comandos: get, getnext, getbulk, y set requests. La aplicación del sistema de respuesta realiza la operación con un protocolo adecuado, utilizando el control de acceso, y generará un mensaje de respuesta que se enviará a donde se originó la solicitud.

- **Notification originator. -** Genera capturas SNMP y notificaciones. Un "notification originator" debe tener un mecanismo para determinar dónde enviar

[11] **MD5:** Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5
[12] **SHA:** Secure Hash Algorithm, Algoritmo de Hash Seguro
[13] **DES:** Data Encryption Standard

los mensajes, que versión de SNMP y que parámetros de seguridad se debe utilizar al enviar mensajes.

- **Notification receiver.-**Recibe las trampas y mensajes de informe.

- **Proxy forwarder.-** Facilita el paso de mensajes entre las entidades.

La figura 12 muestra los componentes que conforman la entidad SNMPv3 según el RFC 3411.

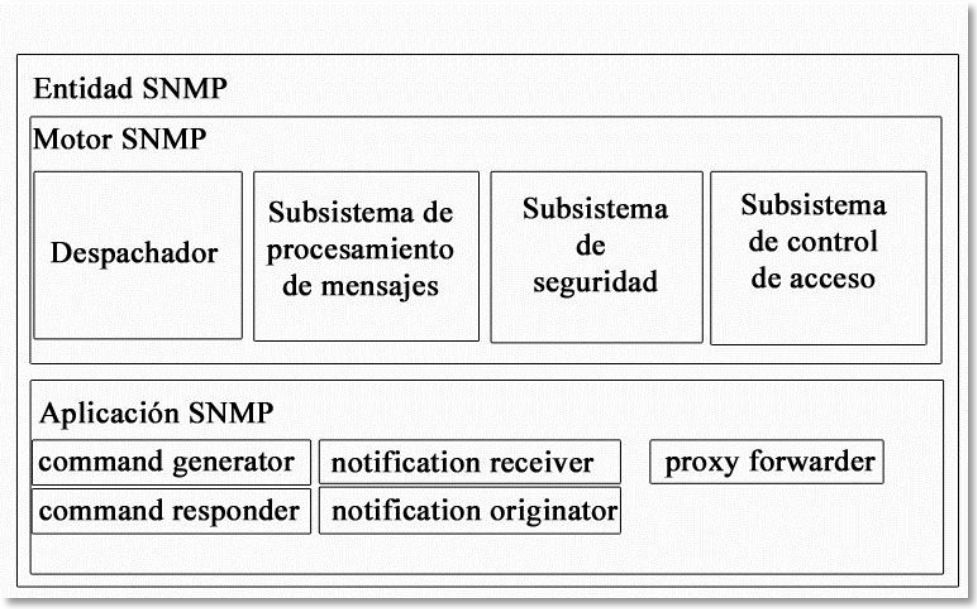


Figura 12 Entidad SNMPv3
Fuente: RFC 3411. (2002). An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

1.3.3.3. Estructura de datos del PDU en snmpv3

El formato de mensaje SNMPv3 tiene los siguientes campos:

- **msgVersion:** La versión de SNMP del mensaje, establecido en tres, con el tamaño de 4 bytes.
- **msgiD:** El msgID se utiliza entre un gestor y agente para coordinar los mensajes de solicitud y respuesta, con el tamaño de 4 bytes.
- **msgMaxSize:** El msgMaxSize es el tamaño máximo de mensajes soportado por un remitente de un mensaje SNMP, con el tamaño de 4 bytes.

- **msgFlags:** Es un valor de 8 bits que especifica que un reporte se va a generar, usando privacidad o usando la autenticación, con el tamaño de 1 byte.
- **msgSecurityModel:** Especifica que el modelo de seguridad fue utilizado por el remitente del mensaje. Los valores son 1, 2 y 3, para SNMPv1, SNMPv2, y SNMPv3 respectivamente, con el tamaño de 4 bytes.
- **msgSecurityParameters:** Contiene información específica de seguridad.
- **contextEngineID:** Identifica de forma exclusiva una entidad SNMP.
- **ContextName:** Identifica a un contexto particular en un motor SNMP
- **SecurityParameters:** Los msgSecurityParameters en SNMPv3 son los siguientes:
    - **msgAuthoritativeEngineID:** EL snmpEngineID del motor autoritativo
    - **msgAuthoritativeEngineBoots:** Los snmpEngineBoots del motor autoritativo
    - **msgAuthoritativeEngineTime:** El snmpEngineTime del motor autoritativo.
    - **msgUserName:** El usuario que pueden autenticar y codificar el mensaje.
    - **msgAuthenticationParameters:** Este valor es nulo si no se usa la autenticación. De lo contrario, actualmente el RFC 3412 especifica que se deben utilizar MD5 y SHA.
    - **msgPrivacyParameters:** Este valor es nulo si no se usa encriptación. De lo contrario este campo se usa para formar el valor inicial del modo de cifrado progresivo del algoritmo DES[14].

La figura 13 muestra el mensaje PDU de SNMPv3.

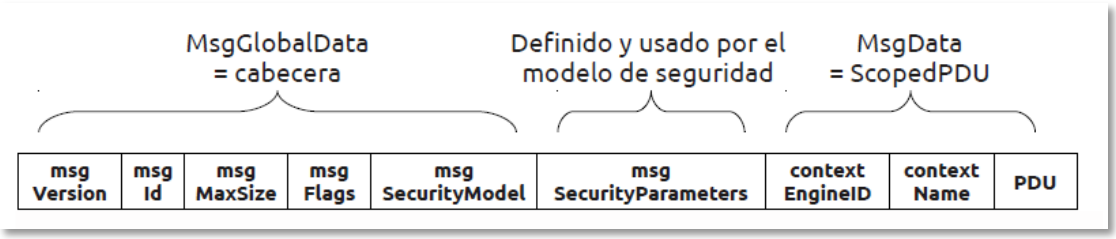


Figura 13 Formato de mensaje SNMPv3.
Fuente: Adaptado de: RFC 2272. (1998). Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

[14] **DES:** Data Encryption Standard

1.4. ESTADO ACTUAL Y FUTURO DE LA GESTIÓN DE RED

Un sistema de administración de red actual se basa en el protocolo SNMP, la mayoría de los componentes de red comerciales han incorporado agentes con este protocolo debido a la universalidad de las redes IP, además la mayoría de los sistemas host operativos populares vienen con un conjunto de protocolos TCP/IP, por lo tanto son susceptibles de gestión SNMP.

Sin embargo un sistema de administración actual sufre varias limitaciones, una de estas es que los valores de los objetos gestionados deben definirse en su mayoría como valores escalares.

Los basados en CMIP de OSI, está orientado a objetos, sin embargo no ha tenido éxito debido a la complejidad de las especificaciones de objetos gestionados y la gran limitación de usar una alta cantidad de memoria en los sistemas informáticos.

Otra limitación de la administración basada en SNMP es que se trata de un sistema basado en encuesta, el gestor envía encuestas a sus agentes para saber en qué estado se encuentra, o para pedir cualquier otro dato que necesita para la gestión de red, solo un pequeño grupo de transacciones es iniciada por un agente de gestión a un sistema de administración de red con alarmas.

Por lo que la gestión de red orientada a objetos está siendo reconsiderada, las tecnologías de información en sí, se están expandiendo y da lugar a nuevos retos para expandir el horizonte de la gestión de red.

CAPÍTULO 2: SITUACIÓN ACTUAL.

En este capítulo se realizará el levantamiento de información del estado y ubicación de los equipos y servidores de la red LAN de EMAPA-I. Se documentará que equipos soportan el protocolo snmpv2 y se elaborará un inventario de la información obtenida.

2.1. HISTORIA

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Ibarra (EMAPA), fue fundada el 19 de agosto de 1969, siendo desde su fundación una empresa, que brinda servicios de agua potable y alcantarillado a la población del cantón Ibarra, proyectándose siempre a la satisfacción del cliente. Siendo su finalidad la captación, tratamiento, distribución, producción y venta de agua potable y la prestación de los servicios de alcantarillado a la comunidad de Ibarra y sus parroquias rurales, garantizando eficiencia y eficacia, con criterio de equidad y justicia, comprometida con una concepción ecológica que preserve las cuencas hidrográficas y proteja el medio ambiente todo un trabajo con responsabilidad social.

2.2. ORGANIGRAMA DEPARTAMENTAL EMAPA-I

El organigrama se encuentra distribuido de la siguiente manera:

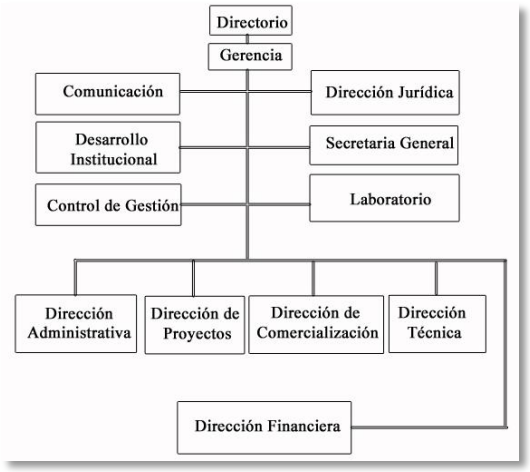


Figura 14 Organigrama departamental EMAPA
Fuente: Adaptado de: http://www.emapaibarra.gob.ec/wp-content/uploads/2015/03/ORGANIGRAMA-EMAPA-I.pdf

2.3. ANALISIS INTERNO

Dentro de la dirección administrativa se encuentra el departamento de recursos informáticos, la situación actual de este departamento se recopiló evaluando el método COBIT[15] el cual es una guía que permite el desarrollo de políticas y buenas prácticas para el control de las tecnologías de información dentro de una organización, desarrollado por ISACA[16]. (Víctor Reyes, 2015).

El marco de referencia de COBIT clasifica los procesos de las unidades de tecnología de información agrupándolos en cuatro dominios. (Josmell Ocrospoma, 2014).

- **Planificación y organización:** Este dominio se refiere a la identificación de la forma en que las tecnologías de información pueden contribuir de la mejor manera al logro de los objetivos institucionales, y al establecimiento de una organización e infraestructura tecnológica apropiada

- **Adquirir e implantar:** Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

- **Soporte y servicios:** En este dominio se hace referencia a la entrega de los servicios requeridos, desde las tradicionales operaciones sobre seguridad y continuidad, hasta la capacitación, así como los procesos de soporte necesarios

- **Monitoreo:** Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

[15] COBIT: Objetivos de Control para la Información y Tecnologías Relacionadas
[16] ISACA: Asociación de Auditoría y Control de Sistemas de Información

El análisis interno realizado consiste en separar las actividades de las áreas y componentes tecnológicos existentes, con el fin de que nos muestren su comportamiento, para posteriormente encontrar la problemática según la cual desarrollar opciones de solución que estén de acuerdo con los objetivos de la institución.

2.3.1. Departamento de Recursos informáticos

El departamento de recursos informáticos se encuentra dividido en dos partes las cuales son:

- Unidad de hardware redes y telecomunicaciones
- Unidad de software y desarrollo

2.3.1.1. Unidad de hardware redes y telecomunicaciones

Las actividades que realiza esta unidad son:

- Plan de mantenimiento de hardware existente, el cual tiene como objetivo asegurar a EMAPA-I de cualquier eventualidad que impida la continuidad, buen funcionamiento y un crecimiento tecnológico adecuado dentro de la institución.

- Informe de ejecución de proyectos tecnológicos de información y comunicación que facilitarán para la toma de decisiones correcta durante la realización de un nuevo proyecto.

- Informe de características y especificaciones técnicas para la adquisición de hardware en que se establecen las prioridades y la selección tomando en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad.

- Informe sobre el soporte técnico a los usuarios internos y externos sobre la utilización de hardware que garantizan la continuidad de la institución en el caso de que se produzcan incidencias, fallos, actuaciones malintencionadas por parte de terceros, pérdidas accidentales o desastres que afecten a los datos e

informaciones que son almacenados y tratados, ya sea a través de sistemas informáticos como en otro tipo de soportes, como el papel.

- Inventario de equipos informáticos que permite mantener actualizados en forma automática los inventarios de PCs y equipos de red.

- Mantenimiento de los servicios de red, aplicaciones y equipos que permitan realizar las operaciones de manera normal de las unidades de la Institución.

- **Mantenimiento de equipos de cómputo**

En esta área los reportes de mantenimiento de los equipos de cómputo se realizan en hojas de Excel en base a un cronograma de mantenimiento planificado por el personal que administra el hardware, algunos servidores, no están a cargo de este departamento por lo que su mantenimiento es realizado por entes externos.

- **Soporte técnico a usuarios internos**

El soporte técnico al personal de la empresa se lo realiza de acuerdo a las necesidades y requerimientos de los usuarios mediante petición verbal, o por vía telefónica al personal de la unidad de hardware, para que sean resueltos inmediatamente

2.3.1.2. Unidad de software y desarrollo

Las actividades que realiza esta unidad son:

- Participar en el proceso de planificación de mediano y largo plazo, así como el control y elaboración de las normas correspondientes a su área de responsabilidad, para sistematizar previamente objetivos, estrategias y políticas en planes y programas de acción

- Administrar las bases de datos y sistemas operativos para mantener tanto la integridad como la seguridad de los datos.

- Definir y establecer políticas de respaldos de información electrónica a nivel institucional, para tener la tranquilidad acerca de la integridad y seguridad de la información.

- Asignar claves de usuarios a los sistemas en producción, que permiten controlar el acceso a la información de la Institución.

- Elaborar el plan de contingencias del sistema informático, con el propósito de estructurar y ejecutar aquellos procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables.

2.4. INFRAESTRUCTURA TECNOLÓGICA DISPONIBLE

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

2.4.1.- Cuarto de Equipo

El cuarto de equipo se encuentra ubicado en la primera planta del edificio, aquí se encuentran los equipos de ruteo y conmutación así como también los servidores, los cuales se encuentran montados en racks entandares de diecinueve pulgadas.

El cuarto de equipo es administrado por el departamento de tecnologías de la información y comunicación, que se encarga de realizar el mantenimiento y verificación del buen funcionamiento de la infraestructura tecnológica.

2.4.2. Servidores

Los servidores, los cuales son de vital importancia para el buen funcionamiento de la institución se los presenta en la siguiente tabla:

Tabla 2. Servidores internos EMAPA

Marca	Servidor	Importancia
Hp	Aplicaciones	Alta
Hp	Base de datos	Alta
Clon	Correo	Alta
Clon	Active Directory	Alta
Hp	Quipux	Alta
Clon	Cobro online	Alta
Clon	Telefonía IP	Alta

Fuente: Base de datos EMAPA

Del banco de servidores, algunos cuentan son soporte externo, mientras que los siguientes corresponden al departamento de informática:

Tabla 3. Servidores que cuentan con mantenimiento del departamento de informática

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

Fuente: Base de datos EMAPA

Sus características técnicas son las siguientes:

- **HP PROLIANT DL380PGEN8**

• Modelo HP ProLiant DL380p Gen8

• 2 x Intel(R) Xeon(R) CPU E5-2670 @ 2.60GHz

• Memoria RAM[17] RDIMM[18] de 32 GB (2 x 16 GB)

• 4 puertos ethernet en una única tarjeta de expansión

• Disco SAS[19] 600GB

- **MIKROTIK SERIE1100**

• 3 puertos LAN/WAN GE 10/10/1000Mbps

[17] RAM (Random Access Memory): La memoria de acceso aleatorio es donde el procesador recibe las instrucciones y guarda los resultados.

[18] RDIMM (módulo dual registrado de memoria en línea): Es un dispositivo que almacena los datos más utilizados en el caso de las RDIMM estas son utilizados para servidores por su alto rendimiento y bajo consumo.

[19] SAS (Serial Attached SCSI): Es una interfaz de transferencia de datos en serie

• 5 puertos con interconexión de 1Gbps compartida.
• 1 puerto PoE para una alimentación de 12-24VDC.
• CPU de 800Mhz con una RAM de 512Mb expandible hasta 1,5GB.

2.4.2.1. Importancia de los Servidores

- **Active Directory**

La importancia del servidor Active Directory es alta pues en este se manejan todas las cuentas de los usuarios de la empresa y la falla o inhabilitación del mismo causaría que ningún usuario dentro de la empresa pueda ingresar a sus cuentas de pc, o a sus respectivos servicios. (Alejandro Corletti, 2011)

- **Servidor DNS**

Un servidor DNS es un servidor que permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio. La importancia del mismo resalta en que sin este servidor no podríamos comunicarnos con nuestro servidor principal de internet o de las aplicaciones internas. (Alejandro Corletti, 2011)

- **Servidor DHCP**

Un servidor DHCP es un servidor que recibe peticiones de clientes solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando los parámetros que permitan a los clientes auto-configurarse. La importancia de este servidor es alta pues sin este servidor podríamos establecer una configuración de IP similar en una o dos computadores provocando conflictos en la red de datos, impidiendo el ingreso a algún sistema a los mismos. (Alejandro Corletti, 2011)

- **Servidor Correo**

Un servidor de correo tiene como objetivo, enviar, recibir y gestionar mensajes a través de las redes de transmisión de datos existentes, al ser corporativo la comunicación entre los usuarios cuenta con una seguridad y confiabilidad de los datos superior a la ofrecida

gratuitamente por otras empresas. La importancia es alta puesto que en él se manejan datos importantes de la empresa. (Alejandro Corletti, 2011)

- **Servidor Firewall**

Un servidor firewall está diseñado para impedir el acceso a personal no autorizado o restringir páginas que puedan perjudicar el buen desenvolvimiento de la disponibilidad de la institución, la importancia es alta pues puede significar un mal uso de ancho de banda, provocando que colapsen algunos servicios. (Alejandro Corletti, 2011)

2.4.3. Equipos de red

En lo referente a la infraestructura tecnológica, la institución cuenta con los siguientes equipos de conmutación:

Tabla 4. Equipos de red EMAPA

	Tipo	**MARCA**	**MODELO**
PISO 1	SWITCH	DLINK	DGS-3120
	SWITCH	DLINK	DES-3028
	SWITCH	DLINK	DGS-3120
	SWITCH	CISCO	WS-C3750X-24
PISO 2	SWITCH	DLINK	DGS-3120
	SWITCH	3 COM	BASELINE 2928 SFP-PLUS
PISO 3	SWITCH	CISCO	SGE-2010

Fuente: Base de datos EMAPA

Sus características técnicas son las siguientes:

SWITCH DGS-3120-24TC

- 20 puertos 1000Base-T y 4 puertos 1000Base-T/SFP
- Soporta para Stack Físico 10GE; 40GE en total
- Soporta fuente de poder redundante

- Soporta SD[20] Card, para respaldos de configuración e información
- Soporte para proveer Alta Disponibilidad
- Seguridad Avanzada; D-Link E2E Security

SWITCH DES-3028

- Switch con 24 puertos FE y 4 puertos GE SFP
- Soporte QoS
- Soporte 802.1Q VLAN
- Soporte Stack Virtual de D-Link, vía SIM
- Alto Rendimiento, D-Link SafeGuard EngineTM
- Características avanzadas de administración
- Soporta múltiples estándares y protocolos de administración

SWITCH WS-C3750X-24T-S

- Puertos: 24 10/100BASE-TX
- Memoria RAM 256 MB
- Memoria Flash 128 MB Flash
- Rendimiento Banda ancha de fibra de interconexión : 160 Gbps

SWITCH BASELINE 3COM 2928

- Puertos: 28 puertos en total
- Características de manejo: Administrado. Protocolos: SNMP, NTP[21], HTTPS[22].
- Conectividad: 10BASE-T/100BASE-X/1000BASE-T
- Protocolo de direccionamiento: Direccionamiento IP estático

[20] SD (Secure Digital): Cuenta con un cifrado de seguridad en el hardware para protección de datos

[21] NTP (Network Time Protocol): Es un protocolo de Internet ampliamente utilizado para transferir el tiempo a través de una red. NTP es normalmente utilizado para sincronizar el tiempo en clientes de red a una hora precisa.

[22] HTTPS (Hypertext Transfer Protocol Secure): es una combinación del protocolo HTTP y protocolos criptográficos

SWITCH CISCO SGE-2010

- 48 puertos de alta velocidad 10BASE-T/100BASE-TX/1000BASE-T, optimizados para el núcleo de la red o para aplicaciones de alto consumo de ancho de banda.
- Los clústeres flexibles permiten gestionar varios switches como si fueran uno solo para respaldar el crecimiento de la empresa
- La seguridad avanzada protege el tráfico de la red para evitar el acceso de usuarios no autorizados
- Gestión por Internet simplificada que facilita la instalación y configuración

2.4.4. Direccionamiento IP

Por motivos de seguridad puesto que EMAPA-I es una institución pública no se detalla el direccionamiento IP, este direccionamiento esta seccionado de acuerdo a sus servidores, telefonía IP, red de computadores.

2.4.5. Topología de Red

La red se encuentra en topología en estrella, en donde cuenta con conmutadores como distribuidores centrales y un firewall.

2.4.5.1. Cableado Horizontal

El edificio de EMAPA-I tiene 4 pisos los cuales cuentan con cableado UTP[23] para la conexión entre los departamentos con los que cuenta cada piso. El cableado horizontal de la institución es de tipo UTP categoría 6 y 5e, los cuales están instalados en el cuarto de equipos, los servidores, y en los departamentos de la institución respectivamente.

[23] UTP: Cable de par trenzado

2.4.5.2. Cableado Vertical

Los cuatro pisos dentro de la institución se conectan mediante fibra óptica desde el cuarto de equipo hasta los racks de distribución que se encuentran en cada nivel.

2.4.6. Esquema de Red

El esquema de red con el que cuenta la empresa se muestra en la figura 15.

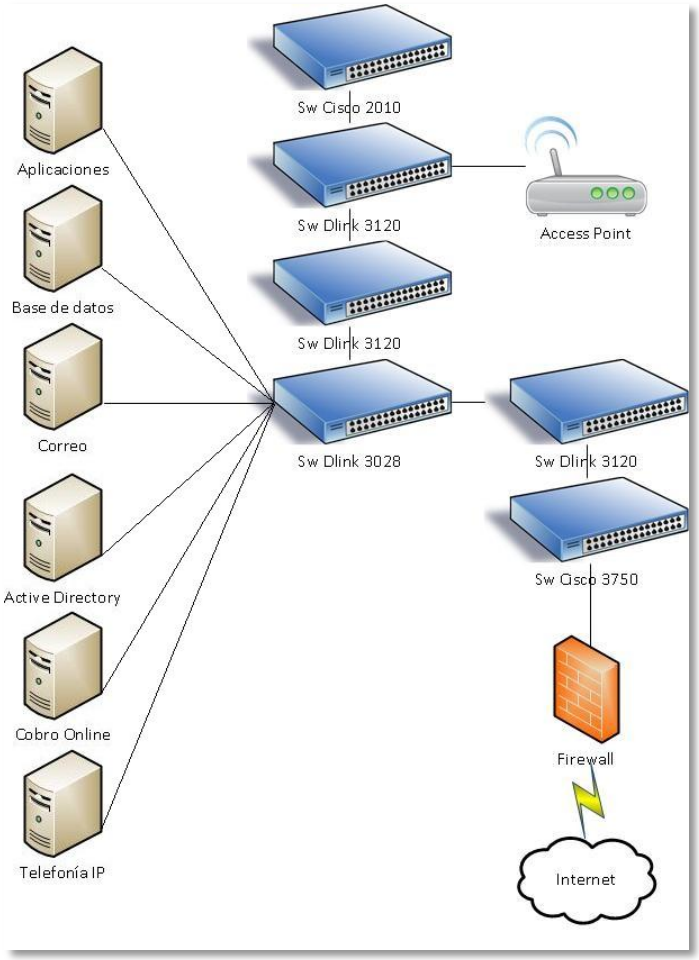


Figura 15 Esquema de red EMAPA
Fuente: Elaborado por el autor

La red de la empresa incorpora a su esquema un dispositivo cortafuego, además de un conmutador cisco que enlaza las redes virtuales con el firewall.

2.4.7. Enlaces a Internet

El enlace a Internet es de 5Mbps contratado a la empresa CNT.

2.5. PROBLEMÁTICA

Existen falencias en lo referente al monitoreo a los equipos de red; actualmente el departamento de tecnologías de la información y comunicación se encuentra en la fase de búsqueda de un software que le permita monitorear los recursos informáticos que se encuentran dentro de su red LAN, por tanto aún no se han establecido políticas ni procesos que aseguren tanto la confiabilidad de la información como la disponibilidad en la red de comunicaciones.

La falta de disponibilidad de tiempo del personal de la Unidad de Hardware ya que tienen múltiples funciones y además realizan actividades propias de sus responsabilidades fuera de la Institución por ejemplo en las agencias o bodega, ocasiona que no se dé un mantenimiento adecuado que permita una vida útil de los equipos en forma razonable lo que puede provocar pérdida de información, acumulación de trabajo y costos mayores de lo presupuestado, además tampoco existe un inventario de hardware actualizado.

Al no tener un control de las capacidades tanto de disco duro, ancho de banda, memoria RAM, o interfaces de los servidores, estas características pueden sobrecargarse, y causar disminución tanto en la disponibilidad como en la confiabilidad de la información, la cual afecta directamente a la comunidad.

El departamento de Recursos Informáticos no mantiene comunicación directa con los funcionarios de la institución para atender y solventar los problemas informáticos que se presenten, así que la solicitud para ser atendidos se realiza directamente en la oficina o vía llamada telefónica, pero en muchas de las ocasiones no es una respuesta inmediata debido a que ciertos momentos del día el personal técnico no se encuentra en la matriz sino en las agencias solventando otras incidencias de la institución.

Luego de haber presentado la situación actual de EMAPA-I, se puede concluir que existe la necesidad de garantizar la confiabilidad de la red de datos y de igual forma mejorar el manejo de incidencias las cuales deben estar fundamentadas en las Normas de Control Interno en su apartado 410 para Tecnologías de la Información, por lo que la implementación de un sistema basado en un modelo de gestión permitirá establecer políticas de mantenimiento, destinadas a asegurar la disponibilidad de la red LAN de la institución.

CAPITULO 3: MODELO FUNCIONAL SNMP

En este capítulo se procederá con la configuración del sistema de gestión en el servidor proporcionado por la empresa EMAPA-I en el cual se instalaran las herramientas de monitoreo en base a funciones SNMP de operación, administración y mantenimiento para la red LAN de la institución. Luego en base a los resultados obtenidos se establecerán las notificaciones que el administrador recibirá para controlar fallos que puedan presentarse. Además se realizará un estudio acerca de la transición de snmpv2 a snmpv3 para mantener niveles confiables de seguridad en el sistema de gestión. A continuación se realizará las pruebas de funcionamiento al sistema de monitoreo con el propósito de corregir inconsistencias que se puedan presentar en la ejecución del mismo.

3.1. DISEÑO DEL SISTEMA DE GESTIÓN

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

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

- Establecer como prioridad la seguridad y protección de la información del sistema computacional y de los recursos informáticos de la empresa.

- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.

- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.

<table>
<tr><td colspan="3">EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA</td></tr>
<tr><td colspan="3">POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL</td></tr>
<tr><td rowspan="3"></td><td>Versión</td><td>• 1.0</td></tr>
<tr><td>Elaborado por:</td><td>• Richard Armando Mallamas</td></tr>
<tr><td colspan="2">Revisado por:
• Ing. Carlos Danilo Maldonado-Analista Informático 1
• Ing. Darío Edison Páez-Analista Informático 2</td></tr>
</table>

I. Propósito.

El propósito de este documento es el de optimizar y asegurar la disponibilidad de los recursos informáticos, previniendo los daños o riesgos que se puedan presentar ya sea por causas humanas involuntarias o conductas indebidas, proporcionando una gestión eficiente de los procesos en la red de comunicaciones.

II. CONCEPTOS PRELIMINARES

- **Gestión de red**

La gestión de red reúne una serie de características organizadas que permiten a un sistema computacional garantizar un alto porcentaje de eficacia y eficiencia de sus recursos informáticos a un costo asequible para la empresa.

- **Políticas de gestión**

Son el medio por el cual las metas u objetivos se encaminan a alcanzarse, no hay un orden o un formato establecido por lo que se deben establecer según el entorno donde se van a aplicar, en este caso están basadas exclusivamente en las necesidades de la red de datos actual, con el fin de optimizar y asegurar la disponibilidad de los recursos informáticos.

III. GENERALIDADES

a) Este documento se redactó de tal forma que pueda ser entendido por las personas que están a cargo del departamento de tecnologías de la información, por lo que debe tener conocimiento básico de computación.

b) Las políticas de gestión presentadas en este escrito se utilizan de referencia, no serán tomadas como definitivas, por lo que está totalmente expuesta a cambios, siempre y cuando las modificaciones a este documento complementen el objetivo del modelo de gestión de red.

c) Toda persona que haga uso de las políticas sin importar el nivel organizacional en el que se encuentre dentro del departamento de tecnologías de la información, deberá orientar sus esfuerzos en cumplir las políticas que estén enfocadas a su entorno de trabajo.

IV. NIVELES ORGANIZACIONALES

a) Jefe de Infraestructura Tecnológica

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

b) Analista informático 1

Ejecutar y coordinar actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones

c) Analista informático 2

Ejecutar y coordinar actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones

V. VIGENCIA

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

VI. REFERENCIA

El presente documento se lo realizó mediante el formato realizado por un proyecto que se encuentra dentro de la municipalidad(Cevallos Michilena, 2013, págs. 55-82) el cual se encuentra estructurado en base a dominios y controles tomados de la Norma ISO/IEC 27002:2005, al no existir un estándar específico para la administración de red, las políticas de gestión están realizadas en base al modelo de gestión SNMP, establecido por la IETF:

1. Política de Gestión de la red de datos

1.1 Objetivo de la Política de Gestión.

1.2 Compromiso de las Autoridades.

2. Gestión de Operación.

2.1 Inventario de la red

2.2 Configuración de equipos.

3. Gestión de Administración.

3.1. Mantenimiento del inventario e ingreso de equipos.

3.2. Mesa de ayuda.

4. Gestión de Mantenimiento.

4.1. Parámetros de monitoreo

4.2. Manejo de Fallos.

4.3. Reportes

5. Gestión de Seguridad.

5.1. Acceso al Software de Gestión.

5.2. Acceso a los dispositivos de red.

6. Cumplimiento.

6.1. Cumplimiento de Políticas.

VII. TÉRMINOS Y DEFINICIONES

EMAPA-I	Empresa pública municipal de agua potable y alcantarillado de Ibarra
SNMP	(Simple Network Management Protocol), Protocolo simple de administración de redes, es un estándar de administración de redes utilizado en redes TCP/IP.
OSC-INVENTORY	Software que recopila información sobre el hardware y software de equipos que hay en la red, permitiendo obtener un inventario.
Reporte	Es un informe o una noticia de una información o evento sucedido, este tipo de documento puede ser presentado impreso, digital, audiovisual, etc.
Software	Componentes lógicos intangibles necesarios que hacen posible la realización de tareas informáticas.
Hardware	Componentes físicos tangibles que funcionan dentro de un sistema informático.
Resultados Estadísticos	Datos que se indican en forma porcentual del estado de los recursos como también gráficos que recolectan información del tráfico ocurrido en las interfaces de los dispositivos.

VIII. DESARROLLO DE POLITICAS DE GESTIÓN DE RED

<table>
<tr><td colspan="3">EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA</td></tr>
<tr><td colspan="3">POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL</td></tr>
<tr><td rowspan="3"></td><td>Dominio</td><td>Política de Gestión de la red de datos</td></tr>
<tr><td>Control</td><td>Objetivo de la Política de Gestión.</td></tr>
<tr><td>Destinatario</td><td>Administradores de red y usuarios</td></tr>
<tr><td colspan="3">Art 1. Entregar tanto al personal encargado de la administración de red como a los usuarios información del funcionamiento del sistema de gestión con el fin de que sean aplicadas para garantizar la disponibilidad y el buen uso de los recursos

Art 2. Socialización de la información necesaria a los encargados de la administración de los recursos de la red para el buen uso de los mismos.</td></tr>
</table>

<table>
<tr><td colspan="3">EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA</td></tr>
<tr><td colspan="3">POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL</td></tr>
<tr><td rowspan="3"></td><td>Dominio</td><td>Política de Gestión de la red de datos</td></tr>
<tr><td>Control</td><td>Compromiso de las Autoridades.</td></tr>
<tr><td>Destinatario</td><td>Administradores de red y usuarios</td></tr>
<tr><td colspan="3">Art 3. El departamento de informática y el jefe de recursos informáticos, como responsables de la elaboración de las Políticas de Gestión para la red de área local en EMAPA-I, toman el compromiso de revisión constante y socialización de los lineamientos descritos en este documento.</td></tr>
</table>

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Operación
	Control	Inventario de la red
	Destinatario	Administradores de red
Art. 4. El departamento de tecnologías de información tendrá a su disposición un software de inventario de los recursos de red (OCS/GLPI) en el cual podrá observar el direccionamiento IP, MAC, y ubicación de los recursos informáticos (computadores, impresoras, monitores, software y hardware) de los host mediante una interfaz web. Art 5. El departamento de tecnologías de información realizará cada cierto periodo el inventario de la red, en el cual se estudiaran los indicadores de desempeño de los recursos informáticos para tomar los correctivos que se requieran.		

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Operación
	Control	Configuración de equipos
	Destinatario	Administradores de red
Art. 6. Para el ingreso de equipos en la base de datos se usará la nomenclatura establecida por departamento de tecnologías de información de EMAPA-I especificada en la tabla 6. Art. 7. Para que el administrador de la red pueda proceder a la configuración de los equipos estos deben soportar como mínimo el protocolo SNMP, el cual deberá ser configurado con su respectiva sintaxis para poder ser gestionado, la cual se especifica en la tabla 8 y 9.		

Art. 8. Si se realiza cambios en los equipos de la red o en sus configuraciones, estos cambios deberán ser actualizados en la base de datos, con el fin de llevar una auditoria actualizada que nos permita mantener la disponibilidad de los recursos informáticos.

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Administración
	Control	Mantenimiento del inventario e ingreso de equipos
	Destinatario	Administradores de red
Art. 9. El departamento de tecnologías de información efectuará periódicamente el inventario tanto del hardware como del software de la red de datos mediante una aplicación instalada en el sistema de gestión (OCS/GLPI) con el fin de asegurar la seguridad y confiabilidad de los recursos informáticos Art. 10. Antes de ingresar un dispositivo al software de gestión el administrador deberá analizar el estado actual en el que se encuentra la red y posteriormente instalar el agente OSC-Inventory al computador que se desee agregar, proceso que permitirá inventariarlo y buscarlo de manera fácil en el sistema.		

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Administración
	Control	Mesa de ayuda
	Destinatario	Usuarios y administradores de red
Art. 11. Los usuarios finales deberán reportar los problemas informáticos que se les presenten como por ejemplo: falla de ingreso al sistema integrado de Emapa-I o internet, fallos en la impresora, falla en el teclado, mouse, teléfono, monitor, computador, mediante una plataforma web (GLPI) con el fin de que las acciones que realiza el		

departamento informático como soporte a esas incidencias se vaya almacenando en una base de datos para al fin de cada mes obtener un reporte de las acciones realizadas.

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Mantenimiento
	Control	Parámetros de monitoreo
	Destinatario	Administradores de red
Art. 12. El departamento de tecnologías de información deberá revisar los niveles de umbrales que se establecen en el software de gestión (Zabbix) los cuales estarán establecidos para generar alertas del estado de funcionamiento de la red.		

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Mantenimiento
	Control	Manejo de fallos
	Destinatario	Administradores de red
Art. 13. El departamento de tecnologías de información al determinar una inconsistencia en la red de datos, mediante el software de monitoreo, definirá y ejecutará procedimientos, que permitan aislar, diagnosticar y corregir la falla en el menor tiempo posible.		

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Mantenimiento
	Control	Reportes
	Destinatario	Administradores de red

Art. 14. El departamento de tecnologías de información, podrá tomar los reportes del software de gestión (Zabbix) en forma, diaria, mensual y anual, para estar al tanto del proceso de funcionamiento de los recursos activos de la red.

Art. 15. Al término de cada mes el administrador deberá sacar un reporte del software de gestión (Zabbix) para tener constancia de la disponibilidad de funcionamiento de los recursos de los servidores monitoreados por el software de gestión.

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Seguridad
	Control	Acceso al Software de Gestión
	Destinatario	Acceso a los dispositivos de red

Art. 16. Solamente las personas encargadas de la administración de la red podrán ingresar al sistema de gestión mediante el acceso único e intransferible.

Art. 17. El departamento de tecnologías de información tendrá que cambiar las contraseñas de ingreso al sistema de monitorización cada cuatro meses con el fin de evitar el intento de acceso a esta información a personal no autorizado, la longitud mínima de caracteres que se usaran en una contraseña se establece en 6 caracteres, los cuales incluyan tanto alfanuméricos como especiales.

Art. 18. El sistema de gestión está sujeto a cambios de configuraciones, por lo que alguna configuración equivocada dentro del equipo donde se encuentra instalado, podría afectar su rendimiento, por tanto el ingreso debe ser manejado solo por el personal autorizado del departamento de tecnologías de información de EMAPA-I, ya sea por medio de SSH o por intervención directa en el equipo.

Art. 19. El departamento financiero al mantener información confidencial requiere ser monitoreado mediante el protocolo snmpv3 en la plataforma Cacti con la nomenclatura establecida en la tabla 11.

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Gestión de Seguridad
	Control	Control de acceso
	Destinatario	Usuarios
Art. 20. El ingreso forzoso a las páginas que se encuentran bloqueadas por parte de los usuarios será motivo de una llamada de atención verbal, y de ser necesaria, la suspensión temporal del servicio, ya que puede ser motivo de degradación del rendimiento de la red así como también incluir perdida de información.		

EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA		
POLÍTICAS DE GESTIÓN DE LA RED DE DATOS DE ÁREA LOCAL		
	Dominio	Cumplimiento
	Control	Cumplimiento de Políticas
	Destinatario	Administradores de red
Art. 21. El departamento de tecnologías de información de EMAPA-I será el responsable de supervisar el cumplimiento de las políticas presentadas en este documento.		

3.1.2. Criterios de Evaluación para escoger las herramientas del sistema de gestión de red en base al estándar ISO/IEC/IEEE 29148-2011.

I.- Introducción

Tomando en cuenta los requerimientos de red analizados, y la auditoría sistemática al departamento de recursos informáticos realizada en un proyecto de grado previo (Portilla Lissett, 2013), se consideró elegir las herramientas de monitoreo de los recursos informáticos en EMAPA-I en base al estándar de Especificación de Requerimientos de Software ISO/IEC/IEEE 29148-2011 en el cual se define una registro de requisitos que nos sirven de guía en el diseño y posteriormente en la implementación. A continuación se presenta la siguiente plantilla que representa el estudio realizado.

- **Propósito**

En este documento se añadirá información referente a la gestión de la red de datos de EMAPA-I para monitorear sus recursos informáticos y de esta manera de obtener un diseño robusto, económico y confiable. Está dirigido tanto al personal encargado del departamento de tecnologías de comunicación como a los usuarios de los recursos de la red LAN.

- **Ámbitos del sistema**

El software que se va a implementar tiene dos finalidades en primer lugar se centrará en la elaboración de un registro topológico de la red LAN de EMAPA-I que nos permita conocer tanto el direccionamiento IP, ubicación física de host, de servidores y equipos de interconexión, además analizar su estado operacional, evaluar estadísticamente la red, configurar la programación de las alarmas, y que esta información se almacene en una base de datos, la segunda finalidad consiste en realizar la auditoria e inventario de la red como :equipos, monitores, periféricos, etc., presentar una plataforma en la cual los usuarios presenten sus inconvenientes, los técnicos cuenten con herramientas para dar seguimiento de incidencias y por último puedan generar un historial completo de los mantenimientos realizados en la red.

- **Acrónimo**

SNMP.- Protocolo Simple de Administración de Red
LAN.- Red de área local
IP.- El protocolo de IP
IEEE.- Instituto de Ingenieros Eléctricos y Electrónicos

- **Referencias**

ISO/IEC. (2011). Systems and software engineering —Life cycle processes — Requirements engineering. Recuperado el 20 de agosto de 2015 de: https://cow.ceng.metu.edu.tr/Courses/download_courseFile.php?id=7200.

- **Visión general del documento**

El documento presenta tres secciones, la primera la describe el propósito y ámbitos del proyecto; la segunda descripción general del sistema especificando su prospectiva y funciones del sistema; la tercera la descripción específica de los requisitos de la aplicación.

II. Descripción General

El sistema de gestión de red debe permitir colectar datos de los dispositivos de red mediante el monitoreo realizado en base del protocolo SNMPv2 y SNMPv3, en el cual se logre obtener datos de la red que puedan servir para revisar estadísticamente el comportamiento de la infraestructura tecnológica de la institución. Además, proporcionar una plataforma que permita a los usuarios entregar un reporte de incidencias a los técnicos, para que de esta forma el departamento de informática cuente con una herramienta en la que se genere un histórico de reportes, mantenimientos realizados y admita establecer una base de ayuda para próximas incidencias que se presenten.

- **Funciones de la aplicación**

Las funciones generales que la aplicación debe contener:

- ✓ Facilidad de configuración
- ✓ Función de monitoreo de red para varios dispositivos
- ✓ Función de notificaciones
- ✓ Función de almacenamiento en la base de datos
- ✓ Función de elaboración, consulta y soporte
- ✓ Función de control de acceso

- **Características de los usuarios**

Los usuarios están en la capacidad de ingresar incidencias, enviar reportes, revisar las actividades que se estén realizando para cubrir sus problemas. Los usuarios deben estar registrados en el sistema para poder acceder a las funcionalidades de la plataforma por medio de un usuario y una contraseña únicos; los usuarios que no estén registrados no podrán acceder al sistema.

- **Restricciones**

La implementación se realizará en el departamento financiero en el cual se hará una demostración, pero el proyecto es escalable y puede adaptarse a toda la empresa. Los técnicos deben poseer conocimientos de electrónica e informática para poder administrar y gestionar los incidentes de los usuarios.

- **Suposiciones y dependencias**

Se supone que los usuarios finales del sistema cuentan con conocimientos básicos de computación, por otra parte también se supone que los usuarios de soporte cuentan con conocimientos básicos y fundamentales en sistemas como para poder realizar configuraciones de uso o mantenimiento de las herramientas.

El servidor debe disponer de al menos un puerto de red para gestionar la red. El sistema operativo debe soportar las aplicaciones y base de datos a desarrollar. El almacenamiento de los datos se debe efectuar utilizando la base de datos relacional SQL Server, ofreciendo una solución con licencia GPL, facilidad de configuración e instalación, análisis de datos y seguridad de la información.

III. Requisitos Específicos

- **Interfaces Externas**

  - ✓ **Interfaz con el usuario**

El sistema debe ser amigable y predictivo con el usuario. Los usuarios o técnicos deben poder acceder mediante el uso de su ordenador, o laptop de la empresa, utilizando sus cuentas de usuario, realizar sus incidencias o la revisión de incidencias respectivamente. El sistema debe ser para el usuario interactivo, intuitivo y fácil de utilizar.

  - ✓ **Funciones**

Facilidad de configuración permita la simplicidad para realizar determinadas tareas de monitoreo.

Función de monitoreo de red permita el monitoreo de red mediante el protocolo SNMPv2, SNMPv3, los siguientes parámetros:

Tabla 5 Parámetros de los dispositivos que serán monitoreados

Dispositivo a monitorear	Parámetro	Descripción
Servidor/PC de Usuario	Memoria	Cantidad de Memoria RAM utilizada
	Estado	Si esta encendido y/o apagado
	Uso CPU	Estadística del uso del CPU

	Disco Duro	Cantidad de disco duro ocupado y libre
	Interfaces de Red	Número de Interfaces de Red que posee el Servidor
SWITCH	Interfaces	Monitoreo de interfaces

Fuente: Diseño personal

Función de notificaciones Permita funciones automáticas de notificaciones en caso de sobrepasar un umbral establecido.

Función de almacenamiento En la base de datos las actividades de control y monitoreo sean registradas en una base de datos.

Función de elaboración, consulta y soporte al usuario final Los usuarios finales deben poder realizar una incidencia, consultar el estado actual de la misma, por otra parte los técnicos debe tener funciones de visualización de las alarmas generadas, los estados actuales de los equipos de computación, y facilidad de interpretación de los gráficos de la red en un intervalo de tiempo.

Función de control de acceso Permita el acceso solo a los usuarios registrados en el sistema, en su modo de acceso, ya sea en administrador y modo cliente.

- **Requisitos de rendimiento**

Debe permitir al usuario tener documentación electrónica constante tanto para el uso como para el mantenimiento de la aplicación.

El sistema de gestión debe permitir la modificación de las aplicaciones después de cierto tiempo permitiendo corregir defectos, para mejorar su rendimiento.

- **Restricciones de diseño**

Las herramientas deben basarse en aplicaciones de software libre por requerimientos económicos y legales planteados por la institución pública.

La evaluación de herramientas escogidas se la realiza detalladamente en el Anexo E.

3.2. FUNCIONES DEL MODELO SNMP

Los aspectos tomados en cuenta para el levantamiento de requerimientos están orientados a las cuatro áreas funcionales del modelo SNMP, las cuales se muestran en la figura 16.

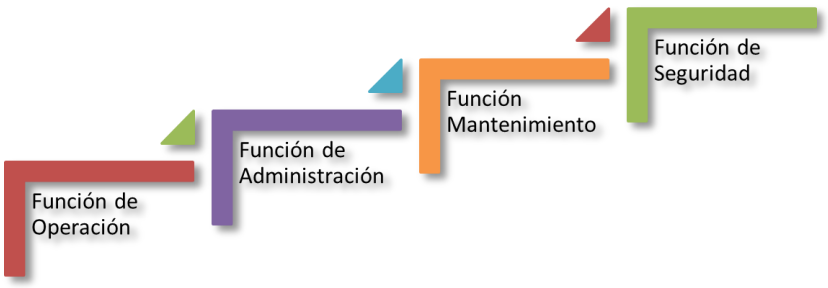


Figura 16 Modelo Funcional SNMP
Fuente: Adaptado de: Subramanian, A. & Timothy A. (2010). Network Management. 2da edición. Sitio de Publicación: Pearson Education India

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

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

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

Función de Mantenimiento.- Incluye las funcionalidades que garantizan la operación de la red y de los servicios de comunicación conforme lo esperado. Comprende actividades tales como diagnóstico, resolución de problemas, y reparación de componentes que no trabajan de acuerdo a lo planificado, a fin de mantener la red en un estado en el que pueda

ser utilizada continuamente y proporcionando el servicio apropiado. (Cátedra redes de información, 2010).

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

3.2.1. Función de operación del modelo SNMP

3.2.1.1. Inventario de la red

En primer lugar se realizó la configuración del centro de administración de red y la respectiva configuración de los agentes SNMP, las pruebas de funcionamiento se lo realizaron en los servidores los cuales están descritos en la tabla 3 y también en los equipos de encaminamiento que el departamento de informática está a cargo de dar un buen mantenimiento. Se escogió este sector al ser los principales equipos que hacen funcionar la red de datos, por lo que es necesario evaluar la capacidad de disco duro, memoria RAM y ancho de banda con el que cuentan para determinar de forma oportuna alguna falla o inconsistencia que suceda dentro de la red. Las configuraciones de los agentes SNMP se describen en el Anexo D.

Para la realización del monitoreo de la red, nos ayudamos de la herramienta Zabbix, al poseer un mecanismo que permite tener notificaciones flexibles para e-mail o SMS en cualquier evento que lo requiera, dando al administrador una rápida reacción a los problemas, es una solución en código libre que ofrece una interfaz web para monitorear y almacenamiento de la información en una base de datos, de igual forma existe una variedad de ayuda sobre esta herramienta en línea en el sitio web de Zabbix donde podremos encontrar las funciones, pasos de instalación y opciones de configuración. Tiene una amplia gama de plantillas incorporadas para notificaciones o se pueden crear dependiendo de las necesidades que tengamos, además nos presenta reportes en línea y los gráficos fáciles de interpretar. (Susan Perschke, 2015)

El funcionamiento básico de Zabbix es el siguiente: el servidor monitoriza por SNMP los equipos de red ingresados al sistema, realiza comprobaciones de ping y latencia, también procesa todas las operaciones “TRAPs” generados por los equipos. Los agentes monitorizan las características de los dispositivos y envían los datos al servidor de monitorización que se encarga de evaluarlos. El servidor revisa estos datos, y si se cumplen determinados parámetros que se establecen previamente se ejecutaran acciones como: envió de e-mails de aviso o mensajes SMS. (Javier Rodríguez, 2012)

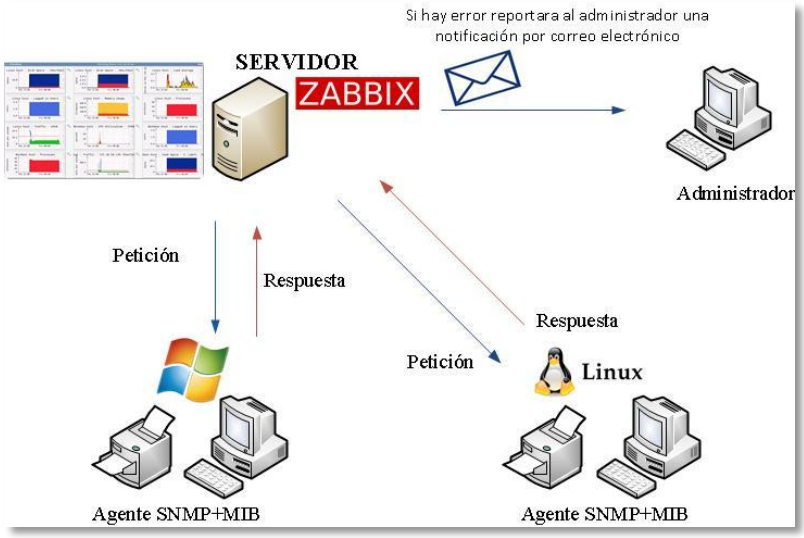


Figura 17 Funcionamiento Zabbix
Fuente: Adaptado de: Susan Perschke. (2015). Monitoreo de red.

Además para la realización del inventario y descubrimiento de los equipos de usuario final, nos ayudamos de la herramienta: Open Computer and Software Inventory Next Generation (OCS-NG) que es un software libre que permite a los usuarios de soporte administrar el inventario de los activos de la red, basada en un modelo cliente-servidor entre las cuales se intercambian información para obtener un diagnóstico, recopilando la información del software y el hardware instalado en los equipos de nuestra red en un sistema centralizado. Es multiplataforma, el servidor de administración utiliza como servidor web: Apache, como base de datos: MySQL. El diálogo entre los equipos clientes y el servidor se basan en HTTP (Hypertext Transfer Protocol) y el formato de los datos se

realiza en XML24, el soporte se lo realiza por medio de una comunidad de voluntarios y usuarios del mismo, que se encargan de actualizaciones o ingreso de plugins del mismo. (Comunidad OSC, 2013)

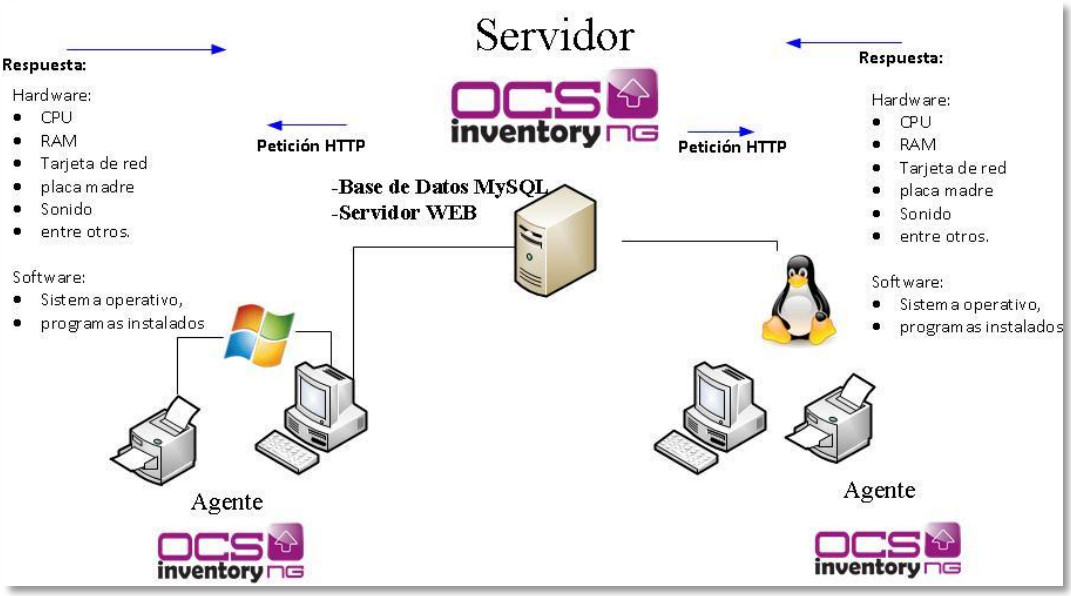


Figura 18 Funcionamiento OCS Inventory
Fuente: Adaptado de: Hypertextual. (2008). Automatiza la gestión de tus equipos con OCS.

La instalación del agente ocs-inventory en los equipos de usuario final se muestra en el Anexo D, esta herramienta se complementó con la plataforma GLPI para obtener el inventario de hardware y software instalado en los equipos de usuario final constantemente actualizado.

- **Fusión entre OCS-Inventory con GLPI.**

GLPI (Gestión Libre de Parque Informático) es una aplicación web con licencia GPL, es una plataforma en software libre que nos ayuda al momento de realizar la administración de los recursos informáticos con los que cuenta la institución, nos ayuda con el inventario del software y hardware existente en los usuarios finales, estos datos son almacenados en una base de datos, ya sea de forma manual, o uniendo el inventario que se obtiene con el servidor OCS-Inventory. Además GLPI incluye también software de mesa de ayuda para el registro y atención de solicitudes de servicio de soporte técnico, con posibilidades de notificación por correo electrónico a usuarios y al mismo personal de

[24] XML (eXtensibleMarkupLanguage): Lenguaje de marcas extensible es un lenguaje de marcas que permite definir la gramática de lenguajes específicos

soporte, el soporte se lo realiza por medio de una comunidad de voluntarios así como los usuarios del mismo, que se encargan de actualizaciones o ingreso de plugins al software. (Proyecto GLPI, 2012).

Tanto la instalación de OCS-Inventory como la de la plataforma GLPI se encuentran en el Anexo B.

- **Pruebas de funcionamiento de OCS-Inventory y GLPI**

Las pruebas de funcionamiento de estas herramientas se las realizó en el segundo piso de la institución, por ser a consideración del departamento de sistemas una zona ideal para iniciar el plan piloto, en donde se pueda ir observando con minuciosidad la colección de datos y evaluación de resultados. Los datos que se recolectó mediante este software se los presenta a continuación, en primer lugar tenemos la pantalla de inicio en donde se encuentran los equipos inventariados tanto en la red LAN como en la WLAN, en este caso tenemos 87 computadores inventariados y 187 interfaces sin inventariar en la base de datos.

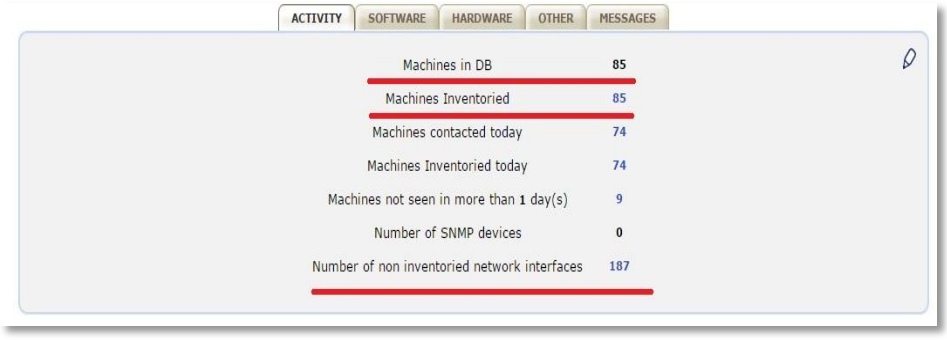


Figura 19 Elementos inventariados en la red de datos Emapa-I
Fuente: Datos obtenidos de la plataforma OCS

Las direcciones de red no se muestran por motivos de confidencialidad, en OCS-Inventory se almacenan los dispositivos que tenemos inventariados y los que aún no se encuentran con el agente OCS. Los equipos que se encuentran con el agente tendrán información sobre las características de software y hardware con los que cuentan los dispositivos finales y los que aún no se encuentran con el agente nos mostraran información básica del equipo gestionado, sin embargo una de las características que

indica un dispositivo sin el agente es la dirección IP, la cual nos puede ayudar para administrar o restringir servicios en ese dispositivo.

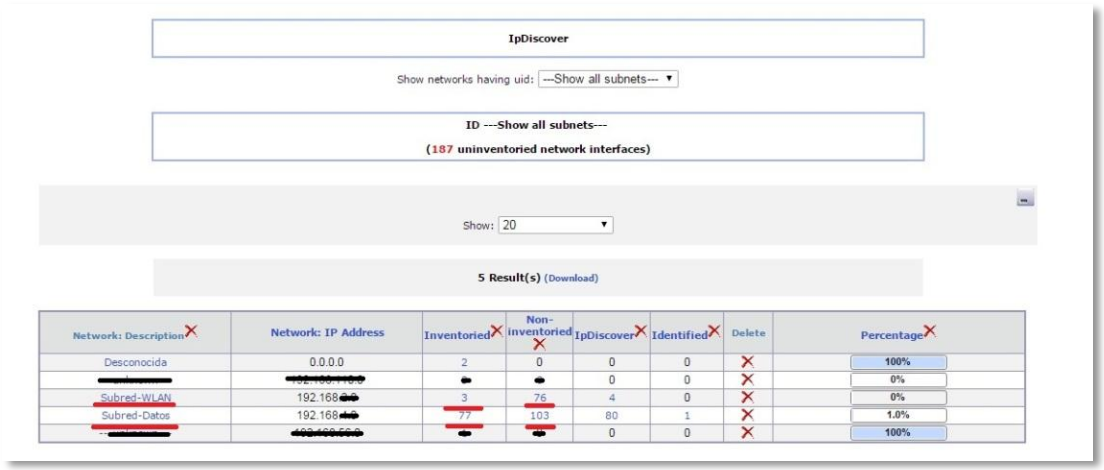


Figura 20 Equipos inventariados y no inventariados en la red de datos Emapa-I
Fuente: Datos obtenidos de la plataforma OCS

El inventario del direccionamiento IP y ubicación física de los host de usuario final, se muestran a continuación, los computadores en las que fueron instaladas el agente OCS-Inventory se les agregó una etiqueta en la que se indica el departamento al que pertenece, el cargo que ejerce y el nombre de la persona encargada del computador para ser utilizada por el departamento de informática, permitiéndole una mejor organización de los dispositivos de usuario final, datos que actualmente se manejaban mediante hojas en excel.

La etiqueta de ingreso de dispositivos de usuarios finales a la plataforma de inventario se lo estableció con el departamento de informática tomando en cuenta la siguiente nomenclatura: departamento de trabajo, sección en la cual se encuentra laborando, el cargo que ocupa y el primer nombre y primer apellido. Así como se lo muestra en la siguiente tabla.

Tabla 6 Nomenclatura de los computadores para el inventario en EMAPA-I

Departamento de Trabajo	**Sección**	**Cargo**	**Primer nombre/Primer Apellido**
Dirección Administrativa	Tecnologías de la Información y Comunicación	Asistente Administrativa	Pozo Dora

Fuente: **Diseño Personal**

Por motivos de confidencialidad no se muestran en su totalidad los usuarios que se inventariaron así como también las direcciones IP y direcciones MAC se ocultaron por la misma razón.

Nombre	Modelo	Número de serie	Sistema Operativo	Contacto	IP	MAC	Ubicación
CATASTROS01	HP Compaq Pro 6300 MT	MXL3111NGN	Microsoft Windows 7 Professional	ediaz	192.168	6C:3B:E5: C	Dirección Comercialización/ Acometidas Y Catastros/Asistent e De Catastros/Díaz Edwin
CATASTROS02	HP ProDesk 400 G1 MT	MXL4290N39	Microsoft Windows 7 Professional	fpaspuel	192.168	A0:D3:C1 D	Dirección Comercialización/ Acometidas Y Catastros/Asistent e De Comercialización/ Paspuel Fabricio
COMER09	HP ProDesk 400 G1 MT	MXL4232R90	Microsoft Windows 7 Professional	ymolina	192.168	9C:B6:54: 0	Dirección Comercialización/ Acometidas Y Catastros/Auxiliar Administrativa 1/Molina Yadira
ATCLIENTE	HP Compaq Pro 6300 MT	MXL3111PCJ	Microsoft Windows 7 Professional	wfarinango	192.168	6C:3B:E5: 1	Dirección Comercialización/ Atención al cliente/Asistente administrativo/Fari nango Willian
COMMER01	HP Compaq 6200 Pro MT PC	MXL2090NF9	Microsoft Windows 7 Professional	cmorejon	192.168	E8:39:35: 0	Dirección Comercialización/ Atención al cliente/Asistente cartera y cobranzas/Morejón Carlos
ATCLIENTE1B	HP Compaq 6200 Pro MT PC	MXL2072C8C	Microsoft Windows 7 Professional	rvizcaino	192.168	E8:39:35: A	Dirección Comercialización/ Atención Al Cliente/Asistente De Comercialización/ Vizcaíno Rosa
ATCLIENTE3M	HP Compaq Pro 6300 MT	MXL3111NBB	Microsoft Windows 7 Professional	fbrito	192.168	6C:3B:E5: 5	Dirección Comercialización/ Atención Al Cliente/Auxiliar Administrativa 1/Brito Fernanda
ATCLIENTE2M	HP Compaq Pro 6300 MT	MXL3111PCD	Microsoft Windows 7 Professional	jandrade	192.168	6C:3B:E5: C	Dirección Comercialización/ Atención Al Cliente/Auxiliar Administrativo 1/Andrade Jakeline
CARTECOBRA01	HP Compaq Pro 6300 MT	MXL3111NGQ	Microsoft Windows 7 Professional	mtapia	192.168	6C:3B:E5: C	Dirección Comercialización/ Cartera Y Cobranzas/Analist a Cartera Y Cobranzas/Tapia Marlon
CARTECOBRA02	HP Compaq 6200 Pro MT PC	MXL2090NF1	Microsoft Windows 7 Professional	fcaicedo	192.168	E8:39:35: 5	Dirección Comercialización/ Cartera Y Cobranzas/Asisten te Comercialización/ Caicedo Flor
VENTANILLA1B	HP Pro 3000/3080		Microsoft Windows 7 Professional	ocifuentes	192.168	40:61:86: C	Dirección Comercialización/ Cartera Y Cobranzas/Recau dador/Cifuentes Oscar

Nombre	Modelo	Número de serie	Sistema Operativo	Contacto	IP	MAC	Ubicación
COMPRASPUBLIC01	HP ProDesk 400 G1 MT	MXL4232R8C	Microsoft Windows 7 Professional	jvillamil	192.168	9C:B6:54:C	Dirección Administrativa/Director Administrativo/Director Administrativo/Villamil Javier
SEGURIDAD04	HP Compaq 6200 Pro MT PC	MXL2090NF5	Microsoft Windows 7 Professional	cgalindo	192.168	E8:39:35:	Dirección Administrativa/Seguridad Industrial Y Salud Ocupacional/Analista Seguridad Industrial/Galindo Christian
SEGURIDAD03	HP ProDesk 400 G1 MT	MXL4232R8S	Microsoft Windows 7 Professional	cgalindo	192.168	9C:B6:54:	Dirección Administrativa/Seguridad Industrial Y Salud Ocupacional/Analista Seguridad Industrial/Galindo Christian
SEGURIDAD02	HP Compaq 6200 Pro MT PC	MXL2090NF6	Microsoft Windows 7 Professional	cgalindo	192.168	E8:39:35:	Dirección Administrativa/Seguridad Industrial Y Salud Ocupacional/Asistente Administrativo 2/Ortiz Iván
BODEGA07	HP ProDesk 400 G1 MT	MXL4241QQG	Microsoft Windows 7 Professional	morbe	192.168	A0:D3:C19	Dirección Administrativa/Servicios y logística/Asistente de serv. Generales/Orbe Marianita
SGENERALES01	HP Compaq 6005 Pro SFF PC	MXL125177Q	Microsoft Windows 7 Professional	nflores	192.168	2C:27:D7:2	Dirección Administrativa/Servicios Y Logística/Auxiliar De Seguridad Industrial/Flores Nikhole
TALENTO03	HP Compaq 6005 Pro MT PC	MXL0310D62	Microsoft Windows 7 Professional	mcardenas	192.168	1C:C1:DEB	Dirección Administrativa/Talento Humano/Asistente De Talento Humano/Cardenas Miriam
HARDWARE	GA-MA785GM-US2H		Microsoft Windows 7 Professional	dpaez	192.168 192.168 0	00:24:1D:2	Dirección Administrativa/Tecnologías De La Información Y Comunicación/Analista Informático 2/Páez Darío

Figura 21 Direccionamiento IP y ubicación de los host de usuario final
Fuente: Datos obtenidos de la plataforma GLPI

La plataforma también nos permite obtener el número y marca tanto de impresoras como de monitores, software instalado, dispositivos de red, tarjetas de memoria RAM, etc, con los que cuenta cada usuario final. A continuación se muestra el inventario de las impresoras y monitores que se obtuvo en las pruebas de funcionamiento.

Nombre	Contacto
HP LaserJet Professional P1606dn	jandrade
HP LaserJet Professional P1606dn	restevez
HP LaserJet Professional P1606dn	lnavarrete
HP LaserJet Professional P1606dn	avillacis
HP LaserJet Professional P1606dn	mcardenas
HP LaserJet Professional P1606dn	cvalarezo
HP LaserJet Professional P1606dn	lmorales
HP LaserJet Professional P1606dn	mgomez
HP LaserJet Professional P1606dn	morbe
HP LaserJet Professional P1606dn	lcazar
HP LaserJet Professional P1606dn	pasante2
HP LaserJet Professional P1606dn	fbrito
HP LaserJet Professional P1606dn	jvillamil
HP LaserJet Professional P1606dn	Sistemas1
HP LaserJet Professional P1606dn	cescobar
HP LaserJet Professional P1606dn	gsiguencia
HP LaserJet Professional P1606dn	dproanio
HP LaserJet Professional P1606dn	Sistemas1
HP LaserJet Professional P1606dn	menriquez
HP LaserJet Professional P1606dn	epozo
HP LaserJet Professional P1606dn	ToshibaPortatil
HP LaserJet Professional P1606dn	jlecheverria
HP LaserJet Professional P1606dn	svega
HP LaserJet Professional P1606dn	Dir_Financiera
HP LaserJet P4515 UPD PCL 6	dalvarez
HP LaserJet P4515 UPD PCL 6	LUCIA GUERRON
HP LaserJet P4515 UPD PCL 6	Jorge
HP LaserJet P4515 UPD PCL 6	EProyectar
HP LaserJet P2015 Series UPD PCL 6	srivadeneira
HP LaserJet P2015 Series UPD PCL 6	EProyectar
HP LaserJet P2015 Series UPD PCL 6	bduenias
HP LaserJet P2015 Series PCL 6	srivadeneira
HP LaserJet P2015 PCL6 Class Driver	dalvarez

Figura 22 Inventario de impresoras de usuario final
Fuente: Datos obtenidos de la plataforma GLPI

Nombre	Fabricante	Contacto
HP LV1911	Hewlett Packard	jimbacuan
HP LV1911	Hewlett Packard	pandrade
HP LV1911	Hewlett Packard	wfarinango
HP LV1911	Hewlett Packard	morbe
HP LV1911	Hewlett Packard	mcastillo
HP LV1911	Hewlett Packard	bduenias
HP S1933	Hewlett Packard	stafur
HP S1933	Hewlett Packard	mpozo
HP S1933	Hewlett Packard	Sistemas1
HP S1933	Hewlett Packard	gjacome
HP S1933	Hewlett Packard	afarinango
HP S1933	Hewlett Packard	gsiguencia
HP S1933	Hewlett Packard	Sistemas1
HP S1933	Hewlett Packard	iortiz
HP S1933	Hewlett Packard	Sistemas1
HP S1933	Hewlett Packard	menriquez
HP S1933	Hewlett Packard	cgalindo
HP S1933	Hewlett Packard	fcaicedo
HP S1933	Hewlett Packard	jhidalgo
HP S1933	Hewlett Packard	yflores
HP S1933	Hewlett Packard	svega
Lenovo Group Limited RGB color	Lenovo Group Limited	lmorales
Lenovo Group Limited RGB color	Lenovo Group Limited	lmorales
Lenovo Group Limited RGB color	Lenovo Group Limited	lmorales
Lenovo Group Limited RGB color	Lenovo Group Limited	lmorales
Lenovo Group Limited RGB color	Lenovo Group Limited	lmorales
Lenovo Group Limited RGB color	Lenovo Group Limited	lmorales
LG Electronics Inc. (GoldStar Technology, Inc.) RGB color	LG Electronics Inc. (GoldStar Technology, Inc.)	ocifuentes
LG Electronics Inc. (GoldStar Technology, Inc.) RGB color	LG Electronics Inc. (GoldStar Technology, Inc.)	hvinueza
LG Electronics Inc. (GoldStar Technology, Inc.) RGB color	LG Electronics Inc. (GoldStar Technology, Inc.)	Sistemas1
LG Electronics Inc. (GoldStar Technology, Inc.) RGB color	LG Electronics Inc. (GoldStar Technology, Inc.)	jvillamil
LG Electronics Inc. (GoldStar Technology, Inc.) RGB color	LG Electronics Inc. (GoldStar Technology, Inc.)	lvaca
LG Electronics Inc. (GoldStar Technology, Inc.) RGB color	LG Electronics Inc. (GoldStar Technology, Inc.)	mdavila
LG Electronics Inc. (GoldStar Technology, Inc.) RGB color	LG Electronics Inc. (GoldStar Technology, Inc.)	drosero
LM765	AOC International (USA) Ltd.	marmas
S22B300	Samsung	ediaz
SMB1930N	Samsung	jaguilar
SMB1930N	Samsung	xpeñafiel
SMB1930N	Samsung	adelavega

Figura 23 Inventario de monitores de usuario final
Fuente: Datos obtenidos de la plataforma GLPI

Si se realiza cambios en los host de la red o en sus recursos informáticos, estos cambios deberán ser actualizados en la base de datos, con el fin de llevar una auditoria actualizada.

3.2.2. Función de administración del modelo SNMP

3.2.2.1. Mantenimiento del inventario

Las funciones de administración que abarcaremos están enfocadas en el seguimiento del inventario inicial así como también el proceso de ingreso de incidencias por parte de los usuarios finales.

Para realizar el mantenimiento del inventario inicial de los equipos de usuario final, usamos la herramienta GLPI, que como se mencionó anteriormente cuenta con las siguientes ventajas:

- Económica: Es una herramienta con licencia de código abierto
- Optimización de recursos: realiza la administración del inventario, con lo que podemos gestionar de mejor manera nuestros dispositivos dentro de la red.
- La mayoría de foros revisados dan calificaciones satisfactorias sobre esta plataforma
- Seguridad: Cuenta con niveles de usuarios por defecto a los cuales se les asigna ciertas características según el nivel configurado los cuales van desde usuario final, técnico de soporte y administrador total del sistema.

Se debe tomar en cuenta que antes de ingresar un computador para ser inventariado, el administrador deberá analizar el estado actual en el que se encuentra la red y posteriormente incluir el agente OSC-Inventory con su respectiva etiqueta de identificación al computador, para ser integrado directamente al software de inventario, lo cual posteriormente permitirá buscarlo de manera fácil en el sistema. El manual de usuario de esta plataforma se encuentra en el Anexo C.

3.2.2.2. Reporte de incidencias informáticas por parte de los usuarios finales

Mediante la auditoría realizada anteriormente (Portilla, Lissett, 2013), y mediante una conversación de confirmación con el departamento de informática se pudo concluir que:

- No existe un reporte bien estructurado al final del mes de las acciones que se realizan por parte del departamento de informática ya que las incidencias que los usuarios realizan en su mayoría son mediante teléfono o de forma verbal, lo que ocasiona en muchas circunstancias que la solución al daño existente no se registre por la urgencia de la solicitud realizada

- Al no haber un registro de las actividades realizadas por parte del departamento de informática no se puede determinar qué tiempo se llevó en dar una solución al problema, y las pocas cosas que se registran se las hacen en hojas de papel o en hojas de Excel, tomando un tiempo extra para organizar esa información.

Por lo tanto una mesa de ayuda entre el usuario final y el departamento de informática ayudaría a agilitar, organizar y documentar las funciones realizadas por ambas partes, permitiendo evaluar las actividades, ya sean diarias o mensuales, permitirá también tener una visión global de cual departamento requiere mayor atención y las causas más recurrentes para poder solventarlas con mayor rapidez, aumentando así tanto la calidad como la satisfacción en la atención del usuario final que es uno de los objetivos del departamento de informática.

Para asociar una herramienta a este sistema de mesa de ayuda se tomó en cuenta las siguientes características:

- Los usuarios deben reportar los incidentes en línea mediante una plataforma web
- Las respuestas a los usuarios finales y al departamento de informática deben ser ingresadas y recibidas tanto por la plataforma web como por el correo electrónico.
- Debe guardar la información tanto del hardware y software de cada usuario.
- Debe permitir adjuntar y almacenar documentos asociados a la incidencia.
- Debe permitir almacenar las soluciones que se vayan creando, para asociarlas a las incidencias que ingresen.
- Permita la creación de gráficos estadísticos
- Permita su instalación en un entorno Linux
- Permita realizar búsquedas especificas o globales

Por lo tanto, teniendo en cuenta que la herramienta GLPI nos sirve tanto como para la administración de los recursos informáticos y también cuenta con las características nombradas anteriormente, se escogió esta herramienta.

En primer lugar se realizó el siguiente flujograma que indica el proceso que tendrá la solución de incidentes en Emapa-I, el cual está abierto a cualquier cambio que realice el departamento de informática en el futuro.

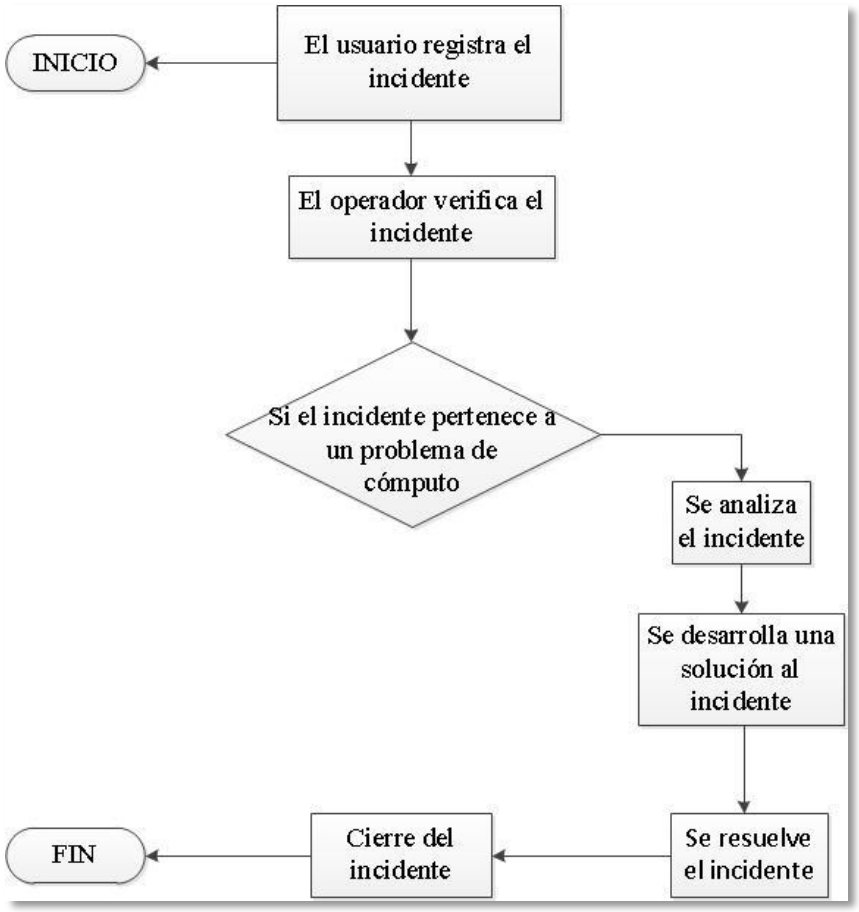


Figura 24: Registro y solución de incidentes en EMAPA
Fuente: Diseño personal

El funcionamiento de GLPI consistirá en que el usuario final ingrese a la plataforma web y emita la incidencia que puede estar relacionada con: problemas de ingreso al internet o al sistema integrado, problemas de impresión, daños con el mouse, el teclado, el teléfono, monitor, y daños relacionados con los recursos informáticos en general, por su parte el equipo de soporte, recibirá la incidencia tanto por la plataforma web como por el correo, y

de acuerdo a la urgencia del problema se tomaran las debidas consideraciones para resolver la incidencia, la cual se almacenará en una base de datos tanto para obtener reportes de las acciones realizadas como para hacer un seguimiento a la incidencia producida.

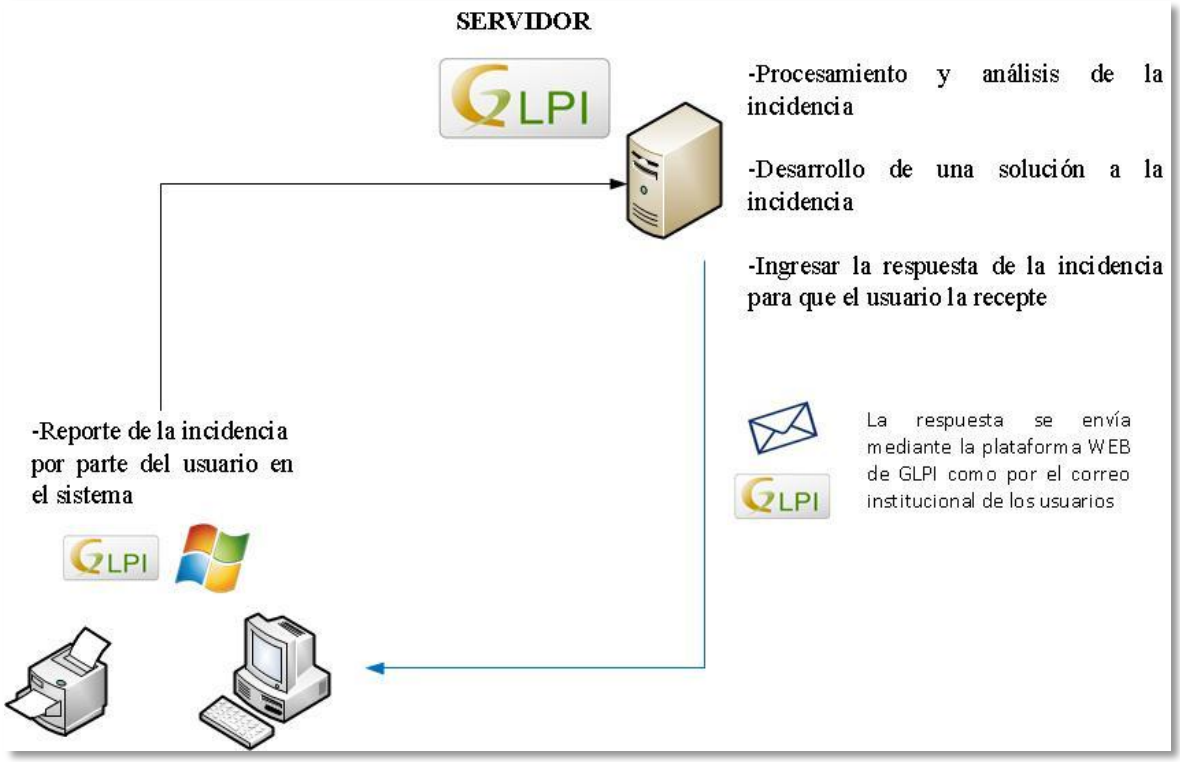


Figura 25 Funcionamiento GLPI
Fuente: Adaptado de: GLPI. (2012). El proyecto GLPI.

- **Pruebas de funcionamiento de GLPI**

Las pruebas de funcionamiento se lo realizaron en el segundo piso por ser a consideración del departamento de informática el que tiene un nivel recurrente de incidencias a la semana, para lo cual se realizó la respectiva socialización acerca del funcionamiento y la importancia de evaluar una herramienta que permita él envió y control de incidencias centralizadamente a través de una interfaz web.

Una vez instalada la herramienta, proceso que se muestra en el Anexo B, se creó los usuarios que van a ser parte del sistema, dividiéndoles como: técnicos de soporte y usuario final.

Para la creación de los usuarios se estableció el nombre de usuario con la unión de la primera letra del nombre seguido del primer apellido, y la contraseña con otro formato que por motivos de confiabilidad no se la menciona, además agregamos los correos electrónicos a los cuales les va a llegar las incidencias creadas o para dar el seguimiento a las mismas. De tal forma que los usuarios dentro del departamento de informática los cuales se encargaran de resolver las incidencias se los presenta a continuación.

Usuario	Apellido	Nombre	Perfiles (- Entidad)	Direcciones de correo electrónico	Activar
dpozo	Pozo	Dora	Technician - Entidad Raíz Admin - Entidad Raíz	dpozo@emapai.gob.ec	Si
jfuel	Fuel	Jorge	Technician - Entidad Raíz Admin - Entidad Raíz	jfuel@emapai.gob.ec	Si
dagarrido	Garrido	Daniel	Technician - Entidad Raíz Admin - Entidad Raíz	dgarrido@emapai.gob.ec	Si
chidrobo	Hidrobo	Carlos	Technician - Entidad Raíz Admin - Entidad Raíz	chidrobo@emapai.gob.ec	Si
dpaez	Paez	Dario	Super-Admin - Entidad Raíz Admin - Entidad Raíz	dpaez@emapai.gob.ec	Si
dmaldonado	Maldonado	Danilo	Super-Admin - Entidad Raíz Admin - Entidad Raíz	dmaldonado@emapai.gob.ec	Si

Figura 26 Usuarios para el soporte técnico de la plataforma GLPI
Fuente: Datos obtenidos de la plataforma GLPI

Los usuarios finales, son las personas que realizarán las incidencias, se los muestra a continuación, los cuales por motivos de confidencialidad no se muestran en su totalidad.

Usuario	Apellido	Nombre	Perfiles (- Entidad)	Direcciones de correo electrónico	Activar
gcevallos	Cevallos	Gloria	Self-Service - Entidad Raíz		Si
acevallos	Cevallos	Andrea	Self-Service - Entidad Raíz	acevallos@emapai.gob.ec	Si
lchicaiza	Chicaiza	Luis	Self-Service - Entidad Raíz		Si
grivadeneira	Rivadeneira	Giovani	Self-Service - Entidad Raíz		Si
ocifuentes	Cifuentes	Oscar	Self-Service - Entidad Raíz		Si
adavila	Dávila	Alexandra	Self-Service - Entidad Raíz		Si
srivadeneira	Rivadeneira	Sonia	Self-Service - Entidad Raíz	srivadeneira@emapai.gob.ec	Si
adelacruz	De La Cruz	Alejandra	Self-Service - Entidad Raíz		Si

Figura 27 Usuarios para el soporte técnico de la plataforma GLPI
Fuente: Datos obtenidos de la plataforma GLPI

En el periodo de pruebas se pudo obtener varias incidencias, en la cual se iban realizando algunas adecuaciones indicadas por el departamento de informática para obtener un diseño de acuerdo a las necesidades de la empresa, las cuales están especificadas tanto en los manuales de usuario y de soporte en el Anexo C.

A continuación se muestran algunas de las incidencias que se fueron almacenadas en el periodo de pruebas, en donde se puede observar, la descripción del problema. A que categoría pertenece, el estado en el que se encuentra la incidencia, la prioridad que se le asigno, el usuario que presenta la incidencia, y el técnico que está encargado de resolver la incidencia.

ID	Título	Categoría (Clase)	Estado	Última actualización	Fecha de Apertura	Prioridad	Autor	Asignado a: - Técnico
6	Monitor		Resuelto	2015-10-15 15:48	2015-10-15 15:45	Mediana	prueba	
8	Daño de contrasena	Sistema Compras	Resuelto	2015-11-13 13:03	2015-10-15 16:46	Mediana	Tixilima Silvia	Garrido Daniel
9	Fallo en el monitor	Pc-Monitor	Resuelto	2015-11-13 13:01	2015-10-16 14:41	Mediana	Maldonado Danilo	Garrido Daniel
16	No imprime	Pc-Impresora	En curso (asignada)	2015-11-13 12:56	2015-11-05 11:32	Mediana	Morales Lauro	Pozo Dora
17	Ya no hay tinta	Pc-Impresora	Resuelto	2015-11-13 12:58	2015-11-05 12:13	Mediana	Espinosa Carlos	Garrido Daniel
18	Solicito la instalacion de autocad	Pc-Programas .	Resuelto	2015-11-13 12:58	2015-11-06 10:34	Mediana	Castillo Ana	Garrido Daniel
19	No imprime	Pc-Impresora	En curso (asignada)	2015-11-13 12:54	2015-11-06 11:28	Mediana	Brito Fernanda	Maldonado Danilo
29	Sale ruidoso	Teléfono	Resuelto	2015-11-13 13:06	2015-11-11 14:57	Mediana	Vega Katherine	Fuel Jorge

Figura 28 Incidencias almacenadas en la base de datos
Fuente: Datos obtenidos de la plataforma GLPI

Esta herramienta nos permite exportar la información que se encuentra en la plataforma en formato pdf lo cual nos ayuda en la creación de informes o reportes que tengamos que entregar tanto al fin del día, o fin de mes.

También tenemos dentro de la plataforma una opción que nos despliega gráficamente las incidencias que se realizaron en un determinado tiempo, por ejemplo, a continuación se muestra en azul el número de incidencias que se realizaron por parte de los usuarios, y en color verde el número de incidencias que se resolvieron.

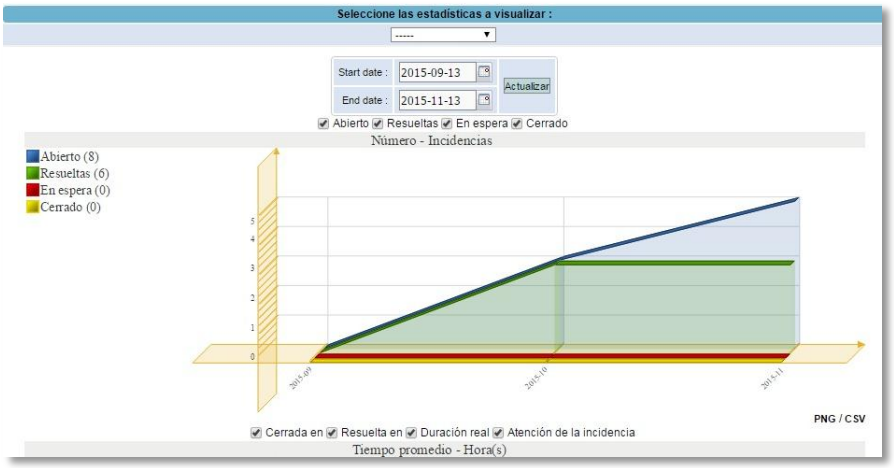


Figura 29 Estadísticas de resolución de incidencias almacenadas en la base de datos
Fuente: Datos obtenidos de la plataforma GLPI

3.2.3. Función de mantenimiento del modelo SNMP

3.2.3.1. Proceso de detección de fallas

Se realizará la monitorización de los equipos de encaminamiento y servidores descritos anteriormente con el fin de determinar el comportamiento de la red, a continuación se presenta la estructura de corrección de fallas que seguiremos en la institución.

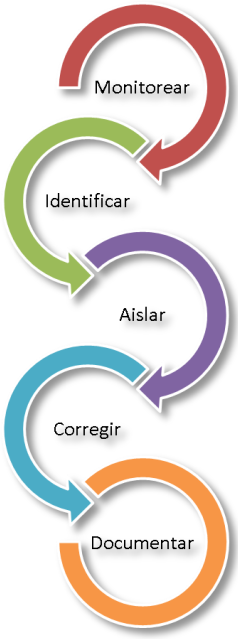


Figura 30 Proceso de detección de fallas en la institución
Fuente: Diseño Personal

- **Monitoreo de alarmas**

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

Por este motivo para el establecimiento de los umbrales que contará el sistema de gestión se tomó en cuenta el criterio basado en la descripción del rendimiento de la plataforma Microsoft Exchange (2012), en el cual nos dice que: "El uso del procesador en un servidor debería mantener una carga del 60 % aproximadamente durante las horas de máxima actividad. Este porcentaje deja margen para períodos de carga muy elevada. Si el uso del procesador está por encima del 75% de manera continuada, el rendimiento del procesador se considera un cuello de botella".

Llevando este criterio a nuestra red, se propone plantear los siguientes umbrales para mantener las condiciones más seguras y optimas de funcionamiento de los equipos y dispositivos de red. Por lo tanto si estos niveles se superan se recomienda ejecutar alguna notificación que ayude al personal de soporte efectuar medidas necesarias para reducir el tiempo de degradación de un dispositivo dentro de la red.

Tabla 7 Umbrales escogidos en los dispositivos monitoreados

Dispositivo a monitorear	**Parámetro**	**Umbrales Nivel Informativo**	**Umbrales Nivel Alta**	**Umbrales Nivel Critico**
Servidor/PC de Usuario	Uso CPU		>60%	>80%
	Memoria RAM		>60%	>80%
	Disco duro		>60%	>80%
Switches/Firewall	CPU		>60%	>80%

	Ancho de banda en interfaces troncales	>60% >80%	

Fuente: **Diseño personal**

- **Identificación de la falla**

Al momento que se encuentra una incidencia en los equipos de red, se procederá a buscar la causa del origen del problema, los iniciadores de alamas que nos muestre la plataforma Zabbix, nos ayudará a encontrar el equipo que generó la incidencia, pero para resolverla se necesita de pruebas adicionales las cuales dependerán de conocimiento de red del administrador para que pueda proponer posibles soluciones, básicamente se puede presentar las siguientes soluciones encaminadas al modelo TCP/IP. (Alexander Clemm, 2007).

  - **Capa acceso a la red.** En primer lugar se debe revisar si los equipos de red como switch, router, servidores se encuentran encendidos, igualmente revisar los cables de conexión si se encuentran en perfecto estado y conectados al puerto correcto.

  - **Capa internet.** En segundo lugar se debe verificar si las direcciones IP y máscaras de red están de acuerdo a la red a la que se encuentran, y realizar pruebas de conectividad como por ejemplo, un "ping" a la puerta de enlace.

  - **Capa Transporte y Aplicación.** Una vez que hemos verificado la conectividad física y la comunidad lógica procedemos a observar los tiempos de respuesta tanto desde el equipo que produjo la alarma como del equipo que realiza la función de puerta de enlace, en estas pruebas se debe revisar si existe pérdida en los paquetes que se envían.

- **Aislamiento**

Se debe tomar en cuenta que los equipos que presentan algún inconveniente critico afectan drásticamente al funcionamiento de red, por este motivo se debería tener un

documento basado en las configuraciones de los equipos o adquirir un dispositivo que sirva de respaldo para ayudar a solventar el problema por un cierto tiempo, de tal forma que se disminuya el impacto de la falla en la red de datos. (Dolores Gómez, 2014).

- **Corrección de la Falla**

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

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

- **Documentación**

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

3.2.3.2. Monitoreo de los equipos de red

En primer lugar se verifico que los equipos a los que configuramos el agente snmp se encuentren activados, en esta plataforma los dispositivos que se encuentran con color verde en el icono del protocolo son tomado como disponibles, mientras que el color rojo indica que el equipo es inaccesible a la petición snmp.

Figura 31 Equipos activos y no activos con snmp
Fuente: Obtenida de la plataforma Zabbix

El método para ingresar un usuario a la plataforma se encuentra indicado en el manual de usuario el cual se encuentra en el anexo C, la etiqueta de ingreso de dispositivos de red y servidores a la plataforma de monitoreo de red se lo estableció con el departamento de informática tomando en cuenta la siguiente nomenclatura.

Tabla 8 Nomenclatura de servidores de red snmp

Nombre del protocolo	Siglas Servidor o conmutador	Nombre del servicio
snmp	Srv	Correo

Fuente: **Diseño personal**

Tabla 9 Nomenclatura de conmutadores de red snmp

Nombre del protocolo	Siglas conmutador	Número de puertos	Inicial de la marca del dispositivo seguida de su numeración	Piso en el que se encuentra
snmp	Sw	24p	D3028	pp

Fuente: Diseño personal

A continuación se muestran los equipos que vamos a gestionar en esta plataforma que por motivos de confidencialidad se ocultó la dirección IP.

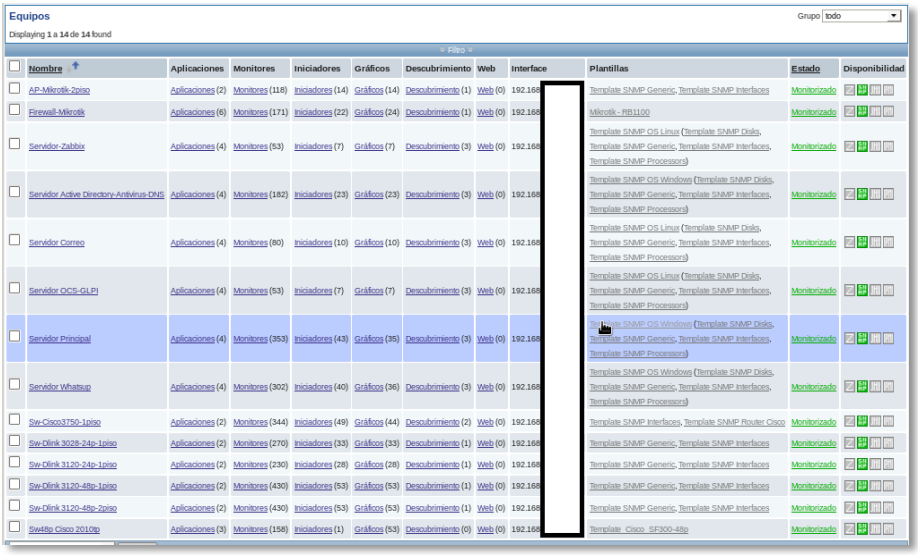


Figura 32 Equipos monitoreados con Zabbix
Fuente: Obtenida de la plataforma Zabbix

Una vez que agregamos los equipos a la plataforma y confirmamos que están activos, procedemos a graficar el mapa topológico de la red, proceso que se encuentra en el manual de usuario ubicado en el anexo C.

Para la graficar el mapa topológico se tomó en cuenta agregar tanto un icono que represente al dispositivo gestionado, la información que lo identifique y la dirección IP para su pronta ubicación.

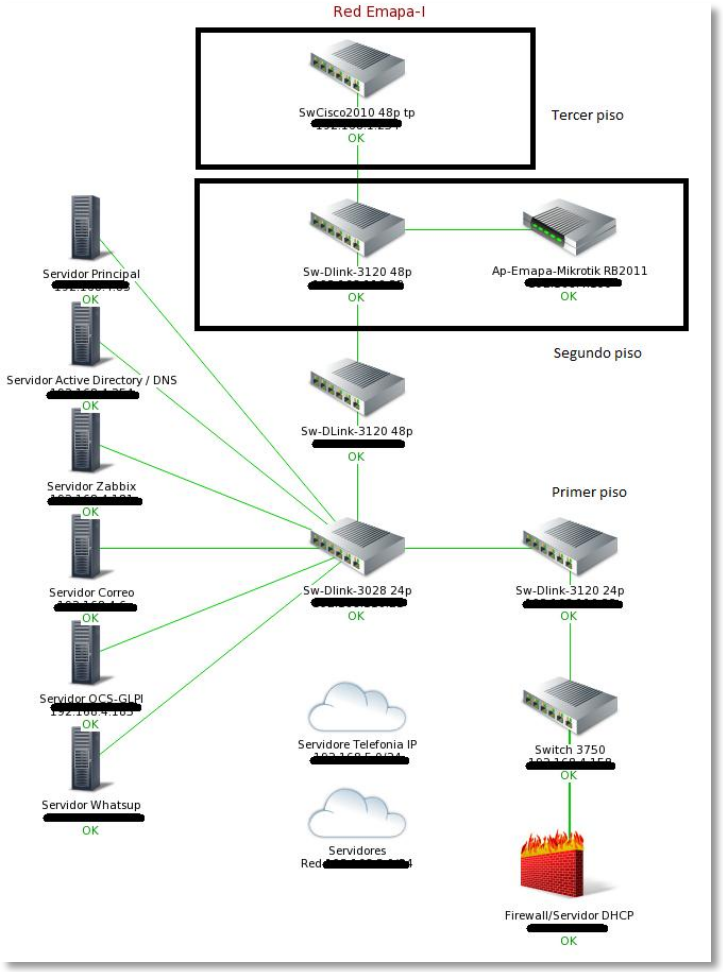


Figura 33 Mapa topológico de Emapa-I
Fuente: Obtenida de la plataforma Zabbix

La plataforma Zabbix nos permite configurar los umbrales, los cuales se pueden visualizar mediante niveles de gravedad los cuales se describen a continuación.

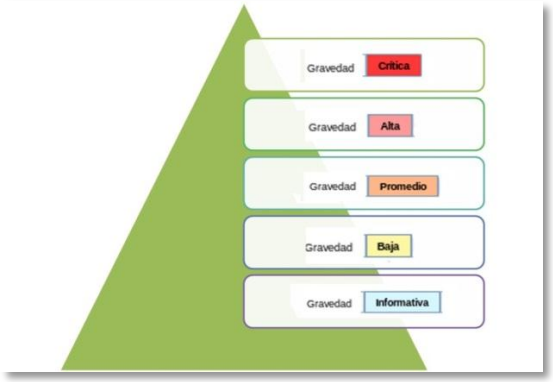


Figura 34 Niveles de gravedad en la plataforma Zabbix
Fuente: Adaptado de: Zabbix. (2014). Documentation. **Recuperado de:** https://www.zabbix.com/documentation/2.4/manual/config/triggers/severity

- **Informativa:** Para propósitos de información como por ejemplo: el cambio de estados de interface
- **Baja:** Incidencias que al producirse, no afecta mayormente el funcionamiento de la red.
- **Promedio:** Mal funcionamiento de equipos de red.
- **Alta:** Umbrales que permiten un tiempo prudente para dar solución
- **Critica:** Umbrales que al sobrepasarlos nos puede causar falla en los servicios, daños en el software o en el hardware.

Los umbrales que se escogieron son los especificados en la tabla 8, en los cuales al sobrepasarse se enviará un correo al administrador notificándole que algún valor ya sea en la memoria RAM, disco duro, o si el uso del CPU fue sobrepasado de los valores establecidos. El proceso de configuración del envío de correo electrónico cuando se sobrepase un umbral se muestra en el anexo B.

Figura 35 Umbrales establecidos en los equipos de Emapa-I
Fuente: Obtenida de la plataforma Zabbix

- **Resultados del monitoreo de la red**

En la pantalla de inicio de la plataforma Zabbix se puede observar el número de elementos que se están gestionando, y si algún equipo tiene problemas se mostrarán de esta manera.

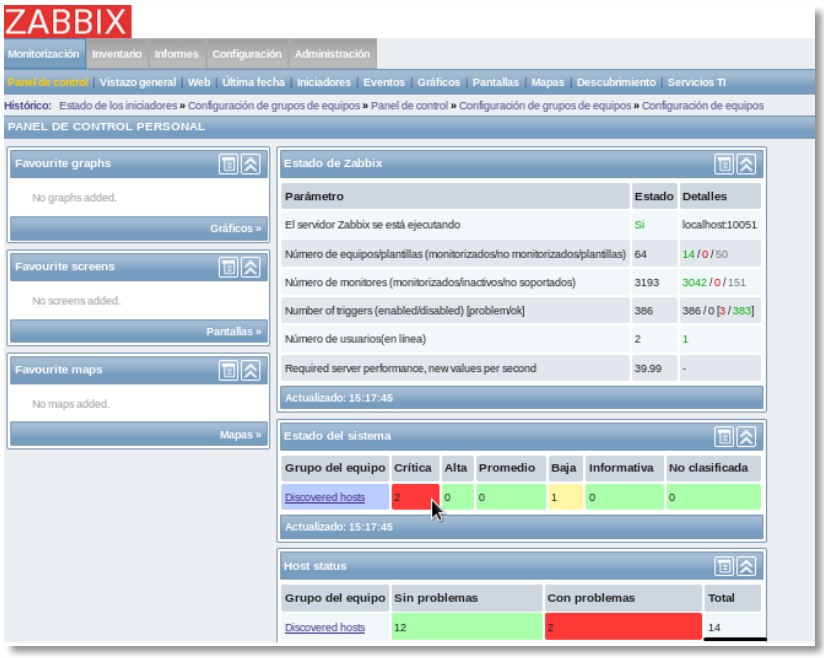


Figura 36 Niveles de gravedad en los equipos de Emapa-I
Fuente: Obtenida de la plataforma Zabbix

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

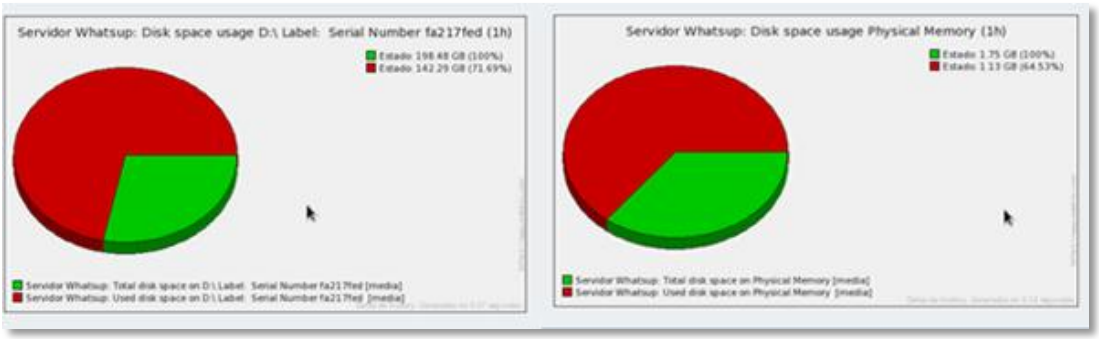


Figura 37 Espacio de discos duros
Fuente: Obtenida de la plataforma Zabbix

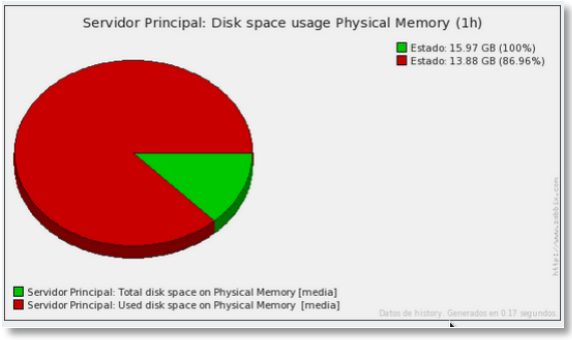


Figura 38 Espacio de memoria RAM
Fuente: Obtenida de la plataforma Zabbix

- . **Posibles fallos que pueden encontrarse en los Servidores**

Cuando el dispositivo presenta una alerta de color rosa, quiere decir que los umbrales establecidos permiten un tiempo prudente para dar solución, las situaciones podrían ser las siguientes:

- Carga de CPU, memoria RAM, espacio del disco, utilizadas en un 60% de su capacidad

En esta situación lo más prudente es realizar pruebas de funcionamiento para encontrar la razón de la sobrecarga antes que llegue a un estado crítico.

Cuando el dispositivo presenta una alerta de color rojo, quiere decir que los umbrales establecidos se sobrepasaron, las situaciones podrían ser las siguientes:

- Carga de CPU, memoria RAM, espacio disco, utilizadas en más del 80% de su capacidad, o perdida de conexión con el equipo gestionado

Para solventar este tipo de inconvenientes se debe retomar los pasos establecidos en la identificación, aislamiento y corrección de la falla mencionados anteriormente.

Una vez que se decide una solución a este incidente procedemos a documentarlo, para este proceso se deja como opción el uso de la plataforma GLPI que nos permite almacenar datos de las incidencias producidas en una plantilla digital como se muestra a continuación.

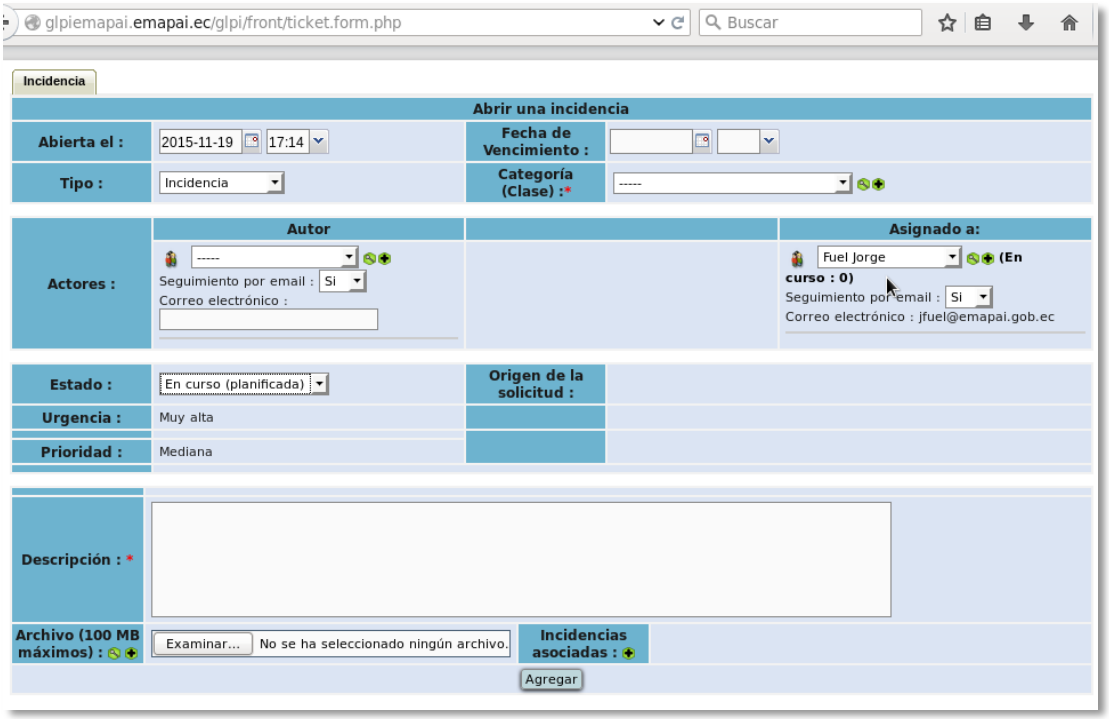


Figura 39 Plantilla de incidencias GLPI
Fuente: Obtenida de la plataforma GLPI

A continuación se describe cada campo de la plantilla de incidencias en la plataforma GLPI:

- **Fecha:** Tanto para agregar la fecha del inicio como el fin de la incidencia.
- **Tipo**: Se debe escoger entre si es una Incidencia (comunicar la falla de un servicio/equipo) o un Requerimiento (solicitar un equipo o un reporte al administrador/técnico).
- **Autor:** Campo para agregar el nombre del técnico que está revisando o resolviendo la incidencia.
- **Asignado a técnico:** Campo para asignar el problema a otro técnico dentro de la institución.
- **Categoría:** Se debe escoger una opción de la lista despegable, se puede escoger una categoría de las ya establecidas o agregar una categoría al problema que se está resolviendo.
- **Urgencia:** Si la incidencia debe atenderse muy rápidamente se escogerá los niveles altos, caso contrario se ubicaría un nivel bajo, medio, alta, muy alta.

- **Estado:** El estado en el que se encuentra la incidencia, se puede elegir si está abierta, solucionándose o si la incidencia está resuelta.
- **Descripción:** Aquí se realiza una descripción detallada y clara sobre su incidencia.
- **Archivo:** Se puede adjuntar un archivo (máximo 100MB) con información sobre la incidencia, en el que podemos adjuntar captura de pantalla de lo que esté sucediendo, o algún documento referente a la situación de la incidencia.

- **Posibles fallos que pueden encontrarse en los Conmutadores**

Cuando el dispositivo presenta una alerta de color rosa quiere decir que los umbrales establecidos permiten un tiempo prudente para dar solución, las situaciones podrían ser las siguientes:

- Carga de CPU, 60% de su capacidad

En esta situación lo más prudente es realizar pruebas de funcionamiento para encontrar la razón de la sobrecarga antes que llegue a un estado crítico.

Cuando el dispositivo presenta una alerta de color rojo, quiere decir que los umbrales establecidos se sobrepasaron, las situaciones podrían ser las siguientes:

- Carga de CPU o temperatura en el 80% de su capacidad

Al tener dentro de la red una serie de switches interconectados, da origen a un dominio de broadcast, lo que puede ser causa de consumo elevado en el CPU, por la razón siguiente: si un conmutador recibe una trama de broadcast la reenvía a cada uno de sus puertos excepto al puerto por donde fue recibida esta trama, entonces cada dispositivo conectado al conmutador recibe la trama y la procesa, causando que se use un cierto porcentaje de ancho de banda para propagar este tipo de tráfico. (Oscar Gerometta, 2012)

Para solventar inconvenientes relacionados a conmutadores, se debe considerar la disminución del dominio de broadcast, como por ejemplo con la creación de VLANs, para

descartar otras incidencias se debe retomar los pasos establecidos en la identificación, aislamiento, corrección y documentación de la falla mencionados anteriormente.

- **Informes históricos**

Es importante registrar los problemas de una forma global, para realizar un análisis general, de tal manera que obtengamos datos estadísticos del desempeño de la red. (Cátedra redes de información, 2010). El historial de lo que va ocurriendo en la red se la puede revisar en la plataforma Zabbix, permitiendo evaluar los distintos fallos que se van produciendo, y revisar tendencias que permitan anticipar las incidencias.

A continuación se muestra los datos históricos obtenidos del monitoreo de la red en la plataforma Zabbix.

Figura 40 Informe histórico de umbrales superados
Fuente: Obtenida de la plataforma Zabbix

En donde la tendencia en varios servidores es que tanto el uso de la memoria RAM como del disco duro están utilizados casi en su máxima capacidad lo que puede incitar a

que algunos servidores dejen de funcionar, provocando que el rendimiento de la red se degrade. Por lo que es recomendable realizar la planificación para un respectivo mantenimiento a estos equipos.

- **Gráficos**

Los gráficos en un sistema de monitorización son de gran de ayuda, pues nos permiten evaluar tanto con valores actuales como su evolución en un parámetro especifico a través del tiempo.

Los siguientes gráficos pertenecen al equipo MIKROTIK que es usado como firewall en EMAPA-I, para el resto de equipos se tiene un formato similar.

El uso del CPU en intervalos de porcentaje

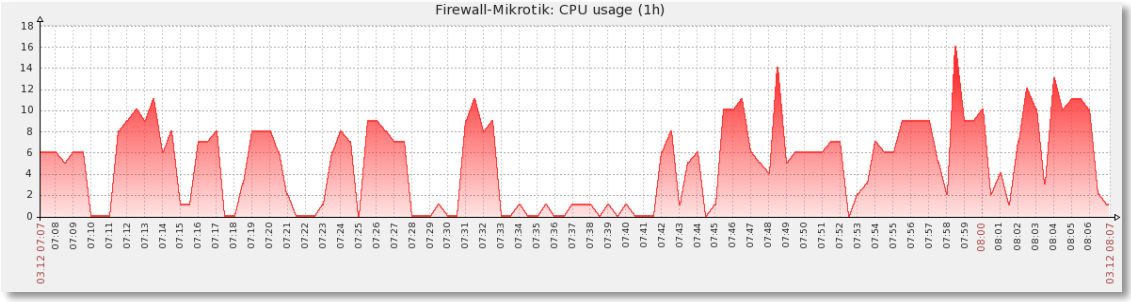


Figura 41 Uso del CPU en el equipo Firewall
Fuente: Obtenida de la plataforma Zabbix

El uso del disco duro se encuentra identificado por la línea color verde, mientras que su capacidad se encuentra con color violeta.

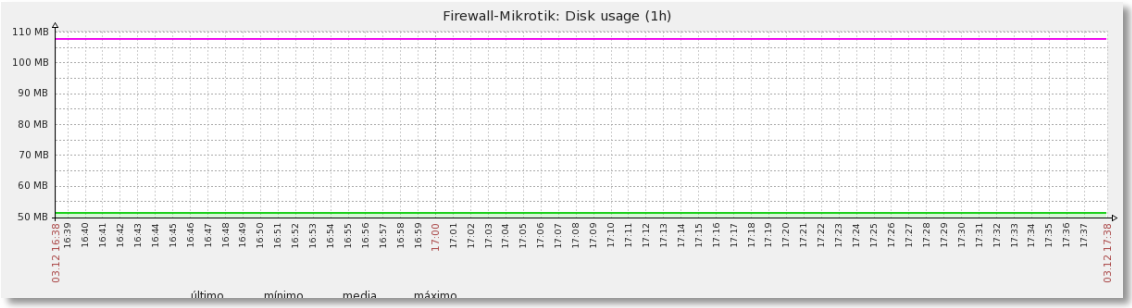


Figura 42 Uso del disco en el equipo Firewall
Fuente: Obtenida de la plataforma Zabbix

El uso de la memoria se identifica de color amarillo, mientras que la capacidad de memoria se encuentra identificada de color verde.

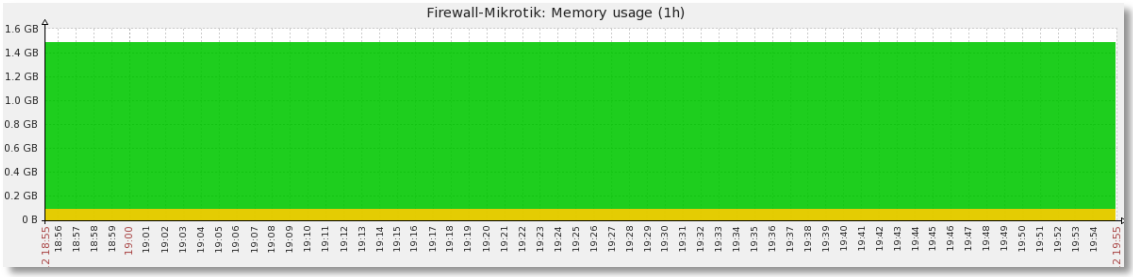


Figura 43 Uso de la memoria en el equipo Firewall
Fuente: Obtenida de la plataforma Zabbix

La temperatura del CPU se identifica con el color rojo

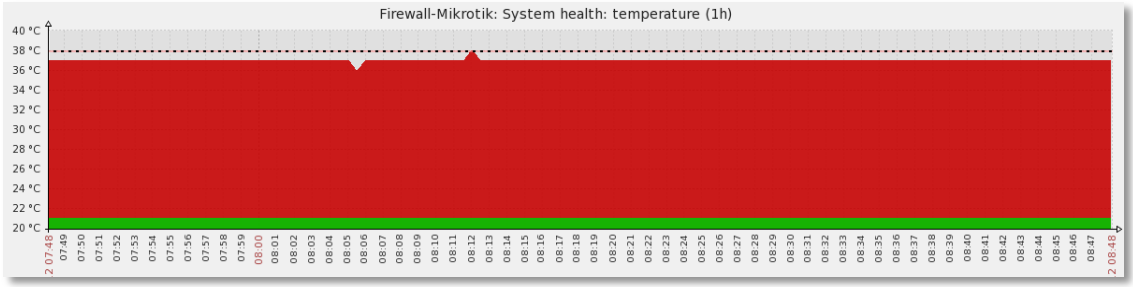


Figura 44 Temperatura en el equipo Firewall
Fuente: Obtenida de la plataforma Zabbix

El tráfico de la red en la VLAN de datos se lo puede revisar en la siguiente grafica donde el tráfico entrante se encuentra de color verde, mientras que el tráfico saliente en color violeta.

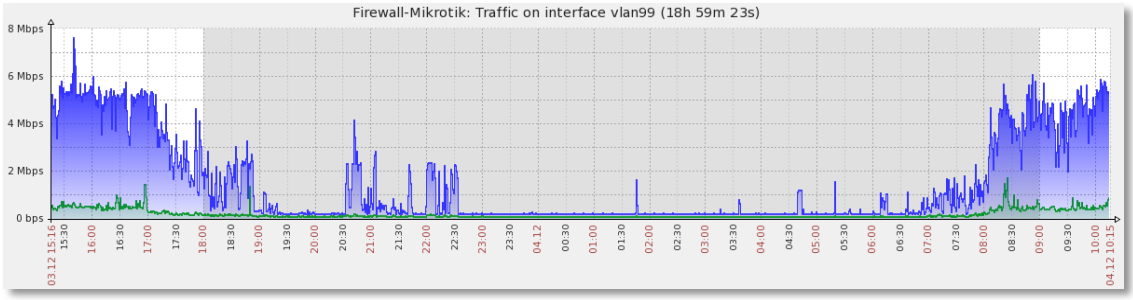


Figura 45 Tráfico de red en la VLAN de datos
Fuente: Obtenida de la plataforma Zabbix

3.2.3.3. Mantenimiento de los servidores de inventario y monitoreo

Se debe tomar en cuenta que estos servidores al realizar una constante petición de datos la capacidad en disco duro ira disminuyendo poco a poco. Una forma de realizar el mantenimiento a estos equipos es realizando periódicamente la limpieza de archivos logs. Ya que son datos que se van acumulando según la plataforma realice su actividad normal, estos datos a largo plazo, nos ocuparan espacio en disco duro y que para el estudio nos resultaran obsoletos. Para vaciar estos archivos y empiecen su actividad desde cero aplicaremos el siguiente comando en modo administrador:

cat /dev/null >/var/log/zabbix/zabbix_server.log

Donde el comando cat /dev/null borra el contenido del archivo zabbix_server.log ubicado en la dirección: var/log/zabbix/

Esto nos ayuda a vaciar todos los datos que se acumularon en el proceso del funcionamiento del servicio Zabbix. Este proceso se lo puede realizar cada semana una vez que hayamos recopilado los datos que necesitemos para evaluar nuestra red de datos.

3.2.4. Función de seguridad del modelo SNMP

3.2.4.1. Seguridad de la administración

Es la que se encarga de garantizar el acceso solo a usuarios que estén autorizados a las aplicaciones que realizan configuraciones o monitorizaciones a los equipos, ya que cualquier plataforma está sujeta a cambios, y alguna configuración equivocada dentro de estos dispositivos puede estar vinculada a los siguientes aspectos: permitir el acceso de los servicios a usuarios que no están autorizados, interrumpir servicios, vulnerar la confidencialidad de la información, lo que poco a poco provocaría la degradación del rendimiento de la red. (Alexander Clemm, 2007)

Por lo tanto, en las herramientas que fueron instaladas se tomaron en cuenta las siguientes observaciones, mientras que para los demás equipos que se encuentran en la red de datos se dejó como recomendación a seguir.

- Asignación de privilegios de acceso solo aquellas personas que necesitan un constante ingreso ya sea para obtener reportes o ingresar nuevos equipos al sistema de monitoreo.

- Ingresar una contraseña robusta que integre letras, número y símbolos, para que sean más difícil de vulnerar.
- Realizar un cambio de contraseña a los equipos que se encuentren a su cargo cada cierto tiempo
- Tener un punto de restauración de los equipos en caso de alguna falla para tener un respaldo de los datos obtenidos

El ingreso a los servidores se lo puede realizar mediante el acceso directo al equipo o vía remota mediante un cliente SSH, el cual estará disponible solo a los usuarios que dispongan de cuenta de administrador en los equipos.

3.2.4.2. Monitoreo basado en snmpv3

El protocolo Simple Network Management Protocol (SNMP) es un protocolo ampliamente utilizado tanto para la vigilancia como para el mantenimiento de los equipos de red y equipo de cómputo, pero con ciertas vulnerabilidades en la seguridad, por este motivo en el año 1998 la IETF en los RFC del 2271 al 2275 definen un conjunto medidas para cubrir las debilidades que tenía este protocolo, las cuales eran: autenticación, seguridad y control de acceso. (Alejandro Corletti, 2011).

- **Niveles de seguridad en SNMPv3**

El agente SNMPv3 admite el siguiente conjunto de niveles de seguridad tal como se define en el RFC 2574:

- **noAuthNoPriv.-** Comunicación sin autenticación y privacidad.
- **authNoPriv.-** Comunicación con la autenticación y sin privacidad. Los protocolos utilizados para la autenticación son MD5 y SHA.
- **authPriv.-** Comunicación con la autenticación y privacidad. Los protocolos utilizados para la autenticación son MD5 y SHA; y de privacidad, se pueden utilizar los protocolos de DES (Data Encryption Standard) y AES (Advanced Encryption Standard).

La diferencia entre los algoritmos DES y AES son básicamente la longitud la contraseña, pues mientras DES admite 64 bits en su contraseña, AES usa 128 hasta 256 bits de longitud de contraseña, recalcando que entre más bits abarque, se hace más difícil que alguien pueda vulnerarla. (Alejandro Corletti, 2011).

Igualmente la diferencia entre el protocolo MD5 y SHA, es que a partir de un texto cualquiera, genera una serie de caracteres con un tamaño de 128 bits mientras que SHA genera una serie de 160 bits. Convirtiendo al protocolo SHA más seguro porque se debe procesar varios bits adicionales que MD5. (Alejandro Corletti, 2011).

- **Usuarios predeterminados en el agente de SNMPv3**

Por defecto, el agente SNMPv3 proporciona soporte para tres niveles de usuarios:

- **noAuthUser**.- Los usuarios con nivel de seguridad noAuthNoPriv
- **authUser.-** Los usuarios con nivel de seguridad authNoPriv
- **privUser** - Los usuarios con nivel de seguridad authPriv

- **Modelo de seguridad basado en usuario**

El modelo de seguridad basado en usuario o USM (User-Based Security Model) proporciona los servicios de autentificación y privacidad en SNMPv3. El mecanismo de autentificación en USM asegura que un mensaje sea trasmitido y recibido por la entidad correspondiente, para esto tanto el agente como el gestor verifican el campo correspondiente en la cabecera del mensaje; este modelo también nos indica que el

mensaje no fue alterado o retardado durante su transmisión. Las contraseñas no son almacenadas en la MIB y no son accesibles mediante SNMP. (RFC 3414).

- **El modelo de control de acceso basado en vistas**

El modelo de control de acceso basado en vistas o VCAM (Views-Based Access Control Model) permite proporcionar diferentes niveles de acceso a las MIB de los agentes para los distintos gestores en SNMPv3, es decir, un agente puede restringir el acceso de los gestores a cierta parte de su MIB. La política de control de acceso a ser utilizada por el agente para cada gestor debe estar configurada previamente; consistiendo básicamente en una tabla que detalla los privilegios de acceso para los distintos gestores autorizados. (RFC 3415).

3.2.4.3. Pruebas de funcionamiento del monitoreo con SNMPv3

Las pruebas de funcionamiento con el protocolo SNMPv3 se lo realizaron en el departamento financiero, donde por tener información confidencial se requiere monitoreo con cierto nivel de seguridad.

En primer lugar se revisó el número de dispositivos a monitorear y el usuario encargado del equipo, este proceso se lo realizó con el departamento de informática el cual me brindo el nombre de los usuarios del departamento financiero, y mediante la herramienta GLPI que me ayudo tanto con la obtención del sistema operativo que tiene cada usuario como también su dirección IP.

A continuación se presenta los miembros que se encuentran en el departamento financiero, por motivos de seguridad solo se presenta la inicial del primer nombre seguido de su primer apellido, y de igual forma no se presenta la dirección IP en su totalidad.

Tabla 10 Miembros del departamento financiero en EMAPA

Número de Usuarios	Usuario	Sistema Operativo	Dirección IP
1	Drosero	Windows 7 Professional	192.168.
2	Inieto	Windows 7 Professional	192.168.

3	Jlandeta	Windows 7 Professional	192.168.
4	Kvega	Windows 7 Professional	192.168.
5	Nvalencia	Windows 7 Professional	192.168.
6	Acevallos	Windows 7 Professional	192.168.
7	Xtocain	Windows 7 Professional	192.168.
8	Jsubia	Windows 7 Professional	192.168.

Fuente: Diseño Personal

- **Agente SNMPv3**

Como podemos observar en la tabla anterior todos los usuarios cuentan con un computador con sistema operativo Windows, cabe recalcar que la versión de SNMP que viene por defecto en los equipos de plataforma Windows, no incorpora funciones que permita monitorear la red mediante el protocolo SNMPv3 que es la versión con características de autenticación y encriptación.

Como solución se planteó el uso de Net-SNMP, al ser una plataforma en software libre, que cuenta con un conjunto de aplicaciones utilizados para implementar SNMP v1, SNMP v2c y SNMP v3 utilizando IPv4 y/o IPv6, existe una variedad de ayuda sobre esta herramienta en línea en el sitio web de Net-SNMP donde podremos encontrar las funciones, pasos tanto de instalación como opciones de configuración, es compatible y puede ser usado conjuntamente con la versión SNMP que viene nativamente en la plataforma Windows. (Net-SNMP, 2013)

Una vez instalado los requisitos de instalación del agente snmpv3, proceso que se muestra en el Anexo B, y la configuración que se muestra en el anexo D, se creó los usuarios que van a ser parte del sistema, para la creación de los usuarios se estableció el nombre de usuario con la unión de la primera letra del nombre seguido del primer apellido, y la contraseña con otro formato que por motivos de confiabilidad no se la menciona, el formato de los usuarios en la versión snmpv3 dentro del departamento financiero se los presenta a continuación con un ejemplo.

Tabla 11 Nomenclatura del usuario en snmpv3

Nombre del protocolo	Siglas del departamento	Nombre de usuario	Piso en el que se encuentra
snmp	DF	cespinosa	SP

Fuente: Diseño personal

- **Gestor SNMPv3**

Para la realización del monitoreo de la red con el protocolo snmpv3 nos ayudamos de la herramienta: Cacti, el cual es un software en código abierto que permite monitorizar y visualizar resultados estadísticas de dispositivos conectados a una red que tengan el protocolo SNMP activado y configurado. Es una herramienta que nos permite visualizar gráficos del estado de parámetros de red como: ancho de banda, detección de congestiones o picos de tráficos en su interfaz. La comprensión de estas graficas no es complicado si es que se tiene un conocimiento básico en sistemas computacionales, que es con el cual cuentan todos los integrantes del departamento de informática, el soporte se lo realiza por medio de una comunidad de voluntarios y usuarios del mismo, que se encargan de actualizaciones o ingreso de plugins del mismo, como es el caso del envío de correo electrónico como parte de notificación si es que un parámetro configurado como umbral es superado. (Comunidad Cacti, 2013).

El funcionamiento es el siguiente: la aplicación sondea cada uno de los hosts que tiene dentro de su configuración solicitando los valores de los parámetros definidos y los va almacenando en una base de datos que emplea Planificación Round Robin, así como se indica en la figura 23. Esta planificación comienza al tratar la base de datos como si fuese un círculo, sobrescribiendo los datos almacenados una vez que se llena la capacidad de ésta. Cualquier tipo de datos puede ser almacenado siempre y cuando sean temporales, como es el caso de SNMP. (Andrés Araque, 2013).

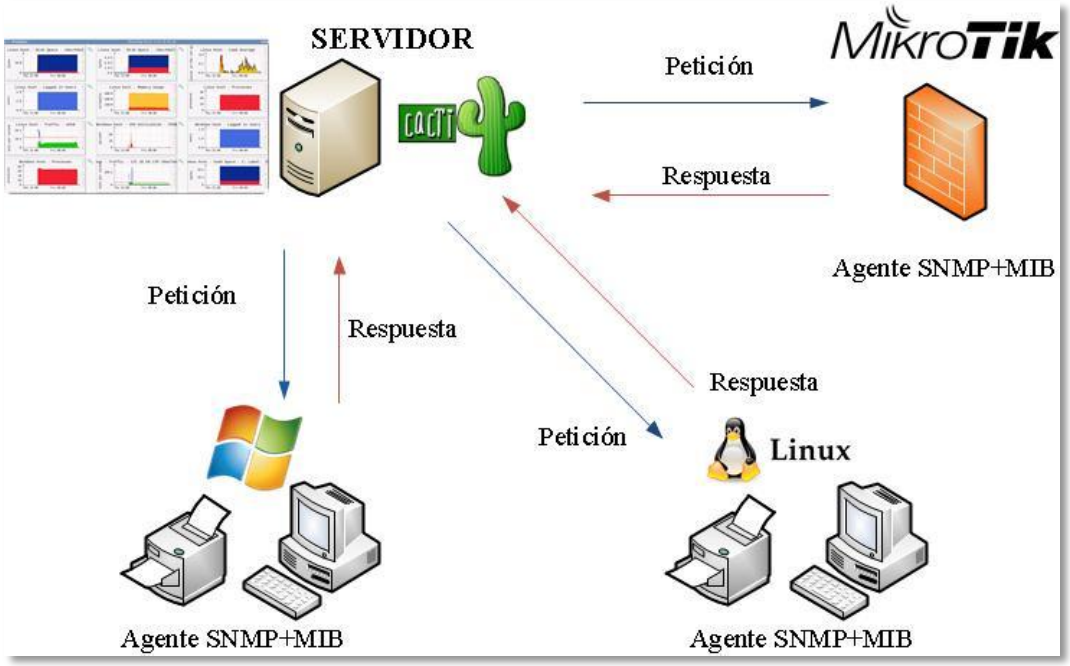


Figura 46 Funcionamiento CACTI
Fuente: Adaptado de: Cacti. (2012). About Cacti.

- **Analizador de paquetes de red**

Para comprobar que los datos del monitoreo están siendo autenticados se utiliza la herramienta WireShark, ya que es una herramienta gratuita y de código abierto que nos permite diagnosticar problemas de red, además de ayudarnos en la captura de paquetes, haciendo fácil la visualización de contraseñas, estas funcionalidades dependerán solo del usuario que maneje esta herramienta, en nuestro caso la usaremos a manera de aprendizaje para ver como fluyen los paquetes cuando se encuentra instalado el agente snmpv3. (Fernando Catoira, 2013).

- **Escenarios de aplicación**

Para indicar las diferencias existentes entre la versión 2 y la versión 3 de snmp se tomó en cuenta dos escenarios realizados en máquinas virtuales para su mejor comprensión, los cuales se muestran a continuación.

- **Primer escenario**

Monitoreo de los host con el protocolo SNMPv2.

- Se mostrará las operaciones: GetRequest, GetBulk y GetResponse desde el agente, para comprobar el funcionamiento de las operaciones en esta versión.

- **Segundo escenario**

Monitoreo de los host con el protocolo SNMPv3.

- En cuanto a seguridad se harán las pruebas respectivas del acceso con contraseña al momento de la monitorización para observar cómo responde el protocolo.

- **Pruebas de funcionamiento en el primer escenario**

- Se mostrará las operaciones: GetRequest, GetBulk y GetResponse desde el agente, para comprobar el funcionamiento de las operaciones en esta versión.

Una vez configurado el agente en snmp en plataformas Windows como se indica en el anexo D, se verificará que los usuarios se encuentren en estado activo como se indica a continuación.

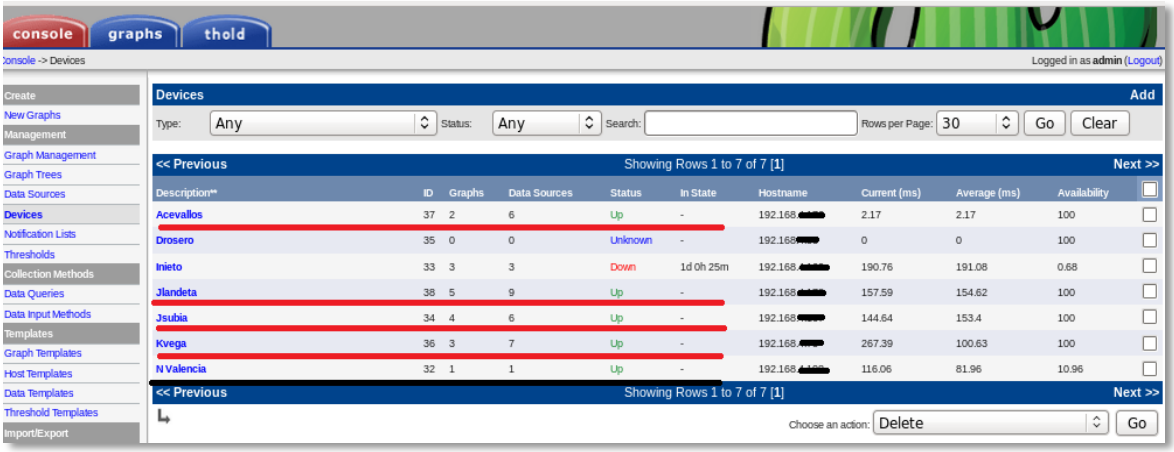


Figura 47 Usuarios del departamento financiero de Emapa-I
Fuente: Obtenida de la plataforma Cacti

En primer lugar se inicializa el comando snmpwalk la estación gestora, para comprobar si está corriendo el servicio snmp correctamente, en este ejemplo queremos obtener una descripción pequeña del equipo a gestionar para lo cual ingresamos el siguiente comando.

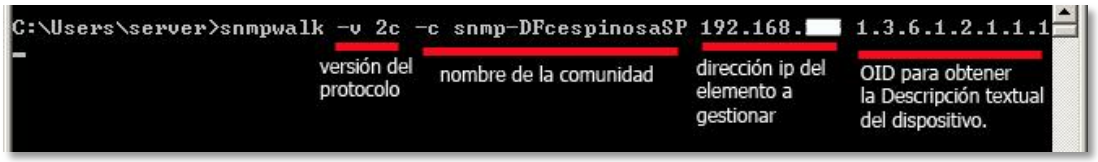


Figura 48 Comando de obtención de datos snmp
Fuente: Datos ingresados en la plataforma gestora

Si todo está funcionando adecuadamente nos mostrará una respuesta similar a la siguiente, donde nos indica que es un equipo de 64 bits con sistema operativo Windows.

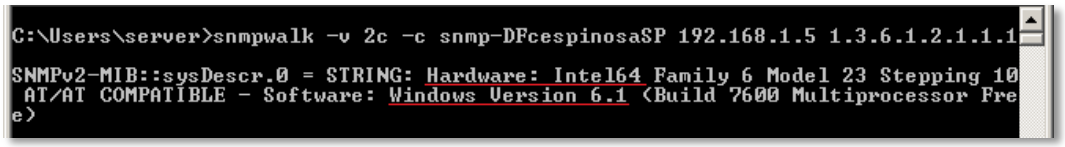


Figura 49 Obtención de datos snmp
Fuente: Datos obtenidos por snmp

Una vez realizado este proceso revisamos los paquetes de las consultas realizadas en WireShark, al haber hecho la petición al agente se observa paquetes de la operación "GetNextRequest" por parte de la estación gestora además nos permite visualizar la versión y el nombre de la comunidad.

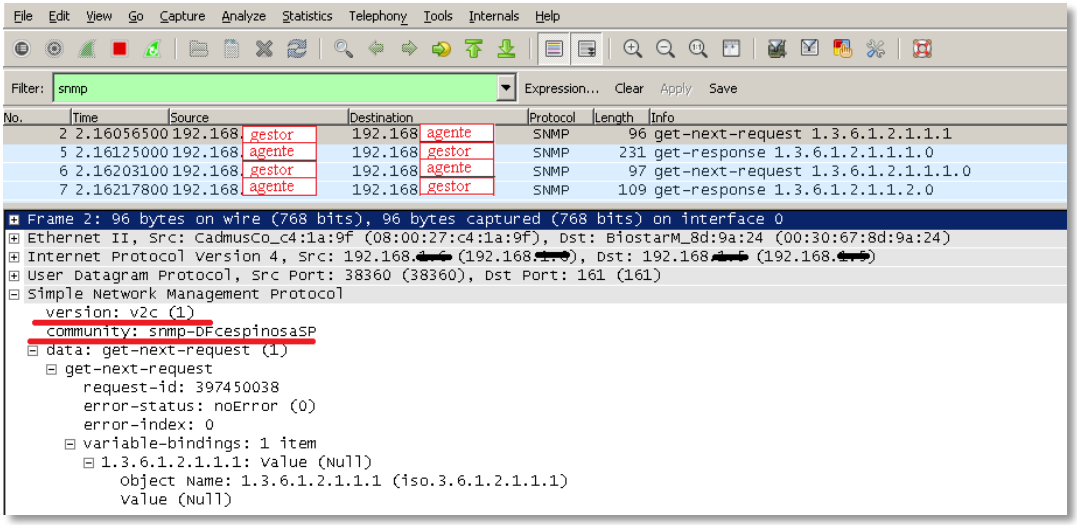


Figura 50 Operación get-next-request
Fuente: Datos obtenidos por la aplicación WireShark

De igual forma se puede visualizar la operación “GetResponse” que es la respuesta del elemento gestionado, además nos permite visualizar la versión y el nombre de la comunidad.

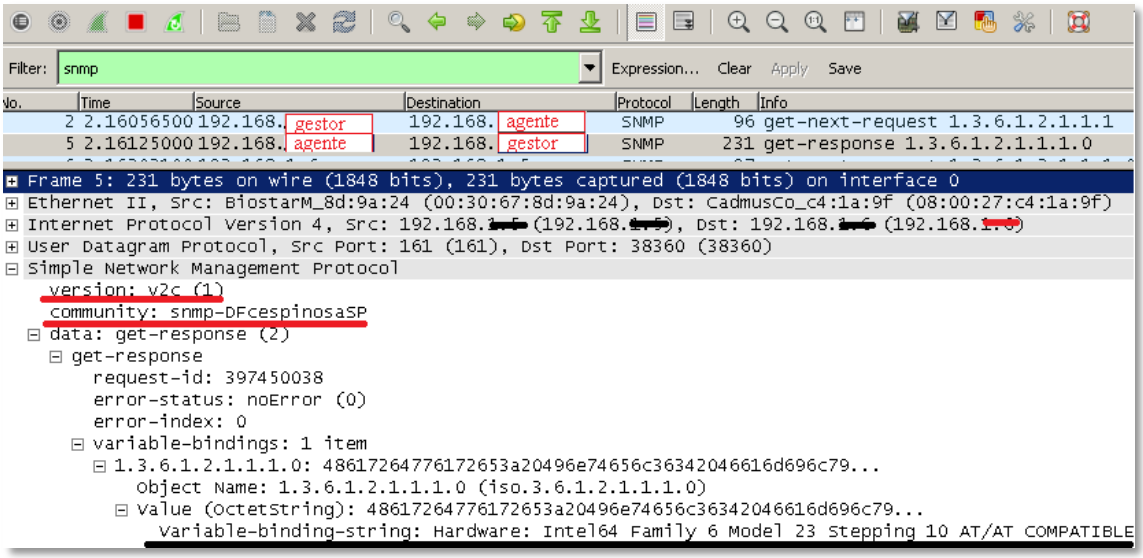


Figura 51 Operación get-response
Fuente: Datos obtenidos por la aplicación WireShark

Para obtener paquetes de la operación GetBulk, del anterior comando solo se sustituirá el comando “snmpwalk” por el comando “snmpbulkwalk”.

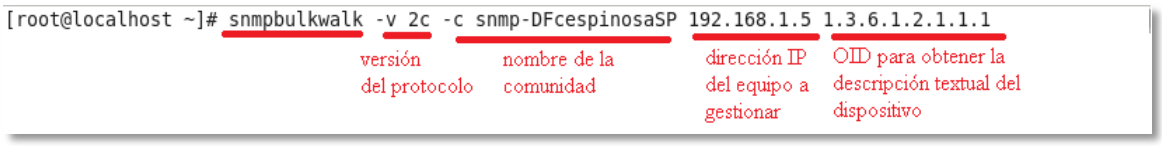


Figura 52 Comando de obtención de datos snmpbulk
Fuente: Datos ingresados en la plataforma gestora

Si todo está funcionando adecuadamente nos mostrará una respuesta similar a la siguiente, donde nos indica que es un equipo de 64 bits con sistema operativo Windows.

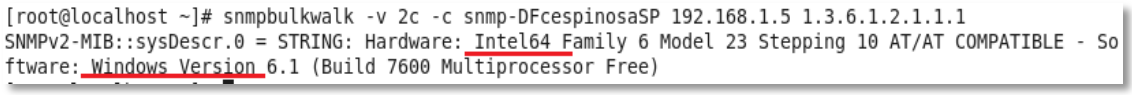


Figura 53 Obtención de datos snmpbulk
Fuente: Datos obtenidos por snmp

Una vez realizado este proceso revisamos los paquetes de las consultas realizadas en WireShark, al haber hecho la petición al agente se observa paquetes de la operación "GetBulkRequest" por parte de la estación gestora además nos permite visualizar la versión y el nombre de la comunidad.

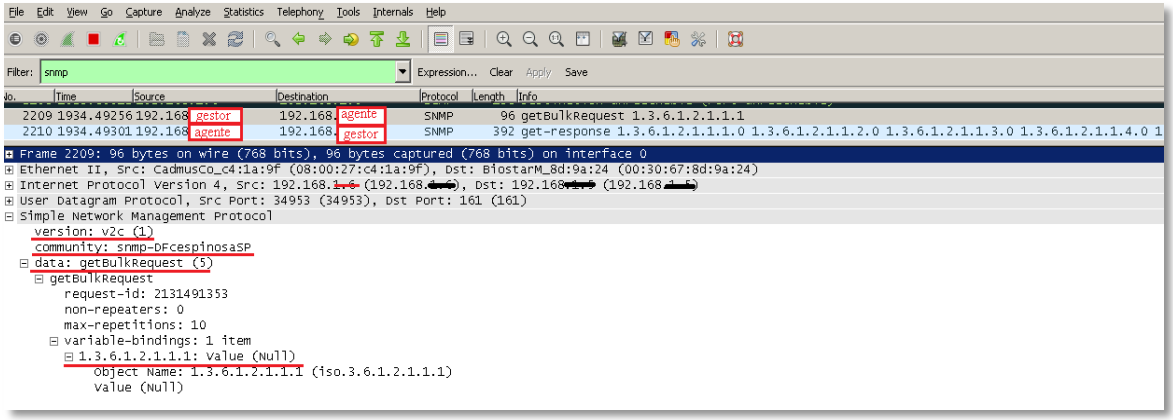


Figura 54 Operación get-bulk-request
Fuente: Datos obtenidos por la aplicación Wireshark

De igual forma se puede visualizar la operación "GetResponse" que es la respuesta del elemento gestionado, además nos permite visualizar la versión y el nombre de la comunidad. Como podemos observar al usar el comando snmpbulkwalk recibimos datos de forma masiva.

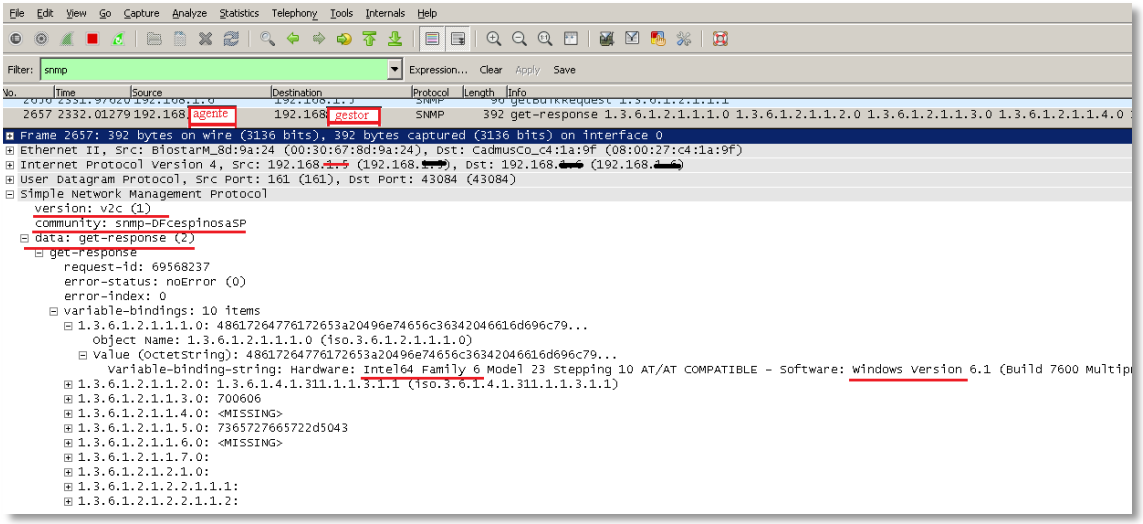


Figura 55 Operación get-response
Fuente: Datos obtenidos por la aplicación WireShark

- **Pruebas de funcionamiento en el segundo escenario**

  - En cuanto a seguridad se harán las pruebas respectivas del acceso con contraseña al momento de la monitorización para observar cómo responde el protocolo.

Una vez configurado el agente en snmp en plataformas Windows como se indica en el anexo D, se inicializa el comando snmpwalk la estación gestora, para comprobar si está corriendo el servicio snmp correctamente, en este ejemplo queremos obtener una descripción pequeña del equipo a gestionar para lo cual ingresamos el siguiente comando.

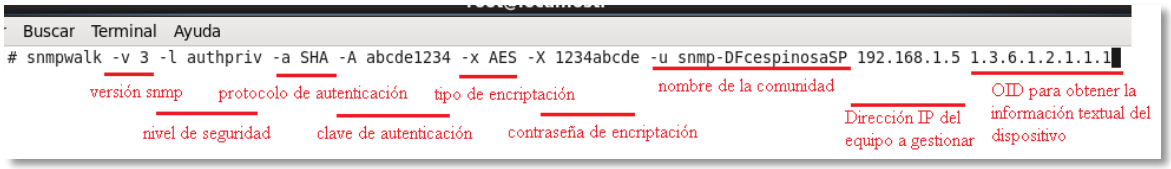


Figura 56 Comando de obtención de datos snmpv3
Fuente: Datos ingresados en la plataforma gestora

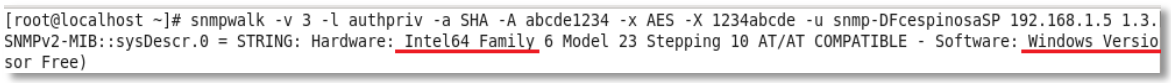


Figura 57 Obtención de datos snmp
Fuente: Datos obtenidos por snmp

Una vez realizado este proceso revisamos los paquetes de las consultas realizadas en WireShark, al haber hecho la petición al agente se observa paquetes de la operación “GetRequest” por parte de la estación gestora además nos permite visualizar la versión de la comunidad.

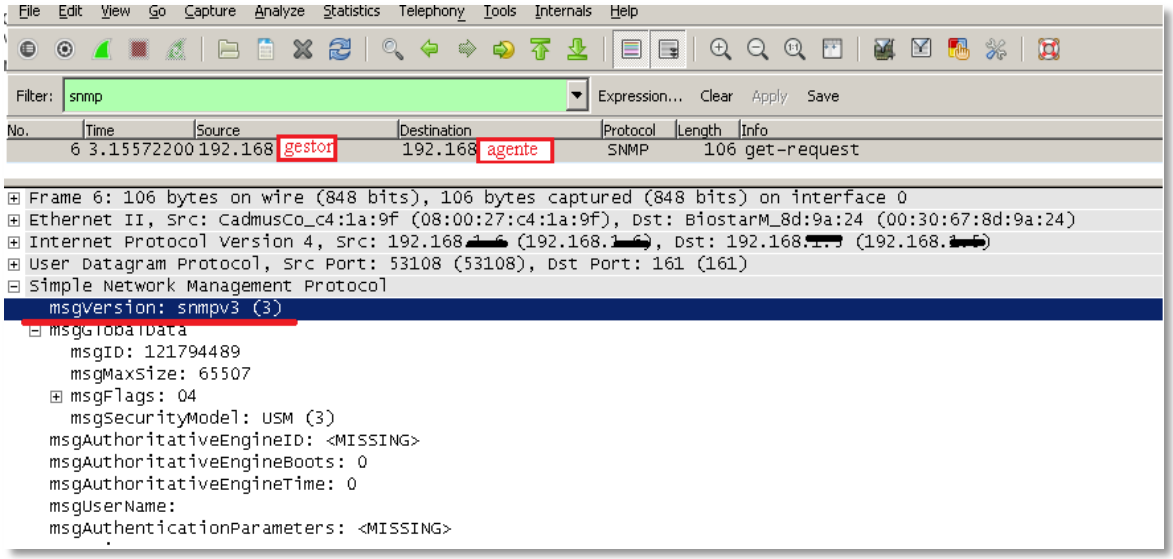


Figura 58 Operación get-request
Fuente: Datos obtenidos por la aplicación WireShark

Una vez que reporta la solicitud al agente, se puede notar cómo el nombre del paquete cambia para mostrarnos “encryptedPDU”, además de mostrarnos las opciones de encriptación y autenticación activadas, de esta forma se puede apreciar que la información que se transmite entre el agente y el gestor, se encuentran cifradas como lo sería también para cualquier otra persona que intente observar el tráfico de la red y no forme parte este monitoreo.

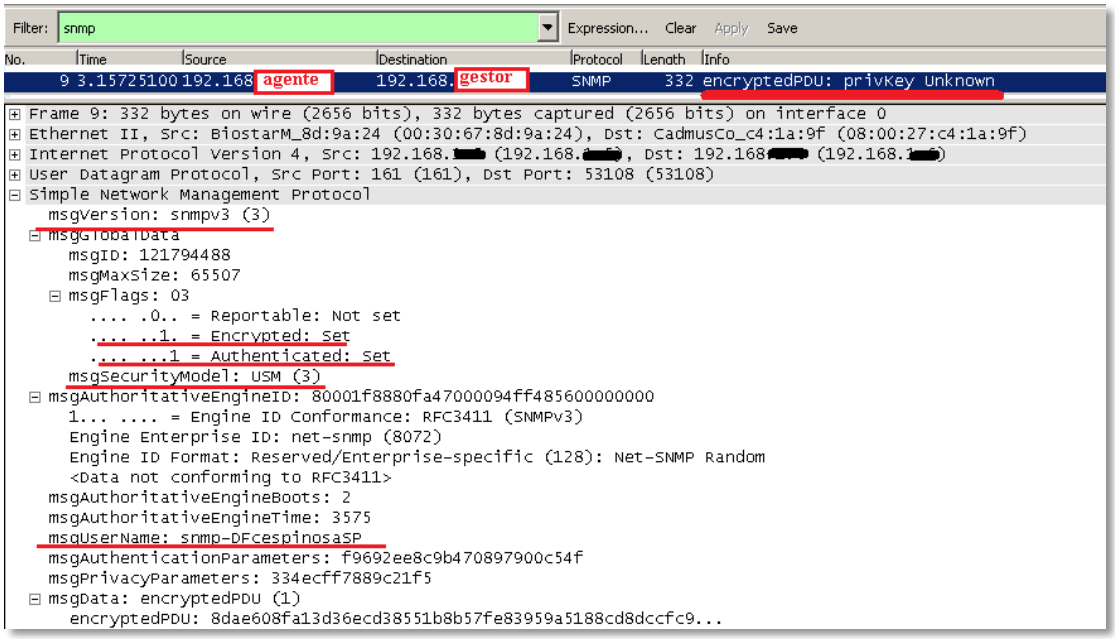


Figura 59 Flujo de datos snmp encriptados
Fuente: Datos obtenidos por la aplicación WireShark

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

El monitoreo de los recursos de los computadores de usuario final en el departamento financiero, se lo realizó con la plataforma Cacti, sus pasos de instalación se muestran en el anexo B y su manual de usuario se encuentra en el anexo C, una vez que agregamos al usuario que vamos a gestionar podemos observar que datos recolecta para crear las gráficas tanto de la utilización del CPU, el tráfico de red en su interfaz, y el uso de la memoria RAM, cada uno previamente autenticado con su respectiva contraseña.

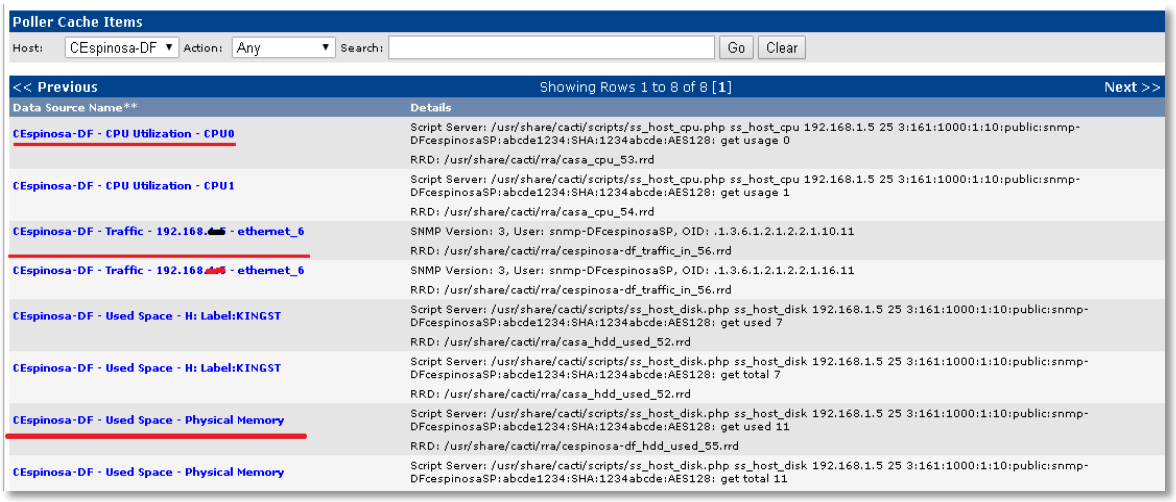


Figura 60 Datos para el monitoreo de recursos delos computadores en snmpv3
Fuente: Datos obtenidos por la aplicación Cacti

Una vez especificado que graficas deseamos visualizar esperamos que el software empiece a graficar los datos obtenidos, como resultados podemos observar cuanto consume el usuario de ancho de banda de internet, la memoria RAM, y la utilización del CPU.

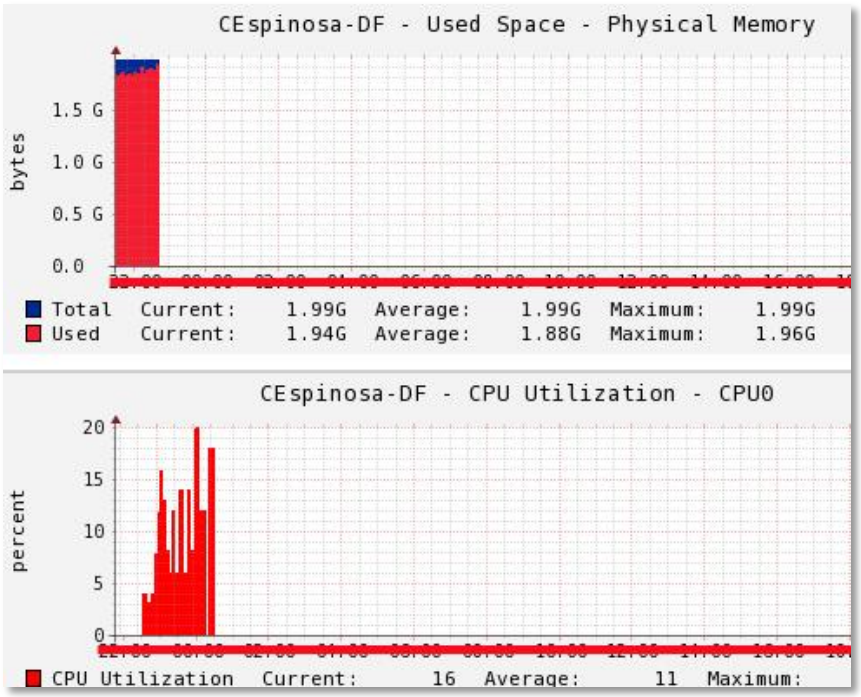


Figura 61 Monitoreo de recursos de los computadores en snmpv3
Fuente: Datos obtenidos por la aplicación Cacti

El manual de usuario de la plataforma Cacti se encuentra en el anexo C.

3.2.4.4. Restricción de páginas web

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

En primer lugar se estableció la lista de direcciones IP que si contaran con el ingreso a páginas como: YouTube y Facebook, ya que existen departamentos que trabajan mediante estas plataformas, los cuales se presenta en la siguiente tabla.

Tabla 12 Lista de direcciones IP permitidas a las plataformas: Youtube, Facebook

Lista de direcciones IP que tienen ingreso a las plataformas: Youtube, Facebook	
Departamento	**Dirección IP**
Tecnologías de información	192.168.4.4 192.168.4.10
Imagen Corporativa	192.168.4.17
Compras Públicas	192.168.4.45
Nuevos Productos	192.168.4.51
Dirección de comercialización	192.168.4.65 192.168.4.66

Fuente: Diseño Propio

Considerando que la institución cuenta con un equipo RouterBoard Mikrotik, se realizó las respectivas configuraciones en este dispositivo, ya que cuenta con funcionalidades específicas para este tipo de configuraciones.

A continuación se muestra la lista de direcciones a la que vamos a permitir el acceso a páginas como Facebook y Youtube, cabe destacar que a pesar de que esta lista es pequeña, las características y las configuraciones realizadas en el equipo pueden ser utilizadas para aplicarlas a una lista más robusta, que estén enfocadas a mejorar el rendimiento de los recursos informáticos de la institución.

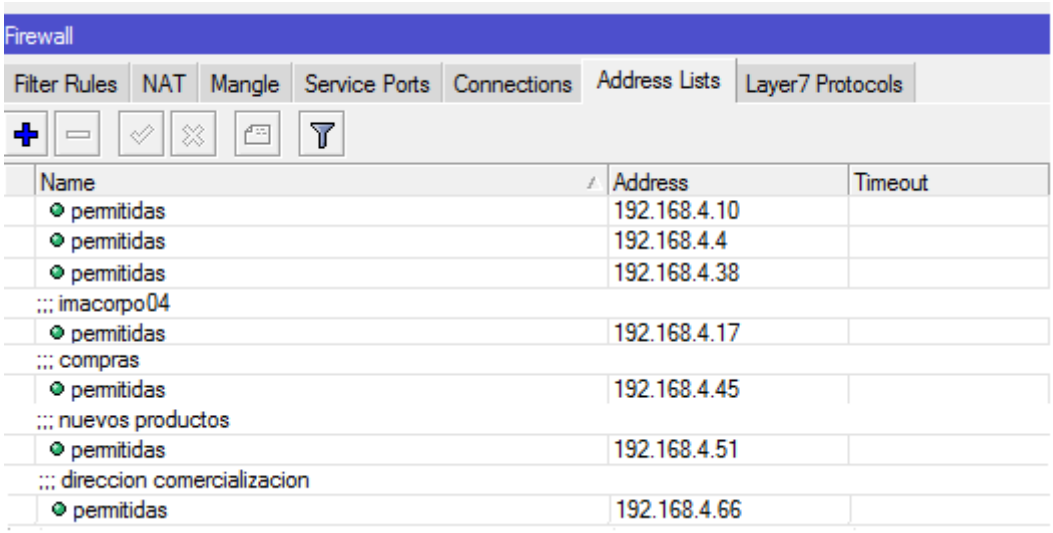


Figura 62 Lista de direcciones IP con acceso total a páginas web
Fuente: Equipo RouterBoard Mikrotik

Seguidamente procedemos a configurar las páginas que vamos a denegar, las cuales se enlistan a continuación:

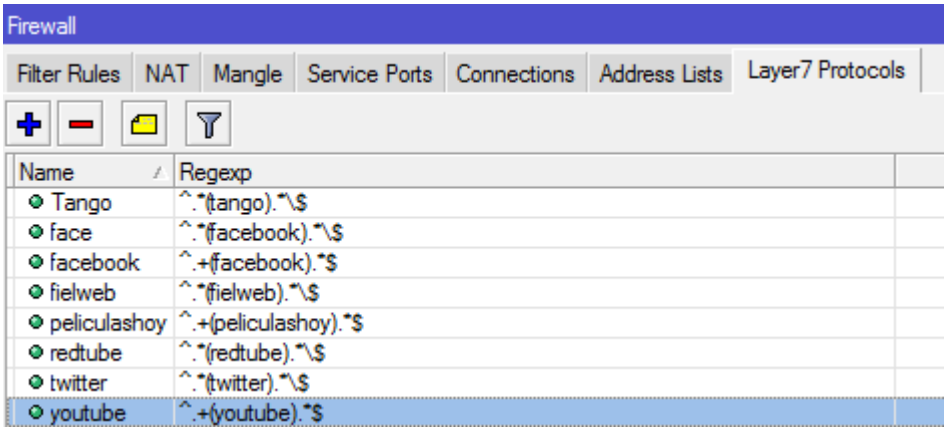


Figura 63 Lista de páginas web que se denegarán
Fuente: Equipo RouterBoard Mikrotik

Una vez que tenemos tanto la lista de direcciones IP como la lista de páginas web que deseamos aceptar o denegar, las asociamos de la siguiente manera.

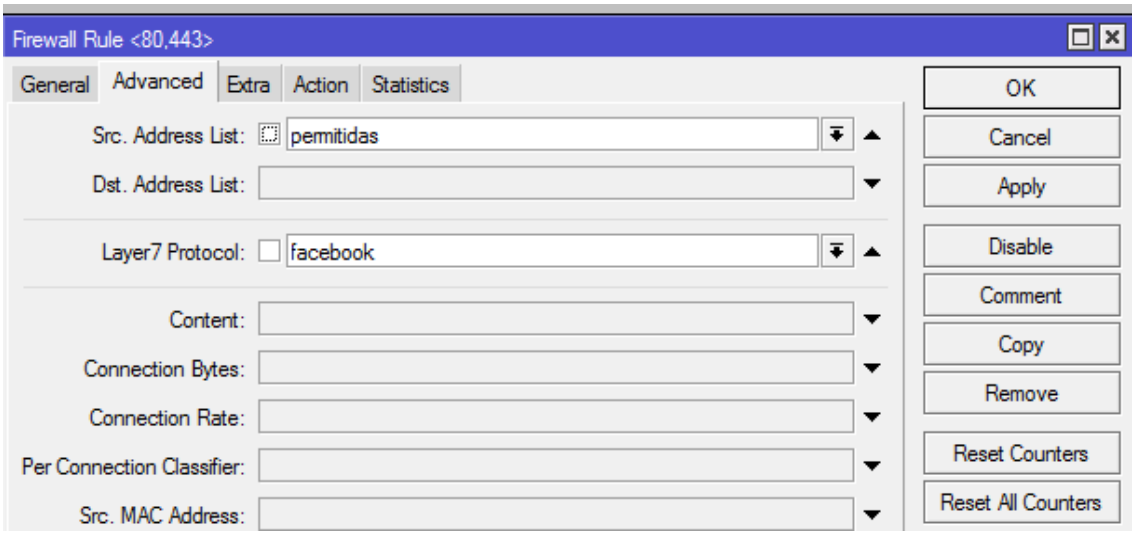


Figura 64 Asociación de lista de IP con páginas web
Fuente: Equipo RouterBoard Mikrotik

Por último se procede a escoger una acción la cual puede ser denegar o aceptar las páginas web a la lista de direcciones IP seleccionada.

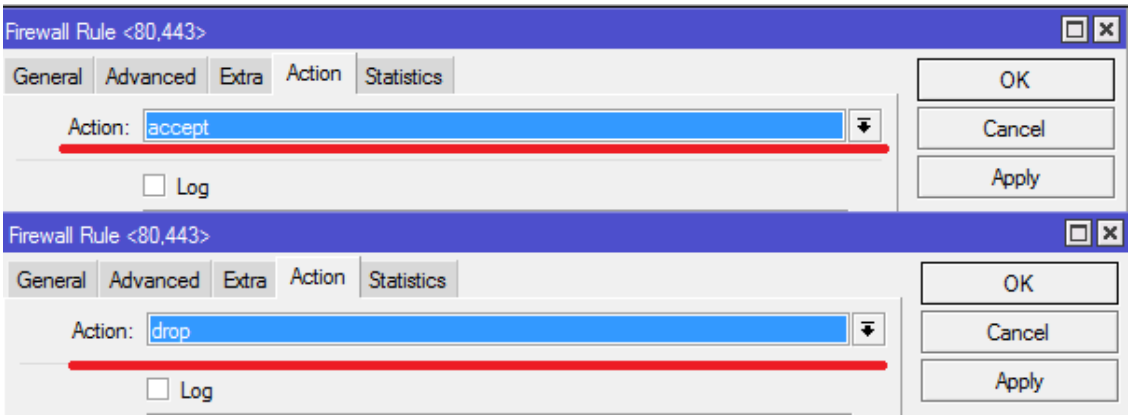


Figura 65 Configuración de reglas firewall
Fuente: Equipo RouterBoard Mikrotik

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

CAPITULO 4: DOCUMENTACIÓN

En este capítulo se documentará detalladamente cada proceso realizado tanto en la detección como en la solución de fallas en un manual de procedimientos con el fin de que el administrador intervenga rápidamente en caso de presentarse algún inconveniente para así minimizar la interrupción del servicio de los usuarios.

4.1. MANUAL DE PROCEDIMIENTOS

4.1.1. Introducción

El departamento de recursos informáticos tiene por objeto contribuir en el mantenimiento y mejoramiento de la infraestructura tecnológica, que son el apoyo fundamental para el buen manejo, funcionamiento, estructura y organización de la institución.

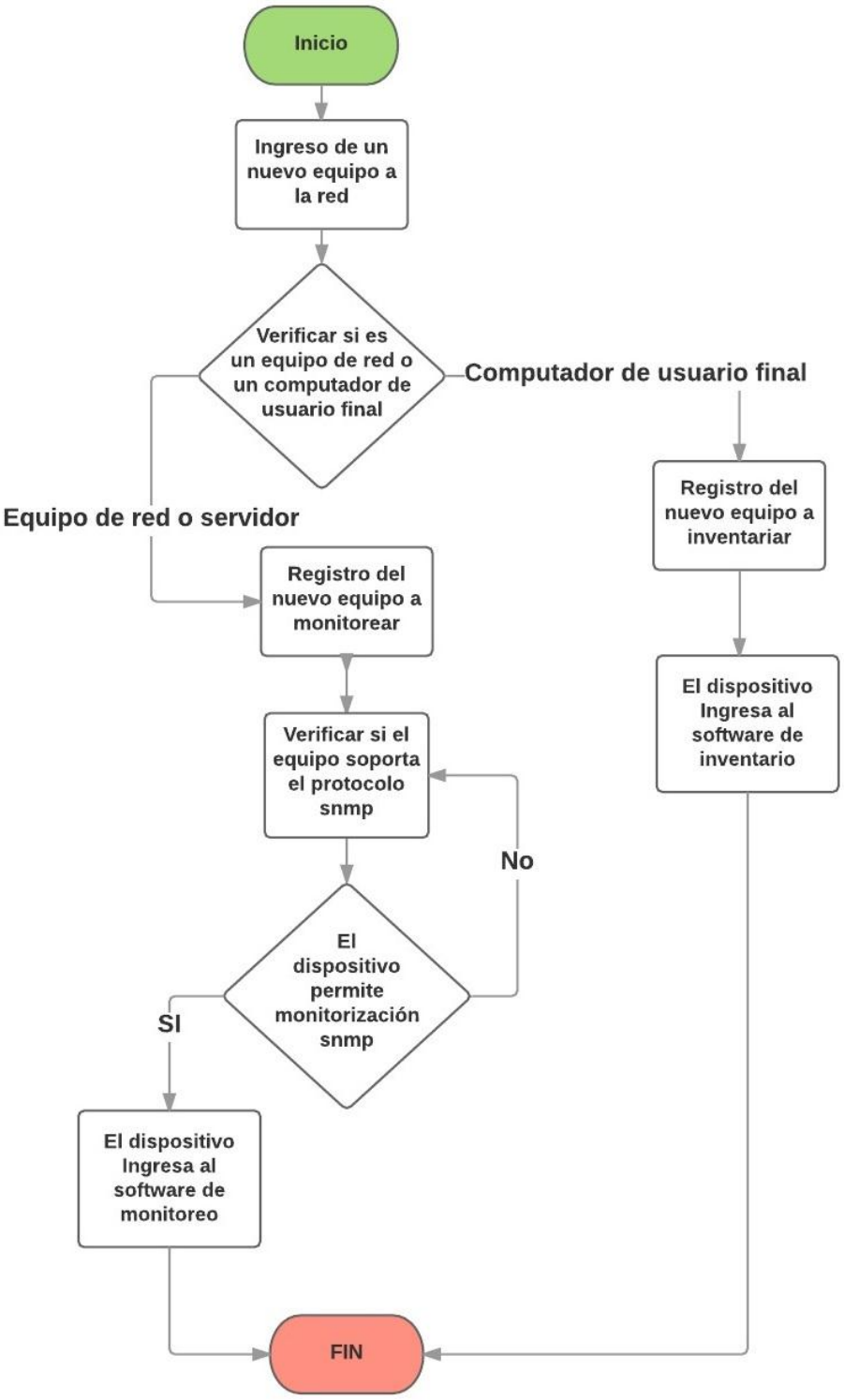
Por este motivo el manual de procedimientos que se presenta a continuación incluye procesos que permitan a este departamento analizar, identificar y corregir los incidentes que se presenten en la red de datos en base al modelo funcional SNMP, el cual tiene como prioridad minimizar los riesgos que se presenten ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

En la actualidad existe una gran variedad de métodos en los cuales basarnos para presentar un manual de procedimientos, pero debido a la importancia que presentan tanto las entidades públicas como privadas se debe cumplir con estándares que garanticen la uniformidad tanto en el contenido, como su forma de presentación, es por este motivo que el presente manual está basado en la norma ISO 9001:2008.

4.1.2. Manual de procedimientos para la función Operación

<table>
<tr><td colspan="4">EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">PROCEDIMIENTO</td><td>Código</td><td>PR-HW-01</td></tr>
<tr><td>Versión:</td><td>1.0</td></tr>
<tr><td colspan="4">Área responsable: Unidad de hardware redes y telecomunicaciones</td></tr>
<tr><td colspan="4">Objetivo Proporcionar la información que permita supervisar la configuración de los equipos de red y de los servidores que van a ser monitoreados</td></tr>
<tr><td colspan="4">Alcance Se indicará los procesos que permitan la configuración de los equipos y servidores de red para agregarlos al sistema de gestión, además se presentará los procesos que permitan agregar los computadores de usuario final al sistema de inventario.</td></tr>
<tr><td colspan="4">Definiciones
<table>
<tr><th>No.</th><th>Termino</th><th>Definición</th></tr>
<tr><td>1</td><td>Software de inventario de red</td><td>Conjunto de herramientas que permiten tanto la supervisión de componentes en la red como su visualización en una interfaz web.</td></tr>
<tr><td>2</td><td>Software de gestión</td><td>Conjunto de herramientas que permiten tanto monitorear los equipos y servidores en la red como brindar su visualización en una interfaz web.</td></tr>
<tr><td>3</td><td>IP</td><td>Las direcciones IP son un número único e irrepetible con el cual se identifica una computadora conectada a la red</td></tr>
<tr><td>4</td><td>SNMP</td><td>El Protocolo simple de administración de redes es un estándar de administración de redes utilizado en redes TCP/IP.</td></tr>
<tr><td>5</td><td>Comunidad SNMP</td><td>Se utiliza como un sencillo mecanismo de control de acceso a la información</td></tr>
<tr><td>6</td><td>Diagrama de Flujo</td><td>Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso</td></tr>
<tr><td>7</td><td>Nomenclatura para dispositivos de red</td><td>Formato y sintaxis que se utilizan para nombrar los elementos de la red que permitan su fácil ubicación</td></tr>
<tr><td>8</td><td>Anexo</td><td>Documento utilizado para agregar más información al documento original.</td></tr>
</table></td></tr>
</table>

Diagrama de flujo



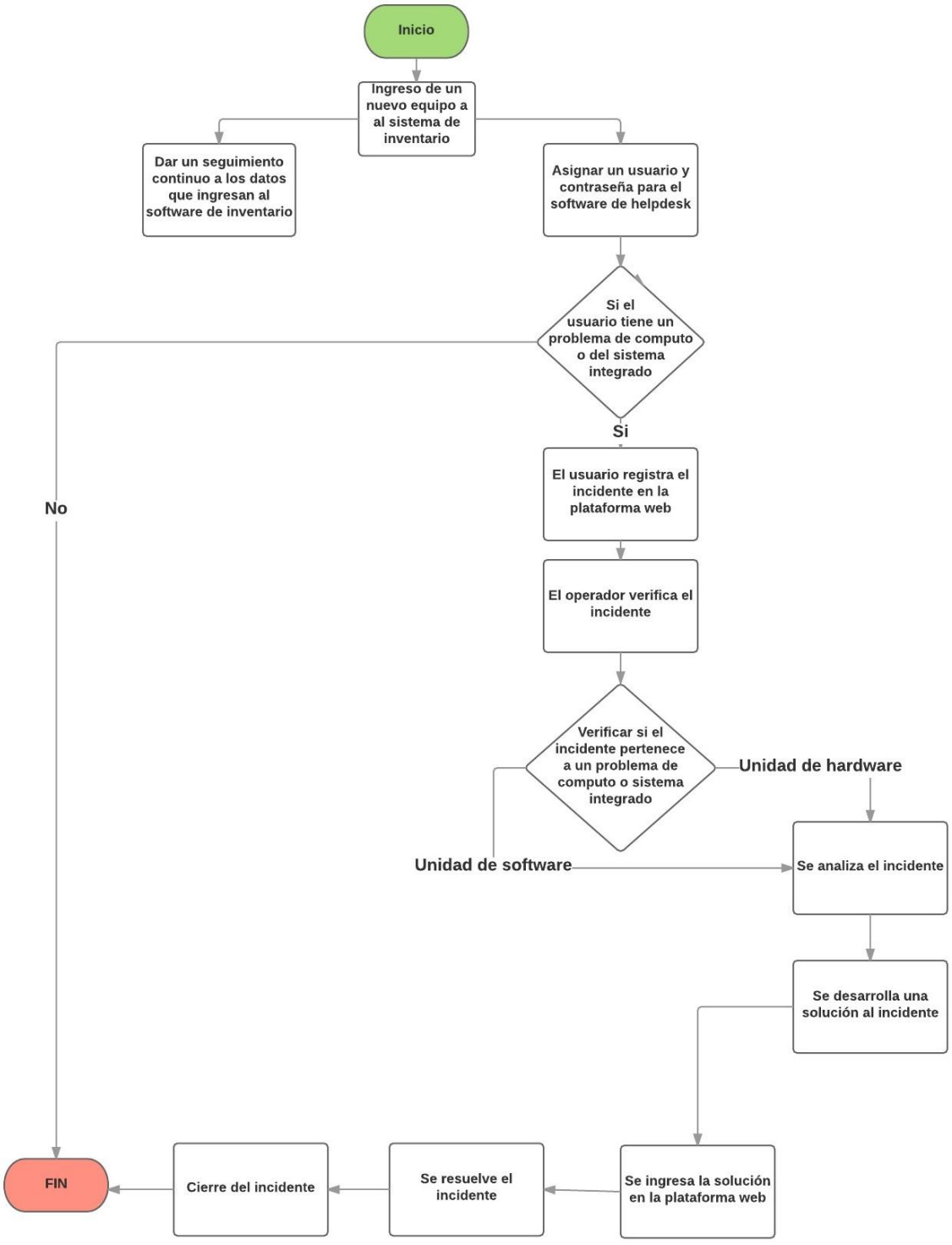
Descripción de actividades

Paso	Responsable	Actividad	Descripción
1	Unidad de hardware redes y telecomunicaciones	Ingreso de un nuevo equipo a la red	El equipo que ingrese debe ser notificado al departamento de recursos informáticos
2	Unidad de hardware redes y telecomunicaciones	Verificar si es un equipo de red o un computador de usuario final	Identificar si es un equipo de red como un conmutador, o un computador que va a ser usado por el personal de la empresa
3	Unidad de hardware redes y telecomunicaciones	Registro del nuevo equipo a monitorear	El ingreso de un nuevo equipo a la red debe ser registrado.
4	Unidad de hardware redes y telecomunicaciones	Verificar si el equipo soporta monitorización snmp	Se debe verificar con la hoja de datos del equipo si tiene soporte al protocolo snmp
5	Unidad de hardware redes y telecomunicaciones	El dispositivo permite monitorización snmp	Si el dispositivo soporta la versión snmp se continua con el siguiente paso de lo contrario solo se lo registra.
6	Unidad de hardware redes y telecomunicaciones	El dispositivo ingresa al software de monitoreo	Si el dispositivo soporta la versión snmp se procede a agregar al software de monitorización con su respectiva nomenclatura.
7	Unidad de hardware redes y telecomunicaciones	Registro del nuevo equipo a inventariar	Si el equipo que ingresa es un computador para uso del personal se lo registra
8	Unidad de hardware redes y telecomunicaciones	El equipo ingresa al software de inventario	Una vez registrado se procede a agregarlo al software de inventario con su respectiva nomenclatura.

4.1.3. Manual de procedimientos para la función Administración

<table>
<tr><td colspan="4">EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA</td></tr>
<tr><td rowspan="2"></td><td>PROCEDIMIENTO</td><td>Código</td><td>PR-HW-02</td></tr>
<tr><td>MANUAL DE GESTIÓN DE ADMINISTRACIÓN</td><td>Versión:</td><td>1.0</td></tr>
<tr><td colspan="4">Área responsable: Unidad de hardware redes y telecomunicaciones/ Unidad de software y desarrollo</td></tr>
<tr><td colspan="4">Objetivo Dar información acerca del seguimiento al inventario inicial y el reporte de incidencias de parte del usuario final mediante helpdesk</td></tr>
<tr><td colspan="4">Alcance Esta función se relaciona conjuntamente tanto con la gestión de operación como la gestión de mantenimiento, por lo tanto aquí se determina el seguimiento de los componentes de los dispositivos ya inventariados, y también se explicará la forma en que se procederá a recibir las incidencias que reporten los usuarios finales.</td></tr>
<tr><td colspan="4">Definiciones
<table>
<tr><th>No.</th><th>Termino</th><th>Definición</th></tr>
<tr><td>1</td><td>Software de inventario de red</td><td>Conjunto de herramientas que permiten tanto la supervisión de componentes en la red como su visualización en una interfaz web.</td></tr>
<tr><td>2</td><td>Diagrama de Flujo</td><td>Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso</td></tr>
<tr><td>3</td><td>Reporte</td><td>Documento que pretende transmitir una información acerca de las incidencias que suceden en la red</td></tr>
</table></td></tr>
</table>

Diagrama de flujo



Descripción de actividades

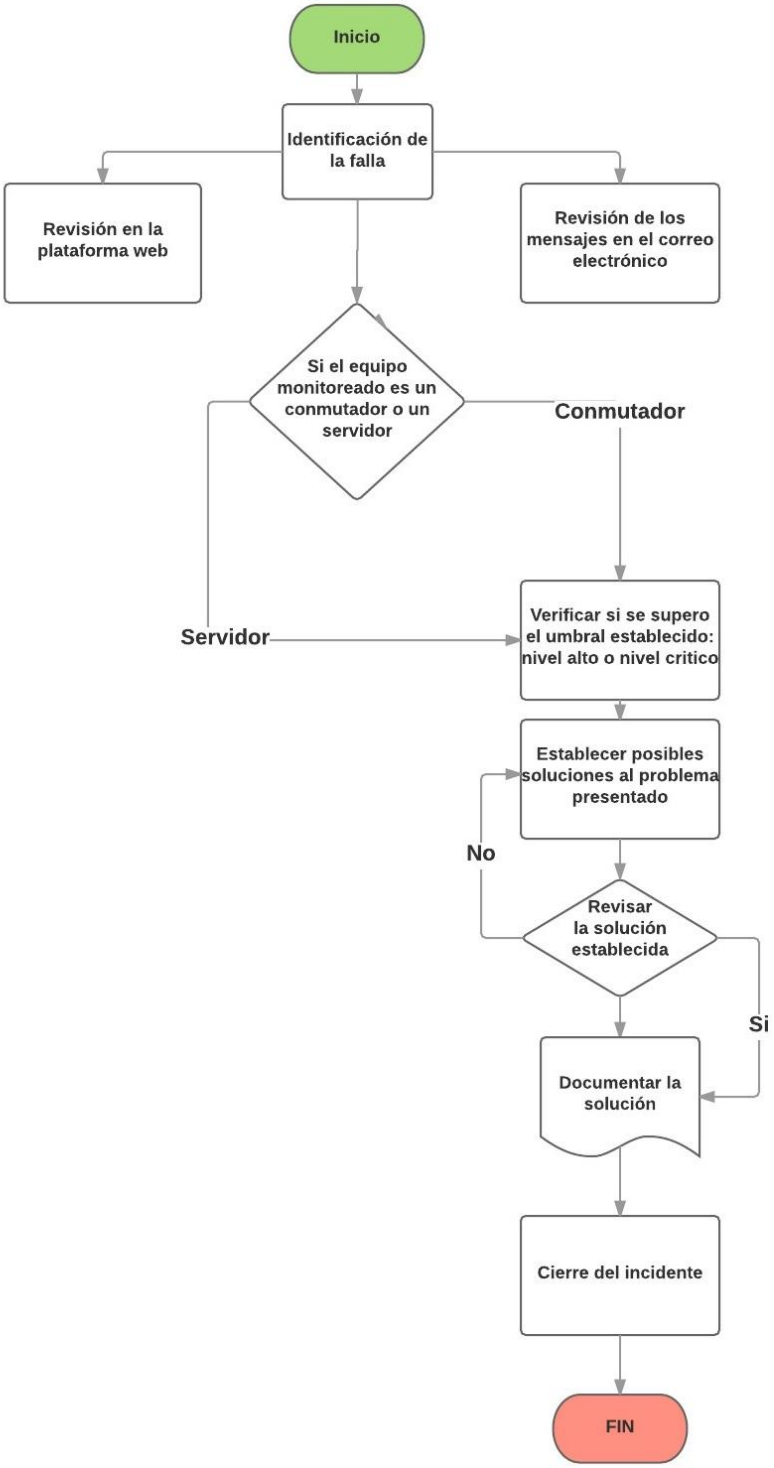
Paso	Responsable	Actividad	Descripción
1	Unidad de hardware redes y telecomunicaciones	Ingreso de un nuevo equipo a al sistema de inventario	El ingreso de un nuevo equipo a la red debe ser registrado.
2	Unidad de hardware redes y telecomunicaciones	Dar un seguimiento continuo a los datos que ingresan al software de inventario	Verificar los datos que ingresan al software de inventario continuamente para evaluación de información
3	Unidad de hardware redes y telecomunicaciones	Asignar un usuario y contraseña para el software de helpdesk	Si el usuario es nuevo se le asignará un nombre de usuario y una contraseña para que pueda ingresar a la plataforma de incidencias
4	Unidad de hardware redes y telecomunicaciones	Si el usuario tiene un problema de computo o del sistema integrado	El usuario identificará si tiene un problema con algún componente de su computador o alguna dificultad al ingresar al sistema integrado
5	Unidad de hardware redes y telecomunicaciones	El usuario registra el incidente en la plataforma web	Si el usuario tuviere algún problema con respecto al sistema integrado o problema de computo lo registrará en la plataforma web
6	Unidad de hardware redes y telecomunicaciones	El operador verifica el incidente	El operador identificará la petición del usuario
7	Unidad de hardware redes y telecomunicaciones	Verificar si el incidente pertenece a un problema de computo o sistema integrado	Se verificará si el problema que ingresa es por motivo de problema de computo o problema de ingreso al sistema

8	Unidad de hardware redes y telecomunicaciones/ Unidad de software y desarrollo	Se analiza el incidente	La unidad encargada de resolver el problema analizará las posibles soluciones a la incidencia revisada
9	Unidad de hardware redes y telecomunicaciones/ Unidad de software y desarrollo	Se desarrolla una solución al incidente	Se realizará las pruebas que permitan la solución a este problema
10	Unidad de hardware redes y telecomunicaciones/ Unidad de software y desarrollo	Se ingresa la solución en la plataforma web	La solución provista se documentará en la plataforma web para llevar un inventario de soluciones
11	Unidad de hardware redes y telecomunicaciones/ Unidad de software y desarrollo	Se resuelve el incidente	Se le resuelve el problema al usuario que hizo la petición
12	Unidad de hardware redes y telecomunicaciones/ Unidad de software y desarrollo	Cierre del incidente	Se da por cerrado el incidente solucionado

4.1.4. Manual de procedimientos para la función Mantenimiento

<table>
<tr><td colspan="4">EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA</td></tr>
<tr><td rowspan="2"></td><td>PROCEDIMIENTO</td><td>Código</td><td>PR-HW-03</td></tr>
<tr><td>MANUAL DE GESTIÓN DE MANTENIMIENTO</td><td>Versión:</td><td>1.0</td></tr>
<tr><td colspan="4">Área responsable: Unidad de hardware redes y telecomunicaciones</td></tr>
<tr><td colspan="4">Objetivo Establecer procesos que permitan la revisión de los umbrales que generan notificaciones específicas, las cuales son una base para analizar, e identificar las fallas que sucedan en los equipos monitoreados.</td></tr>
<tr><td colspan="4">Alcance Se establecen los umbrales que los equipos a gestionar deben mantener, y si son sobrepasados los técnicos encargados busquen una solución oportunamente permitiendo ofrecer un nivel de continuidad alto en la red.</td></tr>
<tr><td colspan="4">Definiciones
<table>
<tr><th>No.</th><th>Termino</th><th>Definición</th></tr>
<tr><td>1</td><td>Software de gestión</td><td>Conjunto de herramientas que permiten tanto monitorear los equipos y servidores en la red como brindar su visualización en una interfaz web.</td></tr>
<tr><td>2</td><td>Reporte</td><td>Documento que pretende transmitir una información acerca de las incidencias que suceden en la red</td></tr>
<tr><td>3</td><td>SNMP</td><td>El Protocolo simple de administración de redes es un estándar de administración de redes utilizado en redes TCP/IP.</td></tr>
<tr><td>4</td><td>Definición de umbrales</td><td>Porcentaje referencial de funcionamiento normal de un dispositivo de red.</td></tr>
<tr><td>5</td><td>Diagrama de Flujo</td><td>Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso</td></tr>
</table></td></tr>
</table>

Diagrama de flujo



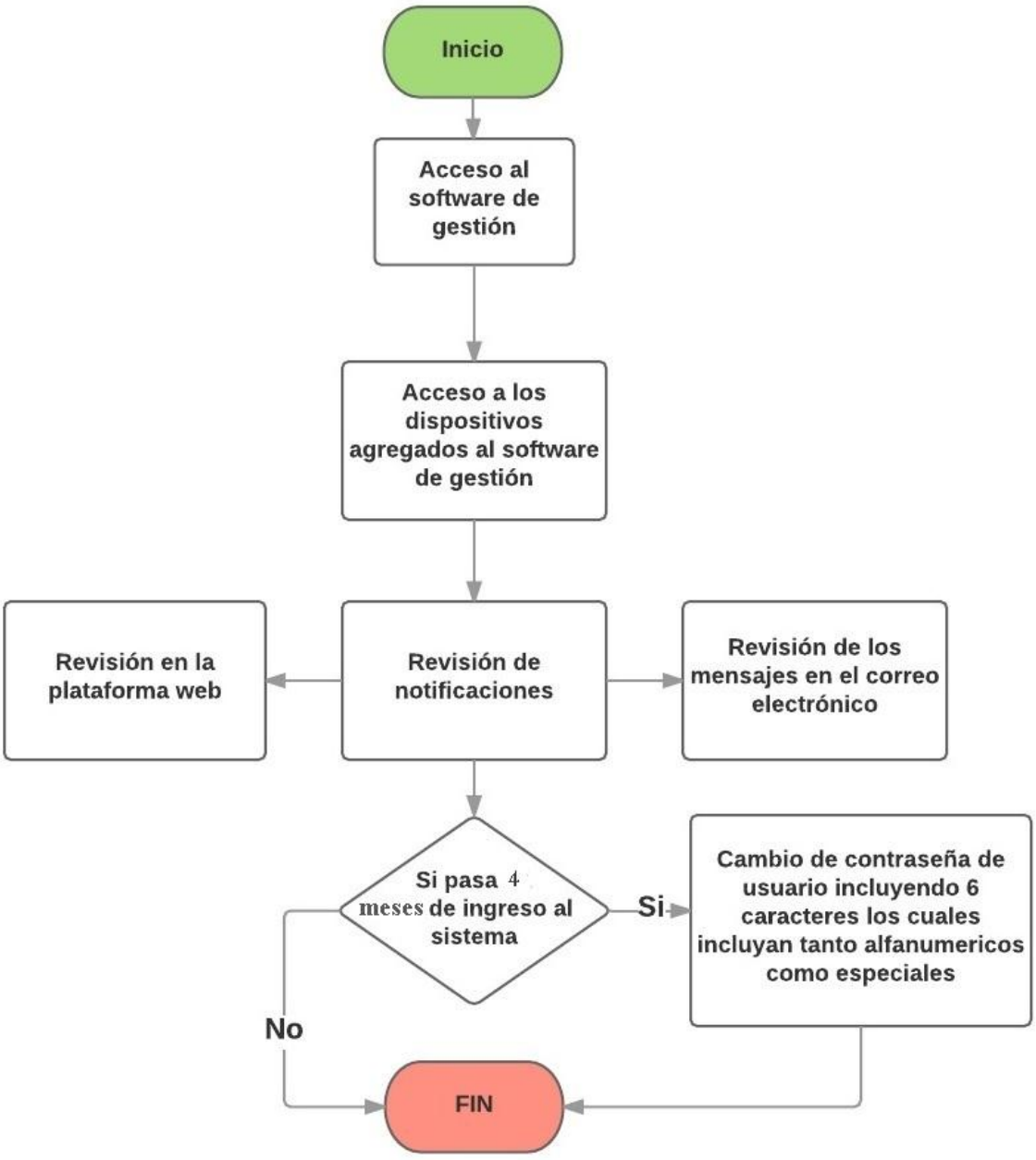
Descripción de actividades

Paso	Responsable	Actividad	Descripción
1	Unidad de hardware redes y telecomunicaciones	Identificación de la falla	Si un nivel de umbral se ha superado se notificará al operador por medio del correo electrónico o por la plataforma web
2	Unidad de hardware redes y telecomunicaciones	Si el equipo es un conmutador o un servidor	Se verificará si el equipo que notifico la alerta es un servidor o un conmutador y que nivel de umbral supero, ya que existen dos niveles: **Alto,** que es un nivel aceptable pero nos indicará cual recurso es el que puede desgastarse hasta llegar a un nivel crítico. **Crítico**, que es un nivel en el cual se debe actuar con más prontitud.
3	Unidad de hardware redes y telecomunicaciones	Establecer posibles soluciones al problema presentado	La unidad encargada de resolver el problema analizará las posibles soluciones a la incidencia revisada
4	Unidad de hardware redes y telecomunicaciones	Revisar la solución establecida	Se realizará las pruebas que permitan la solución a este problema
5	Unidad de hardware redes y telecomunicaciones	Documentar la solución	La solución provista se documentará en la plataforma web GLPI para llevar un inventario de soluciones
6	Unidad de hardware redes y telecomunicaciones	Cierre del incidente	Se da por cerrado el incidente solucionado

4.1.5. Manual de procedimientos para la función Seguridad

<table>
<tr><td colspan="4">EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE IBARRA</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">PROCEDIMIENTO</td><td>Código</td><td>PR-HW-04</td></tr>
<tr><td>Versión:</td><td>1.0</td></tr>
<tr><td colspan="4">Área responsable: Unidad de hardware redes y telecomunicaciones</td></tr>
<tr><td colspan="4">Objetivo Ofrecer seguridad al sistema de gestión mediante la autenticación e ingresos intransferibles a los usuarios del departamento de recursos informáticos para garantizar la integridad de la información</td></tr>
<tr><td colspan="4">Alcance Supervisar y vigilar los cambios del sistema de gestión revisando las amenazas o modificaciones no documentadas, previniendo los accesos no autorizados a la información.</td></tr>
<tr><td colspan="4">Definiciones
<table>
<tr><th>No.</th><th>Termino</th><th>Definición</th></tr>
<tr><td>1</td><td>Software de gestión</td><td>Conjunto de herramientas que permiten tanto monitorear los equipos y servidores en la red como brindar su visualización en una interfaz web.</td></tr>
<tr><td>2</td><td>Reporte</td><td>Documento que pretende transmitir una información acerca de las incidencias que suceden en la red</td></tr>
<tr><td>3</td><td>SNMP</td><td>El Protocolo simple de administración de redes es un estándar de administración de redes utilizado en redes TCP/IP.</td></tr>
<tr><td>4</td><td>Notificación</td><td>Son alertas acerca del rendimiento de cada uno de los recursos de los dispositivos de red dentro del software de gestión</td></tr>
<tr><td>5</td><td>Diagrama de Flujo</td><td>Representación gráfica de la secuencia de pasos que describen cómo funciona un proceso</td></tr>
</table>
</td></tr>
</table>

Diagrama de flujo



Descripción de actividades

Paso	Responsable	Actividad	Descripción
1	Unidad de hardware redes y telecomunicaciones	Acceso al software de gestión	Acceso al software de gestión mediante la plataforma web
2	Unidad de hardware redes y telecomunicaciones	Acceso a los dispositivos agregados al software de gestión	Revisar que los equipos se encuentren gestionándose verificando su color donde: **Verde** significa que está monitoreando y **Rojo** indica que hay un error de comunicación snmp con ese equipo.
3	Unidad de hardware redes y telecomunicaciones	Revisión de notificaciones	Si se supera un umbral establecido se verificará las notificaciones que se encuentren tanto en la plataforma web como en el correo electrónico.
4	Unidad de hardware redes y telecomunicaciones	Si pasa un mes de ingreso al sistema	Verificar que tiempo ingresado con la misma contraseña no supere de un mes por motivos de seguridad
5	Unidad de hardware redes y telecomunicaciones	Cambio de contraseña de usuario incluyendo 6 caracteres los cuales incluyan tanto alfanuméricos como especiales	El cambio de contraseña se debe realizar incluyendo mínimo 6 caracteres los cuales incluyan tanto alfanuméricos como especiales para que sea robusta y sea más difícil el ingreso a usuarios no autorizados

CONCLUSIONES

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

- El monitoreo de los equipos en la red de EMAPA-I se lo realizó mediante el protocolo snmpv2, ya que fue de fácil implementación tanto para los equipos de red como los servidores de la entidad; también se configuró un sistema de alarmas para indicar al departamento técnico que los umbrales establecidos del 60% y 80% en las capacidades tanto de consumo de ancho de banda, memoria RAM y disco duro se están sobrepasando, disminuyendo considerablemente el tiempo de respuesta en dar una solución

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

- Se realizaron pruebas de funcionamiento de las plataformas instaladas las cuales ayudaron a elaborar y mantener un inventario actualizado, llevar el control de las capacidades técnicas de los dispositivos, y establecer políticas de seguridad, que son la base para cumplir los objetivos institucionales que incluyen actividades como: elaboración de informes técnicos, realizar planificaciones y organizar su

infraestructura tecnológica, tomando en cuenta estándares que contribuyan a asegurar la disponibilidad de los recursos dentro de la institución

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

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

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

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

- Mediante la implementación de las plataformas destinadas al sistema de inventario, el sistema de incidencias, y el sistema de monitorización se logró elaborar los manuales de procedimiento en base a las áreas del modelo de gestión SNMP, las cuales son un conjunto de instrucciones que sirven de guía al personal técnico para

mantener la red de datos de la entidad actualizada y en constante monitorización, asegurando de esta manera la disponibilidad de funcionamiento de sus recursos informáticos.

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

RECOMENDACIONES

- Es recomendable revisar este documento periódicamente y continuar con la investigación acerca del modelo de gestión SNMP, para de esta manera actualizarlo acorde con los requerimientos institucionales que vaya presentando la entidad.

- En caso de existir un crecimiento de equipos a monitorear, se recomienda que el servidor donde se encuentra el sistema de gestión debe adecuarse a las características tanto de almacenamiento como de memoria física, además se recomienda realizar periódicamente una copia de respaldo de las plataformas instaladas como medida de contingencia.

- Al personal técnico que manipula los equipos de red se recomienda seguir las políticas expuestas en este documento y de ser necesario añadir o modificar los artículos descritos, a fin de encaminarlos a mejorar el control de la red de datos de la institución.

- Se recomienda que se continúe con la investigación acerca del monitoreo en base al protocolo snmpv3 para complementar el conocimiento tanto de los métodos de encriptación como de autenticación de este protocolo, los cuales proporcionan un nivel alto de privacidad, confidencialidad e integridad de los datos.

- En base a los resultados obtenidos también se recomienda que existan capacitaciones continuas a los técnicos acerca de las configuraciones de los equipos de red con los que cuenta la institución, con la finalidad de que los procesos de respuesta sean más eficientes, mejorando así el desempeño de sus actividades y por ende se incrementen las prestaciones de la infraestructura tecnológica en beneficio de la comunidad

REFERENCIAS BIBLIOGRÁFICAS

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

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

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

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

ISOCOR. (2008). *Importancia del modelo OSI*. Recuperado el 16 de febrero del 2015 de : http://sandrabezisocor.files.wordpress.com/2008/05/redes_de_computadoras.pdf

X.700. (1992). *Marco de gestión para la interconexión de sistemas abiertos para aplicaciones del CCITT*. Recuperado el 20 de febrero del 2015 de: https://www.itu.int/rec/T-REC-X.700-199209-I/en

M.3010. (2000). *Principios para una Red de Gestión de las Telecomunicaciones*. Recuperado el 2 de marzo del 2015 de: https://www.itu.int/rec/T-REC-M.3010-200002-I/es

The Internet Engineering Task Force. (2009). *Request for Comments (RFC).* Recuperado el 4 de marzo del 2015 de: http://www.ietf.org/rfc.html.

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

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

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

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

RFC 3412. (2002). *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).* Recuperado el 10 de abril del 2015 de: https://www.ietf.org/rfc/rfc3412.txt

RFC 3413. (2002). *Simple Network Management Protocol (SNMP) Applications.* Recuperado el 10 de abril del 2015 de: https://www.ietf.org/rfc/rfc3413.txt

RFC 3414. (2002). *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).* Recuperado el 13 de abril del 2015 de: https://www.ietf.org/rfc/rfc3414.txt

RFC 3415. (2002). *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).* Recuperado el 13 de abril del 2015 de: https://www.ietf.org/rfc/rfc3415.txt

Servidores HP ProLiant DL. (2013). *Servidor HP ProLiant DL380p Gen8 E5.* Recuperado el 10 de Agosto del 2015 de: http://www8.hp.com/es/es/products/proliant-servers/product-detail.html?oid=5409733#!tab=specs

DLINK. (2014). *SWITCH DLINK DGS-3120-24TC-SI*. Recuperado el 10 de Agosto del 2015 de: http://www.dlinkla.com/dgs-3120-24tc-si

DLINK. (2014). *SWITCH DLINK DES-3028*. Recuperado el 11 de Agosto del 2015 de: http://www.dlinkla.com/des-3028

DS3 Comunicaciones. (2013). *Switch Cisco Catalyst Administrable capa L3 con 24 puertos GigE 350W - WS-C3750X-24T-S.* Recuperado el 11 de Agosto del 2015 de: http://www.ds3comunicaciones.com/cisco/WS-C3750X-24T-S.html

CISCO. (2008). *Cisco SGE2010*. Recuperado el 12 de Agosto del 2015 de: http://www.cisco.com/c/dam/en/us/products/collateral/switches/sge2010-48-port-gigabit-switch/data_sheet_c78-502072_es.pdf

ISO/IEC. (2011). *Systems and software engineering —Life cycle processes — Requirements engineering.* Recuperado el 20 de agosto de 2015 de: https://cow.ceng.metu.edu.tr/Courses/download_courseFile.php?id=7200.

Debian. (2014). *Razones para escoger debían*. Recuperado el 1 de septiembre del 2015 de: https://www.debian.org/intro/why_debian.es.html

Centos. (2015). *Acerca de Centos*. Recuperado el 1 de septiembre del 2015 de: https://wiki.centos.org/es

Red Hat Enterprise Linux Server. (2015). *Bringing Open Source to the connected enterprise.* Recuperado el 1 de septiembre del 2015 de: http://www.redhat.com/overview/bringing-open-source-to-the-connected-enterprise/

Hypertextual. (2010). *Automatiza la gestión de tus equipos con OCS.* Recuperado el 10 de septiembre del 2015 de: http://hipertextual.com/archivo/2010/09/automatiza-la-gestion-de-tus-equipos-con-ocs/

Cevallos Michilena, M. A. (2013). *Metodología de seguridad informática con base en la norma ISO 27002 y en herramientas de prevención de intrusos para la red*

administrativa del Gobierno Autónomo Descentralizado de San Miguel de Ibarra. Ibarra: Universidad Técnica del Norte.

Portilla Flores L. J. (2013). *Auditoría sistemática a la "Empresa Pública Municipal De Agua Potable Y Alcantarillado De Ibarra", ubicada en la ciudad de Ibarra, Provincia de Imbabura. Sangolqui*: Escuela Politécnica del Ejército.

Cacti. (2012). *About Cacti*. Recuperado el 1 de octubre del 2015 de: http://www.cacti.net/index.php

CHICANO, E. (2014). *Gestión de servicios en el sistema informático*. 1mera. Edición. Sitio de publicación: IC Editorial

Colombia Virtualizada. (2013). *Instalar y fusionar Cacti y Nagios*. Recuperado el 1 de octubre del 2015 de: http://www.colombiavirtualizada.com/2013/08/31/cacti-nagios-ipfix-ntop-vmware-p2/

Como instalar Linux. (2013). *Centos ssh para acceder a tu servidor Linux*. Recuperado el 10 de octubre del 2015 de: http://www.comoinstalarlinux.com/centos-ssh-para-acceder-a-tu-servidor-linux/

Luauf.com. (2008). *Limpiar archivos de log en Linux*. Recuperado el 10 de octubre del 2015 de: http://luauf.com/2008/09/07/limpiar-archivos-de-log-en-linux/

ZOHO Corp. (2012). *Configuring SNMPv3 Security Settings*. Recuperado el 20 de octubre del 2015 de:
https://www.webnms.com/simulator/help/sim_network/netsim_conf_snmpv3.html

Zandonadi, Luis. (2015). Z*abbix + Postfix + GoogleApps: Alertas por email no Debian Wheezy*. Recuperado el 1 de noviembre del 2015 de: http://luiszandonadi.com/zabbix-alertas-por-email-debian-wheezy/

ANEXOS

Anexo A: Tipos de objetos relacionados con SMI y MIB en SNMP.

- **Tipo de datos soportados en SMIv1**

Tabla A. 1 Tipo de datos SMIv1

Tipo de datos	Descripción
Integer	Es un número de 32 bits utilizado para especificar numéricamente el estado de funcionamiento de un único objeto gestionado. Por ejemplo la interfaz de un host, se puede especificar un "1" para habilita y un "2" para inhabilitada.
Octect String	Una cadena de octetos utilizada para representar cadenas de texto, también se usa para representar direcciones físicas.
Object Identifier	Una cadena decimal con puntos que representa un objeto administrado en el árbol de objetos
ipAddress	Representa una dirección ipv4 de 32 bits, ni snmpv1, ni snmpv2 discute las direcciones ipv6 de 128 bits
Counter	Un número de 32 bits con un valor mínimo de 0 y un valor máximo de 2^{32}-1, se utiliza para rastrear información como el número de octetos enviados y recibidos en una interfaz. Es constantemente creciente.
Gauge	Un número de 32 bits con un valor mínimo de 0 y un valor máximo de 2^{32}-1. A diferencia del counter, un gauge puede aumentar o disminuir a voluntad. Por ejemplo se puede medir la velocidad de la interfaz de un router.
TimeTicks	Un número de 32 bits con un valor mínimo de 0 y un valor máximo de 2^{32}-1. TimeTicks mide el tiempo en centésimas de segundo.
Opaque	Permite el paso de una sintaxis ASN.1, el dato se codifica usando las reglas de codificación básica (BER) y además se codifica como un Octect String para su transmisión.

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

- **Grupo de objetos MIB-II**

  - **Grupo "system".-** Su identificador de objeto es: 1.3.6.1.2.1.1, este grupo cuenta con información administrativa con la cual puede describir el sistema, se compone de las siguientes entidades:

Tabla A. 2 Grupo de objetos "system" en MIB-II

Objeto	O.I.D.	Descripción
sysDesr	1.3.6.1.2.1.1.1	Descripción textual del dispositivo.
sysObjectID	1.3.6.1.2.1.1.2	Indica una identificación de la entidad.
sysUpTime	1.3.6.1.2.1.1.3	Tiempo en centésimas de segundo desde el último reinicio del dispositivo.
sysContact	1.3.6.1.2.1.1.4	Campo que puede contener el nombre de la persona responsable del dispositivo.
sysName	1.3.6.1.2.1.1.5	Nombre administrativo del sistema.
sysLocation	1.3.6.1.2.1.1.6	Define la ubicación física del dispositivo.
sysServices	1.3.6.1.2.1.1.7	Valor que indica los niveles de red que proporciona el dispositivo.

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

  - **Grupo "interfaces".-** Su identificador de objeto es 1.3.6.1.2.1.2, contiene entidades asociadas con las interfaces de un dispositivo.

Tabla A. 3 Grupo de objetos "interfaces" en MIB-II

Objeto	O.I.D.	Descripción
ifNumber	1.3.6.1.2.1.2.1	Número total de interfaces de red en el sistema
ifTable	1.3.6.1.2.1.2.2	Tabla que describe la información en cada interfaz del sistema
ifEntry	1.3.6.1.2.1.2.2.1	Entradas para una interfaz en particular.
ifIndex	1.3.6.1.2.1.2.2.1.1	Un valor entero y único para cada interfaz.
ifDescr	1.3.6.1.2.1.2.2.2	Datos textuales del nombre

		del producto y la versión.
ifType	1.3.6.1.2.1.2.2.3	Tipo de interfaz
ifMtu	1.3.6.1.2.1.2.2.4	Valor del mayor tamaño del datagrama para la interfaz.
IfSpeed	1.3.6.1.2.1.2.2.5	Velocidad de datos en la interfaz en un momento dado
ifPhyAddress	1.3.6.1.2.1.2.2.6	Direcciones físicas de las interfaces
ifAdminStatus	1.3.6.1.2.1.2.2.7	Estado administrativo de la interfaz
ifOpenStatus	1.3.6.1.2.1.2.2.8	Estado del funcionamiento actual de la interfaz
ifInLastChange	1.3.6.1.2.1.2.2.9	Tiempo desde el último cambio de estado de la interfaz
ifInOctects	1.3.6.1.2.1.2.2.10	Número total de octetos recibidos.
ifInUcastPkts	1.3.6.1.2.1.2.2.11	Número de paquetes unicast enviados desde la capa de red hasta la capa aplicación.
ifInNUcastPkts	1.3.6.1.2.1.2.2.12	Número de paquetes no unicast enviados desde la capa de red hasta la capa aplicación.
ifInDiscards	1.3.6.1.2.1.2.2.13	Numero de paquetes entrantes descartados independientemente de la condición de error.
ifInErrors	1.3.6.1.2.1.2.2.14	Numero de paquetes entrantes con errores
ifInUnknowProtos	1.3.6.1.2.1.2.2.15	Numero de paquetes de protocolos no compatibles, son recibidos pero son descartados por ser desconocidos.
ifOutOctects	1.3.6.1.2.1.2.2.16	Número de octetos transmitidos fuera de la interfaz.
ifOutUcastPkts	1.3.6.1.2.1.2.2.17	Número de paquetes unicast solicitados por las capas más altas para ser transmitidos hacia direcciones unicast.
ifOutNUcastPkts	1.3.6.1.2.1.2.2.18	Número de paquetes solicitados por las capas más altas para ser

		trasmitidos hacia direcciones no unicast
ifOutDiscards	1.3.6.1.2.1.2.2.19	Número de paquetes salientes descartados independientemente del error
ifOutErrors	1.3.6.1.2.1.2.2.20	Número de paquetes de salida que no se pudieron transmitir debido a errores
ifOutQLen	1.3.6.1.2.1.2.2.21	Número de paquetes en la cola de salida
ifSpecific	1.3.6.1.2.1.2.2.22	Menciona a objetos MIB relacionados con los medios de comunicación utilizados en la interfaz.

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

- **Grupo "at".-** Su identificador de objeto es 1.3.6.1.2.1.3. Traduce direcciones entre ip y las direcciones físicas, este grupo se encuentra desaprobado y se mantiene solo por razones de compatibilidad.

- **Grupo "ip"`.-** Su identificador de objeto es 1.3.6.1.2.1.4. Este grupo tiene información sobre varios para metros del protocolo ip. Sus entidades se dividen en diferentes áreas: información y tipos de paquetes, tabla de direcciones IP, tabla de enrutamiento IP, y el mapa de traducción de direcciones IP con otros protocolos.

Tabla A. 4 Grupo de objetos "ip" en MIB-II

Información y tipos de paquetes		
Objeto	**O.I.D.**	**Descripción**
ipForwarding	1.3.6.1.2.1.4.1	Indica si el dispositivo está configurado para reenviar trafico
ipDefaultTTL	1.3.6.1.2.1.4.2	Valor de tiempo de vida para la cabecera de los datagramas enviados por la entidad
ipInReceives	1.3.6.1.2.1.4.3	Cantidad de datagramas recibidos incluyendo los del error
ipInHdrErrors	1.3.6.1.2.1.4.4	Número de datagramas descartados debido a errores en la cabecera IP
ipInAddrErrors	1.3.6.1.2.1.4.5	Número de datagramas

		descartados debido a errores de direcciones IP
ipForwDatagrams	1.3.6.1.2.1.4.6	Número de datagramas reenviados a su destino final
ipInUnkownProtos	1.3.6.1.2.1.4.7	Número de datagramas recibidos con éxito pero descartados debido al protocolo no soportado
ipInDiscards	1.3.6.1.2.1.4.8	Número de datagramas IP de entrada en los cuales no tenían problema de compatibilidad con el protocolo pero que fueron descartados (por ejemplo, por falta de espacio en el buffer)
ipInDelivers	1.3.6.1.2.1.4.9	Datagramas recibidos y entregados al nivel superior
ipOutRequest	1.3.6.1.2.1.4.10	Datagramas enviados, no se toma en cuenta los reenviados
ipOutDiscards	1.3.6.1.2.1.4.11	Datagramas de salida que no tenían error pero que fueron descartados (por ejemplo, falta de espacio en el buffer)
ipOutNoRouters	1.3.6.1.2.1.4.12	Número de datagramas Ip descartados por que no se pudo encontrar la ruta para transmitirlos a su destinación
ipReamsTimeOut	1.3.6.1.2.1.4.13	Número máximo de segundos que los fragmentos recibidos son retenidos mientras esperan ser re-ensamblados en esta entidad
ipReasmReqds	1.3.6.1.2.1.4.14	Datagramas IP recibidos que necesitan ser re-ensamblados
ipReasmOks	1.3.6.1.2.1.4.15	Número de datagramas IP que han sido re-ensamblados con éxito
ipReasmFails	1.3.6.1.2.1.4.16	Número de fallos detectados por el algoritmo de re-ensamblaje IP
ipFragOk	1.3.6.1.2.1.4.17	Número de datagramas

		fragmentados con éxito
ipFragFails	1.3.6.1.2.1.4.18	Número de datagramas Ip no fragmentados debido a que la bandera de "no fragmentación" fue habilitada
ipFragCreates	1.3.6.1.2.1.4.19	Número de fragmentos de datagrama generados como resultado de la fragmentación
ipAddrTable	1.3.6.1.2.1.4.20	Tabla de información de direccionamiento IP
ipRouteTable	1.3.6.1.2.1.4.21	Tabla de enrutamiento ip
ipNetToMediaTable	1.3.6.1.2.1.4.22	Tabla de traducción de direcciones Ip a direcciones físicas
IpRoutingDiscards	1.3.6.1.2.1.4.23	Número de entradas de enrutamiento descartadas a pesar de que eran validas

Tabla de Direcciones IP		
Objeto	**O.I.D.**	**Descripción**
ipAddrTable	1.3.6.1.2.1.4.20	Tabla de información de direccionamiento IP
ipAddrEntry	1.3.6.1.2.1.4.20.1	Una información de direccionamiento para una de las direcciones ip de esta entidad
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1	La dirección Ip a la que se refiere la información de direccionamiento de esta entrada
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2	El valor que identifica de manera única a la interfaz en la cual esta entrada es aplicable
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3	Máscara de subred asociada con la dirección Ip
ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4	Valor del bit menos significativo de la dirección de broadcast, usado para enviar datagramas en la interfaz asociada con la dirección IP de esta entrada
ipAdEntReasmMaxSize	1.3.6.1.2.1.4.20.1.5	El tamaño del datagrama

		más grande que esta interfaz puede volver a re-ensamblar de los datagramas IP fragmentados entrantes recibidos en esta interfaz.

Tabla de enrutamiento IP		
Objeto	**O.I.D.**	**Descripción**
ipRouteTable	1.3.6.1.2.1.4.21	Tabla de enrutamiento ip
ipRouteEntry	1.3.6.1.2.1.4.21.1	Ruta a un destino concreto
ipRouteDest	1.3.6.1.2.1.4.21.1.1	Dirección IP de destino de esta ruta
ipRouteIfIndex	1.3.6.1.2.1.4.21.1.2	Valor de índice único que identifica la interfaz local
ipRouteMetric1	1.3.6.1.2.1.4.21.1.3	Métrica de ruteo primario alternativo para esta ruta
ipRouteMetric2	1.3.6.1.2.1.4.21.1.4	Métrica de ruteo alternativo para esta ruta
ipRouteMetric3	1.3.6.1.2.1.4.21.1.5	Métrica de ruteo alternativo para esta ruta
ipRouteMetric4	1.3.6.1.2.1.4.21.1.6	Métrica de ruteo alternativo para esta ruta
ipRouteNextHop	1.3.6.1.2.1.4.21.1.7	Dirección IP del siguiente salto de esta ruta
ipRouteType	1.3.6.1.2.1.4.21.1.8	Tipo de ruta
ipRouteProto	1.3.6.1.2.1.4.21.1.9	Mecanismo de enrutamiento por la que esta ruta fue aprendida
IpRouteAge	1.3.6.1.2.1.4.21.1.10	Número de segundos desde que el enrutamiento se actualizo por última vez
ipRouteMask	1.3.6.1.2.1.4.21.1.11	Muestra la máscara “AND” lógico de la dirección de destino antes de ser comparada con el valor del campo IpRouteDest
ipRouteMetric5	1.3.6.1.2.1.4.21.1.12	Métrica de ruteo alternativo para esta ruta
ipRouteInfo	1.3.6.1.2.1.4.21.1.13	Menciona a objetos MIB relacionados al protocolo de ruteo que es responsable de la ruta

Mapa de traducción de direcciones IP		
Objeto	**O.I.D.**	**Descripción**
ipNetToMediaTable	1.3.6.1.2.1.4.22	Tabla de traducción de direcciones IP a direcciones físicas
ipNetToMediaEntry	1.3.6.1.2.1.4.22.1	Cada entidad contiene una dirección IP con su dirección física equivalente.
ipNetToMediaIfIndex	1.3.6.1.2.1.4.22.1.1	Interfaz en la que esta equivalencia de entradas es valida
ipNetToMediaPhysAddr	1.3.6.1.2.1.4.22.1.2	Dirección física dependiente del medio
ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3	Dirección IP correspondiente a la dirección física dependiente del medio
ipNetToMediaType	1.3.6.1.2.1.4.22.1.4	Tipo de mapeo

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

- **Grupo "icmp".-** Su identificador de objeto es 1.3.6.1.2.1.5. Todos los parámetros relacionados con el protocolo ICMP se tratan en ese grupo, el cual tiene las siguientes entidades.

Tabla A. 5 Grupo de objetos "icmp" en MIB-II

Objeto	**O.I.D.**	**Descripción**
icmpInMsgs	1.3.6.1.2.1.5.1	Número total de mensajes icmp recibidos por la entidad
icmpInErrors	1.3.6.1.2.1.5.2	Número de mensajes recibidos por la entidad con errores icmp especificas
icmpInDestUnreachs	1.3.6.1.2.1.5.3	Número de mensajes icmp recibidos con destino inalcanzable
icmpInTimeExcds	1.3.6.1.2.1.5.4	Número de mensajes icmp recibidos con tiempo excedido
icmpInParmProbs	1.3.6.1.2.1.5.5	Número de mensajes icmp recibidos con problemas de parámetros
icmpInSrcQuenchs	1.3.6.1.2.1.5.6	Número de mensajes icmp recibidos con origen extinguido

icmpInRedirects	1.3.6.1.2.1.5.7	Número de mensajes icmp recibidos re-direccionados
icmpInEchos	1.3.6.1.2.1.5.8	Número de mensajes icmp recibidos con petición de eco
icmpInEchoReps	1.3.6.1.2.1.5.9	Número de mensajes de respuesta de eco icmp recibidos
icmpInTimeStamps	1.3.6.1.2.1.5.10	Número de mensajes icmp recibidos con petición de marca de tiempo
icmpInTimeStampReps	1.3.6.1.2.1.5.11	Número de mensajes icmp recibidos con respuesta de marca de tiempo
icmpInAddrMask	1.3.6.1.2.1.5.12	Número de mensajes icmp recibidos con petición de mascara de red
icmpInAddrMaskReps	1.3.6.1.2.1.5.13	Número de mensajes icmp recibidos con respuesta de marca de tiempo
icmpOutMsgs	1.3.6.1.2.1.5.14	Número de mensajes icmp que la entidad intenta enviar
icmpOutErrors	1.3.6.1.2.1.5.15	Número de mensajes icmp que la entidad no pudo enviar debido a problemas descubiertas con el protocolo icmp
icmpOutDestUnreachs	1.3.6.1.2.1.5.16	Número de mensajes icmp enviados con destino inalcanzable
icmpOutTimeExcds	1.3.6.1.2.1.5.17	Número de mensajes icmp enviados con tiempo excedido
icmpOutParmProbs	1.3.6.1.2.1.5.18	Número de mensajes icmp enviados con problemas de parámetros
icmpOutScrQuenchs	1.3.6.1.2.1.5.19	Número de mensajes icmp enviados con origen extinguido
icmpOutRedirects	1.3.6.1.2.1.5.20	Número de mensajes icmp enviados y re-direccionados
icmpOutEchos	1.3.6.1.2.1.5.21	Número de mensajes icmp Echo Request enviados
icmpOutEchoReps	1.3.6.1.2.1.5.22	Número de mensajes icmp Echo Replay enviados
icmpOutTimeStamps	1.3.6.1.2.1.5.23	Número de mensajes icmp enviados con petición de

		marca de tiempo
icmpOutTimeStampReps	1.3.6.1.2.1.5.24	Número de mensajes icmp enviados con respuesta de marca de tiempo
icmpOutAddrMask	1.3.6.1.2.1.5.25	Número de mensajes icmp enviados con petición de máscara de red
icmpOutAddrMaskReps	1.3.6.1.2.1.5.26	Número de mensajes icmp enviados con respuesta de máscara de red

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

- **Grupo "tcp".-** Su identificador de objeto es 1.3.6.1.2.1.6, contiene parámetros relacionados con el protocolo tcp, las entidades pertenecientes a este grupo son las siguientes.

Tabla A. 6 Grupo de objetos "tcp" en MIB-II

Objeto	**O.I.D.**	**Descripción**
tcpRtoAlgorithm	1.3.6.1.2.1.6.1	Algoritmos de tiempo de espera para retransmisión de objetos
tcpRtoMin	1.3.6.1.2.1.6.2	Valor mínimo para el tiempo de espera de retransmisión
tcpRtoMax	1.3.6.1.2.1.6.3	Valor máximo para el tiempo de espera de retransmisión
tcpMaxConn	1.3.6.1.2.1.6.4	El número máximo de conexiones tcp que soporta la entidad
tcpActiveOpens	1.3.6.1.2.1.6.5	Cantidad de tiempo en la que la conexión tcp debe hacer una transición directa al estado de envió sincrónico desde el estado de conexión cerrada
tcpPasiveOpens	1.3.6.1.2.1.6.6	Cantidad de tiempo en la que la conexión tcp debe hacer una transición directa al estado de recepción sincrónica desde el estado de escucha
tcpAttemptFails	1.3.6.1.2.1.6.7	Número de intentos fallidos en hacer la conexión
tcpestabResets	1.3.6.1.2.1.6.8	Cantidad de tiempo en la

		conexión tcp debe hacer una transición directa al estado de conexión terminada desde el estado de conexión establecida o desde el estado de conexión en espera de terminación
tcpCurrEstab	1.3.6.1.2.1.6.9	Número de conexiones tcp para que el estado actual este entre conexión establecida o conexión en espera de terminación
tcpInSegs	1.3.6.1.2.1.6.10	El número total de segmentos recibidos, incluyendo aquellos recibidos por error. Este conteo incluye segmentos recibidos en las conexiones establecidas actualmente
tcpOutSegs	1.3.6.1.2.1.6.11	El número total de segmentos enviados, incluyendo a aquellos con conexiones actuales, pero excluyendo aquellos que contienen octetos retransmitidos
tcpRetransSegs	1.3.6.1.2.1.6.12	Número total de segmentos retransmitidos
tcpConnTable	1.3.6.1.2.1.6.13	Tabla de conexiones tcp
tcpInErrs	1.3.6.1.2.1.6.14	Número total de segmentos recibidos con error
tcpOutRsts	1.3.6.1.2.1.6.15	Número de segmentos tcp enviados que contienen la bandera de reset, número de veces que se intenta resetear una sesión.

Conexiones tcp		
Objeto	**O.I.D.**	**Descripción**
tcpConnTable	1.3.6.1.2.1.6.13	Tabla de conexiones tcp
tcpConnEntry	1.3.6.1.2.1.6.13.1	Información particular sobre una conexión tcp actual
tcpConnState	1.3.6.1.2.1.6.13.1.1	Estado de la conexión tcp actual

tcpConnLocalAddress	1.3.6.1.2.1.6.13.1.2	Dirección ip local para esta conexión
tcpConnLocalPort	1.3.6.1.2.1.6.13.1.3	Número de puerto local para esta conexión
tcpConnRemAddress	1.3.6.1.2.1.6.13.1.4	Dirección ip remota para esta conexión
tcpConnRemPort	1.3.6.1.2.1.6.13.1.5	Número de puerto remoto para esta conexión

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

- **Grupo "udp".-** Su identificador de objeto es 1.3.6.1.2.1.7. Contiene información asociada con el protocolo de transporte sin conexión, las entidades pertenecientes a este grupo son las siguientes.

Tabla A. 7 Grupo de objetos "udp" en MIB-II

Objeto	**O.I.D.**	**Descripción**
udpInDatagrams	1.3.6.1.2.1.7.1	Número total de datagramas entregados a los usuarios
udpNoPorts	1.3.6.1.2.1.7.2	Número total de datagramas que no fueron enviados a un puerto válido
udpInErrors	1.3.6.1.2.1.7.3	Número de datagramas recibidos con errores
udpOutDatagrams	1.3.6.1.2.1.7.4	Número total de datagramas enviados
udpTable	1.3.6.1.2.1.7.5	Tabla de puertos UDP en escucha
udpEntry	1.3.6.1.2.1.7.5.1	Información particular sobre un puerto UDP de escucha
udpLocalAddress	1.3.6.1.2.1.7.5.1.1	Dirección IP local
udpLocalPort	1.3.6.1.2.1.7.5.1.2	Puerto UDP local

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

- **Grupo "egp".-** Su identificador de objeto es 1.3.6.1.2.1.8. Contiene información asociada con el protocolo egp, las entidades que pertenecen a este grupo son las siguientes.

Tabla A. 8 Grupo de objetos "egp" en MIB-II

Objeto	**O.I.D.**	**Descripción**
egpInMsgs	1.3.6.1.2.1.8.1	Número de mensajes egp

		recibidos sin errores
egpInErrs	1.3.6.1.2.1.8.2	Número de mensajes egp que probablemente contienen errores
egpOutMsgs	1.3.6.1.2.1.8.3	Número de mensajes egp generados localmente
egpOutErrs	1.3.6.1.2.1.8.4	Número de mensajes egp generados localmente que no han sido enviados debido a limitaciones de recursos
egpNeighTable	1.3.6.1.2.1.8.5	Tabla de la comunidad egp
egpNeighEntry	1.3.6.1.2.1.8.5.1	Información particular sobre un vecino egp
egpNeighState	1.3.6.1.2.1.8.5.1.1	Estado local de la entidad egp respecto al vecindario o comunidad egp
egpNeighAddr	1.3.6.1.2.1.8.5.1.2	Dirección ip de esta entrada de comunidad egp
egpNeighAs	1.3.6.1.2.1.8.5.1.3	Sistema autónomo de este sistema egp
egpNeighInMsgs	1.3.6.1.2.1.8.5.1.4	Número de mensajes egp recibidos desde un punto egp del vecindario
egpNeighInErrs	1.3.6.1.2.1.8.5.1.5	Número de mensajes recibidos sin error
egpNeighOutMsgs	1.3.6.1.2.1.8.5.1.6	Número de mensajes generados en este punto egp
egpNeighOutErrs	1.3.6.1.2.1.8.5.1.7	Número de mensajes generados localmente pero que no han sido transmitidos debido a limitaciones de la entidad
egpNeighInErrsMsgs	1.3.6.1.2.1.8.5.1.8	Número de errores de mensajes recibidos en este punto del vecindario egp
egpNeighOutErrsMsgs	1.3.6.1.2.1.8.5.1.9	Número de errores de mensajes definidos enviados hacia este punto egp
egpNeighStateUps	1.3.6.1.2.1.8.5.1.10	Número de transiciones de estado egp hacia el estado up (en el estado up el vecino puede comenzar a intercambiar información).
egpNeighStateDowns	1.3.6.1.2.1.8.5.1.11	Número de transiciones del estado “up” hacia otro estado

egpNeighIntervalHello	1.3.6.1.2.1.8.5.1.12	Intervalo entre las retransmisiones del comando Hello
egpNeighIntervalPoll	1.3.6.1.2.1.8.5.1.13	Intervalo entre las retransmisiones del comando
egpNeighMode	1.3.6.1.2.1.8.5.1.14	Modo de polling (sondeo) de esta entidad
egpNeighEventTrigger	1.3.6.1.2.1.8.5.1.15	Control variable empleado para disparar los eventos start y/o stop sobre la entidad

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

- **Grupo "cmot".-** Su identificador de objeto es: 1.3.6.1.2.1.9. El grupo existe por razones históricas, se introdujo para ayudar a la transmisión CMIS/CMIP, aunque existe definición para cmot, no se ha hecho un trabajo significativo con este protocolo.
- **Grupo "transmission".-** Su identificador de objeto es 1.3.6.1.2.1.10. Es este grupo se tratan aspectos relacionados con la transmisión de datos en los medios físicos.
- **Grupo "snmp".-** Su identificador de objeto es 1.3.6.1.2.1.11. Contiene información asociada al protocolo snmp. Las entidades que lo conforman son las siguientes.

Tabla A. 9 Grupo de objetos "snmp" en MIB-II

Objeto	**O.I.D.**	**Descripción**
snmpInPkts	1.3.6.1.2.1.11.1	Número total de mensajes entregados a la entidad snmp desde el servicio de transporte
snmpOutPkts	1.3.6.1.2.1.11.2	Número total de mensajes que fueron pasados desde la entidad a través del protocolo snmp hacia el servicio de transporte
snmpInBadVersions	1.3.6.1.2.1.11.3	Número total de mensajes que fueron pasados desde la entidad a través del protocolo snmp y que no soportan la versión del protocolo snmp
snmpInBadCommunityNames	1.3.6.1.2.1.11.4	Número total de mensajes

		que fueron pasados desde la entidad a través del protocolo snmp y que usan un nombre de comunidad snmp erróneo o desconocido
snmpInBadCommunityUse	1.3.6.1.2.1.11.5	Número total de mensajes que fueron pasados desde la entidad a través del protocolo snmp que representan una operación que no está permitida por el nombre de comunidad snmp en el mensaje.
snmpInAsnParseErrs	1.3.6.1.2.1.11.6	Número de errores de notación ASN.1 o de errores de reglas básicas de codificación(BER)
snmpInTooBigs	1.3.6.1.2.1.11.8	Número total de unidades de procesamiento de datos snmp que ingresaron a la entidad con un valor demasiado grande
snmpInNoSuchNames	1.3.6.1.2.1.11.9	Número total de unidades de procesamiento de datos snmp que ingresaron a la entidad “NoSuchName”
snmpInBadValues	1.3.6.1.2.1.11.10	Número total de unidades de procesamiento de datos snmp que ingresaron a la entidad con valores erróneos.
snmpInReadOnly	1.3.6.1.2.1.11.11	Número total de unidades de procesamiento de datos snmp que ingresaron a la entidad con un valor de solo lectura
snmpInGenErrs	1.3.6.1.2.1.11.12	Número total de unidades de procesamiento de datos snmp que ingresaron a la entidad y generaron errores.
snmpInTotalReqVars	1.3.6.1.2.1.11.13	Número total de objetos MIB que han sido entregados satisfactoriamente a las entidad como resultado de haber recibido PDUs válidas

snmpInTotalSetVars	1.3.6.1.2.1.11.14	Número total de objetos MIB que han sido cambiados satisfactoriamente en la entidad como resultado de haber recibido PDUs válidos.
snmpInGetRequest	1.3.6.1.2.1.11.15	Número total de PDUs snmp "get-request" que han sido aceptados y procesados por la entidad snmp
snmpInGetNexts	1.3.6.1.2.1.11.16	Número total de PDUs snmp "get-next" que han sido aceptados y procesados por la entidad snmp
snmpInSetRequest	1.3.6.1.2.1.11.17	Número total de pdus snmp "set-request" que han sido aceptados y procesados por la entidad snmp
snmpInGetResponses	1.3.6.1.2.1.11.18	Número total de PDUs snmp "get-response" que han sido aceptados y procesados por la entidad SNMP
snmpInTraps	1.3.6.1.2.1.11.19	Número total de PDUs snmp "trap" que han sido aceptados y procesados por la entidad snmp
snmpOutTooBigs	1.3.6.1.2.1.11.20	Número total de unidades de procesamiento de datos snmp que han sido generados en la entidad con un valor demasiado grande
snmpOutNoSuchNames	1.3.6.1.2.1.11.21	Número total de unidades de procesamiento de datos snmp que se generaron en la entidad con la condición de error "NoSuchName"
snmpOutBadValues	1.3.6.1.2.1.11.22	Número total de unidades de procesamiento de datos snmp que se generaron en la entidad y poseen errores
snmpOutGenErrs	1.3.6.1.2.1.11.24	Número total de unidades

		de procesamiento de datos snmp que se generaron en la entidad y poseen errores
snmpOutGetRequest	1.3.6.1.2.1.11.25	Número total de PDUs snmp "get-request" que han sido generados por la entidad
snmpOutGetNext	1.3.6.1.2.1.11.26	Número total de PDUs snmp "get-next" que han sido generados por la entidad
snmpInSetRequest	1.3.6.1.2.1.11.27	Número total de PDUs snmp "set-request" que han sido generados por la entidad
snmpOutGetResponses	1.3.6.1.2.1.11.28	Número total de PDUs snmp "get-response" que han sido generados por la entidad
snmpOutTraps	1.3.6.1.2.1.11.29	Número total de PDUs snmp "trap" que han sido generados por la entidad
snmpEnableAuthenTraps	1.3.6.1.2.1.11.30	Indica que el proceso de agente snmp está en capacidad de generar trampas de autenticación de fallos.

Fuente: RFC 1213. (1991). Management Information Base for Network Management of TCP/IP-based internets

- **Tipo de datos soportados en SMIv2**

Tabla A. 10 Tipo de datos SMIv2

Tipo de datos	Descripción
Integer32	Es un número de 32 bits utilizado para especificar numéricamente el estado de funcionamiento de un único objeto gestionado. Por ejemplo la interfaz de un host, se puede especificar un "1" para habilita y un "2" para inhabilitada.
Counter32	Un número de 32 bits con un valor mínimo de 0 y un valor máximo de 2^{32}-1, se utiliza para rastrear información como el número de octetos enviados y recibidos en una interfaz. Es constantemente creciente.
Counter64	Similar a un Counter32 pero su valor máximo es 2^{64}-1

Gauge32	Un número de 32 bits con un valor mínimo de 0 y un valor máximo de 2^{32}-1. A diferencia del counter, un gauge puede aumentar o disminuir a voluntad. Por ejemplo se puede medir la velocidad de la interfaz de un router.
BITS	Una numeración de bits identificados con un nombre
UnitsPart	Es una descripción textual de las unidades que están asociadas con el objeto, en caso de medir una variable de tiempo se podría determinar si se trata de segundos, milisegundos, etc
MAX-ACCESS	Describe los tipos de acceso a un objeto con las siguientes opciones: **Read-write:** Permisos para leer y escribir pero no crear **Read-create:** Permisos para leer, escribir y crear un objeto **Not-accesible:** El gestor no puede acceder al objeto para ninguna operación **Accesible-for-notify:** solo accesible via una notificación. **Read-only:** acceso solamente para lectura
STATUS	Indica si la definición del objeto es actual u obsoleta con las siguientes opciones: **Current:** significa que la definición es válida y vigente **Obsolete:** Significa que la definición es obsoleta y no debe ser implementada **Deprecated:** Significa que el objeto está obsoleto pero puede ser necesario para la compatibilidad con aplicaciones antiguas
AUGMENTS	En algunos casos es útil agregar una columna a una tabla existente, la cláusula AUGMENT permite extender una tabla mediante la adición de una o más columnas

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

- **Cambios en el grupo de objetos MIB-II**

  - **Grupo system**

Tabla A. 11 Cambios en el grupo de objetos "system" en MIB-II

Objeto	O.I.D.	Descripción
sysOrLastChange	1.3.6.1.2.1.1.8	El valor de sysUpTime en el momento del más reciente cambio de estado o el valor de cualquier instancia de sysOrID
sysOrTable	1.3.6.1.2.1.1.9	Tabla que enumera los recursos del sistema que controla el agente, el gestor puede configurar estos recursos a través del agente.
sysOrEntry	1.3.6.1.2.1.1.9.1	Una entrada en el sysOrTable
sysOrIndex	1.3.6.1.2.1.1.9.1.1	Índice de la fila, también el índice para la tabla
sysOrID	1.3.6.1.2.1.1.9.1.2	ID del módulo de recursos
sysOrDescr	1.3.6.1.2.1.1.9.1.3	Descripción textual del módulo de recursos
sysOrUpTime	1.3.6.1.2.1.1.9.1.4	El tiempo de funcionamiento desde que el objeto en esta fila fue última instancia

Fuente: RFC 3418. (2002). Management Information Base for the Simple Network Management Protocol

- **Grupo snmp**

El grupo snmp en snmpv2 ha sido considerablemente simplificado, se eliminaron un gran número de entidades que se consideraron innecesarias, tiene ocho entidades, seis antiguas y 2 nuevas

Tabla A. 12 Cambios en el grupo de objetos "snmp" en MIB-II

Objeto	O.I.D.	Descripción
snmpInPkts	1.3.6.1.2.1.11.1	Número total de mensajes entregados a la entidad snmp desde el servicio de transporte
snmpInBadVersions	1.3.6.1.2.1.11.3	Número total de mensajes que fueron pasados desde la entidad a través del protocolo snmp y que no soportan la versión del protocolo snmp
snmpInBadCommunityNames	1.3.6.1.2.1.11.4	Número total de mensajes

		que fueron pasados desde la entidad a través del protocolo snmp y que usan un nombre de comunidad snmp erróneo o desconocido
snmpInBadCommunityUse	1.3.6.1.2.1.11.5	Número total de mensajes que fueron pasados desde la entidad a través del protocolo snmp que representan una operación que no está permitida por el nombre de comunidad snmp en el mensaje.
snmpInAsnParseErrs	1.3.6.1.2.1.11.6	Número de errores de notación ASN.1 o de errores de reglas básicas de codificación(BER)
snmpEnableAuthenTraps	1.3.6.1.2.1.11.30	Indica que el proceso de agente snmp está en capacidad de generar trampas de autenticación de fallos.
snmpSilentDrops	1.3.6.1.2.1.11.31	Número total de los 5 tipos de PDU recibidos que fueron silenciosamente abandonados debido a las excepciones en el campo variable-bindings
snmpProxyDrops	1.3.6.1.2.1.11.32	Número total de los 5 tipos de PDU recibidos que fueron silenciosamente abandonados debido a la imposibilidad de responder a un proxy de destino.

Fuente: RFC 3418. (2002). Management Information Base for the Simple Network Management Protocol

- **Información para la notificación en snmpv2**

La información sobre trampas en snmpv1 se ha re-estructurado en la versión 2 para ajustarse al resto de PDUs. La macro TRAP-TYPE usada en la versión 1 y descrita en el

RFC 1215, se ha hecho obsoleta en snmpv2. La información sobre las notificaciones se define bajo snmp MIBObjects y una breve descripción de los sub-nodos y objetos. Hay 2 módulos bajo el nodo snmpMIBObjects: snmpTrap (4), snmpTraps (5), y snmpset (6).

Tabla A. 13 Grupo de objetos "snmpMIBObjects" en MIB-II

Objeto	**O.I.D.**	**Descripción**
snmpTrap	1.3.6.1.6.3.1.1.4	Grupo de información que contiene la ID de la notificación y la ID de la empresa
snmpTrapOID	1.3.6.1.6.3.1.1.4.1	OBJECT IDENTIFIER de la notificación
snmpTrapEnterprise	1.3.6.1.6.3.1.1.4.2	OBJECT IDENTIFIER asociada con la empresa que envió la notificación
snmpTraps	1.3.6.1.6.3.1.1.5	Colección de notificaciones utilizados en snmpv1
coldStart	1.3.6.1.6.3.1.1.5.1	Trampa informando de un arranque en frio del objeto
warmStart	1.3.6.1.6.3.1.1.5.2	Trampa informando de un arranque en caliente de un objeto
linkDown	1.3.6.1.6.3.1.1.5.3	Agente detectando de un fallo de un enlace de comunicación.
linkUp	1.3.6.1.6.3.1.1.5.4	Agente detectando que está subiendo un enlace de comunicación.
AuthentificationFailure	1.3.6.1.6.3.1.1.5.5	Agente reportando la recepción de informes de un mensaje de protocolo no autenticado.
snmpSet	1.3.6.1.6.3.1.1.5.6	Notificaciones de mensajes gestor-gestor
snmpSetSerialNo	1.3.6.1.6.3.1.1.5.6.1	Bloqueo consultivo entre los administradores para coordinar el funcionamiento conjunto

Fuente: RFC 3418. (2002). Management Information Base for the Simple Network Management Protocol

- **Tipos de PDU y campos “error-status” en snmpv2**

Tabla A. 14 Valores para los tipos de PDU y campos “error-status” en snmpv2

Campo	Tipo	Valor	Descripción
PDU	0	Get-Request	
	1	Get-Next-Request	
	2	Response	
	3	Set-Request	
	4	Obsolete	
	5	Get-Bulk-Request	
	6	Inform-Request	
	7	Snmpv2-Trap	
	8	Report	
Error-Status	0	NoError	No ha ocurrido ningún error, este código también se utiliza en todas las PDU de petición, ya que no tienen estado de error para informar
	1	tooBig	El tamaño del mensaje Response es demasiado grande para el transporte
	2	noSuchName	No se encontró el nombre de un objeto solicitado
	3	badValue	Un valor en la solicitud no coincide con la estructura que el destinatario de la solicitud tenía por objeto
	4	readOnly	Se hizo un intento para establecer una variable que tiene un valor de acceso que indica que es de solo lectura
	5	genErr	Ha ocurrido un error distinto a uno indicado en esta tabla
	6	noAccess	Se denegó el

			acceso al objeto por razones de seguridad
	7	wrongType	El tipo de objeto en una variable de enlace es incorrecto para el objeto
	8	wrongLength	Un campo variable especifica una longitud incorrecta para el objeto
	9	wrongEncoding	Un campo variable especifica una codificación incorrecta para el objeto
	10	wrongValue	El valor dado en un campo variable no es posible para el objeto
	11	noCreation	No existe una variable especificada y no puede ser creada
	12	inconsistentValue	Un campo variable especifica un valor que podría realizarse por la variable, pero no puede asignarse a la misma en este momento
	13	resourceUnavailable	Un intento de establecer una variable requiere un recurso que no está disponible
	14	commitFailed	Un intento de configurar una variable en particular falló
	15	undoFailed	Un intento de configurar una variable en

			particular como parte de un grupo de variables falló y el intento de deshacer luego las configuraciones de otras variables no tuvo éxito
	16	authorizationError	Se produjo un problema en la autorización
	17	noWritable	La variable no puede ser escrita o creada

Fuente: RFC 3416. (2002). Version 2 of the Protocol Operations for the Simple Network Management Protocol

Anexo B: Manual de instalaciones de los software instalados

B.1. Instalación y de requisitos para Ocs-Inventory

El sistema operativo sobre el que se instalará el software de gestión es CENTOS, es importante actualizar el sistema operativo completo, para ello emplearemos la herramienta terminal y aplicaremos el comando: yum update

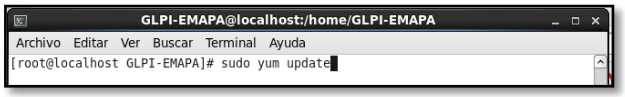


Figura B. 1 Actualización del sistema

Se empiezan a actualizar las librerías del sistema operativo, este proceso lleva tiempo y su proceso sería similar al de la siguiente figura.

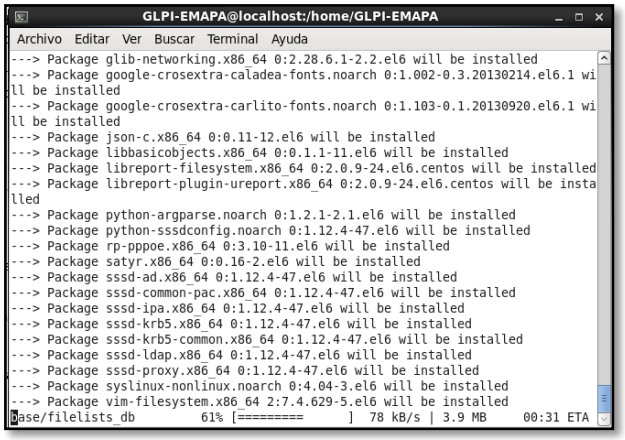


Figura B. 1 Actualización de librerías

El programa necesita la instalación de dependencias, que se lleva a cabo con el siguiente comando: yum install httpd mod_perl php php-gd php-pear php-devel php-mysql php-mbstring perl mysql-server mysql make perl-XML-Simple perl-Compress-Zlib perl-DBI perl-DBD-MySQL perl-Net-IP perl-SOAP-Lite perl-Digest-SHA1 lynx gcc zlib-devel pcre pcre-devel mod_perl-devel

Figura B. 2 Instalación de librerías

En el proceso de instalación requerirá la confirmación de instalación y reemplazo de los antiguos paquetes por los nuevos, presione la letra “S” y presione la tecla “enter”.

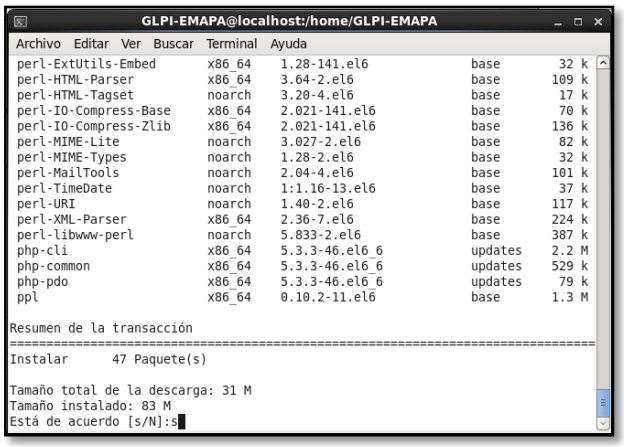


Figura B. 3 Confirmación de reemplazo de paquetes.

Configuramos una librería PHP

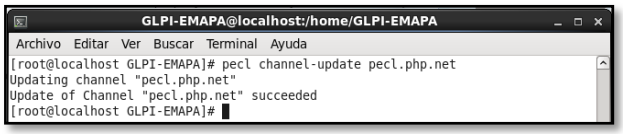


Figura B. 4 Agregar una librería PHP

Iniciamos MySQL.

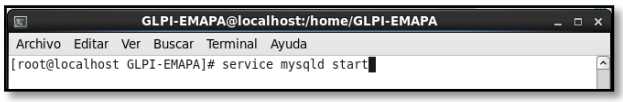


Figura B. 5 Iniciar MySQL

Una vez iniciado MySQL, le colocamos contraseña al usuario root.

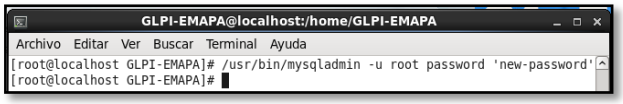


Figura B. 6 Agregar contraseña al usuario root

Activamos su ejecución cada vez que iniciemos el servidor.

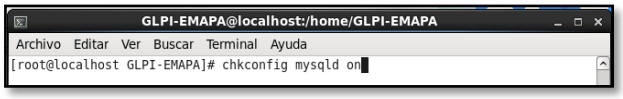


Figura B. 7 Iniciación del servidor

Descargamos el modulo perl apache2.

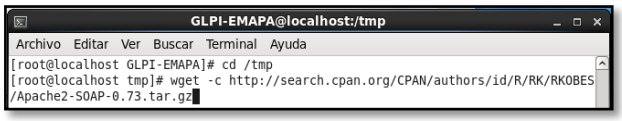


Figura B. 8 Descarga del módulo perl

Lo desempaquetamos con el comando

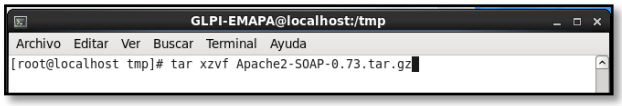


Figura B. 9 Desempaquetar módulo Perl

Lo compilamos e instalamos, conforme a lo mostrado en las figuras

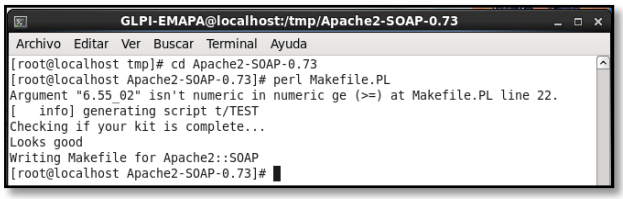


Figura B. 10 Compilación e instalación

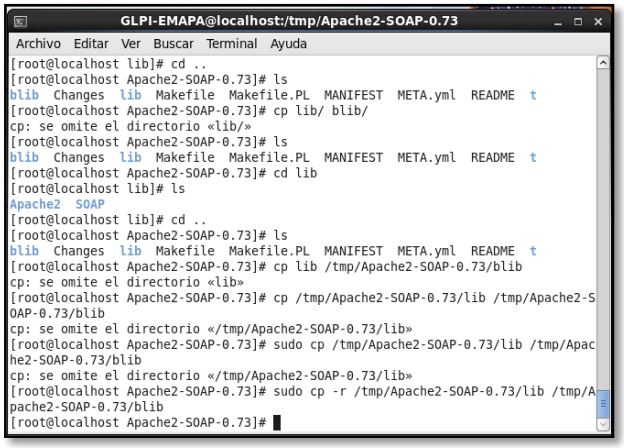


Figura B. 11 Compilación e instalación

Ingresamos a la carpeta cd /root dentro del archivo Apache

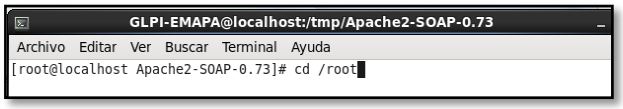


Figura B. 12 Localización del directorio respectivo

Descarga del ocs-inventory-server dentro del módulo perl-Apache.

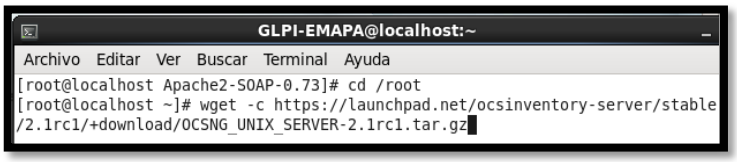


Figura B. 13 Descarga ocsnventory-server

Descomprimimos el paquete descargado.

Figura B. 14 Descomprimir el paquete descargado

Iniciamos apache

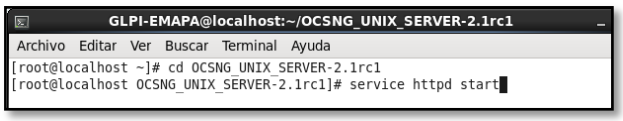


Figura B. 15 Inicio de servicio httpd

Ejecutamos apache, para que inicie por defecto al iniciar el sistema.

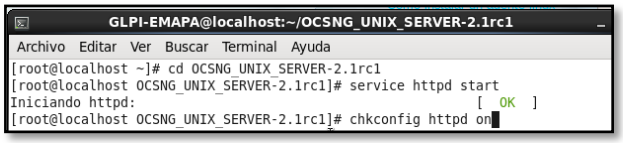


Figura B. 16 Ejecutar apache

Configuramos ocsinventory-server. Por lo general la respuesta por default es el valor correcto y ENTER es suficiente.

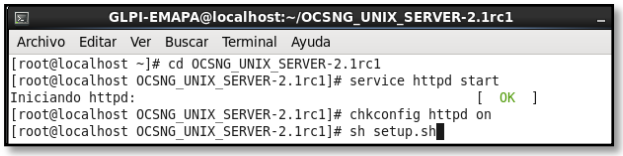


Figura B. 17 Configuración de ocs-inventory

A continuación, se presentarán una serie de requerimientos a los cuales debemos confirmar con la tecla enter.

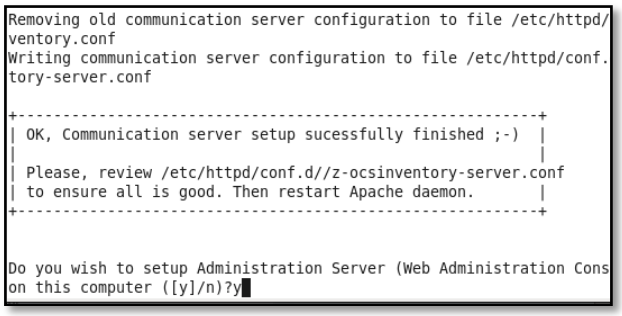


Figura B. 18 Confirmación de ajustes en las librerías de OCS Agent

Modificamos en php.ini, con el editor de texto gedit.

Figura B. 19 Modificar el fichero php.ini

Ubicamos la línea post_max_size, el valor por defecto de 40 megas.

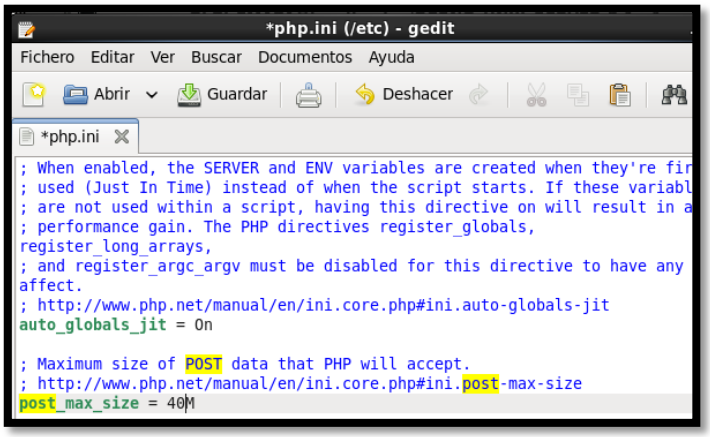


Figura B. 20 Edición de fichero, línea post_max_size

Cambiamos el valor de la línea upload_max_size para que el valor sea de 100 megas, este valor dependerá del tamaño que necesitamos que los usuarios suban sus archivos.

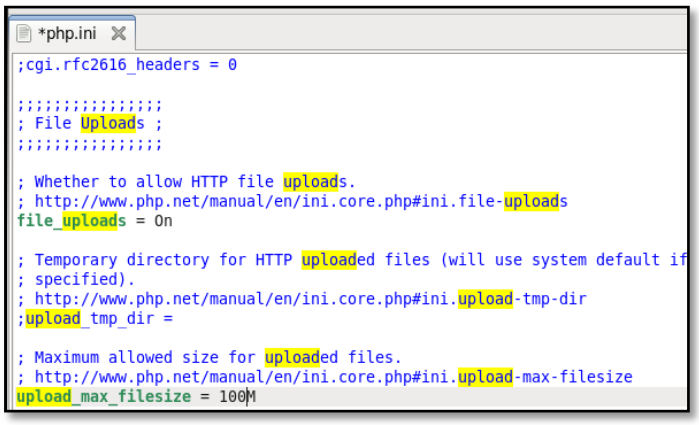


Figura B. 21 Edición de fichero php, línea upload_max_filesize

Modificamos y colocamos la información del usuario root de mysql, el primer paso es abrir el siguiente fichero con el editor gedit.

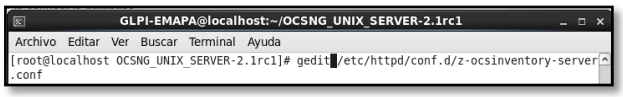


Figura B. 22 Fichero para agregar usuario de root de MySQL

Asociamos la base de datos de mysql con la base de datos de ocs inventory.

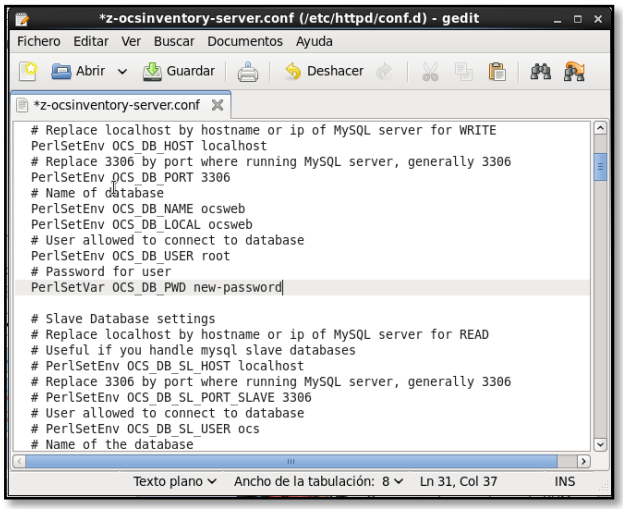


Figura B. 23 Agregar la password de MySQL en ocs-inventory

Instalamos los complementos de paquetes EPEL.

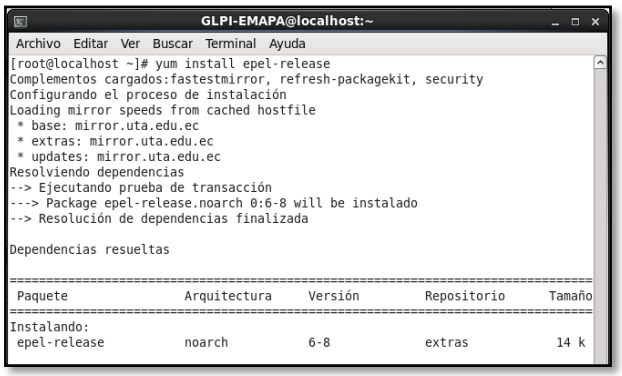


Figura B. 24 Instalación de paquetes EPEL

A continuación, instalar algunos paquetes de módulos Perl necesarios.

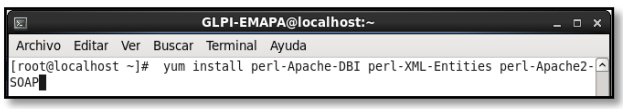


Figura B. 25 Instalar algunos paquetes PERL

Confirmamos la ejecución de la instalación.

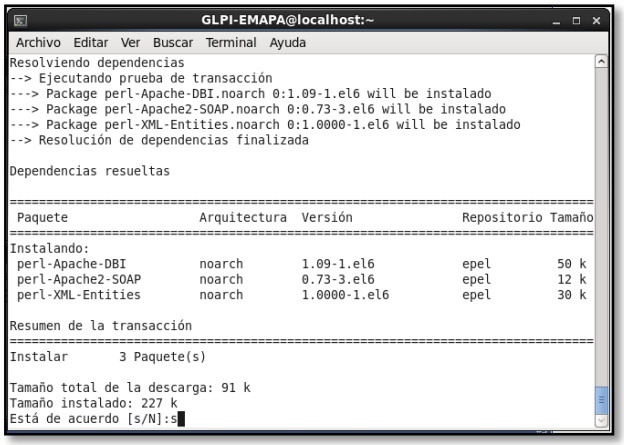


Figura B. 26 Confirmación de instalación

Reinicio del servicio httpd

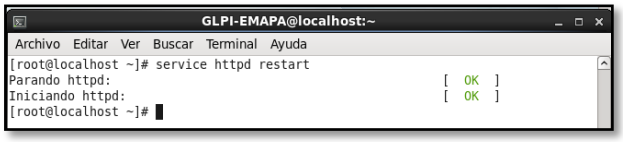


Figura B. 27 Reinicio del servicio http

- **CONFIGURACION DE OCS-INVENTORY AGENT**

En un navegador web ingresamos la dirección: localhost/oscreports.

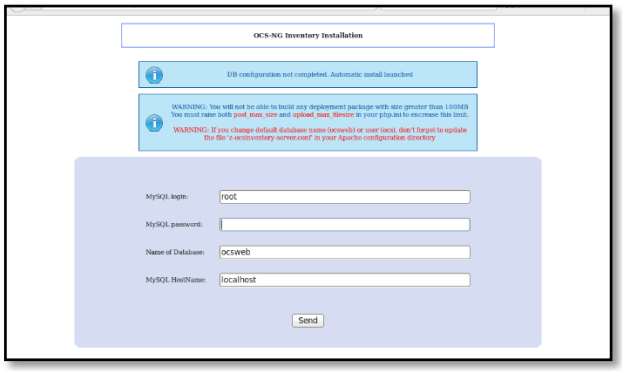


Figura B. 28 Página inicial del OCS-Inventory Agent

Generalmente se produce un error con el enlace con la base de datos.

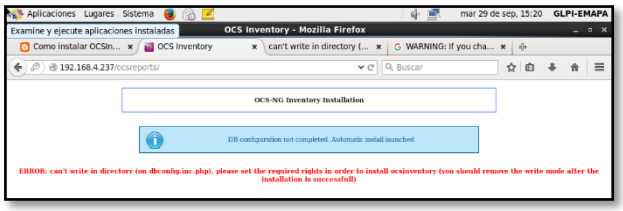


Figura B. 29 Error en un fichero

Editamos el fichero db.config.inc.php, como se muestra, agregando el nombre de la base de datos y la contraseña de la base de datos.

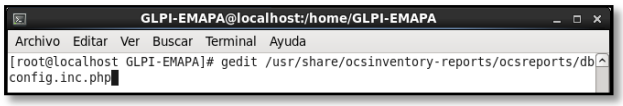


Figura B. 30 Edición del fichero db.config.inc.php

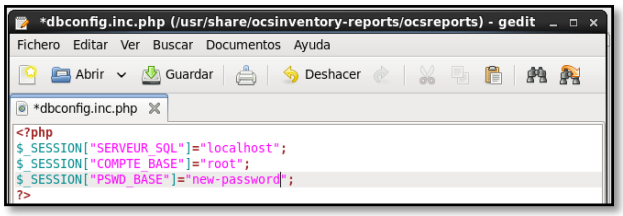


Figura B. 31 Edición del fichero db.config.inc.php

Una vez editado ese fichero ya podemos ingresar al sistema

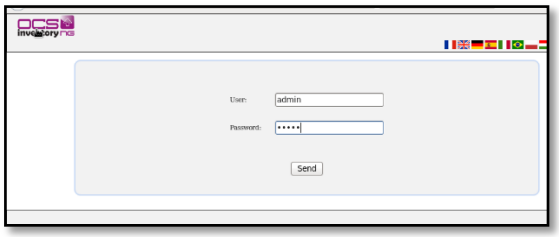


Figura B. 32 Pantalla inicial de OCS-Inventory

Ingresamos los usuarios que tendrán privilegios de administrador.

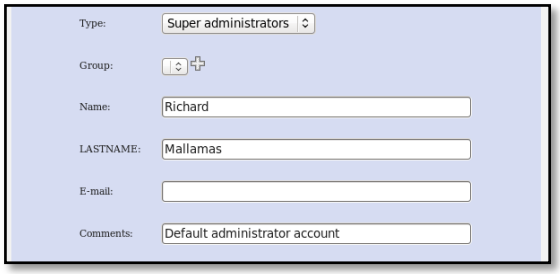


Figura B. 33 Agregar usuarios administradores

En el proceso de configuración puede presentarse una alerta como la que se visualiza en la figura, respecto a que se solicita que cambiemos la contraseña de la base de datos para que sea más seguro el ingreso al sistema.

Figura B. 34 Alerta en la seguridad de la base de datos

Editamos la siguiente línea de comandos en el terminal.

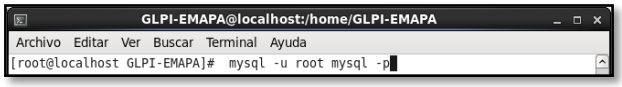


Figura B. 35 Activar la base de datos OCS

Cambiamos la contraseña de la base de datos y agregar los privilegios a la base de datos.

Figura B. 36 Agregar privilegios

La alerta que se mostraba, después de este proceso se ha solucionado.

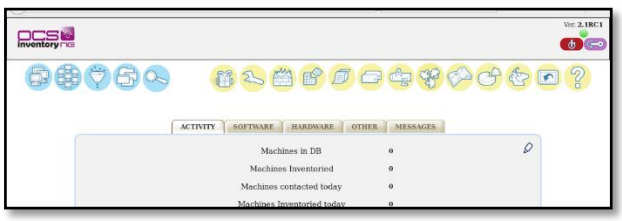


Figura B. 37 Pantalla inicial del agente OCS

Para agregar una red, para monitorear se debe llenar los requerimientos en la siguiente pantalla.

Figura B. 38 Parámetros necesarios para agregar la red a monitorear

Una vez agregada la red damos click en el botón agregar y comienza el proceso de monitoreo de la auditoria.

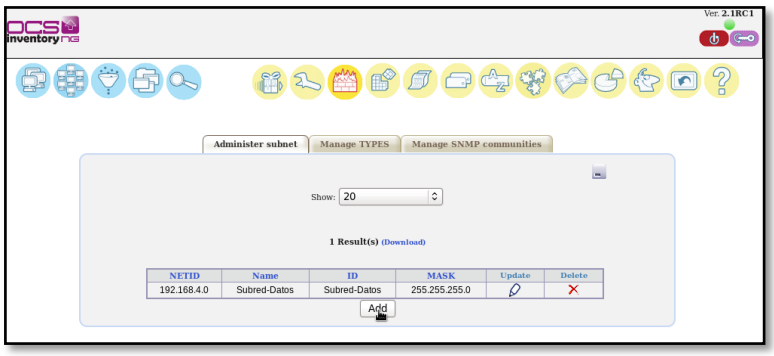


Figura B. 39 Configuración de la red administradora

B.2 Instalación y configuración GLPI

Para la instalación de GLPI, empezamos editando la primera línea de comandos en el terminal.

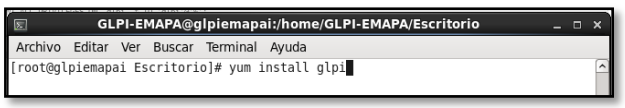


Figura B. 40 Instalación GLPI

Confirmamos todas las peticiones por parte del sistema y reiniciamos el servicio httpd.

Figura B. 41 Reinicio del servicio httpd

Selección del idioma, en el proceso de instalación GLPI.

Figura B. 42 Selección del idioma

Leemos la licencia, y aceptamos los términos

Figura B. 43 Leer los términos y aceptar términos de licencia

Especificar que es una instalación.

Figura B. 44 Especificar que es una instalación

En la ventana siguiente, selecciona la opción, continuar.

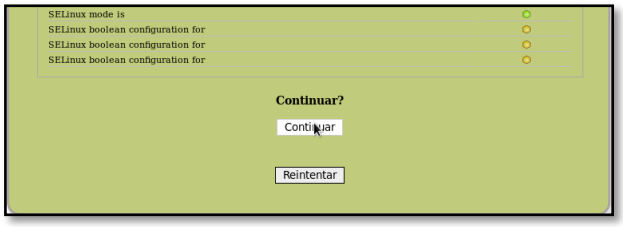


Figura B. 45 Continuar con la instalación y configuración GLPI

Configuración de la conexión a la base de datos.

Figura B. 46 Configuración de la conexión a la base de datos

Selección de la base de datos, ocsweb.

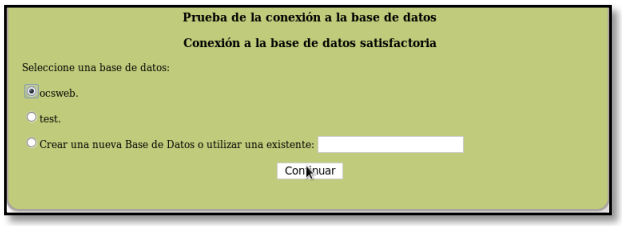


Figura B. 47 Selección de la base de datos

Inicialización de la base de datos.

Figura B. 48 Inicializar la base de datos

Señal de culminación de la instalación y usar GLPI.

Figura B. 49 Finalización de la instalación GLPI

Para ingresar a la aplicación GLPI ingresamos con la dirección web: localhost/glpi, las modificaciones generales en el modo gráfico de GLPI, empieza en la opción configuración/general.

Figura B. 50 Configuración GLPI

Activamos el modo OCSNG, que sirve para asociar OCS-Inventory con GLPI

Figura B. 51 Activar el modo OCSNG

Configuramos el servidor GLPI para que se asocie con la base de datos de OCS-Inventory, agregamos los campos como nombre, nombre de la BDD, usuario de la BDD, y damos click en el botón actualizar.

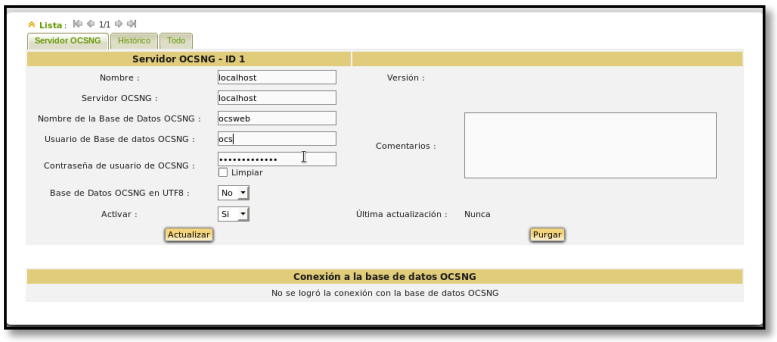


Figura B. 52 Configuración del servidor GLPI

A continuación las opciones importación, en los dispositivos, monitores, impresoras, software, será escogida la opción importación única.

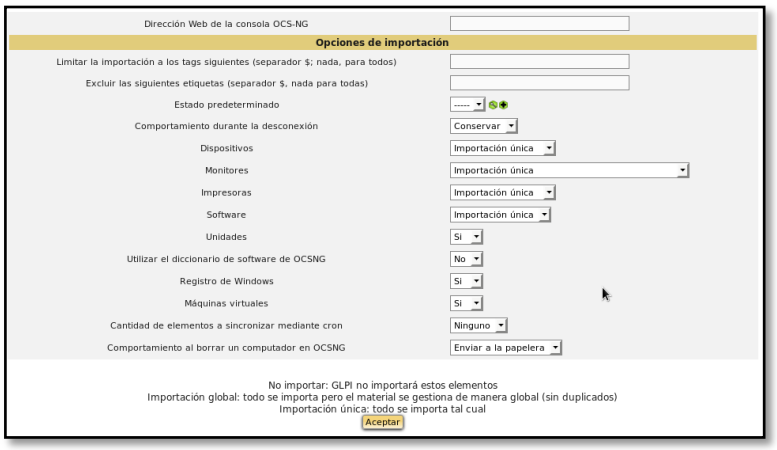


Figura B. 53 Configuración de opciones de importación

Para realizar la importación de dispositivos, ingresamos al menú Útiles y escogemos la opción Importación de computadores nuevos

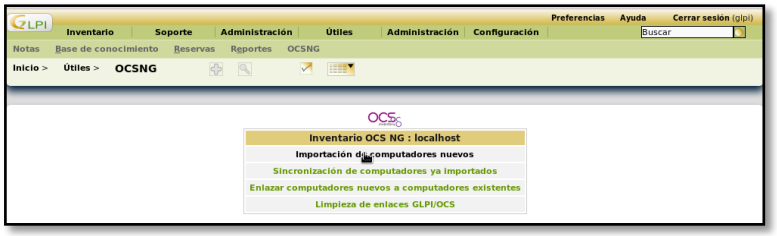


Figura B. 54 Importación de nuevos dispositivos

El proceso se inicia y tendremos una ventana como la siguiente.

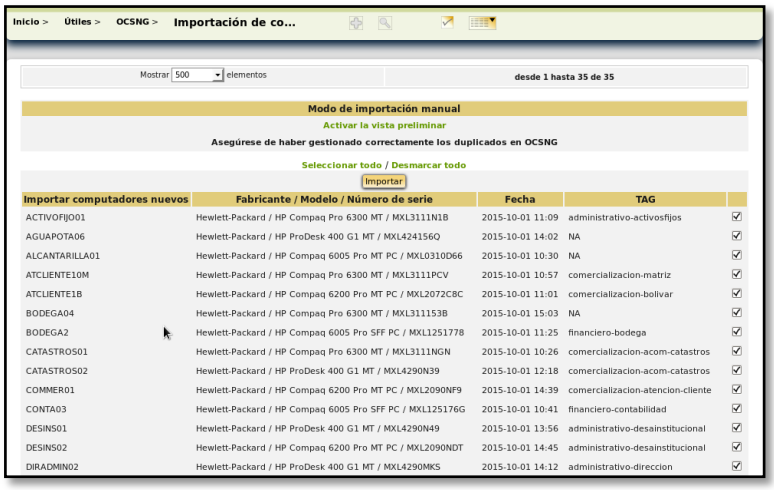


Figura B. 55 Importación en proceso.

B.3. Instalación y configuración CACTI

Descargar el repositorio EPEL que permite la instalación de paquetes no oficiales en CENTOS y los cuales son necesarios por el software Cacti, ingresando el siguiente comando:

#wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm

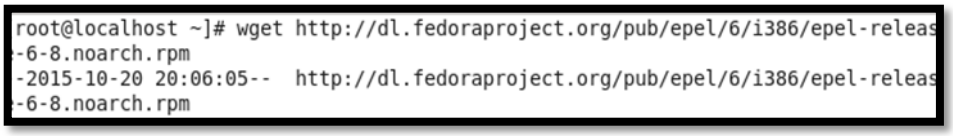


Figura B. 56 Descargando el repositorio EPEL

Una vez descargado el repositorio EPEL, instalar el sistema de gestión de paquetes rpm.

rpm -ivh epel-release-6-8.noarch.rpm

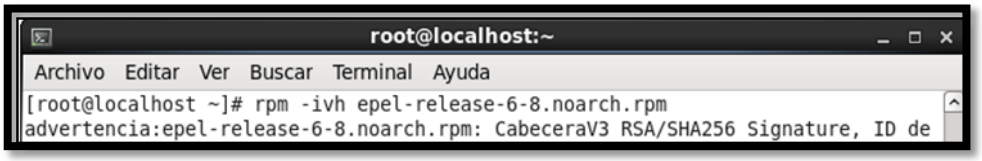


Figura B. 57 Instalando el sistema de gestión de paquetes que no son oficiales de Centos.

A continuación instalar Apache el cual permitirá visualizar las gráficas creadas en la red.

yum install httpd httpd-devel –y

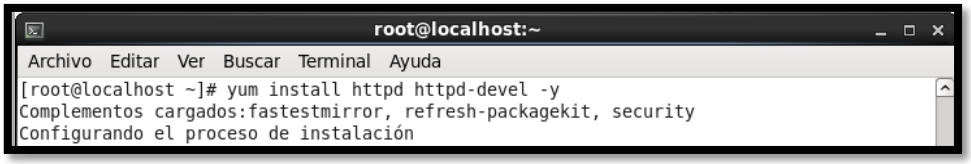


Figura B. 58 Instalación de Apache HTTP

Instalar el paquete de la base de datos MYSQL en la cual se alojarán todos datos del software Cacti.

yum install mysql mysql-server –y

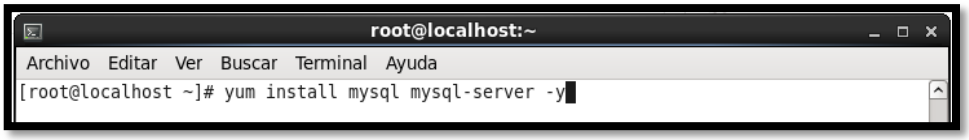


Figura B. 59 Instalación de la base de Datos MYSQL

Después instalar el módulo PHP utilizando el siguiente comando:

yum install php-mysql php-pear php-common php-gd php-devel php php-mbstring php-cli php-mysql –y

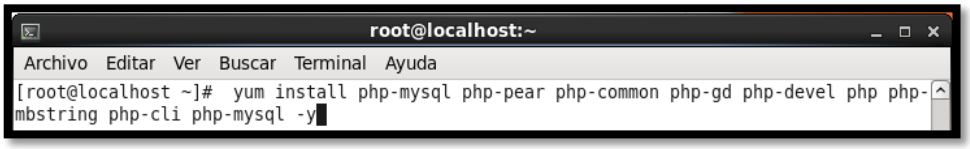


Figura B. 60 Instalación de PHP para la visualización de las gráficas de la red.

Instalar la extensión SNMP para permitir el acceso a los datos y diagnóstico de problemas que se pueden originar en la red.

yum install php-snmp –y

Figura B. 61 Instalación de la extensión PHP SNMP

A continuación se debe instalar los complementos de snmp para administración y gestión de la red.

yum install net-snmp-utils net-snmp-libs php-pear-Net-SMTP –y

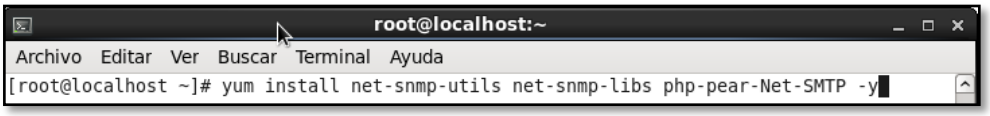


Figura B. 62 Instalación de complementos SNMP**.**

También es necesario instalar la herramienta RRDtool, la cual permite obtener y recuperar datos como el espacio en el disco, el ancho de banda, las interfaces en estado up y down, etc.

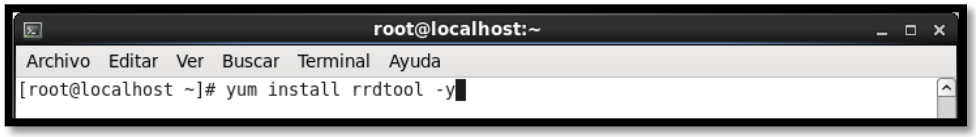


Figura B. 63 Instalación de la herramienta RRDTool.

Una vez instalados todos estos paquetes adicionales es necesario iniciarlos tanto el servicio httpd, mysqld como el snmpd respectivamente. Iniciar el paquete httpd, y comprobar que el reporte esté en OK.

/etc/init.d/httpd start

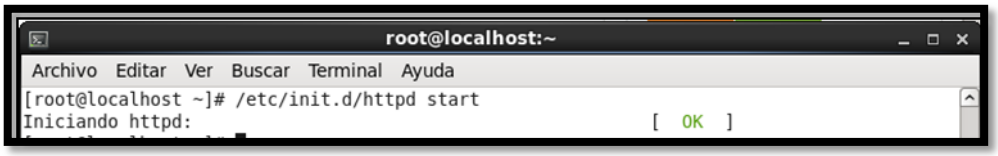


Figura B. 64 Iniciando el servicio httpd

Iniciar el paquete mysqld, y comprobar que el servicio esté en OK.

/etc/init.d/mysqld start

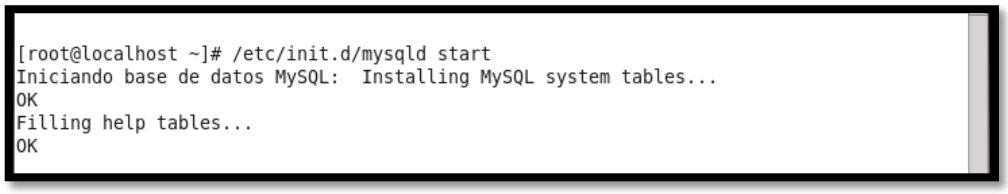


Figura B. 65 Iniciando el servicio mysqld

Iniciar el paquete snmpd, y comprobar que el reporte esté en OK.

/etc/init.d/snmpd start

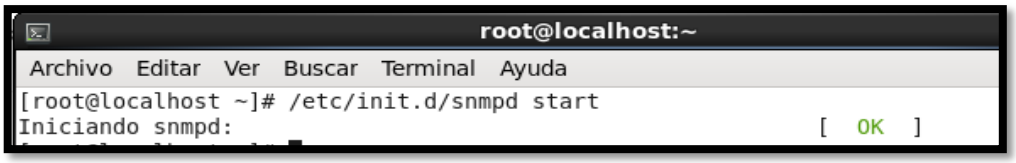


Figura B. 66 Iniciando el servicio snmpd

Para iniciar cada uno automáticamente cada vez que reiniciamos nuestra PC debemos ingresar los siguientes comandos:

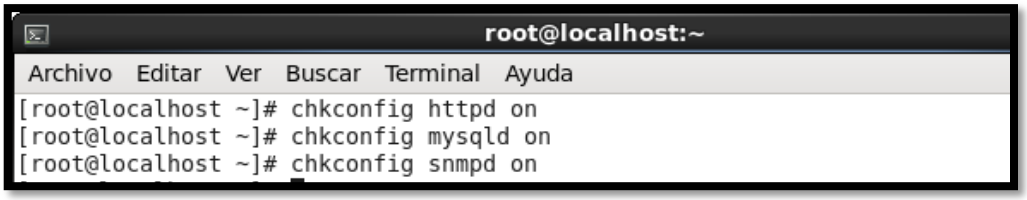


Figura B. 67 Iniciar servicios automáticamente.

Una vez realizados todos los pasos anteriores se puede proceder a instalar el software Cacti , usando el comando:

#yum install cacti –y

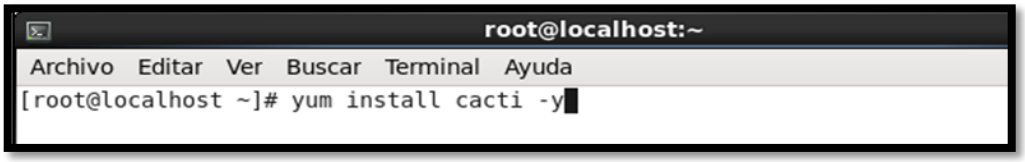


Figura B. 68 Instalación del software Cacti

Luego debemos crear una base de datos para el programa Cacti, en este caso debemos agregar un nombre a la base de datos, una contraseña y darle los privilegios para poder acceder a ella.

Iniciar la base como root y a continuación escribir la contraseña del administrador.

#mysql -u root –p

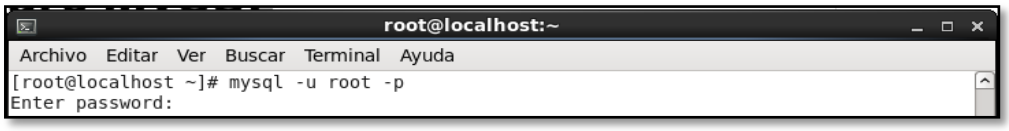


Figura B. 69 Iniciar sesión como root en la Base de datos

Ingresamos los siguientes comandos para crear la base de datos del cacti, asignarle una contraseña y darle los privilegios:

- create database cacti;
- GRANT ALL ON cacti.* TO cacti@localhost IDENTIFIED BY '***contraseña***';
- flush privileges;

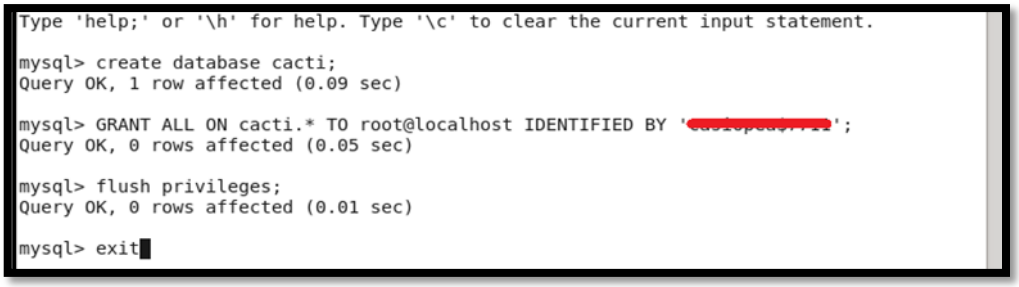


Figura B. 70 Creación de la base de datos que utilizará Cacti

Determinar la ubicación del archivo cacti.sql a través del gestor de paquetes rpm.

#rpm -ql cacti | grep cacti.sql

/usr/share/doc/cacti-0.8.8b/cacti.sql

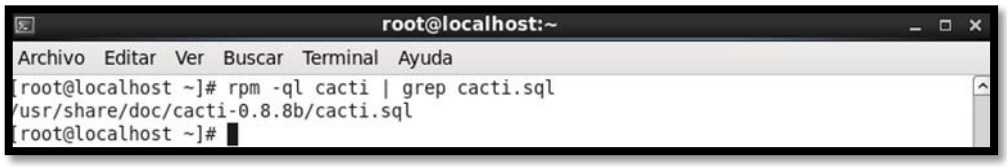


Figura B. 71 Ubicación del archivo de acceso a la base de datos del Cacti en los ficheros

Una vez encontrada la ubicación del archivo cacti.sql se debe importarlo a la base de datos del Cacti que se creó anteriormente, en este caso está en la ubicación:

#mysql -u cacti -p cacti < /usr/share/doc/cacti-0.8.8b/cacti.sql

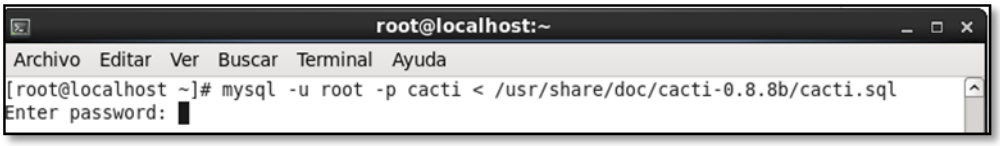


Figura B. 72 Importación de archivos a la base de datos del Cacti

Después debemos dirigirnos a la siguiente ubicación usando el siguiente comando.
#gedit /etc/cacti/db.php

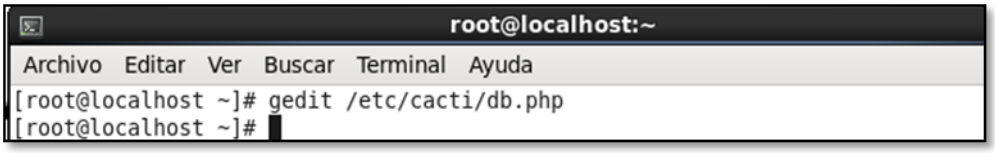


Figura B. 73 Editando la base de datos del programa Cacti

Nos aparecerá la siguiente ventana en la cual debemos actualizar los datos de la base de datos del Cacti:

- El nombre de la base de datos del Cacti.
- El usuario de la base de datos del Cacti
- La contraseña de la base de datos del Cacti

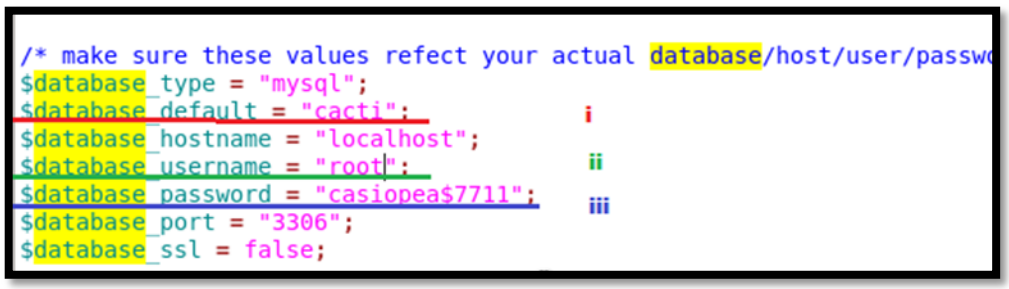


Figura B. 74 Actualización de la base de datos de Cacti

Para añadir la dirección ip del servidor a la cual apuntaremos para acceder al programa Cacti, se debe editar el siguiente archivo:

#gedit /etc/httpd/conf.d/cacti/cacti.conf

A continuación nos mostrará el siguiente archivo e ingresamos la dirección IP definida o un rango de direcciones.

El rango de red es de ejemplo para guardar datos de confidencialidad.

```
<Directory /usr/share/cacti/>
        <IfModule mod_authz_core.c>
                # httpd 2.4
                Require host localhost
        </IfModule>
        <IfModule !mod_authz_core.c>
                # httpd 2.2
                Order deny,allow
                Deny from all
                Allow from 192.168.1.0/24
        </IfModule>
</Directory>
```

Figura B. 75 Asignación de una dirección IP para acceder a Cacti

Se debe reiniciar el servidor apache para para verificar que los cambios se efectuaron correctamente.

/etc/init.d/httpd restart

```
[root@localhost ~]# /etc/init.d/httpd restart
Parando httpd:                                             [  OK  ]
Iniciando httpd:                                           [  OK  ]
```

Figura B. 76 Reiniciando el servidor Apache

Antes de ingresar al Cacti se debe editar el archivo de cron, el cual permite recibir una actualización de los datos de los hosts que se encuentren configurados en el Cacti.

gedit /etc/cron.d/cacti

Figura B. 77 Editando el archivo de cron para obtener datos de hosts automáticamente.

Se debe descomentar la siguiente línea en el archivo cron.d (quitar este símbolo #)

*/5 * * * * cacti /usr/bin/php /usr/share/cacti/poller.php > /dev/null 2>&1

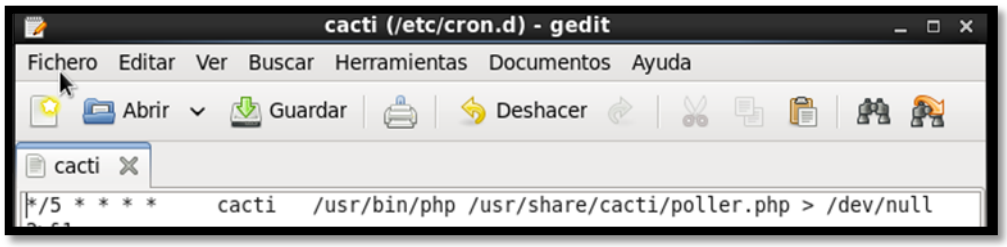


Figura B. 78 Permitiendo actualización de datos en Cacti

Ingresamos con la dirección: localhost/cacti en nuestro navegador web de preferencia y aparecerá la siguiente ventana de instalación.

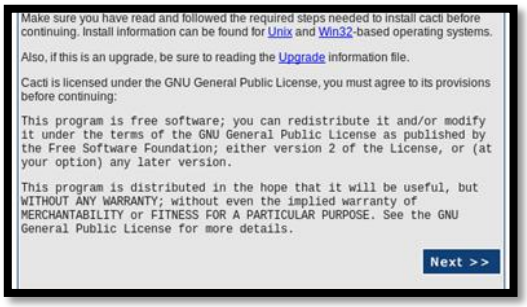


Figura B. 79 Accediendo a la instalación de Cacti a través de la Web

A continuación dar click en Siguiente para continuar con la instalación del programa Cacti.

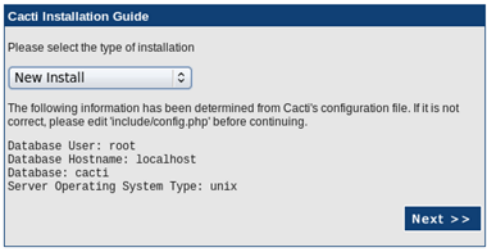


Figura B. 80 Proceso de instalación del software Cacti

Después aparece la siguiente ventana con toda la información válida del programa y para terminar el proceso dar click en Finalizar

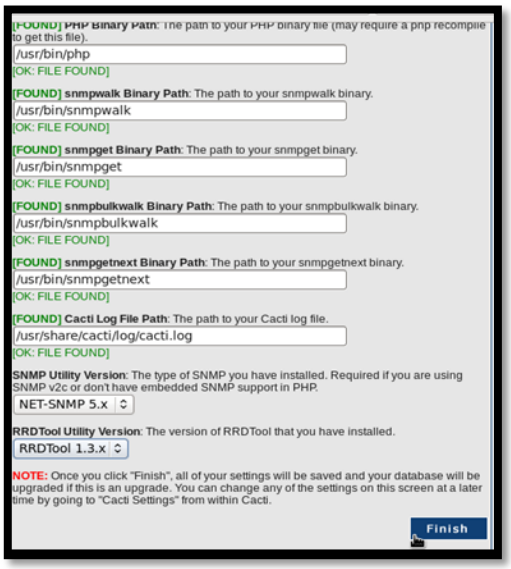


Figura B. 81 Finalización del proceso de instalación de Cacti

Una vez culminada toda la instalación iniciamos la sesión de Cacti ingresando el usuario y la contraseña en este caso ambas por defecto son admin.

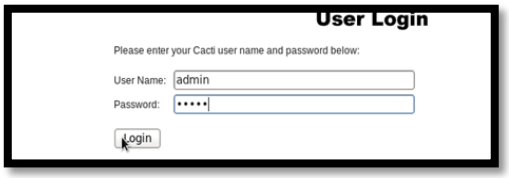


Figura B. 82 Iniciando sesión de Cacti como Administrador

Inmediatamente se puede visualizar la página principal de Cacti y a continuación seleccionar la pestaña Consola, escogemos en la opción de Utilities la pestaña User Management.

Se recomienda eliminar las cuentas que vienen instaladas por defecto y dejar únicamente la cuenta que va a acceder el administrador de la red.

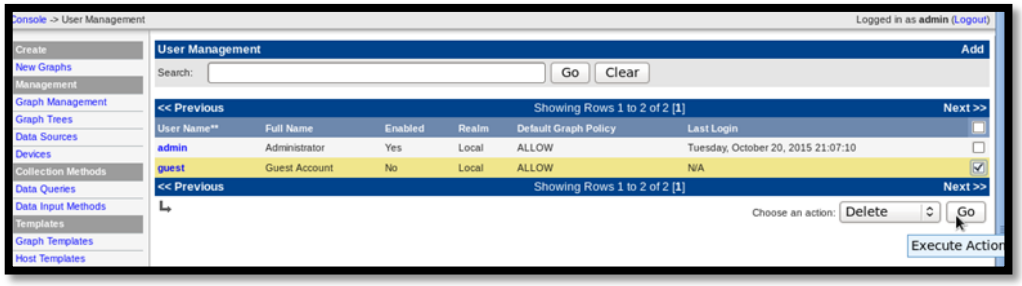


Figura B. 83 Agregación y eliminación de cuentas instaladas por defecto

Para observar el estado de los dispositivos, seleccionar la pestaña Management y escogemos la opción Devices. En este caso el único dispositivo agregado es el servidor local.

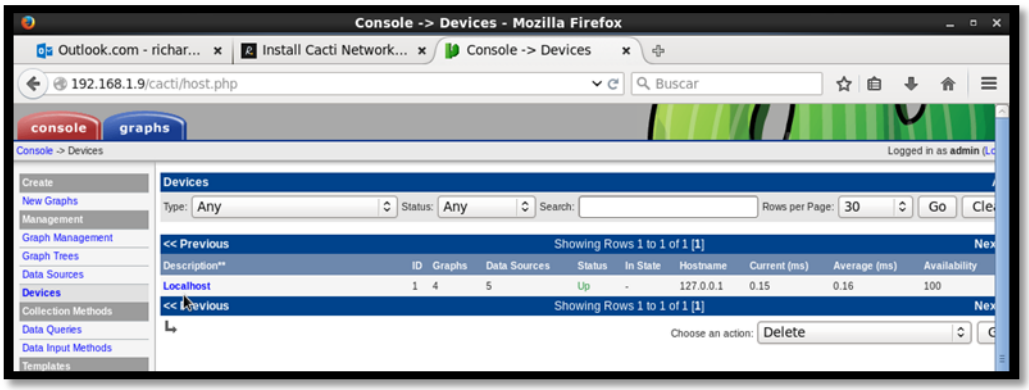


Figura B. 84 Estado del dispositivo localhost

En la pestaña Graphs podemos visualizar las gráficas de los datos del servidor local. Y además si configuramos SNMP se puede monitorear los dispositivos que tenga SNMP habilitado.

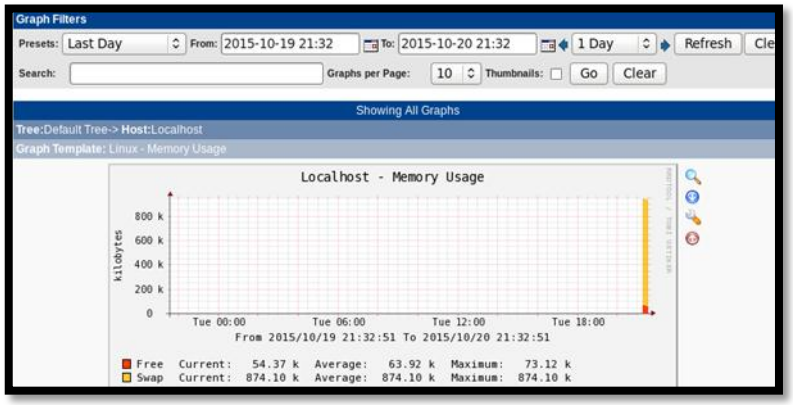


Figura B. 85 Gráfica de la memoria usada en el servidor local

B.4. Instalación y configuración de los requisitos para la instalación de Net-SNMP en Windows

- Como requisito previo se necesita instalar Visual C++ 2008, en caso que se desee usar net snmp con SNMPv3.

Descargar el link de instalación de la siguiente página: http://www.microsoft.com/en-us/download/details.aspx?id=15336, Visual C++ 2008 redistributable installation.

Una vez que se abra el link, proceder a hacer clic en el botón download.

Figura B. 86 Ventana con link de descarga de Visual C++ 2008

Una vez completada la descarga, ir al lugar de ubicación y doble clic en vcredist_x64.exe, y se iniciará la instalación, cuando se complete la instalación clic en el botón finish.

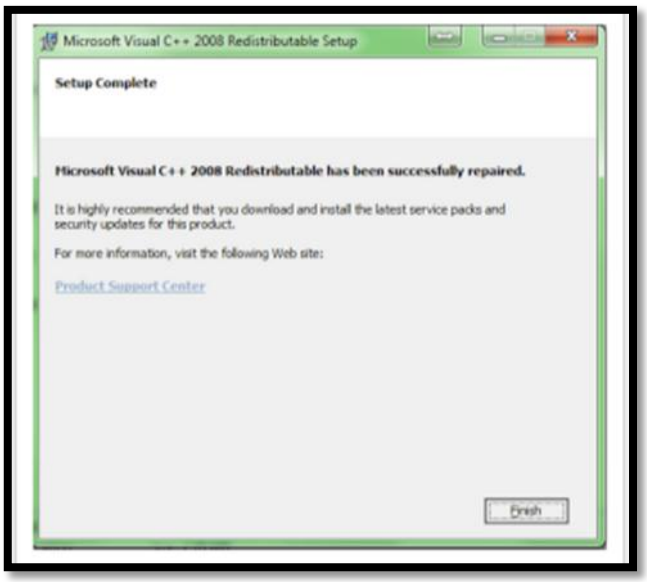


Figura B. 87 Iniciar la instalación del programa.

- Como segundo requerimiento necesitamos la aplicación Win64 OpenSSL v0.9.8zf, si desea utilizar la funcionalidad de SNMPv3 con el servicio net-snmp necesitará abrir SSL para los estándares de criptografía. Solamente 0.9.8.zf es la versión apoyada por net-snmp.

- Descargar el link de instalación de la siguiente página: https://slproweb.com/products/Win32OpenSSL.html, win64 openssl

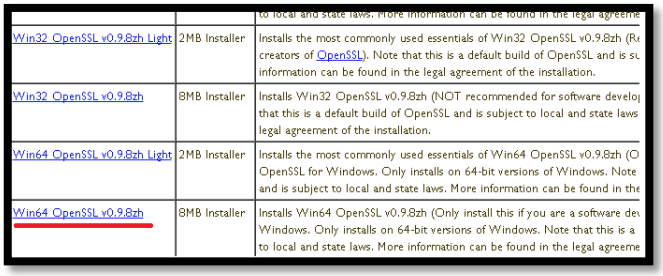


Figura B. 88 El enlace de descarga para OpenSSL

Una vez descargado el archivo se hace doble clic en el archivo descargado y comienza la instalación

Figura B. 89 Instalación de Open v0.9.8zf SSL.

Continuamos con el proceso de instalación, en la mayoría damos siguiente para continuar con la instalación, en la ventana de adicionar tareas, damos click en: The Windows system directory

Figura B. 90 Seleccionamos Windows system directory.

Luego comienza el proceso de instalación y por ultimo damos click en el botón finalizar.

Figura B. 91 Proceso de instalación finalizado

- Como tercer requerimiento instalamos el agente net-snmp-5.5.0.2.x64, cuando inicie la instalación de net-snmp, seleccione encryption support, de lo contrario SNMPv3 no funcionará.

- Link de descarga: http://sourceforge.net/projects/net-snmp/files/net-snmp%20binaries/5.5-binaries/net-snmp-5.5.0-2.x64.exe/download

  Cada vez se van actualizando las versiones de net-snmp por lo que se debería revisar cual es la versión más reciente.

Figura B. 92 Proceso de instalación de net-snmp

Aceptamos los términos y condiciones y damos click en siguiente

Figura B. 93 Aceptar términos y condiciones

Luego damos click en continuar y en la pantalla siguiente damos click en las opciones de encriptación que se encuentran por defecto sin marcar.

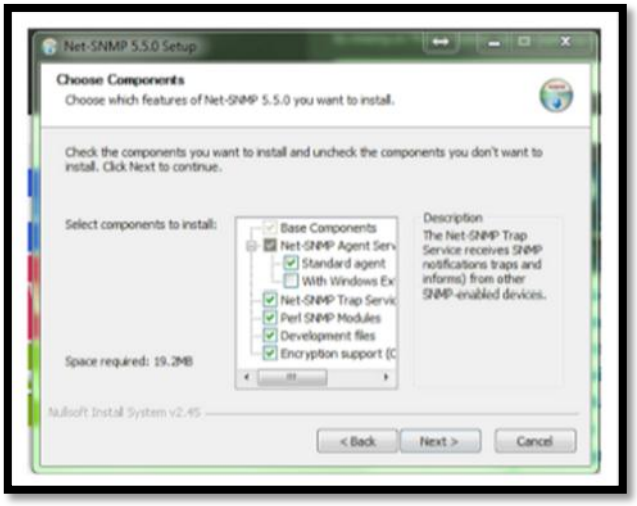


Figura B. 94 Seleccionar las opciones de encriptación

Las demás opciones damos click en siguiente hasta que nos aparezca el botón de finalizar

Figura B. 95 Finalizamos la instalación de net-snmp

- Como cuarto y último requerimiento instalamos Active Perl, que se lo necesitará para configurar net-snmp desde la línea de comandos.

- Link de descarga: http://www.activestate.com/activeperl, active perl.

Figura B. 96 Descargamos la versión que necesitemos

Iniciamos la instalación

Figura B. 97 Inicio de instalación de ActivePerl

Aceptamos los términos y condiciones de uso

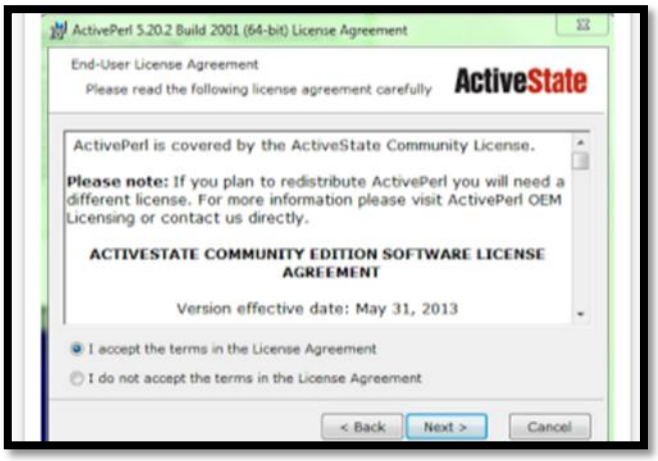


Figura B. 98 Aceptamos los términos y condiciones

En las demás ventanas dejamos las opciones que vienen por defecto y damos click en continuar.

Figura B. 99 Dejamos las opciones que vienen por defecto

Finalmente damos click en el botón finish, terminando con la instalación de requisitos necesarios para configurar para SNMPv3 en un computador con plataforma Windows.

Figura B. 100 Fin de la instalación

B.5. Instalación y configuración ZABBIX

Primeramente se debe instalar ciertos servicios que son necesarios por el software Zabbix, en este caso para instalar la extensión PHP, ingresar el siguiente comando:

yum install php php-cli php-common php-devel php-pear php-gd php-mbstring php-mysql php-xml

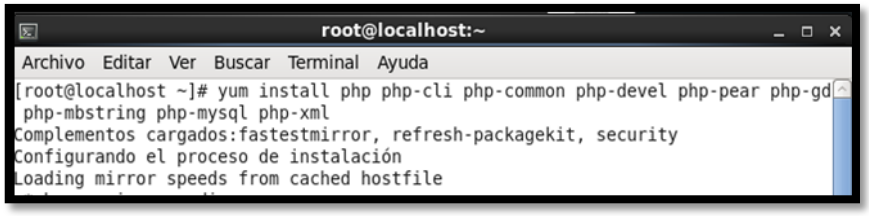


Figura B. 101 Instalando la extensión PHP a su versión más reciente

A continuación instalar la extensión SSH2 PHP con todas sus dependencias disponibles.

yum install gcc php-devel php-pear libssh2 libssh2-devel

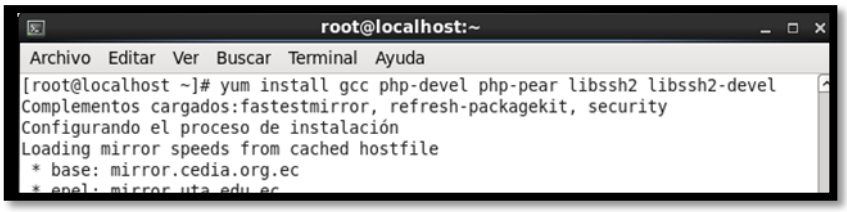


Figura B. 102 Instalando la extensión SSH2 para el paquete PHP

También es necesario instalar la dependencia pecl, la cual nos permitirá construir la extensión SSH2 de PHP.

pecl install –f ssh2

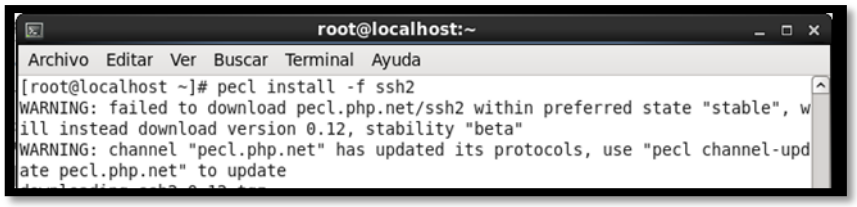


Figura B. 103 Instalando la dependencia pecl del paquete PHP ssh2

Después para instalar la herramienta IPMI en Centos, la cual añade la característica de acceso remoto al servidor, se debe ingresar el siguiente comando.

yum install OpenIPMI OpenIPMI-tools

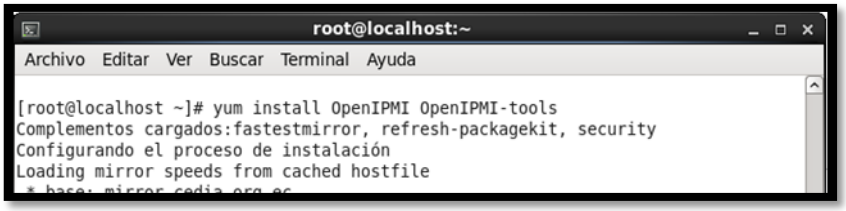


Figura B. 104 Instalando e iniciando la herramienta IPMI en Centos

Una vez instalados los anteriores servicios se debe configurar la zona zabbix del repositorio rpm en el sistema, con el siguiente comando:

#rpm -Uvh http://repo.zabbix.com/zabbix/2.2/rhel/6/x86_64/zabbix-release-2.2-1.el6.noarch.rpm

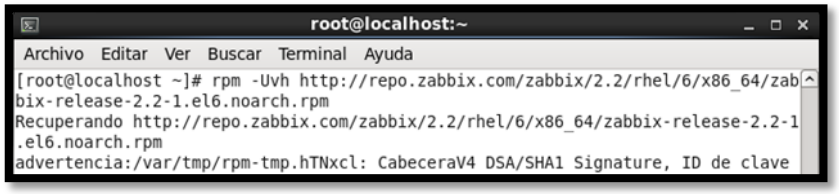


Figura B. 105 Configurando el repositorio rpm de Zabbix

Instalar el paquete de la base de datos MYSQL en la cual se alojarán todos datos del servidor Zabbix.

yum install zabbix-server-mysql zabbix-web-mysql zabbix-agent zabbix-java-gateway

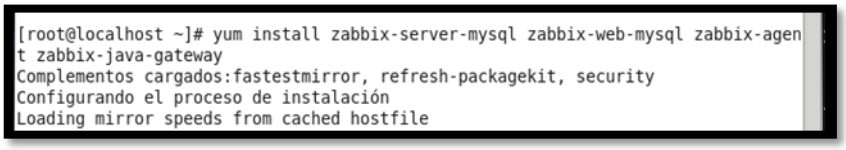


Figura B. 106 Instalando la base de datos MYSQL

Es necesario cambiar la zona horaria del servidor apache para esto, para esto se debe editar el archivo zabbix.conf que se encuentra en el fichero /etc/httpd/conf.d

#gedit /etc/httpd/conf.d/zabbix.conf

Específicamente se debe descomentar la línea: php_value date.timezone America/Guayaquil y agregar la zona horaria de nuestra localidad.

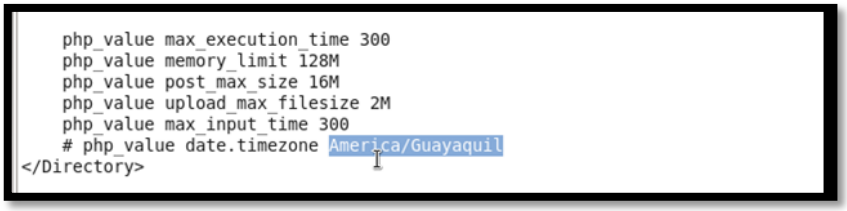


Figura B. 107 Configurando zona horaria del servidor apache en Zabbix.conf

Se debe reiniciar el servidor apache para verificar que los cambios se efectuaron correctamente.

/etc/init.d/httpd restart

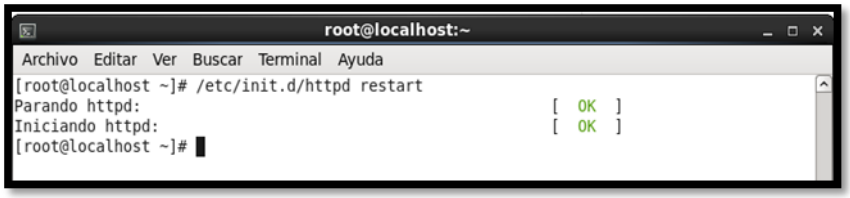


Figura B. 108 Reiniciando el servidor Apache

Luego se debe crear una base de datos para el programa Zabbix, en este caso debemos agregar un nombre a la base de datos, una contraseña y darle los privilegios para poder acceder a ella.

- Iniciar la base como root y a continuación escribir la contraseña del administrador.

#mysql -u root –p

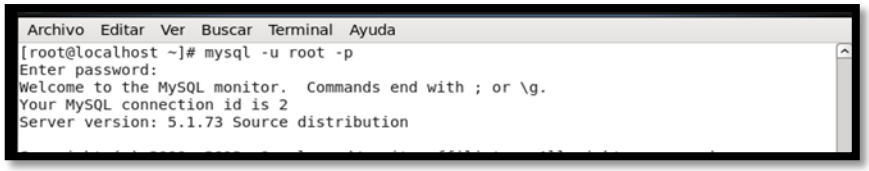


Figura B. 109 Iniciando sesión como root en la base de datos Mysql

Ingresar los siguientes comandos para crear la base de datos de Zabbix:

- create DATABASE zabbix CHARACTER SET UTF8;
- GRANT ALL PRIVILEGES on zabbix.* to 'zabbix'@'localhost' IDENTIFIED BY 'contraseña';

- flush privileges;
- quit

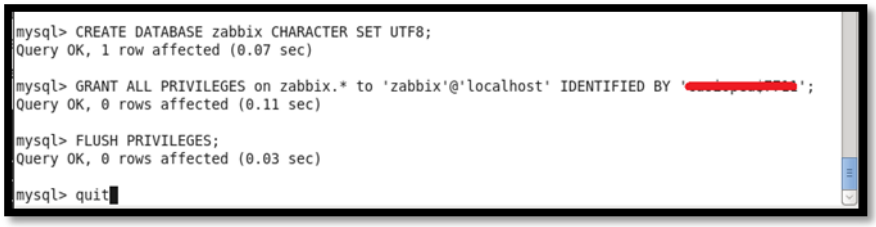


Figura B. 110 Creando la base de datos que utilizará Zabbix

Una vez creada la base de datos para Zabbix es necesario restaurar la base de datos mysql predeterminada, cuyos archivos se encuentran en los siguientes directorios:

mysql -u zabbix -p zabbix < /usr/share/doc/zabbix-server-mysql-2.2.10/schema.sql

mysql -u zabbix -p zabbix < /usr/share/doc/zabbix-server-mysql-2.2.10/create/images.sql

mysql -u zabbix -p zabbix < /usr/share/doc/zabbix-server-mysql-2.2.10/create/data.sql

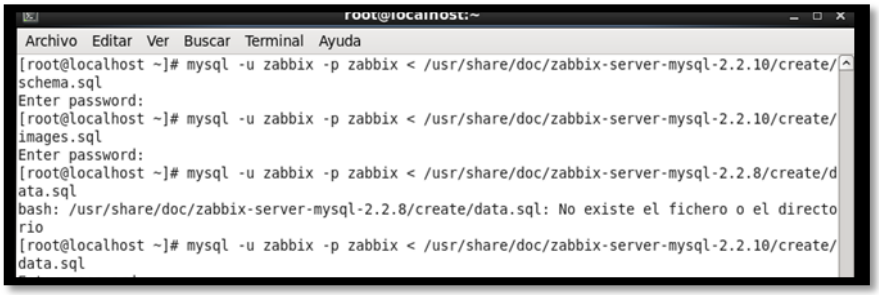


Figura B. 111 Restaurando los archivos de zabbix en la base de datos preestablecida

Agregar una dirección IP para el servidor de Zabbix en el fichero de configuración que se encuentra en la siguiente ubicación: #gedit /etc/zabbix/zabbix_server.conf

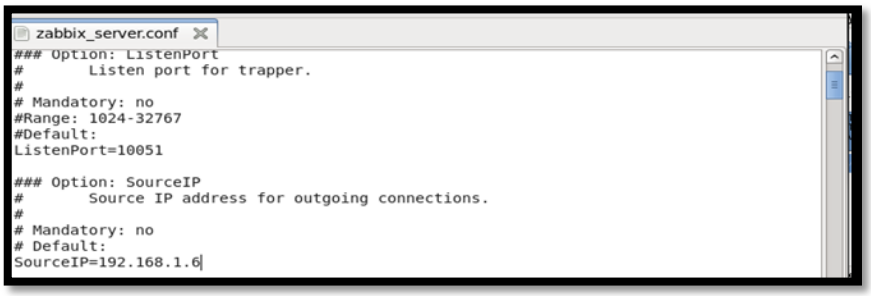


Figura B. 112 Agregamos la dirección IP del servidor

Iniciar el servidor Zabbix, y comprobar que el reporte esté en OK.

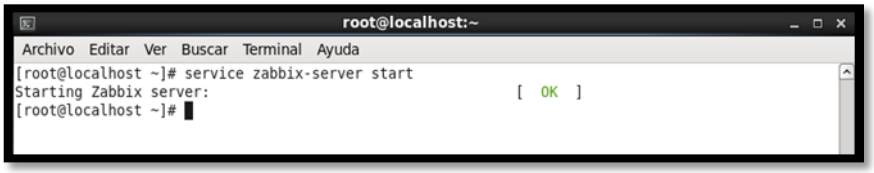


Figura B. 113 Iniciando el servidor Zabbix en el sistema

A continuación para continuar con el instalador Web de Zabbix, se debe ingresar la dirección: localhost/zabbix en nuestro navegador web de preferencia y aparecerá la siguiente ventana de instalación y en la cual damos click en Siguiente.

Figura B. 114 Accediendo al instalador Web de Zabbix

Verificar que todos los paquetes requeridos estén instalados correctamente, dar click

Figura B. 115 Chequeo de pre-requisitos del servidor Zabbix

Configurar la base de datos con los datos del servidor y del usuario de la base de datos que ingresamos cuando creamos la base de datos mysql y damos click en Testear la conexión y si todo esta correcto click en Siguiente.

Figura B. 116 Verificación de la base de datos de Zabbix

En el siguiente paso se necesita configurar el nombre, el puerto y la dirección del servidor de Zabbix, si no se realiza ningún cambio dar click en Siguiente.

Figura B. 117 Asignando el nombre y puerto al servidor Zabbix

Se desplegará una ventana con todos los parámetros que se ha configurado si todos son válidos dar click en Siguiente.

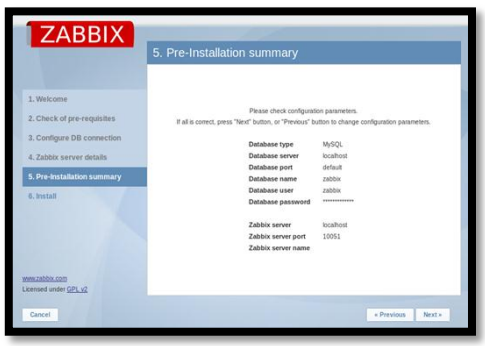


Figura B. 118 Verificación de datos antes de instalar el servidor Zabbix Web

Cumplidos todos los requisitos de instalación y para culminar dicho proceso, dar en click en el botón Finalizar.

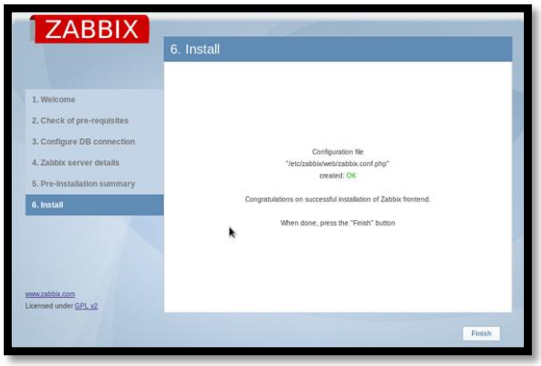


Figura B. 119 Finalización del proceso de instalación de Zabbix

Una vez culminada toda la instalación iniciamos la sesión de Zabbix ingresando el usuario y la contraseña en este caso el usuario es admin y la contraseña es zabbix.

Figura B. 120 Iniciando sesión en el servidor de Zabbix

Iniciada la sesión en el servidor, aparece el siguiente aviso de que el servidor de Zabbix no está corriendo, para lo cual ser debe realizar las siguientes modificaciones que se detallarán a continuación.

Figura B. 121 Mensaje que avisa que el servidor Zabbix no está corriendo

22. Se debe comprobar que el selinux este en modo prevención para esto ejecutar el siguiente comando: #tail -f /var/log/audit/audit.log |grep -i av

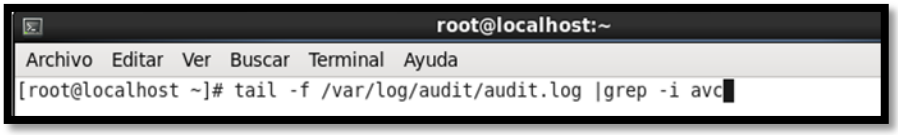


Figura B. 122 Verificación de la conexión httpd

Como se puede observar se despliega una lista de denegación de acceso, por lo que es necesario crear una política para tener privilegios de acceso.

Figura B. 123 Listado de denegación de acceso

Luego el atributo que debemos verificar que este en estado de off es la conexión network.

#getsebool httpd_can_network_connect

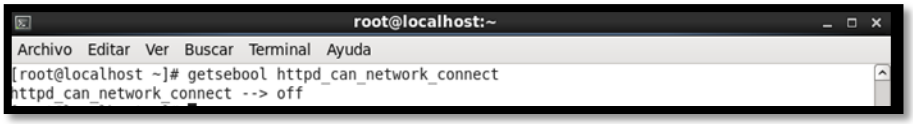


Figura B. 124 Conexión Network en estado off

Para cambiar el estado a on de la conexión network, ejecutar los siguientes comandos.

#setsebool -P httpd_can_network_connect on

#getsebool httpd_can_network_connect

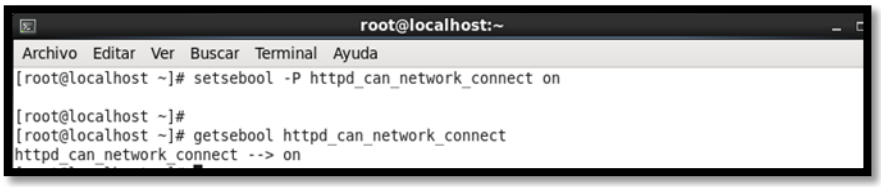


Figura B. 125 Habilitando la conexión Network

También es necesario verificar los datos en el archivo zabbix_server.conf, para editarlo ingresar a la ubicación /etc/zabbix

#gedit /etc/zabbix/zabbix_server.conf

En este archivo debemos verificar que la línea del nombre de usuario de zabbix este descomentada así como la línea en la que debemos ingresar la contraseña de la base de datos de zabbix que se ingresó en pasos anteriores

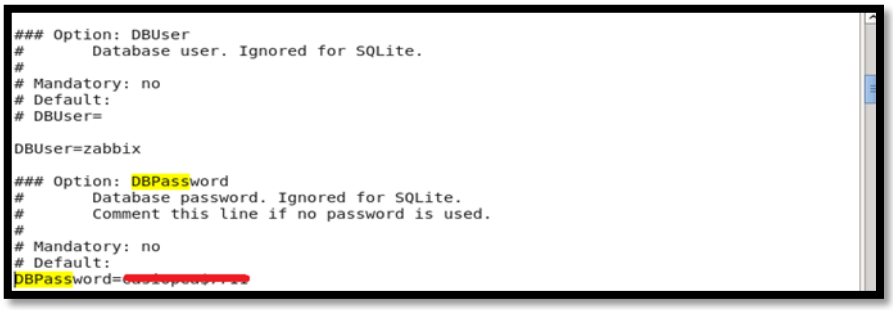


Figura B. 126 Verificación de datos en el archivo de configuración del servidor Zabbix

Ya con los datos actualizados en el fichero de la base de datos se puede verificar que ya se tiene acceso al fichero del servidor de zabbix, que se encuentra ubicado en:

#getdit /var/zabbix/zabbix_server.log

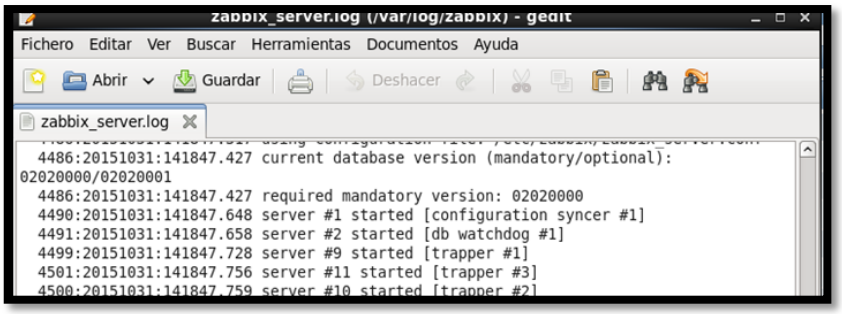


Figura B. 127 Fichero del servidor Zabbix con acceso

Al iniciar nuevamente la sesión se observa que el servidor de Zabbix ya no tiene el error y sale un aviso de que se ejecutando correctamente.

Figura B. 128 Servidor iniciado y ejecutándose correctamente

Para iniciar automáticamente el Servidor de Zabbix cada vez que se reinicie la PC se debe ingresar la siguiente línea en el terminal:

#chkconfig zabbix-server on

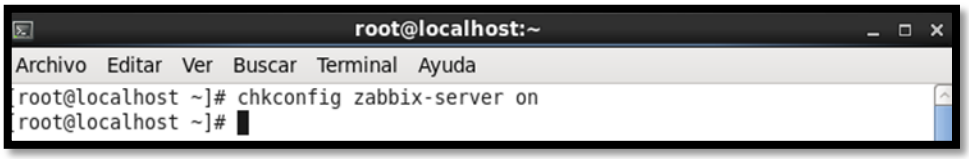


Figura B. 129 Configurando para que Zabbix se inicie automáticamente con el sistema

2.2.5.1 Instalación y configuración de POSTFIX

Para recibir alertas y avisos al correo electrónico es necesario instalar un servidor de correo en este caso se asociará Postfix con Zabbix de la siguiente manera:

Instalar el paquete de postfix (este paquete en la mayoría de los casos ya se instala a la versión más reciente cuando se ejecuta el comando yum update), en caso de ya tenerlo instalado omitir este paso.

#yum install postfix

A continuación se debe proceder a configurar el fichero de postfix, en el cual se debe añadir las siguientes líneas en el caso de asociar postfix con un servidor de correo en gmail:

#gedit /etc/postfix/main.cf

- smtp_sasl_security_options = noanonymous
- relayhost = [smtp.gmail.com]:587
- smtp_use_tls = yes
- #smtp_tls_CAfile = /etc/postfix/cacert.pem
- smtp_sasl_auth_enable = yes
- smtp_sasl_password_maps = hash:/etc/postfix/googleapps/password

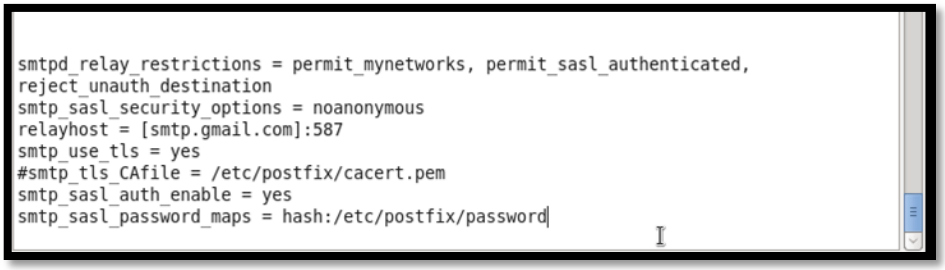


Figura B. 130 Configurando el fichero de Postfix

Además es necesario agregar la cuenta de correo electrónico a la cual se quiere que lleguen los avisos en este caso se agrega una cuenta gmail y la contraseña en el siguiente fichero.

gedit /etc/postfix/password

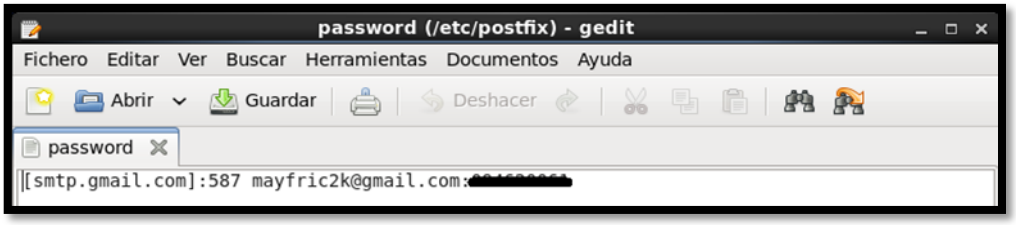


Figura B. 131 Agregando una cuenta de correo electrónico con su contraseña.

También es necesario asegurarse de que postfix tenga permisos de ejecución agregando el siguiente comando:

#sudo chown postfix /etc/postfix

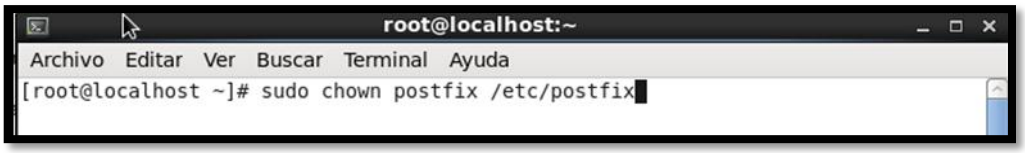


Figura B. 132 Agregando permisos de ejecución a postfix

Es necesario asociar tanto el correo como la contraseña al fichero de postfix.

sudo postmap /etc/postfix/password

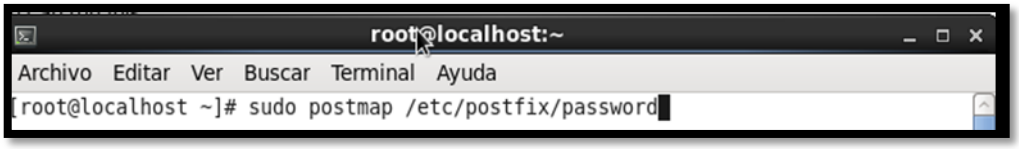


Figura B. 133 Asociando la cuenta del correo electrónico al fichero de postfix

Realizar una prueba de envió de correo electrónico para verificar que el correo llegó a sus destinatario correctamente.

#echo “Prueba” | mail –s “Prueba postfix” correo del destinatario

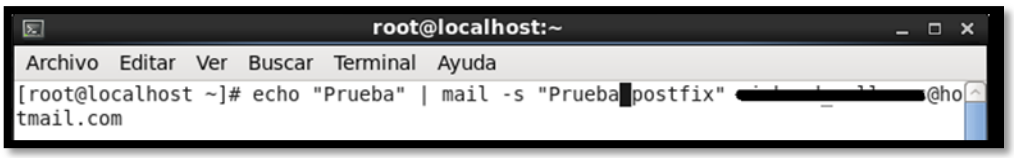


Figura B. 134 Enviando un correo de prueba desde el terminal

Para iniciar automáticamente el servidor de correo postfix cada vez que se reinicie el sistema, agregar esta línea en el terminal.

#chkconfig postfix on

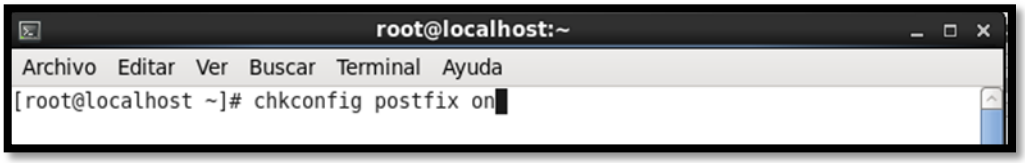


Figura B. 135 Agregando permisos para que postfix se inicie automáticamente

Luego configurar el correo desde el cual se va a enviar las notificaciones y alertas que generen los dispositivos, seleccionando la pestaña Administración y la opción de Tipos de medios. Una vez llenados todos los campos dar click en Guardar.

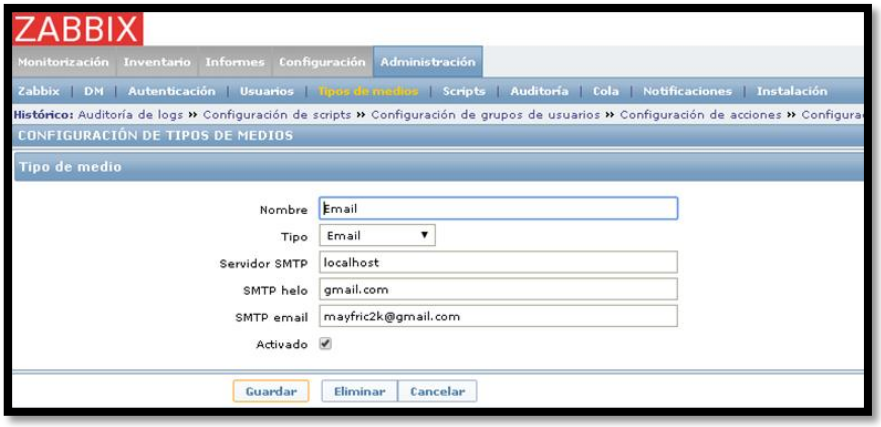


Figura B. 136 Configurando correo origen en el servidor de Zabbix

También se debe configurar el correo al cual va a llegar las notificaciones, seleccionando la pestaña Administración y la opción de Usuarios. Una vez ingresado el correo destino dar click en Guardar.

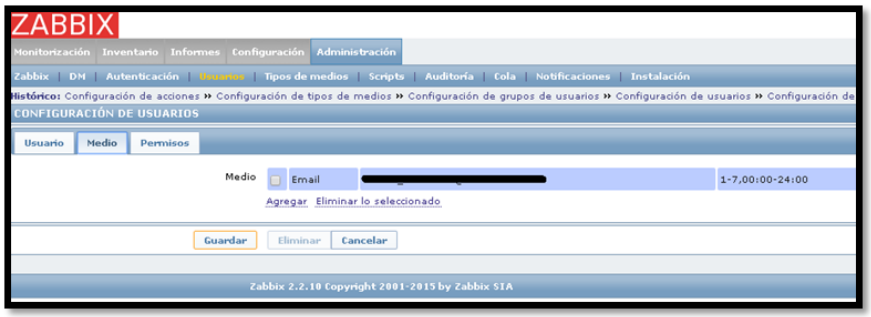


Figura B. 137 Configurando correo destino en el servidor de Zabbix

Verificar que se encuentre activa la acción de envío de correo, cuya opción se encuentra en la pestaña Administración y la opción Acciones.

Figura B. 138 Verificación del estado activo de la opción Envío de correos en el servidor Zabbix

Ahora el administrador de red podrá analizar el estado de todos los dispositivos que se encuentren siendo monitoreados, debido a que si se presenta cualquier tipo de alerta esta llegara automáticamente a la bandeja de correos del administrador.

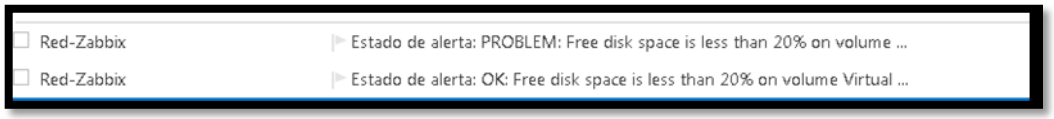


Figura B. 139 Prueba de envió de correo en la cuenta del administrador

El correo contendrá la información de las alertas generadas, las cuales indicarán los valores o umbrales que generó determinado parámetro en el host lo que agiliza un proceso de solución más oportuno para el administrador y técnicos de la red.

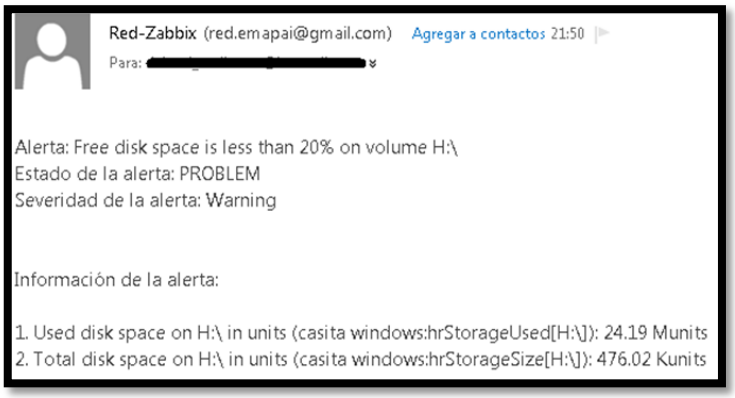


Figura B. 140 Prueba de envió de correo indicando la alarma que se registró en dicho equipo

Por motivos de seguridad en los servidores se habilito el puerto ssh, para que los usuarios ingresen remotamente al equipo de forma segura.

Para instalar el paquete open-ssh utilizamos el siguiente comando:

Figura B. 141 Instalamos el paquete ssh

Una vez instalado procedemos a configurarlo, el fichero donde se encuentran las configuraciones se encuentran en el directorio: /etc/ssh/sshd_config, para abrirlo lo podemos hacer mediante cualquier editor de textos, en este caso lo haremos con “nano”.

```
[root@localhost ~]# nano /etc/ssh/sshd_config
[root@localhost ~]#
```

Figura B. 142 Abrimos el fichero ssh

Al ingresar al fichero tendremos varios textos, en primer lugar descomentaremos el puerto por donde vamos a ingresar remotamente, en este caso es el puerto TCP: 22

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

Port 22
```

Figura B. 143 Descomentamos el puerto tcp 22

Nos aseguramos que utilice la versión 2 de este protocolo ya que por defecto se habilita la versión 1.

```
# installations. In future the default will change to require explicit
# activation of protocol 1
Protocol 2
```

Figura B. 144 Activamos la versión 2 del protocolo ssh

Guardamos los cambios en el editor de textos y finalmente reiniciamos el servicio ssh con el siguiente comando.

```
[root@localhost ~]# service sshd restart
Parando sshd:                                              [  OK  ]
Iniciando sshd:                                            [  OK  ]
[root@localhost ~]#
```

Figura B. 145 Reiniciamos el servicio SSH

Cabe recalcar que estos pasos son básicos para configurar ssh ya que existen más pasos si se desea mejorar la seguridad, una vez realizado estos pasos, realizaremos un ingreso de

prueba por medio de la plataforma Putty al servidor. En esta plataforma debemos ingresar la dirección IP de nuestro servidor, el puerto y especificar el tipo de conexión.

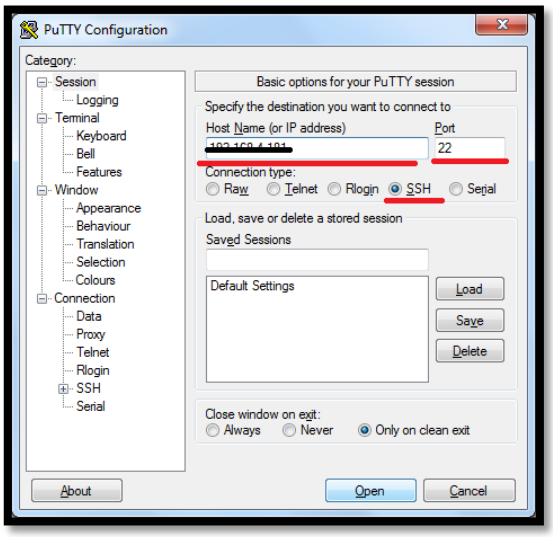


Figura B. 146 Plataforma Putty para ingreso via ssh

Si todo está bien, nos aparecerá una pantalla similar a la siguiente, en la cual nos solicitará el usuario y la contraseña de nuestro servidor.

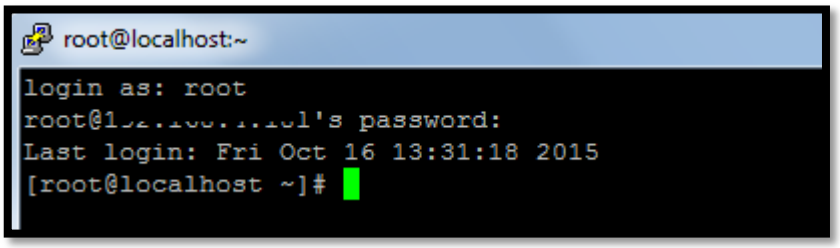


Figura B. 147 Ingreso via ssh en la plataforma Putty

Anexo C: Manuales de usuario de las herramientas instaladas

C.1. MANUAL DE USUARIO OCS-INVENTORY

- **Acceso al Sistema OCS-INVENTORY**

Open Computer and Software Inventory Next Generation (OCS) es un software libre que permite al departamento de recursos informáticos administrar el inventario de sus recursos computacionales. OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de agente OCS. OCS puede utilizarse para visualizar el inventario de la red de datos a través de una interfaz web.

Una vez en la ventana de acceso a OCS-INVENTORY, por defecto se inicia con el lenguaje en Ingles, para poder cambiarlo a español, damos click en la bandera de la parte superior derecha.

Figura C. 1 Cambiar idioma OCS-INVENTORY

Posteriormente nos solicitará un usuario y contraseña para acceder, por defecto el usuario que tiene todos los privilegios viene dado inicialmente por **admin** y la contraseña **admin,** así que ingresaremos al sistema con ese usuario para poder configurar y administrar la aplicación.

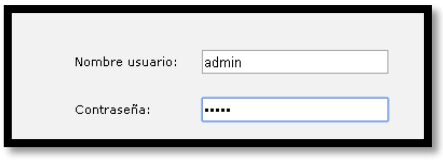


Figura C. 2 Ingreso a la aplicación

Aquí podemos ver los diferentes menús que tiene la aplicación, como primer paso que realizamos por motivos de seguridad es el de crear un usuario con privilegios totales o editar el usuario **admin** y modificarlo, para que se pierdan los valores que vienen por defecto. Para ello nos vamos al menú **Usuario** y luego a **Super Administrador,** y finalmente damos click en la pestaña **Edit,** para agregar valores al usuario **admin**.

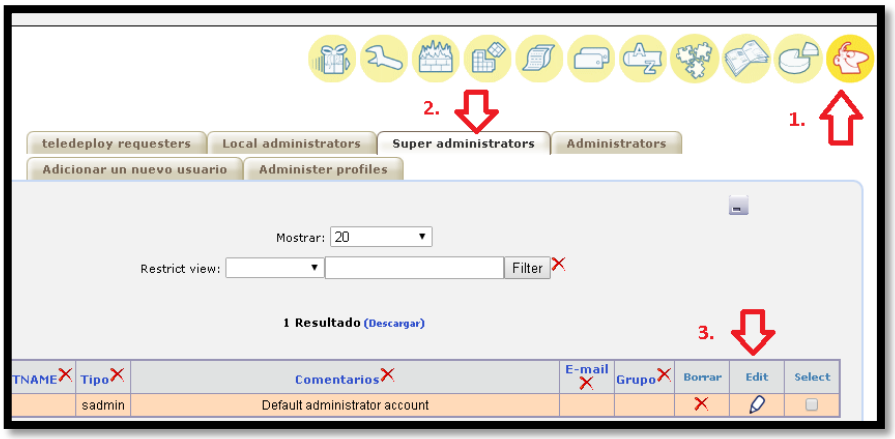


Figura C. 3 Edición del usuario que viene por defecto

En la pantalla de edición agregaremos los parámetros que se solicitan en la pantalla

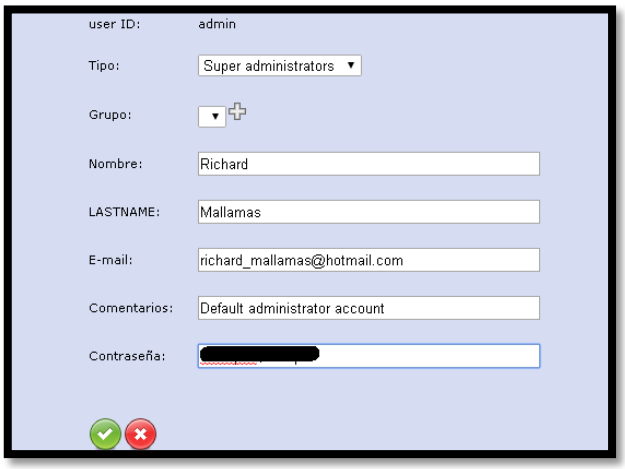


Figura C. 4 Agregamos valores que consideremos necesarios

Una vez cambiado los valores por defecto cerramos la sesión y volvemos a ingresar con la nueva contraseña agregada.

Figura C. 5 Ingresar a la consola con el nuevo usuario

Para administrar una red o subred, la agregamos dando click en la pestaña **Red** y elegimos la opción **Administer**, esto desplegara un menú, elegimos la pestaña **Administer-Subred**, finalmente escogemos la opción **Adicionar** que se encuentra en la parte inferior.

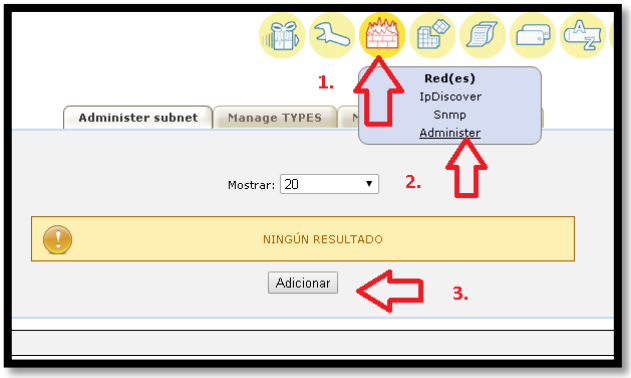


Figura C. 6 Pasos para adicionar una red o subred para administrarla

En la pantalla de edición agregaremos los parámetros que se solicitan en la pantalla, y damos click en el visto de color verde para que se apliquen los cambios.

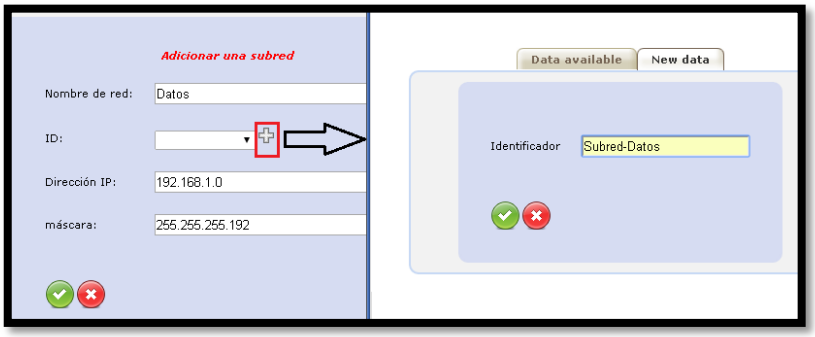


Figura C. 7 Adicionar datos de la subred a administrar

Una vez creada la subred que deseamos administrar, buscamos el menú **Red** y escogemos la opción **IPDiscover**, finalmente damos click en el menú desplegable y escogemos la Subred o red que hemos creado.

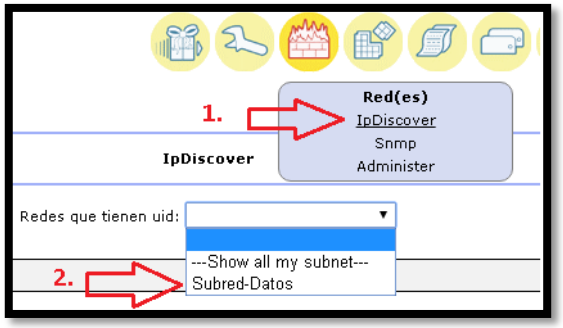


Figura C. 8 Elegir la Subred que vamos a administrar

Al acceder a IPDiscover y dar click en la subred a administrar, se nos mostrara esta ventana, la cual está vacía, pues aún no hemos introducido los ordenadores.

Figura C. 9 Menú IPDiscover

- **Instalación del agente OCS-INVENTORY**

Procedemos a instalar el agente en la pc que queremos gestionar. Para esto nos descargamos el agente de la página oficial de OCS-INVENTORY http://www.ocsinventory-ng.org/en/download/download-agent.html una vez descargado el archivo procedemos con la instalación del archivo "OCS-NG-Windows-Agent-Setup.exe", dando click en el botón Next.

Figura C. 10 Instalación del Agente OCS Inventory

Aceptamos los términos de la licencia

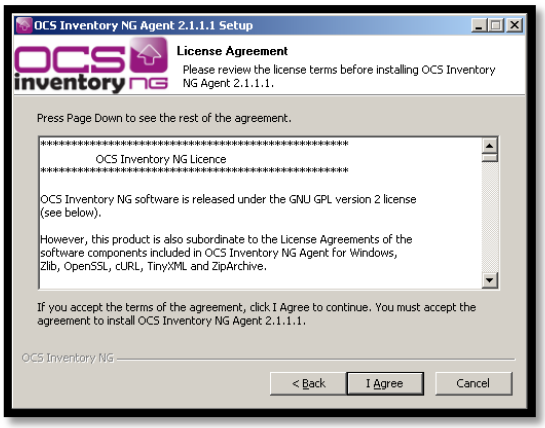


Figura C. 11 Aceptamos los términos de licencia

Luego seleccionamos el tipo de instalación que deseamos:

Network Inventory: El computador puede alcanzar a OCS Inventory Server a través de la red, y por lo tanto, el agente se pondrá en marcha utilizando un servicio de Windows, o una secuencia de comandos de inicio de sesión.

Local Inventory: El equipo no está conectado a una red, o nunca será capaz de llegar a OCS Inventory NG Server. Se puede generar un inventario de este equipo y guardar en el archivo a importar más adelante en el servidor.

Para nuestro caso elegimos la opción **Network Inventory** ya que estamos dentro de una subred.

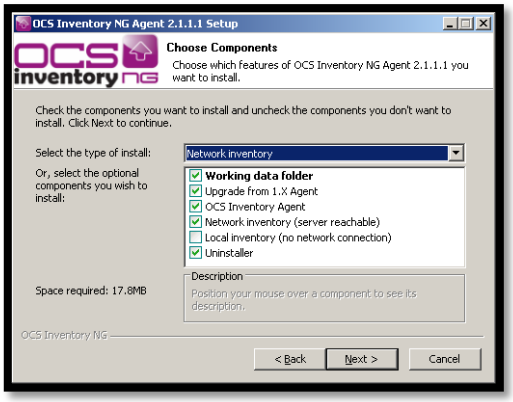


Figura C. 12 Elegimos el tipo de instalación

En la siguiente ventana, apuntamos la dirección IP en la cual se encuentra nuestro servidor OCS-Inventory, y agregamos el usuario que creamos previamente para este computador.

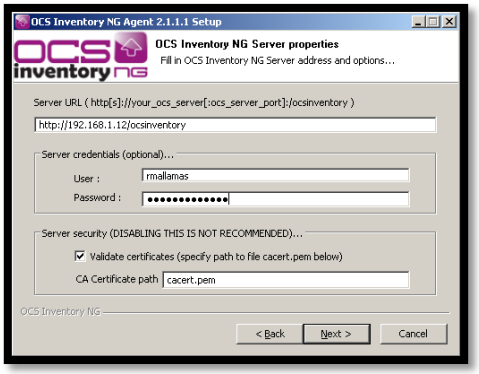


Figura C. 13 Agregamos la dirección IP de nuestro Servidor

En la siguiente ventana, si es necesario, seleccionamos el tipo de proxy que se utilizará para conectarse al servidor de comunicación, la dirección del proxy, el puerto, y las credenciales del proxy, para nuestro caso no añadimos nada a esta ventana.

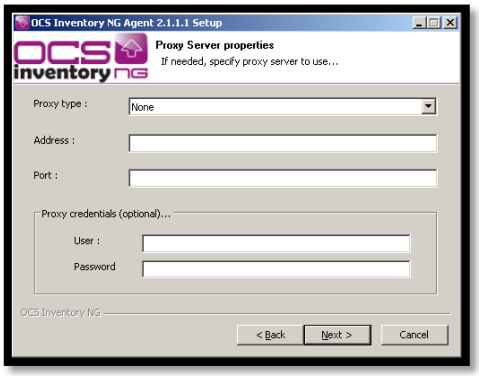


Figura C. 14 Si es necesario se edita datos del Proxy del servidor

Por defecto, el agente OCS Inventory solo se añade pocos datos en los archivos de registro, se puede aumentar habilitando "Verbose log", también podemos añadir una etiqueta para reconocerlo de mejor manera a nuestro usuario, y habilitamos la casilla "Immediatly lauch inventory" para que el agente comience a funcionar inmediatamente.

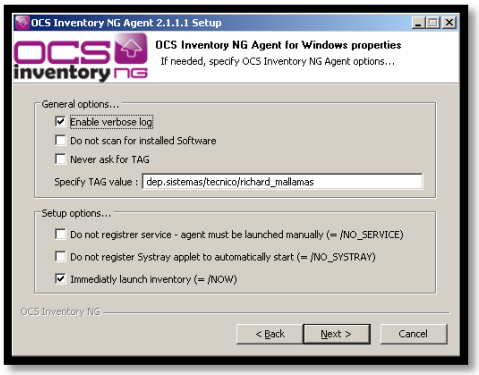


Figura C. 15 Agregamos una etiqueta al computador gestionado

Se escoge una carpeta para instalar el agente, por defecto se guarda en el directorio: C**:\Program Files (x86)\OCS Inventory Agent**

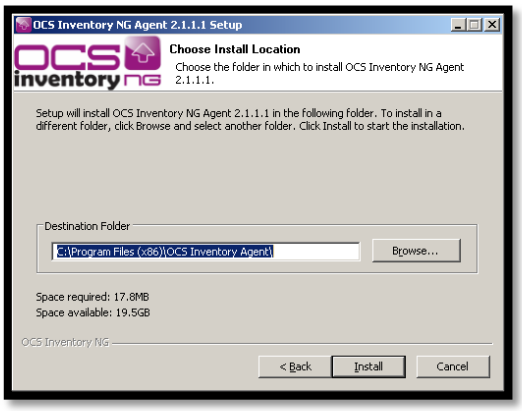


Figura C. 16 Escogemos la carpeta de instalación del agente

Hacemos clic en "Finalizar" para cerrar la instalación del agente OCS-Inventory.

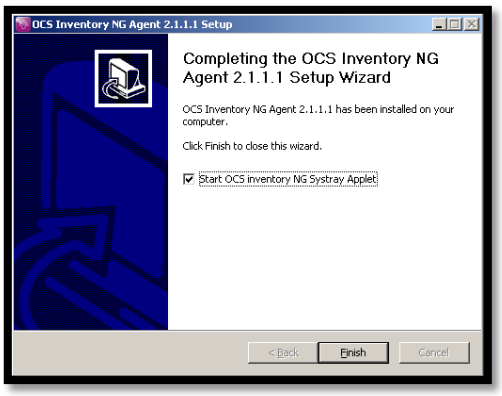


Figura C. 17 Finalizamos la instalación del agente

- **Revisión de los computadores inventariados**

Una vez creado nuestro agente, en la sesión de administrador de OCS-Inventory, buscamos el menú **Red** y escogemos la opción **IPDiscover**, finalmente damos click en el menú desplegable y escogemos la Subred o red que hemos creado y nos aparecerá nuestro primer computador agregado a nuestro sistema.

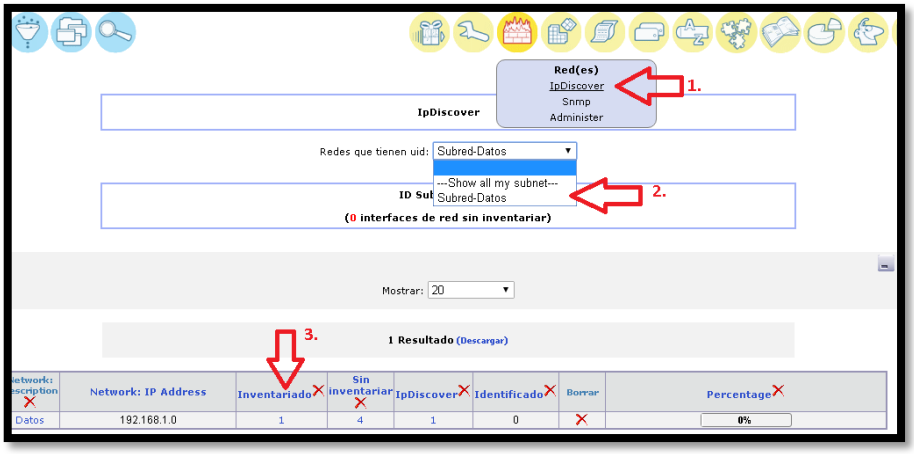


Figura C. 18 Pantalla del pc agregado a nuestro inventario.

Una vez dentro del pc inventariado nos mostrara la siguiente pantalla en la cual muestra algunas características del computador, para poder desplegar más opciones damos click en el nombre del PC.

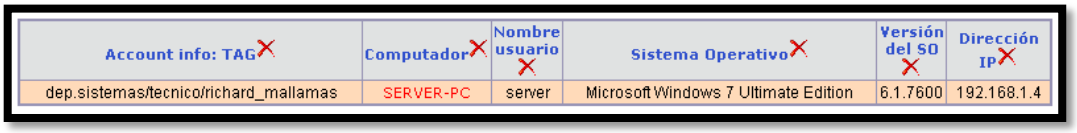


Figura C. 19 Características básicas del PC gestionado

Una vez que damos click en el nombre del PC nos despliega un menú en el que nos indica el nombre del dispositivo, el sistema operativo, el tamaño de la memoria RAM, etc en la parte inferior, podemos encontrar estas opciones de manera específica, en este caso en la opción **Procesador,** nos muestra datos del fabricante, el Tipo, arquitectura, etc.

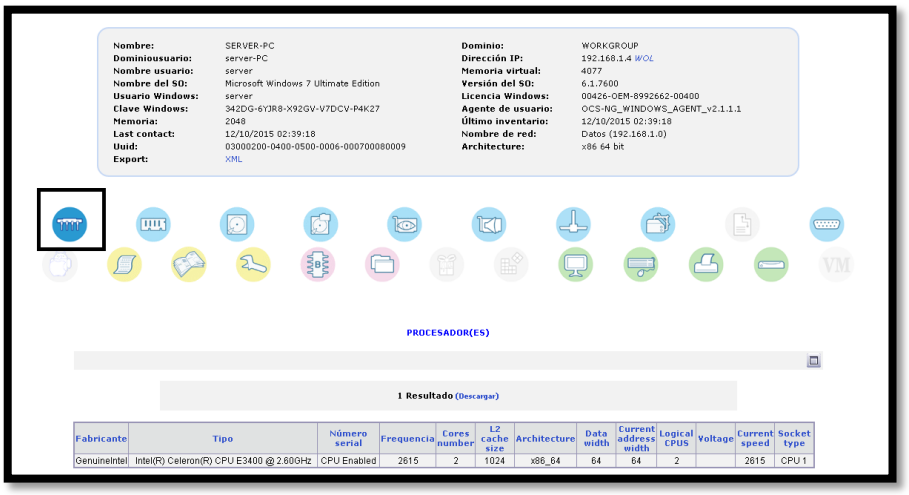


Figura C. 20 Visualización del procesador en OCS

En la opción **Memoria RAM,** nos muestra la descripción, el número de ranuras y el tamaño de memoria existente, etc.

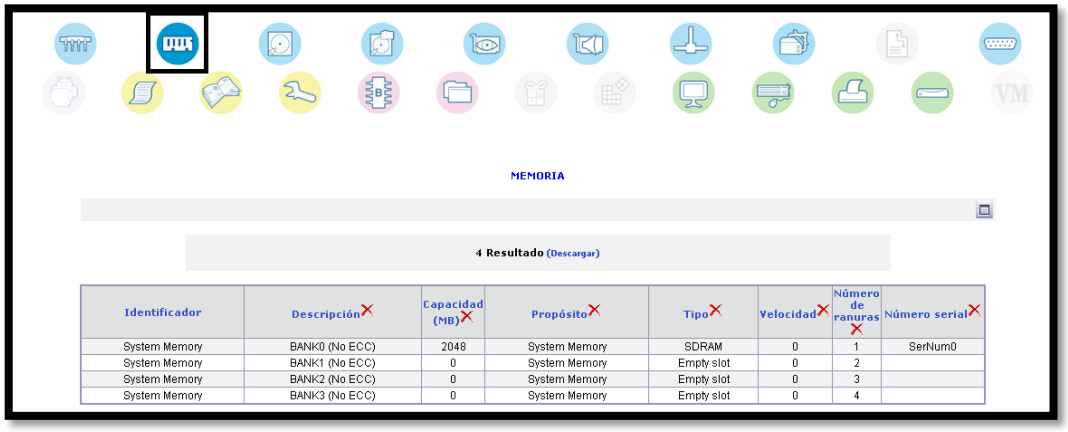


Figura C. 21 Visualización de la Memoria RAM en OCS

En la opción **Almacenamiento,** nos muestra el nombre de la unidad, el modelo, la descripción de cada unidad, el tamaño del disco, etc.

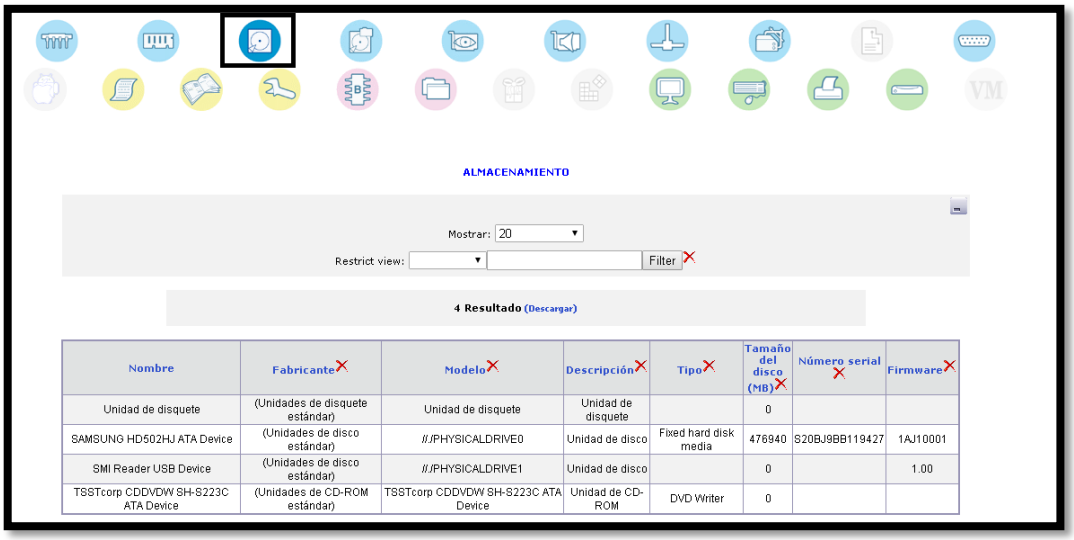


Figura C. 22 Visualización de los periféricos de almacenamiento en OCS

En la opción **Disco,** nos muestra el nombre de las particiones que tenemos en nuestro disco, el tipo de sistema de archivos, el espacio total, el espacio usado y el espacio libre del o los discos duros existentes.

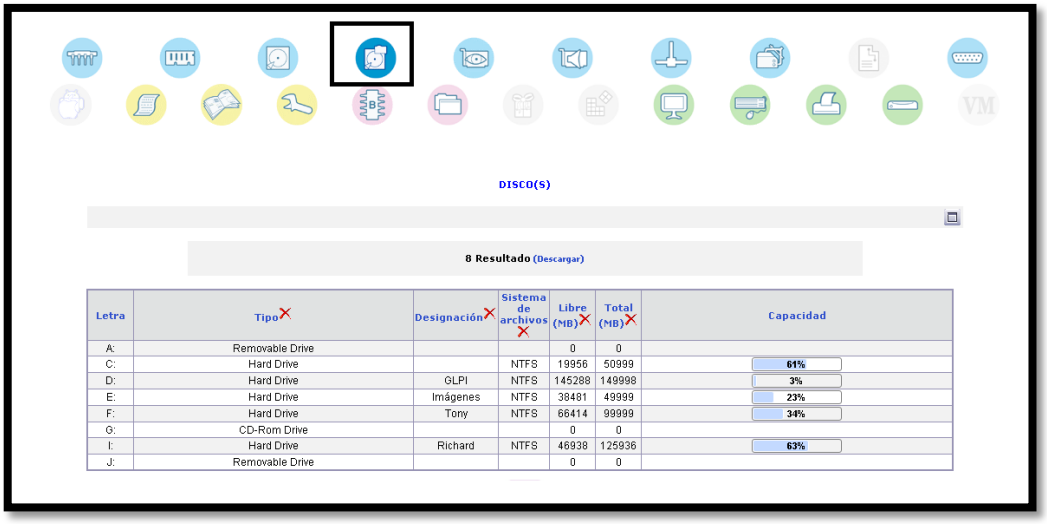


Figura C. 23 Visualización de los discos de almacenamiento en OCS

En la opción **Video,** nos muestra el nombre de la tarjeta de video, la marca, y la resolución de la pantalla en uso.

Figura C. 24 Visualización de la tarjeta de video en OCS

En la opción **Sonido,** nos muestra el nombre de la tarjeta de sonido, y su descripción.

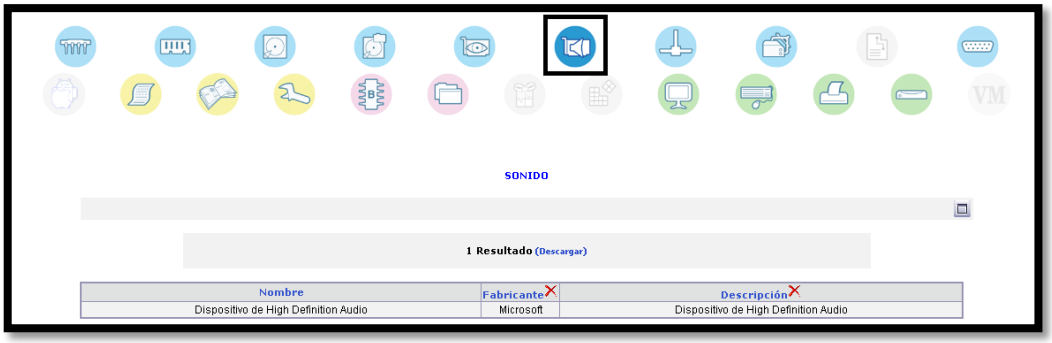


Figura C. 25 Visualización de la tarjeta de sonido en OCS

En la opción red, nos muestra, la descripción de la tarjeta de red, la dirección MAC, la dirección IP, el estado de la interfaz, etc.

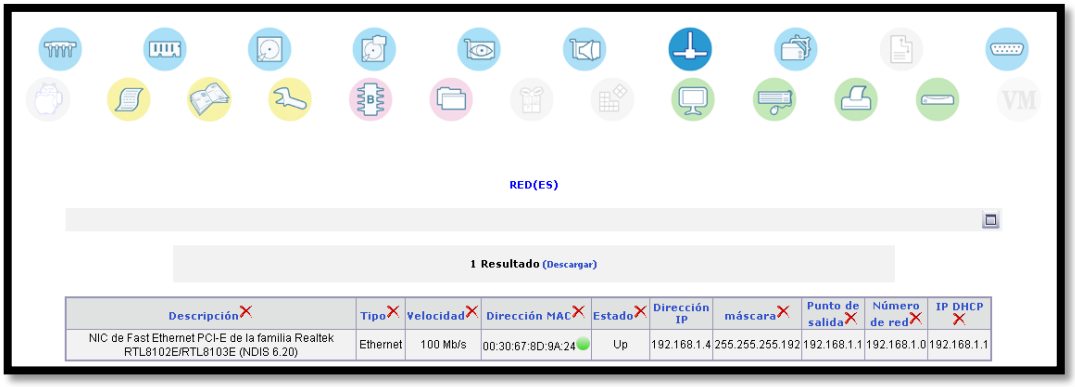


Figura C. 26 Visualización de la tarjeta de red en OCS

C.2. MANUAL DE SOPORTE DE LA PLATAFORMA GLPI

C.2.1. Cambiar los usuarios y las contraseñas que vienen por defecto:

Una vez en la ventana de acceso a GLPI, se nos solicitará un usuario y contraseña para acceder, por defecto el usuario que tiene todos los privilegios viene dado inicialmente por **glpi** y la contraseña **glpi,** así que ingresaremos al sistema con ese usuario para poder configurar y administrar la aplicación.

Figura C. 27 Ventana de acceso GLPI

Pulsado el botón de **Aceptar**, entramos en la aplicación y se nos mostrara la pantalla de la aplicación que es la siguiente:

Figura C. 28 Pantalla inicial del sistema GLPI

Aquí podemos ver los diferentes menús que tiene la aplicación, como primer paso que realizamos por motivos de seguridad es el de crear un usuario con privilegios totales o editar el usuario **glpi** y modificarlo, para que se pierdan los valores que vienen por defecto. Para ello nos vamos al menú **Administración** y luego a **Usuarios,** entonces pulsamos sobre el usuario **glpi**.

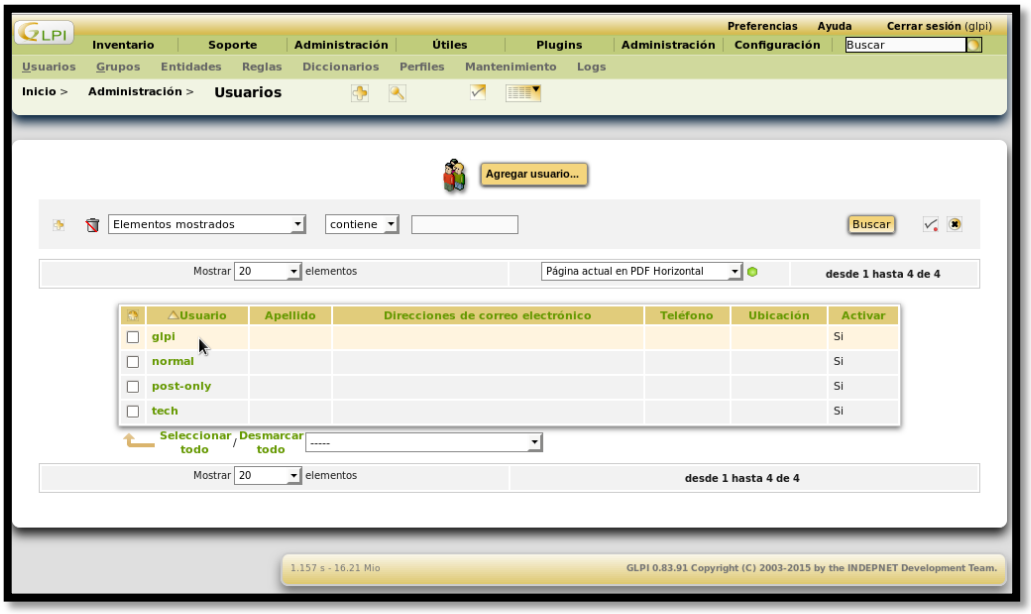


Figura C. 29 Menú de Edición del usuario que viene por defecto

Aquí editamos los datos del usuario **glpi** y agregamos los que creamos convenientes, de esta manera el usuario que tiene todos los privilegios será **administrador** en lugar de glpi,

así mismo, también le cambiaremos la contraseña, y actualizaremos algunos datos, como son su dirección de correo electrónico y su número de teléfono.

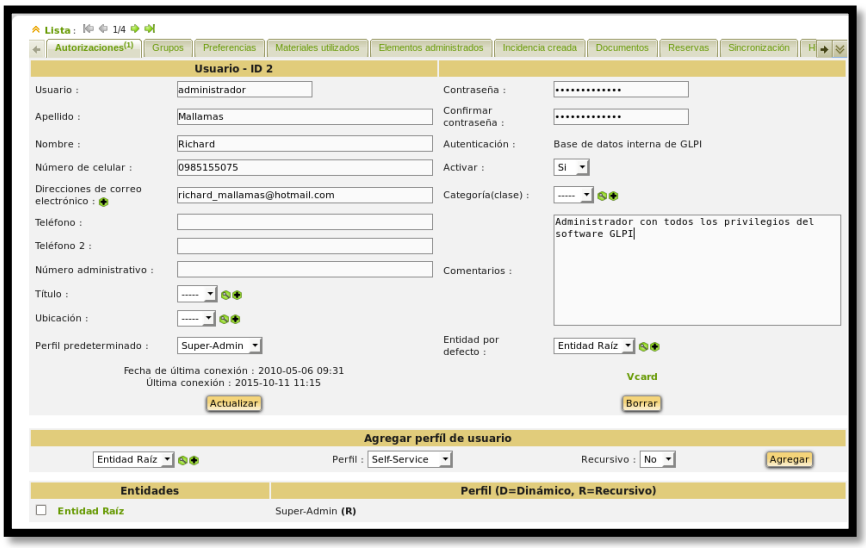


Figura C. 30 Agregamos el usuario con todos los privilegios en GLPI

Una vez realizados los cambios pulsamos el botón Actualizar para que se guarden. Ya modificado o creado el usuario **administrador**, salimos de la aplicación y volveremos a iniciar con los datos creados recientemente.

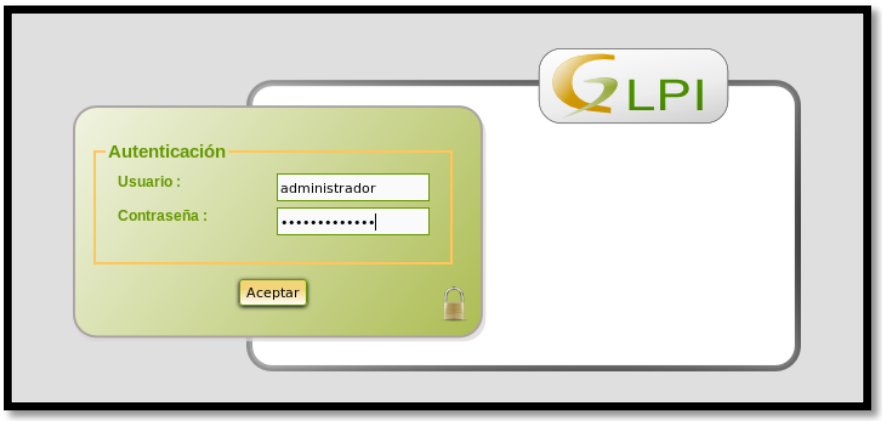


Figura C. 31 Pantalla de ingreso con el usuario administrador

C.2.2. Borrar usuarios que vienen por defecto

Seguidamente procedemos a borrar los demás usuarios existentes, para que solo tengamos una entrada única a nuestra aplicación, con la finalidad de prevenir que personas ajenas al sistema tengan un ingreso completo de todos los privilegios.

Para borrar el usuario o los usuarios que no deseamos, vamos al menú **Administración** y luego a **Usuarios**, aquí marcamos la casilla a la izquierda del o los usuarios y en el desplegable inferior seleccionamos la opción **Borrar**, y por último en el botón **Aceptar**.

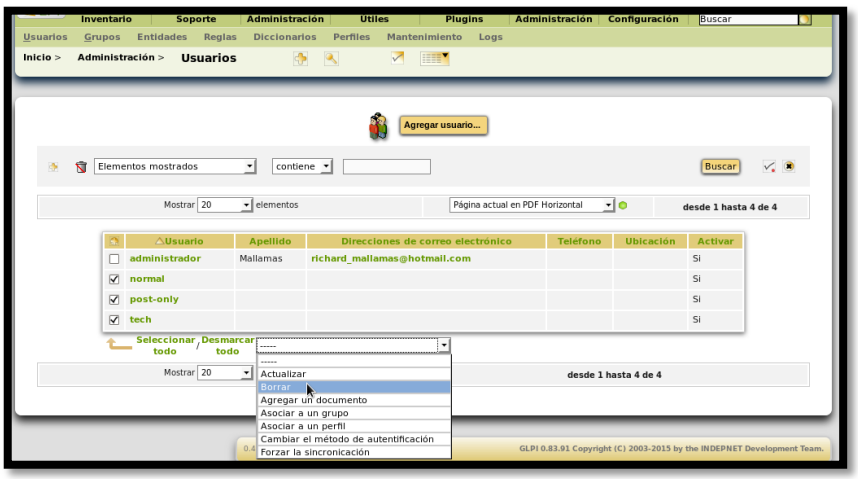


Figura C. 32 Eliminar uno o varios usuarios de ingreso a la aplicación

Una vez borrados los usuarios no deseados, solo aparecerán en pantalla los usuarios que confirmamos conservar.

Figura C. 33 Pantalla con la lista de usuarios de ingreso al sistema GLPI

C.2.3. Creación de usuarios

Para crear un usuario que tenga funciones básicas como la de crear una incidencia, y luego reportarla al administrador, vamos al menú **Administración**, luego a **Usuarios** y por ultimo damos click en **Agregar usuario**.

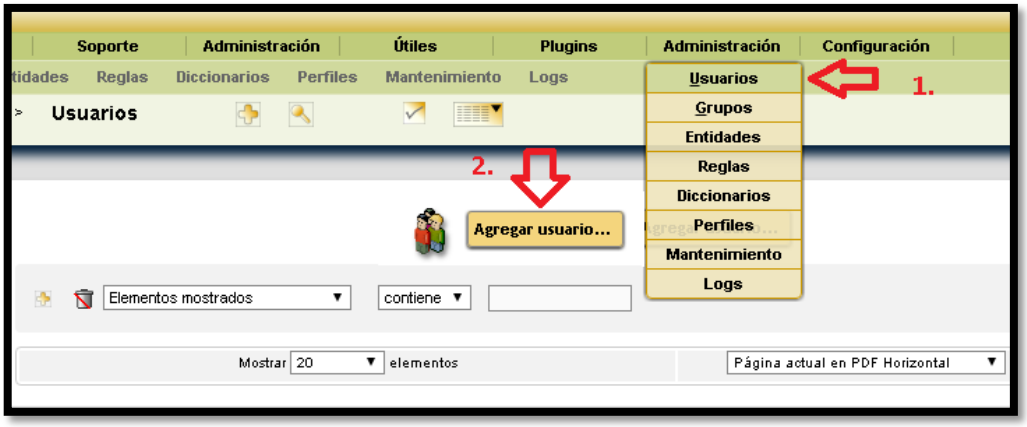


Figura C. 34 Agregar Usuario GLPI

Para añadir el usuario agregamos un nombre que para este caso, es la unión de la primera letra del nombre junto al primer apellido. Para lo cual se presenta el siguiente ejemplo:

Nombre: Danilo Maldonado

Nombre de usuario: dmaldonado(la inicial del primer nombre junto al primer apellido)

Contraseña: dmaldonado(la inicial del primer nombre junto al primer apellido)

En la mayoría de los casos se estableció el usuario de tal manera que sea el mismo con el que ingresan al computador, para hacer más fácil el ingreso a la plataforma. Se agregan datos como el teléfono o correo electrónico si se requiere. Por ultimo damos click en agregar para guardar los cambios.

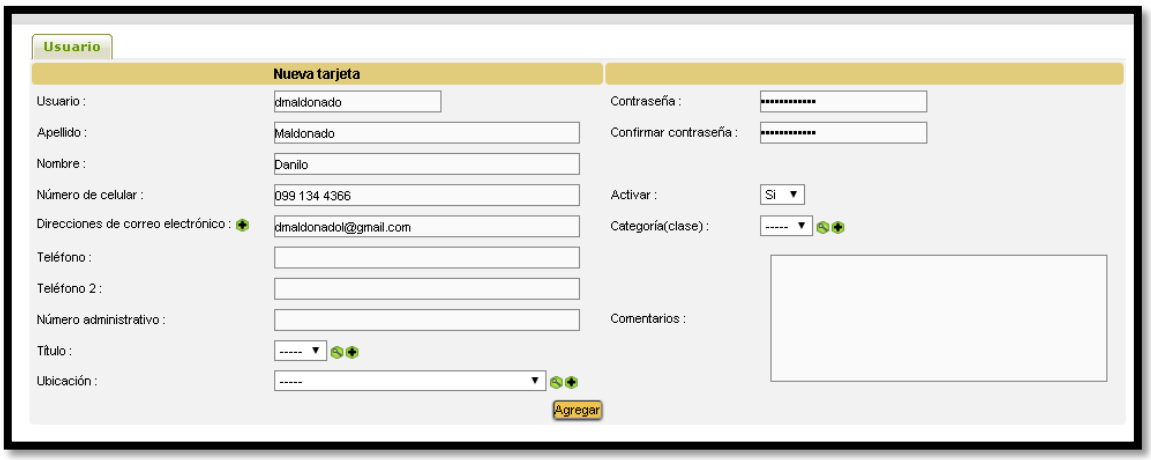


Figura C. 35 Agregar datos del usuario

Una vez creado el usuario damos click en su nombre, para otorgarle los permisos de perfil Self-Service, el cual es solo para usuario final.

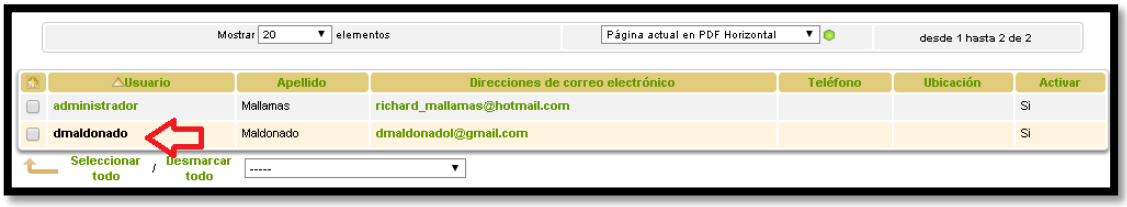


Figura C. 36 Ingresamos al usuario creado

En esta ventana, buscamos la opción **Perfil predeterminado,** elegimos la opción **Self Service**, si tendríamos que actualizar algún dato más lo podríamos agregar y para que se guarden los cambios damos click en el botón **Actualizar**

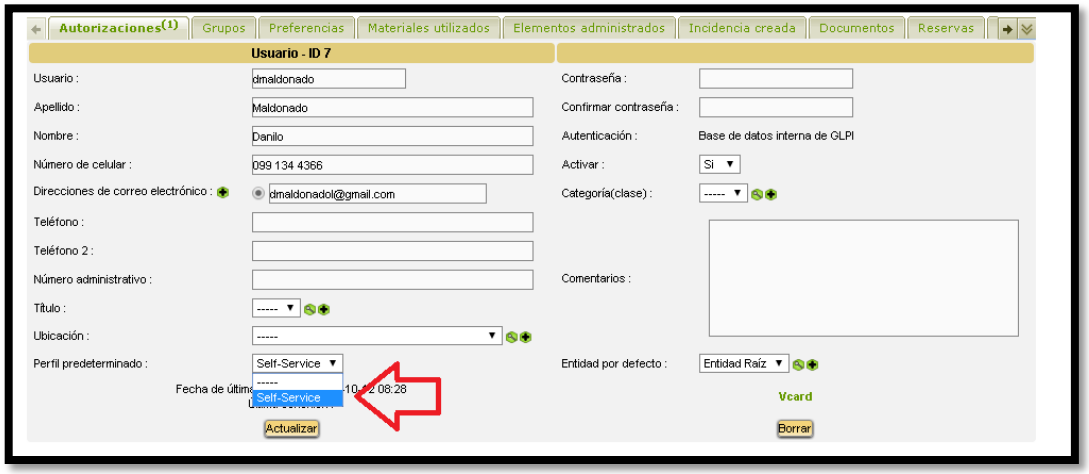


Figura C. 37 Damos permisos Self Service al usuario creado

Para añadir un pc a un usuario nos dirigimos al menú **Inventario,** damos click en la opción **Computadores**, en esta ventana, buscamos la opción Usuario, para agregar el computador al usuario que deseemos, una vez realizado este procedimiento damos click en actualizar para que se guarden los cambios.

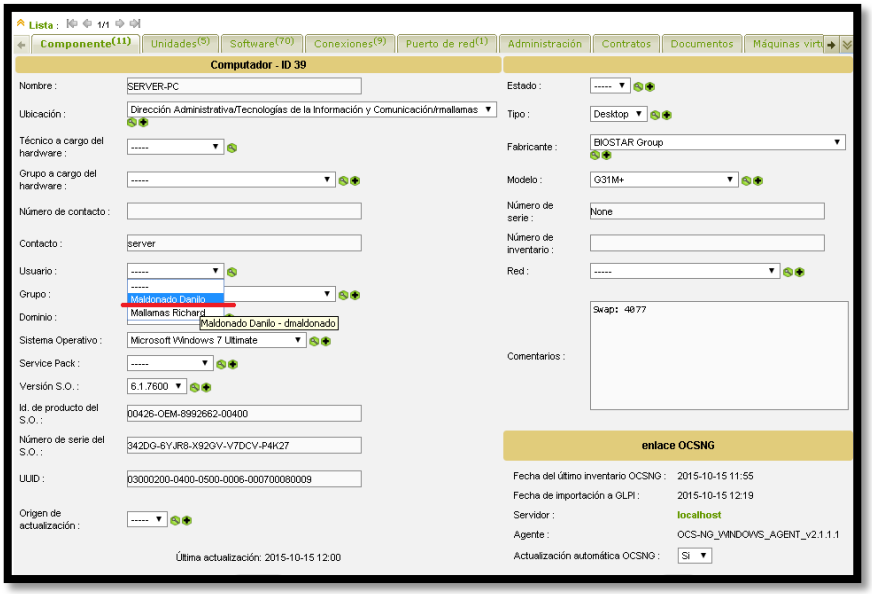


Figura C. 38 Añadir un usuario a un Pc inventoriado

En este momento el usuario puede ingresar a su cuenta y enviar requerimientos o incidencias.

C.2.4. Creación de grupos

Para un control mejor de nuestros usuarios los podemos agrupar, en pequeñas secciones, para lograr esto procederemos a realizar los siguientes pasos:

Nos dirigimos al menú **Administración**, y escogemos la opción **Grupos**, una vez en este menú buscamos el botón Agregar ubicado en la parte superior derecha.

Figura C. 39 Menú administración, opción Grupos.

Una vez en este menú, procederemos a agregar los datos que consideremos necesarios, como el nombre del grupo, y un comentario en el cual explique una pequeña referencia del contenido de este nuevo grupo a crearse, y por último damos click en el botón agregar para que se guarden los cambios.

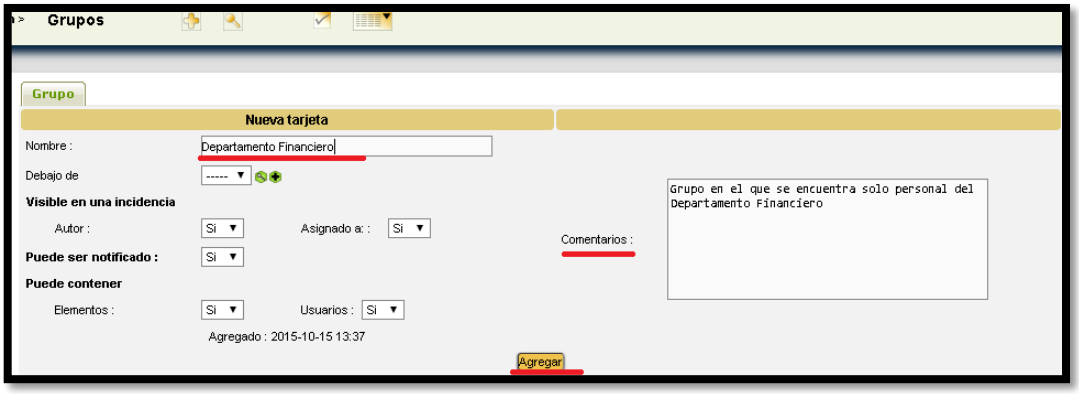


Figura C. 40 Plantilla para agregar grupos

Al crear el grupo, lo confirmamos dirigiéndonos en el menú **Administración** y escogemos la opción **Grupos**, y podremos visualizar el grupo que acabamos de crear.

Figura C. 41 Grupos creados en GLPI

Para agregar usuarios, damos click en el nombre del Grupo que deseemos, y damos click en la pestaña Usuarios, y en la parte inferior del menú nos saldrá un menú desplegable de los usuarios que deseemos agregar al grupo, también nos mostrará la opción de que si es un usuario Supervisor o un usuario Delegado, escogemos la opción que más se acople a lo que deseamos y damos click en el botón Agregar para guardar los cambios.

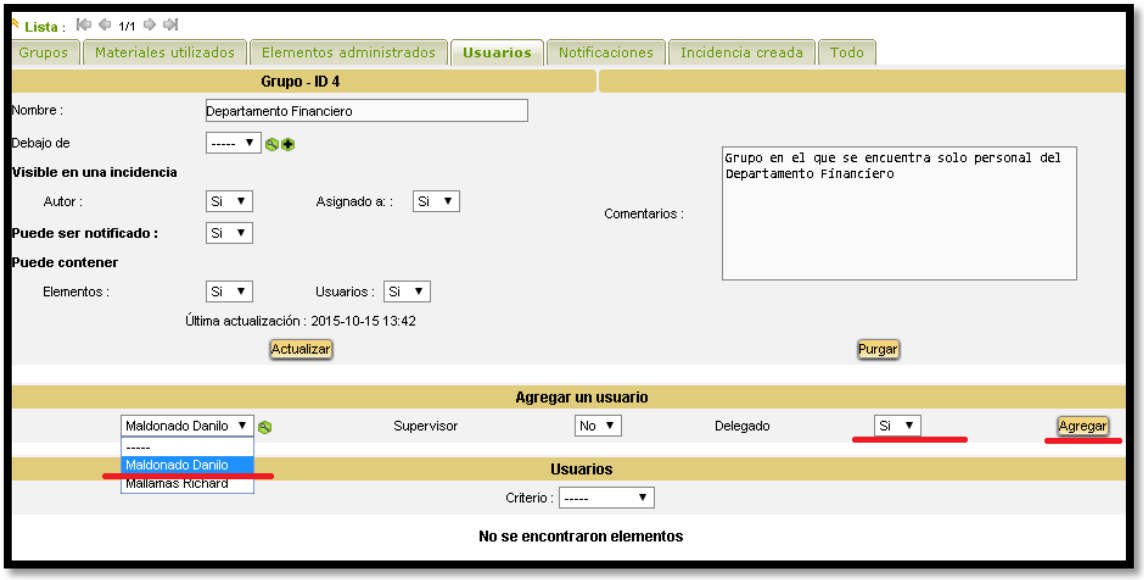


Figura C. 42 Agregar usuarios al grupo

Una vez añadido el usuario al grupo, regresamos al menú del grupo para confirmar su creación.

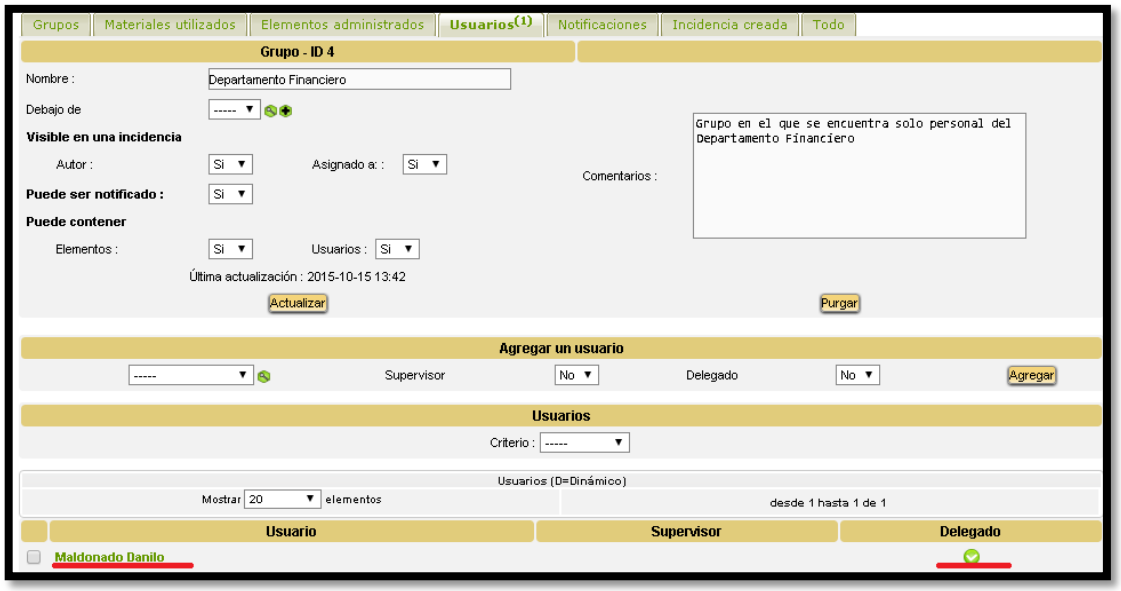


Figura C. 43 Grupo con usuarios

La creación de grupos nos ayuda en gran manera cuando se quiere sacar una información estadística de las incidencias, pues en vez de ver los problemas individualmente, estaríamos al tanto de uno o varios departamentos en específico.

C.2.5. Menú Computadores

Para acceder al inventario de los ordenadores, vamos al menú **Inventario** y luego a **Computadores**.

Figura C. 44 Menú Inventario-Computadores

Al acceder a la opción Computadores dentro del menú Inventario, se nos mostrará esta ventana, en el cual tenemos uno o varios pc en este menú, los cuales fueron previamente sincronizados con OCS-INVENTORY.

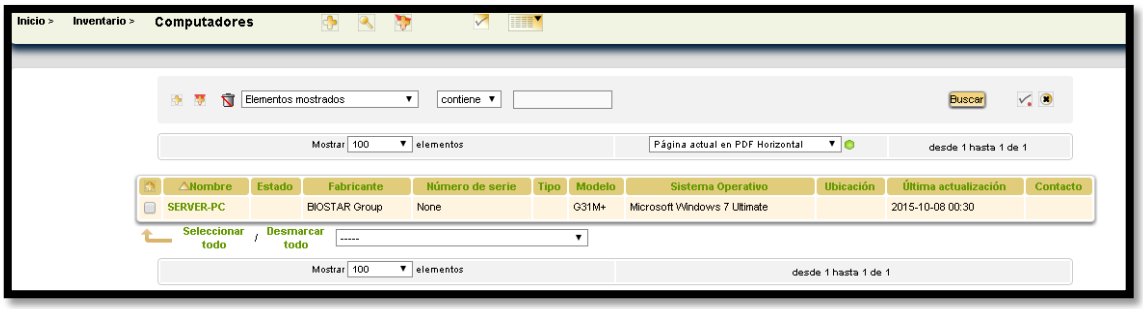


Figura C. 45 Menú Computadores

Una vez realizado estos pasos regresamos al menú **Inventario** y luego a **Computadores** y elegimos el computador que nos sale en esta ventana, en la cual aparecen pestañas con varias opciones, las cuales son Componente, Utilidades, Software, Conexiones, Puerto de red, etc. Y en las opciones descritas aparece información básica como el nombre del PC, versión del Windows, serie, modelo, fabricante, y dependiendo del texto de la etiqueta TAG en OCS-Inventory, nos mostrará información como la ubicación, la red en que se encuentra, el número de contacto, etc. Para nuestro ejemplo solo agregaremos información de ubicación en nuestra etiqueta, quedando el informe de nuestro computador gestionado de la siguiente manera.

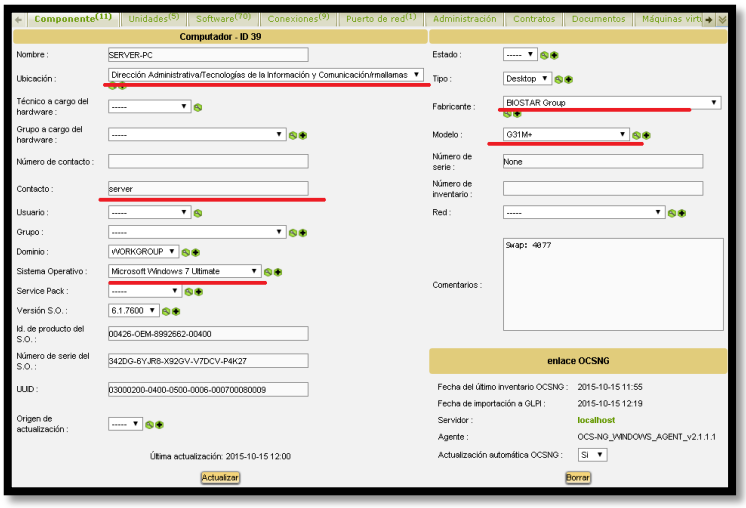


Figura C. 46 Menú inicial del computador registrado

C.2.6. Menú Componente

Nos mostrara los dispositivos existentes en el pc, como el procesador, la memoria RAM, el Disco Duro, la tarjeta de Red, Tarjeta Gráfica, etc.

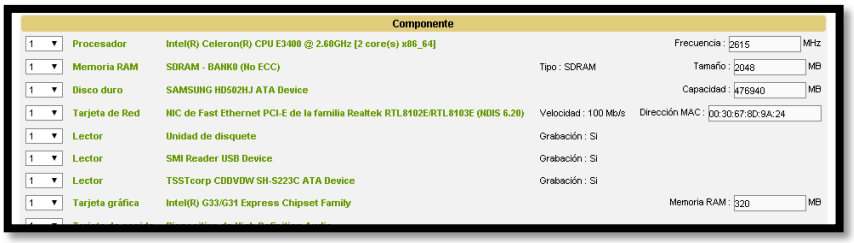


Figura C. 47 Menú componente GLPI

C.2.7. Menú Unidades

En el menú unidades tenemos todo lo referente al disco duro, su tamaño, sus particiones y el espacio libre que actualmente tiene.

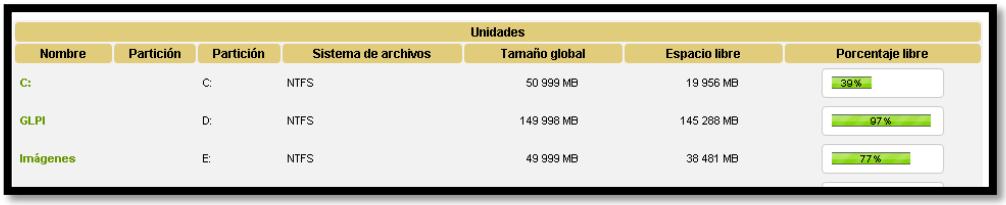


Figura C. 48 Menú Unidades GLPI

C.2.8. Menú Software

En el menú software podemos monitorear los programas que se encuentran instalados actualmente en este PC, también nos da la opción de Desinstalar, si fuera necesario.

Figura C. 49 Menú Software GLPI

C.2.9. Menú Puerto de red

En el menú puerto de red, podemos encontrar información como el nombre de la tarjeta de red, la dirección MAC, la dirección IP, etc.

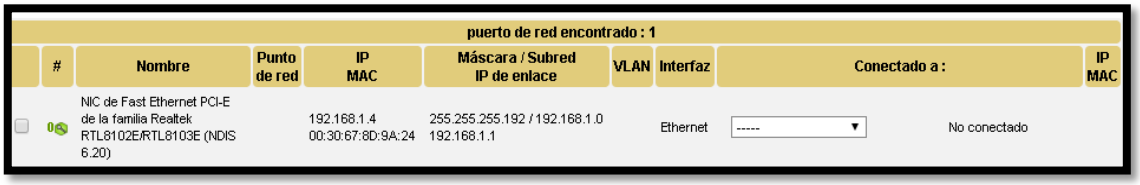


Figura C. 50 Menú puerto de red

C.2.10. Menú Conexiones

En el menú conexiones podemos encontrar que dispositivos se encuentran conectados al computador, en esta caso tenemos el mouse, el teclado, el monitos, la impresoras.

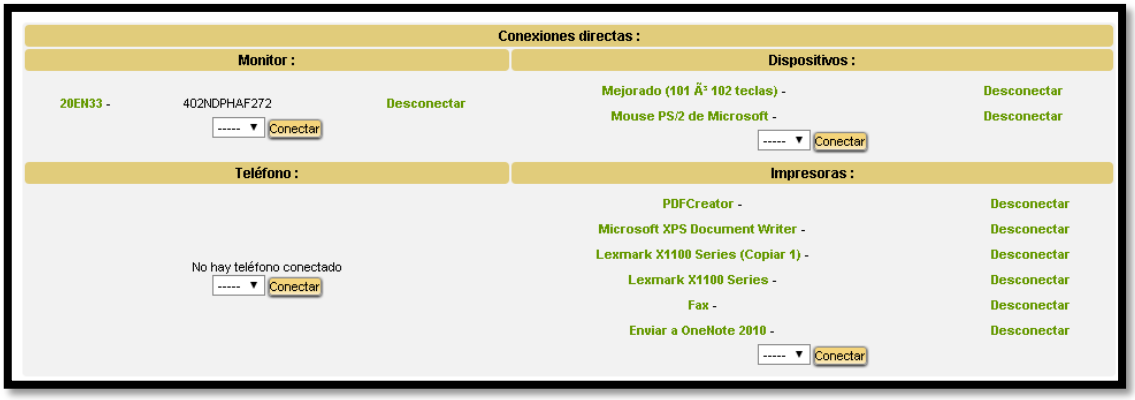


Figura C. 51 Menú conexiones

C.2.11. Menú Monitor

Si damos click en la opción **monitor**, podemos observar la marca del monitor, la ubicación, el número de serie, además nos permite visualizar las opciones generales de este monitor, etc.

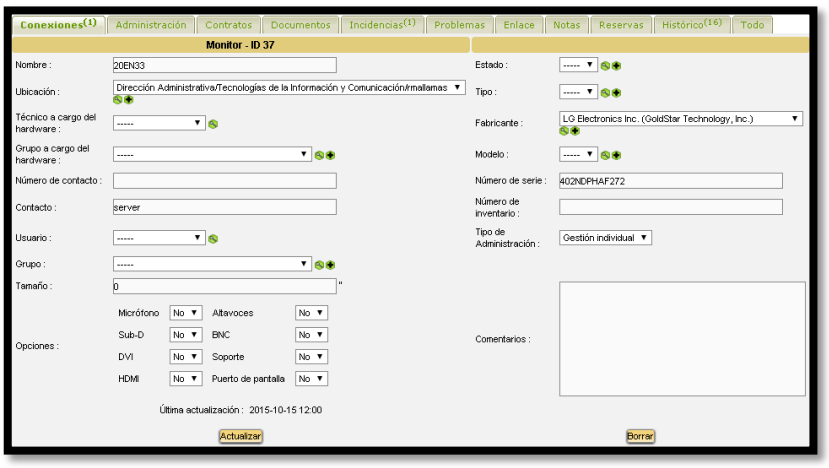


Figura C. 52 Menú Monitor GLPI

C.2.12. Menú Impresoras

Si damos click en la opción **impresora**, podemos observar la marca de la impresora, la ubicación, también observar las opciones que tiene esta impresora, que puertos utiliza para enlazarse al pc, etc.

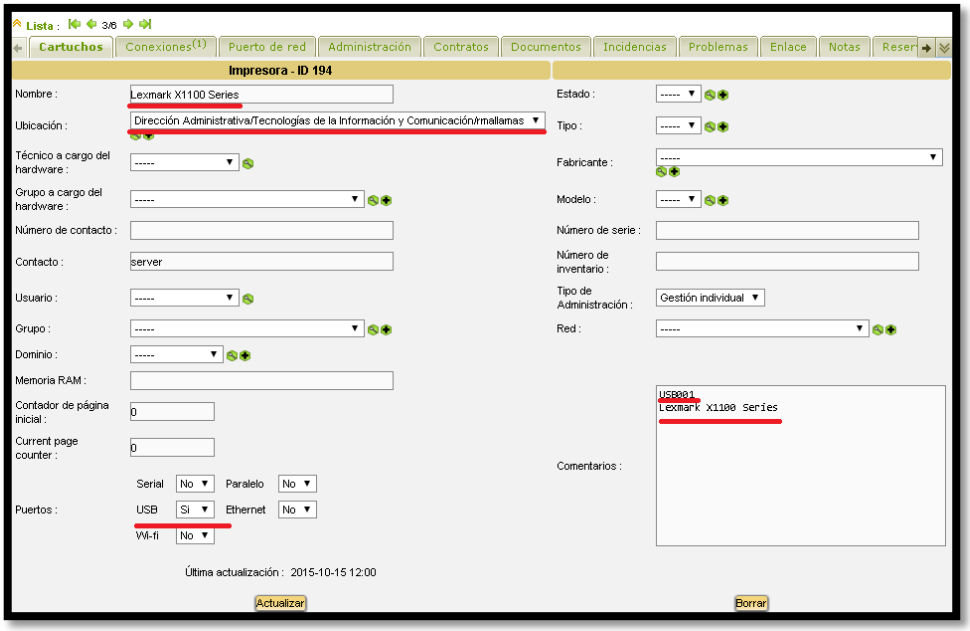


Figura C. 53 Menú Impresora GLPI

C.2.13. Menú Incidencias

Normalmente las incidencias las hacen los usuarios finales, es decir los que tienen como perfil Self-Service. Las opciones cuando entran con este perfil son entre otras las necesarias para añadir, consultar incidencias y la Base de Datos de Conocimiento para poder encontrar solución a algún problema conocido. Para este menú damos click en **Soporte**, y escogemos la opción **Incidencias**.

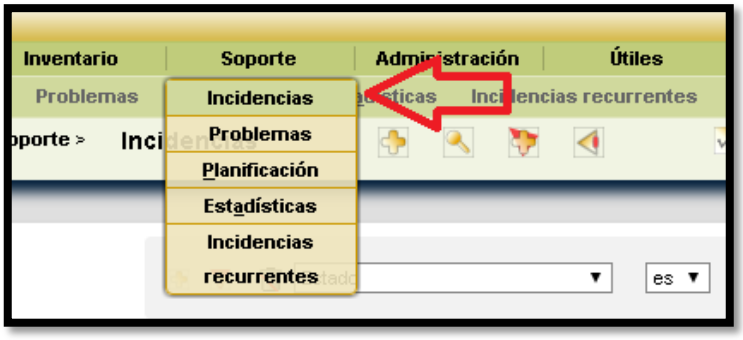


Figura C. 54 Menú Incidencias

- **Plantilla de mesa de ayuda defecto**

En nuestro caso utilizaremos la opción mesa de ayuda que viene por defecto. Para obtener esto, nos dirigimos al menú **Administración**, escogemos la pestaña **Perfiles**, en el menú que visualizamos, buscamos la opción **Self-Service** y le damos un click para que nos muestre sus propiedades.

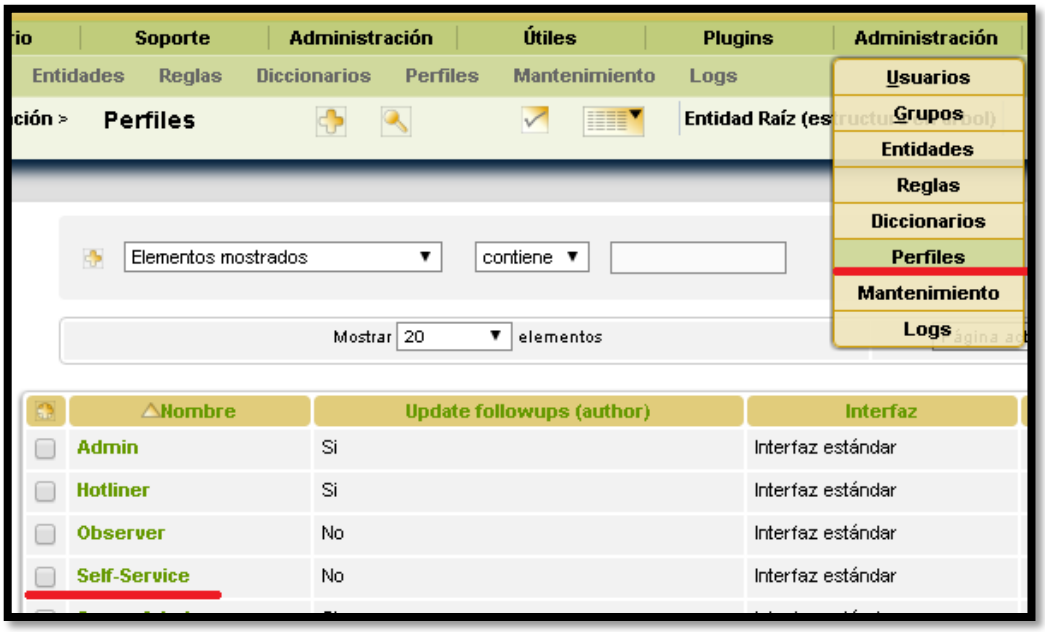


Figura C. 55 Menú perfiles, opción Self-Service

En la ventana que nos aparece, verificamos que la opción de Interfaz se encuentre establecida en **Mesa de Ayuda,** la cual nos da una plantilla solo con opciones básicas que el usuario debe ingresar, damos click en el botón actualizar para que los cambios se realicen.

Figura C. 56 Menú del perfil de usuario Self-Service

A continuación se describe cada campo de la plantilla mesa de ayuda:

- **Tipo**: Se debe escoger entre si es una **Incidencia** (comunicar la falla de un servicio/equipo) o un **Requerimiento** (solicitar un equipo o un reporte al administrador/técnico).

Figura C. 57 Opción Tipo

- **Categoría:** Se debe escoger de la lista despegable, la categoría que más se ajusta a la necesidad que tenga el usuario.

Figura C. 58 Opción Clase

- **Urgencia:** Si la incidencia debe atenderse muy rápidamente se escogerá los niveles altos, caso contrario se ubicaría un nivel medio/Bajo.

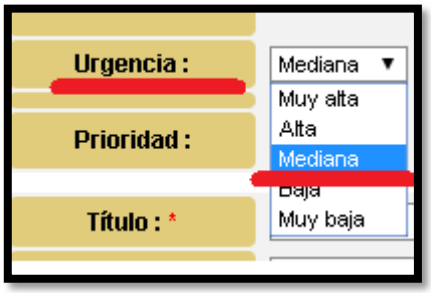


Figura C. 59 Opción Urgencia

- **Tipo de Hardware:** Podemos agregar el tipo de hardware con el que estamos teniendo problemas para hacer más fácil la búsqueda de solución al problema ocurrido.

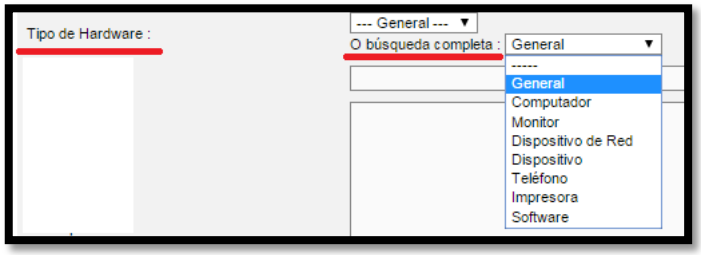


Figura C. 60 Opción Elemento asociado

- **Título:** Se debe especificar una idea general sobre su incidencia, para el ejemplo hemos puesto de título Fallo de monitor.

Figura C. 61 Opción Titulo

- **Descripción:** Aquí se realiza una descripción detallada y clara sobre su requerimiento/incidencia.

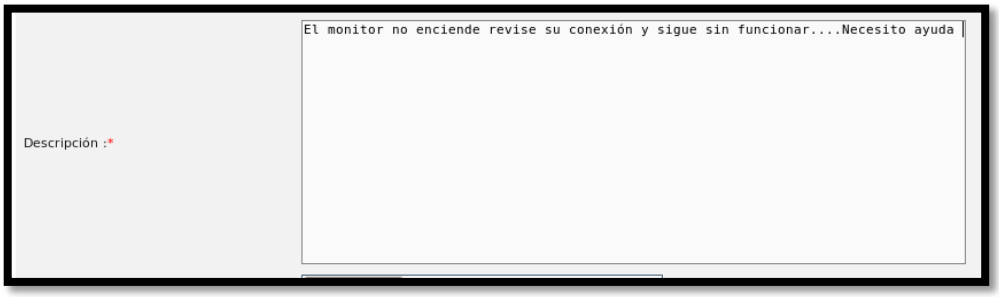


Figura C. 62 Opción Descripción

- **Archivo:** Se puede adjuntar un archivo (máximo 100MB) con información sobre la petición, en el que podemos enviar una captura de pantalla de lo que esté sucediendo, o algún documento referente a la situación de la incidencia.

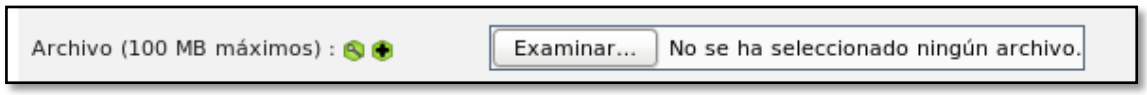


Figura C. 63 Opción Archivo

Y estaríamos listos recibir las incidencias o requerimientos que el usuario nos enviará a través de la plataforma GLPI.

- **Revisión de Incidencias**

Para revisar las incidencias recibidas, nos dirigimos al menú **Soporte**, y escogemos la opción **Incidencias**. De esta manera podemos visualizar la primera incidencia enviada por nuestro usuario.

Figura C. 64 Revisión de Incidencias

Para la revisión de incidencias la ventana por defecto nos saldrá con las incidencias más recientes sin resolver, si deseamos visualizar algunas incidencias en específico ya sea por usuario o por grupo, damos click en el menú desplegable:

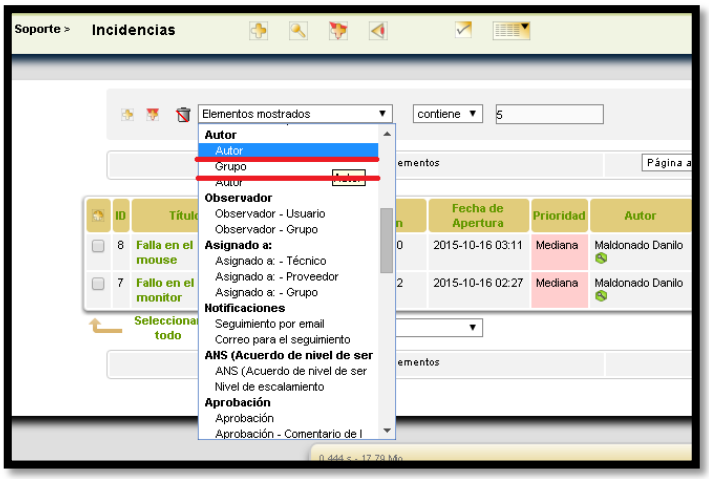


Figura C. 65 Buscar incidencias en específico

Si escogemos la opción por grupo nos desplegará un menú con el nombre del grupo del que queremos visualizar las incidencias, y por último damos click en el botón buscar para que se puedan observar todas las incidencias pertenecientes a este grupo.

Figura C. 66 Visualizar incidencias por grupo

Al dar click en el título de la incidencia que deseemos revisar nos mostrará un menú desplegable en el cual distinguiremos las opciones que tenemos a nuestra disposición, entre las cuales están las de comunicarnos con el usuario que puso la incidencia, así como añadir la solución en la Base De Datos de Conocimiento (esto permite en el caso de una incidencia similar disponer de una ayuda para solventarla), coste de la intervención, etc.

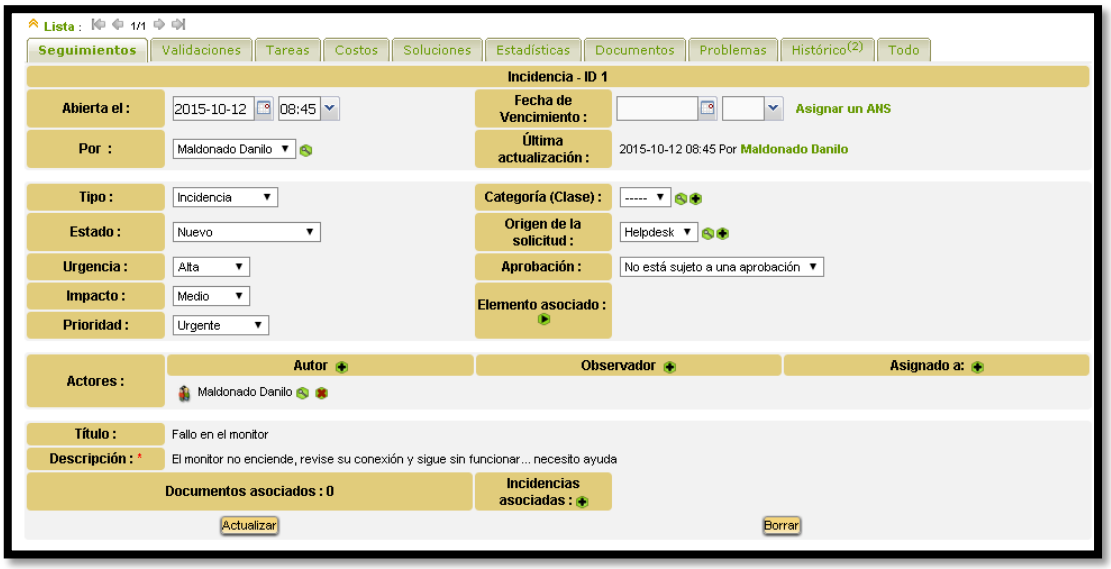


Figura C. 67 Menú Seguimiento GLPI

Antes de proceder a dar una solución agregamos en el menú **Actores**, el grupo al que pertenece este usuario, con la finalidad de que esta incidencia se asocie tanto al usuario como al grupo o departamento al que pertenece y establecer soluciones de forma individual o grupal si es que la situación lo amerita.

Para esto damos click en la ventana **Autor** y elegimos la opción **grupo:**

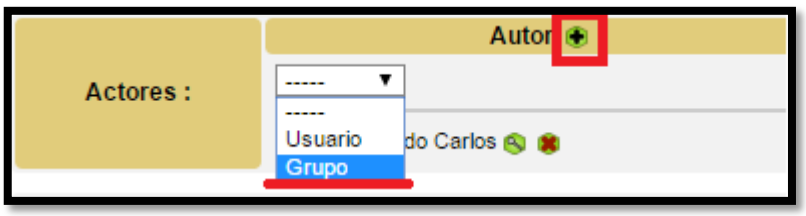


Figura C. 68 Añadir un actor a la incidencia

Una vez en la opción grupo, nos saldrá un menú desplegable en cual podremos escoger a que departamento pertenece nuestro usuario a gestionar.

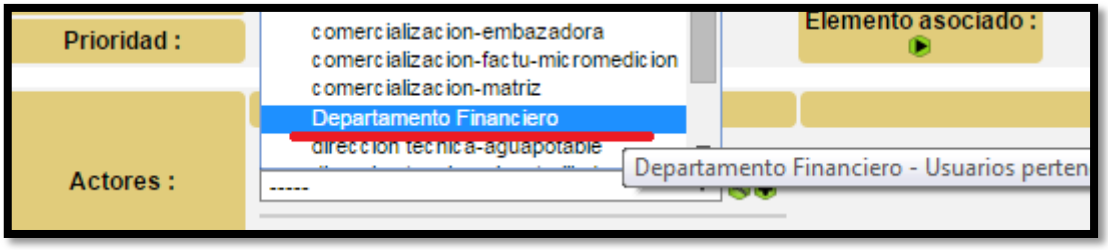


Figura C. 69 Escogemos el grupo al que pertenece nuestro usuario

Seguidamente, procedemos a dar una solución a la incidencia, como primera solución a esta incidencia, nos dirigiremos al menú **Inventario**, luego a la opción **Monitores** o al dispositivo que haya asociado nuestro usuario, y verificar el estado de funcionamiento. Como respuesta de ejemplo podemos agregar un mensaje con el cual, por ejemplo, el usuario se acerque para revisar su dispositivo personalmente o algún mensaje que distinga una solución. Esto lo lograríamos dando click en la pestaña **Soluciones** del menú **Incidencias,** y nos aparecerá una plantilla de la siguiente manera.

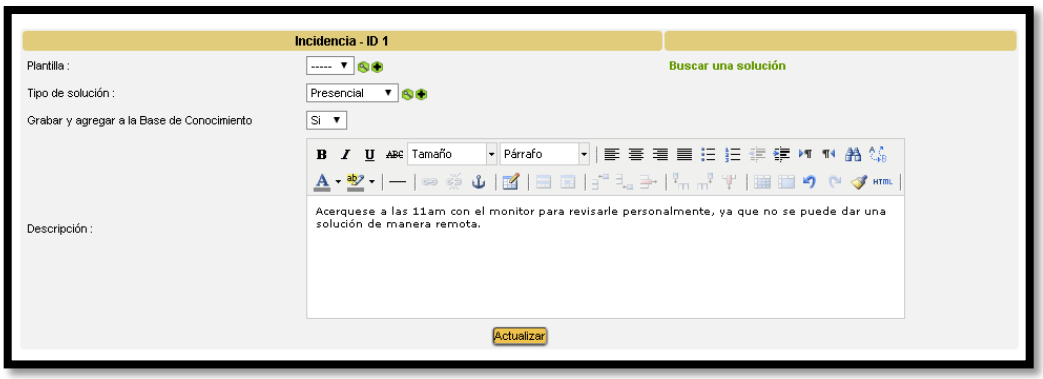


Figura C. 70 Responder dando una solución textual a una incidencia

En esta plantilla podremos escoger:

Tipo de solución, en este caso creamos el tipo de solución Presencial, ya que este tipo de problemas no se puede resolver remotamente. De esta forma el mensaje de respuesta se dirigirá al usuario que envió la incidencia.

Grabar y agregar a la base del conocimiento, esta opción nos permite guardar esta solución para problemas similares que puedan presentarse y así agilitar el proceso en una próxima ocasión.

Descripción, donde escribiremos la solución que más nos parezca conveniente.

Para que se guarden los cambios daremos click en Actualizar, y esta solución se nos guardará en nuestra base de datos y de igual forma le llegara al usuario para que el la revise.

C.2.14. Menú Planificación

Entre las opciones que podemos asignar a una incidencia, la planificación es una de las más importantes al momento de dar seguimiento a un problema, porque algunas soluciones no las podemos dar directamente ya sea, por falta de materiales o actualizaciones del sistema etc, entonces para activarla nos dirigimos a la plantilla de la incidencia que le vamos a dar una solución, en la pestaña **tareas**, buscamos la opción Agregar una nueva tarea.

Figura C. 71 Asignación de tareas

Nos saldrá una plantilla para crear una tarea en la cual se encuentran los siguientes campos:

Descripción: Agregar una pequeña descripción de la planificación que se le va a asignar a esta incidencia.

Estado: podremos agregar en qué estado se encuentra la tarea que vamos a asignar, la tarea puede estar pendiente, terminada o solo para información.

Planificación: en esta opción podemos asignar una fecha en la cual vamos realizar esta tarea.

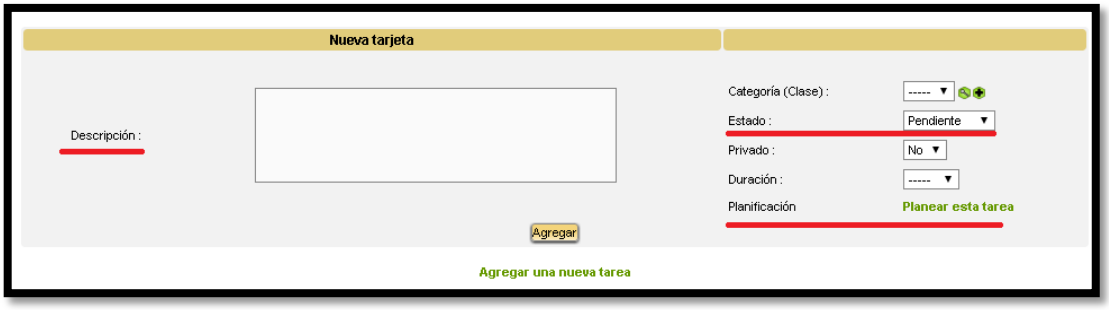


Figura C. 72 Plantilla de asignación de tareas

En la opción Planificación damos click en **Planear esta tarea**, para asignar una fecha a nuestra en la cual realizaremos la tarea que solucionará la incidencia, en esta ventana nos desplegará la opción de asignar la tarea a un usuario, establecer la fecha y hora de realización así como el periodo de duración de esta tarea. Llenamos estos datos, damos click en el botón **Agregar** para guardar los cambios.

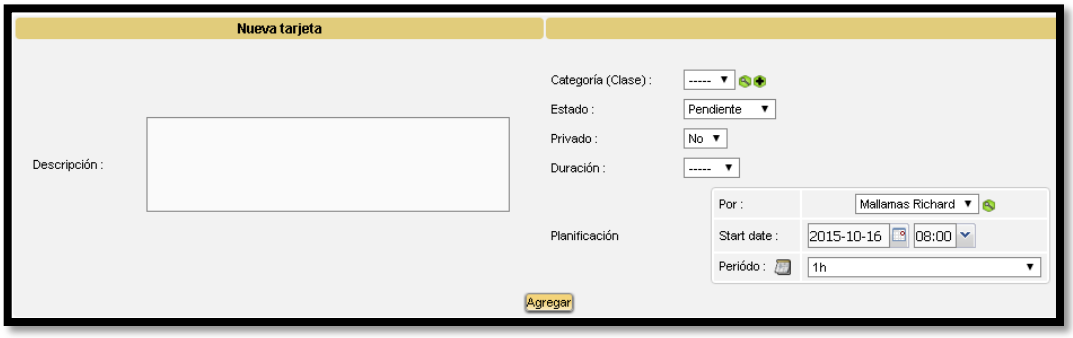


Figura C. 73 Plantilla de creación de tareas con fecha de ejecución

Y se nos guardara con el siguiente formato, en donde se encuentra la fecha de creación, la descripción, la duración, el autor, y la fecha en la que se realizará la tarea.

Figura C. 74 Formato de la tarea creada

Para ver las planificaciones que hemos asignado nos dirigimos al menú **Soporte**, y escogemos la opción **Planificación**, en la cual se nos desplegará una ventana que contiene un calendario con las tareas que hemos asignado en un cierto intervalo de tiempo, el cual podemos escoger en el menú de esta pantalla.

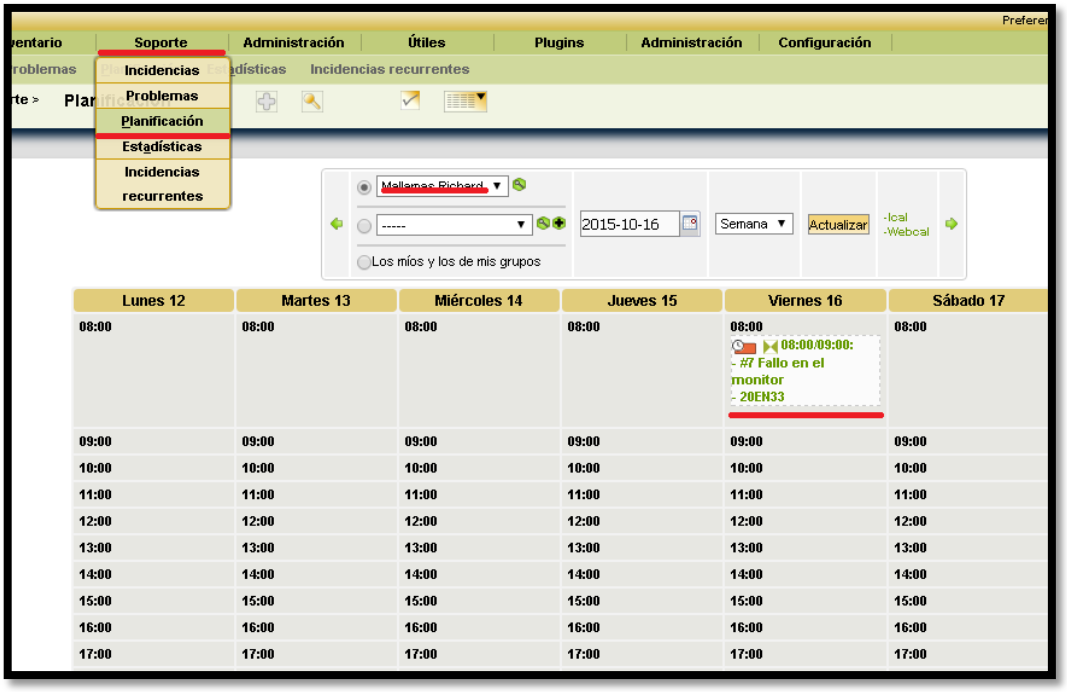


Figura C. 75 Menú Planificación

C.2.15. Estadísticas de las incidencias

Para mantener un control de nuestras incidencias, podemos entrar al menú **Soporte** en la opción **Estadísticas**, en este menú podemos seleccionar las estadísticas que deseamos visualizar, agregando la fecha en la que ocurrieron, o el nombre de quien las realizo, para tener un historial de lo ocurrido.

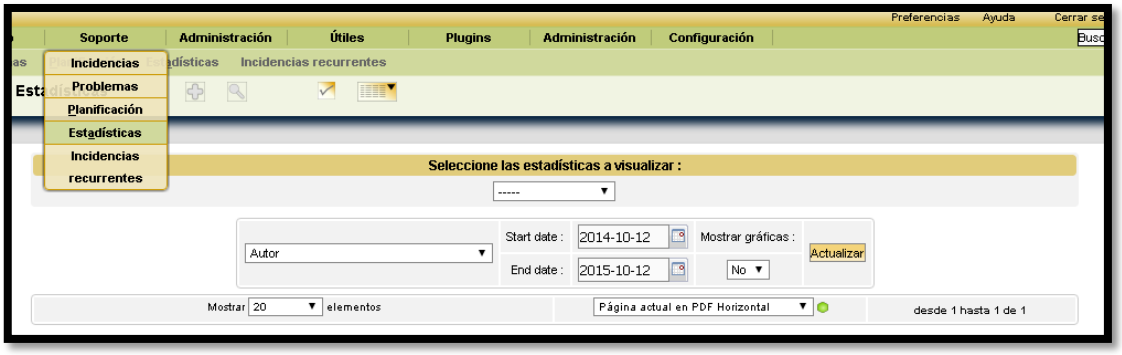


Figura C. 76 Menú Soporte con opción Estadísticas

Para el ejemplo elegiremos la opción **Por Incidencias** en la cual nos despliega las incidencias ya sea de forma individual o de manera grupal, dependiendo de la opción que escojamos en el menú desplegable, en esta opción nos desplegara información relevante de

las incidencias como: el nombre de quien la realizo la incidencia, la hora de llegada, la hora en que se dio la solución, y si deseamos exportar esta información a formato PDF damos click en el botón de luz verde ubicado en la parte central del menú. Esto nos ayuda para llevar un registro de que usuarios nos presentan más frecuentemente un problema o un incidente, permitiéndonos así detectar un problema a nivel personal o global para posteriormente planificar alguna solución.

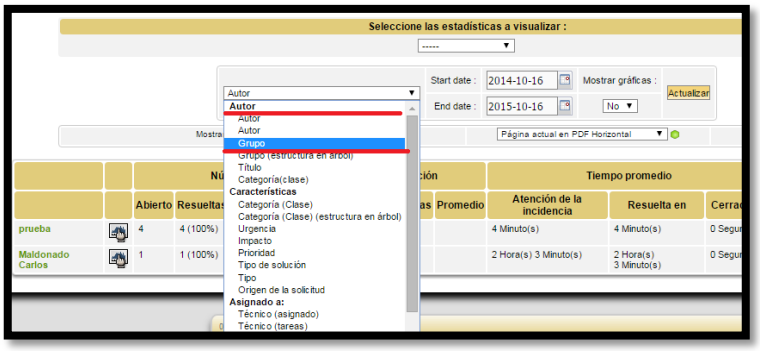


Figura C. 77 Desplegar Incidencias

De esta manera nos saldrá una inventario de los problemas resueltos, ya sea de forma o individual o grupal dependiendo de la elección antes realizada, y nos desplegará información relacionada con los tiempos de solución de problemas. También podemos ver gráficamente la evaluación de soluciones, esto lo realizaremos dando click en icono de la gráfica.

Figura C. 78 Ver gráficos de las estadísticas de los problemas resueltos

En esta opción nos grafica estadísticamente, el tiempo promedio de resolución que se les ha dado a las incidencias que han llegado en un determinado tiempo.

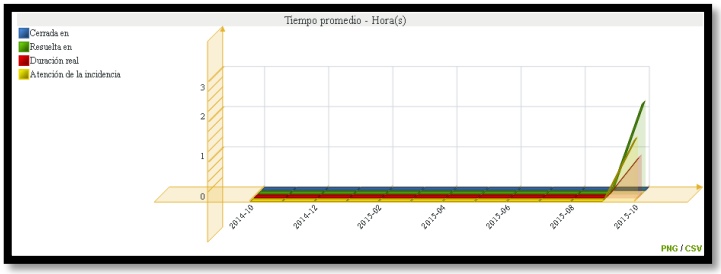


Figura C. 79 Gráfica de tiempo promedio de resolución de incidencias

C.2.16. Agregar un enlace externo al inventario

Para acceder a la configuración vamos al menú Configuración y luego a enlaces externos. En los enlaces externos, se configuran enlaces a ficheros que están asociados a los distintos elementos del inventario, en estos enlaces, se pueden poner los drivers de las impresoras, de esta manera si el técnico de soporte está instalando una impresora, en la aplicación donde tiene la incidencia de dicha impresora también tendrá los drivers para llevar a cabo su trabajo.

Para añadir un nuevo enlace pulsamos sobre el icono en agregar y se nos mostrará el siguiente formulario donde se configuran los enlaces externos.

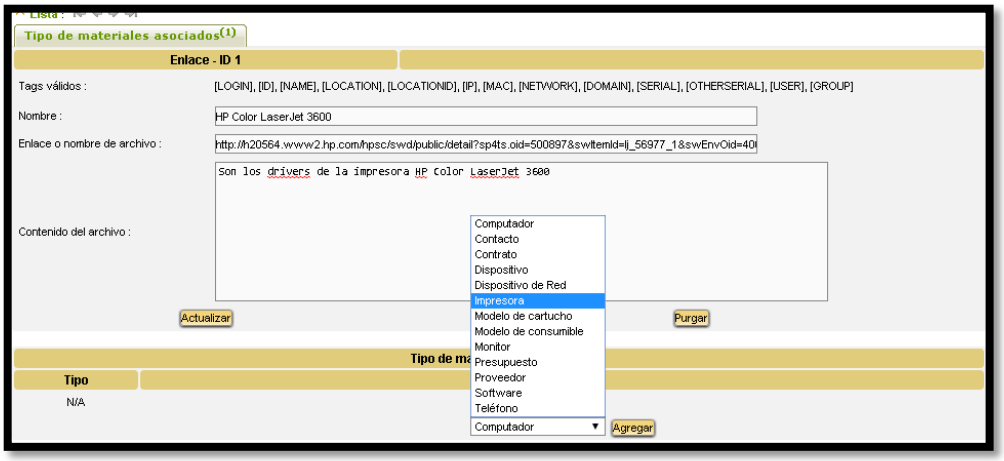


Figura C. 80 Enlaces externos

En este formulario le daremos un nombre al enlace para saber cuál es, así mismo pondremos una dirección válida y por ultimo escribiremos el contenido del fichero o la descripción del enlace.

Un enlace externo correcto sería el siguiente, que descarga de los Drivers Impresora HP LaserJet Color 3600dn desde página Web del fabricante.

Una vez que hemos rellenado la tarjeta con los datos del enlace externo, pulsamos el botón añadir, tras lo cual la tarjeta se cerrará, entonces para asociar el enlace que hemos creado anteriormente y asociarla lo que queramos, deberemos entrar nuevamente a la plantilla pulsando sobre el enlace que hemos creado

Este botón que hemos creado aparecerá en todas las impresoras que tengamos en el inventario, ya que el enlace se asocia al apartado Impresoras y no a una impresora en particular, lo mismo sucedería si la asociamos a ordenadores, periféricos, clientes, etc.

C.2.17. Actualizar computadores gestionados con OCS-Inventory

Si se añaden más usuarios y deseamos actualizar el inventario realizado en OCS-Inventory con la plataforma GLPI, nos dirigimos al menú **Inventario** en la opción **Computadores.**

Figura C. 81 Menú Inventario-Computadores

Una vez dentro de la ventana, nos dirigimos a la parte inferior izquierda, y pulsamos en **Seleccionar todo** y en el menú desplegable, escogemos la opción **Forzar la sincronización**, de esta manera se actualizarán los datos que se estén inventariando en OCS-Inventory.

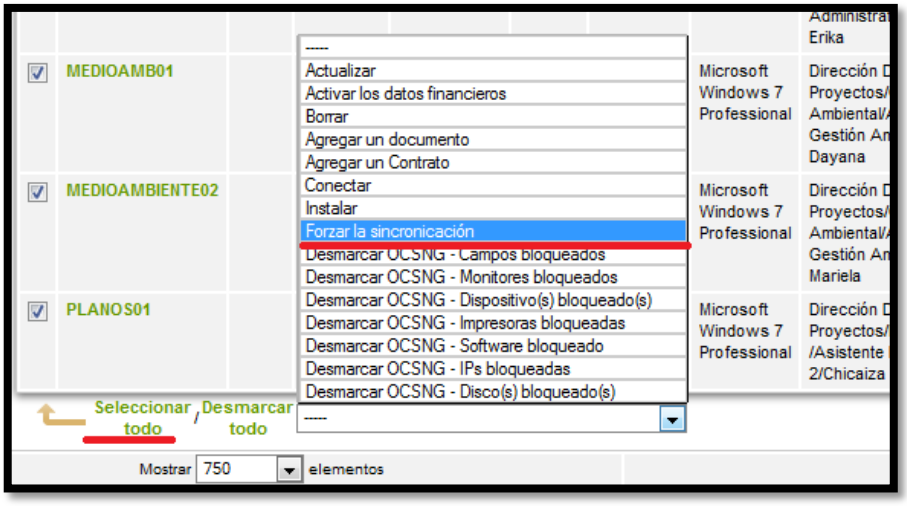


Figura C. 82 Actualización de los datos de OCS-Inventory

C.2.18. Realizar copia de seguridad en GLPI

Para realizar una copia de seguridad de los datos almacenados en la plataforma, nos dirigimos al menú Administración y elegimos la opción Mantenimiento.

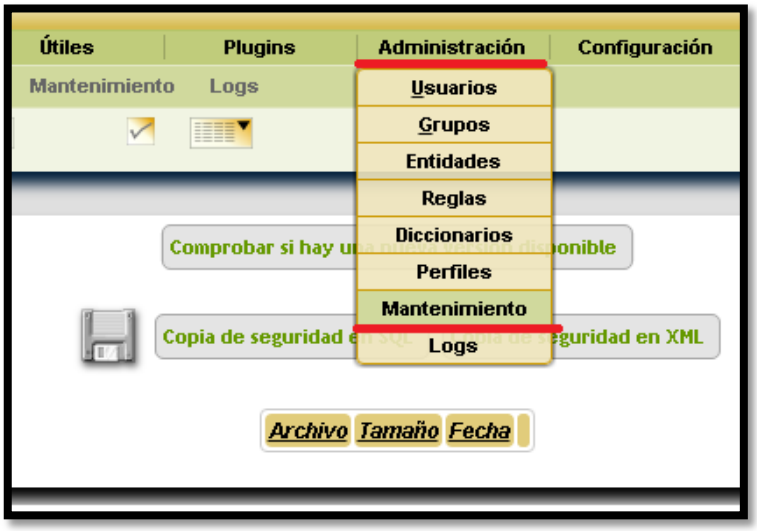


Figura C. 83 Menú Administración-Mantenimiento

En esta ventana escogemos la opción **Copia de seguridad en SQL,** luego nos desplegará una ventana en la cual nos pedirá confirmación para realizar la copia de seguridad y damos click en Aceptar, para que se guarden los cambios.

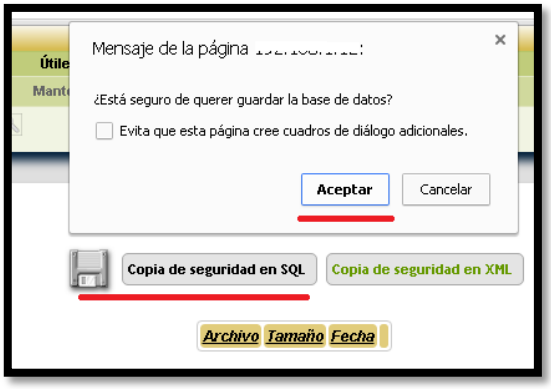


Figura C. 84 Guardar copia de seguridad

Seguidamente nos desplegará la siguiente ventana en la cual podremos observar la base de datos que acabamos de realizar. Tenemos las opciones de borrar, reemplazar, o descargar.

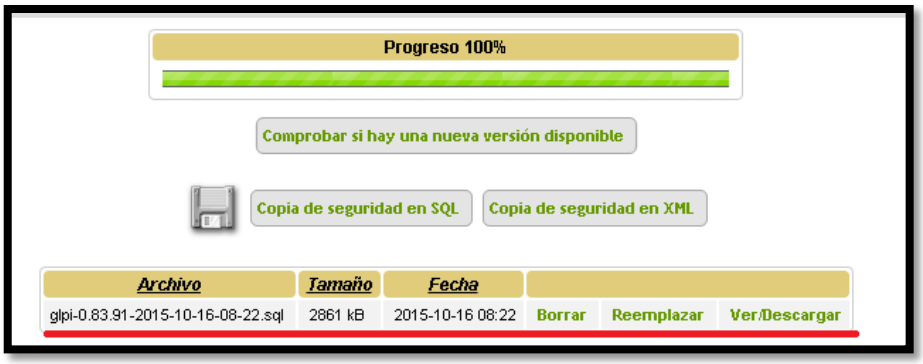


Figura C. 85 Visualización de la copia de seguridad

C.2.19. Impresión de documentos

Podemos realizar la impresión tanto del inventario como de las incidencias, para la impresión del inventario nos dirigimos al menú **Inventario** en la opción **Computadores**.

Figura C. 86 Menú Inventario-Computadores

Al acceder a la opción Computadores dentro del menú Inventario, se nos mostrará esta ventana, en el cual tenemos uno o varios pc en este menú, elegimos el pc del cual deseamos imprimir el inventario.

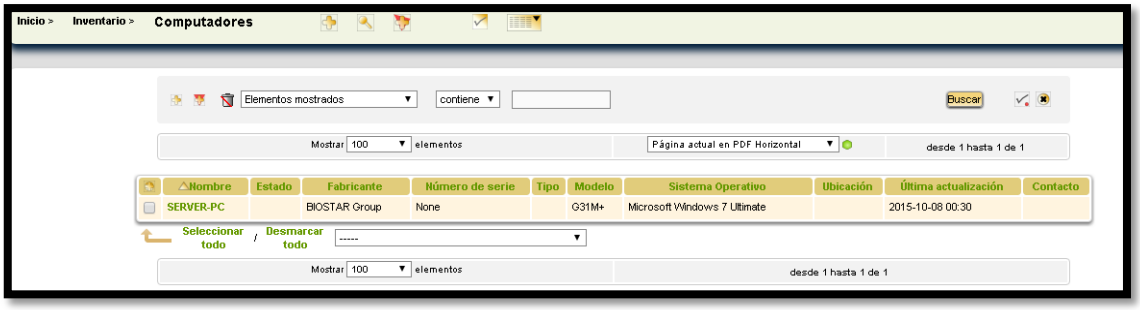


Figura C. 87 Menú Computadores

Una vez dentro del computador que deseamos imprimir el inventario escogemos la pestaña **Print to pdf**, y escogemos las opciones que deseamos imprimir, en este caso solo elegimos la opción computador y damos click en el botón **Print**.

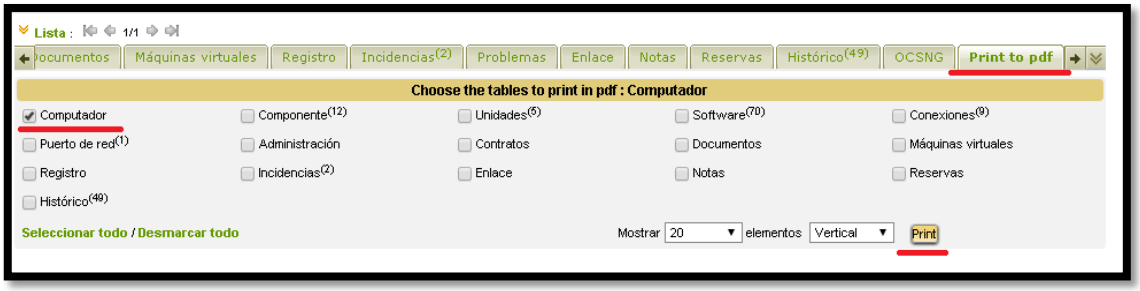


Figura C. 88 Opción Print to pdf

Nos mostrará la plantilla de impresión de la siguiente manera:

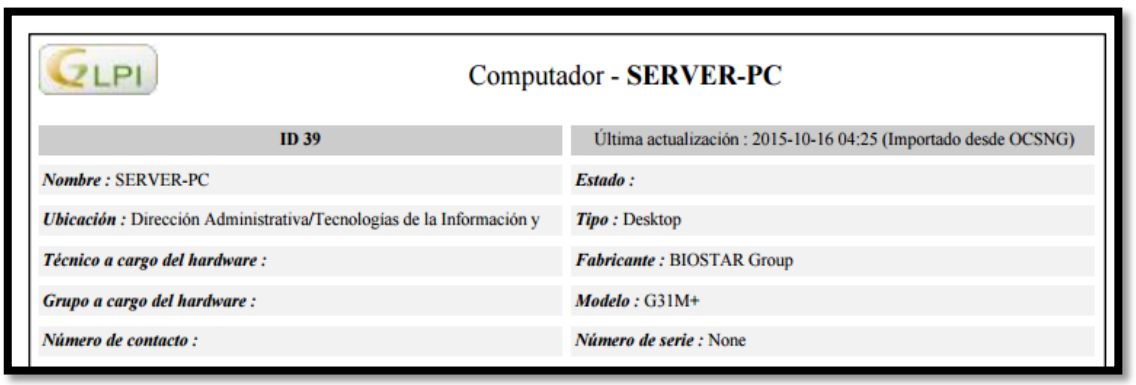


Figura C. 89 Plantilla de impresión

De igual forma para la impresión de incidencias nos dirigimos al menú **Soporte** en la opción **Incidencias.**

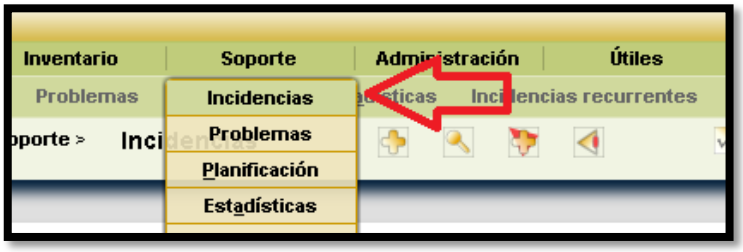


Figura C. 90 Menú Incidencias

Para la revisión de incidencias la ventana por defecto nos saldrá con las incidencias más recientes sin resolver, si deseamos visualizar algunas incidencias en específico ya sea por usuario o por grupo, damos click en el menú desplegable:

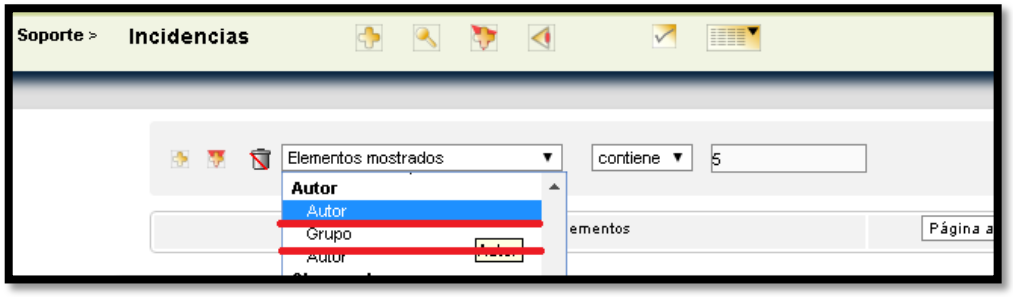


Figura C. 91 Buscar incidencias en específico

Una vez dentro de la incidencia que deseamos imprimir el inventario escogemos la pestaña **Print to pdf**, y escogemos las opciones que deseamos imprimir, en este caso solo elegimos la opción incidencia y damos click en el botón **Print**.

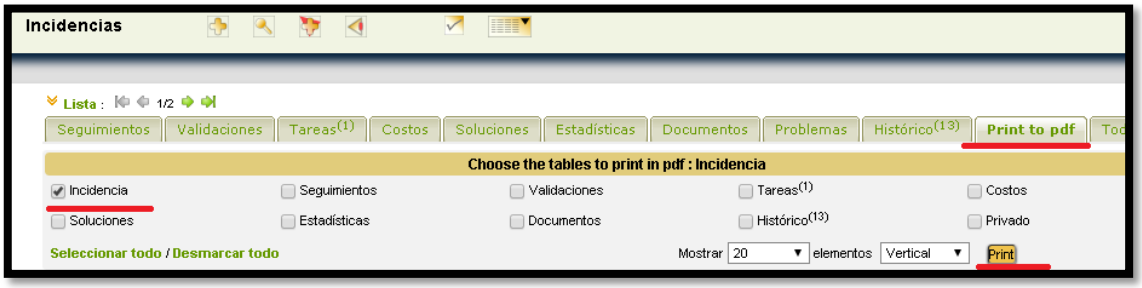
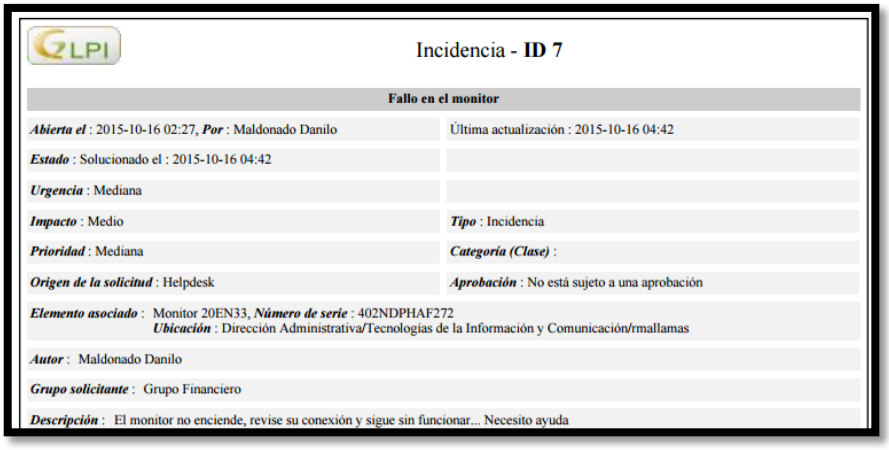


Figura C. 92 Opción Print to pdf

Nos mostrará la plantilla de impresión de la siguiente manera:



Incidencia - **ID 7**

Fallo en el monitor	
Abierta el : 2015-10-16 02:27, ***Por*** : Maldonado Danilo	Última actualización : 2015-10-16 04:42
Estado : Solucionado el : 2015-10-16 04:42	
Urgencia : Mediana	
Impacto : Medio	***Tipo*** : Incidencia
Prioridad : Mediana	***Categoría (Clase)*** :
Origen de la solicitud : Helpdesk	***Aprobación*** : No está sujeto a una aprobación
Elemento asociado : Monitor 20EN33, ***Número de serie*** : 402NDPHAF272 ***Ubicación*** : Dirección Administrativa/Tecnologías de la Información y Comunicación/rmallamas	
Autor : Maldonado Danilo	
Grupo solicitante : Grupo Financiero	
Descripción : El monitor no enciende, revise su conexión y sigue sin funcionar... Necesito ayuda	

Figura C. 93 Plantilla de impresión

C.3. MANUAL DE USUARIO DE LA PLATAFORMA GLPI

C.3.1. Acceso al Sistema de gestión de incidencias GLPI

GLPI es una herramienta que permite registrar y administrar inventarios tanto de hardware como de software de los equipos de EMAPA –I, lo que incluye también la atención de incidencias y solicitudes de servicio que necesiten soporte técnico inmediato.

Las ventajas de esta herramienta son:

- ✓ Gestión de recursos informáticos
- ✓ Soporte Técnico para ofrecer soluciones lo más oportunamente posible.

- Para acceder al sistema, ingresamos la dirección **glpiemapai.emapai.ec/glpi** en nuestro navegador de preferencia, el que puede ser Google Chrome o Firefox, y a continuación nos mostrará la siguiente pantalla:

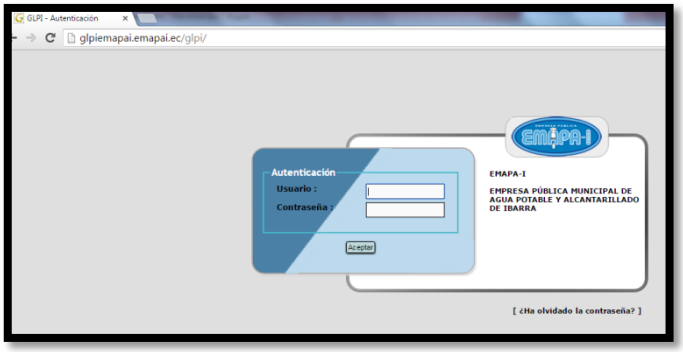


Figura C. 94 Ingreso al sistema GLPI

- En la pantalla que nos muestra nos pedirá ingresar nuestros datos de usuario y contraseña, los cuales tienen el formato siguiente:

El nombre de usuario y contraseña, se deben ingresar en minúsculas, asociando la inicial del primer nombre junto al primer apellido. Para lo cual se presenta el siguiente ejemplo:

Nombre: Danilo Maldonado
Nombre de usuario: dmaldonado(la inicial del primer nombre junto al primer apellido)
Contraseña: dmaldonado(la inicial del primer nombre junto al primer apellido)

- Una vez ingresados nuestros datos, hacemos click en el botón **Aceptar.**

Figura C. 95 Ingreso del nombre de usuario y contraseña

C.3.2. Edición de contraseña y preferencias de usuario

- Como primer paso, editamos a conveniencia nuestros datos personales, para esto escogemos la opción **Preferencias,** que se encuentra en la parte superior derecha.

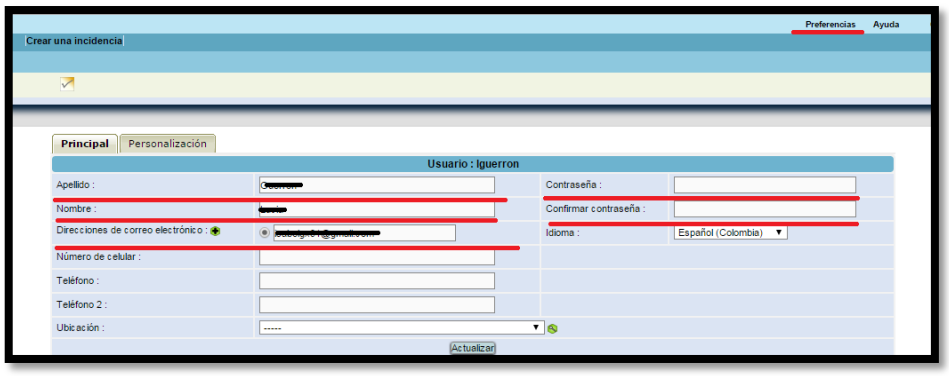


Figura C. 96 Opción-Preferencias

- En esta ventana podemos editar nuestros datos personales y agregar información adicional según lo desee el usuario, entre las opciones que se pueden mencionar son las siguientes:

  - ✓ Nombre y Apellido
  - ✓ Dirección de correo electrónico
  - ✓ Número de celular/teléfono
  - ✓ Agregar una nueva contraseña

Si realizamos algún cambio en la información del usuario damos click en el botón de **Actualizar**, que está en la parte inferior del menú, para que se guarden los cambios realizados.

C.3.3. Creación de una incidencia

- Para crear un requerimiento de recursos informáticos o reportar un problema con nuestro computador, hacemos click en la opción Crear una **Incidencias**, ubicada en la parte superior izquierda del menú.

Figura C. 97 Crear una incidencia

- Se nos mostrará la siguiente pantalla en la que se debe tomar en cuenta los siguientes aspectos.

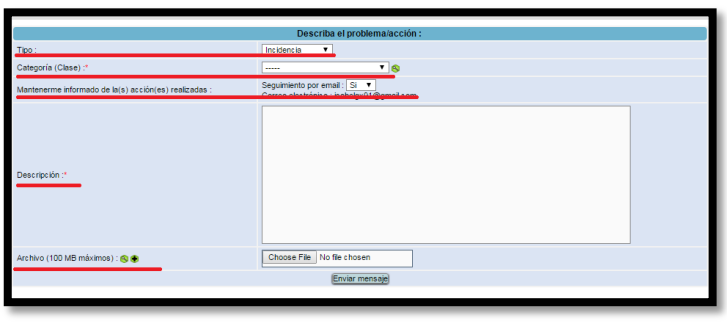


Figura C. 98 Plantilla para crear la incidencia

A continuación se describe cada campo de la plantilla:

- **Tipo**: Se debe escoger entre si es una **Incidencia** (comunicar la falla de un servicio/equipo) o un **Requerimiento** (solicitar un equipo o un reporte al administrador/técnico).

Figura C. 99 Opción Tipo

- **Categoría:** Se debe escoger de la lista despegable, la categoría que más se ajusta a la necesidad que tenga el usuario.

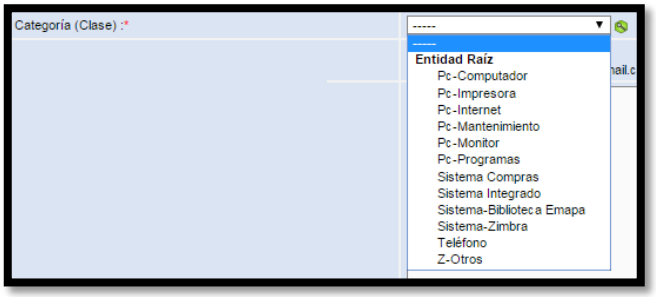


Figura C. 100 Opción Clase

- **Mantenerme informado de las acciones realizadas:** Esta opción nos permite recibir avisos al correo electrónico acerca de cómo se encuentra la incidencia que creamos.

Figura C. 101 Recibir notificaciones al correo

- **Descripción:** Aquí se realiza una descripción detallada y clara sobre su requerimiento/incidencia.

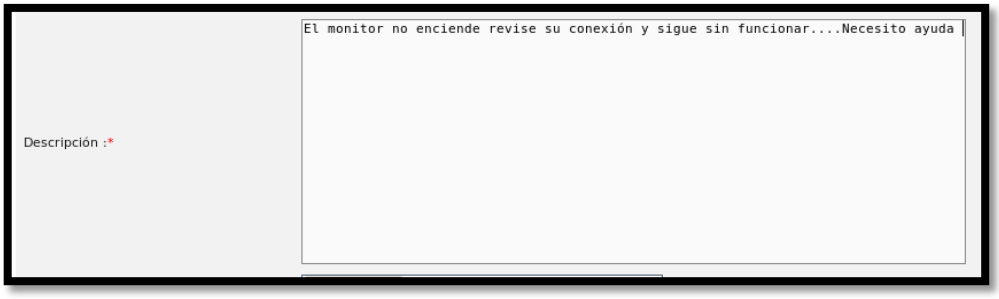


Figura C. 102 Opción Descripción

- **Archivo:** Se puede adjuntar un archivo (máximo 100MB) con información sobre la petición, en el que podemos enviar una captura de pantalla de lo que esté sucediendo, o algún documento referente a la situación de la incidencia.

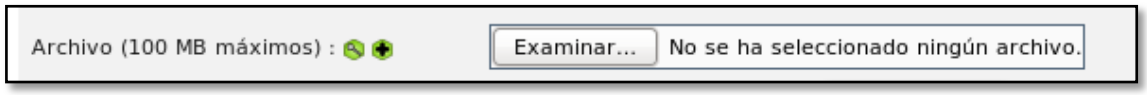


Figura C. 103 Opción Archivo

Y estaríamos listos para enviar incidencias o requerimientos a través de la plataforma GLPI. Una vez llenado todos los campos descritos anteriormente damos click en el botón **Enviar mensaje** ubicado en la parte inferior de la pantalla, para guardar los cambios realizados y se enviará la incidencia al administrador de la red.

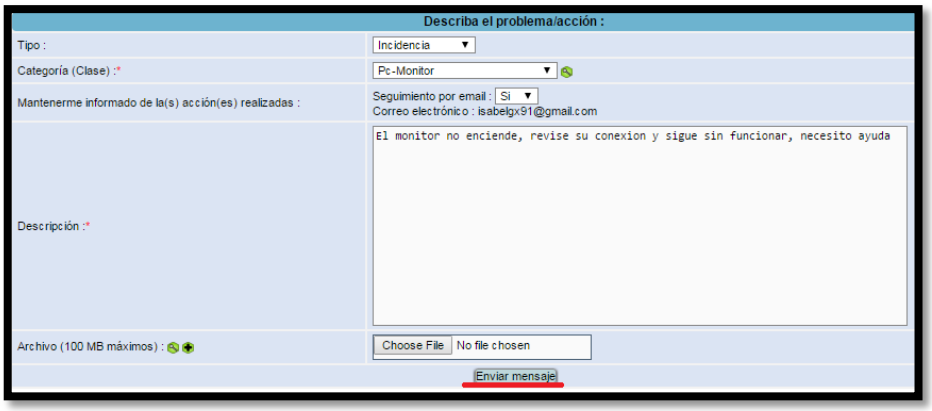


Figura C. 104 Enviar incidencia

Y nos saldrá un aviso de que el mensaje fue enviado exitosamente.

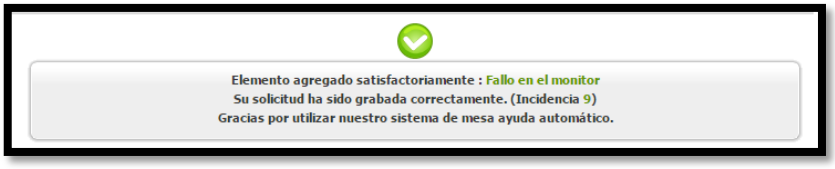


Figura C. 105 Confirmación del envío de la incidencia

C.3.4. Revisión de una incidencia

Una vez creada nuestra incidencia para visualizar las actividades y darle un seguimiento hacemos click en la opción **Inicio** y nos desplegara el menú de incidencias. En donde nos mostrará las siguientes opciones:

- **Nueva:** nos mostrará la incidencia más reciente que hemos realizado
- **En proceso:** nos mostrará la incidencia que está siendo procesada por el administrador
- **En espera:** el personal de soporte puede dejar la incidencia en estado de espera cuando no depende directamente del área de soporte. Por ejemplo: reserva de materiales, actualizaciones del sistema, etc.
- **Resuelto:** aquí nos indicará la solución que el personal encargado habría asignado a nuestras incidencias.
- **Cerrado:** las incidencias que se resuelven se asignaran a estado de cerradas.
- **Eliminado:** el personal encargado puede determinar si elimina o no una incidencia, dependiendo de la situación que crea conveniente.

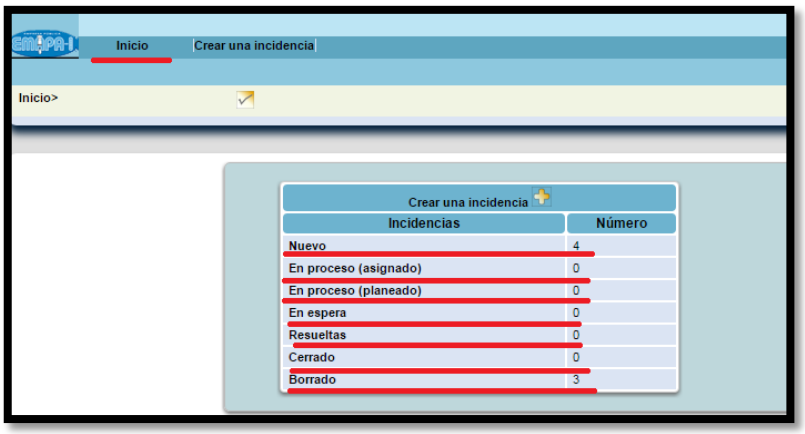


Figura C. 106 Vista de incidencias

C.4. MANUAL DE USUARIO DE LA PLATAFORMA ZABBIX

C.4.1. Guía rápida de los menús existentes en Zabbix

El monitoreo y administración de los equipos de la red con Zabbix se lo realiza mediante la interfaz web, la cual nos permite organizar, agregar y configurar las opciones disponibles en esta plataforma como las gráficas y las alarmas que deseamos notificar.

En primer lugar luego de haber ingresado con nuestra cuenta de usuario tenemos la pantalla principal en la cual nos muestra el estado general del sistema, indicándonos por ejemplo cuantos equipos tenemos agregados y cuántos de ellos presentan alguna falla.

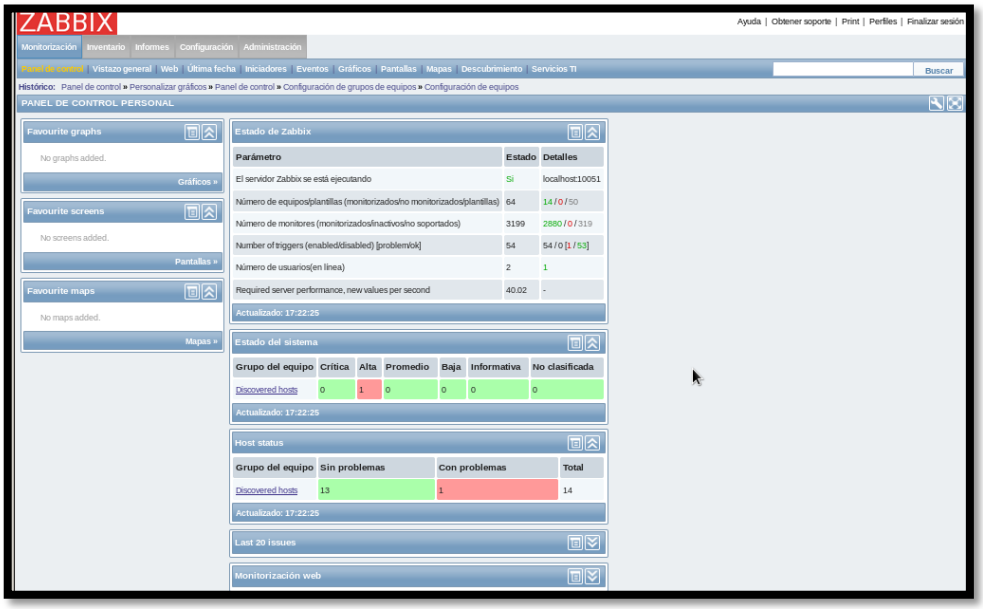


Figura C. 107 Pantalla principal Zabbix

Como se puede observar, las pestañas de inicio son cinco las cuales se presentan a continuación:

Figura C. 108 Menú principal de Zabbix

- **Monitorización:** Esta categoría contiene enlaces relacionados con la monitorización de los equipos que agregamos al software. En este menú se presentan los datos, los problemas existentes y los gráficos construidos en base a la información recopilada. Los submenús que se encuentran esta pestaña son los siguientes:
    - **Panel de control:** Aquí veremos información como el número de equipos monitorizados, el estado de cada equipo de la plataforma, los últimos eventos ocurridos, etc.

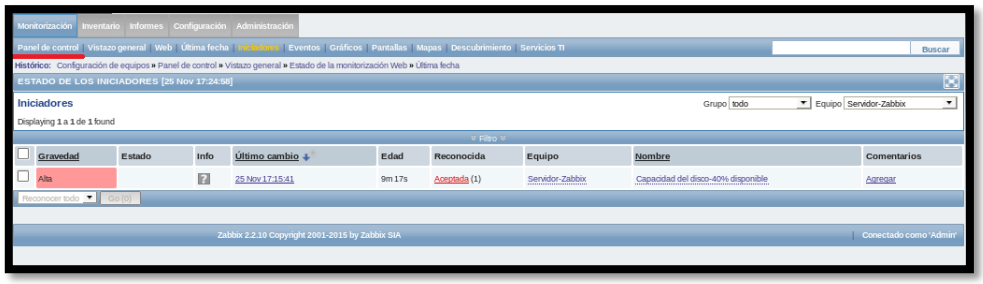


Figura C. 109 Menú Panel de control Zabbix

- **Gráficos**: Aquí podemos observar los gráficos que se han creado para cada equipo introducido en la plataforma.

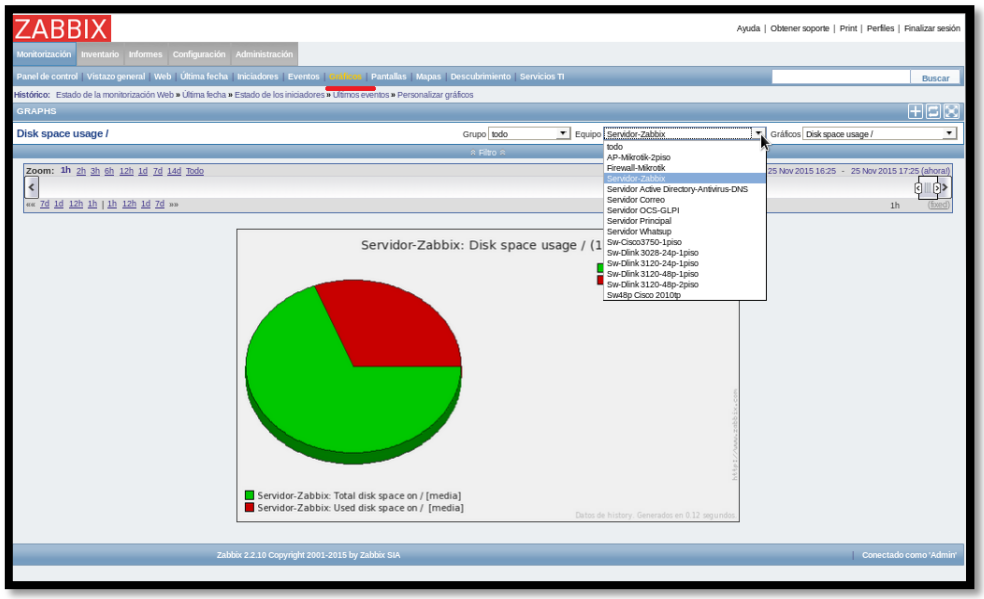


Figura C. 110 Menú gráficos Zabbix

- **Mapas:** En esta pestaña podremos ver los mapas que previamente hayamos creado.

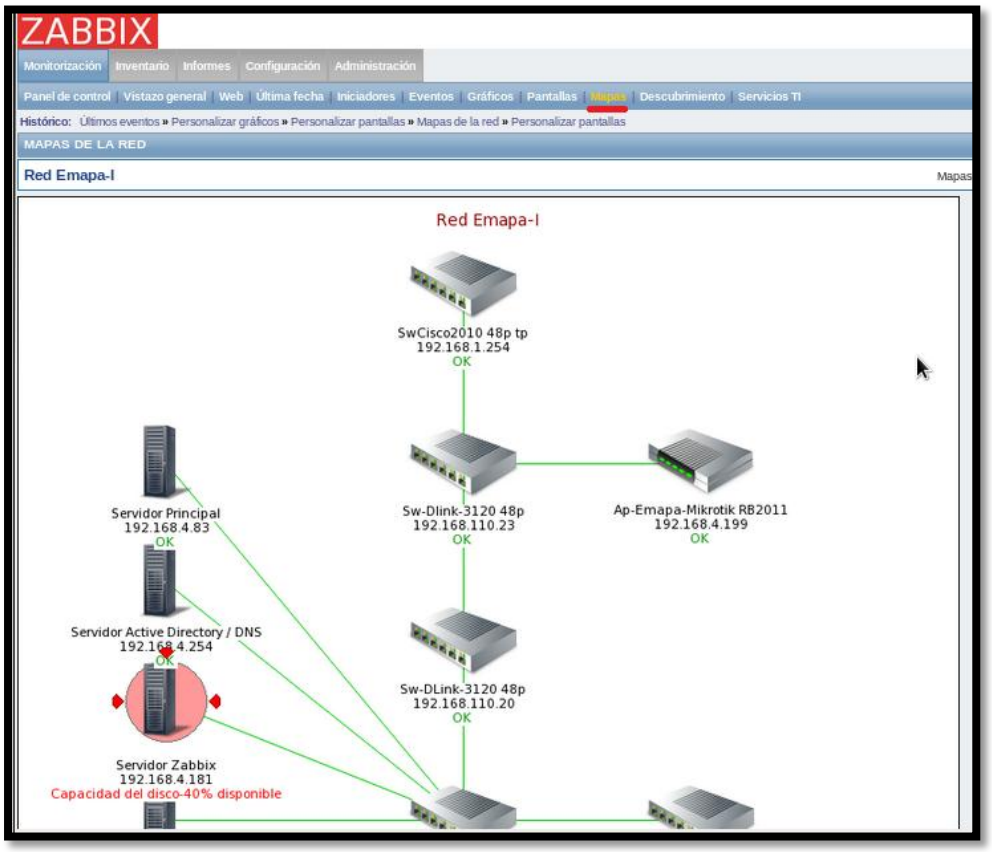


Figura C. 111 Menú mapas Zabbix

- **Descubrimiento:** Nos muestra aquí el estado de las reglas de descubrimiento que se hayan definido para identificar nuevos equipos conectados a la plataforma.

- **Inventario:** Si agregamos datos de inventario a los equipos, esta opción nos permite la visualización de los datos de inventario que hayamos ingresado
- **Informes:** En este menú podemos obtener un informe detallado de los datos que se estén recopilando. Los submenús que se encuentran esta pestaña son los siguientes:
  - **Estado de Zabbix:** Aquí podemos visualizar el estado de la plataforma con los siguientes datos: el número de equipos monitorizados, número de parámetros monitorizados, eventos generados y alarmas.

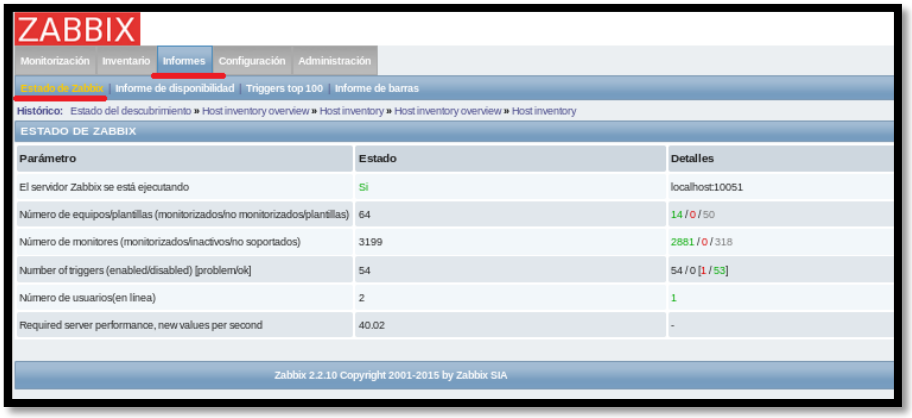


Figura C. 112 Menú Estado de Zabbix

- **Informe de disponibilidad:** Podremos visualizar el porcentaje de tiempo que las alarmas han estado activas o inactivas, nos informa sobre la disponibilidad de cada equipo monitorizado.

Figura C. 113 Informe de disponibilidad Zabbix

- **Trigger top 100:** Aquí se muestra una lista con el nombre de los 100 iniciadores de alarmas que han registrado más actividad en la plataforma.

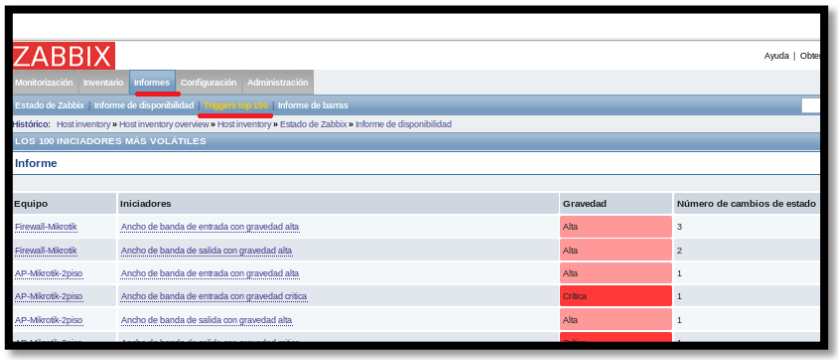


Figura C. 114 Menú Trigger top 100 Zabbix

- **Configuración:** En este menú podremos agregar los dispositivos, los parámetros a monitorizar, los mensajes de notificación en caso de alertas, la programación de, etc. Los submenús que se encuentran esta pestaña son los siguientes:
    - **Grupos de equipos:** En esta sección se podrán crear grupos dentro de los cuales organizar los equipos que ingresemos a la plataforma.

Figura C. 115 Menú grupo de equipos Zabbix

- **Plantillas:** En este menú podremos observar las plantillas disponibles para usar en los equipos que deseemos agregar, son plantillas de ayuda donde se encuentran los parámetros a monitorear para diferentes equipos.

Figura C. 116 Menú plantillas Zabbix

- **Equipos:** Desde aquí se introducen los equipos que se vayan a monitorizar en la plataforma.

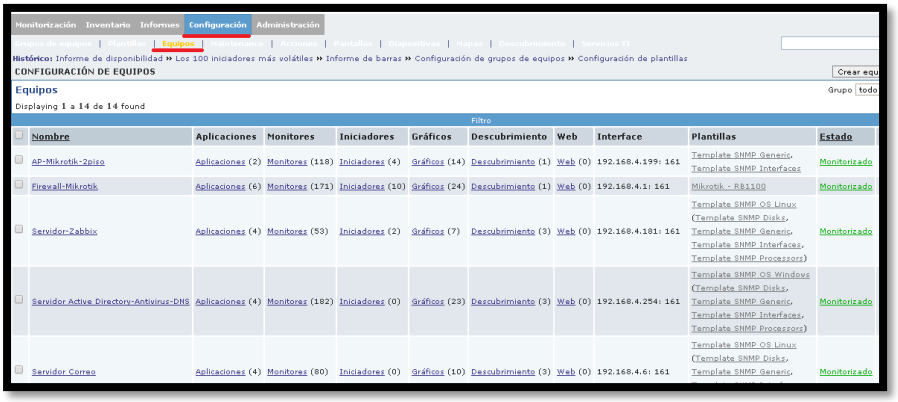


Figura C. 117 Menú Equipos Zabbix

- **Acciones:** en este menú podemos crear, borrar, activar y desactivar las notificaciones por ejemplo: envío de e-mail, o mensaje de texto, asociadas a una determinada alarma. En este menú podremos personalizar las condiciones bajo las cuales se ejecutarán las alarmas.

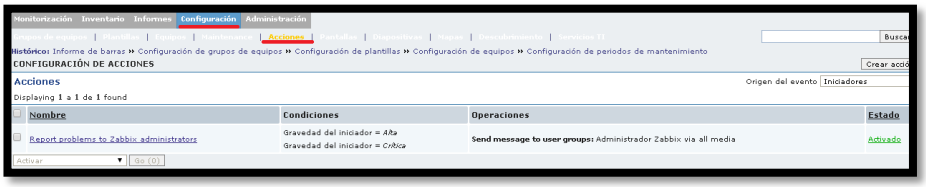


Figura C. 118 Menú Acciones Zabbix

- **Mapas:** Aquí se pueden crear mapas con los que representar el estado de la plataforma a través de iconos e imágenes

- **Administración:** En este menú podemos personalizar los aspectos internos de Zabbix tales como los métodos de autenticación, los usuarios, los permisos. Los submenús que se encuentran esta pestaña son los siguientes:
  - **Usuarios:** Aquí añadiremos y configuraremos los usuarios o grupos de usuarios de la herramienta Zabbix.
  - **Tipo de medios:** En esta pestaña definimos los medios a través de los cuales se comunica Zabbix con los usuarios cuando se produce un evento en el sistema.

Figura C. 119 Menú tipo de medios Zabbix

- **Scripts:** En este menú el usuario puede crear scripts a ejecutar sobre los equipos de la plataforma.
- **Auditoría:** Refleja los cambios llevados a cabo en la configuración de Zabbix y un registro de los inicios de sesión a través de la interfaz Web.

Figura C. 120 Menú Auditoria de logs Zabbix

- **Notificaciones:** Este menú muestra los mensajes enviados a través de los medios configurados previamente

C.4.2. Administrar cuentas y agregar un equipo para monitorear en Zabbix

En la pestaña Administración opción Usuarios se recomienda eliminar las cuentas que vienen instaladas por defecto y dejar únicamente la cuenta que va a acceder el administrador de la red.

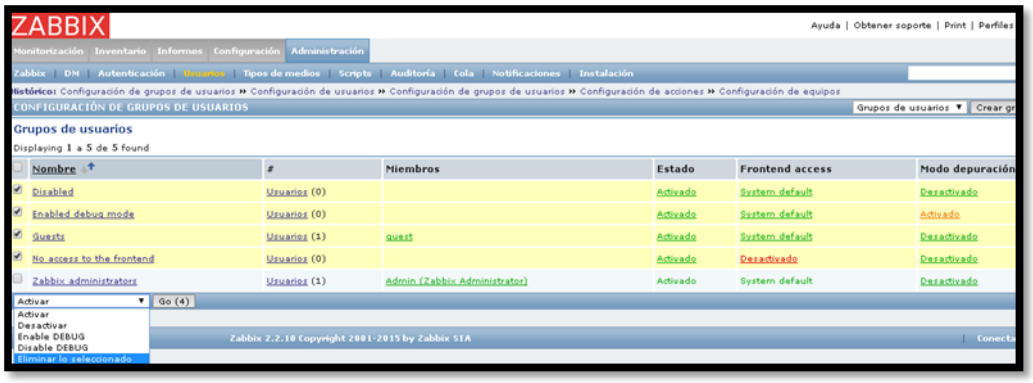


Figura C. 121 Eliminando cuentas por defecto en el servidor de Zabbix

Además en la ventana de Administración se puede editar los datos personales del administrador, o agregar cierta información como:

- Nombre Completo
- Cambiar Idioma
- Agregar una nueva contraseña

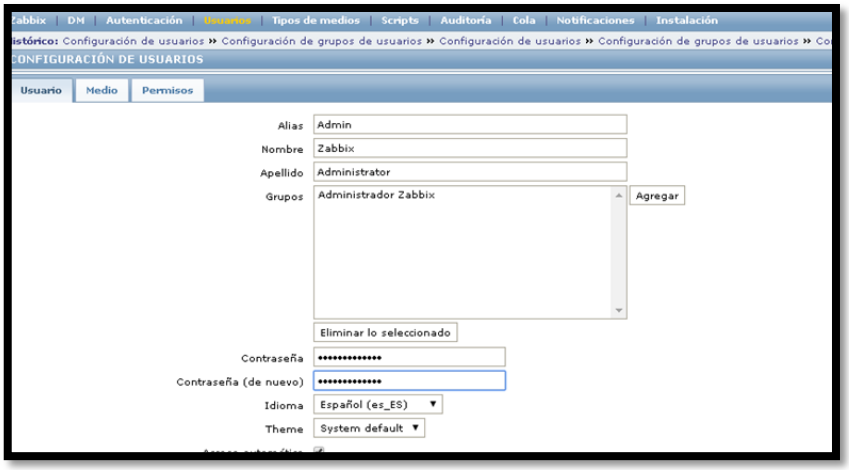


Figura C. 122 Editando campos en la cuenta del Administrador

Una vez realizada la configuración inicial se visualiza el panel de control con el estado del servidor de Zabbix, así como estadísticas o acciones de monitoreo que al momento se están ejecutando en el servidor

Figura C. 123 Panel de control del servidor Zabbix

Para empezar a configurar los equipos en el servidor de Zabbix es necesario agregarlos, seleccionando la pestaña Configuración y la opción de Equipos y dar click en el botón Crear Equipos.

Figura C. 124 Agregando equipos al servidor Zabbix

A continuación se desplegará la siguiente ventana de Equipos en cuyos campos se debe ingresar la información del dispositivo.

- Nombre del Host
- Dirección IP
- Puerto SNMP

Una vez añadida esta información dar click en el botón Guardar.

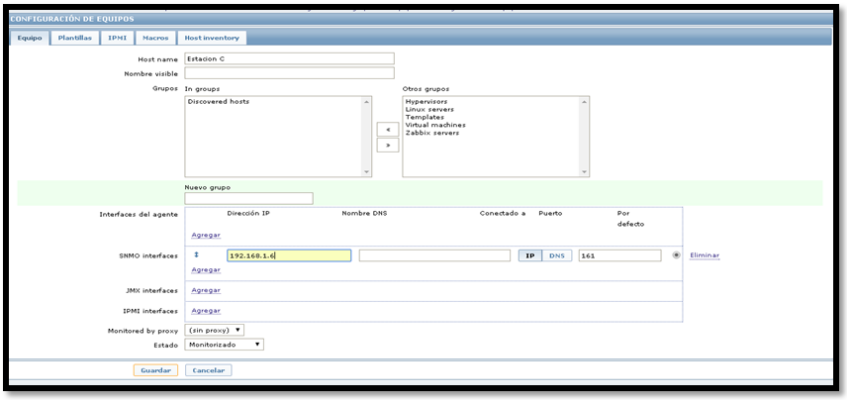


Figura C. 125 Ingresando información del host y especificando dirección IP y # puerto snmp

En la misma ventana de configuración de Equipos, seleccionar la pestaña Plantillas, para especificar una plantilla SNMP en los equipos que tengan sistema operativo Windows/ Linux que vienen predefinidas y dar click en el botón Guardar.

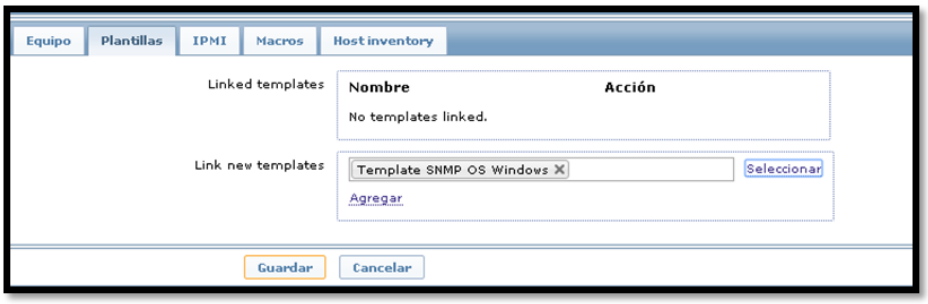


Figura C. 126 Seleccionando una plantilla SNMP para los equipos con S.O Windows

El monitoreo de los dispositivos se realizará a través de protocolo SNMP por lo tanto es necesario agregar la comunidad SNMP, escogiendo la pestaña Configuración, Equipos y la opción de Macros en cuyo Macro se debe ingresar esta condición: {$SNMP_COMMUNITY} y en Estado el nombre de la comunidad SNMP, hecho esto Guardar los cambios.

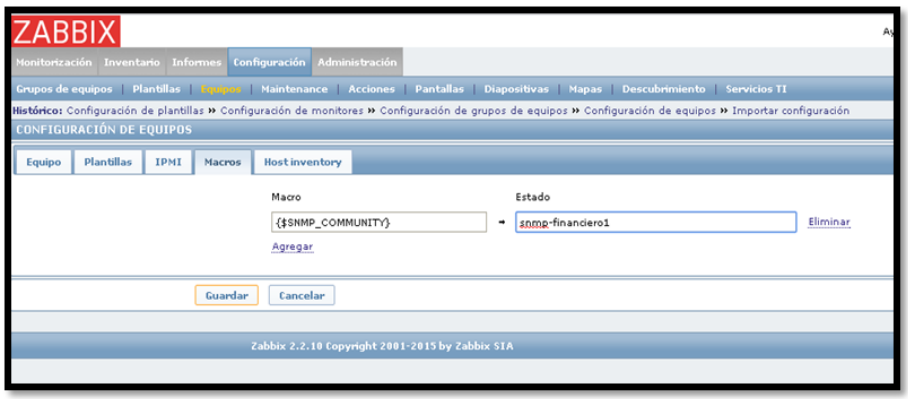


Figura C. 127 Especificando comunidad SNMP para los equipos

Si la configuración de los equipos, se realizó correctamente esperar unos minutos y verificar que el estado de la monitorización SNMP cambia a color verde (disponible)

Figura C. 128 Verificando el estado de la monitorización SNMP del equipo

Para observar los indicadores del equipo anteriormente agregado, escoger la pestaña Monitorización y la opción de Indicadores, se desplegara una lista con todos los parámetros indicando si alguno de estos tiene algún problema y necesita ser revisado.

Figura C. 129 Visualización de problemas en los indicadores de monitoreo del equipo

Si se quiere observar el registro histórico de los indicadores escoger la opción Monitorización, en Eventos para verificar la fecha, el estado, los problemas y la gravedad de cada incidencia registrada.

Figura C. 130 Registro histórico de los indicadores generados en el host

En la pestaña Monitorización y en la opción Gráficos se puede visualizar las gráficas que generan cada uno de los parámetros que fueron configurados en el equipo.

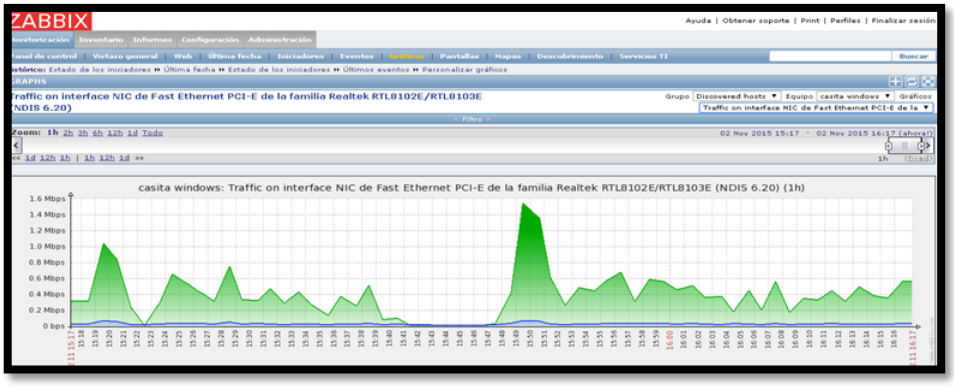


Figura C. 131 Gráfico que indica el tráfico Mbps en la interface Ethernet conectado al host

Además es posible agregar cada dispositivo registrado en el servidor Zabbix, de manera que se pueda construir un mapa topológico con todos los dispositivos de la red que se desee monitorear.

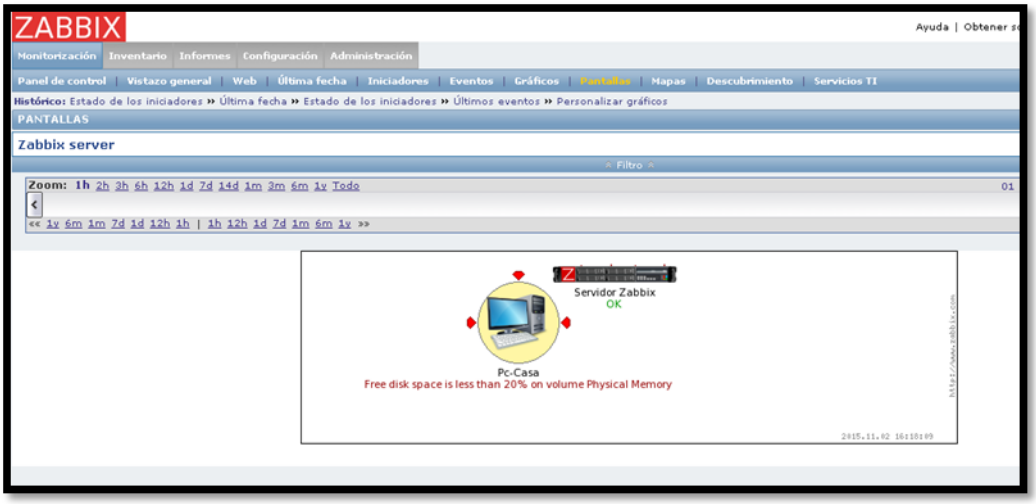


Figura C. 132 Visualización gráfica del dispositivo agregado en el servidor Zabbix

Los mapas nos ayudan a tener una visión centralizada de los equipos que se están monitoreando, dándonos la posibilidad de visualizar el estado de cada equipo de una manera gráfica. Para elaborar los mapas topológicos nos dirigimos al menú configuración en la opción Mapas.

Figura C. 133 Opción Mapas en Zabbix

En primer lugar procedemos a darle un nombre y personalizar el tamaño en el que deseemos que nos muestre el mapa.

Figura C. 134 Tamaño del mapa en Zabbix

Seguidamente nos mostrará un pequeño menú en la parte superior de esta opción en donde la opción Icono nos indica si deseamos agregar o quitar un nuevo dispositivo al mapa, y la opción vinculo que nos da la opción de enlazar 2 dispositivos

Figura C. 135 Menú de la configuración de mapas

Al ingresar un nuevo icono al mapa, nos pedirá una serie de opciones que nos ayudaran a personalizarlo a nuestro gusto.

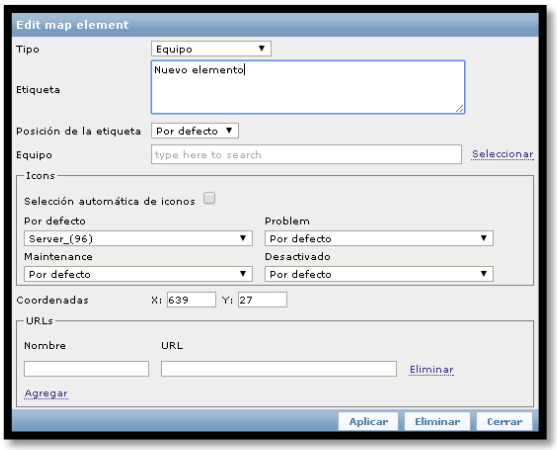


Figura C. 136 Opciones del icono en mapas

En la opción tipo podremos indicar si se trata de un nuevo equipo que deseamos ingresar o si se trata de una imagen, o anexar un mapa sobre el mapa que estamos creando.

En la opción etiqueta podemos agregar una pequeña descripción sobre el equipo que estamos creando por ejemplo el nombre del equipo, la marca, o su dirección IP para encontrarlo más rápidamente.

En la opción equipo podremos escoger uno de los dispositivos que estamos monitoreando.

En la opción icono podemos escoger la forma del icono que deseamos que nos aparezca en pantalla, en los cuales puede ser una nube, un router encriptado, un firewall, servidor, entre otros.

Como por ejemplo nos puede quedar de la siguiente manera:

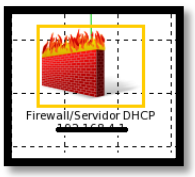


Figura C. 137 Icono del mapa en Zabbix

C.5. MANUAL DE USUARIO DE LA PLATAFORMA CACTI

C.5.1. Visualizar los equipos agregados en Cacti

Ingresamos al servidor Cacti y nos registramos para acceder.

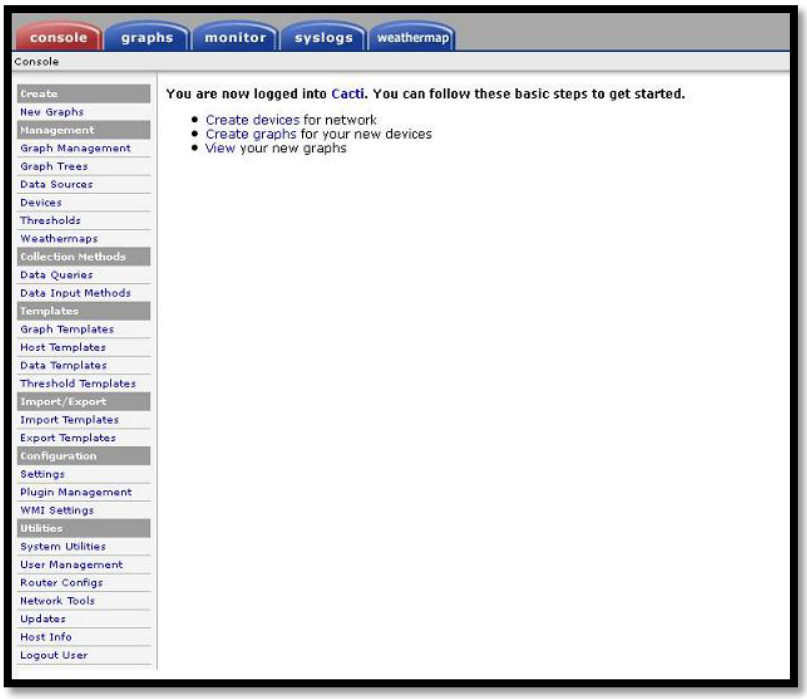


Figura C. 138 Pantalla inicial Cacti

Para observar los elementos agregados en la plataforma Cacti, nos dirigimos a la pestaña Console, en el titulo Management y la opción Devices, de esta manera nos aparecerá una pantalla como esta:

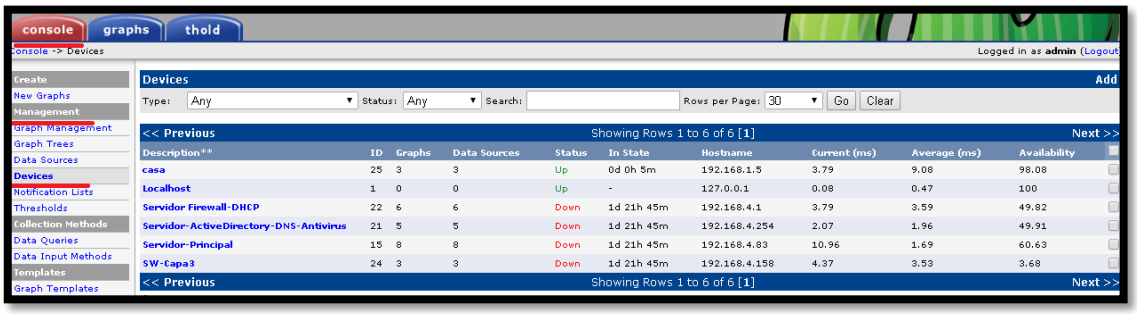


Figura C. 139 Lista de equipos ingresados a Cacti

Para ver detalladamente los parámetros con los que cuenta por ejemplo: dirección IP, comunidad, descripción, etc. bastará con ingresar en el equipo correspondiente.

C.5.2. Ingresar nuevos equipos a la plataforma

Para agregar un nuevo equipo a la plataforma damos click en el botón "Add" y nos aparecerá una pantalla como la siguiente, donde se describen los parámetros más importantes:

Description: Agregamos una descripción para el nuevo dispositivo
Hostname: Agregamos el nombre del dispositivo o ingresamos la dirección IP.
Host Template: Aquí podemos seleccionar plantillas que vienen por defecto para obtener los gráficos, por ejemplo podemos escoger "ucd/net SNMP" en caso de que el dispositivo a agregar sea un sistema UNIX/LINUX, en la opción "Cisco Router" en el caso de tratarse de un dispositivo Cisco como switch/router, o "Windows Host" en caso de tener equipos con sistema operativo Windows.
SNMP Community: En el caso de no tener configurada la comunidad SNMP de forma predeterminada, debemos agregarla en este campo.
SNMP Versión: En este opción debemos especificar si el equipo que deseamos ingresar al sistema pertenece a una comunidad snmp en la versión 1, 2 o 3

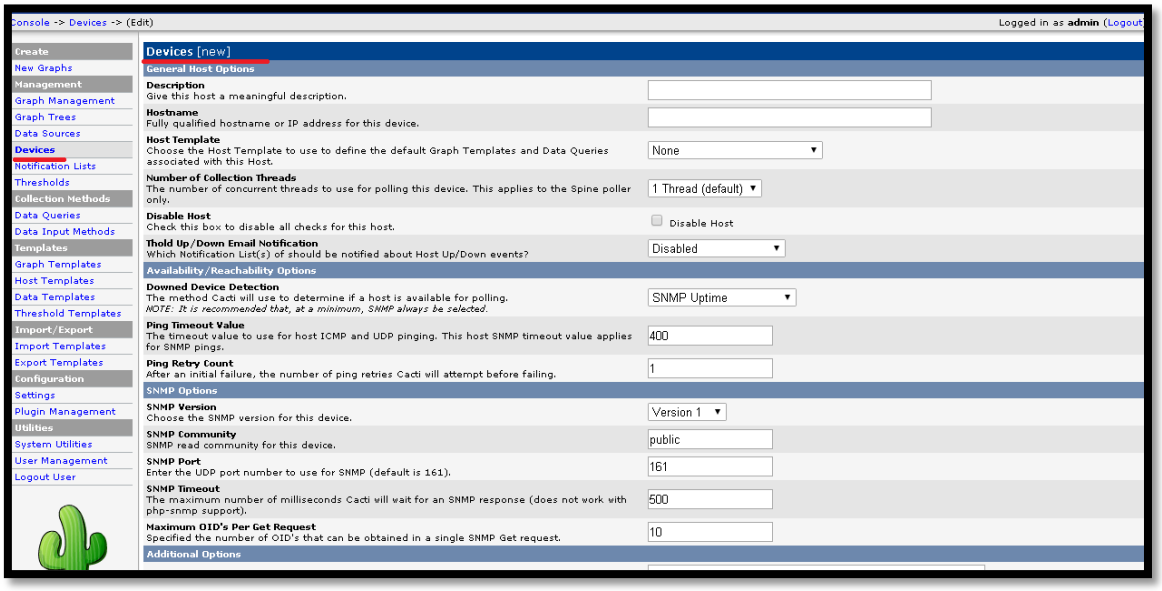


Figura C. 140 Plantilla para añadir nuevos dispositivos Cacti

Una vez que hemos llenado la plantilla con los datos correspondientes damos click en el botón “create” ubicado en la parte inferior derecha de la plantilla.

Para verificar si se están obteniendo datos por medio de SNMP en la parte inferior de la plantilla, en el menú “Associated Data Queries” debe tener valores superiores a cero la columna Status.

Figura C. 141 Verificamos que existan valores SNMP en el equipo gestionado

Si existen datos procedemos a crear los gráficos que deseemos monitorear en el botón de la parte superior derecha

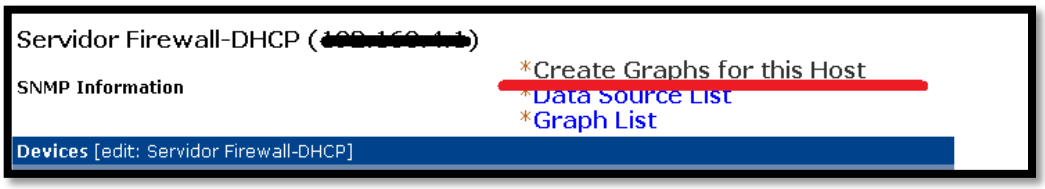


Figura C. 142 Botón para crear graficas Cacti

Seleccionamos las interfaces que deseemos monitorear en el dispositivo, así como los ítems “SNMP - Get Mounted Partitions”, “SNMP - Get Processor Information” y “SNMP - Interface Statistics” para gráficos de discos de almacenamiento, procesador, o ancho de banda en las interfaces respectivamente.

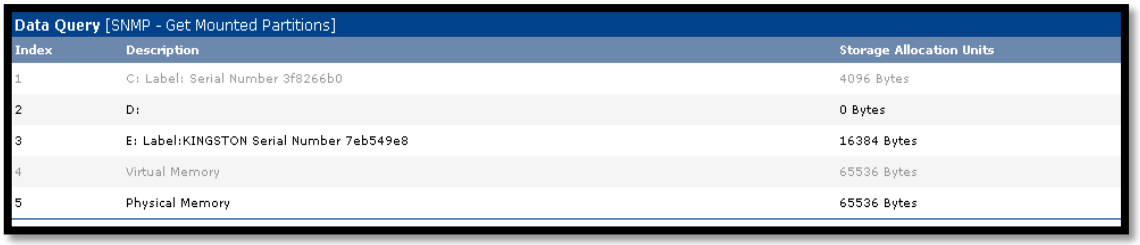


Figura C. 143 Items a graficar en Cacti

Después de seleccionar los ítems que deseamos graficar hacemos click en el botón “créate” ubicado en la parte inferior derecha de la plantilla.

C.5.3. Gráficas

Cacti nos permite visualizar gráficas asociadas a cada equipo ingresado, para lo cual se toma como referencia las más importantes como son:

- Tráfico de Red
- Uso de la CPU
- Uso de la memoria RAM

Para visualizar las gráficas asociadas a los equipos ingresados nos dirigimos a la pestaña “graphs” y podremos ver un menú desplegable con el nombre de los equipos que se encuentran monitoreándose, para visualizar los gráficos solo daremos click en el equipo correspondiente.

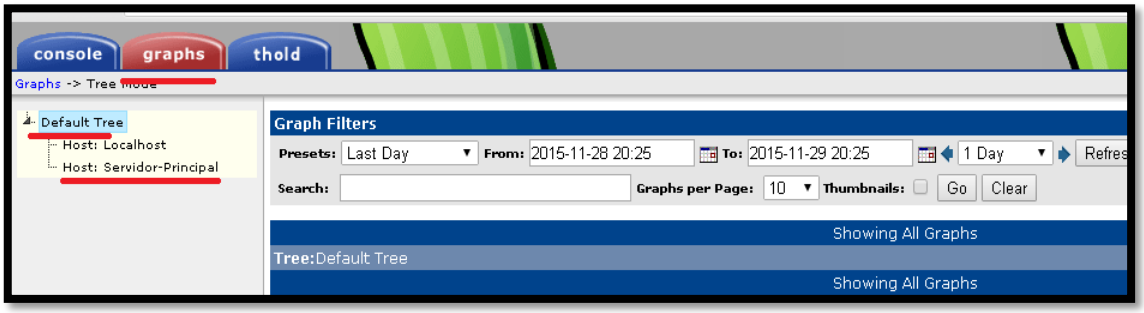


Figura C. 144 Visualización del árbol de gráficas Cacti

Si damos click en algún equipo podremos visualizar sus gráficas correspondientes

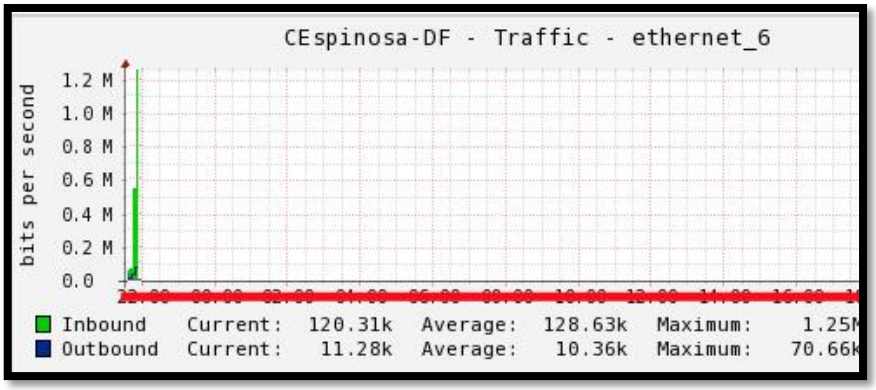


Figura C. 145 Gráficas representadas en Cacti

C.5.4. Notificaciones

Cacti nos da la opción de enviar alertas a nuestra cuenta de correo electrónico en caso de que ocurra alguna irregularidad en nuestros equipos.

Para activarla nos dirigimos a la pestaña Console en el menú Configuration y la opción Settings, seguidamente damos click en la pestaña Mail/DNS y llenamos los campos con información perteneciente a nuestro servidor de correo.

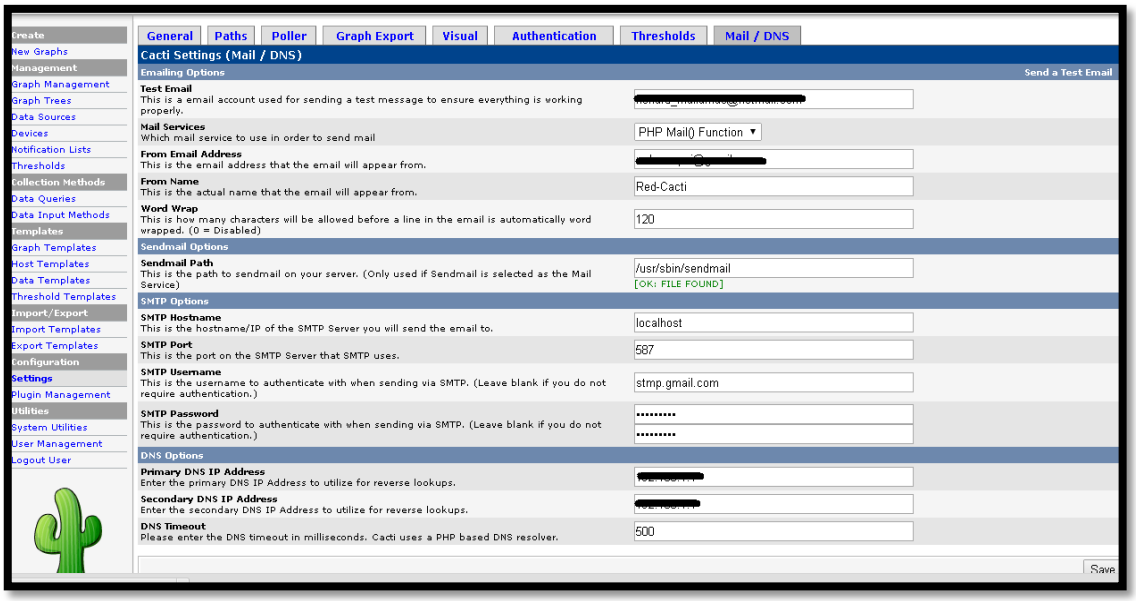


Figura C. 146 Configuración de correo en Cacti

Luego establecemos los parámetros, nos dirigimos a la pestaña Console en el menú Configuration y la opción Settings, seguidamente damos click en la pestaña Thresholds.

En esta opción podemos personalizar las opciones de alerta tales como el texto que nos llegará en el mensaje del correo, elegimos la cuenta a la que deseamos que nos notifique, etc. Si marcamos la opción “Dead Hosts Notifications” recibiremos una notificación al correo electrónico cada vez que se pierda la conectividad con algún dispositivo que estemos monitoreando.

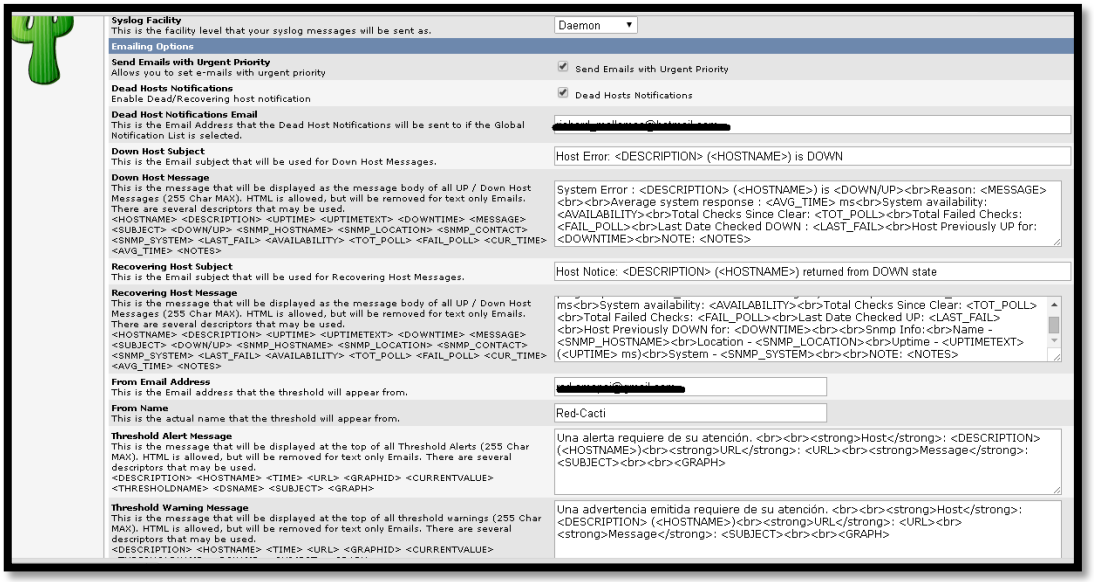


Figura C. 147 Parámetros de envío al correo electrónico en Cacti

Anexo D: Configuraciones de los agentes SNMP en los equipos de Emapa-I

D.1. Activar agente SNMP en entorno Windows

Procedemos a crear la comunidad en la pc que vamos a monitorear, en este lo vamos a hacer en una Pc con Windows versión 7, como primer paso activamos estas características en Windows dirigiéndonos al panel de control y buscar **Activar o Desactivar características de Windows**.

Figura D. 1 Activamos características de Windows

En la ventana que nos despliega damos click en las casillas nombradas **Protocolo simple de administración de redes**, que por defecto vienen desactivas, para guardar los cambios realizados damos click en aceptar y esperamos un momento para que se active este servicio.

Figura D. 2 Agregar características SNMP en Windows 7

Para poder configurarlo nos dirigimos al botón Inicio y buscamos Servicios, y damos click en esta opción

Figura D. 3 Entramos en el menú Servicios

En el menú servicios, buscamos la opción **Servicio SNMP**, y en la ventana que nos despliega, elegimos en primer lugar la pestaña Agente, y procedemos a llenar datos de administrador:

Contacto: proporciona una ubicación para que escriba el nombre de la persona que administra este equipo.

Ubicación: proporciona una ubicación para que escriba la ubicación física del equipo (por ejemplo, el número de edificio y oficina).

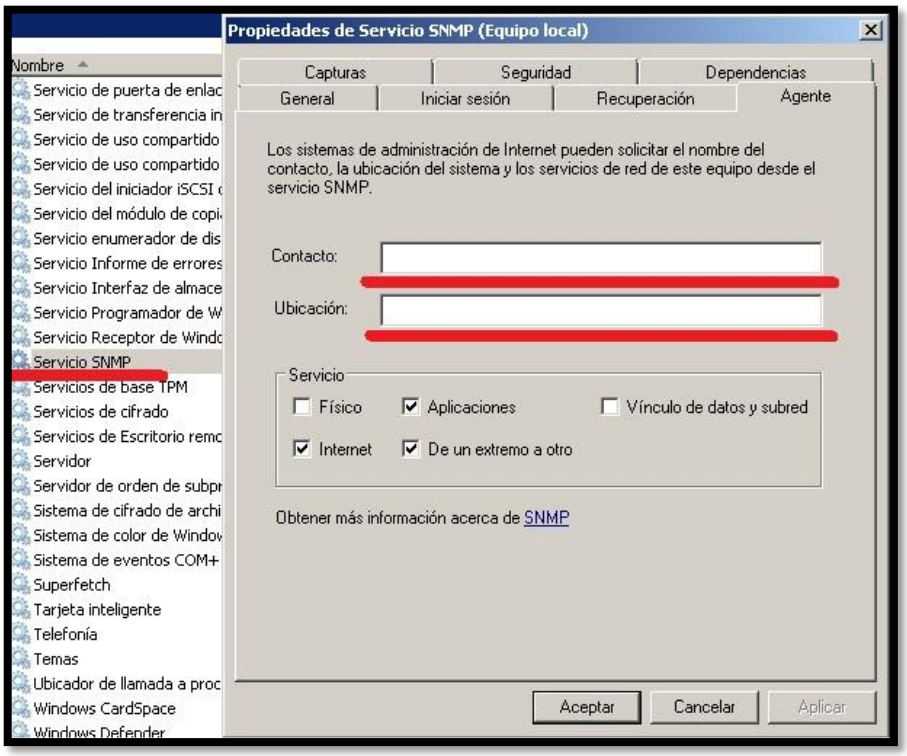


Figura D. 4 Agregamos el nombre y la ubicación de la persona que administra este equipo

Una vez llenados estos datos, nos dirigimos a la pestaña Seguridad en la cual como primer paso, en la opción de agregar comunidad agregaremos la creada en nuestro servidor llamada “ocs-inventory, las opciones a elegir vienen dadas de la siguiente manera:

- **Ninguna:** impide que este host procese cualquier petición SNMP.
- **Notificar:** permite que este host envíe únicamente capturas de SNMP a la comunidad.
- **Sólo lectura:** impide que este host procese peticiones SNMP SET. Los objetos administrados SNMP disponen de valores predeterminados especificados por el agente. Algunas aplicaciones pueden solicitar la modificación de estos valores con el comando SNMP SET.
- **Lectura y escritura:** permite que este host procese peticiones SNMP SET.
- **Lectura y creación:** permite que este host cree nuevas entradas en las tablas SNMP.

Para el ejemplo escogeremos la opción de **SOLO LECTURA**, y le damos click en el botón agregar.

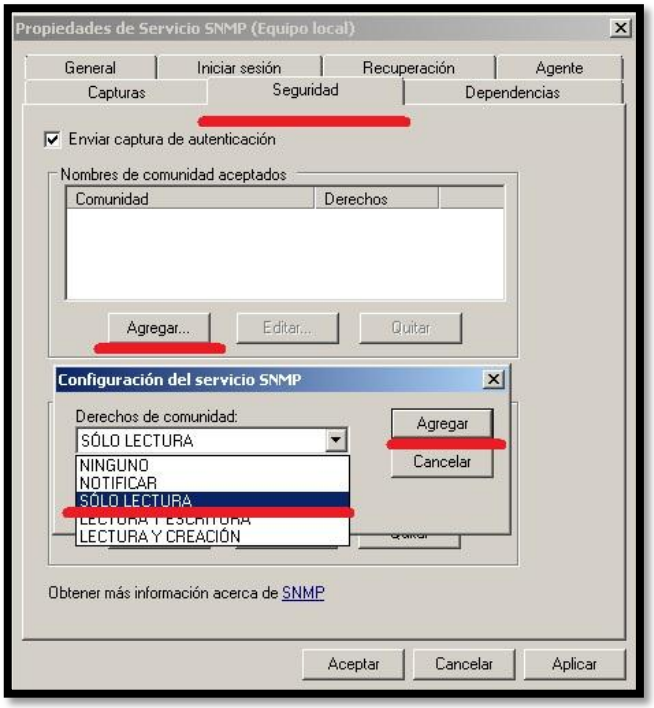


Figura D. 5 Agregar la comunidad SNMP con la opción de SOLO LECTURA

Luego, en la misma pestaña **Seguridad**, agregamos la dirección IP de nuestro servidor SNMP, y damos click en el botón Agregar y por último damos click en Aplicar.

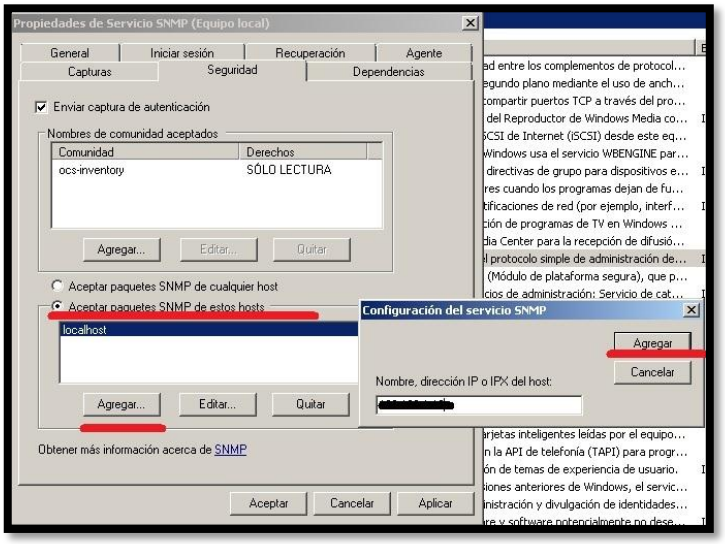


Figura D. 6 Agregamos la dirección IP del servidor SNMP

Por último, para que los cambios se realicen correctamente, damos click derecho en Servicio SNMP, y escogemos la opción Reiniciar.

Figura D. 7 Reiniciamos el servicio SNMP para que se activen los cambios realizados

Por último verificamos que las reglas del firewall permitan el tráfico de protocolo snmp.

D.2. Activar agente SNMP en entorno Linux

En primer lugar instalamos el agente ejecutando el siguiente comando:

yum -y install net-snmp net-snmp-utils

Luego revisamos el archivo /etc/snmp/snmpd.conf que se instala junto con el paquete. Se recomienda hacer un respaldo del archivo original, para evitar algún percance.

Figura D. 8 Realizamos una copia del archivo original snmpd.conf

Abrimos el archivo /etc/snmp/snmpd.conf con un editor de textos.

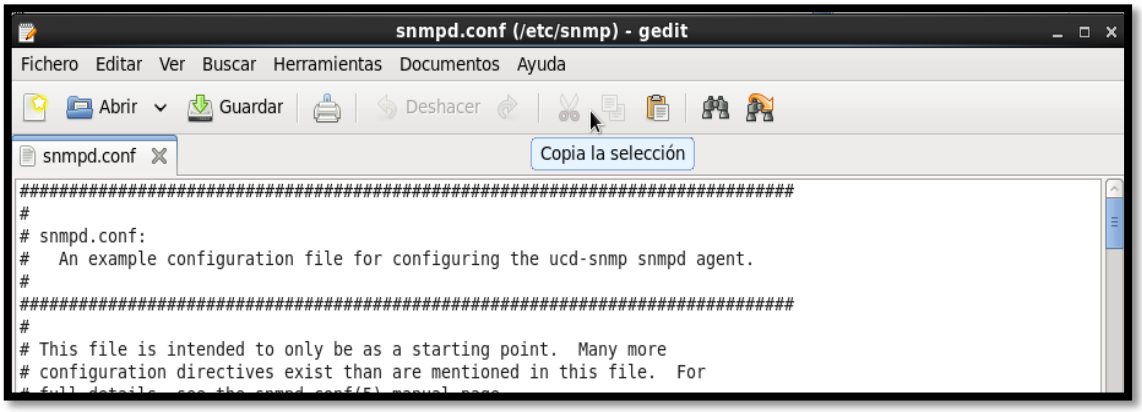


Figura D. 9 Abrimos el archivo snmpd

En este fichero lo primero que hacemos es agregar la comunidad, y agregamos la dirección IP del gestor SNMP.

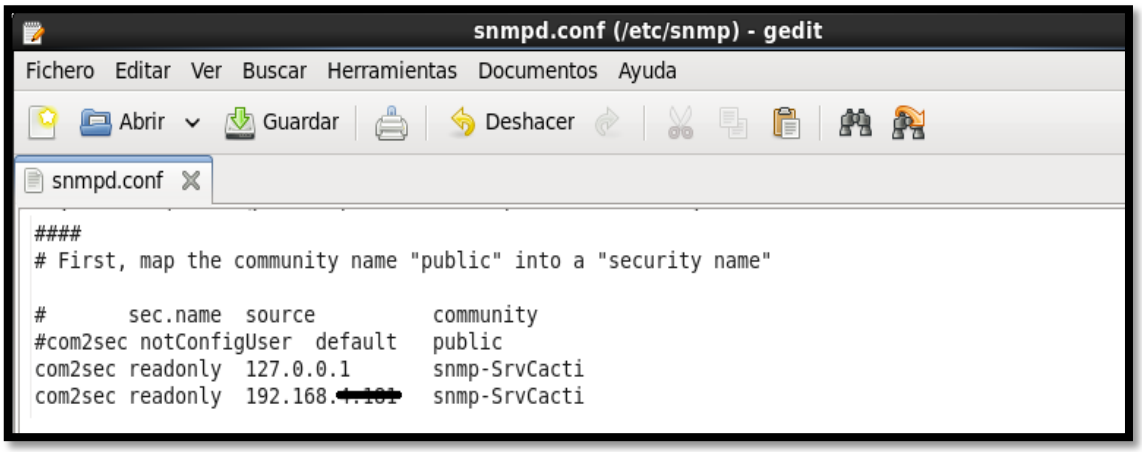


Figura D. 10 Agregamos la comunidad y la ip de nuestro servidor

Luego agregamos un grupo para la comunidad que creamos y especificamos la versión de la comunidad que deseamos, también la acción deseamos que realice, en este caso escogemos la versión 2 de snmp y con capacidad solo de lectura de los datos.

```
####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
#group   notConfigGroup v1           notConfigUser
#group   notConfigGroup v2c           notConfigUser
group    MyROGroup      v2c             readonly
```

Figura D. 11 Agregamos un grupo para nuestra comunidad

Escogemos el grupo de MIB que deseamos mostrar al gestor snmp.

```
####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree          mask(optional)
view all    included  .1                               80
view    systemview    included   .1.3.6.1.2.1
```

Figura D. 12 Incluimos el grupo de MIB que deseamos que el gestor visualice

Finalmente damos permisos de solo lectura al grupo al que pertenece nuestra comunidad.

```
####
# Finally, grant the group read-only access to the systemview view.

#       group          context sec.model sec.level prefix read   write  notif
#access  notConfigGroup ""      any       noauth    exact  systemview none none

access MyROGroup ""      any       noauth    0            all   none   none
```

Figura D. 13 Damos permisos de lectura a nuestra comunidad snmp

Una vez editado el fichero reiniciamos el servicio snmpd para que se guarden los cambios que realizamos

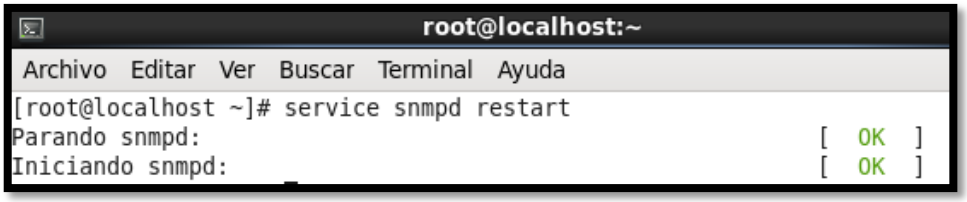


Figura D. 14 Reiniciamos el servicio snmp

Por último verificamos que las reglas del firewall permitan el tráfico de protocolo snmp.

D.3. Activar agente SNMP en Switch Dlink

En primer lugar entramos a la plataforma web del switch al que vamos a habilitar SNMP, en la pestaña Management escogemos la opción SNMP y en el menú desplegable escogemos la pestaña SnmpGlobalSetting, y habilitamos el servicio.

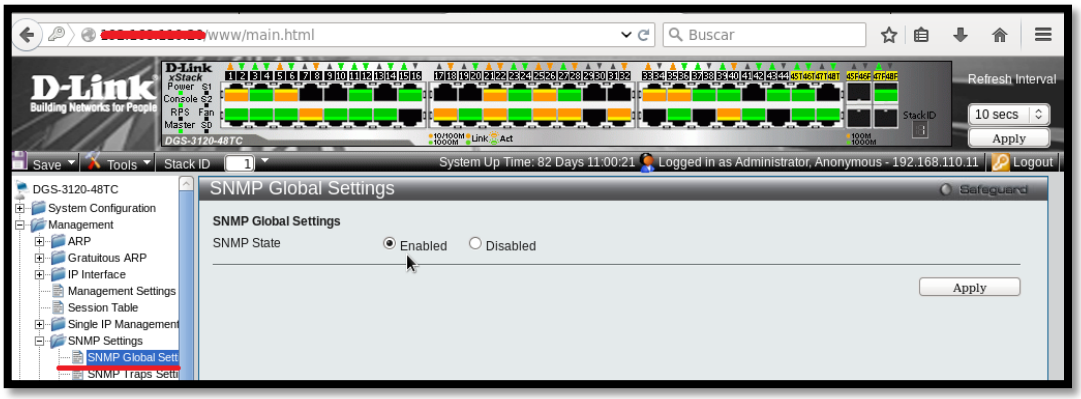


Figura D. 15 Habilitamos el servicio SNMP

Luego en el menú desplegable escogemos la opción SNMP Community, en la cual vamos a agregar nuestra comunidad, asignándole permisos de solo lectura, y para guardar los cambios damos click en el botón Apply.

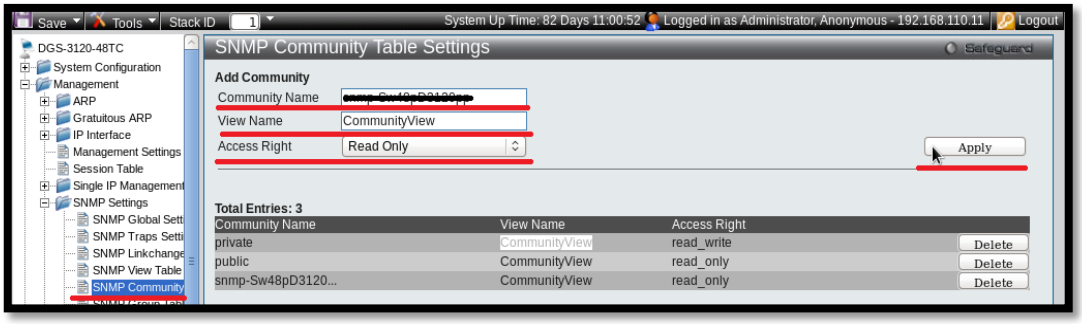


Figura D. 16 Agregamos la comunidad al Swicth

D.4. Activar agente SNMP en equipos Mikrotik

En primer lugar ingresamos al equipo mikrotik por la plataforma winbox, logueandonos con nuestros datos de administrador.

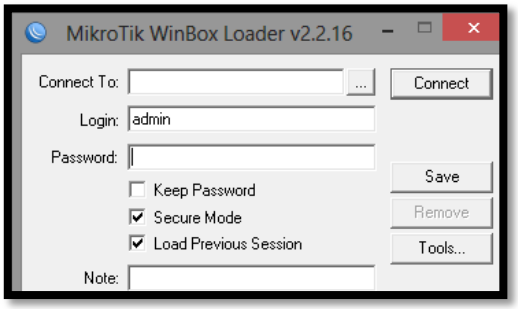


Figura D. 17 Ingresamos al equipo mikrotik por winbox

En el panel izquierdo en la opción IP nos aparecerá un menú desplegable del cual escogeremos la opción SNMP.

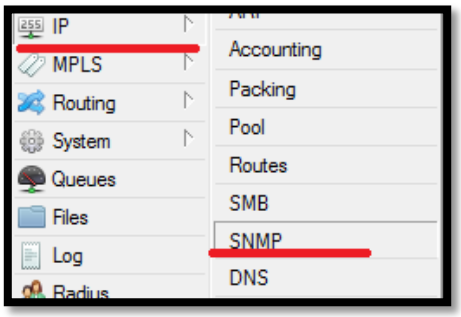


Figura D. 18 Escogemos la opción SNMP

Nos mostrará un menú SNMP Communities en donde procederemos a agregar la nuestra dando click en el botón azul “+”

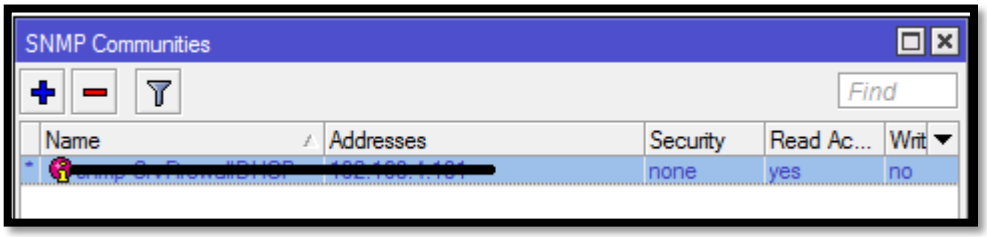


Figura D. 19 Agregamos una comunidad snmp al equipo

Al dar click en agregar una comunidad nos solicitará el nombre y la dirección del gestor snmp, agregamos estos datos y damos click en el botón Apply

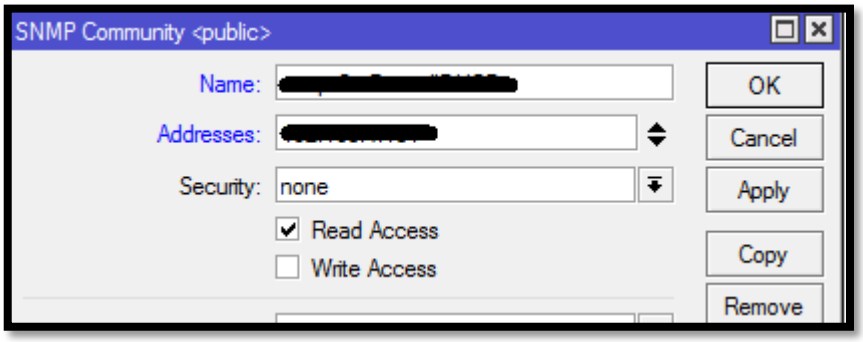


Figura D. 20 Agregamos el nombre de la comunidad snmp

Por último en la configuración SNMP habilitamos el protocolo y especificamos la versión de la comunidad que agregamos

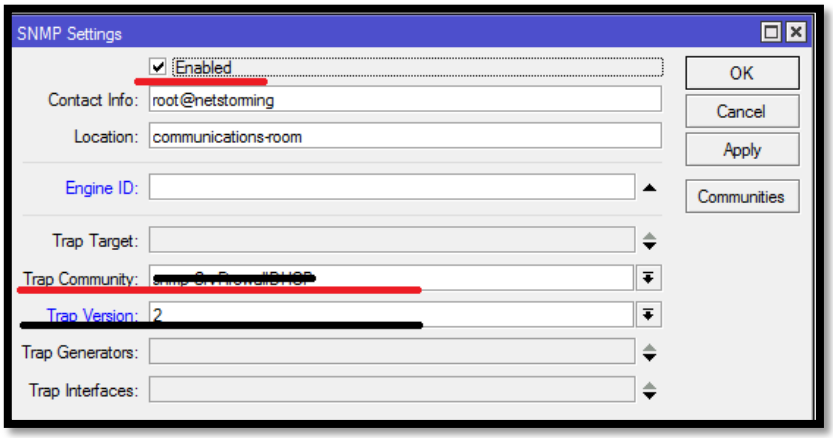


Figura D. 21 Habilitamos SNMP

D.5. Activar agente SNMP en Switch Cisco 3750

Una vez ingresado al equipo ya sea por el puerto de consola o via telnet, nos logueamos con nuestros datos, y en el modo de configuración global, activamos las siguientes líneas: snmp-server community xxxx ro, en donde especificamos la comunidad y con los respectivos permisos de lectura.

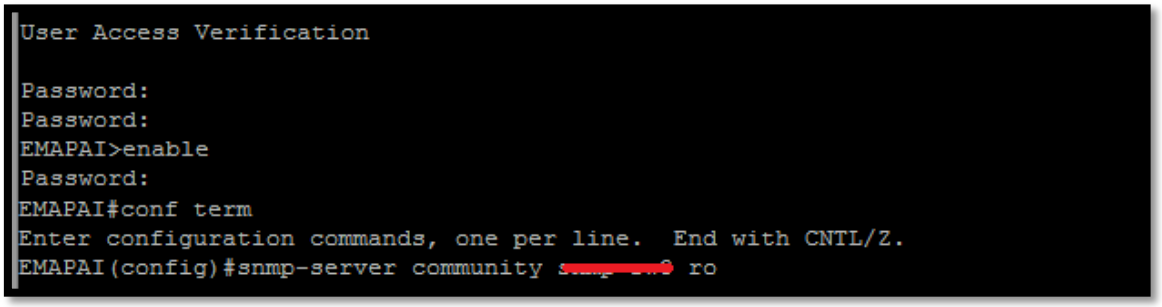


Figura D. 22 Agregamos la comunidad y permisos de lectura

Luego indicamos la dirección IP del gestor snmp y especificamos la versión de la comunidad que creamos anteriormente con las siguientes líneas: snmp-server host x.x.x.x version 2 comunidad

Figura D. 23 Indicamos la version de la comunidad y la dirección IP del gestor

Finalmente habilitamos las operaciones traps en el switch con el comando: snmp-server enable traps

Figura D. 24 Habilitamos las operaciones traps-snmp en el switch

D.6. Activar agente SNMP en Switch CiscoSGE2010

En primer lugar entramos a la plataforma web del switch al que vamos a habilitar SNMP, en la pestaña SNMP escogemos la opción Communities y en el menú desplegable escogemos la opción agregar nueva comunidad.

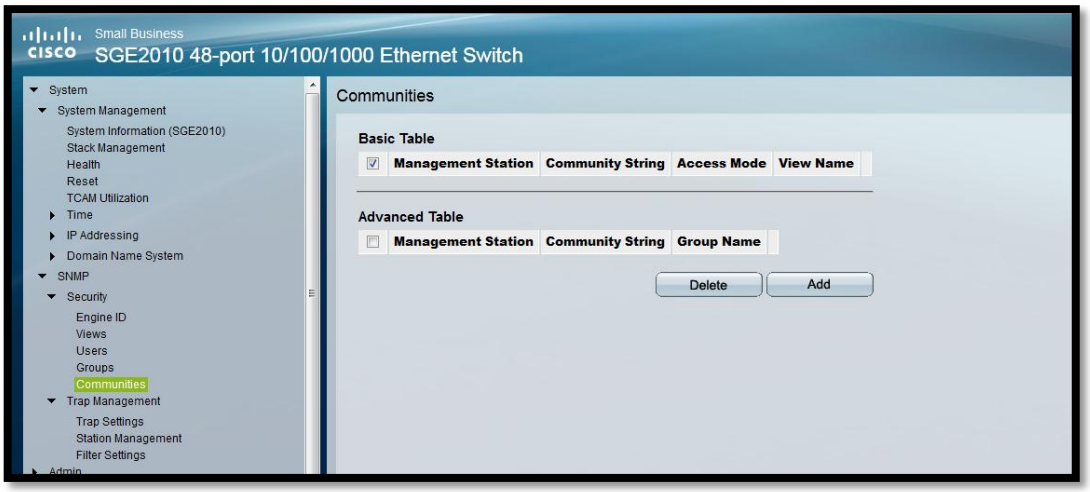


Figura D. 25 Agregar nueva comunidad snmp al switch

En el menú desplegable agregamos las opciones que nos pide entre ellas está la versión IP con la que estamos trabajando, la dirección IP del gestor snmp, el nombre de la comunidad, y el modo de acceso que tendrá el gestor snmp, en este caso pondremos solo lectura, llenamos los datos y damos click en el botón Apply.

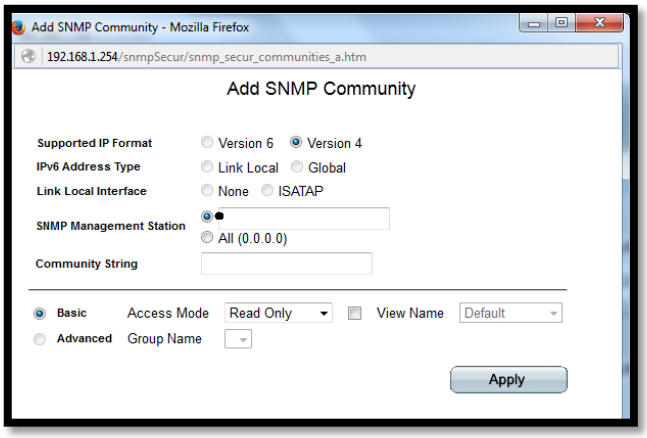


Figura D. 26 Ingresamos el nombre de la comunidad snmp y el modo de acceso

Una vez creada la comunidad en la pestaña comunidades de la plataforma web nos debe desplegar la recién agregada.

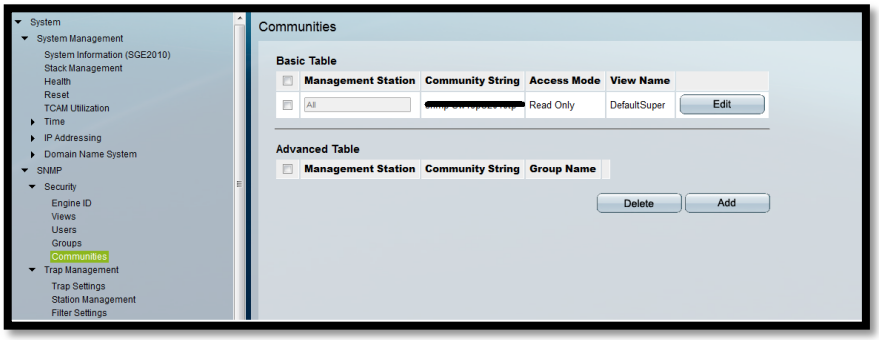


Figura D. 27 Comunidad agregada al SwSGE2010

D.7. Activar agente SNMPv3 en plataformas Windows

Una vez instalado el agente, revisamos su instalación, por defecto se instala en el disco C, en la carpeta: usr, en primer lugar activamos el agente dando click en modo administrador en el archivo registeragent.

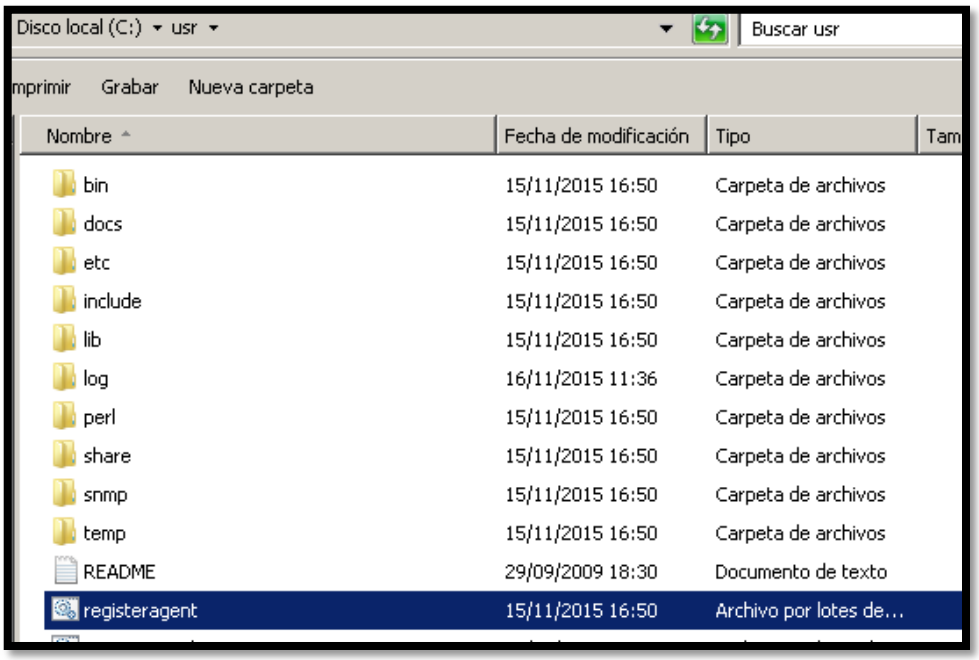


Figura D. 28 Activamos el agente snmpv3

Luego revisamos si existe el archivo snmpd.conf en la dirección: C:\usr\etc\snmp, de no existir, lo creamos.

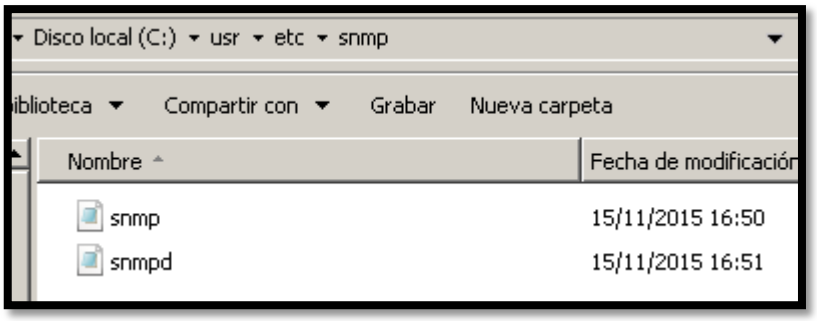


Figura D. 29 Confirmamos que exista el fichero snmpd

Dentro del fichero snmpd.conf creamos nuestro usuario snmpv3, en donde se agregaremos el nombre del usuario snmpv3, el tipo de autenticación con su contraseña y el tipo de encriptación con su contraseña respectivamente, luego en la siguiente línea damos los permisos de lectura al usuario creado.

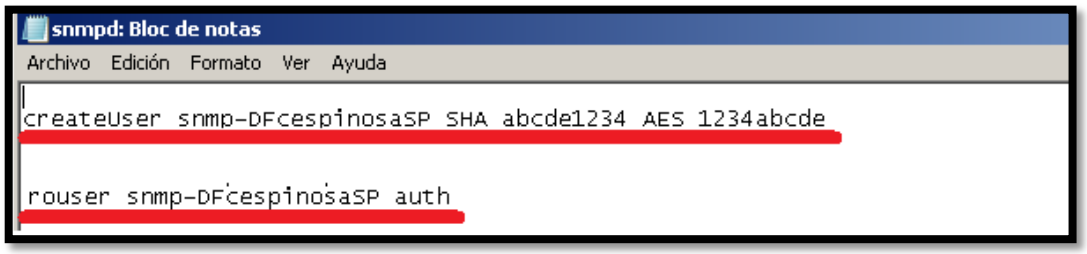


Figura D. 30 Creación del usuario snmpv3

Por ultimo iniciamos el servicio del agente con el comando net start "net-snmp agent", en el cmd de Windows

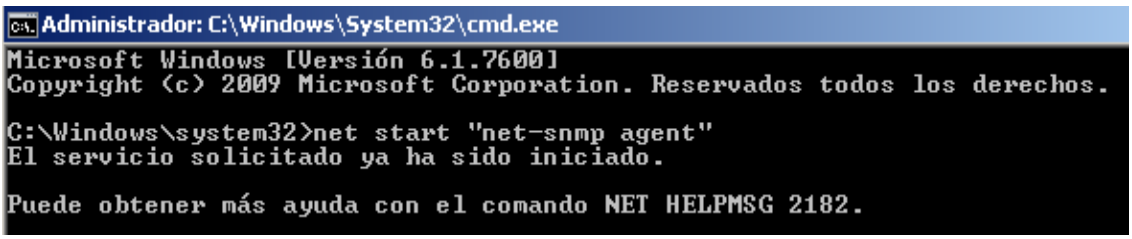


Figura D. 31 Activación del servicio del agente snmpv3

Para que este agente se complemente con el agente que viene por defecto de Windows, en primer lugar debemos detener el servicio snmp de Windows, luego activamos el agente net-snmp, y finalmente activamos el servicio snmp de Windows nuevamente.

D.8. Instalación del agente ocs-inventory

Para instalar el agente, en primer lugar lo descargamos de la página oficial de OCS-INVENTORY http://www.ocsinventory-ng.org/en/download/download-agent.html una vez descargado el archivo procedemos con la instalación del archivo "OCS-NG-Windows-Agent-Setup.exe", dando click en el botón Next.

Figura D. 32 Instalación del Agente OCS Inventory

Aceptamos los términos de la licencia

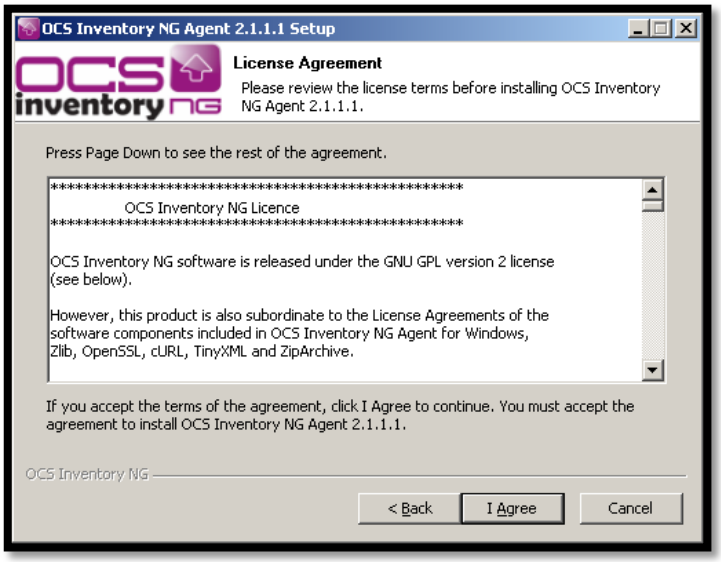


Figura D. 33 Aceptamos los términos de licencia

Luego seleccionamos el tipo de instalación que deseamos:

Network Inventory: El computador puede alcanzar a OCS Inventory Server a través de la red, y por lo tanto, el agente se pondrá en marcha utilizando un servicio de Windows, o una secuencia de comandos de inicio de sesión.

Local Inventory: El equipo no está conectado a una red, o nunca será capaz de llegar a OCS Inventory NG Server. Se puede generar un inventario de este equipo y guardar en el archivo a importar más adelante en el servidor.

Para nuestro caso elegimos la opción Network Inventory ya que estamos dentro de una subred.

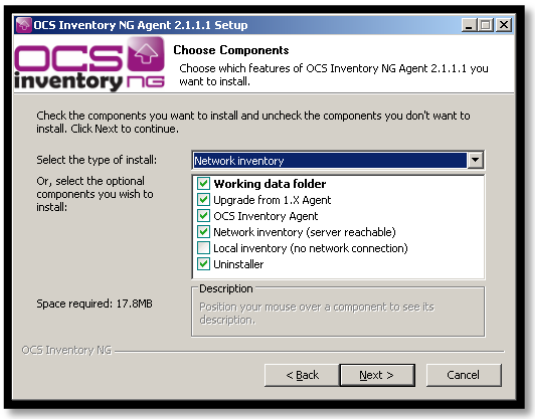


Figura D. 34 Elegimos el tipo de instalación

En la siguiente ventana, apuntamos la dirección IP en la cual se encuentra nuestro servidor OCS-Inventory, y agregamos el usuario que creamos previamente para este computador.

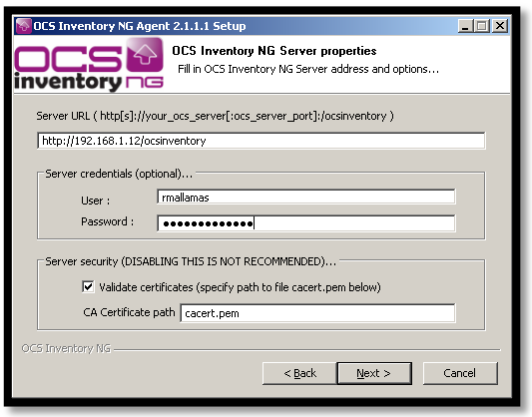


Figura D. 35 Agregamos la dirección IP de nuestro Servidor

En la siguiente ventana, si es necesario, seleccionamos el tipo de proxy que se utilizará para conectarse al servidor de comunicación, la dirección del proxy, el puerto, y las credenciales del proxy, para nuestro caso no añadimos nada a esta ventana.

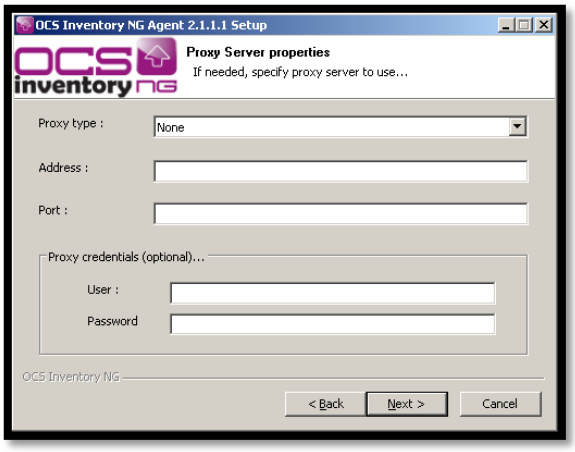


Figura D. 36 Si es necesario se edita datos del Proxy del servidor

Por defecto, el agente OCS Inventory solo se añade pocos datos en los archivos de registro, se puede aumentar habilitando "Verbose log", también podemos añadir una etiqueta para reconocerlo de mejor manera a nuestro usuario, y habilitamos la casilla "Immediatly lauch inventory" para que el agente comience a funcionar inmediatamente.

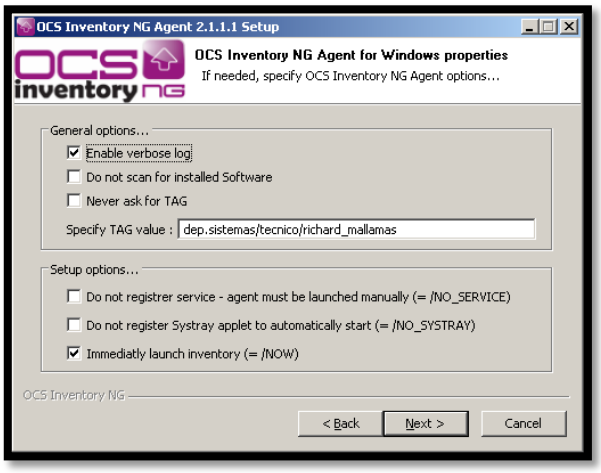


Figura D. 37 Agregamos una etiqueta al computador gestionado

Se escoge una carpeta para instalar el agente, por defecto se guarda en el directorio: C:\Program Files (x86)\OCS Inventory Agent\

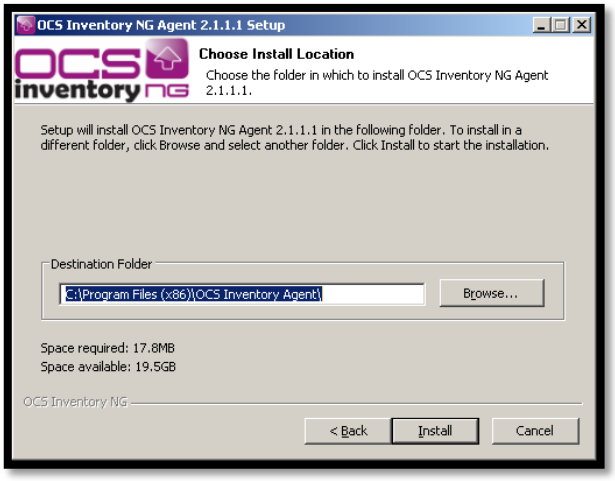


Figura D. 38 Escogemos la carpeta de instalación del agente

Hacemos clic en "Finalizar" para cerrar la instalación del agente OCS-Inventory.

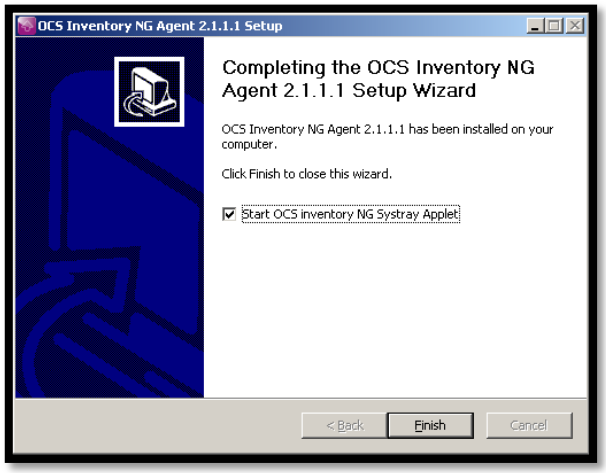


Figura D. 39 Finalizamos la instalación del agente

Anexo E: Selección de herramientas a utilizar

E.1. Selección del sistema operativo para el sistema de gestión

La elección del software que se va a utilizar como sistema operativo es la primera y más importante tarea pues a partir de aquí se instalaran las siguientes herramientas de apoyo para la gestión de red, tomando en cuenta los requerimientos antes establecidos por medio de la norma ISO/IEC/IEEE 29148-2011, se realizó el estudio de diferentes alternativas, las cuales están basadas en aplicaciones de código abierto y se muestran a continuación.

- **Debian:** Destaca por ser un software de libre distribución, este sistema operativo no es aconsejable para aquellas personas procedentes de Windows, pues se necesita un previo conocimiento en Linux para instalar y posteriormente usar con comodidad el Sistema Operativo, aunque algunas versiones actuales van encaminando a mejorar el proceso de instalación. el soporte es realizado por una comunidad creada por voluntarios o usuarios. Algunos dispositivos no están soportados debido a que el vendedor decidió no dejar las especificaciones disponibles. Esta también es un área en la que se está trabajando. Debian. (2014).

- **CentOS:** CentOS es una distribución mantenida por la comunidad de voluntarios y derivada de los paquetes fuentes liberados al público por Red Hat para Red Hat Enterprise Linux (RHEL). Destaca por ser una solución empresarial libre. Cada versión de CentOS es mantenida por 10 años. Las versiones de CentOS son actualizadas periódicamente actualizada aproximadamente cada seis meses para mejora de su rendimiento o incorporar nuevo hardware. Esto resulta en un entorno Linux seguro, de bajo mantenimiento, confiable. Centos. (2015).

- **Red Hat Linux Enterprise** Distribución comercial de Linux desarrollada por Red Hat. Ofrece calidad, estabilidad y seguridad. Es una plataforma abierta que ofrece flexibilidad, al tener contacto con la mayoría de proveedores de software y hardware le hace más capaz de ofrecer las innovaciones en hardware más

> recientes de numerosos fabricantes; e incluye un ciclo de vida de soporte y actualizaciones de siete años. La diferencia entre esta opción y las dos anteriores es el costo en el soporte y actualización de este software. Red Hat Enterprise Linux Server. (2015).

Se opta por la distribución CentOS que cumple con los requisitos funcionales, legales y económicos exigidos por la institución, cuenta con un foro tanto de voluntarios como de usuarios para un mantenimiento estable, destaca por su calidad, fácil configuración, estabilidad y seguridad ya que las actualizaciones o parches se realizan en periodos de 6 meses. Además es un sistema operativo con características optimizadas para correr servicios web como Apache, base de datos como MySQL, y una variedad de otros componentes necesarios para el funcionamiento de cualquier sistema de monitorización de red.

E.2. Evaluación de herramientas de gestión de red

Para la elección de herramientas, se tomó en cuenta las siguientes plataformas de código abierto: Cacti, Zennos, Zabbix y Nagios, debido a su uso ampliamente difundido, disponibilidad, estabilidad y además cuentan con documentación de mantenimiento en sus comunidades.

E.2.1. Cacti

Es una herramienta para sondear, almacenar y presentar gráficos estadísticos de equipos de red, recolecta datos vía SNMP y las funciones pueden configurarse a través de su interfaz web.

Es un software en código abierto que permite monitorizar y visualizar resultados estadísticas de dispositivos conectados a una red que tengan el protocolo SNMP activado y configurado. Es una herramienta que nos permite visualizar gráficos del estado de parámetros de red como: ancho de banda, detección de congestiones o picos de tráficos en su interfaz. La comprensión de estas graficas no es complicado si es que se tiene un conocimiento básico en sistemas computacionales, que es con el cual cuentan todos los

integrantes del departamento de informática, el soporte se lo realiza por medio de una comunidad de voluntarios y usuarios del mismo, que se encargan de actualizaciones o ingreso de plugins del mismo, como es el caso del envío de correo electrónico como parte de notificación si es que un parámetro configurado como umbral es superado. (Comunidad Cacti, 2013).

- **Ventajas**

- **Medir disponibilidad y capacidad de parámetros en la red**
  - Cacti puede monitorear el tráfico de red en las interfaces de los rutadores, conmutadores y computadores.
  - Puede medir capacidad de disco duro, carga de CPU, y la capacidad de memoria RAM.
- **Gráficos**
  - Permite la creación de grafico en base a los datos colectados y organizarlos en árboles jerárquicos
- **Colección de datos**
  - Los datos se van actualizando vía el protocolo SNMP
- **Plantillas**
  - Permite crear o editar las plantillas predeterminadas para usarlas en las definiciones de gráficos
- **Gestión de usuarios**
  - Permite definir distintos niveles de autorización de ingreso al sistema

- **Desventajas**

- En comparación a otras plataformas Cacti es de alguna manera limitada en características. No ofrece a primera vista un panel de control con estado de la infraestructura tecnológica, ni tampoco tiene la capacidad de notificar alertas. Aunque algunas de estas características se pueden adicionar mediante el uso de plugins.

E.2.2. Zenoss

Zenoss es una herramienta Open Source que mediante el monitoreo a los recursos de red puede gestionar su rendimiento a través de la interfaz web, cuenta con la versión de core y la empresarial, la diferencia principal en estas dos versiones es que en la empresarial cuenta con soporte profesional.

Cuenta con personalización de umbrales dinámicos, que permiten manejar valores distintos dependiendo de la organización, los cuales pueden activarse para enviar notificaciones al administrador de red si se sobrepasan los límites establecidos. (Zenoss. Inc, 2012).

- **Ventajas**

- Puede ser utilizado para monitorizar dispositivos de red mediante el protocolo SNMP
- Puede medir capacidad de disco duro, carga de CPU, y la capacidad de memoria RAM.
- Descubrir automáticamente los recursos de la red y los cambios en la configuración de la red
- Sistema de alerta basado en las notificaciones de conjuntos de reglas y de atención cíclica.

- **Desventajas**

- Necesita hardware de altas prestaciones

E.2.3. Zabbix

Zabbix es una herramienta Open Source creada por Alexei Vladishev, las actividades de monitoreo se la realizan a través de su interfaz web, los datos se colectan vía el protocolo SNMP el cual nos permite conocer el estado de los dispositivos de red como su carga de cpu, capacidad de disco duro, y estado de uso de la memoria RAM, cuenta con

notificaciones personalizables las cuales permiten emitir una alerta al administrador de red si se ha sobrepasado algún umbral establecido. (Zabbix, 2010)

- **Ventajas**

- Administración vía plataforma web.
- Escalabilidad en el número de dispositivos.
- Permite monitorizar redes internas y externas.
- Sistema de alertas vía: email, SMS, Jabber
- Variedad de idiomas, incluido el español
- Creación de plantillas de configuración exportables/importables.
- Autodescubrimiento de dispositivos.
- Permite monitorear varios parámetros a la vez.
- Permite ver mapas de red por grupos

- **Desventajas**

- Al no disponer de una versión enterprise ha provocado que no sea tan conocida en referencia a las demás herramientas.

E.2.4. Nagios

Fue creado por Ethan Galstad, está escrito en C y se trata de un software que proporciona una gran versatilidad para consultar cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red. (Nagios, 2010).

- **Ventajas**

- Es un software popularmente conocido y posee variedad de información en su comunidad
- Alertas de correo electrónico o SMS

- Permite monitorear varios parámetros a la vez.
- Escalable
- Registro automático de logs.
- Interfaz web para visualizar el estado actual de la red y las gráficas de los parámetros que se estén monitoreando.

- **Desventajas**

- La versión libre no cuenta con soporte oficial, solo con la documentación que se pueda encontrar en los foros de discusión y en general todo el material que se pueda encontrar en internet.
- Su interfaz web es en su mayoría es de sólo lectura.
- La configuración es realizada mediante la personalización de ficheros de texto

E.3. Cuadro de evaluación de herramientas de monitoreo de red

La evaluación de herramientas de monitoreo de red se lo realizó en base a la siguiente tabla de valorización.

Tabla E. 1 Escala de valoración

Escala	**Valor**
0	No tiene/Mala
1	Regular
2	Bueno
3	Muy bueno

Fuente: Diseño personal

Tomando en cuenta la escala de valorización, el resultado de las pruebas realizadas es el siguiente.

Tabla E. 2 Evaluación de herramientas de monitoreo de red

Descripción	**Zennos**	**Cacti**	**Nagios**	**Zabbix**
Facilidad de Instalación	2	3	2	3
Facilidad de Configuración	2	3	2	3
Administración de Interfaz Web	2	2	3	3
Documentación	3	3	3	3

Integración con Plugins	2	2	3	3
Facilidad de Uso	2	3	2	3
Alertas y Notificaciones	2	2	3	3
Creación Personalizada de Scripts	2	2	3	3
Soporte en Línea	3	3	3	3
Actualizaciones	2	2	3	3
Monitorear distintos sistemas operativos	3	3	3	3
El servidor se instala en ambiente Linux	3	3	3	3
Generación de reportes operativos y estadísticos	2	2	3	3
Enviar Alarma si no responde el equipo computacional	3	3	3	3
Enviar Alarma si no responde el equipo de red	3	3	3	3
Enviar alarma si se llega a determinados umbrales de disco duro	3	3	3	3
Enviar alarma si se llega a determinados umbrales de memoria RAM	3	3	3	3
Enviar alarma si se llega a determinados umbrales de CPU	3	3	3	3
Permitir el envío de notificaciones vía Correo Electrónico	3	2	3	3
Los datos se deben poder exportar a una base de datos Open Source	3	3	3	3
Gráficos	3	3	3	3
Compatible con SNMP	3	3	3	3
Mapas	3	2	3	3
Control de acceso	3	3	3	3
TOTAL	63	64	69	72

Fuente: Diseño personal

Se escogió la herramienta Zabbix por las características que se evaluaron, una de las necesidades principales que justificaron su uso fue que el departamento de informática solicito una plataforma que sea configurable en su totalidad por medio de una interfaz

gráfica. Además los equipos a monitorizar se encuentran en su totalidad con sistema operativo Windows, y Zabbix da muchas opciones para obtener datos en esta plataforma.

Otra de las opciones que destaca esta plataforma son los gráficos por defecto que se realizan automáticamente, y la posibilidad de crear gráficos a partir de las plantillas que vienen incluidas.

También se escogió esta herramienta ya que poco a poco se va abriendo camino, y por tanto la documentación va creciendo, de igual forma las actualizaciones que se van generando de forma estable en base a las recomendaciones que son aportadas por los usuarios.

E.4. Requerimientos del sistema

Los requisitos de hardware son muy variables dependiendo de la configuración (Zabbix SIA, 2008):

Tabla E. 3 Requerimientos mínimos del sistema Zabbix

Parámetros	**Requerimientos**
Hardware	Pequeña hasta 20 host; 256 MB de RAM, CPU Pentium II 350 MHz y disco duro de 40 GB. Mediana hasta 500 host; 2 GB de RAM, CPU AMD Athlon 3200 y disco duro de 80 GB. Grande hasta 1000 host; 4 GB de RAM, CPU Intel Dual Core 6400 y Disco Duro de 100 GB. Muy Grande hasta 10000; 8 GB de RAM, CPU Intel Xeon 2x y disco duro de 120 GB.
Sistemas Operativos	Zabbix funciona con las siguientes plataformas; SUSE Linux, CENTOS, FreeBSD, Solaris, Open BSD, HP-UX.
Agentes	Windows (2000, 2003, XP, Vista), Linux, Solaris, FreeBSD, AIX., SNMP

Fuente: Diseño personal en base a las características de la plataforma Zabbix

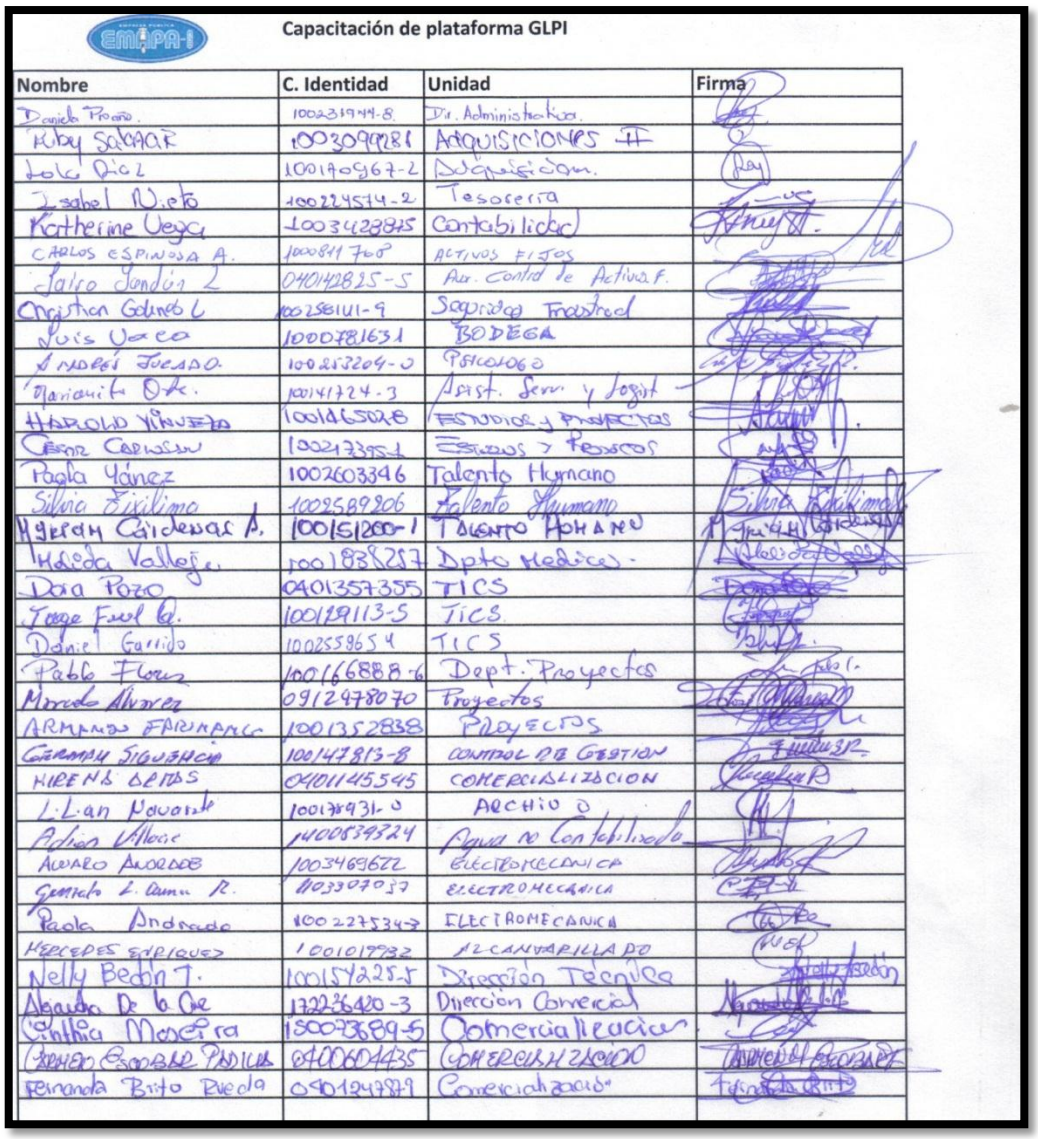
Los requisitos utilizados para la implementación del sistema de monitorización y control fueron los siguientes.

Tabla E. 4 Requerimientos utilizados para la plataforma Zabbix

Parámetros	**Requerimientos utilizados**
Hardware	Al ser una red mediana se virtualizó dentro del servidor HP PROLIANT DL380PGEN8 del cual se usó 2GB de memoria RAM, una interfaz de red y un disco duro de 50GB.
Sistemas Operativos	El sistema operativo utilizado fue: CENTOS ya que cumple con los requisitos funcionales, legales y económicos exigidos por la institución
Agentes	Los agentes por defecto se configuraron mediante el protocolo SNMP por su fácil implementación y gran compatibilidad con los equipos de red.

Anexo F: Constancia de la socialización realizada de la plataforma GLPI a los usuarios del segundo piso en la empresa EMAPA-I.

Se brindó una capacitación a los funcionarios de la institución sobre el uso, aplicación y beneficios que tiene tanto para ellos como para el departamento de informática la plataforma GLPI, misma que ayuda a procesar las incidencias informáticas dentro de la empresa. Para constancia de la socialización y explicación impartida acerca de la plataforma, las personas abajo firmantes ratifican la capacitación impartida a los 16 días del mes de Noviembre del 2015.



Capacitación de plataforma GLPI

Nombre	C. Identidad	Unidad	Firma
Daniela Pozo	1002319448	Dir. Administrativa	
Kiley Salcedo	1003099181	Adquisiciones	
Lolo Diaz	1001905967-2	Adquisición	
Isabel Nieto	1002245742	Tesorería	
Katherine Vega	1003428875	Contabilidad	
Carlos Espinosa A.	1000841768	Activos Fijos	
Jairo Jordán L.	0401428255	Aux. Control de Activos F.	
Christian Galarza L.	1002581419	Seguridad Financiera	
Luis Vaca	1000781631	Bodega	
Andrés Tocagon	1002532040	Psicología	
Mariuxi Ortiz	1001417243	Asist. Serv. y Logist.	
Harold Viveros	1001465028	Estudios y Proyectos	
Cesar Cadena	1002173951	Estudios y Proyectos	
Paola Yánez	1002603346	Talento Humano	
Silvia Sisalima	1002589206	Talento Humano	
Yeraldin Cárdenas A.	1001512001	Talento Humano	
Maleda Vallejo	1001885217	Dpto Medico	
Dora Pozo	0401357355	TICS	
Jorge Fuel G.	1001291135	TICS	
Daniel Garrido	1002558654	TICS	
Pablo Flores	1001668886	Dept. Proyectos	
Marcelo Alvarez	0912478070	Proyectos	
Armando Espinoza	1001352838	Proyectos	
Gerardo Siguencia	1001478138	Control de Gestion	
Mirena Ortiz	0401145545	Comercialización	
L. Lan Navarro	1001789310	Archivo	
Adrian Alvear	1400839324	Agua no Contabilizada	
Alvaro Alvarado	1003469672	Electromecanica	
Gerardo L. Cuenca R.	1103907037	Electromecanica	
Paola Andrade	1002275342	Electromecanica	
Mercedes Enriquez	1001017932	Alcantarillado	
Nelly Bedon T.	1001582255	Dirección Tecnica	
Abgda De la Cruz	1722256203	Dirección Comercial	
Cinthia Moreira	1500736895	Comercialización	
Rocher Escobar Padilla	0400604435	Comercialización	
Fernanda Brito Pineda	0401247879	Comercialización	

Tabla F. 1 Firmas de constancia en la capacitación de la plataforma GLPI

A continuación se detalla la información impartida.

F.1. Ejemplificación del uso del software GLPI

La socialización de los usuarios se detalló de acuerdo al anexo C en la sección C.3.

El proceso de resolución de incidencias que se presenta a continuación se encuentra de acuerdo al manual de procedimientos para la función de administración.

En primer lugar se verifica que los funcionarios presenten sus incidencias por medio de la plataforma GLPI, los cuales se encuentran clasificados de la siguiente manera:

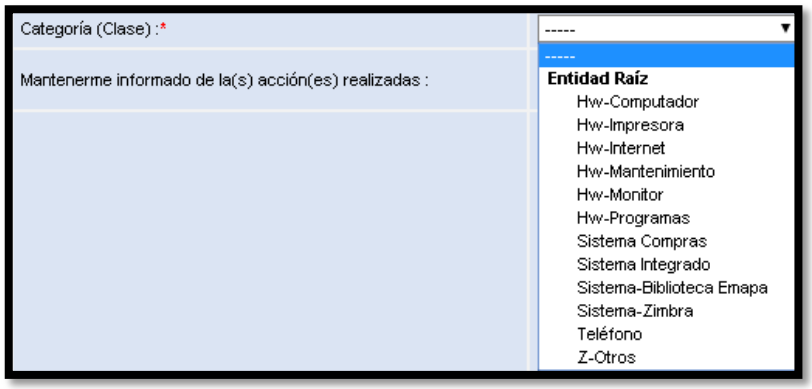


Figura F. 1 Clasificación de los incidentes

El usuario presentará su incidencia de acuerdo a sus necesidades, por ejemplo si la categoría es “computador” la descripción podría ser la siguiente:

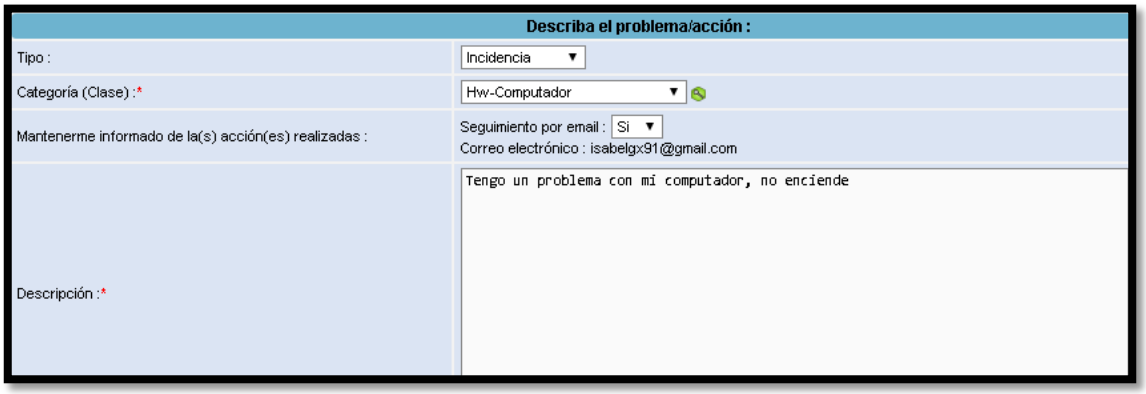


Figura F. 2 Ejemplo de una incidencia de tipo computador

Una vez que el usuario realiza la incidencia por medio de la plataforma web, el administrador por su parte la verificará.

ID	Título	Categoría (Clase)	Estado	Última actualización	Fecha de Apertura	Prioridad	Autor	Asignado a: - Técnico
59	Tengo un problema con mi computador, no enciende	Hw-Computador	En curso (asignada)	2015-12-14 12:18	2015-12-14 12:18	Urgente	Guerron Lucia	
58	FAVOR CONECTAR EL TELÉFONO NEGRO, EN COMUNICACIÓN, YA QUE SE CUENTA CO	Teléfono	En curso (asignada)	2015-12-04 14:39	2015-12-04 14:39	Urgente	Vega Sofia	
57	Conexión de la computadora con la impresora debido a instalaciones	Hw-Computador	En curso (asignada)	2015-12-04 09:25	2015-12-04 09:14	Urgente	Vega Sofia	Paez Dario
53	Por favor revisar el teléfono no salen las llamadas sino una indicació	Teléfono	En espera	2015-12-04 08:57	2015-12-03 12:18	Urgente	Enríquez Teresa	Maldonado Danilo
47	Se necesita la instalación de MS-Project para la elaboración de cronog	Hw-Programas	En curso (asignada)	2015-12-04 08:51	2015-12-02 11:03	Urgente	Vinueza Harold	Paez Dario

Figura F. 3 Plataforma web del administrador de red

En la plantilla de incidencias del administrador, en primer lugar se cambiará el estado a "en curso" y se asignará la incidencia a un técnico de la institución, para que el usuario sea notificado con información del proceso de solución que se está llevando a cabo por el departamento de informática.

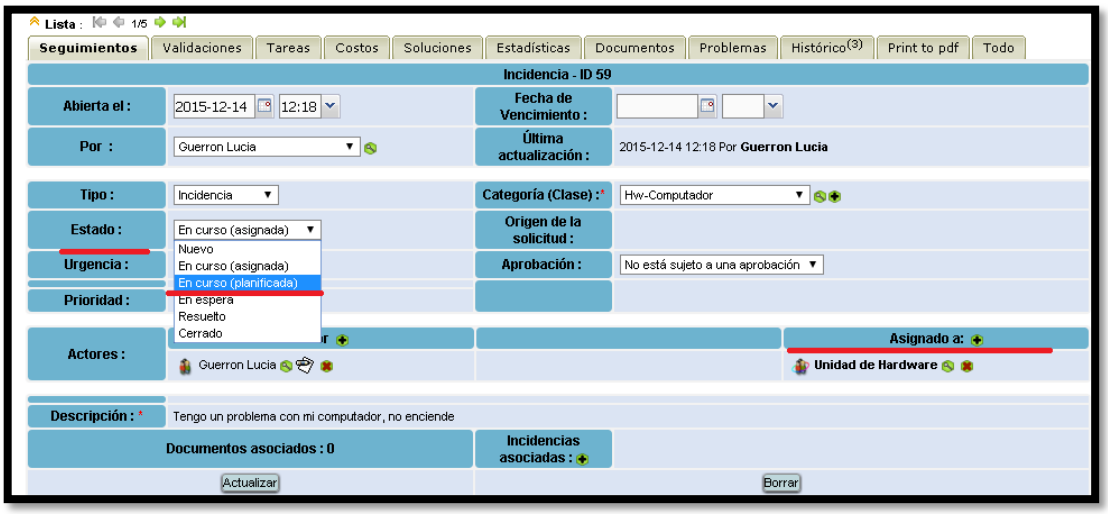


Figura F. 4 Plantilla de incidencias del administrador de red

Se analiza el incidente de forma que demos una solución pronta, siguiendo pasos organizados como son: dirigirse al lugar donde ocurrió el problema, verificar si el problema es eléctrico tanto de la empresa o del equipo, comprobar el estado de los cables de conexión, o examinar el estado de la tarjeta madre, todo esto con el fin de desarrollar una solución.

La solución que proporcionemos, se documentará en la plataforma web, esto nos ayudará en caso de tener problemas similares para dar una respuesta más rápida y también

servirá de guía para el departamento de informática en caso de que un administrador de red no se encuentre en la oficina.

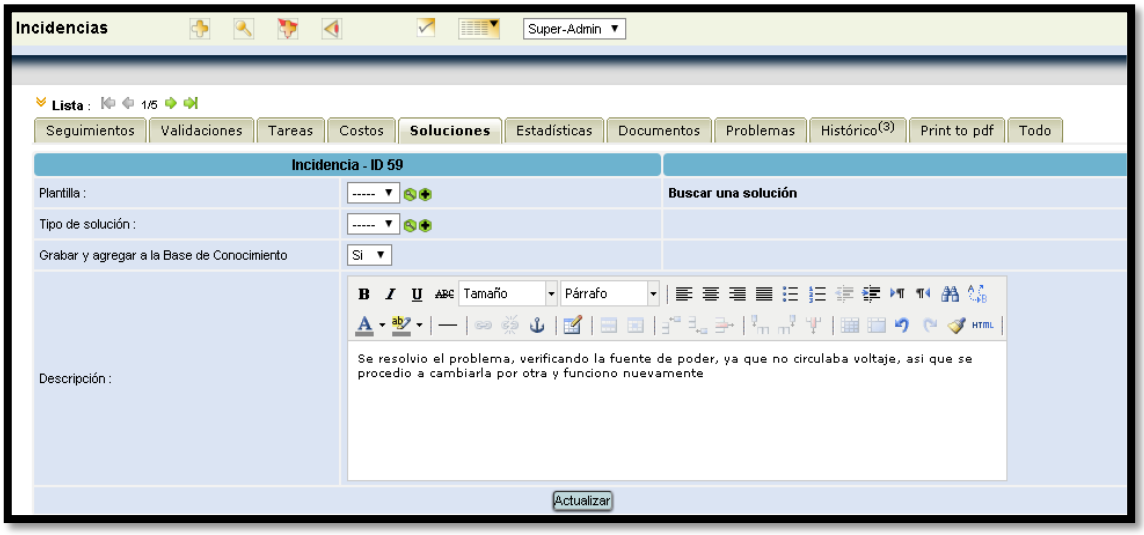


Figura F. 5 Agregamos la solución a la plataforma web

Una vez que solucionamos el problema procedemos a cambiar en la plantilla de incidencias el estado a "resuelto" y agregamos la fecha en la que terminamos de procesar la solución para mantener documentado cada evento realizado.

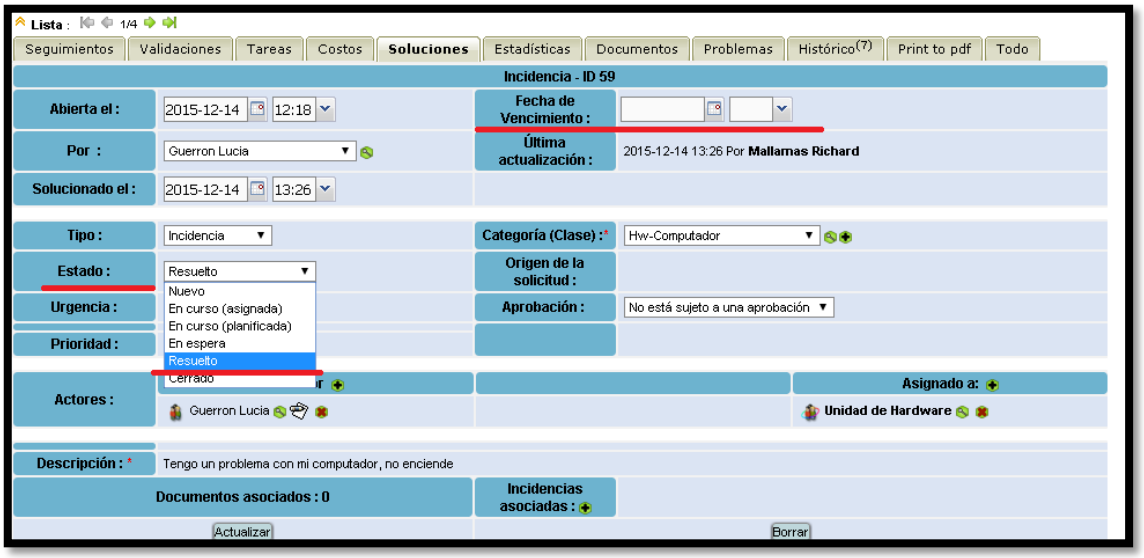


Figura F. 6 Plantilla de incidencias de administrador de red

- **Posibles fallos que pueden encontrarse en la categoría: Computadores**

Según los eventos recurrentes analizados en la empresa, las situaciones podrían ser las siguientes:

- El computador no enciende
- El computador se queda colgado al iniciarse
- El computador se reinicia solo en vez de iniciarse
- No puedo ingresar con mi cuenta de usuario al computador

Para solventar este tipo de inconvenientes en primer lugar el administrador de red, debe dirigirse al lugar donde ocurrió el problema, verificar si el problema es eléctrico tanto de la empresa o del equipo, comprobar el estado de los cables de conexión, o examinar el estado de la tarjeta madre, en caso de revisar el software del computador primero sacar el respectivo respaldo de la información y de ser necesario restablecer o reinstalar el sistema operativo del computador, todo esto con el fin de desarrollar una solución

Una vez que se decide una solución a este incidente procedemos a documentarlo en la plataforma GLPI.

- **Posibles fallos que pueden encontrarse en la categoría: Internet**

Según los eventos recurrentes analizados en la empresa, las situaciones podrían ser las siguientes:

- No tengo internet en mi computador
- El Internet de mi computador esta lento

En primer lugar verificamos la topología de la red, de ser posible verificamos el estado del servidor DNS, o servidor DHCP, mediante la plataforma Zabbix instalada en la institución.

Luego verificamos la conexión con el computador que solicito la revisión, esto se puede realizar mediante una petición “ping”.

Si la petición ping no diera una respuesta, debemos revisar si los cables de conexión se encuentran en perfecto estado y conectados al puerto correcto. Luego se debe verificar si las direcciones IP y máscaras de red están de acuerdo a la red a la que se encuentran.

Se verifica también si el firewall, o el antivirus no estén configurados para impedir un puerto que impida la salida a internet al computador en cuestión.

Una vez que se decide una solución a este incidente procedemos a documentarlo en la plataforma GLPI.

- **Posibles fallos que pueden encontrarse en la categoría: Impresoras**

Según los eventos recurrentes analizados en la empresa, las situaciones podrían ser las siguientes:

- Las hojas salen dobladas y manchadas del lado derecho de tinta
- No puedo imprimir desde mi computadora
- Después del mantenimiento a mi computador, mi impresora no imprime

En primer lugar se debe verificar el estado físico de la impresora, comprobar que ningún componente se encuentre roto o algún objeto este dificulte el buen desenvolvimiento de este dispositivo.

Luego se debe comprobar que la impresora se encuentre en red con el computador, al igual que cuente con los drivers correspondientes.

Una vez que se decide una solución a este incidente procedemos a documentarlo en la plataforma GLPI.

- **Posibles fallos que pueden encontrarse en la categoría: Mantenimiento**

Según los eventos recurrentes analizados en la empresa, las situaciones podrían ser las siguientes:

- Mi computador esta lento
- Los programas no se me abren con normalidad

Para solventar este tipo de inconvenientes en primer lugar el administrador de red, debe dirigirse al lugar donde ocurrió el problema para examinar el estado de la tarjeta madre y sus componentes, en caso de revisar el software del computador primero sacar el respectivo respaldo de la información y de ser necesario restablecer o reinstalar el sistema operativo del computador, todo esto con el fin de desarrollar una solución

Una vez que se decide una solución a este incidente procedemos a documentarlo en la plataforma GLPI.

- **Posibles fallos que pueden encontrarse en la categoría: Monitor**

Según los eventos recurrentes analizados en la empresa, las situaciones podrían ser las siguientes:

- El monitor tiene una línea que se va agrandando poco a poco
- El monitor presenta unas molestas líneas que se mueven constantemente

Para solventar este tipo de inconvenientes en primer lugar el administrador de red, debe dirigirse al lugar donde ocurrió el problema, verificar si el problema es eléctrico tanto de la empresa o del equipo, comprobar el estado de los cables de conexión. Probar si hay problemas similares en computadores cercanos, examinar el lugar para descartar algún elemento que este provocando interferencia electrostática

Una vez que se decide una solución a este incidente procedemos a documentarlo en la plataforma GLPI.

- **Posibles fallos que pueden encontrarse en la categoría: Programas**

Según los eventos recurrentes analizados en la empresa, las situaciones podrían ser las siguientes:

- Se necesita la instalación de MS-Project para la elaboración de cronogramas y seguimiento
- Se necesita la instalación del programa que reproduzca archivos con extensión flv para una exposición que contiene un video con este formato.

En caso de ser necesario se debe revisar la urgencia y la relación de importancia que brinde a la empresa cualquier software que los funcionarios soliciten para proceder con la instalación de un programa

Una vez que se decide una solución a este incidente procedemos a documentarlo en la plataforma GLPI.

- **Posibles fallos que pueden encontrarse en la categoría: Teléfono**

Según los eventos recurrentes analizados en la empresa, las situaciones podrían ser las siguientes:

- No me puedo comunicar con ninguna extensión
- El sonido de la llamada es ruidoso

Para solventar este tipo de inconvenientes en primer lugar el administrador de red, debe dirigirse al lugar donde ocurrió el problema, verificar si el problema es eléctrico tanto de la empresa o del equipo, comprobar el estado de los cables de conexión, en caso de ser necesario reiniciar el servidor de telefonía, todo esto con el fin de desarrollar una solución

Una vez que se decide una solución a este incidente procedemos a documentarlo en la plataforma GLPI.